<table>
<thead>
<tr>
<th>Title</th>
<th>Interpreting finite fields in towers of cyclotomic fields (Model theoretic aspects of the notion of independence and dimension)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Fukuzaki, Kenji</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 1555: 93-103</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2007-05</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/80982">http://hdl.handle.net/2433/80982</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>
Interpreting finite fields in towers of cyclotomic fields

Kenji Fukuzaki
Faculty of Intercultural Studies,
The international University of Kagoshima

Abstract

Let $l$ be an odd prime and $\zeta_{l^n}$ is a primitive $l^n$-th root of unity. We consider the towers of cyclotomic fields $K_l = \bigcup_n \mathbb{Q}(\zeta_{l^n})$. We prove that, for any positive integer $k$, there is a prime $p > k$ such that $\mathbb{Z}/(p)$ is interpretable in $K_l$. The proof uses the method of Julia Robinson by which she proved the undecidability of number fields.

For $K_m = \bigcup_n \mathbb{Q}(\zeta_{m^n})$, where $m$ is an arbitrary positive integer and $\zeta_{m^n}$ is a primitive $m^n$-th root of unity, we prove that for any positive integer $k$, there is a prime $p > k$ such that some finite product of $\mathbb{Z}/(p)$ is interpretable in $K_m$.

1 Introduction

In 1959 Julia Robinson [1] proved that in a given number field, $N$ is $\emptyset$-definable in the ring language, from which follows the undecidability of its theory. She constructed a formula which includes $\mathbb{Z}$ but excludes non-algebraic integers, which only depends on the ramification index of prime ideals of a number field which divides 2. Let $F$ be a number field and $\psi(t)$ be such a formula. Then the ring of algebraic integers $\mathcal{O}$ of $F$ is $\emptyset$-definable in $F$. Let $a_1, \ldots, a_s$ be an integral basis of $\mathcal{O}$ ($s = [F : \mathbb{Q}]$), and let $P_i(x)$ be the minimal polynomial of $a_i$ over $\mathbb{Q}$ (hence over $\mathbb{Z}$) for each $i$. Then in $F$

$$t \in \mathcal{O} \iff \exists x_1, \ldots, x_s, y_1, \ldots, y_s (t = x_1 y_1 + \cdots + x_s y_s \land \bigwedge_i P_i(y_i) = 0 \land \bigwedge_i \psi(x_i))$$

holds. She then constructed a formula which defines $N$ in $\mathcal{O}$, which only depends on $[F : \mathbb{Q}]$.

J. Robinson used the Hasse-Minkowski theorem on quadratic forms. On the other hand, using Hasse's Norm Theorem, R. Rumely [2] proved that the theory of global fields is undecidable. His formula is independent of global fields. Recently B. Poonen [3] extended the results. He proved that the theory of finitely generated fields over $\mathbb{Q}$ is undecidable.
We follow the method of J. Robinson. We will show that $\psi(t)$ includes $\mathbb{Z}$ and excludes non-algebraic integers in $K_l = \bigcup_n \mathbb{Q}(\zeta_{m^n})$, where $\psi(t)$ is the formula which she used in [1]. We then will show that for any positive integer $k$, there is a prime $p > k$ such that $\mathbb{Z} \cup p\psi(K_l)$ is $\emptyset$-definable, from which the interpretability of $\mathbb{Z}/(p)$ in $K_l$ follows.

In section 2, we describe construction of $\psi(t)$ in [1]. In section 3, we extend the result to $K_l$, and in section 4, we prove that for any positive integer $k$, there is a prime $p > k$ such that $\mathbb{Z} \cup p\psi(K_l)$ is $\emptyset$-definable.

In section 5, we prove that for any positive integer $k$, there is a prime $q > k$ such that any direct product of $\mathbb{Z}/(q)$ is interpretable in the ring of algebraic integers of $\bigcup_n \mathbb{Q}(\zeta_{m^n})$, where $m$ is an arbitrary positive integer and $\zeta_{m^n}$ is a primitive $m^n$-th root of unity.

2 Construction of $\psi(t)$

Let $F$ be a number field (a finite algebraic extension of the rationals $\mathbb{Q}$) and let $\mathcal{O}$ be the ring of algebraic integers of $F$. By $p$ we denote a valuation of $F$ and by $F_p$ the completion of $F$ with respect to $p$. Since non-Archemedean valuations of $F$ are $p$-adic valuations for some prime ideal $p$ of $F$, we use the same letter $p$ for both the valuation and the prime ideal. Let $p$ be a prime ideal of $F$ and $a \in F$. By $\nu_p(a)$ we denote the order of $a$ at $p$. Given $a, b \in F^*$, we use Hilbert symbol $(a, b)_p$, which is defined to be $+1$ if $ax^2 + by^2 = 1$ is solvable in $F_p$, otherwise defined to be $-1$.

The following lemma is well-known:

**Lemma 1** $h \in F^*$ can be represented by the form $x^2 - ay^2 - bz^2$ iff $-ab/h \not\in F_p^2$ for any valuation $p$ such that $(a, b)_p = -1$.

This follows the property of quaternary quadratic forms and the Hasse-Minkowski theorem on quadratic forms. See [4, p. 187] and [6, p.111].

Using this lemma, J. Robinson proved the following:

(1) Let $m$ be a positive integer such that $p^m \not\mid 2$ for all prime ideals $p$. Let $\varphi(s, u, t)$ be

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

For $t \not\in \mathcal{O}$, there are $a, b \in \mathcal{O}$ such that

1. $F \models \neg \varphi(a, b, t),$
2. $F \models \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1)).$
Then we can use inductive form: Let $\psi(t)$ 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 $F$, $\psi(F)$, includes $\mathbb{Z}$ but excludes non-algebraic integers, that is, $\mathbb{Z} \subseteq \psi(F) \subseteq \mathcal{O}$. Since $\varphi(s, u, 0)$ holds for every $s, u \in F$, the inductive form insures that every positive integer satisfy $\psi$. Since $\varphi(s, u, t) \leftrightarrow \varphi(s, u, -t)$, every rational integer also satisfies $\psi$. The above statement (†) shows that non-algebraic integers fail to satisfy $\psi$. Note that for $t \not\in \mathcal{O}$ (and for $t \in \mathcal{O}$), it is not so difficult to find $a, b \in F$ such that 1 holds, but difficult to find $a, b$ such that both 1 and 2 hold.

J. Robinson proved the above statement from two lemmas. We state these two lemmas in a little bit different forms for our sake. Before stating these lemmas, we need some lemmas. The following two lemmas are special cases of a theorem proved in [5, p.166].

**Lemma 2** There are infinitely many prime ideals in every ideal class.

**Lemma 3** If $a \in \mathcal{O}$ is prime to an ideal $\mathfrak{m}$, there are infinitely many prime elements $p \in \mathcal{O}$ such that $p \equiv a \pmod{\mathfrak{m}}$.

**Lemma 4** Let $a \in \mathcal{O}$ and $\nu_{\mathfrak{p}}(a) = 1$. Then there is $b \in \mathcal{O}$ with $p \nmid b$ such that $(a, b)_{\mathfrak{p}} = -1$.

**Proof.** It is proved in [4, pp.161-165] that there is a unit in a local field $M$ such that it is congruent to a square $\pmod{4\sigma}$ but not $\pmod{4\mathfrak{p}}$, where $\sigma$ is the ring of integers and $\mathfrak{p}$ a prime ideal of $M$. And if $\epsilon$ is such a unit, $(a, \epsilon)_{\mathfrak{p}} = -1$ for a prime element $a$. Take such a unit $\epsilon \in F_{\mathfrak{p}}$. There is a unit $\epsilon_{0} \in F$ such that $\epsilon_{0} \equiv \epsilon \pmod{4\mathfrak{p}}$. $\epsilon_{0}$ is congruent to a square $\pmod{4\mathcal{O}}$ but not $\pmod{4\mathfrak{p}}$.

J. Robinson proved this lemma using Hasse's formula evaluating the Hilbert symbol.

We state two basic lemmas due to J. Robinson [1, Lemma 8,9].

**Lemma 5** Given a prime ideal $\mathfrak{p}_{1}$ of $F$ and an odd prime number $l$, there are relatively prime elements $a$ and $b$ in $\mathcal{O}^{*}$ such that

1. $(a) = \mathfrak{p}_{1} \cdots \mathfrak{p}_{2k}$, where $\mathfrak{p}_{1}, \ldots, \mathfrak{p}_{2k}$ are distinct prime ideals which include every prime ideals which divides 2, and $p_{j}$ dose not divide $l$ for $j = 2, \ldots, 2k$, and

2. $b$ is a totally positive prime element such that $(a, b)_{\mathfrak{p}} = -1$ iff $p | a$.

**Proof.** Let $\mathfrak{p}_{1}, \ldots, \mathfrak{p}_{2k-1}$ be a set of distinct prime ideals such that it includes every prime idals dividing 2 and $p_{j}$ dose not divide $l$ for $j = 2, \ldots, 2k - 1$. Let $\mathfrak{R}$ be the ideal class which contains the product $\mathfrak{p}_{1} \cdots \mathfrak{p}_{2k-1}$. By Lemma 2 we can choose a
prime ideal \( p_{2k} \) in the ideal class \( \mathfrak{R}^{-1} \) with \( p_{2k} \neq p_i \) for \( i = 1, \ldots, 2k - 1 \) and with \( p_{2k} \not\parallel (l) \).

For \( i = 1, \ldots, 2k \), by Lemma 4 we can choose \( b_i \in \mathcal{O} \) prime to \( p \) so that \( (a, b_i)_p = -1 \). Let \( m \) be a positive integer such that \( p^m \not\parallel 2 \) for every prime ideal \( p \). Consider the simultaneous system of congruences

\[ x \equiv b_i \pmod{p_i^{2m}} \text{ for } i = 1, \ldots, 2k. \]

By the Chinese Remainder Theorem, there is a solution \( c \in \mathcal{O} \) and so is every element which is congruent to \( c \pmod{p_1^{2m} \cdots p_{2k}^{2m}} \). Since \( c \) is prime to the modulus, by Lemma 3 there are infinitely many totally positive prime elements \( p \) such that

\[ p \equiv c \pmod{p_1^{2m} \cdots p_{2k}^{2m}}. \]

Let \( b \) be one of such elements. \( b \) is coprime to \( a \).

We claim that \( b_i/b \in F^2_{p_i} \) for each \( i \); since \( b \equiv b_i \pmod{p_i^{2m}} \) and \( b_i \) is prime to \( p_i \), \( \nu_{p_i}(1 - b_i/b) > \nu_{p_i}(4) \), then applying Hensel's lemma ([5, p.42]) with \( x^2 - b_i/b \) and \( x = 1 \), we get that \( b_i/b \in F^2_{p_i} \). Hence \( (a, b)_p = -1 \) for each \( i \). On the other hand, \( (a, b)_p = +1 \) for all Archimedean valuations \( p \) since \( b \) is totally positive. It is easy to see that if \( (a, b)_p = -1 \) then \( p \) is an Archimedean valuation or the prime ideal \( p \) dividing \( 2ab \) (see [4, p. 166]). Then the only other valuation for which \( (a, b)_p = -1 \) could hold would be \( p = (b) \); but, by the product formula for the Hilbert symbol ([4, p.190]), \( (a, b)_p = -1 \) for an even number of valuations. Therefore \( (a, b)_p = -1 \) iff \( p|a \).

\[ \square \]

**Lemma 6** Let \( (a) = p_1 \cdots p_{2k} \) such that \( p_1, \ldots, p_{2k} \) are distinct prime ideals which include every prime ideals which divides 2, and let \( b \in \mathcal{O}^* \) be coprime to a such that \( (a, b)_p = -1 \) iff \( p|a \), and \( m \) be a positive integer such that \( p^m \not\parallel 2 \) for every prime ideal \( p \). Then,

\[ 1 - abc^{2m} = x^2 - ay^2 - bz^2 \text{ is solvable for } x, y \text{ and } z \text{ in } F \text{ iff } \nu_{p_i}(c) \geq 0 \text{ for each } i. \]

**Proof.** Let \( h = 1 - abc^{2m} \). Suppose that \( \nu_{p_i}(c) \geq 0 \) for each \( i \). Since \( \nu_{p_i}(h) = 0 \) and \( \nu_{p_i}(-ab) = 1 \), \( h/(-ab) \notin F^2_{p_i} \) for each \( i \). By Lemma 1 and the assumption, \( h = x^2 - ay^2 - bz^2 \) is solvable for \( x, y \) and \( z \) in \( F \).

Now suppose that \( \nu_{p_i}(c) < 0 \) for some \( i \). Let \( \nu_{p_{i_0}}(c) < 0 \). We show that \( -ab/h \in \mathcal{O}^* \). Since \( \nu_{p_{i_0}}(1 - (-ab/h)) > \nu_{p_{i_0}}(4) \), applying again Hensel's lemma with \( x^2 - (-ab/h) \) and \( x = 1 \), we get that \( -ab/h \in \mathcal{O}^* \). It follows that \( h = x^2 - ay^2 - bz^2 \) is not solvable for \( x, y \) and \( z \) in \( F \).

\[ \square \]

It is easy to derive the statement (†) from the above two lemmas, noting \( \nu_p(c) = \nu_p(c+1) \) for every prime ideal \( p \).
3 \( \psi(t) \) in towers of cyclotomic fields

Let \( F_n = \mathbb{Q}(\zeta_l) \), where \( l \) is an odd prime and \( \zeta_l \) is a primitive \( l^n \)-th root of unity, and let \( K_l = \bigcup_n \mathbb{Q}(\zeta_{l^n}) \) \((F_0 = \mathbb{Q})\). We denote by \( \mathcal{O}_n \) the ring of algebraic integers in \( F_n \) and by \( \mathcal{O}_{K_l} \) the ring of algebraic integers in \( K_l \). Then \( \mathcal{O}_{K_l} = \bigcup_n \mathcal{O}_n \).

The following lemma is well-known and proved in [7, pp.256-258]. We denote by \( \phi \) Euler’s function.

**Lemma 7** Let \( M = \mathbb{Q}(\zeta_m) \), where \( m \) is an positive integer and \( \zeta_m \) is a primitive \( m \)-th root of unity. Then

1. \( [M : \mathbb{Q}] = \phi(m) \),

2. the only ramified prime ideals in \( M \) are those dividing \( m \), and especially there is only one prime \( \mathfrak{p} = (1 - \zeta_m) \) of \( F_n \) lying above \( l \), and it is totally ramified,

3. given a prime number \( p \) coprime to \( m \), we let \( f \) be the least positive integer such that \( p^f \equiv 1 \pmod{m} \), and set \( \phi(m) = fg \). Then in \( M \), \( \mathfrak{p} = \mathfrak{p}_{1} \cdots \mathfrak{p}_{g} \), where \( \mathfrak{p}_{i} \) are primes of \( M \). The residue degree of each \( \mathfrak{p}_{i} \) in \( M/\mathbb{Q} \) is equal to \( f \), and the degree of the decomposition field \( \mathfrak{p}_{i} \) in \( F_n \) over \( \mathbb{Q} \) is equal to \( g \) for each \( i \).

From the above lemma we easily see that,

**Lemma 8** Let \( 0 < i < j \) and \( \mathfrak{p} \) be a prime ideal of \( F_i \). Then

1. If \( \mathfrak{p} \nmid l \), then in \( F_j \), \( \mathfrak{p} = \mathfrak{P}_{1} \cdots \mathfrak{P}_{k} \), where \( \mathfrak{P}_{r} \) are primes in \( F_j \) and \( k \) divides \( [F_j : F_i] = l^{j-i} \).

2. If \( \mathfrak{p} \mid l \), then in \( F_j \), \( \mathfrak{p} = \mathfrak{P}^{l^{j-i}} \), where \( \mathfrak{p} = (1 - \zeta_{l^i}, \mathfrak{P} = (1 - \zeta_{l^i}) \).

The next lemma is also proved in [7, p.272].

**Lemma 9** Let \( K \supset k \) be number fields and \( \mathfrak{P} \supset \mathfrak{p} \) be primes of \( K \) and \( k \) respectively. For \( \alpha \in K_{\mathfrak{P}}^{*} \), let \( a = N_{K_{\mathfrak{P}}/k_{\mathfrak{P}}} (\alpha) \) and \( b \in k_{\mathfrak{P}} \). Then, \( (\alpha, b)_{\mathfrak{P}} = (a, b)_{\mathfrak{P}} \).

The next lemma follows from Lemma 9.

**Lemma 10** Let \( 0 < i < j \), \( \mathfrak{p} \) a prime ideal of \( F_i \) and \( \mathfrak{P} \) be a prime in \( F_j \) lying over \( \mathfrak{p} \). Then for \( a, b \in F_{i}^{*} \), \((a, b)_{\mathfrak{p}} = 1 \) iff \((a, b)_{\mathfrak{P}} = 1 \).

**Proof.** Since \( F_j/F_i \) is an abelian extension, the local degree at \( \mathfrak{P} \) divides the degree of \( F_j/F_i \), that is, \( [(F_j)_{\mathfrak{P}} : (F_i)_{\mathfrak{P}}][F_j : F_i] \) (see [4, p.32]). Let \( u \) be the local degree at \( \mathfrak{P} \). Then \( N_{K_{\mathfrak{P}}/k_{\mathfrak{P}}} (a) = a^{u} \) and \( (a, b)_{\mathfrak{P}} = (a^{u}, b)_{\mathfrak{P}} = (a, b)_{\mathfrak{P}}^{u} \) since \( u \) is odd, it follows that \((a, b)_{\mathfrak{p}} = 1 \) iff \((a, b)_{\mathfrak{P}} = 1 \). \( \square \)

We now extend J. Robinson’s result [1] to \( K_{l} \). Note that in each \( F_n \), \( \mathfrak{p}^2 \nmid 2 \) for every prime ideal in \( F_n \).
Theorem 11 Let \( \varphi(s, u, t) \) be

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

and \( \psi(t) \) be

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

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

Proof. It is clear that \( \mathbb{Z} \subseteq \psi(K_l) \). Let \( t \in K_l \setminus \mathbb{O}_K \). For this \( t \), we show that there are \( a, b \in K_l \) such that

\[ K_l \models \neg \varphi(a, b, t) \land \forall c(\varphi(a, b, c) \rightarrow \varphi(a, b, c + 1)). \]

We fix \( F_m \) such that \( t \in F_m \) and \( m > 1 \). Then \( \nu_{p_1}(t) < 0 \) for some prime \( p_1 \) in \( F_m \).

By Lemma 5, there are relatively prime elements \( a \) and \( b \) in \( \mathbb{O}_m \) such that

1. \( (a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k} \), where \( \mathfrak{p}_1, \ldots, \mathfrak{p}_{2k} \) are distinct prime ideals in \( F_m \) which include every prime ideals in \( F_m \) which divides 2, and \( \mathfrak{p}_j \) dose not divide \( l \) for \( j = 2, \ldots, 2k \), and

2. \( b \) is a totally positive prime element in \( F_m \) such that \( (a, b)_p = -1 \) iff \( p|a \).

By Lemma 6, \( 1 - abt^4 = x^2 - ay^2 - bz^2 \) is not solvable for \( x, y \) and \( z \) in \( F_m \), and for every \( c \in F_m \), if \( F_m \models \varphi(a, b, c) \) then \( F_m \models \varphi(a, b, c + 1) \).

For this \( a, b \), it is enough to show that for every \( s > m \) such that \( s - m \) is even, \( 1 - abt^4 = x^2 - ay^2 - bz^2 \) is not solvable for \( x, y \) and \( z \) in \( F_s \), and for every \( c \in F_s \), if \( F_s \models \varphi(a, b, c) \) then \( F_s \models \varphi(a, b, c + 1) \).

Note that \( a, b \) are relatively prime also in \( \mathbb{O}_s \).

Case 1: \( p_1 \nmid l \).

By Lemma 8, the decomposition of the ideal \( (a) \) in \( F_s \) is given by \( (a) = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r} \), where \( \mathfrak{P}_1, \ldots, \mathfrak{P}_{2r} \) are mutually distinct prime ideals and include every prime ideals which divides 2. By Lemma 10, \( (a, b)_{\mathfrak{P}} = -1 \) iff \( \mathfrak{P}|a \). We let \( p_1 \subseteq \mathfrak{P}_1 \). Since \( \nu_{p_1}(t) < 0 \), we have that \( \nu_{p_1}(t) < 0 \). By Lemma 6, we conclude that \( 1 - abt^4 = x^2 - ay^2 - bz^2 \) is not solvable for \( x, y \) and \( z \) in \( F_s \), and for every \( c \in F_s \), if \( F_s \models \varphi(a, b, c) \) then \( F_s \models \varphi(a, b, c + 1) \).

Case 2: \( p_1|l \).

By Lemma 8, the decomposition of the ideal \( (a) \) in \( F_s \) is given by

\[ (a) = \mathfrak{P}_1^{t_{p_1} - m} \cdots \mathfrak{P}_{2r}, \]
where $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2r'}$ are mutually distinct prime ideals and include every prime ideals which divides $2$, and $p_1 = (1 - \zeta_{l^m})$, $\mathfrak{P}_1 = (1 - \zeta_{l^r})$.

Let $a' = a/(1 - \zeta_{l^r})^{l^m-1}$. Then $a' \in \mathcal{O}_s$ and $(a') = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r'}$ in $F_s$.

Since $a = a'((1 - \zeta_{l^r})^{(l^m-1)/2})^2$, $(a, b)\mathfrak{P}_i = (a', b)\mathfrak{P}_i$ for each $i$. Hence we have that $(a', b)\mathfrak{P}_1 = -1$ iff $\mathfrak{P}|a'$.

Suppose that $1 - abt^4 = x^2 - ay^2 - bz^2$ were solvable for $x, y$ and $z$ in $F_s$. Then

$$1 - a'b(t(1 - \zeta_{l^r})^{(l^m-1)/4})^4 = x^2 - a'((1 - \zeta_{l^r})^{(l^m-1)/2}y)^2 - bz^2$$

is solvable for $x, y$ and $z$ in $F_s$, noting that $(l^{s-m}-1)/4$ is a positive integer since $l - m$ is even. But $\nu_{\mathfrak{P}_1}(t(1 - \zeta_{l^r})^{(l^m-1)/4}) < 0$ since $p_1 = \mathfrak{P}_1^{l^m-1}$. We have a contradiction by Lemma 6.

Next we show that if $F_s \models \varphi(a, b, c)$ then $F_s \models \varphi(a, b, c + 1)$. Suppose that $F_s \models \varphi(a, b, c)$, that is, $1 - abc^4 = x^2 - ay^2 - bz^2$ is solvable for $x, y$ and $z$ in $F_s$. Then

$$1 - a'b(c(1 - \zeta_{l^r})^{(l^s-m-1)/4})^4 = x^2 - a'((1 - \zeta_{l^r})^{(l^s-m-1)/2}y)^2 - bz^2$$

is solvable for $x, y$ and $z$ in $F_s$. By Lemma 6, $\nu_{\mathfrak{P}_i}(c(1 - \zeta_{l^r})^{(l^s-m-1)/4}) \geq 0$ for each $\mathfrak{P}_i$. It follows that $\nu_{\mathfrak{P}_i}((c + 1)(1 - \zeta_{l^r})^{(l^s-m-1)/4}) \geq 0$ for each $\mathfrak{P}_i$. Therefore we have that $F_s \models \varphi(a, b, c + 1)$. \qed

### 4 Interpreting finite prime fields in $K_l$

The next lemma follows from [7, p.145].

**Lemma 12** Let $F/\mathbb{Q}$ be a finite Galois extension, and $p$ be an extension of a prime number $p$ to $F$. Let $F_{Z}$ denote the decomposition field of $p$ in $F/\mathbb{Q}$. Finally, let $F'$ be an intermediate field of $F/\mathbb{Q}$, and let $p'$ denote the restriction of $p$ to $F'$. Then we have:

$F' \subseteq F_{Z}$ iff both the ramification index and the residue degree of $p'$ in $F'/\mathbb{Q}$ are equal to 1.

Recall that when $F/\mathbb{Q}$ is abelian, all the prime ideals $p$ dividing $p$ have the same decomposition field in $F/\mathbb{Q}$, and we call it the decomposition field of $p$ in $F/\mathbb{Q}$. Furthermore, under the additional assumption that $F/\mathbb{Q}$ is unramified at $p$ (that is, $F/\mathbb{Q}$ is unramified at every prime ideal dividing $p$), the Galois group $G(F/F_{Z})$ is cyclic and generated by the Artin automorphism $\sigma = (p, F/\mathbb{Q})$ which is characterized by the congruence $\sigma(a) \equiv a^p \pmod{p}$ for $a \in \mathcal{O}_F$, where $\mathcal{O}_F$ is the ring of algebraic integers in $F$.

**Lemma 13** Let $l$ be an odd prime. Then, for any positive integer $k$, there is a prime number $p > k$ such that $p$ is a primitive root modulo every power of $l$. 

Proof. Let \( r \) be a primitive root modulo \( l \). Since \( r^{l-1} \equiv 1 \pmod{l} \), \( r^{l-1} = 1 + kl \) for some \( k \). We may suppose that \( (k, l) = 1 \), that is, \( k \) is coprime to \( l \): if \( r^{l-1} = 1 + kl^{m} \) with \( m > 1 \), then we may take \( r + l \) as a primitive root. By the Theorem of Arithmetic Progression, the congruence class \( r \pmod{l^{2}} \) contains an infinity of primes. Let \( p > k \) be a prime in that class. \( p \) is coprime to \( l \), and is a primitive root modulo \( l \) such that \( p^{l-1} = 1 + k'l \) for some \( k' \) with \( (k', l) = 1 \).

Let \( a \) be an integer of the form \( 1 + k'l \) for some \( k' \) with \( (k', l) = 1 \). By the binomial formula, for every \( h \geq 2 \), we can show that \( f = l^{h-1} \) is the least positive integer such that \( a^{f} \equiv 1 \pmod{l^{h}} \). Therefore \( p \) is a primitive root modulo every power of \( l \). \( \square \)

Lemma 14 Let \( F/\mathbb{Q} \) be a finite abelian extension, and be unramified at a prime number \( p \). Let \( F_{Z} \) be the decomposition field of \( p \), and let \( \sigma, \sigma_{Z} \) be the ring of algebraic integers of \( F, F_{Z} \) respectively. Then, for \( a \in \sigma \),

\[
a \in \sigma_{Z} \cup p\mathfrak{o} \iff a^{p} \equiv a \pmod{p}.
\]

Proof. Let \( \sigma \) denote the Artin automorphism in \( G(F/F_{Z}) \). Let \( a \in \sigma \).

If \( a \in \sigma_{Z} \), then \( \sigma(a) = a \) and \( \sigma(a) \equiv a^{p} \pmod{p} \). Thus we have that \( a^{p} \equiv a \pmod{p} \). If \( a \in p\mathfrak{o} \), clearly \( a^{p} \equiv a \pmod{p} \) holds.

Suppose that \( a \not\in \sigma_{Z} \cup p\mathfrak{o} \). Let \( \sigma' \) denote the ring of algebraic integers in \( \mathbb{Q}(a) \).

Since \( p\mathfrak{o}' \) is the intersection of prime ideals in \( \sigma' \) including \( p\mathbb{Z} \), there is an extension \( p\mathfrak{o}' \) of \( p\mathbb{Z} \) to \( \sigma' \) such that \( a \not\in p\mathfrak{o}' \). The ramification index of \( p\mathfrak{o}' \) in \( \mathbb{Q}(a)/\mathbb{Q} \) is equal to 1 since \( p \) is unramified in \( F/\mathbb{Q} \). Since \( \mathbb{Q}(a) \not\subset F_{Z} \), by Lemma 12, the residue degree of \( p\mathfrak{o}' \) in \( \mathbb{Q}(a)/\mathbb{Q} \) is greater than 1, that is, \( [\sigma'/p\mathfrak{o}' : \mathbb{Z}/(p)] > 1 \). Hence we have that \( a^{p} \not\equiv a \pmod{p} \).

We keep the notation of section 3.

Theorem 15 For any positive integer \( k \), there is a prime \( p > k \) such that \( \mathbb{Z} \cup p\mathcal{O}_{K_{i}} \) is \( \emptyset \)-definable in \( \mathcal{D}_{K_{i}} \), hence \( \mathbb{Z}/(p) \) is interpretable in \( \mathcal{D}_{K_{i}} \).

Proof. Take a prime number \( p > k \) as in Lemma 13. Then, by Lemma 7, the decomposition field of \( p \) in \( F_{n}/\mathbb{Q} \) is \( \mathbb{Q} \) for every \( n \), and \( p \) is unramified in every extension \( F_{n}/\mathbb{Q} \). Let \( \theta(t) \) be the formula \( \exists w(t^{p} - t = pw) \). By Lemma 14, \( \theta(t) \) defines \( \mathbb{Z} \cup p\mathcal{O}_{K_{i}} \) in \( \mathcal{D}_{K_{i}} \). \( \square \)

Theorem 16 \( \mathbb{Z} \cup p\psi(K_{i}) \) is \( \emptyset \)-definable in \( K_{i} \), hence \( \mathbb{Z}/(p) \) is interpretable in \( K_{i} \).

Proof. Consider the formula

\[
\psi(t) \land \exists w(\psi(w) \land t^{p} - t = pw).
\]

It is evident that this formula defines \( \mathbb{Z} \cup p\psi(K_{i}) \) in \( K_{i} \). \( \square \)
5 Interpreting direct products of finite fields in $\mathcal{D}_{K_m}$

Let $m$ be a positive integer, and let $K_m, \mathcal{D}_{K_m}, F_n$ and $\mathcal{D}_n$ be as before. Our methods do not suffice to treat $K_2$, since Lemma 10 fails. They also do not suffice to treat $K_m$ with $m$ odd; Lemma 10 holds but the proof of Theorem 11 fails. In this section we will prove that for a given positive integer $k$, there is a prime $q > k$ such that certain direct products of $\mathbb{Z}/(q)$ is interpretable in $\mathcal{D}_{K_m}$ with $m$ arbitrary.

Lemma 17 Let $m$ be a positive integer with the prime factorization $2^{h_0}p_1^{h_1}p_2^{h_2} \cdots p_k^{h_k}$.

Then for a given positive integer $k$, there is a prime number $q > k$ coprime to $m$ such that

1. if $h_0 = 0$, then the order of $q$ in $(\mathbb{Z}/m^{r}\mathbb{Z})^*$ is equal to $p_1^{rh_1-1}p_2^{rh_2-1} \cdots p_k^{rh_k-1}$ for every $r \geq 1$,

2. if $h_0 > 0$, then the order of $q$ in $(\mathbb{Z}/m^{r}\mathbb{Z})^*$ is equal to $2^{rh_0-2}p_1^{rh_1-1}p_2^{rh_2-1} \cdots p_k^{rh_k-1}$ for every $r \geq 2$.

Proof. For each odd prime $p_i$, we know that there is an integer $u_i$ such that $u_i^{p_i-1}$ is of the form $1 + k'p_i$ for some $k'$ which is coprime to $p_i$, and every integer of that form is of order $p_i^{r-1}$ in $(\mathbb{Z}/p_i^r\mathbb{Z})^*$ for every $r \geq 1$. Let $s_i = u_i^{p_i-1}$. On the other hand, we see that by the binomial formula, the order of 5 in $(\mathbb{Z}/2^r\mathbb{Z})^*$ is equal to $2^{r-2}$ for every $r \geq 2$, and

$$(\mathbb{Z}/2^r\mathbb{Z})^* \cong \langle -1 \rangle \times \langle 5 \rangle.$$ 

Furthermore, also by the binomial formula, we see that every integer of the form $1 + 2^r k'$ with $k'$ odd is also of order $2^{r-2}$ in $(\mathbb{Z}/2^r\mathbb{Z})^*$ for $r \geq 2$. By the Chinese Remainder Theorem and the Theorem of Arithmetic Progression, there is a prime number $q$ such that

$q \equiv 5 \pmod{2^3}, q \equiv s_i \pmod{p_i^2}$ for $i = 1, \ldots, k.$

$q$ is coprime to $m$ and is of the form $1 + k' p_i$ for some $k'$ coprime to $p_i$ for each $i$, and is of the form $1 + 2^r k'$ with $k'$ odd. □

Lemma 18 Let $L/\mathbb{Q}$ be a finite Galois extension, and let $M$ be an intermediate field of $L/\mathbb{Q}$ such that $M/\mathbb{Q}$ is a Galois extension. Let $p \supset p' \supset p$ be primes of $L, M$ and $\mathbb{Q}$ respectively and let $L_Z, M_{Z'}$ be the decomposition field of $p$ in $L/\mathbb{Q}$ and $p'$ in $M/\mathbb{Q}$ respectively. Then $M_{Z'} \subseteq L_Z$. 
Proof. Let \( Z, Z' \) be the decomposition groups of \( \mathfrak{p} \) in \( L/\mathbb{Q} \) and \( \mathfrak{p}' \) in \( M/\mathbb{Q} \) respectively. Let \( a \in M_{Z'} \). We must show that for \( \sigma \in Z \), \( \sigma(a) = a \) holds. Since \( M/\mathbb{Q} \) is a Galois extension,

\[
(\mathfrak{p}')^{\sigma} = (\mathfrak{p} \cap M)^{\sigma} = \mathfrak{p}^{\sigma} \cap M = \mathfrak{p} \cap M = \mathfrak{p}.
\]

This shows that the restriction of \( \sigma \) to \( M, \sigma|_{M} \), is in \( Z' \). Then \( \sigma(a) = \sigma|_{M}(a) = a \).

\[
\square
\]

Lemma 19 Let \( M_{0} = \mathbb{Q}(\zeta_{m_{0}}) \), where \( m_{0} = p_{1}p_{2}\cdots p_{k} \), and let \( M_{1} = \mathbb{Q}(\zeta_{m_{1}}) \), where \( m_{1} = 4p_{1}p_{2}\cdots p_{k} \). Furthermore, for \( i = 1, 2 \) let \( a_{i} \) be the ring of algebraic integers in \( M_{i} \) respectively.

Then, for any positive integer \( k \), there is a prime \( p > k \) such that \( 0_{K_{m}} \cup pD_{K_{m}} \) is \( \emptyset \)-definable in \( \mathcal{O}_{K_{m}} \) with \( m \) odd. Similarly, for any positive integer \( k \), there is a prime \( p > k \) such that \( 0_{K_{m}} \cup pD_{K_{m}} \) is \( \emptyset \)-definable in \( \mathcal{O}_{K_{m}} \) with \( m \) even.

Proof. Take a prime number \( q \) as in Lemma 17.

Let \( m \) be odd. Then, by Lemma 7, \( q \) is unramified in \( F_{n}/\mathbb{Q} \) and the decomposition field of \( q \) in \( F_{n}/\mathbb{Q} \) is of degree \((p_{1} - 1)\cdots(p_{k} - 1)\) over \( \mathbb{Q} \) for every \( n \) > 0. By Lemma 18, we see that those decomposition fields coincide. Let \( L \) be the common decomposition field. Also by Lemma 18, for each \( i \), \( L \) includes the decomposition field of \( q \) in \( \mathbb{Q}(\zeta_{p_{1}^{h_{1}}})/\mathbb{Q} \), which is of degree \( p_{i} - 1 \) over \( \mathbb{Q} \). Since \( \mathbb{Q}(\zeta_{p_{i}^{h_{1}}})/\mathbb{Q} \) is a cyclic extension, \( \mathbb{Q}(\zeta_{p_{i}}) \) is the only intermediate field with degree \( p_{i} - 1 \). Hence \( L \) includes \( \mathbb{Q}(\zeta_{p_{1}})\cdots \mathbb{Q}(\zeta_{p_{k}}) \), which is of degree \((p_{1} - 1)\cdots(p_{k} - 1)\). Therefore \( L = \mathbb{Q}(\zeta_{p_{1}})\cdots \mathbb{Q}(\zeta_{p_{k}}) = M_{0} \). (See [5, p. 74].) Let \( \theta(t) \) be as before. By Lemma 14, \( \theta(t) \) defines \( 0_{K_{m}} \cup qD_{K_{m}} \) in \( \mathcal{O}_{K_{m}} \).

Let \( m \) be even. We note that \( \langle q \rangle \) is the only subgroup of order \( 2^{n-2} \) in \( (\mathbb{Z}/2^{r}\mathbb{Z})^{*} \) with \( r > 2 \). Then similarly, \( q \) is unramified in every extension \( F_{n}/\mathbb{Q} \) and the decomposition field of \( p \) in \( F_{n}/\mathbb{Q} \) with \( n \) > 2 is \( M_{1} \). Hence \( \theta(t) \) also defines \( 0_{K_{m}} \cup qD_{K_{m}} \) in \( \mathcal{O}_{K_{m}} \).

\[
\square
\]

Theorem 20 Let \( m \) be as before. Then, for a given positive integer \( k \), there is a prime \( q > k \) such that

if \( m \) is odd,

\[
\frac{(p_{1}-1)\cdots(p_{k}-1)}{\mathbb{Z}/(q) \times \cdots \times \mathbb{Z}/(q)}
\]

is interpretable in \( \mathcal{O}_{K_{m}} \), and

if \( m \) is even,

\[
\frac{2(p_{1}-1)\cdots(p_{k}-1)}{\mathbb{Z}/(q) \times \cdots \times \mathbb{Z}/(q)}
\]

is interpretable in \( \mathcal{O}_{K_{m}} \).
Proof. Let \( n_0 = [M_0 : \mathbb{Q}] = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \), and let \( n_1 = [M_1 : \mathbb{Q}] = 2(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \). Clealy \( \mathfrak{o}_0/q_0 \) is interpretable in \( \mathfrak{O}_K \) with \( m \) odd. Since the decomposition of \( q\mathbb{Z} \) in \( \mathfrak{o}_0 \) is \( \mathfrak{p}_1 \cdots \mathfrak{p}_{n_0} \) and \( \mathfrak{o}_0/q_i \cong \mathbb{Z}/(q) \) for each \( i \), we have

\[
\mathfrak{o}_0/q_0 \cong \mathfrak{o}_0/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n_0}) \cong \mathbb{Z}/(q) \times \cdots \times \mathbb{Z}/(q).
\]

Similarly for \( m \) even. \( \square \)

References


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