数理解析研究所講究録
第 1602 巻 2008 年 37-63

UNDECIDABLE INFINITE TOTALLY REAL EXTENSIONS OF $\mathbb{Q}$

KENJI FUKUZAKI

Abstract

Every number fields are known to be undecidable. Nevertheless the only known undecidable infinite algebraic extensions of the rationals are fields whose descriptions depend on non-recursive sets. No 'natural' such fields seem to be known until now.

Let l be a prime such that $l \equiv -1 \pmod 4$ and let $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$. Furthermore let l be a prime such that 2 is a prime element of the ring of algebraic integers in K_l. There are many such primes. We prove that such K_l is undecidable.

1 Previous results

Let $F_n = \mathbb{Q}(\cos(2\pi/l^n))$, where l is an odd prime , and let $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$ ($F_0 = \mathbb{Q}$). Then K_l is an infinite totally real algebraic extension of $\mathbb{Q}$. We say that an algebraic number a is totally real iff a and its conjugates are all real.

In [5] we proved the following theorem. We denote by $\mathfrak{O}_n$ the ring of algebraic integers in F_n and by $\mathfrak{O}_{K_l}$ the ring of algebraic integers in K_l. Then $\mathfrak{O}_{K_l} = \bigcup_n \mathfrak{O}_n$.

Theorem 1 *Let $\varphi(s,u,t)$ be*

$$\exists x, y, z(1 - abt^4 = x^2 - sy^2 - uz^2)$$

and $\psi(t)$ be

$$\forall s, u(\forall c(\varphi(s,u,c) \to \varphi(s,u,c+1)) \to \varphi(s,u,t)),$$

then the solution set of $\psi(t)$ in K_l, $\psi(K_l)$, includes $\mathbb{Z}$ but excludes non-algebraic integers, that is, $\mathbb{Z} \subseteq \psi(K_l) \subseteq \mathfrak{O}_{k_l}$.

In this paper we will prove that $\psi(t)$ defines a subring of $\mathfrak{O}_{K_l}$ if l is a prime such that $l \equiv -1 \pmod 4$ and that furthermore if l is a prime such that 2 is a prime element of $\mathfrak{O}_{K_l}$, then $\mathbb{N}$ is definable in $\psi(K_l)$. In order to prove these facts, we will prove some facts on quadratic characters with polynomial arguments in section 2.

First of all we need the following remark.

Remark 2 We can easily show the following.

Let $0 < n < m$ and $a, b, \alpha \in F_n$ with $ab \neq 0$. Then

$$F_n \models \varphi(a, b, \alpha) \text{ iff } F_m \models \varphi(a, b, \alpha).$$

For if $F_n \models \neg\varphi(a, b, \alpha)$, then $(1 - ab\alpha^4)/(-ab) \in (F_n)^{*2}_{\mathfrak{p}}$ for some $\mathfrak{p}$ a place of F_n such that $(a, b)_{\mathfrak{p}} = -1$. Let $\mathfrak{P}$ be a place of F_m lying above $\mathfrak{p}$. Then we have $(a, b)_{\mathfrak{P}} = -1$ and $(1 - ab\alpha^4)/(-ab) \in (F_m)^{*2}_{\mathfrak{P}}$. Note that for an Archimmedean place $\mathfrak{p} \subset \mathfrak{P}$, it is also true that $(a, b)_{\mathfrak{p}} = 1$ iff $(a, b)_{\mathfrak{P}} = 1$.

Thus we have

$$F_n \models \varphi(a, b, \alpha) \text{ iff } K_l \models \varphi(a, b, \alpha).$$

Note that if we let l be a prime such that $l \equiv -1 \pmod 4$, then above statemants hold for $0 \leq n < m$ since every $[F_n : \mathbb{Q}]$ is odd.

Note also that it is not necessarily true that

$$F_n \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1) \text{ iff } F_m \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1).$$

Therefore it is also not necessarily true that

$$F_n \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1) \text{ iff } K_l \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1).$$

Remark 3 The result for K_l holds also for towers of cyclotomics similarly. Let $M_n = \mathbb{Q}(\zeta_{l^n})$, where l is an odd prime and ζ_{l^n} is a primitive l^n-th root of unity, and let $N_l = \bigcup_n \mathbb{Q}(\zeta_{l^n})$ $(M_0 = \mathbb{Q})$. We denote by $\mathfrak{O}_{N_l}$ the ring of algebraic integers in N_l. Then, $\mathbb{Z} \subseteq \psi(N_l) \subseteq \mathfrak{O}_{N_l}$.

2 quadratic characters with polynomial arguments

In this section, we will prove some facts on some character sums of finite fields, which we will use later. We let $\mathbb{F}_q$ be a finite field with q elements, and $q = p^f$ where p is an odd prime. We let η be the quadratic character of $\mathbb{F}_q$, that is, $\eta(0) = 0, \eta(c) = 1$ if $c \in \mathbb{F}_q^{*2}$ and $\eta(c) = -1$ otherwise.

We consider the following character sum

$$I_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^n + a),$$

where $a \in \mathbb{F}_q$. Moreover we use the following character sum

$$H_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^{n+1} + ac),$$

which is called a Jacobsthal sum. Using these character sums, we will first show that if $\eta(d) = -1$, $p \equiv -1 \pmod 4$ and $p > 3$, then there are $b \in \mathbb{F}_q$ and $i \in \mathbb{F}_p$ such that $\eta(b^4 + d)\eta((b + i)^4 + d) = -1$.

Lemma 4 *Let $p \equiv -1 \pmod 4$, $q = p^f$, and $a \in \mathbb{F}_q$. Then:*

1. *If f is odd, then $I_4(a) = -1$.*
2. *If f is even and $\eta(a) = -1$, then $I_4(a) = -1$.*

Proof. We first note that $q \equiv -1 \pmod 4$ if f is odd and $q \equiv 1 \pmod 4$ if f is even.

For 1., it is proved in [9, pp. 231–232] that $I_2(a) = -1$ for all $a \in \mathbb{F}_q$, $I_{2n}(a) = I_n(a) + H_n(a)$, and if the largest power of 2 dividing $q-1$ also divides n, then $H_n(a) = 0$. Therefore we get that $H_2(a) = 0$ and $I_4(a) = -1$ for all $a \in \mathbb{F}_q$.

For 2., we use the following formula [9, p. 231].

$$I_n(a) = \eta(a) \sum_{j=1}^{d-1} \lambda^j(-a) J(\lambda^j, \eta),$$

where λ is a multicative character of $\mathbb{F}_q$ of order $d = (n, q-1)$ and $J(\lambda^j, \eta)$ is a Jacobi sum, that is,

$$J(\lambda^j, \eta) = \sum_{\substack{c_1+c_2=1 \\ c_1,c_2 \in \mathbb{F}_q}} \lambda^j(c_1)\eta(c_2).$$

Letting $n = 4$, we see that λ is a multiplicative character of order 4, hence $\eta = \lambda^2$. Therefore we see by [9, p. 207] that

$$J(\lambda^2, \eta) = -\frac{1}{q} G(\eta, \chi_1)^2,$$

where $G(\eta, \chi_1)$ is a Gaussian sum. Furthermore we know by [9, p. 199] that

$$G(\eta, \chi_1) = (-1)^{f-1} i^f q^{1/2}.$$

Therefore we get

$$I_4(a) = \eta(a) \left(\lambda(-a)J(\lambda, \eta) - \lambda^2(-a)(-1)^f + \lambda^3(-a)J(\lambda^3, \eta) \right).$$

It is easy to see that $(q-1)/4$ is even, and $\lambda(-1) = -1$ iff $(q-1)/4$ is odd, hence we see that $\lambda(-1) = 1$. Together with $\eta(-1) = (-1)^{(q-1)/2} = 1$ and $\lambda^3 = \overline{\lambda}$, we have

$$I_4(a) = \lambda^3(a)J(\lambda, \eta) + (-1)^{f+1} + \lambda(a)\overline{J(\lambda, \eta)}.$$

Here we have that $\lambda(a) = \pm i$ since $\eta(a) = -1$. Then we have

$$I_4(a) = -1 \pm 2\mathrm{Im} J(\lambda, \eta).$$

We now calculate $\mathrm{Im}J(\lambda,\eta)$ of $\mathbb{F}_q$. Let $J(\lambda,\eta) = A + Bi$. A and B are rational integers since λ assumes only the values $0, \pm 1$ and $\pm i$. By [9, p. 209], we know that $|J(\lambda,\eta)| = q^{1/2}$, hence we have that $A^2 + B^2 = p^f$. It is well-known that for p^f with $p \equiv 3 \pmod 4$ and f even, it is the case that $A = \pm p^{f/2}$ and $B = 0$, or vice versa. However we can show that $A = p^{f/2}$ if $f/2$ is odd, $A = -p^{f/2}$ if $f/2$ is even, and $B = 0$ by the similar way in [9, p. 233], from which $I_4(a) = -1$ follows.

It is proved in [9, p. 232] that

$$H_n(a) = \eta(a)\lambda(-1)\sum_{j=0}^{d-1} \lambda^{2j+1}(a)J(\lambda^{2j+1},\eta),$$

where $d = (n, q-1)$ and λ is a multiplicative character of $\mathbb{F}_q$ of order $2d$. From this formula we get

$$H_2(1) = \lambda(-1)\left(J(\lambda,\eta) + J(\lambda^3,\eta)\right) = \lambda(-1)\left(J(\lambda,\eta) + \overline{J(\lambda,\eta)}\right) = 2\mathrm{Re}J(\lambda,\eta),$$

hence $\mathrm{Re}J(\lambda,\eta) = \frac{1}{2}H_2(1)$.

We will now show that $\frac{1}{2}H_2(1) \equiv -1 \pmod 4$. Let g be a primitive element of $\mathbb{F}_q$ and let $q = 4k+1$. Since $\eta(-1) = 1$ and $-1 = g^{2k}$, we can write

$$\begin{aligned} H_2(1) &= \sum_{i=1}^{4k} \eta(g^i)\eta((g^i)^2+1) \\ &= \sum_{i=1}^{2k} \eta(g^i)\eta((g^i)^2+1) + \sum_{i=1}^{2k} \eta(-g^i)\eta((-g^i)^2+1) \\ &= 2\sum_{i=1}^{2k} \eta(g^i)\eta((g^i)^2+1), \end{aligned}$$

so that

$$\frac{1}{2}H_2(1) = \sum_{i=1}^{2k} \eta(g^i)\eta((g^i)^2+1).$$

From $I_2(1) = -1$ we get

$$-1 = 1 + \sum_{i=1}^{4k} \eta((g^i)^2+1) = 1 + 2\sum_{i=1}^{2k} \eta((g^i)^2+1),$$

hence

$$-1 = \sum_{i=1}^{2k} \eta((g^i)^2+1).$$

By subtraction, we obtain

$$\frac{1}{2}H_2(1)+1=\sum_{i=1}^{2k}(\eta(g^i)-1)\eta((g^i)^2+1).$$

For $1 \le i \le 2k$, we have

$$(\eta(g^i)-1)(\eta((g^i)^2+1)-1)\equiv 0 \pmod 4 \text{ whenever } \eta((g^i)^2+1)\neq 0.$$

Thus,

$$(\eta(g^i)-1)\eta((g^i)^2+1)\equiv \eta(g^i)-1 \pmod 4 \text{ whenever } \eta((g^i)^2+1)\neq 0.$$

Now $\eta((g^i)^2+1)=0$ if and only if $i=k$ or $3k$. Consequently,

$$\begin{aligned}\frac{1}{2}H_2(1)+1 &\equiv \sum_{i=1}^{2k}(\eta(g^i)-1)-(\eta(g^k)-1)\\ &\equiv \sum_{i=1}^{2k}\eta(g^i)-(2k-1)-\eta(g^k) \pmod 4.\end{aligned}$$

Furthermore,

$$0=\sum_{i=1}^{4k}\eta(g^i)=2\sum_{i=1}^{2k}\eta(g^i)$$

and $\eta(g^k)=\lambda^2(g^k)=\lambda(-1)=1$, so that

$$\frac{1}{2}H_2(1)+1\equiv -2k \pmod 4.$$

Since k is even, we see that

$$\frac{1}{2}H_2(1)+1\equiv 0 \pmod 4,$$

as claimed. □

Remark 5 Let $p \equiv -1 \pmod 4), q = p^f$, f even, and $\eta(a)=1$. Then from the proof of the above lemma, we see that $I_4(a)=-1+2\mathrm{Re}J(\lambda,\eta)$ if order of a in $\mathbb{F}_q^*$ is 0 mod 4, $I_4(a)=-1-2\mathrm{Re}J(\lambda,\eta)$ if order of a is 2 mod 4. Note that the value of $I_4(a)$ is independent of the choice of λ. Therefore $I_4(a)=-1\pm 2p^{f/2}$.

Lemma 6 *Let p be an odd prime such that $p \equiv -1 \pmod 4$, and $q = p^f$. Let $a \in \mathbb{F}_q$ and $\eta(a) = -1$. Then:*

1. *If f is even, there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a) = -1$.*
2. *If f is odd and $p > 3$, there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a) = -1$.*
3. *If $f > 1$ is odd and $p = 3$, there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a) = -1$.*

Proof. For 1., we first note that $x^4+a = 0$ has no solutions in $\mathbb{F}_q$ since $\eta(-1) = 1$ and $\eta(-a) = -1$. Suppose not. Then, for any $c \in \mathbb{F}_q$, $\eta(x^4+a)$ assumes the same value for $\{c, c+1, \dots, c+p-1\}$. Therefore, $I_4(a)$ must be 0 mod p, a contradiction.

For 2., we first note that $x^4+a = 0$ has exactly two solutions in $\mathbb{F}_q$, say, $\pm e$, since $\eta(-1) = -1$ and $\eta(a) = -1$.

Suppose not. Then, for any $c \in \mathbb{F}_q$ such that $c \pm e \notin \mathbb{F}_p$, $\eta(x^4+a)$ assumes the same value for $\{c, c+1, \dots, c+p-1\}$.

If $e-(-e) = 2e \notin \mathbb{F}_p$, then $\eta(x^4+a)$ assumes the same value for $\{e, e+1, \dots, e+p-1\}$ except e, and similarly for $\{-e, -e+1, \dots, -e+p-1\}$ except $-e$. Noting that $\eta(-e+j) = -\eta(e-j)$, $I_4(a)$ must be 0 mod p. Thus we get a contradiction since $I_4(a) = -1$.

If $2e \in \mathbb{F}_p$, then it follows that $\pm e, a \in \mathbb{F}_p$. Let η' be the quadratic character of $\mathbb{F}_p$. Then we see that $\eta(c) = \eta'(c)$ for all $c \in \mathbb{F}_p$ since f is odd. Therefore we have

$$\sum_{c \in \mathbb{F}_p} \eta(c^4+a) = \sum_{c \in \mathbb{F}_p} \eta'(c^4+a) = -1$$

So it is not the case that $\eta(x^4+a)$ assumes the same value for $\{0, 1, \dots, p-1\}$ except $\pm e$ since $p \geq 7$. Hence there are $b \in \mathbb{F}_q$ and $i \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+i)^4+a) = -1$.

For 3., we first note that there are no elements $b, j \in \mathbb{F}_3$ such that $\eta(b^4+a)\eta((b+j)^4+a) = -1$, for 2 is the only element such that $\eta(2) = -1$ and $\eta(1^4+2) = \eta(2^4+2) = 0$. And note that $\eta(2) = -1$ also in $\mathbb{F}_{3^f}$.

For the case $a \notin \mathbb{F}_3$, noting that $\pm e \notin \mathbb{F}_3$, we can prove the assertion.

For the case $a = 2$, suppose not. Since $I_4(2) = -1$, $\eta(2) = -1$, and $\eta(1^4+2) = \eta(2^4+2) = 0$, we have $\sum_{c \in \mathbb{F}_{3^f} \setminus \mathbb{F}_3} \eta(c^4+2) = 0$. Let $q = 3^f$. Since the solution of $x^4+2 = 0$ in $\mathbb{F}_q$ are $\{1, 2\}$, the number of the elements of the set $\{c \in \mathbb{F}_q \setminus \mathbb{F}_3 : \eta(c^4+2) = 1\}$ is $(q-3)/2$.

Now we consider the following system of inequations.

$$\begin{aligned} y^2 - x^4 + 1 &\neq 0 \\ z^2 - (x+1)^4 + 1 &\neq 0 \\ w^2 - (x+2)^4 + 1 &\neq 0 \end{aligned}$$

We consider the number of common solutions of these inequations in $\mathbb{F}_q^4$. By assumption we have $\eta(c^4+2) = \eta((c+1)^4+2) = \eta((c+2)^4+2) = 1$ or $\eta(c^4+2) = \eta((c+1)^4+2) = \eta((c+2)^4+2) = -1$ for any $c \in \mathbb{F}_q \setminus \mathbb{F}_3$. Therefore the number of common solutions is $(q-3)/2 \times q^3 + 3q(q-1)^2$, where $3q(q-1)^2$ is the number of common solutions for $x = 0, 1, 2$.

On the other hand, it is proved in [9, p. 275] that if $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is of degree d, then $f(x_1, \ldots, x_n) = 0$ has at most dq^{n-1} solutions in $\mathbb{F}_q^n$. Thus the equation

$$(y^2 - x^4 + 1)(z^2 - (x+1)^4 + 1)(w^2 - (x+2)^4 + 1) = 0$$

has at most $12q^3$ solutions in $\mathbb{F}_q^4$. Hence we get $12q^3 \geq q^4 - q^3(q-3)/2 + 3q(q-1)^2$, a contradiction since $q \geq 3^3 = 27$. □

We cannot establish an explicit formula for $q = p^f$ with $p \equiv 1 \pmod 4$. For example, in $\mathbb{F}_5$, $\eta(2) = -1$ and $I_4(2) = -5$, $\eta(3) = -1$ and $I_4(3) = 3$. Nevertheless we will prove that for $q = p^f$ with $p \equiv 1 \pmod 4$ and f odd, the similar result as above lemma holds.

Lemma 7 *Let $p \equiv 1 \pmod 4$, q a power of p and f be an odd integer. Let $a \in \mathbb{F}_q$ and $\eta(a) = -1$. We denote by $I_4(a)$ and $I_4'(a)$ the character sum in $\mathbb{F}_q$ and $\mathbb{F}_{q^f}$ respectively. Then*

$$I_4(a) \equiv 0 \pmod p \quad \textit{iff} \quad I_4'(a) \equiv 0 \pmod p.$$

Proof. Let $q = p^r$. We again use the formula

$$I_n(a) = \eta(a) \sum_{j=1}^{d-1} \lambda^j(-a) J(\lambda^j, \eta),$$

Letting $n = 4$, we have that

$$J(\lambda^2, \eta) = -\frac{1}{q} G(\eta, \chi_1)^2,$$

as before. But this time we have by [9, p. 199] that

$$G(\eta, \chi_1) = (-1)^{r-1} q^{1/2}.$$

Therefore we get

$$I_4(a) = \eta(a) \left(\lambda(-a) J(\lambda, \eta) - \lambda^2(-a) + \lambda^3(-a) J(\lambda^3, \eta) \right).$$

Since $\eta = \lambda^2$ and $\eta(-1) = 1$, we have

$$I_4(a) = \lambda^3(-a) J(\lambda, \eta) - 1 + \lambda(-a) \overline{J(\lambda, \eta)}.$$

Here we have that $\lambda(-a) = \pm i$ since $\eta(-a) = -1$. Then

$$I_4(a) = \begin{cases} -1 + 2\mathrm{Im}J(\lambda, \eta) & \text{if } \lambda(-a) = i \\ -1 - 2\mathrm{Im}J(\lambda, \eta) & \text{if } \lambda(-a) = -i \end{cases}$$

We can show that $\mathrm{Re}J(\lambda, \eta) = \frac{1}{2}\lambda(-1)H_2(1)$ in the same way as before. We also can show that $\mathrm{Im}J(\lambda, \eta) = \frac{1}{2}\lambda(-1)H_2(d)$ for any $d \in \mathbb{F}_q$ with $\eta(d) = -1$ similarly. Note that $\lambda(-1) = \pm 1$ since $\eta(-1) = 1$. We see that $\lambda(-1) = 1$ if $q \equiv 1 \pmod 8$, and $\lambda(-1) = -1$ if $q \equiv 5 \pmod 8$

At the same time We can show that $\frac{1}{2}H_2(1) \equiv -1 \pmod 4$ in the similar way as before. Further we can show that $\frac{1}{2}H_2(d) \equiv -2k \pmod 4$ with $k = (q-1)/4$ similarly.

It is proved in [9, p. 210] that

$$J(\lambda'_1, \dots, \lambda'_k) = (-1)^{(f-1)(k-1)} J(\lambda_1, \dots, \lambda_k)^f,$$

where $\lambda_1, \dots, \lambda_k$ are multiplicative characters of $\mathbb{F}_q$, not all of which are trivial, and which are lifted to characters $\lambda'_1, \dots, \lambda'_k$, respectively, of $\mathbb{F}_{q^f}$.

We say that λ_j is lifted to λ'_j if $\lambda'(c) = \lambda(\mathrm{N}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(c))$ for all $c \in \mathbb{F}_{q^f}$. The quadratic character of $\mathbb{F}_q$ is lifted to the quadratic character of $\mathbb{F}_{q^f}$, and characters of order 4 of $\mathbb{F}_q$ are lifted to characters of order 4 of $\mathbb{F}_{q^f}$, since $\mathrm{N}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(c) = cc^q \cdots c^{q^{f-1}} = c^{(q^f-1)/(q-1)}$ and $(q^f-1)/(q-1)$ is odd. Furthermore we see that for $c \in \mathbb{F}_q$, $\eta'(c) = \eta(c)$ where η' is the quadratic character of $\mathbb{F}_{q^f}$, so we use the same letter η. Now we consider characters of order 4. Let λ be a character of order 4 of $\mathbb{F}_q$ and let λ be lifted to λ' of $\mathbb{F}_{q^f}$. Note that there are two characters of order 4 which are conjugate. Obviously, for $c \in \mathbb{F}_q$ with $\lambda(c) = \pm 1$, we have that $\lambda'(c) = \pm 1$, respectively. And wealso have that, for $c \in \mathbb{F}_q$ with $\lambda(c) = \pm i$, $\lambda'(c) = \pm i$ if $f \equiv 1 \pmod 4$ respectively, and $\lambda'(c) = \mp i$ if $f \equiv -1 \pmod 4$ respectively.

Consequently, we have that $J(\lambda', \eta) = J(\lambda, \eta)^f$, and that $\lambda'(-a) = \lambda(-a)$ if $f \equiv 1 \pmod 4$, and $\lambda'(-a) = \overline{\lambda(-a)}$ if $f \equiv -1 \pmod 4$.

On the other hand, also in $\mathbb{F}_{q^l}$, we have

$$I_4(a) = \begin{cases} -1 + 2\mathrm{Im}J(\lambda', \eta) & \text{if } \lambda'(-a) = i \\ -1 - 2\mathrm{Im}J(\lambda', \eta) & \text{if } \lambda'(-a) = -i \end{cases}$$

similarly.

Suppose tha $I_4(a) \equiv 0 \pmod p$. We first let $f \equiv -1 \pmod 4$. Let $J(\lambda, \eta) = A + Bi$, $J(\lambda', \eta) = A' + B'i$. If $\lambda(-a) = \pm i$, then $I_4(a) = -1 \pm 2B$ and $I'_4(a) = -1 \mp 2B'$, respectively. Since $J(\lambda', \eta) = J(\lambda, \eta)^f$, we have $A' + B'i = (A + Bi)^f$. Hence we get

$$B' = \binom{f}{1} A^{f-1}B - \binom{f}{3} A^{f-3}B^3 + \cdots + (-1)^{(j-1)} \binom{f}{2j-1} A^{f-(2j-1)}B^{2j-1} + \cdots - B^f.$$

Let $\lambda(-a) = i$. By the assumption that $I_4(a) \equiv 0 \pmod p$, we have $B \equiv 1/2 \pmod p$. On the other hand, by $|J(\lambda, \eta)| = q^{1/2}$, we have $A^2 \equiv -1/4 \pmod p$. Hence we get $B' \equiv -1/2 \pmod p$ and $I'_4(a) = -1 - 2B' \equiv 0 \pmod p$. In case of $\lambda(-a) = -i$, we have that $B' \equiv 1/2 \pmod p$ and $I'_4(a) = -1 - 2B' \equiv 0 \pmod p$.

Secondly, we let $f \equiv 1 \pmod 4$. Then, if $\lambda(-a) = \pm i$, $I_4(a) = -1 \pm 2B$ and $I'_4(a) = -1 \pm 2B'$, respectively. Similarly, we have $I'_4(a) \equiv 0 \pmod p$.

Conversely let $I_4(a) \not\equiv 0 \pmod p$. In case that $f \equiv -1 \pmod 4$ and $\lambda(-a) = i$, we have that $B \equiv s \pmod p$ with $s \neq 1/2$ and $B' \equiv -2^{f-1}s^f \pmod p$. We easily see that $-2^{f-1}s^f \not\equiv -1/2 \pmod p$ and $I'_4(a) \not\equiv 0 \pmod p$. Similarly for other cases. □

In $\mathbb{F}_5$, there is $a \in \mathbb{F}_5$ with $\eta(a) = -1$ such that $I_4(a) \equiv 0 \pmod 5$: take $a = 2$, then $\eta(2) = \eta(1+2) = \eta(2^4+2) = \cdots = \eta(4^4+2) = -1$. Thus we have $I_4(2) \equiv 0 \pmod 5$ in $\mathbb{F}_{5^f}$ with f odd. For primes greater than 5, we have the following:

Lemma 8 *Let p be a prime greater than 5, then $I_4(a) \not\equiv 0 \pmod p$ in $\mathbb{F}_p$ for any $a \in \mathbb{F}_p$.*

Proof. From the formula

$$I_n(a) = \eta(a) \sum_{j=1}^{d-1} \lambda^j(-a) J(\lambda^j, \eta),$$

we get $|I_4(a)| \leq (d-1)p^{1/2}$, where $d = (4, p-1)$. Hence $|I_4(a)| \leq 3\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $|I_4(a)| \leq \sqrt{p}$ if $p \equiv -1 \pmod 4$. Therefore $|I_4(a)| < p-2$, and the assertion follows since $x^4 + a$ has possively two solutions in case of $p \equiv -1 \pmod 4$ and $\eta'(a) = -1$ where η' is the quadratic character of $\mathbb{F}_p$. □

Lemma 9 *Let p be an odd prime such that $p \equiv 1 \pmod 4$ with $p \neq 5$, and $q = p^f$ with f odd. Let $a \in \mathbb{F}_q$ and $\eta(a) = -1$. Then $I_4(a) \not\equiv 0 \pmod p$.*

Proof. Suppose that $I_4(a) \equiv 0 \pmod p$. First we recall

$$I_4(a) = \begin{cases} -1 + 2\mathrm{Im}J(\lambda, \eta) & \text{if } \lambda(-a) = i \\ -1 - 2\mathrm{Im}J(\lambda, \eta) & \text{if } \lambda(-a) = -i. \end{cases}$$

This formula shows that the value $I_4(a)$ depends only on the value of $\lambda(-a)$. We easily see that there is a $c \in \mathbb{F}_p$ such that $\lambda(c) = \lambda(a)$. Then we have $I_4(c) \equiv 0 \pmod p$ in $\mathbb{F}_q$. It follows that $I_4(a) \equiv 0 \pmod p$ in $\mathbb{F}_p$ since f is odd, a contradiction. □

Lemma 10 *Let $p \neq 5$ be an odd prime such that $p \equiv 1 \pmod 4$, and $q = p^f$ with f odd. Let $a \in \mathbb{F}_q$ and $\eta(a) = -1$. Then there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4 + a)\eta((b+j)^4 + a) = -1$.*

Proof. We first note that $x^4 + a = 0$ has no solutions in $\mathbb{F}_q$ since $\eta(-1) = 1$ in $\mathbb{F}_q$. The assertion follows from the above lemma. □

For $p = 5$ we have $I_4(2) \equiv 0 \pmod 5$ in all $\mathbb{F}_{5^f}$ with f odd. However it is true that there are $b \in \mathbb{F}_{5^f}$ and $j \in \mathbb{F}_5$ such that $\eta(b^4 + a)\eta((b + j)^4 + a) = -1$ for any $a \in \mathbb{F}_{5^f}$ with $\eta(a) = -1$ if f is odd and $f > 1$.

Lemma 11 *Let $f > 1$ be odd. Let $a \in \mathbb{F}_{5^f}$ and $\eta(a) = -1$. Then there are $b \in \mathbb{F}_{5^f}$ and $j \in \mathbb{F}_5$ such that $\eta(b^4 + a)\eta((b + j)^4 + a) = -1$.*

Proof. We again use the same letter η for the quadratic characters of $\mathbb{F}_5$ and $\mathbb{F}_{5^f}$. Let λ_0 be the multiplicative character of of order 4 in $\mathbb{F}_5$ such that $\lambda_0(2) = i$ and let λ_0 be lifted to λ of $\mathbb{F}_{5^f}$.

We first note that $\lambda(-1) = -1$ and $\lambda(a) = \pm i$ since $\eta(a) = -1$. Suppose that $\lambda(a) = -i$. Then we see that $I_4(a) \not\equiv 0 \pmod p$ since $I_4(3) = -i$ and $I_4(3) = 3$. The assertion follows similarly.

Suppose that $\lambda(a) = i$. We now evaluate $I_4(a)$. We easily see that $J(\lambda_0, \eta) = 1+2i$, hence $J(\lambda, \eta) = (1 + 2i)^f$. Letting $J(\lambda, \eta) = A + Bi$, we have

$$B = \binom{f}{1}2 - \binom{f}{3}2^3 + \cdots + (-1)^{j-1}\binom{f}{2j-1}2^{2j-1} + \cdots + (-1)^{(f-1)/2}2^f.$$

Hence we have $-(3^f+1)/2 < B < (3^f+1)/2$. We know that $I_4(a) = -1+2\mathrm{Im}J(\lambda, \eta)$ since $\lambda(-a) = -i$. Thus we see that $-3^f - 2 < I_4(a) < 3^f$. Let $C = \{c \in \mathbb{F}_{5^f} : \eta(c^4 + a) = -1\}$ and let N be the number of elements of C. We see that $N < (5^f + 3^f + 1)/2$ since $|I_4(a)| < 3^f$. Suppose that the assertion does not hold for a. Then it follows that $\eta((c+i)^4+a) = 1 (i = 0, 1, 2, 3, 4)$ for $c \in \mathbb{F}_{5^f} \backslash C$ and $\eta((c+i)^4+a) = -1 (i = 0, 1, 2, 3, 4)$ for $c \in C$. Therefore the equation

$$\prod_{0 \leq i \leq 4} (y_i - x^4 - a) = 0$$

has at least $5^{6f} - 5^{5f}(5^f + 3^f + 1)/2$ solutions in $\mathbb{F}_{5^f}^6$. We know that this equation has at most $20(5^f)^5$ solutions by [9, p. 275]. Thus we have

$$20 \cdot 5^{5f} \geq 5^{6f} - 5^{5f}(5^f + 3^f + 1)/2.$$

It follows that $5^f - 3^f - 41 \leq 0$, a contradiction since $f \geq 3$. □

For $q = p^f$ with f even, we can show that If $I_4(a) \equiv 0 \pmod p$, then $I_4'(a) \equiv -2 \pmod p$ but we can say no more. Note that there is no $c \in \mathbb{F}_p$ such that $\lambda(c) = \lambda(a)$.

However we are interested in residue fields of completions of $F_n = \mathbb{Q}(\cos(2\pi/l^n)$ where l odd prime and $l \equiv -1 \pmod 4$.

Lemma 12 *Let $l > 3$ be an odd prime such that $l \equiv -1 \pmod 4$ and $F_n = \mathbb{Q}(\cos(2\pi/l^n))$ with $n \geq 0$. Let $\mathfrak{p}$ be a prime of f_n lying above a rational prime p with $p \not| 2$. We denote by $\overline{F_n}$ the residue field of $(F_n)_{\mathfrak{p}}$. Let $a \in \overline{F_n}$ and $\eta(a) = -1$. Then there are $b \in \overline{F_n}$ and $j \in \{1, 2, \ldots, p-1\}$ such that $\eta(b^4 + a)\eta((b+j)^4 + a) = -1$.*

Proof. Let f be the residue degree of $\mathfrak{p}$. Then $\overline{F_n} = \mathbb{F}_{p^f}$ and f is odd since $[F_n : \mathbb{Q}]$ is odd. The assertion follows from Lemma 6, 8, 10, 11. □

3 The structure of $\psi(K_l)$.

In this section we let l be an odd prime. We begin with the following lemma.

Lemma 13 *Let p be a rational prime other than l. Then p decomposes into only finitely many factors in $\mathfrak{O}_{K_l}$, the ring of algebraic integers of $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$. And p is unramified in K_l. Furthermore there is n_0 such that for $n \geq n_0$, p decomposes into the same number of factors in $\mathfrak{O}_n$ as in $\mathfrak{O}_{K_l}$.*

Proof. Take $\mathfrak{p}_n$ such that $\mathfrak{p}_n$ is a prime of F_n and $p \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{p}_3 \subset \cdots$, and denote by f_n the residue degree of F_n at $\mathfrak{p}_n$. Then $\mathbb{F}_{p^{f_n}} = \mathfrak{O}_n/\mathfrak{p}_n$. We denote $\mathbb{F}_{p^{f_n}}$ by $\bar{F}_n$. Obviously, $\mathbb{F}_p \subseteq \bar{F}_1 \subseteq \bar{F}_2 \subseteq \cdots$.

Let $\mathfrak{p}'$ be a prime of $M_n = \mathbb{Q}(\zeta_{l^n})$ lying above a rational prime p and let f'_n be the residue degree of $\mathfrak{p}'$. Then f'_n is the smallest positive integer f such that $p^f \equiv 1 \pmod{l^n}$. Let $p^{f'_1} = 1 + kl$. We easily see that if $\gcd(k, l) = 1$, then $f'_n = f'_1 l^{n-1}$ for all n, and if $k = l^b q$ with $\gcd(q, l) = 1$ and $b > 1$, then $f'_1 = f'_2 = \cdots = f'_{b+1}$ and $f'_{b+h} = f'_1 l^{h-1}$ if $h > 1$. In either case, there is n_0 such that $f'_{m+1} = f'_m l$ for all $m \geq n_0$. Let $f'_n g'_n = l^{n-1}(l-1)$. There are exactly g'_n extensions of p to M_n. We see that $g'_{n_0} = g'_{n_0+1} = g'_{n_0+2} = \cdots$. Let $f_n g_n = l^{n-1}(l-1)/2$. Then there are exactly g_n extensions of p to F_n. We see that $f_n | f'_n$ and $g_n | g'_n$. If $f_{n_0} = f'_{n_0}/2$, then we have $g'_{n_0} = g_{n_0} = g_{n_0+1} = g_{n_0+2} = \cdots$ and $f_{m+1} = f_m l$ for all $m \geq n_0$. If $f_n = f'_n$, then we have $g'_{n_0}/2 = g_{n_0} = g_{n_0+1} = g_{n_0+2} = \cdots$ and $f_{m+1} = f_m l$ for all $m \geq n_0$. Thus in either case, we have $f_{m+1} = f_m l$ and p has exactly g_{n_0} factors in F_m for all $m \geq n_0$.

Let $(p) = \mathfrak{p}_{n_0}^{(1)} \mathfrak{p}_{n_0}^{(2)} \cdots \mathfrak{p}_{n_0}^{(g_{n_0})}$ in F_{n_0} and let $\mathfrak{P}_i = \mathfrak{p}_{n_0}^{(i)} \mathfrak{O}_{K_l}$ for each i. Then $\mathfrak{P}_i$ are unramified prime factors of p in $\mathfrak{O}_{K_l}$. □

We will prove that $\psi(t)$ defines a subring of $\mathfrak{O}_{K_l}$ in K_l if $l \equiv -1 \pmod 4$.

We note that if $\eta(c) = 1$ in $\bar{F}_n$ with $n \geq 1$, then $\eta(c) = 1$ in $\bar{F}_m$ for all $m > n$, and similarly for $\eta(c) = -1$ in $\bar{F}_n$. So we use the same symbol η for quadratic characters of all $\bar{F}_n$ with $n \geq 1$. We denote by η' the quadratic character of $\mathbb{F}_p$. Note that if $l \equiv -1 \pmod 4$, then $\eta'(c) = \eta(c)$ for all $c \in \mathbb{F}_p$ since $[F_1 : \mathbb{Q}] = (l-1)/2$ is odd. Note also that in case of $l \equiv 1 \pmod 4$, $\eta(c) = 1$ for all $c \in \mathbb{F}_p$ if f_1 is even.

We recall that $\psi(t)$ is a formula

$$\forall s,u(\forall c(\varphi(s,u,c)\rightarrow\varphi(s,u,c+1))\rightarrow\varphi(s,u,t)),$$

and $\varphi(s,u,t)$ is a formula

$$\exists x,y,z(1-abt^4=x^2-sy^2-uz^2).$$

Furthermore we let $\theta(s,u)$ be a formula

$$\forall c(\varphi(s,u,c)\rightarrow\varphi(s,u,c+1).$$

For $a,b\in F_n$ we denote by $S_n(a,b)$ the set of places $\mathfrak{p}$ of F_n such that $(a,b)_{\mathfrak{p}}=-1$.

By the proof of Theorem 1, we know that there are $a,b\in K_l$ such that

$$\begin{aligned} K_l &\models \forall c(\varphi(a,b,c)\rightarrow\varphi(a,b,c+1)) \text{ and}\\ K_l &\models \exists x,y,z(1-ab\alpha^4=x^2-sy^2-uz^2) \text{ for any } \alpha\in\mathfrak{O}_{k_l},\end{aligned}$$

and such that if $a,b\in F_n$, then $\nu_{\mathfrak{p}}(-ab)=1$ for all $\mathfrak{p}\in S_n(a,b)$ with $\mathfrak{p}\not| l$.

We will prove that almost $a,b\in K_l^*$ with $K_l\models\theta(a,b)$ satisfy $K_l\models\varphi(a,b,\alpha)$ for all $\alpha\in\mathfrak{O}_{k_l}$.

From now on the ring of integers of $(F_n)_{\mathfrak{p}}$ is denoted by $(\mathfrak{o}_n)_{\mathfrak{p}}$, its maximal ideal is also denoted by $\mathfrak{p}$, its residue field $(\mathfrak{o}_n)_{\mathfrak{p}}/\mathfrak{p}$ by $\overline{(F_n)_{\mathfrak{p}}}$, and the group of units in $(\mathfrak{o}_n)_{\mathfrak{p}}$ by $(U_n)_{\mathfrak{p}}$. For $\alpha\in\mathbb{F}_n$, we denote by $\bar{\alpha}$ its residue class in $\overline{(F_n)_{\mathfrak{p}}}$. Furthermore we let $\mathfrak{p}$ lie above a rational prime p. Note that $\overline{(F_n)_{\mathfrak{p}}}\simeq\mathfrak{O}_n/\mathfrak{p}\simeq\mathbb{F}_{p^f}$ where f is the residue degree of F_n at $\mathfrak{p}$.

We note that for $a,b\in F_n^*$, $F_n\models\neg\varphi(a,b,\alpha)$ iff $\alpha^4-1/ab\in(F_n)_{\mathfrak{p}}^{*2}$ for some $\mathfrak{p}\in S_n(a,b)$.

Lemma 14 *Let $a,b\in F_n^*$ such that*

$$K_l\models\forall c(\varphi(a,b,c)\rightarrow\varphi(a,b,c+1))$$

holds. Then every $\mathfrak{p}\in S_n(a,b)$ is not Archimedean.

Proof. Let $\mathfrak{p}\in S_n(a,b)$. Suppose that $\mathfrak{p}$ is Archimedian. Then there is $m\in\mathbb{N}$ such that $m^4-1/ab\in(F_n)_{\mathfrak{p}}^{*2}$. We can take $n_1>n$ such that $F_{n_1}\models\varphi(a,b,m)$ since $K_l\models\varphi(a,b,m)$. Let $\mathfrak{p}'$ be a place of F_{n_1} lying above $\mathfrak{p}$. Then we have $m^4-1/ab\in(F_{n_1})_{\mathfrak{p}'}^{*2}$. Since $(F_n)_{\mathfrak{p}}=(F_{n_1})_{\mathfrak{p}'}\simeq\mathbb{R}$, we have $(a,b)_{\mathfrak{p}'}=-1$. Hence we have $F_{n_1}\models\neg\varphi(a,b,m)$, a contradiction. Therefore $\mathfrak{p}$ is not Archimedean. □

Lemma 15 *Let $n\geq 1$. Let $a,b\in F_n^*$, $\alpha\in\mathfrak{O}_n$ and $\mathfrak{p}_0\in S_n(a,b)$ with $\mathfrak{p}_0\not| 2$ such that*

1. $K_l\models\forall c(\varphi(a,b,c)\rightarrow\varphi(a,b,c+1))$ and

2. $\alpha^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$ *hold.*

Then $\nu_{\mathfrak{p}_0}(-ab) = 0$.

Proof. We note that $-ab \notin (F_n)^{*2}_{\mathfrak{p}_0}$ since $(a,b)_{\mathfrak{p}_0} = (a,-ab)_{\mathfrak{p}_0} = -1$. We have that by Remark 2, $F_n \models \varphi(a,b,1)$ since $K_l \models \varphi(a,b,1)$. Then we have

$$(1-ab)/(-ab) = 1 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}.$$

It is known that $1+\mathfrak{p} = (1+\mathfrak{p})^2$ for $\mathfrak{p} \not| 2$ in $\mathfrak{p}$-adic fields ([10, p. 163]). Hence we have $\nu_{\mathfrak{p}_0}(-1/ab) \leq 0$, so $\nu_{\mathfrak{p}_0}(-ab) \geq 0$. On the other hand, we have

$$(1-ab\alpha^4)/(-ab) = \alpha^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$$

If $\nu_{\mathfrak{p}_0}(-ab) > 0$, then $1 - ab\alpha^4 \in (F_n)^{*2}_{\mathfrak{p}_0}$ since $\alpha \in \mathfrak{O}_n$, hence $-ab \in (F_n)^{*2}_{\mathfrak{p}_0}$, a contradiction since $(a,b)_{\mathfrak{p}_0} = -1$. Therefore we have $\nu_{\mathfrak{p}_0}(-ab) = 0$. □

Lemma 16 *Let $l > 3$ be an odd prime such that $l \equiv -1 \pmod 4$. Let $a,b \in F_n^*$. Suppose that $S_n(a,b)$ contains a $\mathfrak{p}_0$ such that $\mathfrak{p}_0 \not| 2$, and $\nu_{\mathfrak{p}_0}(-ab) = 0$.*

Then $K_l \models \neg\forall c(\varphi(a,b,c) \to \varphi(a,b,c+1))$.

Proof. Using $\varphi(a,b,c) \leftrightarrow \varphi(a,b,-c)$, we see that for any $j \in \mathbb{Z}$,

$$K_l \models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1)) \text{ iff } K_l \models \forall c(\varphi(a,b,c) \leftrightarrow \varphi(a,b,c+j)).$$

It is known that for $\alpha \in (U_n)_{\mathfrak{p}}$ with $\mathfrak{p} \not| 2$, $\alpha \in (F_n)^{*2}_{\mathfrak{p}}$ iff $\eta(\bar{\alpha}) = 1$ in $\overline{(F_n)_{\mathfrak{p}}}$. Hence we see that $\eta(\overline{-1/ab}) = -1$ in $\overline{(F_n)^{*2}_{\mathfrak{p}_0}}$ since $(a,b)_{\mathfrak{p}_0} = -1$.

Let $\mathfrak{p}_0|p$ and $d = -1/ab$. By Lemma 12, there are $\bar{b} \in \overline{(F_n)_{\mathfrak{p}_0}}$, and $j_0 \in \{1,\dots,p-1\}$ such that $\eta(\bar{b}^4+\bar{d})\eta((\bar{b}+\bar{j}_0)^4+\bar{d}) = -1$ in $\overline{(F_n)_{\mathfrak{p}_0}}$. We may assume that $\eta(\bar{b}^4+\bar{d}) = -1$ and $\eta((\bar{b}+\bar{j}_0)^4+\bar{d}) = 1$ without of loss of generality.

We can take $\beta \in \mathfrak{O}_{n_0}$ such that $\bar{\beta} = \bar{b}$ since $\mathfrak{O}_{n_0}/\mathfrak{p}_0 \simeq (\mathfrak{o}_n)_{\mathfrak{p}_0}/\mathfrak{p}_0$. Let $S_n(a,b) = \{\mathfrak{p}_0,\dots,\mathfrak{p}_k\}$. By the Chinese Remainder Theorem, there is $\gamma \in \mathfrak{O}_n$ such that

$$\begin{aligned} \gamma &\equiv \beta \pmod{\mathfrak{p}_0} \\ \gamma &\equiv 0 \pmod{\mathfrak{p}_i} \text{ if } i \neq 0. \end{aligned}$$

Since $\bar{\gamma} = \bar{\beta}$ in $\overline{(F_n)_{\mathfrak{p}_0}}$, we have that $\gamma^4 - 1/ab \equiv \beta^4 - 1/ab \pmod{\mathfrak{p}_0}$. Let $A = \gamma^4 - 1/ab$ and $B = \beta^4 - 1/ab$. Noting that $\beta^4 - 1/ab$ is a unit at $\mathfrak{p}_0$ since $\eta(\bar{\beta}^4 - 1/\bar{a}\bar{b}) \neq 0$, we have $A/B \equiv 1 \pmod{\mathfrak{p}_0}$. Since $(1+\mathfrak{p})^2 = 1+\mathfrak{p}$ if $\mathfrak{p} \not| 2$ in $\mathfrak{p}$-adic fields, we have $\gamma^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}$. Let $i \neq 0$. Since $(a,b)_{\mathfrak{p}_i} = (a,-ab)_{\mathfrak{p}_i} = -1$, we have $-1/ab \notin (F_n)^{*2}_{\mathfrak{p}_i}$. Since

$$\gamma^4 - 1/ab \equiv -1/ab \pmod{\mathfrak{p}_i^4}$$

and $\nu_{\mathfrak{p}_i}(-1/ab) = 0$, we have $\gamma^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_i}$ as before. Consequently we have that $F_n \models \varphi(a, b, \gamma)$, hence $K_l \models \varphi(a, b, \gamma)$.

Now since $\eta((\bar{b}+j_0)^4+\bar{d}) = 1$ in $\overline{(F_n)}_{\mathfrak{p}_0}$, we see that $(\gamma+j_0)^4-1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$, hence we have that $F_n \models \neg\varphi(a, b, \gamma+j_0)$. Then by Remark 2, we have $K_l \models \neg\varphi(a, b, \gamma+j_0)$.

Thus we have $K_l \models \varphi(a, b, \gamma) \wedge \neg\varphi(a, b, \gamma + j_0)$. □

Lemma 17 *Let $l = 3$. Let $a, b \in F_n^*$. Suppose that $S_n(a, b)$ contains a $\mathfrak{p}_0$ such that $\mathfrak{p}_0 \not| 2$ and $\nu_{\mathfrak{p}_0}(-ab) = 0$.*

Then $K_l \models \neg\forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1))$.

Proof. In case that $\mathfrak{p}_0 \not| 3$, we can prove the assertion as before by Lemma 6, since $3 \equiv -1 \pmod 4$. Next we let $\mathfrak{p}_0 | 3$. This time we cannot use Lemma 8. Let $\iota = 2 - 2\cos(2\pi/3^n)$. Then $\mathfrak{p}_0 = \mathfrak{l} = (\iota)$. Let $\iota' = 2 - 2\cos(2\pi/3^{n+1})$. Then $\mathfrak{l}' = (\iota')$ is the only one prime of F_{n+1} lying above $\mathfrak{l}$ and $\mathfrak{l} = \mathfrak{l}'^3$. We know that the residue field of $(F_n)_\mathfrak{l}$ is $\mathbb{F}_3$ and that of $(F_{n+1})_{\mathfrak{l}'}$ is also $\mathbb{F}_3$. Since $\nu_\mathfrak{l}(-ab) = 0$ and $-1/ab \notin (F_n)_\mathfrak{l}$, we have, as an element of $(F_n)_\mathfrak{l}$ and of $(F_{n+1})_{\mathfrak{p}_0}$,

$$\begin{aligned} -1/ab &= -1 + c_1\iota + c_2\iota^2 + c_3\iota^3 + \cdots \\ &= -1 + c_3'\iota'^3 + c_4'\iota'^4 + c_5'\iota'^5 + \cdots, \end{aligned}$$

where $c_i, c_i' \in \{\pm 1, 0\}$. Let $\beta' = \iota'^2$. We easily see that $\beta'^4 - 1/ab \notin (F_{n+1})_{\mathfrak{l}'}$ and $(\beta'+1)^4-1/ab \in (F_{n+1})_{\mathfrak{l}'}$. Similarly as before we have $K_l \models \varphi(a, b, \gamma') \wedge \neg\varphi(a, b, \gamma'+1)$ for some $\gamma' \in \mathfrak{O}_{n+1}$. □

The similar result for $l = 5$ fails to hold; we can construct $a, b \in F_n^* \subset K_5$ such that $S_n(a, b)$ contains $\mathfrak{p}_0 = (2-2\cos(2\pi/5^n))$, $\nu_{\mathfrak{p}_0}(-ab) = 0$ and $K_5 \models \forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1)$ holds.

By the above lemmas and Remark 2, we see that, letting l be an odd prime such that $l \equiv -1 \pmod 4$, for $a, b \in F_n^*$, if $S_n(a, b)$ contains no primes dividing 2, then

$$K_l \models \forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1)) \to \varphi(a, b, \alpha) \quad \text{for all } \alpha \in \mathfrak{O}_{K_l}.$$

Lemma 18 *Let $n \geq 1$. Let $a, b \in F_n^*$, $\alpha \in \mathfrak{O}_n$ and $\mathfrak{p}_0 \in S_n(a, b)$ with $\mathfrak{p}_0 | 2$ such that*

1. *$K_l \models \forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1))$ and*
2. *$\alpha^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$ hold.*

Then $\nu_{\mathfrak{p}_0}(-ab) = \pm 2$.

Proof. We first note that $\nu_{\mathfrak{p}_0}(2) = 1$ since $\mathfrak{p}_0$ is unramified. We have

$$\begin{aligned} & & -1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0} & \qquad (1) \\ (1 - ab)/(-ab) &=& 1 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0} & \qquad (2) \\ (1 - ab\alpha^4)/(-ab) &=& \alpha^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0} & \qquad (3) \end{aligned}$$

It is known that $(1+\mathfrak{p}^r)^2 = 1+2\mathfrak{p}^r$ if $\mathfrak{p}^r \subseteq 2\mathfrak{p}$ in $\mathfrak{p}$-adic fields([10, p. 163]). So we have $1+\mathfrak{p}_0^3 = (1+\mathfrak{p}_0^2)^2$. Hence we have $\nu_{\mathfrak{p}_0}(-1/ab) < 3$ by (2) and $\nu_{\mathfrak{p}_0}(-ab) < 3$ by (3). It follows that $-3 < \nu_{\mathfrak{p}_0}(-ab) < 3$. Further we see that $0 \leq \nu_{\mathfrak{p}_0}(\alpha) < 2$ by (3). If $\nu_{\mathfrak{p}_0}(-1/ab) = -1$, then we have $\nu_{\mathfrak{p}_0}(\alpha^4 - 1/ab) = -1$, a contradiction since $\alpha^4 - 1/ab \in (F_{n_0})^{*2}_{\mathfrak{p}_0}$. Therefore we have $\nu_{\mathfrak{p}_0}(-1/ab) = -2, 0, 1$ or 2.

Let C be the group of $(N\mathfrak{p}-1)^{th}$ roots of unity in $(F_n)_{\mathfrak{p}_0}$. Every elements of C are squares in $(F_n)_{\mathfrak{p}_0}$. Let $C' = C \cup \{0\}$. Let $\delta \in (U_n)_{\mathfrak{p}_0}$. We can wright $\delta = c_0 + c_1 2 + c_2 2^2 + \cdots$, for some $c_i \in C'$ with $c_0 \neq 0$. We easily see that $\delta \in (F_n)^2_{\mathfrak{p}_0}$ iff $c_1 = 0$ and $c_2/c_0 \equiv c(c+1) \pmod{\mathfrak{p}_0}$ for some $c \in C'$.

Let $\nu_{\mathfrak{p}_0}(-1/ab) = 1$. In case $\nu_{\mathfrak{p}_0}(\alpha) = 0$, we have $\alpha^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}$ since $\alpha^4 \equiv c_0^4 \pmod{\mathfrak{p}_0^3}$ for some $c_0 \neq 0$ in C. Hence we see that $\nu_{\mathfrak{p}_0}(-1/ab) \neq 1$ by (3). In case $\nu_{\mathfrak{p}_0}(\alpha) = 1$, we have $\nu_{\mathfrak{p}_0}(\alpha^4 - 1/ab) = 1$, a contradiction since $\alpha^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$. Accordingly $\nu_{\mathfrak{p}_0}(-1/ab) = 0$ or ± 2.

Now we will show that $\nu_{\mathfrak{p}_0}(-1/ab) \neq 0$. Suppose that $\nu_{\mathfrak{p}_0}(-1/ab) = 0$.

We have $\nu_{\mathfrak{p}_0}(\alpha) = 0$ or 1. Suppose that $\nu_{\mathfrak{p}_0}(\alpha) = 1$. Since

$$\alpha^4 - 1/ab \equiv -1/ab \pmod{\mathfrak{p}_0^4}$$

and $\nu_{\mathfrak{p}_0}(-1/ab) = 0$, we have $\alpha^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}$ as before. Hence we see that $\nu_{\mathfrak{p}_0}(\alpha) = 0$.

Let $\nu_{\mathfrak{p}_0}(\alpha^4 - 1/ab) = s$. We see that $s \geq 0$ and s is even since $\nu_{\mathfrak{P}_0}(-ab) = 0$ and $\alpha^4 - 1/ab \in (F_m)^{*2}_{\mathfrak{P}}$.

<u>Case 1</u>: $s = 0$.

We let $\gamma \in \mathfrak{O}_n$ such that

$$\begin{aligned} \gamma &\equiv \alpha \pmod{\mathfrak{p}_0} \\ \gamma &\equiv -1 \pmod{\mathfrak{p}} \text{ if } \mathfrak{p} \in S_n(a,b),\ \mathfrak{p} \neq \mathfrak{p}_0. \end{aligned}$$

Then we have $\gamma^4 \equiv \alpha^4 \pmod{\mathfrak{p}_0^3}$ and that

$$\alpha^4 - 1/ab \equiv \gamma^4 - 1/ab \pmod{\mathfrak{p}_0^3}.$$

Therefore we see that $\gamma^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$ similarly as before. We also have

$$-1/ab \equiv (\gamma+1)^4 - 1/ab \pmod{\mathfrak{p}^4} \text{ if } \mathfrak{p} \neq \mathfrak{p}_0.$$

Thus we see that $(\gamma+1)^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}}$ for $\mathfrak{p} \neq \mathfrak{p}_0$.

We will show that $(\alpha+1)^4 - 1/ab$ is not a square in $(F_n)_{\mathfrak{p}_0}$. Let C be the group of $(N\mathfrak{p}_0 - 1)^{th}$ roots of unity in $(F_n)_{\mathfrak{p}_0}$ and let $C' = C \cup \{0\}$. Let $-1/ab = s_0 + s_1 2 + s_2 2^2 + \cdots$ with $s_i \in C'$ and $s_0 \neq 0$ and let $\alpha = c_0 + c_1 2 + c_2 2^2 + \cdots$ with $c_i \in C'$ and $c_0 \neq 0$. Note that $-1/ab \neq s_0$ since s_0 is a square. Let $d_0 \in C'$ such that $\overline{d_0} = \overline{c_0 + 1}$. Then we have

$$\begin{aligned} \alpha^4 &\equiv c_0^4 \pmod{\mathfrak{p}_0^3} \\ (\alpha+1)^4 &\equiv d_0^4 \pmod{\mathfrak{p}_0^3} \end{aligned}$$

If $c_0 = 1$, then we have $\alpha^4 \equiv 1 \pmod{\mathfrak{p}_0^3}$ and hence $\alpha^4 - 1/ab \equiv 1 - 1/ab \pmod{\mathfrak{p}_0^3}$. Noting $s = 0$, we have $1 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$, a contradiction. Thus we have $c_0 \neq 1$.

We can show that for $c, d \in C$, $\nu_{\mathfrak{p}_0}(c + d) = 0$ iff $c \neq d$. It is enough to show that $\nu_{\mathfrak{p}_0}(1 + c) = 0$ iff $c \neq 1$ for $c \in C$. Since C is the group of $(N\mathfrak{p}_0 - 1)^{th}$ roots of unity in $(F_n)_{\mathfrak{p}_0}$, $C \setminus \{1\}$ is a set of solutions of

$$X^{2^f-2} + X^{2^f-3} + \cdots + X + 1 = 0,$$

letting $N\mathfrak{p}_0 = 2^f$. Hence we have

$$X^{2^f-2} + X^{2^f-3} + \cdots + X + 1 = \prod_{\substack{c \in C \\ c \neq 1}} (X - c).$$

Letting $X = -1$, we have $\nu_{\mathfrak{p}_0}(1 + c) = 0$ for any $c \neq 1$.

Thus we have $c_0^4 \neq s_0$. We consider the carrying of $c_0^4 + s_0$. Let $b_0 \in C$ be such that $b_0^4 = s_0$. Note that $N\mathfrak{p}_0 = 2^f$ with $f > 2$, thereby there is such b_0. We see that $c_0 + b_0 \not\equiv 0 \pmod{\mathfrak{p}_0}$ since $c_0 \neq b_0$. Therefore there is $e_0 \in C$ such that $c_0 + b_0 \equiv e_0 \pmod{\mathfrak{p}_0}$. Since $(c_0 + b_0)^4 \equiv e_0^4 \pmod{\mathfrak{p}_0^3}$, we have

$$c_0^4 + b_0^4 \equiv e_0^4 - (c_0 b_0)^2 2 \equiv e_0^4 + (c_0 b_0)^2 2 \pmod{\mathfrak{p}_0^2}.$$

Thus we have

$$c_0^4 + s_0 \equiv e_0^4 + (c_0 b_0)^2 2 \pmod{\mathfrak{p}_0^2}.$$

and

$$\alpha^4 - 1/ab \equiv e_0^4 + ((c_0 b_0)^2 + s_1) 2 \pmod{\mathfrak{p}_0^2}.$$

Hence we must have $(c_0 b_0)^2 = s_1$.

If $d_0^4 = s_0$, then we have

$$(\alpha + 1)^4 - 1/ab \equiv (s_0 + s_1) 2 \pmod{\mathfrak{p}_0^2}.$$

Here we have

$$s_0 + s_1 = b_0^4 + (c_0 b_0)^2 = b_0^2 (b_0^2 + c_0^2) \not\equiv 0 \pmod{\mathfrak{p}_0}$$

since $b_0 \neq c_0$. Thus we have

$$(\alpha + 1)^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}.$$

Let $d_0^4 \neq s_0$. Then, similarly as before, we see that there is $f_0 \in C$ such that $d_0 + b_0 \equiv f_0 \pmod{\mathfrak{p}_0}$ and we have

$$d_0^4 + s_0 \equiv f_0^4 + (d_0 b_0)^2 2 \pmod{\mathfrak{p}_0^2}.$$

Then we have

$$(\alpha+1)^4 - 1/ab \equiv f_0^4 + ((d_0b_0)^2 + s_1)2 \pmod{\mathfrak{p}_0^2}.$$

But we have

$$(d_0b_0)^2 + s_1 = (d_0b_0)^2 + (c_0b_0)^2 = b_0^2(d_0^2 + c_0^2) \not\equiv 0 \pmod{\mathfrak{p}_0}$$

since $d_0 \neq c_0$. Thus we have

$$(\alpha+1)^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}.$$

Furthermore we see that $(\alpha+1)^4 - 1/ab$ is in $\mathfrak{p}_0 \setminus \mathfrak{p}_0^2$ or in $C(1+\mathfrak{p}_0) \setminus C(1+\mathfrak{p}_0^2)$. Hence we conclude that $(\gamma+1)^4 - 1/ab$ is not a square in $(F_n)_{\mathfrak{p}_0}$ since

$$(\gamma+1)^4 - 1/ab \equiv (\alpha+1)^4 - 1/ab \pmod{\mathfrak{p}_0^3}.$$

Therefore we have

$$K_l \models \neg\varphi(a,b,\gamma) \wedge \varphi(a,b,\gamma+1),$$

a contradiction.

Case 2: $s > 0$.
This time we let $\gamma \in \mathfrak{O}_n$ such that

$$\begin{aligned} \gamma &\equiv \alpha \pmod{\mathfrak{p}_0^{s+1}} \\ \gamma &\equiv -1 \pmod{\mathfrak{p}} \text{ if } \mathfrak{p} \in S_n(a,b),\ \mathfrak{p} \neq \mathfrak{p}_0. \end{aligned}$$

Then we have $\gamma^4 \equiv \alpha^4 \pmod{\mathfrak{p}_0^{s+3}}$ and that

$$2^{-s}(\alpha^4 - 1/ab) \equiv 2^{-s}(\gamma^4 - 1/ab) \pmod{\mathfrak{p}_0^3}.$$

Therefore we see that $\gamma^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$ similarly as before.
Since

$$(\gamma+1)^4 - 1/ab \equiv -1/ab \pmod{\mathfrak{p}^4}$$

for $\mathfrak{p} \neq \mathfrak{p}_0$, we also have $(\gamma+1)^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}}$ for $\mathfrak{p} \neq \mathfrak{p}_0$ similarly.
We see that $(\alpha+1)^4 - 1/ab$ is a unit at $\mathfrak{p}_0$ since

$$(\alpha+1)^4 - 1/ab = 1 + 2\alpha^2 + 4(\alpha + \alpha^2 + \alpha^3) + \alpha^4 - 1/ab.$$

Therefore if $(\alpha+1)^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}$, then we have $(\gamma+1)^4 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}_0}$ similarly and have $F_n \models \neg\varphi(a,b,\gamma) \wedge \varphi(a,b,\gamma+1)$. So we have $K_l \models \neg\varphi(a,b,\gamma) \wedge \varphi(a,b,\gamma+1)$, a contradiction. Thus we see that $(\alpha+1)^4 - 1/ab \in (F_n)^{*2}_{\mathfrak{p}_0}$.

We again let $-1/ab = s_0 + s_1 2 + s_2 2^2 + \cdots$ with $s_i \in C'$ and $s_0 \neq 0$ and let $\alpha = c_0 + c_1 2 + c_2 2^2 + \cdots$ with $c_i \in C'$ and $c_0 \neq 0$. This time we see that $c_0 \neq 1$ since $\nu_{\mathfrak{p}_0}(\alpha + 1) = 0$. We let again $d_0 \in C$ such that $\overline{d_0} = \overline{c_0 + 1}$. Then we have

$$\begin{aligned} \alpha^4 &\equiv c_0^4 \pmod{\mathfrak{p}_0^3} \\ (\alpha+1)^4 &\equiv d_0^4 \pmod{\mathfrak{p}_0^3} \end{aligned}$$

as before. On the other hand, we have $d_0^4 \equiv (c_0 + 1)^4 \pmod{\mathfrak{p}_0^3}$ since $\overline{d_0} = \overline{c_0 + 1}$. Then we can wright

$$(\alpha + 1)^4 = 1 + c_0^4 + c_0^2 2 + (c_0 + c_0^2 + c_0^3)2^2 + \cdots .$$

We claim that $c_0^4 \neq s_0$, from which it follows that $\alpha^4 - 1/ab$ is a unit in $(\mathfrak{o}_m)_{\mathfrak{P}_0}$, a contradiction. Suppose that $c_0^4 = s_0$. Then $\alpha^4 - 1/ab = (s_0 + s_1)2 + s_2 2^2 + \cdots$. Thus we must have $s_0 = s_1$ and $\alpha^4 - 1/ab \equiv (s_0 + s_2)2^2 \pmod{\mathfrak{p}_0^3}$. Hence we have $c_0^4 - 1/ab \equiv (s_0 + s_2)2^2 \pmod{\mathfrak{p}_0^3}$ and

$$(\alpha + 1)^4 - 1/ab \equiv 1 + c_0^2 2 + (c_0 + c_0^2 + c_0^3 + s_0 + s_2)2^2 \pmod{\mathfrak{p}_0^3},$$

a contradiction, since an element in $(1 + \mathfrak{p}_0) \setminus (1 + \mathfrak{p}_0^2)$ is not a square in $(F_n)_{\mathfrak{p}_0}$. Thus we have $c_0^4 \neq s_0$. □

Lemma 19 *Let* $l \equiv -1 \pmod 4$. *Let* $a, b \in F_n^*$. *Suppose that* $S_n(a, b)$ *contains a* $\mathfrak{p}_0$ *such that* $\mathfrak{p}_0 | 2$ *and* $\nu_{\mathfrak{p}_0}(-ab) = -2$.

Then $K_l \models \neg\forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1))$,

Proof. Suppose not. Let $m \geq n$ and $\mathfrak{P}_0$ is a prime of $\mathfrak{O}_m$ lying above $\mathfrak{p}_0$. We note that $\mathfrak{P}_0 \in S_m(a, b)$, $-1/ab \notin (F_m)_{\mathfrak{P}_0}^{*2}$ and $1 - 1/ab \notin (F_m)_{\mathfrak{P}_0}^{*2}$. Now we will prove that for $\alpha \in \mathfrak{O}_m$ with $\nu_{\mathfrak{P}_0}(\alpha) = 0$,

$$\alpha^4 - 1/ab \in (F_m)_{\mathfrak{P}_0}^{*2} \text{ iff } (\alpha + 1)^4 - 1/ab \in (F_m)_{\mathfrak{P}_0}^{*2}.$$

Suppose that $\alpha^4 - 1/ab \in (F_m)_{\mathfrak{P}_0}^{*2}$. We have $\nu_{\mathfrak{P}_0}(\alpha^4 - 1/ab) = 0$ since $\nu_{\mathfrak{P}_0}(-1/ab) = 2$. This time we let $\gamma \in \mathfrak{O}_m$ such that

$$\begin{aligned} \gamma &\equiv \alpha \pmod{\mathfrak{P}_0} \\ \gamma &\equiv -1 \pmod{\mathfrak{P}^2} \text{ if } \mathfrak{P} \in S_m(a, b),\ \mathfrak{P} \neq \mathfrak{P}_0. \end{aligned}$$

Noting that $\alpha^4 - 1/ab$ is a unit at $\mathfrak{P}_0$, we have $\gamma^4 - 1/ab \in (F_m)_{\mathfrak{P}_0}^{*2}$.

Furthermore we have $(\gamma + 1)^4 - 1/ab \notin (F_m)_{\mathfrak{P}}^{*2}$ for $\mathfrak{P} \in S_m(a, b)$, $\mathfrak{P} \neq \mathfrak{P}_0$ also in this case.

We claim that $\nu_{\mathfrak{P}_0}(\alpha + 1) \neq 0$, for if not, we would have $\alpha^4 \equiv 1 \pmod{\mathfrak{P}_0^3}$, and would have $1 - 1/ab \in (F_m)_{\mathfrak{P}_0}^{*2}$ since $\alpha^4 - 1/ab \equiv 1 - 1/ab \pmod{\mathfrak{P}_0^3}$ and since $1 - 1/ab$ is a unit at $\mathfrak{P}_0$. Hence if $(\alpha+1)^4-1/ab \notin (F_m)^{*2}_{\mathfrak{P}_0}$, then we have $(\gamma+1)^4-1/ab \notin (F_m)^{*2}_{\mathfrak{P}_0}$, and have $K_l \models \neg\varphi(a,b,\gamma) \wedge \varphi(a,b,\gamma+1)$. Thus we have $(\alpha+1)^4 - 1/ab \in (F_m)^{*2}_{\mathfrak{P}_0}$. The converse follows similarly.

Let C and C' be as before and again let $\alpha = c_0 + c_1 2 + c_2 2^2 + \cdots$ with $c_i \in C'$ and $c_0 \neq 0$. Let $d_0 \in C'$ be as before and let $-1/ab = s_2 2^2 + s_3 2^3 + \cdots$ with $s_i \in C'$ and $s_2 \neq 0$. Then we have

$$\begin{aligned}\alpha^4 - 1/ab &\equiv c_0^4 + s_2 2^2 \pmod{\mathfrak{P}_0^3}\\ (\alpha+1)^4 - 1/ab &\equiv d_0^4 + s_2 2^2 \pmod{\mathfrak{P}_0^3}\end{aligned}$$

Therefore we have for $c_0 \neq 1$,

$$\begin{aligned}s_2/c_0^4 &\equiv c(c+1) \pmod{\mathfrak{P}_0} \text{ iff } \alpha^4 - 1/ab \in (F_m)^{*2}_{\mathfrak{P}_0}\\ s_2/(c_0^4+1) &\equiv c'(c'+1) \pmod{\mathfrak{P}_0} \text{ iff } (\alpha+1)^4 - 1/ab \in (F_m)^{*2}_{\mathfrak{P}_0}\end{aligned}$$

for some $c, c' \in C'$, since $d_0^4 \equiv c_0^4 + 1 \pmod{\mathfrak{P}_0}$.

Let $N\mathfrak{P}_0 = 2^f$. Then the residue field $\overline{(F_m)_{\mathfrak{P}_0}}$ is the finite field $\mathbb{F}_{2^f}$. Let $\mathrm{Tr} : \mathbb{F}_{2^f} \to \mathbb{F}_2$ be the absolute trace function from $\mathbb{F}_{2^f}$ to $\mathbb{F}_2$ and let χ_1 be the canonical additive character of $\mathbb{F}_{2^f}$, that is, $\chi_1(\bar{c})$ is defined to be $e^{2\pi i \mathrm{Tr}(\bar{c})/2}$ for $\bar{c} \in \mathbb{F}_{2^f}$. Then we know that for $c \in C'$,

$$c \equiv c'(c'+1) \pmod{\mathfrak{P}_0} \text{ for some } c' \in C' \text{ iff } \mathrm{Tr}(\bar{c}) = 0 \text{ iff } \chi_1(\bar{c}) = 1.$$

Then we see that $\chi_1(\bar{s}_2/\bar{c}^4) = 1$ iff $\chi_1(\bar{s}_2/(\bar{c}^4+1)) = 1$ for any $c \in (C \setminus \{1\})$. Note that $\nu_{\mathfrak{P}_0}(1+c) = 0$ if $c \neq 1$.

Let g be a primitive root of $\mathfrak{P}_0$ in F_m, that is, $\bar{g}$ is a primitive element of $\mathfrak{O}_m/\mathfrak{P}_0$. Let S be the set $\{a_0 + a_1 g + a_2 g^2 + \cdots + a_{f-1} g^{f-1} : a_i \in \{0,1\}\}$. S forms a complete representative set in $(F_m)_{\mathfrak{P}_0}$ of the residue field $\overline{(F_m)_{\mathfrak{P}_0}}$. Let

$$D = \{c \in C : c \equiv a_1 g + a_2 g^2 + \cdots + a_{f-1} g^{f-1} \pmod{\mathfrak{p}_0} \text{ for some } a_i\}.$$

Then the set $D \cup \{c+1 : c \in D\} \cup \{0,1\}$ forms a complete representative set of the residue field $\overline{(F_m)_{\mathfrak{P}_0}}$. Since $2^f > 4$, there is $c' \in C$ such that $c = c'^4$ for any $c \in C$. Let $D' = \{c' : c'^4 = c,\ c \in D\}$.

We consider $\chi_1(\bar{c}^4 + \bar{s}_2/\bar{c}^4) + \chi_1(\bar{c}^4 + 1 + \bar{s}_2/(\bar{c}^4+1))$ for $c \in (C \setminus \{1\})$. We see that f is odd since $l \equiv -1 \pmod 4$. It follows that $\chi_1(\bar{1}) = -1$. Hence we have $\chi_1(\bar{c}^4 + \bar{s}_2/\bar{c}^4) + \chi_1(\bar{c}^4 + 1 + \bar{s}_2/(\bar{c}^4+1)) = 0$ for all $c \in (C \setminus \{1\})$.

Now we consider the following character sum of $\mathbb{F}_{2^f}$

$$K(\chi_1; 1, \bar{s}_2) = \sum_{\bar{c} \in \mathbb{F}^*_{2^f}} \chi_1(\bar{c} + \bar{s}_2/\bar{c}),$$

which is called a Kloosterman sum. Since $1 - 1/ab \equiv 1 + s_2 2^2 \pmod{\mathfrak{P}_0^3}$, we have $\chi_1(\bar{s}_2) = -1$. Therefore we see that $K(\chi_1; 1, \bar{s}_2) = 1$ in $\overline{(F_m)_{\mathfrak{P}_0}} = \mathbb{F}_{2^f}$, noting

$$K(\chi_1; 1, \bar{s}_2) = \sum_{\bar{c}' \in D'} (\chi_1(\bar{c}'^4 + \bar{s}_2/\bar{c}'^4) + \chi_1(\bar{c}'^4 + 1 + \bar{s}_2/(\bar{c}'^4 + 1))) + \chi_1(1 + \bar{s}_2).$$

Therefore we see that $K(\chi_1; 1, s_2) = 1$ in $\overline{(F_k)_{\mathfrak{P}}} = \mathbb{F}_{2^{f_0 r}}$ for all $k \geq n$ and all $\mathfrak{P}$, a prime of F_k with $\mathfrak{P} | \mathfrak{p}_0$, where $N\mathfrak{p}_0 = 2^{f_0}$ and $r = [(F_k)_{\mathfrak{P}} : (F_n)_{\mathfrak{p}_0}]$. There are F_k and $\mathfrak{P}$ such that $r > 1$. Fix such r. Note that r is odd.

On the other hand we know by [9, p. 226] that there exist numbers ω_1 and ω_2 that are either complex conjugates or both real, such that

$$\begin{aligned} K(\chi_1; 1, \bar{s}_2) &= -\omega_1 - \omega_2 \text{ in } \mathbb{F}_{2_0^f} \\ K(\chi_1; 1, \bar{s}_2) &= -\omega_1^r - \omega_2^r \text{ in } \mathbb{F}_{2^{f_0 r}}. \end{aligned}$$

So we have $\omega_1 + \omega_2 = \omega_1^r + \omega_2^r = -1$. Furthermore we know by [9, pp. 228–229] that $|\omega_1| = |\omega_2| = 2^{f_0/2}$, $\omega_1\omega_2 = 2^{f_0}$. Let $a_t = \omega_1^t + \omega_2^t$ and $q = 2^{f_0}$. Using the identity

$$\omega_1^t + \omega_2^t = (\omega_1^{t-1} + \omega_2^{t-1})(\omega_1 + \omega_2) - (\omega_1^{t-2} + \omega_2^{t-2})\omega_1\omega_2 \text{ for } t \geq 2,$$

we can show by induction on k that, letting $A_1 = 0$ and $A_2 = -2$,

$$\begin{aligned} a_{2k} &= 1 + qA_{2k}, \quad A_{2k} = -1 - A_{2k-1} - qA_{2k-2} \quad (k \geq 2) \\ a_{2k+1} &= -1 + qA_{2k+1}, \quad A_{2k+1} = 1 - A_{2k} - qA_{2k-1} \quad (k \geq 1), \end{aligned}$$

where for $k \geq 1$, $A_{2k} \equiv 0 \pmod 2$ and $A_{2k+1} \equiv 1 \pmod 2$ hold. Thus we get a contradiction since r is odd and $a_r = \omega_1^r + \omega_2^r = -1$. □

Thus we see that, letting l be an odd prime such that $l \equiv -1 \pmod 4$ and 5 is a prime of K_l, for $a, b \in F_n^*$, if $S_n(a, b)$ contains no primes $\mathfrak{p}$ such that $\mathfrak{p}|2$ and $\nu_{\mathfrak{p}}(-ab) = 2$, then

$$K_l \models \forall c(\varphi(a, b, c) \to \varphi(a, b, c+1)) \to \varphi(a, b, \alpha) \text{ for all } \alpha \in \mathfrak{O}_{K_l}.$$

Let $\bar{\mathfrak{P}}_1, \ldots, \bar{\mathfrak{P}}_g$ be prime factors of 2 in $\mathfrak{O}_{K_l}$ and let n_0 be such that there are exactly g extensions of 2 for all $n \geq n_0$.

Note that for a, b with $ab = 0$,

$$K_l \models \forall c(\varphi(a, b, c) \to \varphi(a, b, c+1)) \to \varphi(a, b, \alpha)$$

for all $\alpha \in \mathfrak{O}_{K_l}$.

Proposition 20 *Let l be an odd prime such that $l \equiv -1 \pmod 4$. Then $\psi(K_l) = \bigcap_i((1 + \bar{\mathfrak{P}}_i) \cup \bar{\mathfrak{P}}_i)$.*

Proof. Let $\alpha \in \bigcap_i((1+\bar{\mathfrak{P}}_i)\cup\bar{\mathfrak{P}}_i)$. We will show that $K_l \models \psi(\alpha)$. Take n such that $n \geq n_0$ and $\alpha \in F_n$. It is enough to show that for any $a, b \in F_n^*$ with $K_l \models \theta(a,b)$ and for any $\mathfrak{p} \in S_n(a,b)$, if $\mathfrak{p}|2$ and $\nu_\mathfrak{p}(-ab) = 2$,then $\alpha^4 - 1/ab \notin (F_n)_\mathfrak{p}^{*2}$.

Fix such a, b and $\mathfrak{p}$. Then $\mathfrak{p} = \bar{\mathfrak{P}}_i \cap \mathfrak{O}_n$ for some i. We have

$$\begin{aligned} & -1/ab \notin (F_n)_\mathfrak{p}^{*2} \\ (1-ab)/(-ab) &= 1 - 1/ab \notin (F_n)_\mathfrak{p}^{*2}. \end{aligned}$$

Since $\alpha \in ((1+\bar{\mathfrak{P}}_i)\cup\bar{\mathfrak{P}}_i)$, we see that $\alpha \in ((1+\mathfrak{p})\cup\mathfrak{p})$.

Let $\alpha \in 1+\mathfrak{p}$. Then we have

$$\alpha^4 - 1/ab \equiv 1 - 1/ab \pmod{\mathfrak{p}^3},$$

hence

$$2^2(\alpha^4 - 1/ab) \equiv 2^2(1 - 1/ab) \pmod{\mathfrak{p}^5}.$$

Noting that $\nu_\mathfrak{p}(-1/ab) = -2$, we have $\alpha^4 - 1/ab \notin (F_n)_\mathfrak{p}^{*2}$.

Let $\alpha \in \mathfrak{p}$. Then we have

$$\alpha^4 - 1/ab \equiv -1/ab \pmod{\mathfrak{p}^4},$$

hence

$$2^2(\alpha^4 - 1/ab) \equiv 2^2(-1/ab) \pmod{\mathfrak{p}^6}.$$

Noting that $\nu_\mathfrak{p}(-1/ab) = -2$, we have $\alpha^4 - 1/ab \notin (F_n)_\mathfrak{p}^{*2}$.

Conversely, let $\alpha \notin \bigcap_i((1+\bar{\mathfrak{P}}_i)\cup\bar{\mathfrak{P}}_i)$. We may suppose that $\alpha \in \mathfrak{O}_{K_l}$. Then $\alpha \notin ((1+\bar{\mathfrak{P}}_i)\cup\bar{\mathfrak{P}}_i)$ for some i. Take n such that $n \geq N_0$ and $\alpha \in F_n$. Let $\mathfrak{p} = \bar{\mathfrak{P}}_i \cap \mathfrak{O}_n$. We denote by f the residue degree of F_n at $\mathfrak{p}$. We see that f is odd. We may suppose that $f \equiv -1 \pmod 4$; if $f \equiv 1 \pmod 4$, we consider F_{n+1} in which the residue degree of $\mathfrak{p}' = \bar{\mathfrak{P}}_i \cap \mathfrak{O}_{n+1}$ is $-1 \bmod 4$.

We will construct $a, b \in F_n^*$ such that $K_l \models \theta(a,b) \wedge \neg\varphi(a,b,\alpha)$. Let C be the group of $(N_\mathfrak{p}-1)^{th}$ roots of unity in $(F_n)_\mathfrak{p}$ and let $C' = C \cup \{0\}$ as before. As an element of $(F_n)_\mathfrak{p}$, we can wright

$$\alpha = c_0 + c_1 2 + c_2 2^2 + \cdots$$

with $c_i \in C'$ and with $c_0 \neq 0, 1$.

We will prove that there is $s_{-2} \in C$ such that $\chi_1(1/\bar{s}_{-2}) = 1$ and $\chi_1(\bar{s}_{-2}) = \chi_1(\bar{c}_0^4/\bar{s}_{-2}) = -1$. We consider the following Kloosterman sum of $\mathbb{F}_{2^k}$,

$$K(\chi_1; 1, 1) = \sum_{\bar{c}\in\mathbb{F}_{2^k}^*} \chi_1(\bar{c} + 1/\bar{c}).$$

Let $K^{(k)}$ be $K(\chi_1;1,1)$ of $\mathbb{F}_{2^k}$. Then we have

$$K^{(k)} = -\omega_1^k - \omega_2^k$$

for any $k \geq 1$, where $\omega_1 + \omega_2 = -1$ and $\omega_1\omega_2 = 2$ since $K^{(1)} = 1$. Using again the identity

$$\omega_1^t + \omega_2^t = (\omega_1^{t-1} + \omega_2^{t-1})(\omega_1 + \omega_2) - (\omega_1^{t-2} + \omega_2^{t-2})\omega_1\omega_2 \text{ for } t \geq 2,$$

we can show by induction on k that for $m \geq 0$,

$$K^{(4m+1)} > 0,\ K^{(4m+2)} > 0,\ K^{(4m+3)} < 0,\ K^{(4m+4)} < 0.$$

We consider the residue field of $(F_n)_\mathfrak{p}$, which is $\mathbb{F}_{2^f}$. Since $f \equiv -1 \pmod 4$, there are more than $2^{f-1} - 1$ elements $\bar{s}$ of $\mathbb{F}_{2^f}^*$ such that $\chi_1(\bar{s} + 1/\bar{s}) = -1$. Therefore there are more than $2^{f-1} - 1$ elements $\bar{s}$ of $\mathbb{F}_{2^f}^*$ such that $\chi_1(\bar{s}) = -1$ and $\chi(1/\bar{s}) = 1$. Since

$$\sum_{\bar{c}\in\mathbb{F}_{2^f}^*} \chi_1(\bar{c}_0^4/\bar{c}) = -1,$$

there is $\bar{s}' \in \mathbb{F}_{2^f}^*$ such that $\chi_1(1/\bar{s}') = 1$ and $\chi_1(\bar{s}') = \chi_1(\bar{c}_0^4/\bar{s}') = -1$. Take $s_{-2} \in C$ such that $\bar{s}_{-2} = \bar{s}'$. Obviously $s_{-2} \neq 1$ since $\chi_1(1) = -1$.

We take $s_0 \in C$ such that $\chi_1(\bar{s}_0/\bar{s}_{-2}) = -1$. Let $\tau' \in \mathfrak{O}_n$ such that $\tau' \equiv s_{-2} + s_0 2^2 \pmod{\mathfrak{p}^5}$. We can take such τ' since $\mathfrak{O}_n/\mathfrak{p}^k \simeq (\mathfrak{o}_n)_\mathfrak{p}/\mathfrak{p}^k$.

Take a prime $\mathfrak{p}'$ of F_n with $\mathfrak{p}'|p'$ where p' is a rational prime other than 2 and l and such that $p' \equiv 1 \pmod{2^3}$. Let $\tau \in \mathfrak{O}_n$ such that

$$\begin{aligned} \tau &\equiv \tau' \pmod{\mathfrak{p}^5} \\ \tau &\equiv p' \pmod{\mathfrak{p}'^2}. \end{aligned}$$

and let $\gamma = 2^{-2}p'^{-2}\tau$. We have $\gamma \in F_n$, $\nu_\mathfrak{p}(\gamma) = -2$ and $\nu_{\mathfrak{p}'}(\gamma) = -1$. We see that γ is not a square of $(F_n)_{\mathfrak{p}'}$. Furthermore we see that γ is not a square of $(F_n)_\mathfrak{p}$ since $\gamma \equiv 2^{-2}(s_{-2} + s_0 2^2) \pmod{\mathfrak{p}^3}$ and $\chi_1(\bar{s}_0/\bar{s}_{-2}) = -1$. Note that $p' \equiv 1 \pmod{\mathfrak{p}^3}$. Therefore γ^{-1} is non-square of $(F_n)_\mathfrak{p}$ and $(F_n)_{\mathfrak{p}'}$.

Then we have by [10, p. 203], that there is $a \in F_n^*$ such that $S_n(a, 1/\gamma) = \{\mathfrak{p}, \mathfrak{p}'\}$. Let $b = -1/a\gamma$. We have $b \in F_n$. We see that $(a,b)_\mathfrak{p} = (a,-ab)_\mathfrak{p} = (a,1/\gamma)_\mathfrak{p} = -1$ and $(a,b)_{\mathfrak{p}'} = (a,-ab)_{\mathfrak{p}'} = (a,1/\gamma)_{\mathfrak{p}'} = -1$, hence $S_n(a,b) = \{\mathfrak{p},\mathfrak{p}'\}$. Since $-1/ab = \gamma$, we have

$$2^2(\alpha^4 - 1/ab) = 2^2(\alpha^4 + \gamma) \equiv s_{-2} + (s_0 + c_0^4)2^2 \pmod{\mathfrak{p}^3}.$$

Then we have $\alpha^4 - 1/ab \in (F_n)_\mathfrak{p}^{*2}$ since $\chi_1((\bar{s}_0 + \bar{c}_0^4)/\bar{s}_{-2}) = \chi_1(\bar{s}_0/\bar{s}_{-2})\chi_1(\bar{c}_0^4/\bar{s}_{-2}) = 1$. Thus we have $F_n \models \neg\varphi(a,b,\alpha)$, hence $K_l \models \neg\varphi(a,b,\alpha)$.

We will prove that $K_l \models \theta(a,b)$, that is,

$$K_l \models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1)).$$

Let $\beta \in K_l$ and suppose that $K_l \models \varphi(a,b,\beta)$.

First we note that $-1/ab \notin (F_n)^{*2}_{\mathfrak{p}}$. On the other hand, we have

$$2^2(1-1/ab) = 2^2(1+\gamma) \equiv s_{-2} + (s_0+1)2^2 \pmod{\mathfrak{p}^3}.$$

Then we have $1 - 1/ab \notin (F_n)^{*2}_{\mathfrak{p}}$ since $\chi_1((\bar{s}_0+1)/\bar{s}_{-2}) = \chi_1(\bar{s}_0/\bar{s}_{-2})\chi_1(1/\bar{s}_{-2}) = -1$. Therefore we suppose that $\beta \neq 0$. Take $m \geq n$ such that $a, b, \beta \in F_m$. Then we have $F_m \models \varphi(a,b,\beta)$. It follows that $\beta^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}}$ and $\beta^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}'}$.

We claim that $\nu_{\mathfrak{p}'}(\beta) \geq 0$ iff $\beta^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}'}$; if $\nu_{\mathfrak{p}'}(\beta) \geq 0$, then we have $\nu_{\mathfrak{p}'}(\beta^4 - 1/ab) = -1$, hence $\beta^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}'}$, and if $\nu_{\mathfrak{p}'}(\beta) < 0$, then applying Newton's method of iteration [8, p. 42] with $x^2 - h$ with $h = \beta^4 - 1/ab$ and $x = \beta^2$, we get that $h \in (F_m)^{*2}_{\mathfrak{p}'}$.

Therefore we have $(\beta+1)^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}'}$. We will prove that $(\beta+1)^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}}$.

Let $\beta = c'_k 2^k + c'_{k+1}2^{k+1} + \cdots$ with $c'_k \neq 0$. Then we have $\beta^4 \in 2^{4k}(c'^4_k + \mathfrak{p}^3)$. Let $k \leq -2$. Since $-1/ab \equiv 2^{-2}(s_{-2} + s_0 2^2) \pmod{\mathfrak{p}^3}$, we have $\beta^4 - 1/ab \in 2^{4k}(c'^4_k + \mathfrak{p}^3)$, hence $\beta^4 - 1/ab \in (F_m)^{*2}_{\mathfrak{p}}$. Thus we have $k \geq -1$, that is, $\nu_{\mathfrak{p}}(\beta) \geq -1$.

If $\nu_{\mathfrak{p}}(\beta) > 0$, then we have

$$2^2((\beta+1)^4 - 1/ab) \equiv 2^2(1-1/ab) \pmod{\mathfrak{p}^5},$$

since $(1+\beta)^4 \in 1 + \mathfrak{p}^3$. Hence we have $(\beta+1)^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}}$.

Let $\nu_{\mathfrak{p}}(\beta) = -1$. We can wright $\beta = c'_{-1}2^{-1} + c'_0 + c'_1 2^1 + \cdots$ with $c'_{-1} \neq 0$. Then we have

$$2^4(\beta^4 - 1/ab) \equiv c'^4_{-1} + s_{-2}2^2 \pmod{\mathfrak{p}^3}.$$

Thus we have $\chi_1(\bar{s}_{-2}/\bar{c}'^4_{-1}) = -1$. Since $\beta + 1 = c'_{-1}2^{-1} + (c'_0 + 1) + c'_1 2^1 + \cdots$, we have

$$2^4((\beta+1)^4 - 1/ab) \equiv c'^4_{-1} + s_{-2}2^2 \pmod{\mathfrak{p}^3}.$$

Therefore we have $(\beta+1)^4 - 1/ab \notin (F_m)^{*2}_{\mathfrak{p}}$ also in this case.

Let $\nu_{\mathfrak{p}}(\beta) = 0$. We can wright $\beta = c'_0 + c'_1 2^1 + \cdots$ with $c'_0 \neq 0$. Then we have

$$2^2(\beta^4 - 1/ab) \equiv s_{-2} + (s_0 + c'^4_0)2^2 \pmod{\mathfrak{p}^3}.$$

Thus we have $\chi_1((\bar{s}_0 + \bar{c}'^4_0)/\bar{s}_{-2}) = -1$. Since $\beta + 1 = (c'_0 + 1) + c'_1 2^1 + \cdots$, we have

$$2^2((\beta+1)^4 - 1/ab) \equiv s_{-2} + (s_0 + (c'_0+1)^4)2^2 \pmod{\mathfrak{p}^3}.$$

Then we have

$$\chi_1((\bar{s}_0 + \overline{(c'_0+1)^4})/\bar{s}_{-2}) = \chi_1((\bar{s}_0 + \bar{c}_0'^4 + 1)/\bar{s}_{-2}) = -1,$$

since $\chi_1(1/\bar{s}_{-2}) = 1$. Therefore we have $(\beta+1)^4 - 1/ab \notin (F_m)_{\mathfrak{p}}^{*2}$ also in this case.

Thus we complete the proof of the proposition. □

We easily see that $\psi(K_l) = \bigcap_i((1+\bar{\mathfrak{P}}_i)\cup\bar{\mathfrak{P}}_i)$ is a ring since $\alpha \in \psi(K_l)$ iff $\alpha \equiv 0 \text{or} 1 \pmod{\bar{\mathfrak{P}}_i}$ for all $i$.

Remark 21 From the above proof of the proposition, we see that, letting $l \equiv -1 \pmod 4$, for $a, b \in F_n^*$ such that $S_n(a,b)$ contains a $\mathfrak{p}_0$ with $\mathfrak{p}_0|2$ and $\nu_{\mathfrak{p}_0}(a,b) = 2$, a statement like Lemma 16 does not hold.

4 Defining $\mathbb{N}$ in K_l

We say that a totally real algebraic number $a$ is totally non-negative iff $a$ and all its conjugates are non-negative. We write $a \ll b$ to indicate that $b - a$ is totally non-negative, following J. Robinson [13].

Kronecker [7] determined all sets of conjugate algebraic integers in the interval $c - 2 \leq x \leq c + 2$, provided $c$ is a rational integer; they have the form

$$x = c + 2\cos(2k\pi/m) \text{ with } 0 \leq k \leq m/2 \text{ and } (k,m) = 1.$$

Note that if $m = 1, 2, 3, 4$, then $x = c+2, c-2, c\pm 1, c$ respectively.

He started by showing that a set of conjugate algebraic integers lying on the unit circle must be roots of unity, that is, he showed that if the absolute value of some algebraic integer together with those of its conjugates are equal to 1, then it must be roots of unity: suppose that there were an algebraic integer $a(= a^{(1)})$ such that it were not a root of unity, and its conjugate were $a^{(2)}, a^{(3)}, \ldots, a^{(n)}$ with $|a^{(i)}| = 1$ for $1, \ldots, n$. Then their infinitely many powers also would lie on the unit circle. They must satisfy finitely many minimal polynomials of degree $n$ over $\mathbb{Z}$, since the absolute value of the coefficients of those polymonials were $\leq \binom{n}{[n/2]}$, which were impossible.

The unit circle $|t| = 1$ was then transformed into the initial segment $-2 \leq x \leq 2$ by the transformation $x = t + 1/t$.

Therefore we know that any algebraic integer satisfying $c - 2 \ll x \ll c + 2$ with $c \in \mathbb{Z}$ must have the above form. Furthermore it is known that an interval of length less than 4 can contain only finitely many complete sets of conjugate algebraic integers. (See [15].)

These facts are used by J. Robinson in [13]. Her results concerns the integral closure of $\mathbb{Z}$ inside totally real fields, not necessarily finite over $\mathbb{Q}$. She calls such a ring a totally real algebraic integer ring. In 1962 she proved the following:

Theorem 22 *The natural numbers can be defined arithmetically in any totally real algebraic integer ring A such that there is a smallest interval $(0, s)$ with s real or ∞, which contains infinitely many complete conjugate sets of numbers of A, i.e. infinitely many $x \in A$ with $0 \ll x \ll s$.*

In particular such a ring is undecidable.

We know that $\psi(K_l)$ is a totally real algebraic integer ring if l is a prime such that $l \equiv -1 \pmod 4$. And we know that algebraic integers in K_l satisfying $0 \ll x \ll 4$ are $\{2 + 2\cos(2k\pi/l^n) : 0 \leq k \leq m/2, (k, m) = 1, n \in \mathbb{N}\}$. Furthermore we know by [15, p. 312], that $2 + 2\cos(2k\pi/l^n)$ are units in $\mathfrak{O}_{K_l}$ and that $1 + 2\cos(2k\pi/l^n)$ are units in $\mathfrak{O}_{K_l}$ if $l \neq 3$, and $|N_{F_{n-1}/\mathbb{Q}}(1 + 2\cos(2k\pi/3^n))| = 3$ for $n \geq 2$. Hence we see that $2 + 2\cos(2k\pi/l^n)$ are not in $\psi(K_l)$. On the other hand $4 + 4\cos(2k\pi/l^n)$ are in $\bigcap_i \bar{\mathfrak{P}}_i$, hence in $\psi(K_l)$. Thus we see that $(0, 8)$ contains infinitely many complete conjugate sets of numbers of $\psi(K_l)$.

Unfortunately we don't know whether or not $(0, 8)$ is the smallest such interval in $\psi(K_l)$. Nevertheless if we let l be a rational prime such that 2 is a prime of $\mathfrak{O}_{K_l}$, then we can show that $(0, 8)$ is the smallest such interval in $\psi(K_l)$. Note that there are many such primes; For example, $3, 7, 11, 19, 23, 43, 47$ are primes such that $l \equiv -1 \pmod 4$ and 2 is a prime of $\mathfrak{O}_{K_l}$. Sophie Germain primes seem to provide many such examples. Note that then $\psi(K_l) = (1 + 2\mathfrak{O}_{K_l}) \cup 2\mathfrak{O}_{K_l}$.

Lemma 23 *Let l be a prime such that $l \equiv -1 \pmod 4$ and 2 is a prime of $\mathfrak{O}_{K_l}$. Then $(0, 8)$ is the smallest interval of the form $(0, c)$ which contains infinitely many complete conjugate sets of numbers of $\psi(K_l)$.*

Proof. Suppose not. Then some interval $(0, \delta)$ with $\delta < 8$ contains infinitely many complete conjugate sets of numbers of $\psi(K_l)$. Then we have that either it contains infinitely many complete conjugate sets of numbers of $1 + 2\mathfrak{O}_{K_l}$ or it contains infinitely many complete conjugate sets of numbers of $2\mathfrak{O}_{K_l}$. In either case it follows that an interval less than 4 contains infinitely many complete conjugate sets of algebraic integers, a contradiction.

□

Theorem 24 *Let l be a prime such that $l \equiv -1 \pmod 4$ and 2 is a prime of $\mathfrak{O}_{K_l}$. Then $\mathbb{N}$ is definable in K_l. Thus such K_l is undecidable.*

References

[1] Darnière, L., *étude modèle-théorique d'anneaux satisfaisant un principe de hasse nonsingulier*, Phd thesis, Université de Rennes 1, January 1998.

[2] Ershov, Y.-L., *Nice local-global fields I*, Algebra and Logic, 35 (1996), no. 4, pp. 229–235.

[3] ————-, *Near regularly Prüfer rings*, Siberian Adv. Math., 9 (1999), no. 1, pp. 1–45.

[4] Fried, M.D., Haran, D. and Völklein, H., *Real Hilbertianity amd the Field of Toatally Real Numbers*, Contemp. Mathematics, 174 (1994), pp. 1–34.

[5] Fukuzaki, K., *On some infinite totally real extensions of* $\mathbb{Q}$, Kokyuroku of the Research Institute of Mathematical Sciences in Kyoto, vol. 1574(2007), pp. 1–21.

[6] Iyanaga, S.(Editor), *The Theory of Numbers*, North-Holland Publishing Company, 1975.

[7] Kronecker, L., *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, Reine. Angew. Math., 53 (1857), pp. 173–175.

[8] Lang, S., *Algebraic Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 1994.

[9] Lidl, R. and Niederreiter, H., *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.

[10] O'Meara, O.T., *Introduction to Quadratic Forms*, Springer-Verlag, Berlin Heidelberg New York, 1973.

[11] Poonen, B., *Uniform first-order definitions in finitely generated fields*, December 2005. Preprint.

[12] Robinson, J., *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc., 10 (1959), pp. 950-957.

[13] ————, *On the decision problem for algebraic rings*, Studies in Mathematical Analysis and Related Topics, no. 42, Stanford Univ. Press, Stanford, Calif., 1962, pp. 297–304.

[14] ————, *The decision problem for fields*, The Theory of Models: Proceedings of the 1963 International Symposium at Berkeley (J. W. Addison et al., eds.), North-Holland, Amsterdam, 1965, pp. 299–311.

[15] Robinson, R.M., *Intervals Containing Infinitely Many Set of Conjugate Algebraic Integers*, Studies in Mathematical Analysis and Related Topics, no. 43, Stanford Univ. Press, Stanford, Calif., 1962, pp. 305–315.

[16] Rumely, R.S., *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. 262 (1980), no. 1, pp. 195–217.

[17] Swinnerton-Dyer. H.P.F., *A Brief Guide to Algebraic Number Theory*, London Mathematical Society Student Texts 50, Cambridge University Press, 2001.

FACULTY OF INTERCULTURAL STUDIES
THE INTERNATIONAL UNIVERSITY OF KAGOSHIMA
KAGOSHIMA 891-0191
JAPAN
E-mail: fukuzaki@int.iuk.ac.jp