数理解析研究所講究録
第 1555 巻 2007 年 93-103

Interpreting finite fields in towers of cyclotomic fields

鹿児島国際大学国際文化学部　福崎賢治 (Kenji Fukuzaki)
Faculty of Intercultural Studies,
The international University of Kagoshima

Abstract

Let l be an odd prime and ζ_{l^n} is a primitive l^n-th root of unity. We consider the towers of cylotomic 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 ζ_{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, $\mathbb{N}$ 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 $\mathfrak{O}$ of F is $\emptyset$-definable in F. Let $a_1, \ldots, a_s$ be an integral basis of $\mathfrak{O}$ ($s = [F : \mathbb{Q}]$) , 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

$$t \in \mathfrak{O} \Longleftrightarrow \exists x_1, \ldots, x_s, y_1, \ldots, y_s(t = x_1y_1 + \cdots + x_sy_s \wedge \bigwedge_i P_i(y_i) = 0 \wedge \bigwedge_i \psi(x_i))$$

holds. She then constructed a formula which defines $\mathbb{N}$ in $\mathfrak{O}$, 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 $K_l = \bigcup_n \mathbb{Q}(\zeta_{l^n})$, 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 some dirct 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 ζ_{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 $\mathfrak{O}$ be the ring of algebraic integers of F. By $\mathfrak{p}$ we denote a valuation of F and by $F_\mathfrak{p}$ the completion of F with respect to $\mathfrak{p}$. Since non-Archemedean valuations of F are $\mathfrak{p}$-adic valuations for some prime ideal $\mathfrak{p}$ of F, we use the same letter $\mathfrak{p}$ for both the valuation and the prim ideal. Let $\mathfrak{p}$ be a prime ideal of F and $a \in F$. By $\nu_\mathfrak{p}(a)$ we denote the order of a at $\mathfrak{p}$. Given $a, b \in F^*$, we use Hilbert symbol $(a,b)_\mathfrak{p}$, which is defined to be $+1$ if $ax^2 + by^2 = 1$ is solvable in $F_\mathfrak{p}$, 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 $-ab/h \notin F_\mathfrak{p}^{*2}$ for any valuation $\mathfrak{p}$ such that $(a,b)_\mathfrak{p} = -1$.*

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:

(†) *Let m be a positive integer such that $\mathfrak{p}^m \not| 2$ for all prime ideals $\mathfrak{p}$. Let $\varphi(s,u,t)$ be*

$$\exists x, y, z(1 - sut^{2m} = x^2 - sy^2 - uz^2).$$

For $t \notin \mathfrak{O}$, there are $a, b \in \mathfrak{O}$ such that

1. $F \models \neg\varphi(a,b,t)$,
2. $F \models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1))$.

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, $\mathbb{Z} \subseteq \psi(F) \subseteq \mathfrak{O}$. Since $\varphi(s,u,0)$ holds for every $s,u \in F$, the inductive form insures that every positive integer satisify ψ. Since $\varphi(s,u,t) \leftrightarrow \varphi(s,u,-t)$, every rational integer also satisfies ψ. The above statement (†) shows that non-algebraic integers fail to satisfy ψ. Note that for $t \notin \mathfrak{O}$ (and for $t \in \mathfrak{O}$), 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 $a \in \mathfrak{O}$ is prime to an ideal $\mathfrak{m}$, there are infinitely many prime elements $p \in \mathfrak{O}$ such that $p \equiv a \pmod{\mathfrak{m}}$.*

Lemma 4 *Let $a \in \mathfrak{O}$ and $\nu_{\mathfrak{p}}(a) = 1$. Then there is $b \in \mathfrak{O}$ with $\mathfrak{p} \not| b$ 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 $\pmod{4\mathfrak{o}}$ but not $\pmod{4\mathfrak{p}}$, where $\mathfrak{o}$ is the ring of integers and $\mathfrak{p}$ a prime ideal of M. And if ϵ 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 $\epsilon_0 \equiv \epsilon \pmod{4\mathfrak{p}}$. ϵ_0 is congruent to a square $\pmod{4\mathfrak{O}}$ 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 $\mathfrak{O}^*$ 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 $\mathfrak{p}_j$ 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 $\mathfrak{p} | a$.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k-1}$ be a set of disticnt prime ideals such that it includes every prime idals dividing 2 and $\mathfrak{p}_j$ dose not divide l for $j = 2, \ldots, 2k-1$. Let $\mathfrak{K}$ 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 $\mathfrak{p}_{2k}$ in the ideal class $\mathfrak{K}^{-1}$ with $\mathfrak{p}_{2k} \neq \mathfrak{p}_i$ for $i = 1, \ldots, 2k-1$ and with $\mathfrak{p}_{2k} \not| (l)$.

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

$$x \equiv b_i \pmod{\mathfrak{p}_i^{2m}} \quad \text{for } i = 1, \ldots, 2k.$$

By the Chinese Remainder Theorem, there is a solution $c \in \mathfrak{O}$ and so is every element which is congruent to $c \pmod{\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}}$. Since c is prime to the modulus, by Lemma 3 there are infinitely many totally positive prime elements p such that

$$p \equiv c \pmod{\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}}.$$

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

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

Lemma 6 *Let $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$ such that $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k}$ are distinct prime ideals which include every prime ideals which divides 2, and let $b \in \mathfrak{O}^*$ be coprime to a such that $(a, b)_{\mathfrak{p}} = -1$ iff $\mathfrak{p} | a$, and m be a positive integer such that $\mathfrak{p}^m \not| 2$ for every prime ideal $\mathfrak{p}$. Then,*

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

Proof. Let $h = 1 - abc^{2m}$. Suppose that $\nu_{\mathfrak{p}_i}(c) \geq 0$ for each i. Since $\nu_{\mathfrak{p}_i}(h) = 0$ and $\nu_{\mathfrak{p}_i}(-ab) = 1$, $h/(-ab) \notin F_{\mathfrak{p}_i}^2$ 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 $\nu_{\mathfrak{p}_i}(c) < 0$ for some i. Let $\nu_{\mathfrak{p}_{i_0}}(c) < 0$. We show that $-ab/h \in F_{\mathfrak{p}_{i_0}}^2$. Since $\nu_{\mathfrak{p}_{i_0}}(1 - (-ab/h)) > \nu_{\mathfrak{p}_{i_0}}(4)$, applying again Hensel's lemma with $x^2 - (-ab/h)$ and $x = 1$, we get that $-ab/h \in F_{\mathfrak{p}_{i_0}}^2$. It follows that $h = x^2 - ay^2 - bz^2$ is not solvable for x, y and z in F. □

It is easy to derive the statement (†) from the above two lemmas, noting $\nu_{\mathfrak{p}}(c) = \nu_{\mathfrak{p}}(c+1)$ for every prime ideal $\mathfrak{p}$.

3 $\psi(t)$ in towers of cyclotomic fields

Let $F_n = \mathbb{Q}(\zeta_{l^n})$, where l is an odd prime and ζ_{l^n} is a primitive l^n-th root of unity, and let $K_l = \bigcup_n \mathbb{Q}(\zeta_{l^n})$ $(F_0 = \mathbb{Q})$. 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 $\mathfrak{O}_{K_l} = \bigcup_n \mathfrak{O}_n$.

The following lemma is well-known and proved in [7, pp.256-258]. We denote by ϕ Euler's function.

Lemma 7 *Let $M = \mathbb{Q}(\zeta_m)$, where m is an positive integer and ζ_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 $\mathfrak{p} = (1 - \zeta_{l^n})$ 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, $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, 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 $\mathfrak{p} \not| l$, 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 $\mathfrak{p}|l$, then in F_j, $\mathfrak{p} = \mathfrak{P}^{l^{j-i}}$, where $\mathfrak{p} = (1 - \zeta_{l^i}), \mathfrak{P} = (1 - \zeta_{l^j})$.*

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 repectively. 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 $(a, b)_{\mathfrak{P}} = 1$. □

We now extend J. Robinson's result [1] to K_l. Note that in each F_n, $\mathfrak{p}^2 \not| 2$ 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

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

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

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

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

We fix F_m such that $t\in F_m$ and $m>1$. Then $\nu_{\mathfrak{p}_1}(t)<0$ for some prime $\mathfrak{p}_1$ in F_m. By Lemma 5, there are relatively prime elements a and b in $\mathfrak{O}_m$ such that

1. $(a)=\mathfrak{p}_1\cdots\mathfrak{p}_{2k}$, where $\mathfrak{p}_1,\dots,\mathfrak{p}_{2k}$ 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 $j=2,\dots,2k$, and
2. b is a totally positive prime element in F_m such that $(a,b)_{\mathfrak{p}}=-1$ iff $\mathfrak{p}|a$.

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 $\mathfrak{O}_s$.

Case 1: $\mathfrak{p}_1\nmid l$.

By Lemma 8, the decomposition of the ideal (a) in F_s is given by $(a)=\mathfrak{P}_1\cdots\mathfrak{P}_{2r}$, where $\mathfrak{P}_1,\dots,\mathfrak{P}_{2r}$ are mutually distinct prime ideals and include every prime ideals which devides 2. By Lemma 10, $(a,b)_{\mathfrak{P}}=-1$ iff $\mathfrak{P}|a$. We let $\mathfrak{p}_1\subset\mathfrak{P}_1$. Since $\nu_{\mathfrak{p}_1}(t)<0$, we have that $\nu_{\mathfrak{P}_1}(t)<0$. 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: $\mathfrak{p}_1|l$.

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

$$(a)=\mathfrak{P}_1^{l^{s-m}}\cdots\mathfrak{P}_{2r'},$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2r'}$ are mutually distinct prime ideals and include every prime ideals which devides 2, and $\mathfrak{p}_1 = (1-\zeta_{l^m}), \mathfrak{P}_1 = (1-\zeta_{l^s})$.

Let $a' = a/(1-\zeta_{l^s})^{l^{s-m}-1}$. Then $a' \in \mathfrak{O}_s$ and $(a') = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r'}$ in F_s.
Since $a = a'((1-\zeta_{l^s})^{(l^{s-m}-1)/2})^2$, $(a,b)_{\mathfrak{P}_i} = (a',b)_{\mathfrak{P}_i}$ for each i. Hence we have that $(a',b)_{\mathfrak{P}} = -1$ 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

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

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 $\nu_{\mathfrak{P}_1}(t(1-\zeta_{l^s})^{(l^{s-m}-1)/4}) < 0$ since $\mathfrak{p}_1 = \mathfrak{P}_1^{l^{s-m}}$. 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

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

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

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

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

Recall that when $F/\mathbb{Q}$ is abelian, all the prime ideals $\mathfrak{p}$ 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 $a \in \mathfrak{o}_F$, where $\mathfrak{o}_F$ 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. □

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 $\mathfrak{o}, \mathfrak{o}_Z$ be the ring of algebraic integers of F, F_Z respectively. Then, for $a \in \mathfrak{o}$,*

$$a \in \mathfrak{o}_Z \cup p\mathfrak{o} \;\; \textit{iff} \;\; a^p \equiv a \pmod{p}.$$

Proof. Let σ denote the Artin automorphism in $G(F/F_Z)$. Let $a \in \mathfrak{o}$.

If $a \in \mathfrak{o}_Z$, 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 $a \notin \mathfrak{o}_Z \cup p\mathfrak{o}$. Let $\mathfrak{o}'$ denote the ring of algebraic integers in $\mathbb{Q}(a)$. Since $p\mathfrak{o}'$ is the intersection of prime ideals in $\mathfrak{o}'$ including $p\mathbb{Z}$, there is an extension $\mathfrak{p}'$ of $p\mathbb{Z}$ to $\mathfrak{o}'$ such that $a \notin \mathfrak{p}'$. The ramification index of $\mathfrak{p}'$ in $\mathbb{Q}(a)/\mathbb{Q}$ is equal to 1 since $\mathfrak{p}$ is unramified in $F/\mathbb{Q}$. Since $\mathbb{Q}(a) \not\subseteq F_Z$, by Lemma 12, the residue degree of $\mathfrak{p}'$ in $\mathbb{Q}(a)/\mathbb{Q}$ is greater than 1, that is, $[\mathfrak{o}'/\mathfrak{p}' : \mathbb{Z}/(p)] > 1$. 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 $\mathbb{Z} \cup p\mathfrak{O}_{K_l}$ is $\emptyset$-definable in $\mathfrak{O}_{K_l}$, hence $\mathbb{Z}/(p)$ is interpretable in $\mathfrak{O}_{K_l}$.*

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 $\mathbb{Z} \cup p\mathfrak{O}_{K_l}$ in $\mathfrak{O}_{K_l}$. □

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

Proof. Consider the formula

$$\psi(t) \wedge \exists w(\psi(w) \wedge t^p - t = pw).$$

It is evident that this formula defines $\mathbb{Z} \cup p\psi(K_l)$ in K_l. □

5 Interpreting direct products of finite fields in $\mathfrak{O}_{K_m}$

Let m be a positive integer, and let $K_m, \mathfrak{O}_{K_m}, F_n$ and $\mathfrak{O}_n$ 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 poistive integer k, there is a prime $q > k$ such that certain direct products of $\mathbb{Z}/(q)$ is interpretable in $\mathfrak{O}_{K_m}$ 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 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 $1 + 2^2k'$ 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

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

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 $1 + 2^2k'$ 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 $\mathfrak{p} \supset \mathfrak{p}' \supset p$ be primes of L, M and $\mathbb{Q}$ respectively and let $L_Z, M_{Z'}$ be the decomposition field of $\mathfrak{p}$ in $L/\mathbb{Q}$ and $\mathfrak{p}'$ 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 σ to M, $\sigma\restriction_M$, is in Z'. Then $\sigma(a) = \sigma\restriction_M(a) = a$. $\square$

Lemma 19 *Let $M_0 = \mathbb{Q}(\zeta_{m_0})$, where $m_0 = p_1p_2\cdots p_k$, and let $M_1 = \mathbb{Q}(\zeta_{m_1})$, where $m_1 = 4p_1p_2\cdots p_k$. Furthermore, for $i = 1, 2$ let $\mathfrak{o}_i$ be the ring of algebraic integers in M_i respectively.*

Then, for any positive integer k, there is a prime $p > k$ such that $\mathfrak{o}_0 \cup p\mathfrak{O}_{K_m}$ is $\emptyset$-definable in $\mathfrak{O}_{K_m}$ with m odd. Similarly, for any positive integer k, there is a prime $p > k$ such that $\mathfrak{o}_1 \cup p\mathfrak{O}_{K_m}$ is $\emptyset$-definable in $\mathfrak{O}_{K_m}$ 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 docomposition fields coincide. Let L be the common decomposition field. Also by Lemma 18, for each i, L includes the decomposition field of q in $\mathbb{Q}(\zeta_{p_i^{h_1}})/\mathbb{Q}$, 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 $\mathfrak{o}_0 \cup q\mathfrak{O}_{K_m}$ in $\mathfrak{O}_{K_m}$.

Let m be even. We note that $\langle q \rangle$ is the only subgroup of order 2^{r-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 $\mathfrak{o}_1 \cup q\mathfrak{O}_{K_m}$ in $\mathfrak{O}_{K_m}$. $\square$

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,

$$\overbrace{\mathbb{Z}/(q) \times \cdots \times \mathbb{Z}/(q)}^{(p_1-1)\cdots(p_k-1)}$$

is interpretable in $\mathfrak{O}_{K_m}$, and

if m is even,

$$\overbrace{\mathbb{Z}/(q) \times \cdots \times \mathbb{Z}/(q)}^{2(p_1-1)\cdots(p_k-1)}$$

is interpretable in $\mathfrak{O}_{K_m}$.

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 $\mathfrak{o}_0/q\mathfrak{o}_0$ is interpretable in $\mathfrak{O}_{K_m}$ with m odd. Since the decomposition of $q\mathbb{Z}$ in $\mathfrak{o}_0$ is $\mathfrak{p}_1 \cdots \mathfrak{p}_{n_0}$ and $\mathfrak{o}_0/\mathfrak{p}_i \cong \mathbb{Z}/(q)$ for each i, we have

$$\mathfrak{o}_0/q\mathfrak{o}_0 \cong \mathfrak{o}_0/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n_0}) \cong \overbrace{\mathbb{Z}/(q) \times \cdots \times \mathbb{Z}/(q)}^{(p_1-1)\cdots(p_k-1)}.$$

Similarly for m even. □

References

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

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

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

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

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

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

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

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