Diophantine Properties of Finite Commutative Rings

Mihai Prunescu *

Abstract

Simple observations on diophantine definability over finite commutative rings lead to a characterization of those rings in terms of their diophantine behavior.
A.M.S. Classification: 13M10, 11T06, 03G99.

1 Introduction

Questions of diophantine definability in the language of rings can be often reduced to diophantine definability of disjunctions, conjunctions or negations of polynomial equations. Over the ring of rational integers $\mathbb{Z}$ these logical relations admit diophantine definitions: $x = 0 \vee y = 0 \Leftrightarrow xy = 0$, $x = 0 \wedge y = 0 \Leftrightarrow x^2 + y^2 = 0$ and $x \neq 0 \Leftrightarrow \exists\, t, s\ tx = (2s-1)(3s-1)$. All these definitions play an important role in Matiyasevich' construction of an universal diophantine equation, see [2].

The first definition is true over all domains. Definitions similar to the second one are possible over all domains having not algebraically closed fields of quotients with suitable polynomials $f(x, y)$. The third definition, basing here on the Chinese Remainder Theorem, has a more difficult nature. For examples of domains of arbitrary characteristic that do not accept at all existential positive definitions for the complement of 0 see [3] and [4].

The aim of this note is to investigate diophantine definability of these relations in a class of commutative rings containing not just domains, namely in the class of all finite commutative rings with 1.

Definition: Let R be a commutative ring with 1. A relation $\mathcal{R}(\vec{x}) \subset R^k$ will be called **diophantine** if there is a polynomial $P \in R[\vec{x}, \vec{\lambda}]$ such that:

$$R \models\ \forall \vec{x}\ (\,\mathcal{R}(\vec{x}) \leftrightarrow \exists\, \vec{\lambda}\ P(\vec{x}, \vec{\lambda}) = 0\,).$$

2 Some Commutative Algebra

We recall here the algebraic facts that will be used in this note.

Definition: Let R be a commutative ring with 1. An element $e \in R$ is called non-trivial **idempotent** if $e^2 = e$ and $e \neq 0, 1$.

In this case $1 - e \neq e$ is another non-trivial idempotent. We observe that $e(1 - e) = 0$, thus the idempotent elements e and $1 - e$ cannot be units. They always belong to different maximal ideals. We will often tacitly use the following identity:

$$(ae + b(1-e))(ce + d(1-e)) = ace + bd(1-e).$$

Lemma 2.1 *Let R be a commutative ring with 1. There are non-trivial rings R_1 and R_2 such that $R \simeq R_1 \times R_2$ if and only if there exists a non-trivial idempotent $e \in R$. In this case one can choose $R_1 = Re$ and $R_2 = R(1-e)$.*

*Universität Greifswald, Germany; and IMAR Bucharest, Romania.

For a proof, see the Exercise 2.26 in [1]. According to this Lemma, if we consider a finite commutative ring with 1 containing idempotent elements, we can write it as product of two rings. We continue the process until we get only idempotent-free rings. The process will always stop, because R is finite.

Definition: A finite commutative ring with 1 will be called **irreducible** if it does not contain non-trivial idempotent elements. R is irreducible if and only if R is not isomorphic with the product of other non-trivial commutative rings with 1.

The following statement generalizes the representation of natural numbers as product of primes.

Lemma 2.2 *Every non-trivial finite commutative ring with* 1 *has a unique representation as a product of non-trivial irreducible commutative rings with* 1.

Proof: There is only to prove that the representation as product of irreducible rings is unique. Let R be a ring with n elements. We make an induction over n. If $n \in \{2, 3\}$ then there exists only one ring with n elements. Both rings are irreducible, so the property is verified. Let n be > 3. We assume that we have already proven that all finite commutative rings with less than n elements admit a unique representation. If R is irreducible then the property is again trivially verified. We assume now that R is not irreducible and consider two possible decompositions of R in irreducible factors:

$$R \simeq R_1 \times R_2 \times \cdots \times R_k \simeq R'_1 \times R'_2 \times \cdots \times R'_l.$$

It is immediate to see that the idempotent elements of a product $R_1 \times R_2 \times \cdots \times R_k$ are the elements $(f_1, \ldots, f_k)$, where for all i, $f_i \in \{0, 1\} \cup \{$ non-trivial idempotents in R_i $\}$. No R_i contains any non-trivial idempotent, so there are exactly $2^k = 2^l$ idempotent elements in R, and $k = l$.

Now let e be the non-trivial idempotent of R given by $(1, 0, \ldots, 0)$ in the first decomposition. Then $1 - e$ is given by $(0, 1, \ldots, 1)$, $Re \simeq R_1$ and $R(1-e) \simeq R_2 \times \cdots \times R_k$. In the second decomposition e has some form $(f_1, \ldots, f_k) \in \{0, 1\}^k$ and $1 - e = (1 - f_1, \ldots, 1 - f_k)$. So $Re \simeq \otimes R'_i$ and $R(1 - e) \simeq \otimes R'_j$, where i exhausts the set $\{s \mid f_s = 1\}$ and j the set $\{s \mid f_s = 0\}$. But $Re \simeq R_1$ is irreducible. Thus exactly one f_i, say $f_1 = 1$ and $R_1 \simeq R'_1$. On the other side $R(1 - e)$ has strictly less elements than R so according to our hypothesis $R(1 - e)$ admits only one representation as product of irreducible rings. Thus modulo a permutation of the rings $R_2 \simeq R'_2$, $\ldots$, $R_k \simeq R'_k$, and we have proved that R has a unique decomposition in irreducible factors. □

Definition: We call **Spectrum** of a ring R the set of all its non-trivial prime ideals $\mathfrak{p}$. The Spectrum of R will be denoted by Spec R. A subset $X \subset$ Spec R is called **closed** if there is an ideal I of R such that $X = \{\mathfrak{p} \mid I \subseteq \mathfrak{p}\}$. This defines the Zariski topology over Spec R.

Lemma 2.3 Spec R *is a disconnected topological space if and only if there exists a non-trivial idempotent* $e \in R$.

For a proof, see the Exercise 2.25 in [1].

We avoid in the following statement the notion of local ring because most of the rings in question are not domains.

Lemma 2.4 *A finite commutative ring* R *with* 1 *is irreducible if and only if* R *contains only one maximal ideal* $\mathfrak{m}$. *In this case* $R \setminus \mathfrak{m}$ *is the set of units of* R.

Proof: We make the following observation: if $\mathfrak{p}$ is a prime ideal of R, the ring $R/\mathfrak{p}$ is a finite commutative domain. But finite commutative domains are always fields, so $\mathfrak{p}$ must already have been a maximal ideal. Therefore, in finite commutative rings with 1 all prime ideals are maximal.

Let R be a finite commutative ring with maximal ideals $\mathfrak{m}_1, ..., \mathfrak{m}_s$. Then Spec $R = \{\mathfrak{m}_1, ..., \mathfrak{m}_s\}$. Any singleton set $\{\mathfrak{m}_i\}$ is a basic clopen set, so Spec R is homeomorphic with the discrete topological space with s elements and is connected if and only if $s = 1$. We recall that R is irreducible if and only if Spec R is connected.

$R \setminus \mathfrak{m}$ is a finite monoid with 1 and simplification, thus it is a multiplicative group. Indeed, if for some elements in $R \setminus \mathfrak{m}$ holds $xy = zy$, then $(x - z)y = 0$ and $x = z$ follows, because all zero-divisors are in $\mathfrak{m}$. In this case $R \setminus \mathfrak{m}$ is the set of units of R. □

Lemma 2.5 *Let R be a finite commutative ring with 1. R is irreducible if and only if there is a natural number $k > 0$ such that for all $x \in R$, $x^k \in \{0, 1\}$. In this case, one has:*

$$x^k = \begin{cases} 0 & \text{if } x \in \mathfrak{m}, \\ 1 & \text{if } x \in R \setminus \mathfrak{m}. \end{cases}$$

Proof: If R is not irreducible, such a number k cannot exist, because for an idempotent $e \notin \{0, 1\}$, $e^k = e$. Assume that R is irreducible.

Let x be in $\mathfrak{m}$. The geometric sequence x, x^2, x^3, ... ranges in the finite set $\mathfrak{m}$, so it must become periodic. If $x^s = x^{s+v}$ then $x^s(1 - x^v) = 0$. But $1 - x^v$ is a unit, so $x^s = 0$. For the finite set $\mathfrak{m}$ there is $m \in \mathbb{N}$ such that $x^m = 0$ for all $x \in \mathfrak{m}$. On the other hand, let u be the order of the finite group $R \setminus \mathfrak{m}$. We take k to be a multiple of u which is $\geq m$. □

Corollary 2.6 *A finite field $\mathbb{F}_q$ with $q = p^s$ elements is an irreducible ring. Its unique maximal ideal is $\{0\}$ and one can take $k = p^s - 1$.*

Proof: The crucial property necessary in order to apply Lemma 2.4 for $\mathbb{F}_q$ is that $\{0\}$ is the unique ideal of a field. The multiplicative group of the field is cyclic, so there are elements of order $p^s - 1$. We cannot give a smaller k. □

Corollary 2.7 *$\mathbb{Z}/n\mathbb{Z}$ is irreducible if and only if n is a prime-power. In this case, if $n = p^s$, the maximal ideal is $\mathfrak{m} = (p)$ and one can take $k = p^s - p^{s-1}$.*

Proof: We may apply again Lemma 2.4 because the only one maximal ideal of $\mathbb{Z}/p^s\mathbb{Z}$ is (p). For the converse, if p_1 and p_2 are different primes dividing n then both ideals (p_1) and (p_2) are maximal. An ideal $\mathfrak{p}$ strictly containing (p_1) would contain also an element y which is not the rest of some multiple of tp_1 modulo n. There are integers u and v such that $up_1 + vy = 1$. Modulo n this means that $1 \in \mathfrak{p}$, which is a contradiction.

The commutative group of units of $\mathbb{Z}/p^s\mathbb{Z}$ has order $p^s - p^{s-1}$. On the other hand for all $x \in \mathfrak{m} = (p)$ one has $x^s = 0$. We observe that $p^s - p^{s-1} = p^{s-1}(p - 1) \geq p^{s-1} \geq s$. The last inequality is true for all natural numbers $p \geq 2$ and $s \geq 1$. For $s = 1$ the rings $\mathbb{Z}/p\mathbb{Z}$ are special finite fields. Observe that Corollary 2.6 and Corollary 2.7 make for this special case the same statements. □

3 Disjunction

Theorem 3.1 *Let R be a finite commutative ring with 1. The binary relation $x = 0 \vee y = 0$ is diophantine in R if and only if R is irreducible.*

Proof: Suppose that $\exists\, \vec{\lambda}\ P(x, y, \vec{\lambda}) = 0$ is a diophantine definition for the relation $x = 0 \vee y = 0$ and that $e, 1 - e \in R$ are non-trivial idempotents. So there are $\vec{\lambda}, \vec{\lambda}' \in R$ such that:

$$P(0, 1 - e, \vec{\lambda}) = 0, \quad P(e, 0, \vec{\lambda}') = 0.$$

Multiplying with the respective idempotent we get:

$$(1-e)P(0,1-e,(1-e)\vec{\lambda}) = 0, \quad eP(e,0,e\vec{\lambda}') = 0.$$

Because $e(1-e) = 0$, it must be also true that:

$$(1-e)P(e,1-e,(1-e)\vec{\lambda}) = 0, \quad eP(e,1-e,e\vec{\lambda}') = 0.$$

Now we take $\lambda_i'' := (1-e)\lambda_i + e\lambda_i'$ for all i. Then:

$$P(e,1-e,\vec{\lambda}'') = (1-e)P(e,1-e,(1-e)\vec{\lambda}) + eP(e,1-e,e\vec{\lambda}') = 0+0 = 0,$$

but both $e, 1-e \neq 0$. This is a contradiction, so R must be irreducible.

On the other hand, if R is irreducible and $k > 0$ is given by Lemma 2.5, then the formula:

$$\exists\, \lambda \;\; (1-\lambda^k)x + \lambda^k y = 0$$

defines $x = 0 \vee y = 0$. □

Corollary 3.2 *The relation $x = 0 \vee y = 0$ is diophantine over $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a prime-power.*

Example:

$$\mathbb{Z}/8\mathbb{Z} \models \quad x = 0 \vee y = 0 \Leftrightarrow \exists\, \lambda \;\; (1-\lambda^4)x + \lambda^4 y = 0.$$

4 Negation

Theorem 4.1 *Let R be a finite commutative ring with 1. The unary relation $t \neq 0$ is diophantine in R if and only if R is irreducible.*

Proof: Suppose that $\exists\, \vec{\lambda}\; P(t,\vec{\lambda}) = 0$ is a diophantine definition for the relation $t \neq 0$ and that $e, 1-e \in R$ are non-trivial idempotents. So there are $\vec{\lambda}, \vec{\lambda}' \in R$ such that:

$$P(e,\vec{\lambda}) = 0, \quad P(1-e,\vec{\lambda}') = 0.$$

Multiplying with the respectively complementary idempotent we get:

$$(1-e)P(0,(1-e)\vec{\lambda}) = 0, \quad eP(0,e\vec{\lambda}') = 0.$$

Now we already take $\lambda_i'' := (1-e)\lambda_i + e\lambda_i'$ for all i. Then:

$$P(0,\vec{\lambda}'') = (1-e)P(0,(1-e)\vec{\lambda}) + eP(0,e\vec{\lambda}') = 0+0 = 0,$$

so we get $0 \neq 0$, which is a contradiction. Thus R must be irreducible.

On the other hand, if R is finite and irreducible then we can list the set $R \setminus \{0\}$ like $a_1, \ldots, a_{r-1}$ and then observe that:

$$x \neq 0 \;\Leftrightarrow\; x = a_1 \vee \ldots \vee x = a_{r-1}.$$

Now we apply the Theorem 3.1 finitely many times in order to get an equivalent formula which is diophantine. □

Corollary 4.2 *The relation $t \neq 0$ is diophantine over $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a prime-power.*

Remark 4.3 *If $n = p^s$, the relation $t \neq 0$ is over $\mathbb{Z}/n\mathbb{Z}$ equivalent with:*

$$\exists\, \vec{\lambda} \;\; \sum_{i=1}^{p^s-2} \lambda_i^{p^s-p^{s-1}} + t + 1 = 0.$$

Example:

$$\mathbb{Z}/4\mathbb{Z} \models \quad t \neq 0 \Leftrightarrow \exists\, \lambda, \mu \;\; \lambda^2 + \mu^2 + t + 1 = 0.$$

5 Conjunction

The case of conjunction is quite different from disjunction and negation. It leads to a class of rings which is heuristically "orthogonal" to the class of irreducible rings.

Theorem 5.1 *Let R be a finite commutative ring with 1. The binary relation $x = 0 \wedge y = 0$ is diophantine over R if and only if R is a product of not necessarily different finite fields.*

Remark: If the relation $x = 0 \wedge y = 0$ has a diophantine definition over some ring, then it has also a quantifier-free diophantine definition. Indeed, if $\exists \vec{\lambda}\ P(x, y, \vec{\lambda}) = 0$ is a diophantine definition, and $\vec{\lambda}_0 \in R$ are elements so that $P(0, 0, \vec{\lambda}_0) = 0$, then we define $Q(x, y) := P(x, y, \vec{\lambda}_0)$. So $Q \in R[x, y]$ and $x = 0 \wedge y = 0$ if and only if $Q(x, y) = 0$.

The following Lemma reduces the problem to the case of irreducible rings:

Lemma 5.2 *Let R be a finite commutative ring with 1 and $R_1 \times \cdots \times R_n$ the decomposition of R in irreducible factors. Then the relation $x = 0 \wedge y = 0$ is diophantine over R if and only if similar relations $x = 0 \wedge y = 0$ are diophantine over every irreducible factor R_i.*

Proof: We identify R with $R_1 \times \cdots \times R_n$ and for each i we consider the canonical projection $\pi_i : R \to R_i$. If Q defines $(0, 0)$ over R in the form $Q(x, y) = 0$, then $\pi_i(Q)$ similarly defines $(0, 0)$ in R_i. On the other side, if for all i the two-variable polynomial $Q_i \in R_i[x, y]$ defines $(0, 0)$ in R_i, then there is a unique pull-back $Q \in R[x, y]$ such that $\pi_i(Q) = Q_i$ that defines $(0, 0)$ in R. If the coefficient of $x^a y^b$ in Q_i is c^i_{ab}, then the coefficient of $x^a y^b$ in Q is $(c^1_{ab}, \ldots, c^n_{ab})$. Only finitely many monomials have coefficients which are not $\vec{0}$. □

The following fact ends the proof of Theorem 5.1.

Lemma 5.3 *An irreducible finite commutative ring R with 1 admits a diophantine definition of $x = 0 \wedge y = 0$ if and only if R is a finite field.*

Proof: Let R be an irreducible finite commutative ring and $Q \in R[x, y]$ a polynomial such that $Q(x, y) = 0$ if and only if $x = y = 0$. Assume that R is not a finite field, or equivalently that the maximal ideal $\mathfrak{m} \neq 0$. We write $Q(x, y) = S(x, y) + ax + by$, where all monomials in S have degree ≥ 2.

If $b = 0$, we take an $y \in \mathfrak{m}$ such that $y \neq 0$ but $y^2 = 0$ and see that $Q(0, y) = S(0, y) = 0$, which is a contradiction. Now, if $b \in \mathfrak{m} \setminus \{0\}$ then we choose an $n \in \mathbb{N}$ such that $b^{n-1} \neq 0$ but $b^n = 0$. Then $Q(0, b^{n-1}) = S(0, b^{n-1}) + b^n = 0$. This can be done independently for a.

So such a definition is possible only if $a, b \in R \setminus \mathfrak{m}$. Now, if a and b are units, the polynomial $Q(a^{-1}x, b^{-1}y)$ defines $(0, 0)$ if and only if $Q(x, y)$ does it. Thus we may assume:

$$Q(x, y) = S(x, y) + x + y.$$

Take again $x \in \mathfrak{m} \setminus \{0\}$ with $x^2 = 0$. Then $Q(x, -x) = 0$. Contradiction.

On the other side, if R is a finite field, there is a non-constant polynomial $f \in R[u]$ such that $0 \notin f(R)$. (Recall that all functions $F : R \to R$ are in this case polynomial.) Let $\tilde{f}$ be $y^{\deg(f)} f(x/y)$. Then $\tilde{f}(x, y) = 0$ only for $x = y = 0$. □

Corollary 5.4 *The relation $x = 0 \wedge y = 0$ is diophantine over $\mathbb{Z}/n\mathbb{Z}$ if and only if n is square-free.*

Example:

$$\mathbb{Z}/6\mathbb{Z} \models \quad x = 0 \wedge y = 0 \Leftrightarrow (x - y)^2 = xy.$$

Proof of the Corollary: If $a, b \geq 2$ and $\gcd(a,b) = 1$ then $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Let $n = p_1^{s_1} \dots p_l^{s_l}$ be the decomposition of n as a product of primes. We get the isomorphism:

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{s_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_l^{s_l}\mathbb{Z}.$$

According to Corollary 2.7 all these rings are irreducible, so we have just written down the unique representation of $\mathbb{Z}/n\mathbb{Z}$ as a product of irreducible rings. Now, if n is square-free then all the powers $s_1 = \dots = s_l = 1$ and $\mathbb{Z}/n\mathbb{Z}$ is a product of fields. Conversely, if $\mathbb{Z}/n\mathbb{Z}$ is a product of fields then we get that all $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ must be fields because all fields are irreducible rings according to Corollary 2.6. But this is true if and only if all $s_i = 1$. □

As we observe, the rings $\mathbb{Z}/n\mathbb{Z}$ that admit a diophantine definition for $x = 0 \wedge y = 0$ are product of necessarily different finite fields. This is not true in general. See for example $\mathbb{F}_2 \times \mathbb{F}_2$, where the relation is defined by $x + y + xy = 0$.

6 Kronecker's Symbol and the Finite Fields

Definition: Let R be a finite commutative ring with 1. We call Kronecker's Symbol over R the function $\delta : R^2 \to R$ given by:

$$\delta_{xy} := \begin{cases} 0 & \text{if } x \neq y, \\ 1 & \text{if } x = y. \end{cases}$$

Theorem 6.1 *Let R be a finite commutative ring with 1. Kronecker's Symbol $\delta_{xy} = z$ is diophantine over R if and only if R is a finite field.*

Proof: Indeed, if $R = \mathbb{F}_q$ is the field with q elements then $\delta_{xy} = z$ is given by $z + (x-y)^{q-1} = 1$ because the multiplicative group $\mathbb{F}_q \setminus 0$ is a cyclic group of order $q - 1$.

Now let R be a commutative ring with 1 and let $P \in R[x, y, z, \vec{\lambda}]$ be a polynomial giving a definition of $\delta_{xy} = z$. Let $Q(u, z, \vec{\lambda})$ be $P(0, u, z, \vec{\lambda})$. It follows:

$$u \neq 0 \;\Leftrightarrow\; \exists \vec{\lambda} \;\; Q(u, 0, \vec{\lambda}) = 0.$$

This means that the relation $u \neq 0$ is diophantine in R, hence R is irreducible according to the Theorem 4.1. Take now $S(u, z, \vec{\lambda}) := Q(u, 1 - z, \vec{\lambda})$. Then:

$$\exists \vec{\lambda} \;\; S(u, z, \vec{\lambda}) = 0 \;\Leftrightarrow\; (u = 0 \wedge z = 0) \;\vee\; (u \neq 0 \wedge z = 1).$$

Let $k \in \mathbb{N}$ be given by Lemma 2.5. We define the relation:

$$\mathcal{R}(x, y) \;:\Leftrightarrow\; \exists \vec{\lambda} \;\; S(x^k y - x - y,\, y^k - y,\, \vec{\lambda}) = 0.$$

If $\mathcal{R}(x, y)$ is true, then $y^k - y \in \{0, 1\}$. The equation $y^k - y = 1$ hasn't any solution in R :$y \in \mathfrak{m} \Rightarrow y = -1$ and y unit $\Rightarrow y = 0$. Hence $y^k - y = 0$ must be true and $y \in \{0, 1\}$. Because of the properties of S, $x^k y - x - y = 0$ must hold. If $y = 1$ we get again the impossible equation $x^k - x = 1$, so $y = 0$ and $x = 0$. Thus the relation $x = 0 \wedge y = 0$ has also a diophantine definition over R irreducible, hence R must be a finite field according to Lemma 5.3. □

Corollary 6.2 *Kronecker's Symbol $\delta_{xy} = z$ is diophantine in $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a prime.*

Since an irreducible product of fields is a field, Theorems 3.1, 4.1, 5.1 and 6.1 give the following characterization of finite fields:

Corollary 6.3 *Let R be a finite commutative ring with* 1*. The following statements are equivalent:*

(1) $x = 0 \vee y = 0$ and $x = 0 \wedge y = 0$ are diophantine over R.

(2) $t \neq 0$ and $x = 0 \wedge y = 0$ are diophantine over R.

(3) Kronecker's Symbol is diophantine over R.

(4) Every existentially definable relation is diophantine over R. In other words, every existentially definable relation is a projection of a basic algebraic set.

(5) R is a finite field.

7 Quantifier-free Diophantine Definitions

The following statements do not only give another characterization of finite fields, but also stress a situation where disjunction and negation behave differently.

We recall that according to the Definition given in the Introduction some relation $\mathcal{R}$ of arity k has a quantifier-free diophantine definition over a ring R if and only if $\mathcal{R}$ is an **algebraic** subset of R^k and can be defined over R^k using **only one** equation $Q(x_1, \ldots, x_k) = 0$, where Q is a polynomial in $R[x_1, \ldots, x_k]$. According to the geometric language already used in Corollary 6.3, $\mathcal{R}$ is a basic algebraic set.

Theorem 7.1 *Let R be a finite commutative ring with* 1*.*

- *R admits a quantifier-free diophantine definition for $x = 0 \vee y = 0$ if and only if R is a finite field.*
- *R admits a quantifier-free diophantine definition for $x = 0 \wedge y = 0$ if and only if R is a product of finite fields.*

Proof: If R is a finite field, then R is a domain and $x = 0 \vee y = 0$ is trivially equivalent with $xy = 0$. Conversely, R must be irreducible according to Theorem 3.1. Let $Q \in R[x, y]$ be a polynomial such that $x = 0 \vee y = 0$ is equivalent with $Q(x, y) = 0$. Because $Q(0, 0) = 0$, we can write $Q(x, y)$ in the form $xyP(x, y) + xX(x) + yY(y)$. Setting $(0, y)$ and $(x, 0)$ we observe that $xX(x)$ and $yY(y)$ must be identically 0, hence $Q(x, y) = xyP(x, y)$. If the maximal ideal $\mathfrak{m} \neq 0$, there must be an $a \in \mathfrak{m} \setminus \{0\}$ with $a^2 = 0$. It follows $Q(a, a) = 0$, which is a contradiction. Thus $\mathfrak{m} = 0$ and R is a field.

The statement about conjunction has already been proven in Section 5. □

What about the relation $t \neq 0$? We observe that the following holds:

$$\mathbb{Z}/4\mathbb{Z} \models \quad t \neq 0 \Leftrightarrow t^3 + 2t^2 - t + 2 = 0,$$

but $\mathbb{Z}/4\mathbb{Z}$ is not a field. Consider also the ring:

$$\mathbb{F}_2[a] := \{0,\, a,\, 1,\, 1 + a\},$$

defined as the quotient of the polynomial ring $\mathbb{F}_2[X]$ modulo the ideal (X^2). $\mathbb{F}_2[a]$ models $a^2 = 0$. $\mathbb{F}_2[a]$ is not a domain, but is an irreducible finite commutative ring because there is no idempotent inside. The maximal ideal is $\mathfrak{m} = (a) = \{0, a\}$ and the units are $\{1, 1 + a\}$ because $(1 + a)^2 = 1$. $\mathbb{F}_2[a]$ is not isomorphic with $\mathbb{Z}/4\mathbb{Z}$ because its additive group is the four-element group of Klein. One has:

$$\mathbb{F}_2[a] \models \quad t \neq 0 \Leftrightarrow t^3 + at^2 + t + a = 0.$$

Theorem 7.2 *Let R be a finite commutative ring with* 1*. The relation $x \neq 0$ has a quantifier-free diophantine definition $f(x) = 0$ for some $f \in R[x]$ if and only if R is one of the following rings:*

- *An arbitrary finite field $\mathbb{F}_q$. In this case $f(x) = x^{q-1} - 1$.*
- *The ring $\mathbb{Z}/4\mathbb{Z}$. In this case $f(x) = x^3 + 2x^2 - x + 2$.*
- *The ring $\mathbb{F}_2[a]$ with $a \neq 0$ but $a^2 = 0$. In this case $f(x) = x^3 + ax^2 + x + a$.*

Proof: Since for all finite fields the statement is evident, let us suppose that R is not a field. According to Theorem 4.1 R must be a finite irreducible commutative ring. Let $\mathfrak{m} \neq 0$ be its unique maximal ideal. We write $f(x) = x^2 g(x) + bx + a$ and observe that $a = f(0) \neq 0$. If $a \in R \setminus \mathfrak{m}$, we choose an $x \in \mathfrak{m} \setminus \{0\}$ and get the contradiction $a \in \mathfrak{m}$. Thus $a \in \mathfrak{m} \setminus \{0\}$.

Now, if $b = 0$, we choose an $x \neq 0$ in $\mathfrak{m}$ with $x^2 = 0$ and get the contradiction $a = 0$. If $b \in \mathfrak{m}$ is not 0, we find an $n > 1$ such that $b^{n-1} \neq 0$ and $b^n = 0$. Again $f(b^{n-1}) = a$, contradiction. So b must be a unit. The polynomial $f(-b^{-1}x)$ defines also $R \setminus \{0\}$ if f does, thus we consider that f has the form $x^2 g(x) - x + a$.

For all $a \in \mathfrak{m}$ there is also an $n > 1$ with $a^{n-1} \neq 0$ and $a^n = 0$. We get $f(a^{n-1}) = -a^{n-1} + a = 0$, hence $a = a^{n-1}$. We multiply with a and get $a^2 = 0$.

By substituting again x with $-x$ in f we may assume that $f(x)$ has the form $x^2 g(x) + x + a$. This implies that $f(a) = a + a = 0$, thus $2a = 0$.

Let $b \neq 0$ be another element of $\mathfrak{m}$ with $b^2 = 0$. Then $f(b) = b + a = 0$, thus $b = a$. We have proved that a is the only one element $x \neq 0$ such that $x^2 = 0$.

Let $x \in R$ be an arbitrary element. Because $(ax)^2 = 0$, ax must be 0 or a.

Take some $x \in \mathfrak{m}$. If $ax = a$, then $a(1 + x) = 0$. But $1 + x$ is a unit, so one has $a = 0$, which is a contradiction. Thus $a\mathfrak{m} = 0$.

Similarly, if x is a unit then ax cannot be 0. So $a(R \setminus \mathfrak{m}) = a$.

Now look again at the elements $y \in \mathfrak{m}$. We know that the sequence y, y^2, y^3, ... is ultimately 0, so there is a biggest $k > 0$ with $y^k \neq 0$ and $(y^k)^2 = 0$. But a is the only one element with $a^2 = 0$. We see that for all $y \in \mathfrak{m} \setminus \{0, a\}$ there is a $k > 0$ such that $y^k = a$.

Now we assume that $\mathfrak{m} \neq \{0, a\}$ and fix an element $y \in \mathfrak{m} \setminus \{0, a\}$. We choose $k \geq 2$ **minimal** such that $y^k = a$. We observe that $k \geq 2$ is equivalent with $2k - 2 \geq k$. Compute the value of:

$$f(y^{k-1}) = y^{2k-2} g(y) + y^{k-1} + a = 0.$$

If $k = 2$ then $2k - 2 = 2$ and we get $ag(y) + y + a = 0$. If $g(y) \in \mathfrak{m}$ then $ag(y) = 0$ and $y = a$, in contradiction with the assumption $y \neq a$. If $g(y) \in R \setminus \mathfrak{m}$ then $ag(y) = a$ and it follows $a + y + a = 0$, so $y = 0$, which is a new contradiction.

If $k > 2$ then $2k - 2 > k$ and $y^{2k-2} g(y) = a y^{k-2} g(y) \in a\mathfrak{m} g(y) = \{0\}$. So we get $y^{k-1} + a = 0$ and $y^{k-1} = a$, in contradiction with the fact that $k \geq 2$ has been chosen minimal with the property $y^k = a$.

Therefore $\mathfrak{m} = \{0, a\}$. Now we consider the finite field $R/\mathfrak{m}$. If its characteristic is different from two, then $1 + 1 \in R \setminus \mathfrak{m}$ and we have:

$$0 = a + a = a(1 + 1) = a,$$

and $\mathfrak{m} = \{0\}$. In this case R must be a field and this is a contradiction.

Thus $R/\mathfrak{m}$ is a field of characteristic 2, so $R/\mathfrak{m} = \mathbb{F}_{2^s}$ for some s. If $R/\mathfrak{m}$ has more than two elements, then there are $u, v \in R/\mathfrak{m}$ such that all u, v, $u + v$ are different from 0. If $\tilde{u}$, $\tilde{v}$ in R are respectively pull-backs, all $\tilde{u}$, $\tilde{v}$, $\tilde{u} + \tilde{v}$ belong to $R \setminus \mathfrak{m}$. This means:

$$0 = a + a = a\tilde{u} + a\tilde{v} = a(\tilde{u} + \tilde{v}) = a,$$

which is the same contradiction like before.

So we have seen that $R/\mathfrak{m} = \mathbb{F}_2$ and $|\, R\,| = 4$. The elements $\{0, 1, a, 1+a\}$ must belong to R and must be pairwise different.

If $1 + 1 = 0$ then the additive group of R is isomorphic with Klein's four-element group and R turns out to be $\mathbb{F}_2[a]$ with $a \neq 0$ and $a^2 = 0$.

If $1 + 1 = a$ then $1 + (1 + a) = 0$ and the additive group of R is cyclic. In this case R is $\mathbb{Z}/4\mathbb{Z}$. $\square$

In the proof of Theorem 3.1 we have got a diophantine formula for $x = 0 \vee y = 0$ holding over irreducible rings and containing just one existential quantifier. Theorem 7.1 implies that if the ring is not a field, there will be no definition without quantifiers. Thus, the formula got in the proof of Theorem 3.1 is in a sense the best possible. We know also that for irreducible rings different from the rings listed in Theorem 7.2 we need quantifiers in order to give diophantine definitions for $t \neq 0$ but we cannot say anything about their minimal number.

Acknowledgments: The first version of the present paper appeared in form of an Appendix in author's Ph. D. Thesis [3]. In this Appendix only the rings $\mathbb{Z}/n\mathbb{Z}$ were considered and our Corollaries were called there Theorems. The author thanks his advisor, Prof. Dr. Alexander Prestel, the German D.A.A.D. and the University of Konstanz for all support. The author had many interesting discussions on this subject with Michael Nuesken, Jochen Koenigsmann, Martin Ziegler, Serban Basarab, and Maxim Vserminov. The e-mail correspondence with Bruno Szabo was a permanent encouragement for the author. Last but not least, the anonymous referee worked a lot to improve the language and readability of this paper.

References

[1] **David Eisenbud**: *Commutative Algebra with a view toward Algebraic Geometry.* Springer Verlag 1995.

[2] **Yuri Matiyasevich**: *Hilbert's Tenth Problem.* The MIT Press, London, 1993.

[3] **Mihai Prunescu**: *A structural approach to diophantine definability.* Konstanzer Dissertationen 564, Hartung-Gorre Verlag, Konstanz 1999.

[4] **Mihai Prunescu**: *Defining constant polynomials.* In "Hilbert's Tenth Problem - Relations with arithmetic and algebraic geometry", Contemporary Mathematics, 270, 2000, 139 - 145.