Proyecciones (Antofagasta. On line) | vol. 39, n. 3 (2020) | pp. 721-736.

10.22199/issn.0717-6279-2020-03-0045

PROYECCIONES
Journal of Mathematics

ISSN 0717-6279 (On line)

The diophantine problem for addition and divisibility for subrings of rational functions over finite fields

Leonidas Cerda-Romero[1] orcid.org/0000-0003-2499-7135
Carlos Martínez-Ranero[2] orcid.org/0000-0002-0919-8207

[1]Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador
lcerda@espoch.edu.ec
[2]Universidad de Concepción, Dept. de Matemática, Concepción, Chile
cmartinezr@udec.cl

Received: July 2019 | Accepted: January 2020

Abstract:

It is shown that the positive existential theory of the structure $\mathcal{F}_S = (S^{-1}F[t];=,F, 0, 1,+, |, f \mapsto tf)$, where $f \mapsto tf$ is the multiplication by t map, S is non-empty a finite set of irreducible polynomials, and F is a finite field of odd characteristic, is undecidable.

Keywords: Positive-existential definability; Finite field of odd characteristic.

MSC (2010): 11U05.

Cite this article as (IEEE citation style):

L. Cerda-Romero and C. Martínez-Ranero, "The diophantine problem for addition and divisibility for subrings of rational functions over finite fields", *Proyecciones (Antofagasta, On line)*, vol. 39, no. 3, pp. 721-736, Jun. 2020, doi: 10.22199/issn.0717-6279-2020-03-0045.

1. Introduction

Given a commutative ring R, one can consider whether the structure

$(R; 0, 1, +, |)$, where $|$ denotes the divisibility relation, is decidable. This line of research has been studied for several years. In [10] J. Robinson showed that the first order theory of $(\mathbf{Z}; 0, 1, +, |)$ is undecidable. Later on, Lipshitz [8] (and independently, Bel'tyukov [1]) proved that the positive existential theory of $(\mathbf{Z}; 0, 1, +, |)$ is decidable; this also holds in any ring of algebraic integers of an imaginary quadratic number field. In [7] and [9] Liphitz proved that multiplication is positive existentially definable from addition and divisibility in the ring of integers $\mathcal{O}_K$, whenever K is a number field which is neither $\mathbf{Q}$ nor imaginary quadratic. Thus, the positive-existential theory of $(\mathcal{O}_K; 0, 1, +, |)$ is decidable if and only if the positive-existential theory of the ring $\mathcal{O}_K$ is decidable.

In [3] Pheidas proved that the existential theory of addition and divisibility in a ring of polynomials $F[t]$, over a field F, with constants for the elements $0, 1$, and t, is decidable if and only if the ring-theory of F is decidable. He also showed, in [4], that this result does not extend to polynomials in two variables. In order to do so, he shows that the positive existential theory of of the structure $(A[t, t^{-1}]; 0, 1, +, |, x \mapsto tx)$, where $x \mapsto tx$ represents the multiplication by t map, is undecidable whenever A is an integral domain. In this paper we extend Pheidas result to holomorphy rings of rational functions over finite fields.

Our main result is the following.

Main Theorem 1.1. *If S is a non-empty finite set of irreducible polynomials, then multiplication is positive existentially definable in*

$$\mathcal{F}_S := (S^{-1}\mathbf{F}[t]; =, \mathbf{F}, 0, 1, +, |, f \mapsto tf).$$

In particular, the positive existential theory of the structure $\mathcal{F}_S$ is undecidable.

The analogous result for the rational integers also holds and it was proved by the authors in [2]. The proof follows closely the one from [2] which is classical in this sort of problems, and consists of gradually defining the multiplication: first we square units, then we multiply a unit by an arbitrary element of the ring, and finally we define the squaring function. Multiplication is definable from the squaring function thanks to the identity $(x + y)^2 = x^2 + 2xy + y^2$.

The main differences whit results presented in [2] are that we need a deep result from Lenstra [6] to define the relation different from zero, and the main formula is different and requires new arguments. However, it is worth pointing out, that Lemmas 3.4, and 3.6 and Proposition 3.5 are straightforward adaptations of Lemmas 2.11, 2.14 and Proposition 2.12 in [2], respectively and are added for the sake of completeness.

Before proceeding any further we need to introduce some notation.

So from now on we fix an arbitrary finite field $\mathbf{F}$ of odd characteristic, and a non-empty finite set

$$S = \{Q_1, \ldots, Q_M\}$$

of M monic irreducible polynomials. Our goal is to define multiplication on the structure

$$\mathcal{F}_S = (S^{-1}\mathbf{F}[t]; =, \mathbf{F}, 0, 1, +, |, f \mapsto tf).$$

Notation 1.2. *1.* **as** (x, y) *stands for the formula* $x|y \wedge y|x$ *(namely,* x *and* y *are associate).*

2. $x \pm y \mid w \pm z$ *stands for*

$$x + y \mid w + z \wedge x - y \mid w - z.$$

3. If $\gamma = (\gamma_1, \ldots, \gamma_M)$ *is a vector of natural numbers and* $Q = (Q_1, \ldots, Q_M)$*, then* Q^γ *will stand for the product*

$$\prod_{i=1}^{M} Q_i^{\gamma_i}.$$

Definition 1.3. *Let* $\mathrm{ord}_Q x$ *be the* Q*-adic order of* $x \in \mathbf{F}(\mathbf{t})$*. We define a norm function* $N\colon S^{-1}\mathbf{F}[t] \longrightarrow \mathbf{F}[t]$ *by*

$$x \longmapsto x \prod Q_i^{-\,\mathrm{ord}_{Q_i} x}$$

if $x \neq 0$*, and* $N(0) = 0$*.*

We observe that the function N satisfies the following:

- $N(xy) = N(x)N(y)$
- $N(x) = 0$ if only if $x = 0$
- $x \mid y$ if only if $N(x) \mid_{\mathbf{F}[t]} N(y)$, where $\mid_{\mathbf{F}[t]}$ means "divisibility in $\mathbf{F}[t]$".
- The norm of a unit is a unit in $\mathbf{F}$.

From now on, whenever it is clear from the context, we use the "$|$" symbol to indicate divisibility both in both rings $S^{-1}\mathbf{F}[\mathbf{t}]$ and $\mathbf{F}[\mathbf{t}]$.

2. Definability of "to be distinct"

We start by proving that the relation "different from 0" is positive-existentially definable in $\mathcal{F}_S$. In order to do this, we need the following results. The first one is an analogue of Dirichlet theorem for primes in arithmetic progressions — see [5].

Theorem 2.1 (Kornblum, '19). *Let $a, m \in \mathbf{F}[t]$ be two relatively prime polynomials. If m has positive degree, then the set*

$$\Gamma = \{p \in \mathbf{F}[t] : p \equiv a \ (mod\ m),\ p \text{ is irreducible}\}$$

has positive Dirichlet density. In particular, Γ is infinite.

Before stating the next result, we need to introduce some notation:

- K is a function field in one variable over a finite field.
- F is a finite Galois extension of K.
- $C \subseteq \ \mathrm{Gal}(F/K)$ is a union of conjugacy classes.
- W is a finitely generated subgroup of K^*, of rank $r \geq 1$ modulo its torsion subgroup.
- k is an integer relatively prime with the characteristic p of K.
- If $\mathbf{p}$ is a prime of K, $(\mathbf{p},\ F/K)$ will denote the Frobenius symbol.

Let $\mathcal{M} = \mathcal{M}(K, F, C, W, k)$ denote the set of primes $\mathbf{p}$ so that:

1. $(\mathbf{p},\ F/K) \subseteq C$,
2. $ord\mathbf{p}\ (w) = 0$ for all $w \in W$, and
3. if $\psi : W \to \overline{K}^*_{\mathbf{p}}$ denote the quotient map to the unit subgroup of the residue class field, then the index of $\psi(W)$ in $\overline{K}^*_{\mathbf{p}}$ divides k.

Lenstra [6] found a formula for the Dirichlet density of $\mathcal{M}$. In order to state this formula, we need to introduce some further notation. Consider K, F, C, W and k as above. For a prime number $\ell \neq p$, let $q(\ell)$ be the smallest power of ℓ not dividing k and let

$$L_\ell = K\left(\zeta_{q(\ell)}, W^{\frac{1}{q(\ell)}}\right)$$

be the field obtained by adjoining all $q(\ell)$-roots of the elements of W to K. If n is a positive square-free integer, relatively prime to p, then define L_n to be the composite of the fields L_ℓ where ℓ is a prime factor of n. Define

$$C_n = \{\sigma \in \ \mathrm{Gal}(F \cdot L_n/K)\colon \sigma_{|F} \in C, \ \text{ and } \sigma_{|Lt} \neq \ \mathrm{Id}_{L_\ell} \ \text{ for } \ \text{all } \ell | n\}$$

and

$$a_n = \frac{|C_n|}{[F \cdot L_n\colon K]}.$$

Note that if n divides m, then $a_n \geq a_m \geq 0$. It follows that the sequence (a_n) has a limit as n ranges over all square free integers relatively prime to p, ordered by divisibility. Let $a = \lim a_n$.

Theorem 2.2 (Lenstra, '77). *If K is a function field in one variable over a finite field then the set $\mathcal{M}$ has Dirichlet density a.*

Lemma 2.3. *There exists an irreducible polynomial q not in S, and a polynomial $b \in \mathbf{F}[t]$ of degree less than q, such that $qx + b$ is never a unit of $S^{-1}\mathbf{F}[t]$ as x varies over $S^{-1}\mathbf{F}[t]$.*

Proof. Let $K = F = \mathbf{F}(t)$, $C = \{Id_K\}, k = 2$ and let W be the multiplicative subgroup of K^* generated by $\mathbf{F}^* \cup S$. Observe that if $\mathbf{p} \notin \mathcal{M}(K, F, C, W, k)$, then the index of $\psi(W)$ in $\overline{K}^*_{\mathbf{p}}$ does not divide 2. In particular, $\psi(W) \neq \overline{K}^*_{\mathbf{p}}$. Since S is non-empty, the identity is not in C_n, hence $a_n < 1$ for each possible $n > 1$, so by Lenstra's theorem, the Dirichlet density of $\mathcal{M}$ is less than 1.

Choose $\mathbf{q}$=(q)$\notin \mathcal{M}$ such that $q \in K$ is irreducible and different from all Q_i, and b a polynomial of degree less than the degree of q whose class modulo q lies in $\overline{K}^*_{\mathbf{q}} \setminus \psi(W)$. The polynomials q and b trivially satisfy the desired condition.

Lemma 2.4. *The relation $\neq$ is positive-existentially definable in the structure $\mathcal{F}_S$.*

Proof. Let q and b be some polynomials given by Lemma 2.3. The formula

$$\psi_{\neq}(y) : \exists A, B, x(y \mid A \wedge qx + b \mid B \wedge A + B = 1)$$

defines the relation "$y \neq 0$" in $\mathcal{F}_S$.

First note that the formula $\psi_{\neq}(y)$ translates to "There exist $r, s, x \in S^{-1}\mathbf{F}[t]$ such that $ry + s(qx + b) = 1$" in $\mathcal{F}_S$.

If $y = 0$, then the formula is false, since by Lemma 2.3, $qx + b$ is never a unit in $\mathbf{S}^{-1}\mathbf{F}[t]$.

Assume $y \neq 0$. Since q and b are relatively prime, by Kornblum's theorem, there exists x such that $qx + b$ is an irreducible, and furthermore coprime with $N(y)$. By Bézout's identity, which holds in any Euclidean domain, there are polynomials r' and s such that

$$r'N(y) + s(qx + b) = 1.$$

Since $y = N(y)u$, where u is a unit, we have $\dfrac{r'}{u}y + s(qx + b) = 1$.

Remark 2.5. *As usual, once we have proved that a relation is positive-existentially definable we can use it freely in forthcoming formulas.*

3. Definability of multiplication

Given $z \in \mathbf{F}(t)^*$, define $\operatorname{sgn}(z)$ to be the unique $a \in \mathbf{F}$ such that

$$z = \frac{ax}{y},$$

and x and y are monic polynomials. By $\operatorname{ord}_\infty z$ we mean the difference of degrees $\deg y - \deg x$. In order to have simpler statements along this section, we may write $\operatorname{ord}_{Q_\infty}$ instead of $\operatorname{ord}_\infty$. It is easy to see that

$$\operatorname{sgn}(x \cdot y) = \operatorname{sgn}(x) \cdot \operatorname{sgn}(y),$$

and if $\operatorname{ord}_{Q_\infty} x \neq \operatorname{ord}_{Q_\infty} y$, then

$$\operatorname{sgn}(x + y) \in \{\operatorname{sgn}(x), \operatorname{sgn}(y)\}.$$

Lemma 3.1. *Let x, y, z and v be arbitrary elements of $S^{-1}\mathbf{F}[t]$. Assume that for all $i \in \{\infty, 1, \ldots, M\}$ we have $\operatorname{ord}_{Q_i} x \neq \operatorname{ord}_{Q_i} y$ and $\operatorname{ord}_{Q_i} z \neq \operatorname{ord}_{Q_i} v$. If the formula $\mathbf{as}(x \pm y, z \pm v)$ holds in $\mathcal{F}_S$, then either we have $xv = yz$ or $xz = yv$.*

Proof. Let u_1, u_2 be units such that

$$x + y = u_1(z + v) \qquad \text{and} \qquad x - y = u_2(z - v). \tag{3.1}$$

Observe that since $\operatorname{ord}_{Q_i} x \neq \operatorname{ord}_{Q_i} y$, we have

$$\operatorname{ord}_{Q_i}(x + y) = \min\{\operatorname{ord}_{Q_i} x, \operatorname{ord}_{Q_i} y\} = \operatorname{ord}_{Q_i}(x - y)$$

and since $\operatorname{ord}_{Q_i} z \neq \operatorname{ord}_{Q_i} v$, we have

$$\operatorname{ord}_{Q_i}(z+v) = \min\{\operatorname{ord}_{Q_i} z, \operatorname{ord}_{Q_i} v\} = \operatorname{ord}_{Q_i}(z-v)$$

for all $1 \leq i \leq M$. Thus, for each $1 \leq i \leq M$, we have

$$\begin{aligned} \operatorname{ord}_{Q_i} u_1 + \min\{\operatorname{ord}_{Q_i} z, \operatorname{ord}_{Q_i} v\} &= \min\{\operatorname{ord}_{Q_i} x, \operatorname{ord}_{Q_i} y\} \\ \operatorname{ord}_{Q_i} u_2 + \min\{\operatorname{ord}_{Q_i} z, \operatorname{ord}_{Q_i} v\} &= \min\{\operatorname{ord}_{Q_i} x, \operatorname{ord}_{Q_i} y\} \end{aligned}$$

so that $\operatorname{ord}_{Q_i} u_1 = \operatorname{ord}_{Q_i} u_2$ (note that the hypothesis of the Lemma imply that all the terms in these equalities are actual integers). This implies that $u_1 = a u_2$ for some $a \in \mathbf{F}^*$. Now we show that $a = \pm 1$.

Since $\operatorname{ord}_{Q_\infty} x \neq \operatorname{ord}_{Q_\infty} y$ and $\operatorname{ord}_{Q_\infty} z \neq \operatorname{ord}_{Q_\infty} v$ we have

$$\operatorname{sgn}(x+y) = \pm \operatorname{sgn}(x-y) \quad \text{and} \quad \operatorname{sgn}(z+v) = \pm \operatorname{sgn}(z-v).$$

On the other hand, since we have

$$\operatorname{sgn}(u_1) = \frac{\operatorname{sgn}(x+y)}{\operatorname{sgn}(z+v)} \quad \text{and} \quad \operatorname{sgn}(u_2) = \frac{\operatorname{sgn}(x-y)}{\operatorname{sgn}(z-v)},$$

we get $a = \pm 1$.

This implies that either $u_1 = u_2$ or $u_1 = -u_2$. We proceed by cases.

If $u_1 = u_2$, then from Equations (3.1), we have $x + y = u_1 z + u_1 v$ and $x - y = u_1 z - u_1 v$. By adding and subtracting these equations, we obtain $x = u_1 z$ and $y = u_1 v$, hence $xv = yz$.

If $u_1 = -u_2$, then from Equations (3.1), we have $x + y = u_1 z + u_1 v$ and $x - y = -u_1 z + u_1 v$. By adding and subtracting these equations again, we obtain $x = u_1 v$ and $y = u_1 z$, hence $xz = vy$.

The next Lemma is a first step to define the squaring function among units of $S^{-1}\mathbf{F}[\mathbf{t}]$.

Lemma 3.2. *Let x and y be units in $S^{-1}\mathbf{F}[\mathbf{t}]$ such that $x \neq \pm 1$ and $y \neq 1$. Assume that for all $i \in \{\infty, 1, \ldots, M\}$ we have $\operatorname{ord}_{Q_i} x \neq \operatorname{ord}_{Q_i} y$. We have:*

$$y = x^2 \text{ if and only if } \mathcal{F}_S \text{ satisfies } \mathbf{as}(x \pm 1, y \pm x).$$

Proof. If $y = x^2$ then $S^{-1}\mathbf{F}[\mathbf{t}]$ trivially satisfies $\mathbf{as}(x \pm 1, y \pm x)$ (since x is a unit). Suppose that $\mathbf{as}(x \pm 1, y \pm x)$ is true in $S^{-1}\mathbf{F}[\mathbf{t}]$. By Lemma 3.1, either $y = x^2$ or $xy = x$. Since x is a unit and $y \neq 1$, we conclude that $y = x^2$.

From Lemma 3.2, we can show that the squaring function between units is positive-existentially definable.

Proposition 3.3. *The set*

$$SQ_u = \{(x, y) \colon x, y \text{ are units in } S^{-1}\mathbf{F}[X] \text{ and } y = x^2\}$$

is positive-existentially definable in the structure $\mathcal{F}_S$.

Proof. Write $I = \{0, 1, 2, 3, 4\}^M$ and consider the formula

$$Sq_u(x, y) \colon x \mid 1 \wedge y \mid 1 \wedge \bigwedge_{\gamma \in I} \mathbf{as}(Q^\gamma x \pm 1, Q^{2\gamma} y \pm Q^\gamma x)$$

where γ reads as $(\gamma_1, \ldots, \gamma_M)$ (see Notation 1.2).

Assume that (x, y) holds. In particular, for each γ_i, for $i \in \{1, ...M\}$, in

$$\gamma_i \in \{0, 1, 2, 3, 4\} \setminus \left\{ -\operatorname{ord}_{Q_i} x, -\frac{1}{2}\operatorname{ord}_{Q_i} y,\ \operatorname{ord}_{Q_i} x - \operatorname{ord}_{Q_i} y \right\},$$

$Q^\gamma x$ and $Q^{2\gamma} y$ satisfy the hypothesis of Lemma 3.2 except maybe for the order at infinity. So we have to make sure that

$$\operatorname{ord}_{Q_\infty} Q^{2\gamma} y - \operatorname{ord}_{Q_\infty} Q^\gamma x \neq 0,$$

hence that

$$\operatorname{ord}_{Q_\infty} y - \operatorname{ord}_{Q_\infty} x + \sum_{i=1}^{M} \operatorname{ord}_{Q_\infty} Q_i^{\gamma_i} \neq 0,$$

which clearly can be done since we still have two degrees of freedom for choosing γ_1 (say). We conclude that $y = x^2$.

Write $\nu(x, y, z)$ for the formula

$$\mathbf{as}(y \pm 1, z \pm x) \wedge \mathbf{as}(y \pm x, z \pm x^2).$$

Lemma 3.4. *Let* x *be a unit in* $\mathcal{F}_S$ *with* $x \neq \pm 1$. *If for all* $i \in \{\infty, 1, ..., M\}$, *we have* $\operatorname{ord}_{Q_i} y \neq 0$, $\operatorname{ord}_{Q_i} z \neq \operatorname{ord}_{Q_i} x$, $\operatorname{ord}_{Q_i} y \neq \operatorname{ord}_{Q_i} x$ *and* $\operatorname{ord}_{Q_i} z \neq \operatorname{ord}_{Q_i} x^2$, *then* $z = xy$ *if and only if* $\mathcal{F}_S$ *satisfies* $\nu(x, y, z)$.

Proof. Assume that the formula $\nu(x, y, z)$ holds in $\mathcal{F}_S$. By Lemma 3.1, since $\mathbf{as}(y \pm 1, z \pm x)$ holds, we have that either $z = xy$ or $x = yz$. Again by Lemma 3.1, since $\mathbf{as}(y \pm x, z \pm x^2)$ holds, we have that either $z = xy$ or $x^3 = yz$. So the only case in which we may have $z \neq xy$ is when $x = yz$ and $x^3 = yz$, which would imply that $x = \pm 1$.

Proposition 3.5. *The set*

$$P = \{(x, y, z) : x \text{ is a unit and } z = xy\}$$

is positive existentially definable in the structure $\mathcal{F}_S$.

Proof. Write $I = \{0,1,2,3,4\}^M$. The formula

$$Pro(x,y,z)\colon x \mid 1 \wedge \bigwedge_{(\delta,\gamma)\in I\times I} \nu(Q^\gamma x, Q^\delta y, Q^{\delta+\gamma} z)$$

defines the set P. Note that if $z = xy$, then $Pro(x,y,x)$ is trivially satisfied for $(x,y,z) \in P$, since $Q^\gamma x$ is a unit. We now prove the converse. We choose δ_i, for $i \in \{1,...,M\}$, such that

$$\delta_i \in \{0,1,2,3,4\} \setminus \{-\operatorname{ord}_{Q_i} y,\ \operatorname{ord}_{Q_i} x - \operatorname{ord}_{Q_i} z\}.$$

Once δ_i has been chosen, we choose γ_i such that

$$\gamma_i \in \{0,1,2,3,4\}\setminus\{-\operatorname{ord}_{Q_i} x, \delta_i + \operatorname{ord}_{Q_i} y - \operatorname{ord}_{Q_i} x, \delta_i + \operatorname{ord}_{Q_i} z - 2\operatorname{ord}_{Q_i} x\}.$$

From $\gamma_i \neq -\operatorname{ord}_{Q_i} x$ we have $Q^\gamma x \neq \pm 1$. In addition for each i, we have

- $\operatorname{ord}_{Q_i} Q^\delta y = \delta_i + \operatorname{ord}_{Q_i} y \neq 0$,
- $\operatorname{ord}_{Q_i} Q^\delta y - \operatorname{ord}_{Q_i} Q^\gamma x = \delta_i + \operatorname{ord}_{Q_i} y - \gamma_i - \operatorname{ord}_{Q_i} x \neq 0$ and
- $\operatorname{ord}_{Q_i} Q^{\delta+\gamma} z - \operatorname{ord}_{Q_i} Q^{2\gamma} x^2 = \delta_i + \operatorname{ord}_{Q_i} z - \gamma_i - 2\operatorname{ord}_{Q_i} x \neq 0$,

as before we still have two degrees of freedom to make the order at infinity differ so that we can arrange that $Q^\gamma x$, $Q^\delta y$ and $Q^{\delta+\gamma} z$ satisfy the hypothesis of Lemma 3.4. Since we assumed that (x,y,z) holds, in particular $\nu(Q^\gamma x, Q^\delta y, Q^{\delta+\gamma} z)$ holds, so we can conclude that $z = xy$.

Lemma 3.6. *Given $x_1, \ldots, x_n \in S^{-1}\mathbf{F}[t] \setminus \{0\}$, there exists a unit $u \neq 1$ so that each of x_1, ..., and x_n divides $u - 1$.*

Proof. Choose any irreducible polynomial P in S and consider

$$u = P^{\operatorname{lcm}\{\varphi(|N(x_i)|):i=1,\ldots,n\}}$$

where "lcm" stands for "least common multiple". Since $N(x_i)$ divides

$$P^{\varphi(|N(x_i)|)} - 1,$$

in $\mathbf{F}[t]$ (by Euler's theorem - note that $N(x_i)$ is prime with P by definition of the norm), also it divides $u - 1$, hence

$$x_i = N(x_i) \prod Q_j^{\operatorname{ord}_{Q_j} x_i}$$

divides $u-1$ in $\mathcal{F}_S$.

Write $I = \{0,1\}^M$. Consider the formula $\varphi(x,y)$

$$\exists u_1 \exists u(u_1 \mid 1 \wedge u_1 \neq 1 \wedge u \neq 1 \wedge x+1 \mid u_1 - 1 \wedge y+1 \mid u_1 - 1 \wedge (u_1-1)^{16} \mid u-1 \wedge \varphi_0(x,y))$$

where $\varphi_0(x,y)$ is defined as:

$$\bigwedge_{\gamma \in I} x \pm Q^{\gamma} u \mid y - Q^{2\gamma} u^2.$$

Lemma 3.7. *Let $x, y \in S^{-1}\mathbf{F}[\mathbf{t}]$. Assume that for all $i \in \{\infty, 1, \ldots, M\}$ we have $ord_{Q_i} x \neq 0$, $ord_{Q_i} y \neq 0$. If $\varphi(x,y)$ holds in $\mathcal{F}_S$, then $y = x^2$.*

Proof. Write

$$x = f \prod_{i=1}^{M} Q_i^{\alpha_i}, \quad y = g \prod_{i=1}^{M} Q_i^{\beta_i} \quad \text{and} \quad u = \kappa \prod_{i=1}^{M} Q_i^{\delta_i}$$

where f (and g) is a polynomial relatively prime with each Q_i, and $\kappa \in \mathbf{F}^*$. From $\operatorname{ord}_{Q_i} x \neq 0$ and $\operatorname{ord}_{Q_i} y \neq 0$ we have

$$N(x+1) = f \prod_{\alpha_i > 0} Q_i^{\alpha_i} + \prod_{\alpha_i < 0} Q_i^{-\alpha_i}$$

and

$$N(y+1) = g \prod_{\beta_i > 0} Q_i^{\beta_i} + \prod_{\beta_i < 0} Q_i^{-\beta_i}.$$

Since $x+1$ divides $u_1 - 1$, also $N(x+1)$ divides $N(u_1 - 1)$ in $\mathbf{F}[\mathbf{t}]$, hence in particular, since u_1 is not 1, we have

$$\deg(N(x+1)) \leq \deg(N(u_1 - 1)).$$

On the other hand, since x has non-zero order at infinity, the degree of $N(x+1)$ is equal to either

$$\deg(f) + \sum_{\alpha_i > 0} \alpha_i$$

or

$$\sum_{\alpha_i < 0} (-\alpha_i),$$

so that we have

$$\deg(f) + \sum_{i=1}^{M} |\alpha_i| \leq 2\deg(N(u_1 - 1)) \tag{3.2}$$

Analogously, we have

$$\deg(g) + \sum_{i=1}^{M} |\beta_i| \leq 2\deg(N(u_1 - 1)) \tag{3.3}$$

From Equations (3.2) and (3.3) and because u is not 1 by hypothesis, we have

$$\begin{aligned} 2\left(2\deg(f) + 2\textstyle\sum_{i=1}^{M} |\alpha_i| + \deg(g) + \sum_{i=1}^{M} |\beta_i|\right) &\leq 12\deg(N(u_1 - 1)) \\ &< 16\deg(N(u_1 - 1)) \\ &< \deg(N(u - 1)), \end{aligned}$$

hence

$$2\deg(f)+2\sum_{i=1}^{M}|\alpha_i|+\deg(g)+\sum_{i=1}^{M}|\beta_i| < \deg(N(u-1))-\left(\sum_{i=1}^{M}|\alpha_i| + \sum_{\alpha_i>\delta_i}(\alpha_i-\delta_i)\right). \tag{3.4}$$

On other hand, we have

$$y - x^2 = P\left(g \prod_{\beta_i - 2\alpha_i \geq 0} Q_i^{\beta_i - 2\alpha_i} - f^2 \prod_{\beta_i - 2\alpha_i < 0} Q_i^{2\alpha_i - \beta_i}\right),$$

where P is a product of powers of the polynomials Q_i, hence

$$\begin{aligned} \deg(N(y - x^2)) &\leq \deg(\prod_{\beta_i - 2\alpha_i \geq 0} Q_i^{\beta_i - 2\alpha_i} - f^2 \prod_{\beta_i - 2\alpha_i < 0} Q_i^{2\alpha_i - \beta_i}) \\ &\leq 2\deg(f) + 2\sum_{i=1}^{M} |\alpha_i| + \deg(g) + \sum_{i=1}^{M} |\beta_i|, \end{aligned}$$

so from the relation (3.4), we get

$$\deg(N(y - x^2)) < \deg(N(u - 1)) - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right). \tag{3.5}$$

For the sake of contradiction, assume that y is not equal to x^2. Since we assume that $\varphi(x, y)$ holds, in particular by choosing $\gamma_i \in \{0, 1\} \setminus \{\alpha_i - \delta_i\}$ for each i, we have

$$x \pm \prod Q_i^{\gamma_i} u \mid y - \prod Q_i^{2\gamma_i} u^2.$$

Since also

$$x \pm \prod Q_i^{\gamma_i} u \mid x^2 - \prod Q_i^{2\gamma_i} u^2,$$

by taking the difference, we obtain

$$x \pm \prod Q_i^{\gamma_i} u \mid y - x^2,$$

therefore

$$\deg\left(N(x \pm \prod Q_i^{\gamma_i} u)\right) \leq \deg(N(y - x^2)). \tag{3.6}$$

We claim that either

$$\deg(N(u-1)) - \sum_{i=1}^{M} |\alpha_i| \leq \deg(N(x + \prod Q_i^{\gamma_i} u)),$$

or

$$\deg(N(u-1)) - \sum_{i=1}^{M} |\alpha_i| \leq \deg(N(x - \prod Q_i^{\gamma_i} u)),$$

hence by (3.5), either

$$\deg(N(y - x^2)) < \deg(N(x + \prod Q_i^{\gamma_i} u))$$

or

$$\deg(N(y - x^2)) < \deg(N(x - \prod Q_i^{\gamma_i} u))$$

which contradicts (3.6).

In order to prove the claim, note that

$$\deg(N(u-1)) \leq \sum_{i=1}^{M} |\delta_i|,$$

hence

$$\deg(N(u-1)) - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right)$$

is less than or equal to

$$\sum_{i=1}^{M} |\delta_i| - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i) \right).$$

On other hand, for some choice of the sign (and from our choice of the γ_i) we have that $\deg(N(x \pm \prod Q_i^{\gamma_i} u))$ is equal to the maximum value between

$$\deg(f) + \sum_{\alpha_i \geq \gamma_i + \delta_i} (\alpha_i - (\gamma_i + \delta_i))$$

and

$$\sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i)$$

(indeed, only choice of sign may produce cancelation in $x \pm \prod Q_i^{\gamma_i} u$). Hence it suffices to show that

$$\sum_{i=1}^{M} |\delta_i| - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i) \right) \leq \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i).$$

We have

$$\begin{aligned}
&\sum_{i=1}^{M} |\delta_i| - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i) \right) - \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i) \\
&\leq \sum |\delta_i - \alpha_i| - \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i) - \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i) \\
&= \sum_{\alpha_i < \delta_i} (\delta_i - \alpha_i) - \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i) \\
&\leq \sum_{\alpha_i < \delta_i} (\delta_i - \alpha_i) - \sum_{\alpha_i < \delta_i} (\gamma_i + \delta_i - \alpha_i) \leq 0.
\end{aligned}$$

Write $J = \{0, 1, 2\}^M$ and consider the following formula $\psi(x, y)$:

$$\bigwedge_{\delta \in J} \varphi \left(Q^{\delta} x, Q^{2\delta} y \right).$$

Proposition 3.8. *If $\psi(x, y)$ holds in $\mathcal{F}_S$, then $y = x^2$.*

Proof. This is an immediate consequence of Lemma 3.7, noting that there exists a choice of δ for which we have $\operatorname{ord}_{Q_i} Q^{\delta} x \neq 0$ and $\operatorname{ord}_{Q_i} Q^{2\delta} y \neq 0$ for each i (from the definition of J).

We can now conclude.

Lemma 3.9. *The set*

$$SQ_u = \{(x, y) \colon x, y \text{ are in } S^{-1}\mathbf{F}[t] \text{ and } y = x^2\}$$

is positive existentially definable in the structure $\mathcal{F}_S$.

Proof. We claim that the formula

$$Sq(x, y) : (x = 0 \wedge y = 0) \vee \bigvee_{\delta \in J} (x = \pm Q^{-\delta} \wedge y = Q^{-2\delta}) \vee \psi(x, y),$$

defines the set SQ_u. Indeed, if the formula holds, then it is immediate from Proposition 3.8 that $y = x^2$.

Assume $(x, y) \in \mathrm{SQ}_u$. Without loss of generality, we can assume $x \neq 0$ and, $x \neq Q^{-\delta}$ and $x \neq -Q^{-\delta}$ for all $\delta \in J$. Thus, for each $\delta \in J$, $Q^{2\delta} y \pm 1 \neq 0$.

From Lemma 3.6, there is a unit u_1 distinct from 1 such that $Q^{\delta} x \pm 1$ divides $u_1 - 1$ and $Q^{2\delta} y \pm 1$ divides $u_1 - 1$. Because $u_1 - 1$ is not zero we deduce, from Lemma 3.6 again, that there is a unit u different from 1 such that

$$(u_1 - 1)^{16} \mid u - 1.$$

In addition, we have $\bigwedge_{(\delta,\gamma) \in J \times I} Q^{\delta} x \pm Q^{\gamma} u \mid Q^{2\delta} y - Q^{2\gamma} u^2$. Thus, the formula $\psi(x, y)$ is satisfied.

Acknowledgements

This is part of the first author doctoral thesis at the Universidad de Concepción (Chile). The first author was supported by SENESCYT Convocatoria Abierta 2011. The second author was partially supported by Proyecto FONDECYT Iniciación No. 11130490.

References

[1] A. P. Beltyukov, "Decidability of the universal theory of natural numbers with addition and divisibility", *Journal of soviet mathematics,* vol. 14, no. 5, pp. 1436–1444, Nov. 1980, doi: 10.1007/BF01693974

[2] L. Cerda-Romero and C. Martínez-Ranero, "The diophantine problem for addition and divisibility over subrings of the rationals", *The journal of symbolic logic,* vol. 82, no. 3, pp. 1140–1149, Sep. 2017, doi: 10.1017/jsl.2016.64

[3] A. C. Pheidas, "The diophantine problem for addition and divisibility in polynomial rings (Decidability, undecidability)", Ph. D. Thesis, Purdue University, 1985. [On line]. Available: https://bit.ly/3cruCUp

[4] T. Pheidas, "Diophantine undecidability for addition and divisibility in polynomial rings", *Fundamenta mathematicae,* vol. 182, no. 3, pp. 205-220, 2004, doi: 10.4064/fm182-3-2

[5] H. Kornblum and E. Landau, "Über die primfunktionen in einer arithmetischen progression", *Mathematische zeitschrift*, vol. 5, no. 1-2, pp. 100–111, Mar. 1919, doi: 10.1007/BF01203156

[6] H. W. Lenstra, "On Artins conjecture and Euclids algorithm in global fields", *Inventiones mathematicae*, vol. 42, no. 1, pp. 201–224, 1977, doi: 10.1007/BF01389788

[7] L. Lipshitz, "Undecidable existential problems for addition and divisibility in algebraic number rings. II", *Proceedings of the American Mathematical Society*, vol. 64, no. 1, pp. 122–128, Jan. 1977, doi: 10.1090/S0002-9939-1977-0536659-5

[8] L. Lipshitz, "The Diophantine problem for addition and divisibility", *Transactions of the American Mathematical Society,* vol. 235, pp. 271-283, 1978, doi: 10.1090/S0002-9947-1978-0469886-1

[9] L. Lipshitz, "Undecidable existential problem for addition and divisibility in algebraic number rings", *Transactions of the American Mathematical Society*, vol. 241, pp. 121-128, 1978, doi: 10.1090/S0002-9947-1978-0536658-9

[10] J. Robinson, "Definability and decision problems in arithmetic", *Journal of symbolic logic,* vol. 14, no. 2, pp. 98–114, Jun. 1949, doi: 10.2307/2266510