PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 3, March 1999, Pages 851–860
S 0002-9939(99)04611-0

ON THE CONSTRUCTIBLE NUMBERS

CARLOS R. VIDELA

(Communicated by Andreas R. Blass)

Abstract. Let Ω be the field of constructible numbers, i.e. the numbers constructed from a given unit length using ruler and compass. We prove $\widetilde{\mathbb{Z}} \cap \Omega$ is definable in Ω.

1. Introduction

In 1930 A. Tarski [7] proved that the theory of the structure $\widetilde{\mathbb{R}} = (\mathbb{R}, +, \cdot, < 0, 1)$ is decidable. He asked whether or not his result could be extended to include certain expansions of the reals, most notably by a predicate for the field of rational numbers, a predicate for the field of real constructible numbers or by the function $f(x) = 2^x$. J. Robinson in [5] defined $\mathbb{Z}$ inside $\mathbb{Q}$ and thus answered negatively Tarski's first problem. The exponential function problem has been studied intensively for the past 12 years and recently A. Macintyre and A. Wilkie [3] have made an important advance. Our paper concerns the second question. If we write Ω for the field of constructible numbers and $\widetilde{\mathbb{Z}}$ for the ring of algebraic integers, then our result is that $\widetilde{\mathbb{Z}} \cap \Omega$ is first order definable in Ω. We expect that $\mathbb{Z}$ should be definable in $\widetilde{\mathbb{Z}} \cap \Omega$. Hence, this paper is a step towards resolving the question negatively.

Our proof relies heavily on R. Rumely's work in the theory of global fields [6]. Here Rumely defines a predicate $P(x, l, c, d)$, x a variable and l, c, d parameters, such that for K a number field and p a prime ideal of O_K there is a choice of $c, d \in K$ and l a prime integer so that for $t \in K$, $K \vDash P(t, l, c, d) \Leftrightarrow t \in O_p$.

O_p is the valuation ring of p, i.e. $\{x \in K : \operatorname{ord}_p x \geq 0\}$. Rumely's idea is to use the norm map from cyclic extensions of K. More precisely, for a number field K containing the $2l$th roots of unity if $K' = K(b^{1/l})$ is a nontrivial extension for some $b \in K$, then K'/K is cyclic and the norm map $N_{K'/K} : K'^{\times} \to K^{\times}$ defines a norm form

$$N_l(b, \vec{a}) = N_{K'/K}(a_0 + a_1 b^{1/l} + \cdots + a_{l-1} b^{l-1/l})$$

where $\vec{a} = (a_0, a_1, \ldots, a_{l-1}) \in K^{(l)}$.

By the theorem on symmetric functions $N_l(b, \vec{a})$ is a homogeneous form of degree l in the $\vec{a}$ variables with coefficients in $\mathbb{Z}[b]$.

For example, $N_2(b, a_0, a_1) = a_0^2 - a_1^2 b$.

Received by the editors March 20, 1996 and, in revised form, June 25, 1997.
1991 *Mathematics Subject Classification.* Primary 03C68, 11R04.
Key words and phrases. Algebraic integer, constructible number, definable.

These forms are therefore expressible in the usual vocabulary of fields. Rumely's basic predicate is:

$$R_l(t,c,d) \Leftrightarrow \exists\vec{a}_1\exists\vec{a}_2\exists\vec{a}_3\exists\omega\ (\omega = N_l(d,\vec{a}_1) \wedge c\omega = N_l(cd,\vec{a}_2) \wedge t = N_l(\omega,\vec{a}_3)).$$

In section 2 we review some of Rumely's results and make some minor but crucial extensions. In section 3 we discuss the local-global properties of sets defined by the predicate $O_l(x,c,d)$ where $O_l(x,c,d) \Leftrightarrow R_l(1+cx^l,c,d)$. Section 4 contains our main result.

All the facts that we need to know about the constructible field may be found in [1]. On the number theory side one uses the Hasse local-global Norm theorem (for cyclic extensions) and Artin's Reciprocity Theorem. These can be found in [4]. For p a prime of K, K_p will denote the p-adic completion of K. If p is archimedean we write K_∞. The notation L_β/K_p implicitly means that L/K is a finite extension of number fields, p a prime of K, and β is a prime of L above p, i.e. β/p.

2. Rumely's results and extensions

Define the predicate $R_l(t,c,d)$ by

$$\exists\vec{a}_1\exists\vec{a}_2\exists\vec{a}_3\exists\omega\ (\omega = N_l(d,\vec{a}_1) \wedge c\omega = N_l(cd,\vec{a}_2) \wedge t = N_l(\omega,\vec{a}_3)).$$

To simplify notation the image $N_{K'/K}(K'^{\times})$ will sometimes be written as $N(K'^{\times})$ and statements like $\omega = N_l(d,\vec{a}_1)$ will simply be expressed as $\omega \in N(d^{1/l})$.

Lemma 2.1. *Let l be a prime number and assume K contains the $2l$th roots of unity. Suppose p is a prime of K such that the characteristic of the residue class field $\bar{K}_p$ is not l. Then we have*:

(a) *If $\mathrm{ord}_p(b) \not\equiv 0 \bmod l$, then K'_β/K_p is totally ramified and of degree l and $N(K'^{\times}_\beta)$ is generated by b and $(K_p^\times)^l$.*
(b) *If $\mathrm{ord}_p(b) \equiv 0 \bmod l$ but $b \notin (K_p^\times)^l$, then K'_β/K_p is unramified and of degree l and $N(K'^{\times}_\beta) = \{x \in K_p^\times \mid \mathrm{ord}_p(x) \equiv 0 \bmod l\}$.*
(c) *If $b \in (K_p^\times)^l$, then K'_β/K_p is trivial and $N(K'^{\times}_\beta) = K_p^\times$.*

For a proof see [6], Lemma 2.1.

Lemma 2.2. *Suppose l is a prime and p a prime of K such that $p \nmid l$. Assume the $2l$th roots of unity belong to K_p. If $d \in K$ is a non-lth power unit at p and $c \in K$ is a prime element at p, then over K_p, $R_l(t,c,d)$ is satisfied only by 0 and by $t \in K_p^\times$ for which $\mathrm{ord}_p\, t \equiv 0 \mod l$.*

For a proof, see [6], Lemma 2.2. The result there is stated for the global case, but the proof remains valid for the local case given here. We will need a generalization of Lemma 2.2 for finite extensions L/K with $L \subset \Omega$. Given a prime β of L over p, we ask what happens when the variables in $R_l(t,c,d)$ are allowed to range over L_β instead of K_p. Because $[L:K]$ is a power of 2, we are able to determine this.

Lemma 2.3. *Let L/K be a finite Galois extension with $L \subset \Omega$. Fix $c,d \in K$, $l \neq 2$ a prime integer, and p a prime of K with $p \nmid l$. Suppose the hypotheses of Lemma 2.2 hold, and let β be a prime of L with β/p. Then over L_β, $R_l(t,c,d)$ is satisfied only by 0 and by $t \in L_\beta^\times$ for which $\mathrm{ord}_\beta(t) \equiv 0 \pmod{l}$.*

Proof. The proof breaks into two cases, according to whether β/p is ramified or not.

(a) First suppose p is unramified in L/K. The ideal pO_L is either prime or a product $\beta_1\beta_2\dots\beta_g$ of distinct primes of L. For any $\beta|p$ $\operatorname{ord}_\beta c = 1$ and $\operatorname{ord}_\beta d = 0$. The degree $[L_\beta : K_p] = f$ is a power of 2 since $[L : K] = 2^s = fg$. It follows that d is a non-lth power in L_β; otherwise $K_p(d^{1/l}) \subset L_\beta$, so $l|[L : K]$. The hypotheses of Lemma 2.2 apply to L_β so $\operatorname{ord}_\beta(t) \equiv 0 \bmod l$.

(b) Now suppose p is ramified in L/K; write $pO_L = \beta_1^e \cdots \beta_g^e$. The ramification index e is a power of 2 larger than 1.

Fix $\beta|p$. Let c' be a prime element at β. Note that d is still a non-lth power unit at β.

Consider the number ω in the predicate $R_l(t, c, d)$. By Lemma 2.1 $L_\beta(d^{1/l})/L_\beta$ is unramified of degree l and $L_\beta((cd)^{1/l})/L_\beta$ is totally ramified of degree l (since $\operatorname{ord}_\beta c = e \not\equiv 0 \bmod l$); hence from the description of the norm groups we have:

$$\omega = uc'^{nl}, \quad \operatorname{ord}_\beta u = 0; \qquad c\omega = (cd)^m x^l, \quad x \in (L_\beta^\times).$$

We may write $c = c'^e v$ with $v \in \beta$-unit.

Substituting we get $c\omega = (c'^e vd)^m x^l$.

Multiplying the first equation by c and equating we get $cuc'^{nl} = (c'^e vd)^m x^l$. Taking ord values we have

$$e + nl = me + l \operatorname{ord}_\beta x.$$

Rearranging, $l(n - \operatorname{ord}_\beta x) = e(m - 1)$.

If $m = 1$, then $c\omega = cdx^l$ so $\omega = dx^l$. So $\omega^{1/l} = xd^{1/l}$ and $L_\beta(\omega^{1/l}) = L_\beta(d^{1/l})$. Hence $\operatorname{ord}_\beta t \equiv 0 \bmod l$ by Lemma 2.1.

If $m \neq 1$, then $l|m - 1$. Therefore there is an integer s so that $1 + ls = m$. We get

$$c\omega = (cd)^{1+ls} x^l = (cd)(c^s d^s x)^l.$$

It follows from this equation that $\omega = d(c^s d^s x)^l$; hence $\omega^{1/l} = d^{1/l} c^s d^s x$ with $c^s d^s x \in L_\beta^\times$. Therefore the fields $L_\beta(\omega^{1/l})$ and $L_\beta(d^{1/l})$ are equal which implies that $\operatorname{ord}_\beta(t) \equiv 0 \pmod l$.

Lemma 2.4. *Let M be any algebraic field extension of $\mathbb{Q}$ and suppose $K \subset M$ is a finite field extension of $\mathbb{Q}$. Fix l a prime number and assume the $2l$th roots of unity belong to K. Take $c, d \in K$. Then there is a finite set of primes $S_{c,d,K}$ of K such that for $t \in M$:*

$$M \vDash R_l(t, c, d) \Leftrightarrow \exists L/K \quad \textit{finite} \quad L \subset M, t \in L$$

such that for any β prime of L above some prime $p \in S_{c,d,K}$ we have $L_\beta \vDash R_l(t, c, d)$.

Proof. The set $S_{c,d,K}$ is $\{$primes p of $O_K : p|l$ or $p|(d)$ or $p|(c)\}$. Here, $p|(d)$ or $p|(c)$ means that p appears in the fractional ideal decomposition of (d) or (c) in O_K.

Suppose $M \vDash R_l(t, c, d)$. Let L be the subfield of M generated over K by the elements of M whose existence is stated by $R_l(t, c, d)$ and t. Then L/K is finite and clearly $L \vDash R_l(t, c, d)$. Since $L \subset L_\beta$ for each prime of L we have $L_\beta \vDash R_l(t, c, d)$.

In particular this holds for primes above primes in $S_{c,d,K}$.

For the other implication note that for each $\beta|p$ with $p \in S_{c,d,K}$ there is an $\omega_\beta \in L_\beta^\times$ such that $\omega_\beta \in N(d^{1/l})$, $c\omega_\beta \in N((cd)^{1/l})$ and $t \in N(\omega_\beta^{1/l})$.

We will prove that $L \vDash R_l(t, c, d)$ by showing that $R_l(t, c, d)$ holds locally at all primes of O_L. More precisely, we will define an element ω in L and show that

$\omega \in N(d^{1/l})$, $c\omega \in N((cd)^{1/l})$ and $t \in N(\omega^{1/l})$. These three conditions will be verified locally.

By the approximation theorem and the theorem on primes in arithmetic progressions (see [6], pp. 201–202, and [2], p. 166) there is an $\omega \in O_L$ such that $\theta = (\omega)$ is a prime ideal and

$$\begin{array}{lll} \omega \equiv \omega_q & \operatorname{mod} q^m & \forall q|l \text{ and } m \text{ sufficiently large} \\ & & \text{so that } \frac{\omega}{\omega_q} \in (L_q^\times)^l, \\ \omega \equiv \omega_\beta & \operatorname{mod}_\beta & \forall_\beta|(d), \\ \omega \equiv \omega_\beta & \operatorname{mod}_\beta & \forall_\beta|(c), \\ \omega \equiv 1 & \operatorname{mod}_\beta & \forall_\beta|(t) \text{ but } \beta \cap O_K \notin S_{c,d,K}. \end{array}$$

We now argue as in [2], pp. 202–203:

Claim 1. $L \vDash \omega \in N(d^{1/l})$.

At archimedean primes: $L_\infty = \mathbb{C}$ so $L_\infty(d^{1/l})/L_\infty$ is trivial.

At $\beta|l : \omega = \omega_\beta \frac{\omega}{\omega_\beta}$. Since $\frac{\omega}{\omega_\beta} \in (L_\beta^\times)^l$ it is a norm; by assumption ω_β is a norm so ω is a norm.

At $\beta|(d)$, $\beta \nmid l$, $\beta \neq \theta : \omega \equiv \omega_\beta$ so $\frac{\omega}{\omega\beta} \equiv 1$. Since $\beta \nmid l$ Hensel's lemma applies and $\frac{\omega}{\omega_\beta} \in (L_\beta^\times)^l$. Hence $\omega = \omega_\beta \frac{\omega}{\omega_\beta}$ is a norm.

At $\beta \nmid (d)$, $\beta \nmid l$, $\beta \neq \theta$: Here $\operatorname{ord}_\beta w = 0$ and we have two possibilities. Either $d \in (L_\beta^\times)^l$ so the extension is trivial or $d \notin (L_\beta^\times)^l$ and $\operatorname{ord}_\beta d = 0$, in which case $L_\beta(d^{1/l})/L_\beta$ is unramified and Lemma 2.1(b) shows ω is a norm.

We have taken care of all primes of L except θ. But here ω is also a norm by Artin Reciprocity. Thus, ω is a global norm by the Hasse Norm Theorem.

Claim 2. $L \vDash c\omega \in N((cd)^{1/l})$.

At archimedean primes: $L_\infty = \mathbb{C}$. So the extension is trivial.

At $\beta|l : \frac{\omega}{\omega_\beta} \in (L_\beta^\times)^l$ and $c\omega_\beta$ is a norm; hence $c\omega = c\omega_\beta \frac{\omega}{\omega_\beta}$ is a norm.

At $\beta|(d)$, $\beta \nmid l$, $\beta \neq \theta$: $\frac{\omega}{\omega_\beta} \equiv 1$ and Hensel's lemma shows $\frac{\omega}{\omega_\beta} \in (L_\beta^\times)^l$.

At $\beta \nmid (d)$, $\beta \nmid l$, $\beta \nmid (c)$, $\beta \neq \theta$: Here $\operatorname{ord}_\beta(c\omega) = 0$. We have two possibilities: either $cd \in (L_\beta^\times)^l$ and then the extension is trivial or $cd \notin (L_\beta^\times)^l$ and $\operatorname{ord}_\beta(cd) = 0$ in which case $c\omega$ is a norm by Lemma 2.1(b).

At $\beta \nmid (d)$, $\beta \nmid l$, $\beta|(c)$, $\beta \neq \theta$: Here again $\frac{\omega}{\omega_\beta} \in (L_\beta^\times)^l$ by Hensel's lemma, and $c\omega_\beta$ is a norm. So $c\omega = c\omega_\beta \frac{\omega}{\omega_\beta}$ is a norm also.

Only $\beta = \theta$ remains and here Artin Reciprocity shows $c\omega$ is a norm.

Claim 3. $L \vDash t \in N(\omega^{1/l})$.

At archimedean primes: $L_\infty = \mathbb{C}$.

At $\beta|l : t \in N(\omega_\beta^{1/l})$; since $\frac{\omega}{\omega_\beta} \in (L_\beta^\times)^l$ it follows that $L_\beta(\omega^{1/l}) = L_\beta(\omega_\beta^{1/l})$.

At $\beta|(d)$, $\beta \nmid l$, $\beta \neq \theta$: As above.

At $\beta \nmid (d)$, $\beta \nmid l$, $\beta|(c)$, $\beta \neq \theta$: Again $\frac{\omega}{\omega_\beta} = a^l$ so $\omega = \omega_p a^l$ and $L_\beta(\omega^{1/l}) = L_\beta(\omega_\beta^{1/l})$.

At $\beta \nmid (d)$, $\beta \nmid (l)$, $\beta \nmid (c)$, $\beta \neq \theta$: If $\beta|(t)$, then $\omega \equiv 1$ so Hensel's lemma shows $\omega \in (L_\beta^\times)^l$; hence $L_\beta(\omega^{1/l})/L_\beta$ is trivial.

If $\beta \nmid (t)$, then $\operatorname{ord}_\beta t = 0$, $\operatorname{ord}_\beta \omega = 0$. If $\omega \in (L_\beta^\times)^l$ also, then the extension is trivial. If not, $L_\beta(\omega^{1/l})$ is unramified so t is a norm.

Finally, at $\beta = \theta$ apply Artin Reciprocity.

For the next lemma fix a prime l and a finite extension $K/\mathbb{Q}$, such that K contains the $2l$th roots of unity. Let p be a prime of O_K such that $p \nmid l$.

Recall that $O_l(x,c,d)$ stands for $R_l(1+cx^l,c,d)$. Then Rumely proves [6, p. 202]

Lemma 2.5. *There is a choice of $c,d \in K$ and p_1 a prime ideal of O_K, $p_1 \neq p$, such that for $t \in K$*

$$K \vDash R_l(t,c,d) \Leftrightarrow \operatorname{ord}_p t \equiv 0 \mod l \quad \textit{and}$$
$$\operatorname{ord}_{p_1} t \equiv 0 \mod l.$$

We do not need to know how this is done but some properties of p_1, c, d will be used. First, p_1 and c are chosen such that $(c) = pp_1$ and there are infinitely many primes p_1 (and c's) so that this can be done. The number d is chosen so that $(d) \neq p$, p_1 is a prime ideal and $c \in (K^{\times}_{(d)})^l$. It follows that for $x \in K$

$$K \vDash O_l(x,c,d) \Leftrightarrow x \in O_p \cap O_{p_1}.$$

We will use this in section 4.

3. Local-global properties of O_l

We write μ_{2l} for a primitive $2l$th root of unity.

Lemma 3.1. *Let $c,d,\mu_{2l} \in K$, with $K/\mathbb{Q}$ finite. Suppose L/K is a further finite extension. Then for each $x \in L$, we have $L \vDash O_l(x,c,d)$ if and only if for all $p \in S_{c,d,K}$ and all β of L with $\beta|p$*

$$L_\beta \vDash O_l(x,c,d).$$

Proof. The proof is clear from Lemma 2.4 and its proof.

Lemma 3.2. *Let $c,d,\mu_{2l} \in K$, with $K/\mathbb{Q}$ finite. For each finite extension L/K, there is an r such that for all $p \in S_{c,d,K}$ and all β of L with $\beta|p$, if $x \in L_\beta$ satisfies*

$$\operatorname{ord}_\beta(x) \geq r, \quad \textit{then } L_\beta \vDash O_l(x,c,d).$$

Proof. For $\alpha \in L_\beta$, if α is sufficiently close to 1 (with respect to β), then it is an lth power. Hence α is a norm from the extension $L_\beta(d^{1/l})$.

Now for $1+cx^l$ to be close to 1 (and hence an lth power) it suffices to have $\operatorname{ord}_\beta(cx^l) = \operatorname{ord}_\beta c + l \operatorname{ord}_\beta x$ be sufficiently large, say $\operatorname{ord}_\beta c + l \operatorname{ord}_\beta x \geq k$.

Therefore if $\operatorname{ord}_\beta x \geq \frac{k-1}{l}$, we have (with $\omega = d$) $L_\beta \vDash O_l(x,c,d)$.

In the next lemmas we consider the following situation: M is an infinite algebraic extension of $\mathbb{Q}$, $K \subset M$ and $c,d,\mu_{2l} \in K$ where l is an odd prime.

Lemma 3.3. *Suppose O_l is closed under addition, i.e.*

$$M \vDash \forall x,y(O_l(x,c,d) \wedge O_l(y,c,d) \Rightarrow O_l(x+y,c,d)).$$

Fix $p_0 \in S_{c,d,K}$ and suppose that in some finite extension L/K with $L \subseteq M$, and for some $\beta_0|p_0$ and $x,y \in L_{\beta_0}$, we have

$$L_{\beta_0} \vDash O_l(x,c,d) \wedge O_l(y,c,d).$$

Then there is a finite extension L'/L with $L' \subseteq M$ such that for all primes β' of L' with $\beta'|\beta_0$, then $L'_{\beta'} \vDash O_l(x+y,c,d)$.

Proof. Given $r > 0$, by the approximation theorem we can find $x', y' \in L$ such that $x' \equiv x \bmod \beta_0^r$, $y' \equiv y \bmod \beta_0^r$; and for all $\beta|p$ with $\beta \neq \beta_0$ and all $p \in S_{c,d,K}$, we have $x' \equiv y' \equiv 0 \bmod \beta^r$.

If r is chosen large enough that

$$\frac{1+cx^l}{1+cx'^l} \in (L_{\beta_0}^\times)^l, \quad \frac{1+cy^l}{1+cy'^l} \in (L_{\beta_0}^\times)^l, \quad \frac{1+c(x+y)^l}{1+c(x'+y')^l} \in (L_{\beta_0}^\times)^l,$$

then $L_{\beta_0} \vDash O_l(x', c, d) \wedge O_l(y', c, d)$.

If r is also large enough that the condition of Lemma 3.2 is satisfied, then for all $p \in S_{c,d,K}$ and all $\beta|p$ with $\beta \neq \beta_0$, we will have $L_\beta \vDash O_l(x', c, d) \wedge O_l(y', c, d)$. From Lemma 3.1 we get $L \vDash O_l(x', c, d) \wedge O_l(y', c, d)$.

By hypothesis, there is a finite L'/L with $L' \subseteq M$ such that $L' \vDash O_l(x'+y', c, d)$. It follows that for all primes β' of L' with $\beta'|\beta_0$, then $L'_{\beta'} \vDash O_l(x'+y', c, d)$. Since $1 + c(x+y)^l = 1 + c(x'+y')^l l \cdot \frac{1+c(x+y)^l}{1+c(x'+y')^l}$ we obtain the result.

Lemma 3.4. *Suppose now $M \vDash \forall_\alpha(O_l(\alpha^2, c, d) \to O_l(\alpha, c, d))$. Fix $\beta_0|p_0$, $p_0 \in S_{c,d,K}$. If $L_{\beta_0} \vDash O_l(\alpha^2, c, d)$, then there exists a finite L'/L with $L' \subset M$ such that $\forall \beta'|\beta_0$ $L'_{\beta'} \vDash O_l(\alpha, c, d)$.*

Proof. As in the previous lemma we find $x \in L$ such that $L_\beta \vDash O_l(x^2, c, d)$ for all β/p with p ranging over $S_{c,d,K'}$ and such that at β_0

$$\frac{1+c\alpha^l}{1+cx^l} \in (L_{\beta_0}^\times)^l.$$

It follows that in some finite extension L'/L we have $L' \vDash O_l(x, c, d)$. By writing

$$1 + c\alpha^l = 1 + cx^l \cdot \frac{1+c\alpha^l}{1+cx^l}$$

we get $L'_{\beta'} \vDash O_l(\alpha, c, d)$ for all $\beta'|\beta_0$.

Lemma 3.5. *Suppose $M \vDash \forall_\alpha(O_l(\alpha^2, c, d) \to O_l(\alpha, c, d))$.*

Take L/K finite with $L \subset M$, and fix a prime β_0 of L with $\beta_0|p$ for some $p \in S_{c,d,K}$. Let $\alpha \in L_{\beta_0}$, $\alpha \in {}_{\beta_0}O_{\beta_0}$.

Then there is a finite extension L'/L with $L' \subset M$ such that for all β' of L' with $\beta'|\beta_0$

$$L'_{\beta'} \vDash O_l(\alpha, c, d).$$

Proof. Since $\mathrm{ord}_{\beta_0}(\alpha) \geq 1$, we have $L_{\beta_0} \vDash O_l(\alpha^{2^s}, c, d)$ for some $s \in \mathbb{N}$ by Lemma 2.3. Using Lemma 3.4 several times we get our result.

Lemma 3.6. *Suppose $M \vDash \forall\alpha(O_l(\alpha^2 - \alpha, c, d) \to O_l(\alpha, c, d))$. Fix $p \in S_{c,d,K}$. Suppose in some finite extension L/K, $L \subset M$ and some $\beta|p$ $L_\beta \vDash O_l(\alpha^2 - \alpha, c, d)$. Then there exists a finite extension L'/L with $L' \subset M$ such that $\forall \beta'|\beta$ $L'_{\beta'} \vDash O_l(\alpha, c, d)$.*

Proof. The proof is similar to the proof of Lemma 3.4. Just note that if $x \equiv 0 \bmod \beta^r$, then $x^2 - x \equiv 0 \bmod \beta^r$.

Lemma 3.7. *Suppose $M \vDash \forall xy((O_l(x^2, c, d) \wedge O_l(y^3, c, d)) \to O_l(xy, c, d))$. Fix $p_0 \in S_{c,d,K}$ and suppose that in some finite extension L/K with $L \subset M$, and for some $\beta_0|p_0$ and $x, y \in L_{\beta_0}$ we have*

$$L_{\beta_0} \vDash O_l(x^2, c, d) \wedge O_l(y^3, c, d).$$

Then there is a finite extension L'/L with $L' \subset M$ such that for all primes β' of L' with $\beta'|\beta_0$, then $L'_{\beta'} \vDash O_l(xy, c, d)$.

Proof. As in the proof of Lemma 3.3, by the approximation theorem we find x', $y' \in L$ such that $x' \equiv x \bmod \beta_0^r$ and $y' \equiv y \bmod \beta_0^r$; and for all $\beta|p$, $\beta \neq \beta_0$ and all $p \in S_{c,d,K}$ $x' \equiv y' \equiv 0 \bmod_\beta^r$. For large enough r we have:

$$\frac{1+c(x^2)^l}{1+c(x'^2)^l} \in (L_{\beta_0}^\times)^l, \quad \frac{1+c(y^3)^l}{1+c(y'^3)^l} \in (L_{\beta_0}^\times)^l, \quad \frac{1+c(xy)^l}{1+c(x'y')^l} \in (L_{\beta_0}^\times)^l.$$

Hence $L_{\beta_0} \vDash O_l(x'^2, c, d) \wedge O_l(y'^3, c, d)$ and $L_\beta \vDash O_l(x'^2, c, d) \wedge O_l(y'^3, c, d)$ for all $\beta|p$, $\beta \neq \beta_0$ and all $p \in S_{c,d,K}$.

From Lemma 3.1 we get $L \vDash O_l(x'^2, c, d) \wedge O_l(y'^3, c, d)$. Therefore there is a finite L'/L, $L' \subset M$ such that $L' \vDash O_l(x'y', c, d)$. It follows that for all primes β' of L', $\beta'|\beta_0$, then $L'_{\beta'} \vDash O_l(x'y', cd)$. Since $1 + c(xy)^l = 1 + c(x'y')^l \cdot \frac{1+c(xy)^l}{1+c(x'y')^l}$ we get the result.

In the next lemma we take $M = \Omega$, the field of constructible numbers. Given $c, d \in \Omega$ we say the formula $O_l(x, c, d)$ is good if

$$\begin{aligned} \Omega \vDash O_l(0, c, d) \wedge O_l(1, c, d) \wedge \forall x, y(O_l(x, c, d) \wedge O_l(y, c, d) \to O_l(x+y, c, d)) \\ \wedge \forall z(O_l(z^2, c, d) \to O_l(z, c, d)) \\ \wedge \forall w(O_l(w^2 - w, c, d) \to O_l(w, c, d)) \\ \wedge \forall x, y((O_l(x^2, c, d) \wedge O_l(y^3, c, d)) \to O_l(xy, c, d)). \end{aligned}$$

Lemma 3.8. *Let $c, d \in \Omega$ and suppose $O_l(x, c, d)$ is good. Let $K/\mathbb{Q}$ be a finite extension, $K \subset \Omega$, such that $c, d, \mu_{2l} \in K$. Fix $p \in S_{c,d,K}$. Let $\alpha \in K$, $\alpha \in O_p$. Then there is a finite extension $L^{(p)}/K, L^{(p)} \subset \Omega$ such that $\forall \beta|p$ $L_\beta^{(p)} \vDash O_l(\alpha, c, d)$.*

Proof. The finite field O_p/pO_p has dimension a power of 2 over $\mathbb{Z}/p\mathbb{Z}$. We distinguish two cases.

Case A. $p \neq 2$.

We have a square-root tower $F_0 = \mathbb{Z}/p\mathbb{Z} \subset F_1 \subset F_2 \subset \cdots \subset F_n = O_p/pO_p$ with

$$F_{i+1} = F_i(\bar{\alpha}_{i+1}), \qquad \bar{\alpha}_{i+1} \in O_p/pO_p, \quad \overline{\alpha_{i+1}}^2 \in F_i, \quad i = 0, \ldots, n-1.$$

By an induction argument we will show that for every $\alpha \in O_p$ there is a finite field extension L/K, $L \subset \Omega$ such that $\forall \beta|p$ $L_\beta \vDash O_l(\alpha, c, d)$.

First suppose $\bar{\alpha} \in F_0$. Then $\alpha = m + \tilde{\alpha}$ for some $m \in \{0, 1, \ldots, p-1\}$ and some $\tilde{\alpha} \in pO_p$.

Since $O_l(x, c, d)$ is good, there is a finite extension L'/K with $L' \subset \Omega$ such that $L'_{\beta'} \vDash O_l(n, c, d)$ for all $n = 0, 1, \ldots, p-1$ and all $\beta'|p$.

Using Lemma 3.5 in another finite extension L''/K with $L'' \subset \Omega$ we have $L''_{\beta''} \vDash O_l(\tilde{\alpha}, c, d)$ for all $\beta''|p$. If we let L''' be the compositum of L' and L'', then for all primes of L''' with $\beta|p$ we have

$$L'''_\beta \vDash O_l(m, c, d) \wedge O_l(\tilde{\alpha}, c, d).$$

Now apply Lemma 3.3

Now suppose the result proved for all $\alpha \in O_p$ with $\bar{\alpha} \in F_{n-1}$; we show it for $\alpha \in O_p$ with $\bar{\alpha} \in F_n$.

Since $(\bar{\alpha}_n)^2 \in F_{n-1}$, there is a finite extension L/K with $L \subset \Omega$ such that for all $\beta|p$, $L_\beta \vDash O_l(\alpha_n^2, c, d)$.

Applying Lemma 3.4 to each β and taking the composite of the corresponding extensions, we obtain a finite L'/L with $L' \subset \Omega$ such that for each β' of L' with $\beta'|p$, $L'_{\beta'} \vDash O_l(\alpha_n, c, d)$.

Since $\bar{\alpha} \in F_n$, we can write $\alpha = m\alpha_n + \tau$ for some $m \in O_p$ with $\bar{m} \in F_{n-1}$ and some $\tau \in O_p$ with $\bar{\tau} \in F_{n-1}$.

Note that $(\overline{m\alpha_n})^2 \in F_{n-1}$ and so by the argument given above $L'_{\beta'} \vDash O_l(m\alpha_n, c, d)$ for some finite extension L'/L with $L' \subset \Omega$ and all β' of L' with $\beta'|p$. Applying Lemma 3.3 several times we get the result.

Case B. The basis step $F_0 = \mathbb{Z}/2\mathbb{Z}$ is done as in case A. Now suppose that for some i, we know that the assertion holds for all $\tau \in O_p$ with $\bar{\tau} \in F_{i-1}$. Let $\alpha \in O_p$ be such that $\bar{\alpha} \in F_i$. Take α_i with $(\bar{\alpha}_i)^2 - \bar{\alpha}_i \in F_{i-1}$ and $F_i = F_{i-1}(\bar{\alpha}_i)$. By induction, the assertion holds for $\alpha_i^2 - \alpha_i$. Since $O_l(x, c, d)$ is good, the assertion holds for α_i by Lemma 3.6.

Since $O_l(x, c, d)$ is good and $\alpha_i^2 = \alpha_i + (\alpha_i^2 - \alpha_i)$, Lemma 3.3 shows the assertion holds for α_i^2. We can write $\alpha = \lambda\alpha_i + \tau$ for some $\lambda, \tau \in O_p$ with $\bar{\lambda}, \bar{\tau} \in F_{i-1}$, and by induction the assertion holds for λ, τ. But we also have $\lambda^3 \in O_p$ and $(\bar{\lambda})^3 \in F_{i-1}$ so the assertion holds for λ^3. By Lemma 3.7 and the fact that $O_l(x, c, d)$ is good we conclude that the assertion holds for $\lambda\alpha_i$. Then applying Lemma 3.3 we conclude that the assertion holds for $\alpha = \lambda\alpha_i + \tau$.

4. Main theorem

In this section we prove that $\widetilde{\mathbb{Z}} \cap \Omega$ is definable in Ω.

Lemma 4.1. *Suppose $\alpha \in \widetilde{\mathbb{Z}} \cap \Omega$. Suppose for $c, d \in \Omega$, that $O_3(\cdot, c, d)$ is good. Then $\Omega \vDash O_3(\alpha, c, d)$.*

Proof. Let $K/\mathbb{Q}$ be finite, with $\alpha, c, d, \mu_6 \in K$ and $K \subset \Omega$ (note that $\mu_6 \in \Omega$). By Lemma 3.8, for each $p \in S_{c,d,K}$ there is a finite extension $L^{(p)}/K$ with $L^{(p)} \subset \Omega$ such that $L^{(p)}_\beta \vDash O_3(\alpha, c, d)$ for all β of $L^{(p)}$ with $\beta|p$. The compositum of all these fields works.

Lemma 4.2. *Suppose $O_5(\cdot, c, d)$ is good. If $\alpha \in \widetilde{\mathbb{Z}} \cap \Omega$, then $\Omega \vDash O_5(\alpha, c, d)$.*

Proof. Similar to the above proof.

Define the formula $\mathrm{Int}(\alpha)$ by

$$\forall c, d(O_3(\cdot, c, d) \text{ good } \rightarrow O_3(\alpha, c, d)) \wedge \forall c, d(O_5(\cdot, c, d) \text{ good } \rightarrow O_5(\alpha, c, d)).$$

Theorem 4.3. *Let $\alpha \in \Omega$. Then*

$$\alpha \in \widetilde{\mathbb{Z}} \Leftrightarrow \Omega \vDash \mathrm{Int}(\alpha).$$

Proof. "$\Rightarrow$": This is proved in Lemmas 4.1 and 4.2.

"$\Leftarrow$": Suppose $\alpha \notin \widetilde{\mathbb{Z}}$. Let $K/\mathbb{Q}$ be a finite extension such that $\alpha, \mu_6, \mu_{10} \in K$ with $K \subset \Omega$ (note that $\mu_{10} \in \Omega$). Let p be a prime of K with $\mathrm{ord}_p(\alpha) < 0$.

Let $P = p \cap \mathbb{Z}$. We distinguish two cases: (a) $P \neq 3$ or (b) $P \neq 5$. In case (a) we find a pair of numbers $c, d \in K$ such that $O_3(\cdot, c, d)$ is good but $O_3(\alpha, c, d)$ does not hold. For case (b) we find $c, d \in K$ such that $O_5(\cdot, c, d)$ is good but $O_5(\alpha, c, d)$ does not hold. We only do one case since the other is similar.

Suppose $P \neq 5$. Choose $c, d \in K$ as in Lemma 2.5 so that, for $x \in K$, $K \vDash O_5(x, c, d) \Leftrightarrow x \in O_p \cap O_{p_1}$.

We show that $\Omega \nvDash O_5(\alpha, c, d)$. If it did, then there is a finite extension L/K $L \subset \Omega$ such that $L \vDash O_5(\alpha, c, d)$. Recall from Lemma 2.5 that $(c) = pp_1$ $(p_1 \nmid 5)$ and (d) is a prime ideal $\neq p, p_1$. The set $S_{c,d,K}$ is $\{p, p_1, (d), q_1, \dots, q_s\}$ where $q_i|5$.

If the prime ideal p does not ramify in L (we may assume $L/\mathbb{Q}$ is a Galois extension) then, applying Lemma 2.3, we get that $\operatorname{ord}_p(1 + c\alpha^5) \equiv 0 \bmod 5$. But $\operatorname{ord}_p(c\alpha^5) = 1 + 5 \operatorname{ord}_p \alpha < 0$ so $\operatorname{ord}_p(1 + c\alpha^5) \equiv 1 \bmod 5$, which is a contradiction.

If p ramifies, again $\operatorname{ord}_\beta(1 + c\alpha^5) \equiv 0 \bmod 5$, for $\beta|p$. Here $\operatorname{ord}_\beta(c\alpha^5) = e(1 + 5 \operatorname{ord}_p \alpha)$ since $c, \alpha \in K$. So again $\operatorname{ord}_\beta(c\alpha^5)$ is negative so $\operatorname{ord}_\beta(1 + c\alpha^5) \equiv e \not\equiv 0 \bmod 5$ (using $e|2^n$) and we have a contradiction.

We show now that $O_5(\cdot, c, d)$ is good.

Claim 1. If $O_5(\gamma^2, c, d)$ is true, then $O_5(\gamma, c, d)$ holds.

Proof. Suppose L/K is finite, $L \subset \Omega$ and $L \vDash O_5(\gamma^2, c, d)$. We show $L \vDash O_5(\gamma, c, d)$.

We consider primes β of L above primes in $S_{c,d,K}$, and verify locally.

If $\beta|(d)$, take $\omega_\beta = 1$. Then $1 \in N(d^{1/5})$ and $c \in N((cd)^{1/5})$ (since $c \in (K^\times_{(d)})^5$; see [6, p. 201]).

Finally $L_\beta(\omega_\beta^{1/5})/L_\beta$ is trivial so $1 + c\gamma^5$ is a norm.

At $\beta|5$: Again take $\omega_\beta = 1$.

At $\beta|p$: Here we have to distinguish two cases: p unramified and p ramified. If p is unramified, take $\omega_\beta = d$. Then $d \in N(d^{1/5})$, $cd \in N((cd)^{1/5})$. Since $\operatorname{ord}_\beta d = 0$ and d is not a 5th power in L_β, we get that $N(d^{1/5}) = \{x \in L_\beta : \operatorname{ord}_\beta x \equiv 0 \mod 5\}$. Since $L \vDash O_5(\gamma^2, c, d)$ we know $\operatorname{ord}_p \gamma \geq 0$. Therefore $\operatorname{ord}_\beta(1+c\gamma^5) = 0$ so $1+c\gamma^5 \in N(\omega_\beta^{1/5}) = N(d^{1/5})$.

If p is ramified, then from $\operatorname{ord}_\beta(1+c\gamma^{10}) \equiv 0 \bmod 5$ we get that $\operatorname{ord}_\beta \gamma \geq \frac{-e}{10} > \frac{-e}{5}$ (see Lemma 2.3).

Let $\omega_\beta = d$. Now $\operatorname{ord}_\beta(c\gamma^5) = e + 5 \operatorname{ord}_\beta \gamma > e - e = 0$. So $\operatorname{ord}_\beta(1 + c\gamma^5) = 0$ and again by Lemma 2.3 we get $1 + c\gamma^5 \in N(d^{1/5}) = N(\omega_\beta^{1/5})$.

At $\beta|p_1$: Similarly.

Claim 2. Suppose $\Omega \vDash O_5(\alpha^2 - \alpha, c, d)$. Then $\Omega \vDash O_5(\alpha, c, d)$.

This is similar to the previous case and we leave the details to the reader.

Claim 3. $\Omega \vDash O_5(0, c, d)$, $O_5(1, c, d)$ and $O_5(\cdot, c, d)$ is closed under addition.

Proof. $K \vDash O_5(0, c, d) \wedge O_5(1, c, d)$ since $0, 1 \in O_p \cap O_{p_1}$. Next, suppose $L \vDash O_5(x, c, d) \wedge O_5(y, c, d)$. We will show that $L \vDash O_5(x + y, c, d)$. Consider primes β of L above primes in $S_{c,d,K}$.

At $\beta|5$: Take $\omega_\beta = 1$.

At $\beta|(d)$: Take $\omega_\beta = 1$.

At $\beta|p$: If p is unramified, then $\operatorname{ord}_\beta x \geq 0$ and $\operatorname{ord}_\beta y \geq 0$. It follows that $\operatorname{ord}_\beta(1 + c(x + y)^5) = 0$.

If p is ramified, then $\operatorname{ord}_\beta x > \frac{-e}{5}$ and $\operatorname{ord}_\beta y > \frac{-e}{5}$.

Here $\operatorname{ord}_\beta x \geq -e/5$ follows from Lemma 2.3 as in the proof of Claim 1; the strict inequality comes from the fact that $e|2^n$, so e is not divisible by 5. Hence $\operatorname{ord}_\beta(x + y) > \frac{-e}{5}$ and so $\operatorname{ord}_\beta(1 + c(x + y)^5) = 0$. So in both the ramified and unramified cases we may take $\omega_\beta = d$.

At $\beta|p_1$: Similarly.

Claim 4. $\Omega \vDash \forall x, y((O_5(x^2, c, d) \wedge O_5(y^3, c, d)) \to O_5(xy, c, d))$.

This is similar to the previous cases. We only consider primes above p. So suppose $L \vDash O_5(x^2, c, d) \wedge O_5(y^3, c, d)$, and β is a prime of L above p. If p is unramified, then $\operatorname{ord}_\beta x \geq 0$ and $\operatorname{ord}_\beta y \geq 0$. It follows that $\operatorname{ord}_\beta(1 + c(xy)^5) = 0$ so $L \vDash O_5(xy, c, d)$ (as in the proof of Claim 1). If p is ramified, then $\operatorname{ord}_\beta x \geq -\frac{e}{10}$ and $\operatorname{ord}_\beta y \geq -\frac{e}{15}$. Hence $\operatorname{ord}_\beta xy = \operatorname{ord}_\beta x + \operatorname{ord}_\beta y \geq -\frac{e}{6}$. Hence $\operatorname{ord}_\beta(c(xy)^5) = e + 5\operatorname{ord}_\beta(xy) \geq e - \frac{5e}{6} > 0$. So $\operatorname{ord}_\beta(1 + c(xy)^5) = 0$. Hence, as in Claim 1, $L \vDash O_5(xy, c, d)$.

Finally, I would like to thank G. Cherlin for introducing me to this problem and for stimulating discussions. The referee made useful comments and improvements, in particular to the proof of Lemma 3.8. The present proof was supplied by the referee who noted that Case B of that Lemma could not be treated along the same lines as Case A in the original proof. I thank him or her also. The referee also suggested that the present methods could be used to define the algebraic integers in pro-p extensions of number fields. This is indeed the case and in this wider context some undecidability results can be obtained. These results will appear in a future paper [8].

References

[1] N. Jacobson, *Basic algebra* I, Freeman & Co., San Francisco, 1974. MR **50:**9457

[2] S. Lang, *Algebraic number theory*, Addison-Wesley, New York, 1970. MR **44:**181

[3] A. Macintyre and A. Wilkie, *On the decidability of the real exponential field*, Oxford Univ., 1993, preprint.

[4] J. Neukirch, *Class field theory*, Springer-Verlag, New York, 1986. MR **87i:**11005

[5] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949). MR **11:**151f

[6] R. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), 195–217. MR **81m:**03053

[7] A. Tarski, *A decision method for elementary algebra and geometry*, Rand Corporation, California, 1948. MR **10:**499f

[8] C. Videla, *Definability of the ring of integers of pro-p extensions of number fields*, in preparation.

Departamento de Matemáticas, CINVESTAV-IPN, Av. IPN No. 2508, 07000 México D.F., Mexico

E-mail address: cvidela@math.cinvestav.mx