Invent. math. 170, 655–670 (2007)
DOI: 10.1007/s00222-007-0078-6

Inventiones
mathematicae

Recursively enumerable sets of polynomials over a finite field are Diophantine

Jeroen Demeyer[⋆]

Ghent University, Department of Pure Mathematics and Computer Algebra, Galglaan 2, 9000 Gent, Belgium (e-mail: `jdemeyer@cage.ugent.be`)

Oblatum 14-VIII-2006 & 16-VIII-2007
Published online: 2 September 2007 – © Springer-Verlag 2007

Abstract We construct a Diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$. Using this together with a previous result that every recursively enumerable (r.e.) relation over $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[W, Z]$, we will prove that every r.e. relation over $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[Z]$. We will also look at recursive infinite base fields $\mathbb{F}$, algebraic over $\mathbb{F}_p$. It turns out that the Diophantine relations over $\mathbb{F}[Z]$ are exactly the relations which are r.e. for every recursive presentation.

1 Introduction

In a previous paper, *Recursively enumerable sets of polynomials over a finite field* [2], we proved that every recursively enumerable (r.e.) relation over $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[W, Z]$. In other words, if we take an r.e. subset of $\mathbb{F}_q[W, Z]^k$ (for some $k \geq 1$) such that no element involves W, then that set will be Diophantine.

In Sects. 2–4, we will construct a Diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$. Putting this interpretation together with [2], we will prove in Sect. 5 that every r.e. subset of $\mathbb{F}_q[Z]^k$ is Diophantine over $\mathbb{F}_q[Z]$. In Sect. 6, we have a look at what happens for $\mathbb{F}[Z]$, where $\mathbb{F}$ is a recursive *infinite* algebraic extension of $\mathbb{F}_q$. Then we have to consider sets $\mathcal{S} \subseteq \mathbb{F}[Z]^k$ which are r.e. for every recursive presentation. These are exactly the sets $\mathcal{S}$ which are r.e. for some recursive presentation and invariant under some Frobenius automorphism.

These results are analogous to the well-known theorem by M. Davis, H. Putnam, J. Robinson and Y. Matiyasevich (see [5] or [1]), stating that every r.e. relation over $\mathbb{Z}$ is Diophantine (over $\mathbb{Z}$). From this followed the

[⋆] The author has a Ph.D. fellowship of the Research Foundation–Flanders (FWO).

negative answer to Hilbert's Tenth Problem, saying that Diophantine equations over $\mathbb{Z}$ are undecidable. We refer to this theorem as DPRM and will often use it to prove that certain formulas are Diophantine.

For rings $\mathcal{R}[Z]$, with $\mathcal{R}$ any integral domain of characteristic $p > 0$, undecidability has been known since J. Denef's 1979 paper [3]. However, nothing was known about r.e. relations being Diophantine.

We assume the reader knows the concepts of Diophantine sets and recursively enumerable sets. We refer to the introductory texts [7] and [6]. We also need some basic recursion theory (especially in Sect. 6); for this we refer to [4] or [8].

We recall the definition of a Diophantine interpretation, since it plays an important role in this paper. The idea is to encode elements of one ring $\mathcal{Z}$ in an other ring $\mathcal{R}$.

Definition 1. Let $\mathcal{R}$ and $\mathcal{Z}$ be rings. Then a *Diophantine interpretation* of $\mathcal{Z}$ over $\mathcal{R}$ consists of a set $\mathcal{M} \subseteq \mathcal{R}^r$ for some $r \geq 1$, an equivalence relation $\sim$ on $\mathcal{M}$ and a bijection $\tau : \mathcal{Z} \xrightarrow{\sim} \mathcal{M}/{\sim}$ such that

1. The set $\mathcal{M}$ is Diophantine.
2. The relation $\sim$ is Diophantine, i.e. the set $\{(X, Y) \in \mathcal{M} \times \mathcal{M} \mid X \sim Y\}$ is Diophantine.
3. The set $\mathcal{G}_+ = \{(X, Y, Z) \in \mathcal{M}^3 \mid \tau^{-1}(X) + \tau^{-1}(Y) = \tau^{-1}(Z)\}$ is Diophantine.
4. The set $\mathcal{G}_\times = \{(X, Y, Z) \in \mathcal{M}^3 \mid \tau^{-1}(X)\tau^{-1}(Y) = \tau^{-1}(Z)\}$ is Diophantine.

If the equivalence relation is simply equality, this is called a *Diophantine model*.

Let $\mathcal{R}$ be an integral domain of characteristic $p > 0$. In [2], we defined a Diophantine model of $\mathbb{N} = \{0, 1, 2, \dots\}$ over $\mathcal{R}[Z]$, with $n \in \mathbb{N}$ corresponding to $Z^n \in \mathcal{R}[Z]$. This was done using Chebyshev polynomials, which are (up to sign) the solutions X, Y of the Pell equation $X^2 - (Z^2 - 1)Y^2 = 1$. We also had a way to define powers of arbitrary elements: "$A = B^n$" is Diophantine as a ternary relation between $A, B \in \mathcal{R}[Z]$ and $n \in \mathbb{N}$. Of course, we have to use our model of $\mathbb{N}$ to represent the power n, so "$A = B^n$" is actually a relation between $A, B, Z^n \in \mathcal{R}[Z]$. Even though all this was written down in [2] for $\mathcal{R} = \mathbb{F}_q[W]$, it works unaltered for other $\mathcal{R}$. This is because the model is strongly based on [3], which works for any integral domain of positive characteristic.

We will use the notational convention that lowercase Latin letters (a, b, $c, \dots$) stand for natural numbers, uppercase Latin letters (A, B, $C, \dots$) for polynomials, and lowercase Greek letters (α, β, $\gamma, \dots$) for elements of the base field $\mathbb{F}_q$ or $\mathbb{F}$. So, if we just write "$(\exists n)$", we really mean "$(\exists n \in \mathbb{N})$".

The Diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$ will be in the language $\mathcal{L}_Z = \{+, \cdot, 0, 1, Z\}$; we do not need any constants from $\mathbb{F}_q$ for this.

However, we will need more constant symbols when giving a Diophantine definition of certain r.e. sets.

Acknowledgements. The author would like to thank Jan Van Geel for reading this paper many times, pointing out mistakes and making plenty of good suggestions.

2 Degree

We will start with the case of finite fields in Sects. 2–5. Before we can construct the Diophantine interpretation, we need some tools.

One of these tools is a Diophantine definition of the degree of a polynomial in $\mathbb{F}_q[Z]$. For this, we will have to work in the field of rational functions $\mathbb{F}_q(Z)$. Since $\mathbb{F}_q[Z]$ admits a Diophantine definition of the set of non-zero elements (see [11, Theorem 4.2]), there exists a Diophantine interpretation of $\mathbb{F}_q(Z)$ over $\mathbb{F}_q[Z]$. This is because any element of $\mathbb{F}_q(Z)$ can be written as P/Q, where $P, Q \in \mathbb{F}_q[Z]$ and $Q \neq 0$. Conversely, P/Q represents an element of $\mathbb{F}_q(Z)$ whenever $Q \neq 0$. There is an equivalence relation $P/Q \sim R/S \leftrightarrow PS = QR$. The equivalence, the addition and multiplication of such fractions are given by simple formulas, which are clearly Diophantine.

In $\mathbb{F}_q(Z)$, "negative degree" defines a discrete valuation v_∞, as follows: $v_\infty(P/Q) = \deg Q - \deg P$. It is well known (see [10] or [11]) that all discrete valuation rings in $\mathbb{F}_q(Z)$ are Diophantine. This means that we can express "$v_\infty(P/Q) \geq 0$" with a Diophantine formula. Then

$$\deg P = \deg Q \iff v_\infty(P/Q) \geq 0 \wedge v_\infty(Q/P) \geq 0.$$

Using our encoding of $\mathbb{N}$, where n is represented by Z^n, the degree function is Diophantine:

$$\deg P = n \iff \deg P = \deg Z^n.$$

3 Stride polynomials

The second tool is what I call *stride polynomials*:

Definition 2. For integers $0 \leq w \leq s$, define the set $\mathcal{S}_{w,s}$ of (w, s)-*stride polynomials* over $\mathbb{F}_q$ as the $\mathbb{F}_q[Z^s]$-submodule of $\mathbb{F}_q[Z]$ with basis $\{1, Z, Z^2, \dots, Z^{w-1}\}$ (if $w = 0$, then $\mathcal{S}_{0,s} = \{0\}$.) Therefore, a general element of $\mathcal{S}_{w,s}$ has the following form:

$$\sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j} \quad \text{(for a certain } d \in \mathbb{N}, \text{ all } \alpha_{ij} \text{ in } \mathbb{F}_q).$$

Next, we define the set containing all stride polynomials where s is a power of q (this includes the case $s = 1$):

$$\mathcal{M} = \left\{(F, w, s) \in \mathbb{F}_q[Z] \times \mathbb{N} \times \mathbb{N} \middle| w \leq s = q^k \text{ for some } k \text{ and } F \in \mathcal{S}_{w,s}\right\}. \tag{1}$$

If we encode a natural number n as Z^n, then $\mathcal{M}$ becomes a subset of $\mathbb{F}_q[Z]^3$. To prove that $\mathcal{M}$ is Diophantine as subset of $\mathbb{F}_q[Z]^3$, we need the following auxiliary set:

$$\begin{aligned}\mathcal{N} = \Big\{(G, F, w, s, d) \in \mathbb{F}_q[Z]^2 \times \mathbb{N}^3 \Big| & w \leq s = q^k \text{ for some } k, d \geq 2, \\ & \deg G < wd \text{ and } F \text{ is the remainder of } G^s \\ & \text{after Euclidean division by } Z^{sd} - Z\Big\}.\end{aligned} \tag{2}$$

We also need two lemmas:

Lemma 3. *Let w, s and d be natural numbers such that $w \leq s$ with s a power of q and $d \geq 2$. Let*

$$G = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{i+dj} \quad \text{and} \quad F = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j}, \tag{3}$$

where the coefficients α_{ij} are in $\mathbb{F}_q$. Then $(G, F, w, s, d) \in \mathcal{N}$ and every element of $\mathcal{N}$ is of this form.

Proof. Let G, F, w, s and d be as in the statement of the lemma. We see that $\deg G \leq (d-1) + d(w-1) < wd$. Using the fact that s is a power of q, we find

$$G^s = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+sdj} \equiv \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j} = F \pmod{Z^{sd} - Z}.$$

It follows that there exists a Q for which $G^s = (Z^{sd} - Z)Q + F$. To have a Euclidean division, the degree of F must be less than the degree of $Z^{sd} - Z$. But $\deg F \leq s(d-1) + (w-1)$, which is less than sd since $w \leq s$.

Conversely, let $(G, F, w, s, d) \in \mathcal{N}$. We have to show that G and F are of the form (3). Looking at the double sum for G in (3), we see that $i + dj$ runs over every element of $\{0, 1, 2, \ldots, wd - 1\}$. Therefore, the fact that G has degree less than wd implies that it can be written as $\sum_{i<d} \sum_{j<w} \alpha_{ij} Z^{i+dj}$. Since F is uniquely determined given G, w, s and d, it follows from the first part of this proof that F must also be as in (3). □

Lemma 4. *The projection of $\mathcal{N}$ on the second, third and fourth coordinates is exactly $\mathcal{M}$.*

Proof. Take an element (G, F, w, s, d) in $\mathcal{N}$. Because of Lemma 3, we know that F can be written as $\sum_{i<d}\sum_{j<w}\alpha_{ij}Z^{si+j}$, which is a (w, s)-stride polynomial; hence $(F, w, s) \in \mathcal{M}$.

Conversely, given $(F, w, s) \in \mathcal{M}$, we have to find G and d such that $(G, F, w, s, d) \in \mathcal{N}$. Since $F \in \mathcal{S}_{w,s}$, there exists a $d \geq 2$ such that $F = \sum_{i<d}\sum_{j<w}\alpha_{ij}Z^{si+j}$ for some $\alpha_{ij} \in \mathbb{F}_q$. Let $G = \sum_{i<d}\sum_{j<w}\alpha_{ij}Z^{i+dj}$. Lemma 3 proves that $(G, F, w, s, d) \in \mathcal{N}$. □

Now we can easily show that $\mathcal{M}$ is Diophantine:

Proposition 5. *The set $\mathcal{N}$ is a Diophantine subset of $\mathbb{F}_q[Z]^5$ and $\mathcal{M}$ is a Diophantine subset of $\mathbb{F}_q[Z]^3$ (where we encode w, s and d as Z^w, Z^s and Z^d).*

Proof. We claim that (2) yields a Diophantine definition of $\mathcal{N}$. The subformula "$w \leq s = q^k \ \wedge\ d \geq 2$" is Diophantine because of DPRM. The Diophantineness of "$\deg G < wd$" follows from Sect. 2 combined with DPRM. The Euclidean division can be written as

$$(\exists Q)(G^s = (Z^{sd} - Z)Q + F \ \wedge\ (F = 0 \ \vee\ \deg(F) < sd)).$$

Since Z^{sd} simply represents the element sd and exponentiation is Diophantine (see [2, Sect. 4.5]), this is Diophantine.

Projections of Diophantine sets are again Diophantine, so it follows from Lemma 4 that $\mathcal{M}$ is also Diophantine. □

4 The interpretation of $\mathbb{F}_q[V, W]$ over $\mathbb{F}_q[Z]$

Inside $\mathbb{F}_q[Z]$, we will now construct a Diophantine interpretation of a two-variable polynomial ring over $\mathbb{F}_q$. In the introduction, we wrote $\mathbb{F}_q[W, Z]$ for this ring, but to avoid confusion between the Z from $\mathbb{F}_q[W, Z]$ and the Z from $\mathbb{F}_q[Z]$, we write $\mathbb{F}_q[V, W]$ instead for the two-variable polynomial ring.

4.1 Construction. We will encode elements of $\mathbb{F}_q[V, W]$ as certain equivalence classes of triples (F, w, s) in $\mathcal{M}$. To explain this, we are going to construct a map $\theta : \mathcal{M} \to \mathbb{F}_q[V, W]$ giving the correspondence (this map is the inverse of the τ in Definition 1). Then two elements of $\mathcal{M}$ are equivalent (notation: $\sim$) if their images under θ are the same.

Take a triple $(F, w, s) \in \mathcal{M}$. By Definition 2 F can be written as $F = \sum_{i<d}\sum_{j<w}\alpha_{ij}Z^{si+j}$ for some $d \in \mathbb{N}$. We define $\theta(F, w, s) = \sum_{i<d}\sum_{j<w}\alpha_{ij}V^iW^j$.

Conversely, suppose we are given an $\widetilde{F} \in \mathbb{F}_q[V, W]$. Then $\theta^{-1}(\widetilde{F})$ is the set of triples $(\widetilde{F}(Z^s, Z), w, s)$ where w and s range over natural numbers such that $\deg_W(\widetilde{F}) < w \leq s = q^k$ for some k. In particular, we see that θ is surjective.

We can characterise equivalence in $\mathcal{M}$ using the set $\mathcal{N}$:

Proposition 6. *Let (F_1, w_1, s_1) and (F_2, w_2, s_2) be elements of $\mathcal{M}$. Then $(F_1, w_1, s_1) \sim (F_2, w_2, s_2)$ if and only if (G, F_1, w_1, s_1, d) and (G, F_2, w_2, s_2, d) are both in $\mathcal{N}$ for some $G \in \mathbb{F}_q[Z]$ and $d \in \mathbb{N}$.*

Proof. Assume $(F_1, w_1, s_1) \sim (F_2, w_2, s_2)$ and let $w = \min\{w_1, w_2\}$. Then for some $d \geq 2$, we have

$$F_1 = \sum_{i<d} \sum_{j<w} \alpha_{ij} Z^{s_1 i+j} \quad \text{and} \quad F_2 = \sum_{i<d} \sum_{j<w} \alpha_{ij} Z^{s_2 i+j}.$$

If we define $G = \sum_{i<d} \sum_{j<w} \alpha_{ij} Z^{i+dj}$, it follows from Lemma 3 that $(G, F_k, w, s_k, d) \in \mathcal{N}$ for $k \in \{1, 2\}$. But $w \leq w_k \leq s_k$, so we also have $(G, F_k, w_k, s_k, d) \in \mathcal{N}$.

Conversely, let (G, F_k, w_k, s_k, d) be in $\mathcal{N}$ for $k \in \{1, 2\}$. Then $\deg G < wd$ with $w = \min\{w_1, w_2\}$. If we write $G = \sum_{i<d} \sum_{j<w} \alpha_{ij} Z^{i+dj}$ as in Lemma 3, it follows from that lemma that

$$F_k = \sum_{i<d} \sum_{j<w} \alpha_{ij} Z^{s_k i+j}, \text{ so } \theta(F_k, w_k, s_k) = \sum_{i<d} \sum_{j<w} \alpha_{ij} V^i W^j$$

for $k \in \{1, 2\}$. The right hand side is independent of k, therefore $(F_1, w_1, s_1) \sim (F_2, w_2, s_2)$. □

4.2 Addition and multiplication. The set $\mathcal{M}/\sim$ gives an interpretation of $\mathbb{F}_q[V, W]$ over $\mathbb{F}_q[Z]$, but is it Diophantine? In Proposition 5 we already showed that the set $\mathcal{M}$ is Diophantine. Since $\mathcal{N}$ is Diophantine, it follows from Proposition 6 that $\sim$ is a Diophantine relation. It remains to show that addition and multiplication in the interpretation are Diophantine.

To define an operator (either addition or multiplication), we may assume that both operands have the same w and s. This follows from the following lemma:

Lemma 7. *Let $(F_1, w_1, s_1), (F_2, w_2, s_2), (F_3, w_3, s_3) \in \mathcal{M}$. Then*

$$\theta(F_1, w_1, s_1) + \theta(F_2, w_2, s_2) = \theta(F_3, w_3, s_3) \tag{4}$$

$$\Updownarrow$$

$$(\exists H_1, H_2, H_3)(\exists w, s) \tag{5}$$

$$(H_1, w, s) \in \mathcal{M} \ \wedge\ (F_1, w_1, s_1) \sim (H_1, w, s) \tag{6}$$

$$\wedge\ (H_2, w, s) \in \mathcal{M} \ \wedge\ (F_2, w_2, s_2) \sim (H_2, w, s) \tag{7}$$

$$\wedge\ (H_3, w, s) \in \mathcal{M} \ \wedge\ (F_3, w_3, s_3) \sim (H_3, w, s) \tag{8}$$

$$\wedge\ \theta(H_1, w, s) + \theta(H_2, w, s) = \theta(H_3, w, s). \tag{9}$$

Proof. The implication $\Uparrow$ is trivial, since $\theta(H_k, w, s) = \theta(F_k, w_k, s_k)$ for $k \in \{1, 2, 3\}$.

Conversely, assume (4) and pick $w \geq \max\{w_1, w_2, w_3\}$ and $s \geq \max\{s_1, s_2, s_3, w\}$ with s a power of q. Let $k \in \{1, 2, 3\}$. From Lemma 4 it follows that there exist G_k and d_k such that $(G_k, F_k, w_k, s_k, d_k) \in \mathcal{N}$. If we let H_k be the remainder of G_k^s after division by $Z^{sd_k} - Z$, then (G_k, H_k, w, s, d_k) will be in $\mathcal{N}$. Using Proposition 6, we get $(F_k, w_k, s_k) \sim (H_k, w, s)$. □

The above lemma was about addition, but exactly the same holds for multiplication. Also remark that w and s can be chosen arbitrarily large. Now we can easily give Diophantine definitions of addition and multiplication:

Proposition 8. *Let* $(F_1, w, s), (F_2, w, s) \in \mathcal{M}$.

1. *Then*

$$\theta(F_1, w, s) + \theta(F_2, w, s) = \theta(F_1 + F_2, w, s). \tag{10}$$

2. *If* $2w \leq s$ *(this can be ensured by choosing* $s \geq 2w$ *in Lemma 7), then*

$$\theta(F_1, w, s) \cdot \theta(F_2, w, s) = \theta(F_1 F_2, 2w, s). \tag{11}$$

Proof. The first item is immediate because the sets $\mathcal{S}_{w,s}$ are $\mathbb{F}_q$-linear, and the map θ is also $\mathbb{F}_q$-linear in the first argument.

For the multiplication, we rely on the fact that if $\deg_W(F_1)$ and $\deg_W(F_2)$ are both less than w, then $\deg_W(F_1 F_2)$ is less than $2w$. If we fix w and s and restrict ourselves to polynomials with W-degree small enough, then the restriction of θ acts as a "isomorphism" of rings between a subspace of $\mathbb{F}_q[Z]$ and a subspace of $\mathbb{F}_q[V, W]$. □

5 Diophantine versus recursively enumerable

Now we show how the Diophantine interpretation of $\mathbb{F}_q[V, W]$ over $\mathbb{F}_q[Z]$ can be used to prove that every recursively enumerable (r.e.) subset of $\mathbb{F}_q[Z]^k$ (with $k \geq 1$) is Diophantine over $\mathbb{F}_q[Z]$. This will be in the language $\{+, \cdot, 0, 1, \alpha, Z\}$, where α is a constant such that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, with p the characteristic of $\mathbb{F}_q$.

We first do the one-dimensional ($k = 1$) case. Consider an r.e. set $\mathcal{S} \subseteq \mathbb{F}_q[Z]$, but write it as $\mathcal{S}(Z)$ to stress that the polynomials are in the variable Z. Let $\mathcal{S}(V) \subseteq \mathbb{F}_q[V, W]$ be the set with the same polynomials, but in V instead of Z. Since $\mathcal{S}(V)$ is an r.e. subset of $\mathbb{F}_q[V]$, it follows from [2] that $\mathcal{S}(V)$ is a Diophantine subset of $\mathbb{F}_q[V, W]$.

But we have an interpretation of $\mathbb{F}_q[V, W]$ over $\mathbb{F}_q[Z]$, such that elements of $\mathbb{F}_q[V, W]$ are seen as equivalence classes in $\mathcal{M}$. We can also translate the Diophantine definition of $\mathcal{S}(V)$ to a Diophantine definition in $\mathcal{M}$ of the elements representing $\mathcal{S}(V)$. Therefore $\theta^{-1}(\mathcal{S}(V))$ is Diophantine over $\mathbb{F}_q[Z]$.

Since $\theta(F(Z), 1, 1) = F(V)$, this yields the following Diophantine definition of $\mathcal{S}(Z)$:

$$F(Z) \in \mathcal{S}(Z) \iff (F(Z), 1, 1) \in \theta^{-1}(\mathcal{S}(V)).$$

For $k = 2$, we use a Diophantine *pairing function*, that is an injection $\mathbb{F}_q[Z]^2 \hookrightarrow \mathbb{F}_q[Z]$:

$$\begin{aligned} \delta : \mathbb{F}_q[Z] \times \mathbb{F}_q[Z] &\to \mathbb{F}_q[Z] \\ (A, B) &\mapsto A^p Z + B^p. \end{aligned}$$

Now let $\mathcal{S}$ be an r.e. subset of $\mathbb{F}_q[Z]^2$. Then $\delta(\mathcal{S})$ is an r.e. subset of $\mathbb{F}_q[Z]$, hence $\delta(\mathcal{S})$ is Diophantine. But then $\mathcal{S}$ is also Diophantine because

$$(A, B) \in \mathcal{S} \iff A^p Z + B^p \in \delta(\mathcal{S}).$$

We can do larger k's inductively, by applying the above pairing function on two of the k components.

6 Infinite fields

So far, we have proven that r.e. equals Diophantine for rings $\mathbb{F}[Z]$, where $\mathbb{F}$ is a finite field. But we can do more: let p be a prime number and fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. We will look at infinite subfields $\mathbb{F}$ of $\overline{\mathbb{F}_p}$, and try to figure out whether r.e. subsets of $\mathbb{F}[Z]^k$ are Diophantine.

First of all, we only need to consider the case $k = 1$ because the argument at the end of the previous section works unaltered for the ring $\mathbb{F}[Z]$ (or any polynomial ring in characteristic p). Therefore, we only need to look at subsets of $\mathbb{F}[Z]$ in the remainder of this section.

6.1 Recursive structure. If $\mathbb{F}$ is an infinite field, some problems arise: First of all, the field $\mathbb{F}$ might not be recursive, which means it is impossible to compute in $\mathbb{F}$. Second, it is not clear how to give a meaningful definition of "recursively enumerable set".

We start by recalling the definition of a recursive presentation; for more details we refer to [4]. A *recursive presentation* of a ring $\mathcal{R}$ is a bijection $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$ such that the following sets are recursive:

$$\begin{aligned} \mathcal{R}_\theta^+ &= \{(\theta(A), \theta(B), \theta(A + B)) \in \mathbb{N}^3 \mid A, B \in \mathcal{R}\}, \\ \mathcal{R}_\theta^\times &= \{(\theta(A), \theta(B), \theta(AB)) \in \mathbb{N}^3 \mid A, B \in \mathcal{R}\}. \end{aligned}$$

$\mathcal{R}_\theta^+$ is called the *addition table*, and $\mathcal{R}_\theta^\times$ the *multiplication table* of $\mathcal{R}$.

A ring admitting a recursive presentation is called a *recursive ring*. Note that such a ring must be countable. Not every subfield of $\overline{\mathbb{F}_p}$ is recursive. This can simply be seen by considering cardinalities: there are $2^{\aleph_0}$ such subfields, but at most $\aleph_0$ of them can be recursive. The latter follows from the fact that every Turing machine has a Gödel number which is simply a natural number. So there are only countably many Turing machines, hence only countably many recursive sets. Since the field $\mathbb{F}$ is determined (up to isomorphism) by the recursive sets $\mathcal{R}_\theta^+$ and $\mathcal{R}_\theta^\times$, only countably many subfields of $\overline{\mathbb{F}_p}$ are recursive.

So we have to assume that $\mathbb{F}$ is a recursive infinite algebraic extension of $\mathbb{F}_p$. The algebraic closure satisfies this condition (see [8]).

Once we have a recursive presentation θ for a ring $\mathcal{R}$, we can define recursively enumerable sets in $\mathcal{R}$: A set $\mathcal{S} \subseteq \mathcal{R}$ is called r.e. if and only if $\theta(\mathcal{S})$ is an r.e. subset of $\mathbb{N}$. The problem with this definition is that it depends on θ.

This happens for example in infinite subfields $\mathbb{F} \subseteq \overline{\mathbb{F}_p}$, where it can be explained by looking at the automorphism group $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$. Let θ be a recursive presentation $\mathbb{F} \xrightarrow{\sim} \mathbb{N}$. It is possible to construct an r.e. set $\mathcal{S}$ (r.e. for θ), and a $\phi \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ such that $\phi(\mathcal{S})$ is *not* r.e. (for θ). Using ϕ, we twist θ to a new recursive presentation $\psi = \theta \circ \phi$. Then $\mathcal{S}$ will be r.e. for θ, but not for ψ. Obviously, we need a way to avoid this problem. First we have a look at how different recursive presentations relate to one another:

Lemma 9. *Let $\mathbb{F}$ be a recursive infinite algebraic extension of $\mathbb{F}_p$. Assume we have two recursive presentations $\sigma : \mathbb{F} \xrightarrow{\sim} \mathbb{N}$ and $\theta : \mathbb{F} \xrightarrow{\sim} \mathbb{N}$. Then there exists a recursive permutation π of $\mathbb{N}$ and an automorphism ϕ of $\mathbb{F}$ such that $\pi \circ \sigma = \theta \circ \phi$.*

$$\begin{tikzcd}
\mathbb{F} \arrow[r, dashed, "\phi\in\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)"] \arrow[d, "\sigma"] & \mathbb{F} \arrow[d, "\theta"] \\
\mathbb{N} \arrow[r, dashed, "\pi \text{ recursive}"] & \mathbb{N}
\end{tikzcd}$$

Proof. Note that the maps σ, θ, π and ϕ are all bijections. To every $\phi \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$, there corresponds a unique permutation π such that the above diagram commutes. For every such π, we look at the value vector $(\pi(0), \pi(1), \pi(2), \dots)$. We take the unique π such that this value vector is lexicographically the first. This fixes the choice of ϕ and π, but we still have to prove that this π is recursive.

We will compute π by induction. Assume that an algorithm knows the values $\pi(0), \pi(1), \dots, \pi(a-1)$ for some $a \geq 0$, and that we have to compute $\pi(a)$. Note that this algorithm knows nothing about ϕ. As extra input, the algorithm needs $\sigma(1)$ and $\pi(\sigma(1)) = \theta(1)$.

The first thing to do is to determine the finite field $\mathbb{F}_q$ generated by $\{\sigma^{-1}(0), \dots, \sigma^{-1}(a-1)\}$. For every $\sigma^{-1}(i)$, we can compute the smallest n such that $\sigma^{-1}(i)^{p^n} = \sigma^{-1}(i)$ by successively taking p-th powers. This powering is done using the multiplication table for the recursive presentation σ. We do this for all $i < a$ and let m be the l.c.m. of the n's, then $q = p^m$. The set $\sigma(\mathbb{F}_q)$ can easily be determined, it contains exactly the elements x such that $\sigma^{-1}(x)^q = \sigma^{-1}(x)$. Given $\pi(0), \dots, \pi(a-1)$, we can also compute π on all of $\sigma(\mathbb{F}_q)$, by taking algebraic combinations of the elements $\sigma^{-1}(0), \dots, \sigma^{-1}(a-1)$ and 1.

Now we will compute $\pi(a)$. Writing $\alpha = \sigma^{-1}(a)$, we can compute its minimal polynomial over $\mathbb{F}_q$:

$$P(Z) = (Z-\alpha)(Z-\alpha^q)(Z-\alpha^{q^2})\cdots(Z-\alpha^{q^{n-1}}) \qquad (\alpha^{q^n} = \alpha \text{ with } n \text{ minimal}).$$

We have to explain what it means to compute this, because an algorithm can only work with natural numbers (representing elements of $\mathbb{F}$ via a recursive presentation). So, our algorithm cannot really compute the polynomial, but only the codes of the coefficients. The minimal polynomial of α will be represented as some numbers $a_i \in \sigma(\mathbb{F}_q)$ such that $P(Z) = \sum_{i=0}^n \sigma^{-1}(a_i)Z^i$ is the actual minimal polynomial.

Since we can compute π on $\sigma(\mathbb{F}_q)$, we can compute $b_i = \pi(a_i)$. Let $b = \pi(a)$ (which we still have to compute) and $\beta = \theta^{-1}(b)$. Expanding $\phi(P(\alpha)) = 0$, and using $\pi \circ \sigma = \theta \circ \phi$, we get

$$0 = \phi\Big(\sum_{i=0}^n \sigma^{-1}(a_i)\alpha^i\Big) = \sum_{i=0}^n \phi\big(\sigma^{-1}(a_i)\big)\phi(\alpha)^i = \sum_{i=0}^n \theta^{-1}(b_i)\beta^i.$$

This gives the minimal polynomial of $\theta^{-1}(b)$. So, to find $\pi(a)$, we try all $x \in \mathbb{N}$ and compute the minimal polynomial of $\theta^{-1}(x)$ (as before, we actually compute θ of the coefficients). If we get the polynomial $\sum \theta^{-1}(b_i)Z^i$, we are done. Since we want π to be the lexicographically first amongst all possible π, we try the x's in order and take the smallest one with the correct minimal polynomial. □

Since the definition of recursively enumerable sets depends on the recursive presentation chosen, we will restrict ourselves to the sets $\mathcal{S} \subseteq \mathbb{F}$ which are r.e. for *every* recursive presentation of $\mathbb{F}$. These sets can also be characterized algebraically, using the q-Frobenius ϕ_q on $\mathbb{F}$, mapping ξ to ξ^q:

Lemma 10. *Let $\mathcal{S}$ be a subset of $\mathbb{F}$. Then $\theta(\mathcal{S})$ is r.e. for every recursive presentation θ if and only if $\mathcal{S}$ is invariant under ϕ_q for some q.*

Proof. First, we do the "if" direction, so we take two recursive presentations σ and θ. Then we take π and ϕ satisfying Lemma 9. Let $\mathcal{S}$ be r.e. for σ, this means by definition that $\sigma(\mathcal{S})$ is r.e. as a subset of $\mathbb{N}$. Since π is recursive, this implies that $\theta(\phi(\mathcal{S})) = \pi(\sigma(\mathcal{S}))$ is r.e. Now $\mathcal{S}$ is invariant under taking q-th powers, therefore $\phi(\mathcal{S}) = \phi_{p^k}(\mathcal{S})$ for a certain k. The Frobenius ϕ_{p^k} is computable and $\theta(\phi(\mathcal{S}))$ is r.e., so $\theta(\mathcal{S})$ is also r.e. This shows that $\mathcal{S}$ is also r.e. for the recursive presentation θ.

The converse can be proven using the theory of profinite groups. Consider the group $G \leq \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ which stabilizes $\mathcal{S}$, this is a closed subgroup of the profinite group $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$. The quotient $Q = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)/G$ determines the possible images of $\mathcal{S}$ under $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$. This Q is a quotient of a profinite group by a closed subgroup, so Q is also profinite (see [9, Proposition 2.2.1]).

Fix one particular recursive presentation θ. If ϕ is any automorphism of $\mathbb{F}$, then $\theta \circ \phi$ is also a recursive presentation. Since θ is a bijection, we get a different set $\theta(\phi(\mathcal{S}))$ for every $\phi \in Q$. By assumption, all sets $\theta(\phi(\mathcal{S}))$ are r.e., so Q can contain at most countably many elements. Since profinite groups cannot have exactly $\aleph_0$ elements (see [9, Proposition 2.3.1]), Q must be finite. We conclude that some power of the Frobenius $\xi \mapsto \xi^p$ must be in G. □

This whole discussion was for the field $\mathbb{F}$, but it also applies to the polynomial ring $\mathbb{F}[Z]$. In [4], it is proven that $\mathbb{F}[Z]$ is recursive whenever $\mathbb{F}$ is. We can extend the Frobenius ϕ_q to an automorphism on $\mathbb{F}[Z]$ by setting $\phi_q(Z) = Z$. In $\mathbb{F}[Z]$, we will work with r.e. subsets $\mathcal{S}$ such that there exists a q for which $\phi_q(\mathcal{S}) = \mathcal{S}$. As above, one can prove that such a set $\mathcal{S}$ will be r.e. for every recursive presentation $\mathbb{F}[Z] \xrightarrow{\sim} \mathbb{N}$. Finally, using the pairing function δ (see Sect. 5), everything also applies to cartesian powers $\mathbb{F}[Z]^k$, if we let ϕ_q act component-wise.

6.2 Some lemmas. In the previous section, we already saw that we cannot work with every r.e. set, we have to assume that our r.e. sets are invariant under a Frobenius automorphism ϕ_q. But there is another, more algebraic reason why we need this assumption: Take any Diophantine subset $\mathcal{D}$ of $\mathbb{F}[Z]$. In the polynomial used to define $\mathcal{D}$, only finitely many elements from $\mathbb{F}$ can appear. This is true even if we allow an infinite language. If $\mathbb{F}_q$ is the finite field generated by these elements of $\mathbb{F}$, then $\mathcal{D}$ will be invariant under the Frobenius ϕ_q.

The following is the main theorem of Sect. 6:

Theorem 11. *Let $\mathbb{F}$ be a recursive infinite algebraic extension of $\mathbb{F}_p$. For all $k \geq 1$, the Diophantine sets in $\mathbb{F}[Z]^k$ are exactly the recursively enumerable sets that are fixed under a Frobenius automorphism. Moreover, an r.e. set invariant under ϕ_q can be Diophantinely defined using only constants from $\mathbb{F}_q[Z]$.*

We need the following Lemma, which is a generalization of the fact that for two polynomials $F \neq G$ over an infinite field, there is a value α such that $F(\alpha) \neq G(\alpha)$. We also want that $F(\alpha) \neq G(\alpha^\sigma)^\tau$ for automorphisms σ and τ:

Lemma 12. *Let $\mathbb{F}_q$ be a finite subfield of $\mathbb{F}$. Consider a finite subset $\{P_1, \ldots, P_n\}$ of $\mathbb{F}[Z]$, such that none of the P_i is a q-th power. Then there exists an $\alpha \in \mathbb{F}$ such that the implication $P_i(\alpha) = P_j(\alpha^\sigma)^\tau \rightarrow P_i^\sigma = P_j$ holds for all $1 \leq i, j \leq n$ and $\sigma, \tau \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$.*

Proof. Without loss of generality, we may assume that if a polynomial P is amongst $\{P_1, \ldots, P_n\}$, all its conjugates P^σ also are. We can assure this by adding a finite number of polynomials to the given set.

Fix a finite subfield $\mathbb{F}_r \subset \mathbb{F}$ containing $\mathbb{F}_q$ and all the coefficients of the P_i. Note that there is a minimal r, but we can take r arbitrarily large.

In symbols, we have to prove that

$$(\exists \alpha \in \mathbb{F})(\forall i, j \leq n)(\forall \sigma, \tau \in \operatorname{Gal}(\mathbb{F}/\mathbb{F}_q))\big(P_i(\alpha) = P_j(\alpha^\sigma)^\tau \rightarrow P_i^\sigma = P_j\big).$$

We will take α in $\mathbb{F}_r$, so everything is well-defined if we see σ and τ as elements of $G = \operatorname{Gal}(\mathbb{F}_r/\mathbb{F}_q)$:

$$(\exists \alpha \in \mathbb{F}_r)(\forall i, j \leq n)(\forall \sigma, \tau \in G)\big(P_i(\alpha) = P_j(\alpha^\sigma)^\tau \rightarrow P_i^\sigma = P_j\big).$$

If we set $P_k = P_j^{\sigma^{-1}}$ and $\rho = \sigma\tau$, this becomes

$$(\exists \alpha \in \mathbb{F}_r)(\forall i, k \leq n)(\forall \rho \in G)\big(P_i(\alpha) = P_k(\alpha)^\rho \;\rightarrow\; i = k\big).$$

We want to prove this by contradiction, so we assume that

$$(\forall \alpha \in \mathbb{F}_r)(\exists i, k \leq n)(\exists \rho \in G)\big(P_i(\alpha) = P_k(\alpha)^\rho \;\wedge\; i \neq k\big). \tag{12}$$

We will use a counting argument to show that (12) is not possible if r is large enough. To every $\alpha \in \mathbb{F}_r$ there corresponds a triple (i, k, ρ) such that $P_i(\alpha) = P_k(\alpha)^\rho$ with $i \neq k$. There are at most $n \cdot n \cdot \log_q r$ such triples, by the pigeonhole principle at least $N = \left\lceil \frac{r}{n^2 \log_q r} \right\rceil$ different α's have the same (i, k, ρ). In other words, there exist certain fixed $i, k \in \mathbb{N}$ and $\rho \in \operatorname{Gal}(\mathbb{F}_r/\mathbb{F}_q)$ such that $P_i(\alpha) = P_k(\alpha)^\rho$ for at least N different values of $\alpha \in \mathbb{F}_r$.

ρ is simply raising to the power q^h, for a certain $h \in \{0, \ldots, \log_q r - 1\}$. But we may assume that $h \leq (\log_q r)/2$, because we can always apply ρ^{-1} to $P_i(\alpha) = P_k(\alpha)^\rho$ and exchange i and k. Like this, q^h is at most $\sqrt{r}$.

So, for N different values of α, the following holds:

$$P_i(\alpha) = P_k(\alpha)^{q^h}.$$

If $P_i(Z) - P_k(Z)^{q^h}$ is the zero polynomial, then either $h = 0$ and $i = k$, or $h > 0$ and P_i is a q-th power. Both these cases are excluded, so $P_i(Z) - P_k(Z)^{q^h}$ has only finitely many zeros. If d is the maximum degree of all given polynomials P_i, then $P_i(Z) - P_k(Z)^{q^h}$ has degree at most $dq^h \leq d\sqrt{r}$. But this polynomial has N different zeros; therefore

$$d\sqrt{r} \geq N \geq \frac{r}{n^2 \log_q r}.$$

Since d, n and q do not depend on r, it is possible to take r large enough to contradict this inequality. □

Definition 13. For all $u \geq 1$, define

$$\mathcal{A}_u = \{X \in \mathbb{F}[Z] \mid (X^p Z^p + Z + 1) | (Z^u - 1)\},$$
$$\mathcal{Z}_u = \{X^p Z^p + Z + 1 \in \mathbb{F}[Z] \mid (X^p Z^p + Z + 1) | (Z^u - 1)\}.$$

Lemma 14. *The sets $\mathcal{A}_u$ and $\mathcal{Z}_u$ satisfy the following properties:*

1. *For all u, $\mathcal{A}_u$ and $\mathcal{Z}_u$ are finite.*
2. *For all $X \in \mathcal{A}_u$, the degree of X is at most u.*
3. *The union of all $\mathcal{A}_u$'s is equal to $\mathbb{F}[Z]$.*

Proof. Since $\mathbb{F}[Z]$ has unique factorization, $(Z^u - 1)$ has only finitely many divisors up to units. There are infinitely many units, but for every divisor $F(Z)$ of $(Z^u - 1)$, there is exactly one unit $\varepsilon \in \mathbb{F}^*$ such that $\varepsilon F(Z) \equiv 1 \bmod Z$. Therefore, $Z^u - 1$ can have only finitely many divisors of the form $X^p Z^p + Z + 1$.

The second item follows immediately from the definition of $\mathcal{A}_u$. It is clear that this is not a very good bound, but that does not matter.

To prove the last item, take any $X \in \mathbb{F}[Z]$ and let $F(Z) = X^p Z^p + Z + 1 \in \mathcal{Z}_u$. The derivative $F'(Z) = 1$, so $F(Z)$ is a separable polynomial. Now consider the ring $\mathcal{R} = \mathbb{F}[Z]/F$. By assumption, $\gcd(F, Z) = 1$, so Z is a unit in $\mathcal{R}$. Since F is seperable, this ring is a product of fields. Each of these fields is a subfield of $\overline{\mathbb{F}_p}$, so Z has finite multiplicative order in them. This means that $Z^u \equiv 1 \mod F$ for a certain u. □

We can use this to give a Diophantine definition of $\mathbb{F}_q[Z]$ in $\mathbb{F}[Z]$. The same definition even works to define $\mathbb{F}_q[Z]$ in $\mathcal{R}[Z]$ where $\mathcal{R}$ is any integral domain of characteristic p. This is because we only need the model of $\mathbb{N}$ (and we have this model in any $\mathcal{R}[Z]$, see Introduction).

Lemma 15. *For $X \in \mathbb{F}[Z]$, the following holds:*

$$X \in \mathbb{F}_q[Z] \tag{13}$$
$$\Updownarrow$$
$$(\exists a, b, u)$$
$$X \in \mathcal{A}_u \tag{14}$$
$$\wedge\ q^a > u \ \wedge\ q^b > u \ \wedge\ \gcd(a, b) = 1 \tag{15}$$
$$\wedge\ X^{q^a} \equiv X \pmod{Z^{q^a} - Z} \tag{16}$$
$$\wedge\ X^{q^b} \equiv X \pmod{Z^{q^b} - Z}. \tag{17}$$

Proof. Assume $X \in \mathbb{F}_q[Z]$ and write $X = \sum_{i=0}^{d} \alpha_i Z^i$ with $\alpha_i \in \mathbb{F}_q$. Choose u such that (14) holds. Then choose a and b such that (15) holds.

Since $\alpha_i \in \mathbb{F}_q$, we find

$$X^{q^a} = \sum_{i=0}^{d} \alpha_i Z^{iq^a} \equiv \sum_{i=0}^{d} \alpha_i Z^i = X \pmod{Z^{q^a} - Z}.$$

Analogously, $X^{q^b} \equiv X \pmod{Z^{q^b} - Z}$.

Conversely, assume (14)–(17). From (14) it follows that $\deg X \leq u$, so we can write X as $\sum_{i=0}^{u} \alpha_i Z^i$, where $\alpha_i \in \mathbb{F}$. We want to prove that every α_i is actually in $\mathbb{F}_q$. Congruence (16) implies that

$$\sum_{i=0}^{u} \alpha_i Z^i = X \equiv X^{q^a} = \sum_{i=0}^{u} \alpha_i^{q^a} Z^{iq^a} \equiv \sum_{i=0}^{u} \alpha_i^{q^a} Z^i \pmod{Z^{q^a} - Z}.$$

The left and right hand sides of this congruence are polynomials of degree at most u, but they are congruent modulo a polynomial of degree $q^a > u$, so they are equal. This means that $\alpha_i = \alpha_i^{q^a}$; in other words, $\alpha_i \in \mathbb{F}_{q^a}$. In the same way, from (17) it follows that $\alpha_i \in \mathbb{F}_{q^b}$. Since $\gcd(a, b) = 1$, we have $\alpha_i \in \mathbb{F}_q$. □

6.3 Recursively enumerable subsets of $\mathbb{F}[Z]$**.** We now prove Theorem 11, it suffices to do the case $k = 1$. Let $\mathcal{S}$ be an r.e. subset of $\mathbb{F}[Z]$, and let q be a power of p such that $\phi_q(\mathcal{S}) = \mathcal{S}$. We want to find a Diophantine definition of the set $\mathcal{S}$, using only constants from $\mathbb{F}_q[Z]$.

Given $\mathcal{S}$, we construct a set $\mathcal{P}_1 \subseteq \mathbb{N} \times \mathbb{F} \times \mathbb{F}$ which will encode the elements of $\mathcal{S}$. For an $F \in \mathcal{S}$, the following procedure gives a triple $(u, \alpha, \beta) \in \mathbb{N} \times \mathbb{F} \times \mathbb{F}$ corresponding to F:

- u is the smallest number for which $F \in \mathcal{A}_u$ (see Definition 13). This means that $G = F^p Z^p + Z + 1 \in \mathcal{Z}_u$.
- α comes from Lemma 12 applied to the elements of $\mathcal{Z}_u$. This α is not uniquely defined, but we can do the following: $\mathbb{F}$ is a recursive field, so it is given with a recursive presentation $\theta : \mathbb{F} \xrightarrow{\sim} \mathbb{N}$. We simply try all numbers in $\mathbb{N}$ and check whether the corresponding $\alpha \in \mathbb{F}$ satisfies Lemma 12. We take the first α we find (Lemma 12 guarantees that we will eventually find one).
- $\beta = G(\alpha) = F(\alpha)^p \alpha^p + \alpha + 1$.

Now we will do a further encoding of $\mathcal{P}_1$ in $\mathbb{N} \times \mathbb{F}_q[Z] \times \mathbb{F}_q[Z]$. We encode a triple $(u, \alpha, \beta) \in \mathcal{P}_1$ as (u, A, B), where A is the minimal polynomial (over $\mathbb{F}_q$) of α and analogously B is the minimal polynomial of β. The set of all these (u, A, B) will be called $\mathcal{P}$.

Both these encodings are recursive procedures, therefore $\mathcal{P}_1$ and $\mathcal{P}$ are r.e. sets. It follows from Sect. 5 that $\mathcal{P}$ is Diophantine over $\mathbb{F}_q[Z]$. By Lemma 15, it is also Diophantine over $\mathbb{F}[Z]$.

Looking back at the definitions of $\mathcal{P}$ and $\mathcal{P}_1$, we can find a Diophantine definition of the set $\mathcal{S}$:

Theorem 16.

$$
\begin{aligned}
& F \in \mathcal{S} && (18)\\
& \Updownarrow && \\
& (\exists u \in \mathbb{N})(\exists A, B \in \mathbb{F}[Z])(\exists \alpha, \beta \in \mathbb{F}) && \\
& (u, A, B) \in \mathcal{P} && (19)\\
& \wedge\ A(\alpha) = 0 \ \wedge\ B(\beta) = 0 && (20)\\
& \wedge\ F \in \mathcal{A}_u \ \wedge\ F(\alpha)^p \alpha^p + \alpha + 1 = \beta. && (21)
\end{aligned}
$$

Remark. In the formula above, we wrote "$(\exists \alpha, \beta \in \mathbb{F})$", so we need $\mathbb{F}$ to be a Diophantine subset of $\mathbb{F}[Z]$, but this is easy: $X \in \mathbb{F} \iff X = 0 \vee (\exists Y)(XY = 1)$. A polynomial evaluation $X(\xi) = \eta$ is also Diophantine because it can be written as $(Z - \xi) | (X - \eta)$.

Proof. If $F \in \mathcal{S}$, we take the corresponding $(u, \alpha, \beta) \in \mathcal{P}_1$ and $(u, A, B) \in \mathcal{P}$. Then (19) is obviously satisfied, and (20) and (21) are true because of the construction of $\mathcal{P}_1$ and $\mathcal{P}$.

Conversely, assume (19)–(21). By definition of $\mathcal{P}$, it follows from $(u, A, B) \in \mathcal{P}$ that there exist α' and β' with $(u, \alpha', \beta') \in \mathcal{P}_1$ with α' a zero of A and β' a zero of B. This triple (u, α', β') has to come from some $F' \in \mathcal{S}$. If we write $G' = F'^p Z^p + Z + 1$, this means that

$$G' \in \mathcal{Z}_u \quad \text{and} \quad G'(\alpha') = \beta'.$$

However, writing $G = F^p Z^p + Z + 1$, if follows from (21) that

$$G \in \mathcal{Z}_u \quad \text{and} \quad G(\alpha) = \beta.$$

But α and α' are zeros of the same irreducible polynomial A, so they are conjugates. The same holds for β and β'. Looking at how we used Lemma 12 on the set $\mathcal{Z}_u$ to construct $\mathcal{P}_1$, we see that $G = G'^\sigma$ for some $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. Since $Z^\sigma = Z$, it follows that $F = F'^\sigma$. But $\mathcal{S}$ is invariant under ϕ_q, so $F' \in \mathcal{S}$ implies that $F \in \mathcal{S}$. □

References

1. Davis, M.: Hilbert's tenth problem is unsolvable. Am. Math. Mon. **80**, 233–269 (1973)
2. Demeyer, J.: Recursively enumerable sets of polynomials over a finite field. J. Algebra **310**, 801–828 (2007)
3. Denef, J.: The Diophantine problem for polynomial rings of positive characteristic. In: Boffa, M., van Dalen, D., McAloon, K. (eds.) Logic Colloquium 78, pp. 131–145. North-Holland, Amsterdam (1979)
4. Fröhlich, A., Shepherdson, C.: Effective procedures in field theory. Philos. Trans. R. Soc. Lond. **248**, 407–432 (1956)

5. Matiyasevich, Y.: Enumerable sets are Diophantine. Sov. Math. Dokl. **11**, 354–358 (1970)
6. Pheidas, T., Zahidi, K.: Undecidability of existential theories of rings and fields: a survey. In: Denef, J. et al. (eds.) Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999). Contemp. Math., vol. 270, pp. 49–105. Am. Math. Soc., Providence, RI (2000)
7. Poonen, B.: Hilbert's tenth problem over rings of number-theoretic interest (2003). Arizona Winter School 2003 notes, http://math.berkeley.edu/∼poonen/papers/aws2003.pdf
8. Rabin, M.: Computable algebra, general theory and theory of computable fields. Trans. Am. Math. Soc. **95**, 341–360 (1960)
9. Ribes, L., Zalesskii, P.: Profinite Groups. Springer, Berlin (2000)
10. Rumely, R.: Undecidability and definability for the theory of global fields. Trans. Am. Math. Soc. **262**, 195–217 (1980)
11. Shlapentokh, A.: Diophantine classes of holomorphy rings of global fields. J. Algebra **169**, 139–175 (1994)