An existential $\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$

Will Anscombe and Jochen Koenigsmann

Abstract

We show that the valuation ring $\mathbb{F}_q[[t]]$ in the local field $\mathbb{F}_q((t))$ is existentially definable in the language of rings with no parameters. The method is to use the definition of the henselian topology following the work of Prestel-Ziegler to give an $\exists\mathbb{F}_q$-definable bounded neighbourhood of 0. Then we ‘tweak’ this set by subtracting, taking roots, and applying Hensel’s Lemma in order to find an $\exists\mathbb{F}_q$-definable subset of $\mathbb{F}_q[[t]]$ which contains $t\mathbb{F}_q[[t]]$. Finally, we use the fact that $\mathbb{F}_q$ is defined by the formula $x^q - x = 0$ to extend the definition to the whole of $\mathbb{F}_q[[t]]$ and to rid the definition of parameters.

Several extensions of the theorem are obtained, notably an $\exists\emptyset$-definition of the valuation ring of a non-trivial valuation with divisible value group.

1 Introduction

This paper deals with questions of definability in power series fields. Unless stated otherwise, all definitions will be in the language $L_{\text{ring}}$ of rings. Let $q = p^k$ be a power of a prime and let $\mathbb{F}_q((t))$ be the field of formal power series over the finite field $\mathbb{F}_q$; sometimes this is called the field of Laurent series over $\mathbb{F}_q$. The ring $\mathbb{F}_q[[t]]$ of formal power series is the valuation ring of the $t$-adic valuation on $\mathbb{F}_q((t))$.

In section 2 of this paper we prove the following theorem.

Theorem 1.1. $\mathbb{F}_q[[t]]$ is existentially definable in $\mathbb{F}_q((t))$ using no parameters.

This result fits into a long history of definitions of valuation rings in valued fields. In the particular case of power series fields, a lot is already known.

Observation 1.2. $K[[t]]$ is not $\exists\emptyset$-definable in $K((t))$ for $K = \mathbb{Q}_p, \mathbb{C}$.

Proof. Let $K((t))^P := \bigcup_{n<\omega} K((t^{1/n}))$ be the field of Puiseux series and let $K[[t]]^P := \bigcup_{n<\omega} K[[t^{1/n}]]$. If $K[[t]]$ is $\exists\emptyset$-definable in $K((t))$ then $K[[t]]^P$ is $\exists\emptyset$-definable in $K((t))^P$ by the same formula. If $K = \mathbb{C}$ then, by Puiseux’s Theorem, $\mathbb{C}((t))^P$ is algebraically closed and thus no infinite co-infinite subsets are definable. In particular, $\mathbb{C}[[t]]^P$ is not definable.

Now let $K = \mathbb{Q}_p$ and let $\phi$ be an existential formula (with no parameters). Suppose that $\phi$ defines $\mathbb{Q}_p[[t]]$ in $\mathbb{Q}_p((t))$; then in $\mathbb{Q}_p((t))^P$ the formula $\phi$ defines $\mathbb{Q}_p[[t]]^P$, which is a proper subring. Note also that $\mathbb{Q}_p$ is contained in this definable set. The field $\mathbb{Q}_p((t))^P$ is

Most of this research forms part of the first author’s doctoral thesis, which was supported by EPSRC and completed under the supervision of the second author.
is $p$-adically closed, thus $\mathbb{Q}_p \preceq \mathbb{Q}((t))^{P_x}$. Thus $\phi$ defines $\mathbb{Q}_p$ in $\mathbb{Q}_p$, which is not a proper subset. This contradicts the elementary equivalence of $\mathbb{Q}_p$ and $\mathbb{Q}_p((t))^{P_x}$. □

In the field $\mathbb{Q}_p$ the valuation ring $\mathbb{Z}_p$ is $\exists \forall \emptyset$-definable by the formula $\exists y \ 1 + x^l p = y^l$, for any prime $l \neq p$. This formula is not, however, uniform in $p$. Analogies between $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ naturally suggest the first, ‘folkloric’ definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$, which is given in the following fact.

**Fact 1.3.** $\mathbb{F}_q[[t]]$ is defined in $\mathbb{F}_q((t))$ by the existential formula $\exists y \ 1 + x^l t = y^l$, for any prime $l$ such that $l \nmid q$.

**Proof.** Let $O := \mathbb{F}_q[[t]]$ denote the valuation ring and $M := tO$ the maximal ideal. Suppose that $x \in O$. Clearly $1 + x^l t \in 1 + M = (1 + M)^l$ by henselianity. Conversely, suppose $x$ is such that $v_t x < 0$. Then $v_t x^l \leq -l$ and $v_t (x^l t) \leq 1 - l < 0$. Thus $v_t (1 + x^l t) = v_t (x^l t) = 1 + lv_t x$ cannot be divisible by $l$ and there can exist no $y$ such that $1 + x^l t = y^l$. □

Other definitions are also well-known. One example is an $\exists \forall \forall$-definition with no parameters due to Ax, from (1), which applies to all power series fields.

**Fact 1.4. (Implicit in (1))** Let $F$ be any field. Then $F[[t]]$ is $\exists \forall \forall \emptyset$-definable in $F((t))$.

Another definition, in even greater generality, which uses no parameters is due to the second author and is from (4). However, this definition is not existential.

**Fact 1.5. (Lemma 3.6, (4))** Let $F$ be any field and suppose that $O$ is an henselian rank $1$ valuation ring on $F$ with a non-divisible value group. Then $O$ is $\emptyset$-definable.

Recent work of Cluckers-Derakhshian-Leenknegt-Macintyre on the uniformity of definitions of valuation rings in henselian valued fields includes the following theorem in the expanded language $\mathcal{L}_{\text{ring}} \cup \{P_2\}$, where the Macintyre predicate $P_2$ is interpreted as the set of squares.

**Fact 1.6. (Theorem 3, (2))** There is an existential formula $\phi$ in $\mathcal{L}_{\text{ring}} \cup \{P_2\}$ which defines the valuation ring in all henselian valued fields $K$ with finite or pseudo-finite residue field of characteristic not equal to $2$.

One consequence of Theorem 1.1 is in the study of definability in $\mathbb{F}_q((t))$: it reduces questions of existential definability in the language of valued fields (for example $\mathcal{L}_{\text{ring}}$ expanded with a unary predicate for the valuation ring) to existential definability in $\mathcal{L}_{\text{ring}}$ conservatively in parameters; i.e. without needing more parameters.

It is famously unknown whether or not the theory of $\mathbb{F}_q((t))$ is decidable, whereas $\mathbb{Q}_p$ is decidable by the work of Ax-Kochen and Ershov. In (3) Denef and Schoutens prove that Hilbert’s $10$th problem has a positive solution in $\mathbb{F}_q[[t]]$ (in the language $\mathcal{L}_{\text{ring}} \cup \{t\}$ of discrete valuation rings) on the assumption of Resolution of Singularities in characteristic $p$. As a consequence of Theorem 1.1 we prove in Corollary 3.3 that Hilbert’s $10$th problem in $\mathcal{L}_{\text{ring}}$ has a solution over $\mathbb{F}_q((t))$ if and only if it has a solution in $\mathbb{F}_q[[t]]$. Of course, the analogous result for the language $\mathcal{L}_{\text{ring}} \cup \{t\}$ follows from the ‘folkloric’ definition in Fact 1.3.

As an imperfect field, $\mathbb{F}_p((t))$ cannot be model complete in the language of rings; however it is still unknown whether it is model complete in a relatively ‘nice’ expansion of that language, for example some analogy of the Macintyre language (see (5)) suitable for positive characteristic.
2 The $\exists$-$\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$

Let $v_t$ be the $t$-adic valuation on $\mathbb{F}_q((t))$. The valuation ring of $v_t$ is the ring $\mathbb{F}_q[[t]]$ of formal power series which has a unique maximal ideal $t\mathbb{F}_q[[t]]$. The value group of $v_t$ is $\mathbb{Z}$ and the residue field is $\mathbb{F}_q$. Importantly, the valued field $(\mathbb{F}_q((t)), \mathbb{F}_q[[t]])$ is henselian.

2.1 Spheres and balls in valued fields

We briefly make a few definitions and notational conventions. Let $(K, \mathcal{O})$ be a valued field, let $v$ be the corresponding valuation, and let $v_K$ denote the value group.

**Definition 2.1.** For $n \in v_K$ and $a \in K$, we let

1. $S(n) := v^{-1}(\{n\})$ be the set of elements of value $n$,
2. $B(n; a) := a + v^{-1}(\langle n, \infty \rangle)$ be the open ball of radius $n$ around $a$, and
3. $\overline{B}(n; a) := a + v^{-1}(\langle n, \infty \rangle)$ be the closed ball of radius $n$ around $a$.

We let $\sqcup$ denote a disjoint union.

**Lemma 2.2.** Let $n \in vK$. Then

1. $B(n; 0) \subseteq S(n) - S(n)$,
2. $B(n; 0) = S(n) \cup B(n; 0)$, and
3. $B(n; 0) - B(n; 0) = \overline{B}(n; 0)$.

**Proof.**

1. Let $x \in B(n; 0)$ and let $y \in S(n)$. Then $v(y) = n < v(x)$, so that $v(x - y) = n$ (by an elementary consequence of the ultrametric inequality) and $x - y \in S(n)$. Thus $x = x - y + y \in S(n) - S(n)$.

2. Let $x \in \overline{B}(n; 0)$. Then either $v(x) = n$ or $v(x) > n$.

3. Let $x, y \in \overline{B}(n; 0)$. By the ultrametric inequality $v(x - y) \geq n$. Thus $x - y \in \overline{B}(n; 0)$. \(\square\)

2.2 An $\exists$-definable filter base for the neighbourhood filter of zero

Following Prestel and Ziegler in (7), we give the definition of a $t$-henselian field. From another paper of Prestel ((6)), we recall a definition of the $t$-henselian topology (in the context of $t$-henselian non-separably closed fields). We obtain an $\exists$-definable bounded neighbourhood of zero. For more information on $t$-henselian fields, see (7).

For $n \in \mathbb{N}$ and any subset $U \subseteq K$, we denote $x^{n+1} + x^n + U[x]^{n-1} := \{x^{n+1} + x^n + u_{n-1}x^{n-1} + \ldots + x_0 : u_i \in U\}$.

**Definition 2.3.** Let $K$ be any field. We say that $K$ is $t$-henselian if there is a field topology $\mathcal{T}$ on $K$ induced by an absolute value or a valuation with the property that, for each $n \in \mathbb{N}$, there exists $U \in \mathcal{T}$ such that $0 \in U$ and such that each $f \in x^{n+1} + x^n + U[x]^{n-1}$ has a root in $K$. 

3
The following definition of the t-henselian topology from (1) corrects an earlier definition given in (3). To define a group topology, we mean that a filter base of the filter of neighbourhoods of zero is a definable family.

Let $D := D_x$ denote the formal derivative with respect to the variable $x$.

**Lemma 2.4. (Proof of Lemma, (6))** Suppose that $K$ is t-henselian and not separably closed. Let $f \in K[x]$ be a separable irreducible polynomial without a zero in $K$. Let $a \in K \setminus Z(Df)$ be any element which is not a zero of the formal derivative of $f$. Let $U_{f,a} := f(K)^{-1} - f(a)^{-1} = \{ \frac{1}{f(x)} - \frac{1}{f(a)} \mid x \in K \}$. Then $U := \{ c \cdot U_{f,a} \mid c \in K^* \}$ is a base for the filter of open neighbourhoods around zero in the (unique) t-henselian topology.

We prove a simple consequence of the Lemma.

**Proposition 2.5.** Suppose that $C \subseteq K$ is a relatively algebraically closed subfield of $K$ which is not separably closed. There exists $V \subseteq K$ which is an $\exists$-C-definable bounded neighbourhood of $0$ in the t-henselian topology.

**Proof.** We choose $f \in C[x]$ to be non-linear, irreducible, and separable. Let $n := \deg(f)$; thus $\deg(Df) \leq n - 1$. If $|C| > n - 1$ then we may choose $a \in C \setminus Z(Df)$. On the other hand, if $C$ is a finite field, then $C$ allows separable extensions of degree 2. So we may choose $f$ to be of degree 2; whence $Df$ is of degree $\leq 1$ and again there exists $a \in C$ which is not a root of $Df$. Let $V := U_{f,a} = f(K)^{-1} - f(a)^{-1}$. Clearly $V$ is $\exists$-C-definable. As discussed in [Lemma 2.4] $V$ is a bounded neighbourhood of 0.

### 2.3 An $\exists$-F-definable set between $O$ and $M$ in $F((t))$

Now let $K := F((t))$ be the field of formal power series over a field $F$. Let $v$ be the $t$-adic valuation, let $O := F[[t]]$ be the valuation ring of $v$, let $M := tO$ be its maximal ideal, and let $vK = Z$ be its value group. Note that $(K, O)$ is henselian. Let $C \subseteq K$ be any subset. Let $P := S(1)$ be the set of elements of value 1; thus $P$ is the set of uniformisers.

In the following proposition we show how to ‘tweak’ a definable bounded neighbourhood of 0 until we obtain a subset of $O$ containing $M$, in such a way as to preserve definability.

**Proposition 2.6.** Suppose that $V \subseteq K$ is an $\exists$-C-definable bounded neighbourhood of 0.

1. There exists $W \subseteq K$ which is bounded, $\exists$-C-definable, and is such that $P \subseteq W$.

2. There exists $X \subseteq K$ which is bounded, $\exists$-C definable, and is such that $M \subseteq X$.

3. There exists $Y \subseteq K$ which is bounded by $O$, $\exists$-C-definable, and is such that $M \subseteq Y$.

**Proof.**

1. $V$ is a neighbourhood of 0. Let $n \in Z$ be such that $B(n; 0) \subseteq V$. Without loss of generality, we suppose that $n \geq 0$. Choose any $m > n$; then $P^m \subseteq S(m) \subseteq B(n; 0) \subseteq V$. Let $\phi(x)$ be the formula expressing $x^m \in V$, and let $W := \phi(K)$ be the set defined by $\phi$ in $K$. Note that $W$ is $\exists$-C-definable, and $P \subseteq W$.

It remains to show that $W$ is bounded. Since $V$ is bounded, there exists $l \in Z$ such that $V \subseteq B(l; 0)$. Let $l' := \min\{l, -1\}$ and let $b \notin B(l'; 0)$. Since $vb \leq l' \leq -1 < 0$, we have that $vb^m = mvb \leq vb \leq l' \leq l$. Thus $b^m \notin V$ and

$$ (x^m \in V \implies x \in B(l'; 0)) . $$

So $W \subseteq B(l'; 0)$.
2. Let \( W' := W \cup \{0\} \) and set \( X := W - W' \). Clearly \( X \) is bounded and \( \exists \mathcal{C} \)-definable.

By Lemma 2.2, we see that \( B(1;0) \subseteq S(1) - S(1) = \mathcal{P} - \mathcal{P} \subseteq W - W \subseteq X \). Also \( \mathcal{P} \subseteq W - 0 \subseteq X \). Thus \( \mathcal{M} = \hat{B}(1;0) = \mathcal{P} \cup B(1;0) \subseteq X \).

3. \( X \) is bounded but contains \( \mathcal{M} \), so there exists \( h \in \mathbb{N} \) such that \( X \subseteq B(-h;0) \). Let \( \psi(x) \) be the formula expressing \( x^h \in X \), and set \( Y := \psi(K) - \psi(K) \). Observe that \( Y \) is \( \exists \mathcal{C} \)-definable. It remains to show that \( Y \) is bounded by \( \mathcal{O} \) and that \( \mathcal{M} \subseteq Y \).

If \( va \leq -1 \) then \( va^h = hva \leq -h \). Thus if \( va \leq -1 \), then \( a^h \notin B(-1,0) \supseteq X \) and \( a \notin \psi(K) \). Therefore \( \psi(K) \subseteq \mathcal{O} \). By Lemma 2.2, \( Y = \psi(K) - \psi(K) \subseteq \mathcal{O} - \mathcal{O} = \mathcal{O} \).

Since \( P^h \subseteq S(h) \) (where \( P^h \) is the set of \( h \)-th powers of elements of \( P \)) and \( S(h) \subseteq \mathcal{M} \subseteq X \); we have that \( \mathcal{P} \subseteq \psi(K) \). Thus \( \mathcal{P} - \mathcal{P} \subseteq \psi(K) - \psi(K) \). By Lemma 2.2, \( B(1;0) \subseteq \mathcal{P} - \mathcal{P} \); thus \( B(1;0) \subseteq \psi(K) - \psi(K) \). Since \( 0^h = 0 \in \mathcal{M} \subseteq X \) and \( 0 \notin \psi(K) \) and \( \mathcal{P} - 0 \subseteq \psi(K) - \psi(K) \). By another application of Lemma 2.2, this means that \( \mathcal{M} = \mathcal{P} \cup B(1;0) \subseteq \psi(K) - \psi(K) = Y \), as required.

\[ \square \]

### 2.4 The \( \exists \mathcal{O} \)-definition of \( \mathbb{F}_q[[t]] \) in \( \mathbb{F}_q((t)) \)

Finally, we consider the special case where \( F \) is the finite field \( \mathbb{F}_q \) for \( q \) a prime power. Thus we fix \( K := \mathbb{F}_q((t)) \) and \( \mathcal{O} := \mathbb{F}_q[[t]] \).

**Lemma 2.7.** There exists an \( \exists \mathcal{F}_q \)-definable bounded neighbourhood of 0.

**Proof.** \( \mathbb{F}_q \subseteq K \) is relatively algebraically closed in \( K \) and is not separably closed. By Proposition 2.5, there exists \( V \) with the required properties. \( \square \)

**Proposition 2.8.** \( \mathcal{O} \) is \( \exists \mathcal{F}_q \)-definable in \( K \).

**Proof.** We combine Lemma 2.7 and Proposition 2.6 to obtain an \( \exists \mathcal{F}_q \)-definable set \( Y \) which contains \( \mathcal{M} \) and is bounded by \( \mathcal{O} \). Note that \( \mathbb{F}_q \) is an algebraic set defined by the formula \( x^a - x^b = 0 \) in \( K \). Let \( \chi(x) := \exists y(y^a - y^b = 0 \wedge x \in y + Y) \). This is obviously an \( \exists \mathcal{F}_q \)-formula. Since \( \mathcal{O} = \mathbb{F}_q + \mathcal{M} \subseteq Y \subseteq \mathcal{O} \), it is clear that \( \chi(K) = \mathcal{O} \). \( \square \)

We will improve Proposition 2.8 by removing the parameters. In the definition of the set \( U_{f,a} \) we used \( a \) and the coefficients of \( f \) as parameters. All of these come from \( \mathbb{F}_q \), but not necessarily from \( \mathbb{F}_p \). Although elements of \( \mathbb{F}_q \) are not closed terms, they are algebraic over \( \mathbb{F}_p \). We use this algebraicity and a few simple tricks to find an existential formula with no parameters which defines \( \mathcal{O} \).

**Fact 2.9.** We state a simple consequence of Euclid’s famous argument about the infinitude of the primes. Let \( \{p_i|i \in I\} \) be a finite set of primes. There exists another prime \( p' \leq \prod_{i \in I} p_i + 1 \) which is not in the set \( \{p_i|i \in I\} \).

Now let \( k \in \mathbb{N} \) and let \( P \) be the set of primes that divide \( k \). Of course \( \prod_{p \in P} p \leq k \).

By the previous remark, there exists another prime \( p' \notin P \) such that \( p' \leq \prod_{p \in P} p + 1 \). If \( p' > k \) then \( k = \prod_{p \in P} p \) and \( p' = k + 1 \). Thus \( p' \leq k + 1 \). Thus the least prime \( p' \) not dividing a natural number \( k \) is no greater than \( k + 1 \). Of course \( k + 1 \) is a very bad upper bound for \( p' \) in general; although if \( k = 1,2 \) then \( p' = k + 1 \).

**Lemma 2.10.** There exists an \( \exists \mathcal{O} \)-definable bounded neighbourhood of 0.
Proof. We seek a polynomial \( f \in \mathbb{F}_p[x] \) which is irreducible in \( \mathbb{F}_q[x] \) and is such that not all elements of \( \mathbb{F}_q \) are roots of \( Df \), i.e. \( x^q - x \not\equiv Df \).

Write \( q = p^k \) and let \( l \) be the least prime not dividing \( k \). By [Fact 2.9] \( l \leq k + 1 \); consequently \( l \leq p^k = q \). Let \( f \in \mathbb{F}_p[x] \) be an irreducible polynomial of degree \( l \). Since \( l \nmid k \), \( f \) is still irreducible in \( \mathbb{F}_q[x] \). Furthermore, \( Df \) is of degree \( \leq l - 1 < q \). Thus it cannot be the case that every element of \( \mathbb{F}_q \) is a zero of \( Df \). For any \( a \in \mathbb{F}_q \) which is not a zero of \( Df \), \( U_{f,a} = f(K)^{-1} - f(a)^{-1} \) is an \( \exists \mathbb{F}_q \)-definable bounded neighbourhood of 0.

We note that the only parameter in this definition not from \( \mathbb{F}_p \) is \( 0 \). Thus it cannot be the case that every element of \( \mathbb{F}_q \) is a zero of \( Df \). For any \( a \in \mathbb{F}_q \) which is not a zero of \( Df \), \( U_{f,a} = f(K)^{-1} - f(a)^{-1} \) is an \( \exists \mathbb{F}_q \)-definable bounded neighbourhood of 0. We note that the only parameter in this definition not from \( \mathbb{F}_p \) is \( a \).

The union of finitely many bounded neighbourhoods of 0 is also a bounded neighbourhood of 0. Thus

\[
\zeta(y) := \exists y \ (y^q - y \equiv 0 \land -Df(y) \equiv 0 \land x \in U_{f,y})
\]

is an \( \exists \mathbb{F}_p \)-formula which defines the union

\[
V := \bigcup \{ U_{f,a} \mid a \in \mathbb{F}_q, Df(a) \neq 0 \}.
\]

Finally note that each element of \( \mathbb{F}_p \) is the image of a closed term; thus each remaining parameter can be replaced by a closed term and we are left with an \( \exists \emptyset \)-definition of \( V \). \( \square \)

Remark 2.11. Here is an alternative method to find an irreducible separable polynomial \( f \in \mathbb{F}_p[x] \) and an element \( a \in \mathbb{F}_p \) which is not a root of \( Df \).

Let \( l \) be a prime such that \( p \nmid l \nmid k \). Let \( g \in \mathbb{F}_p[x] \) be any irreducible polynomial of degree \( l \). Since \( l \nmid k \), \( g \) is still irreducible over \( \mathbb{F}_q \). Let \( \alpha \) be a root of \( g \) in a field extension. Either the coefficient of \( x^{l-1} \) in \( g \) is zero; or else we consider \( h := g(x - 1) \), which is the minimal polynomial of \( \alpha + 1 \). The coefficient of \( x^{l-1} \) in \( h \) is then \( l \neq 0 \). Thus we may assume that the \( x^{l-1} \) term in \( g \) is non-zero. The polynomial \( f := x^l g(1/x) \) is the minimal polynomial of \( 1/\alpha \) and has non-zero linear term. Therefore \( Df(0) \neq 0 \). Thus \( U_{f,0} \) is an \( \exists \mathbb{F}_p \)-definable bounded neighbourhood of 0. As before, elements of \( \mathbb{F}_p \) are closed terms, so we may remove all parameters from the definition.

Finally, we prove Theorem 1.1

Theorem 1.1. \( \mathcal{O} \) is \( \exists \emptyset \)-definable in \( K \).

Proof. From Lemma 2.10 we obtain an \( \exists \emptyset \)-definable bounded neighbourhood of 0. Using again Proposition 2.6 we obtain an \( \exists \emptyset \)-definable set \( Y \) which contains \( \mathcal{M} \) and is bounded by \( \mathcal{O} \). We define \( \chi \) as before:

\[
\chi(x) := \exists y \ (y^q - y \equiv 0 \land x \in y + Y).
\]

This is an \( \exists \)-formula with no parameters and it defines \( \mathcal{O} \). \( \square \)

Nevertheless the formula still depends on \( \mathbb{F}_q \) in several ways: our choices of \( m \) and \( h \) in Proposition 2.6 and our choice of \( f \) in Theorem 1.1 depend on \( \mathbb{F}_q \). The number \( q \) also appears directly in several of the formulas. All these factors tell us that \( \chi \) is highly non-uniform in \( q \). In fact, in recent as-yet-unpublished joint work of Cluckers, Derakhshan, Leenknegt, and Macintyre \( (2) \) it is shown that no definition exists which is uniform in \( p \) or in \( k \) (where \( q = p^k \)).
Remark 2.12. With a little more effort we can be more explicit about the formula $\chi$. Suppose for the moment that $K = \mathbb{F}_p((t))$. Let $\varphi := x^p - x$ and let $f := \varphi - 1$. Observe that $\varphi - 1$ is separable and irreducible in $K[x]$ and $Df(1) = D(\varphi)(1) = -1 \neq 0$. Working back through the formulas and rearranging, we find that

$$\chi(x) := \exists ab(x_i y_i)_{i=1}^4 \left( \varphi(x - a + b) \equiv 0 \land a^h x_i - x_2 \land b^h x_3 - x_4 \land \wedge f(y_i)(x_i^m - 1) - 1 \equiv 0 \right).$$

3 Extensions of the result

3.1 The field $\bigcup_{n \in \mathbb{N}} \mathbb{F}_q((t^{1/n}))$ of Puiseux series

Let $K^{\text{P}} := \bigcup_{n \in \mathbb{N}} \mathbb{F}_q((t^{1/n}))$ denote the field of Puiseux series over $\mathbb{F}_q$, where $(t^{1/n})_{n \in \mathbb{N}}$ is a compatible system of $n$-th roots of $t$ (for $n \in \mathbb{N}$). Note that $K^{\text{P}}$ can be formally defined as a direct limit. Let $O^{\text{P}} := \bigcup_{n \in \mathbb{N}} \mathbb{F}_q[[t^{1/n}]]$ denote the valuation ring of the $t$-adic valuation. Note that the value group is $\mathbb{Q}$.

The following theorem is the first example of an $\exists$-formula of a non-trivial valuation ring with divisible value group.

**Theorem 3.1.** $O^{\text{P}}$ is $\exists-\emptyset$-definable in $K^{\text{P}}$.

**Proof.** By Theorem 1.1 we may let $\chi$ be an $\exists$-formula (with no parameters) which defines $O$ in $K$. In each field $\mathbb{F}_q((t^{1/n}))$ the formula $\chi$ defines the valuation ring $\mathbb{F}_q[[t^{1/n}]]$ since each of these fields is isomorphic to $\mathbb{F}_q((t))$. In the union, $\chi$ defines the union of the valuation rings (in any union of structures an existential formula defines the unions of sets that it defines in each of the structures). Thus $\chi$ defines $O^{\text{P}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_q[[t^{1/n}]]$, as required. $\square$

3.2 The perfect hull $\mathbb{F}_q((t))^{\text{perf}}$

We still denote $K := \mathbb{F}_q((t))$. Let $K^{\text{perf}} := \bigcup_{n \in \mathbb{N}} \mathbb{F}_q((t^{p^{-n}}))$ be the **perfect hull** of $K$; this is also formally defined as a direct limit. Now we use Theorem 1.1 to existentially define the valuation ring $O^{\text{perf}} := \bigcup_{n < \omega} O^{p^{-n}}$ in $K^{\text{perf}}$.

**Theorem 3.2.** $O^{\text{perf}}$ is $\exists-\emptyset$-definable in $K^{\text{perf}}$.

**Proof.** The proof is almost identical to the proof of Theorem 3.1 $\square$

3.3 Consequences for $\exists$-definability in $\mathcal{L}_{\text{val}}$

We return to the field $K := \mathbb{F}_q((t))$. The most important consequence of Theorem 1.1 is that questions of existential definability in $\mathcal{L}_{\text{val}}$ reduce to questions of existential definability in $\mathcal{L}_{\text{ring}}$. Let $C \subseteq \mathbb{F}_q((t))$ be any subfield of parameters and let $\mathcal{L}_{\text{val}} := \mathcal{L}_{\text{ring}} \cup \{ O \}$ be the language of valued fields.

**Proposition 3.3.** Let $\alpha \in \mathcal{L}_{\text{val}}$ be an existential formula with parameters from $C$. Then there exists $\beta \in \mathcal{L}_{\text{ring}}$ with parameters in $C$ such that $\alpha$ and $\beta$ are equivalent modulo the theory of $\mathbb{F}_q((t))$. 

7
Proof. Let $b = (b_i)_{i < q}$ be some indexing of the field $\mathbb{F}_q$ such that $b_0 = 0$. Let $\phi$ be a quantifier-free formula in free variables $y = (y_i)_{i < q}$ expressing the quantifier-free type of $b$. We define
\[
\psi := \exists y \left( x \in \mathcal{O} \land \phi(y) \land \bigwedge_{0 < i < q} y_i + x \in \mathcal{O}^{-1} \right).
\]
We claim that $\psi$ existentially defines $\mathcal{M}$. Let $a \in \mathcal{O}$. Then $a \in \mathcal{M}$ if and only if, for each $b \in \mathbb{F}_q^+$, $a + b \in \mathcal{O} \setminus \mathcal{M} = \mathcal{O}^+$; that is if and only if $K \models \psi(a)$. Thus $\psi$ is an $\exists$-$\emptyset$-definition for $\mathcal{M}$. Consequently, $K \setminus \mathcal{O} = (\mathcal{M} \setminus \{0\})^{-1}$ is $\exists$-$\emptyset$-definable; and so $\mathcal{O}$ is $\forall$-$\emptyset$-definable.

Since $\mathcal{O}$ is both $\forall$-$\emptyset$-definable and $\exists$-$\emptyset$-definable, we may convert any $\exists$-$C$-formula $\alpha$ of $\mathcal{L}_{\text{val}}$ into an $\exists$-$C$-formula $\beta$ of $\mathcal{L}_{\text{ring}}$. \hfill $\square$

**Corollary 3.4.** Hilbert’s 10th problem has a solution over $\mathbb{F}_q((t))$ if and only if it does so over $\mathbb{F}_q[[t]]$, in any language which expands the language of rings.

**Proof.** Let $\phi$ be a quantifier-free formula with $x$ the tuple of free-variables. Suppose that Hilbert’s 10th problem (H10) has a solution over $\mathbb{F}_q((t))$. In order to decide the existential sentence $\exists x \phi(x)$ in $\mathbb{F}_q[[t]]$ we apply our algorithm for $\mathbb{F}_q((t))$ to the sentence
\[
\exists x \left( \phi(x) \land \bigwedge_{x \in \mathcal{X}} \mathcal{O}(x) \right),
\]
where $\mathcal{O}$ denotes the existential formula defining $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$.

Conversely, suppose that H10 has a solution over $\mathbb{F}_q[[t]]$. By standard equivalences in the theory of fields we may assume that $\phi = f \equiv 0$ for some polynomial $f \in \mathbb{F}_p[x]$.

We need to find a quantifier-free formula which is realised in $\mathbb{F}_q[[t]]$ if and only if $f$ has a zero in $\mathbb{F}_p((t))$. For a variable $x \in \mathcal{X}$ we let $d_x$ denote the degree of $f$ in $x$; and for any subtuple $\mathcal{X}' \subseteq \mathcal{X}$ we let $\mathcal{X}'' := (\mathcal{X} \setminus \mathcal{X}') \cup \{x^{-1} | x \in \mathcal{X}'\}$ be a new tuple formed from $\mathcal{X}$ by inverting the elements of $\mathcal{X}'$. Then we set $f_{\mathcal{X}'} := f(\mathcal{X}'') \prod_{x \in \mathcal{X}'} x^{d_x}$. Importantly, $f_{\mathcal{X}'}$ is a polynomial. Finally we let
\[
\phi' := \bigvee_{\mathcal{X}' \subseteq \mathcal{X}} \left( f_{\mathcal{X}'} \equiv 0 \land \bigwedge_{x \in \mathcal{X}'} -x \equiv 0 \right).
\]

Then $\mathbb{F}_q((t)) \models \exists x f(x) \equiv 0$ if and only if $\mathbb{F}_q[[t]] \models \exists x \phi'(x)$. Therefore, in order to decide $\exists x \phi(x)$ in $\mathbb{F}_q((t))$ we apply our algorithm for $\mathbb{F}_q[[t]]$ to the existential sentence $\exists x \phi'(x)$. \hfill $\square$

A simple consequence of the ‘folkloric’ definition of $\mathbb{F}_q[[t]]$ from Fact 1.3 is that Corollary 3.4 holds for any language expanding $\mathcal{L}_{\text{ring}} \cup \{t\}$.

Note that, by the theorem of Denef-Schoutens in (3), Hilbert’s 10th problem has a positive solution in $\mathbb{F}_p[[t]]$ in the language $\mathcal{L}_{\text{ring}} \cup \{t\}$ on the assumption of Resolution of Singularities in positive characteristic.

If Hilbert’s 10th problem could be proved - outright - to have a positive solution in $\mathbb{F}_p[[t]]$ simply in the language of rings, then Corollary 3.4 would ‘lift’ that result to $\mathbb{F}_p((t))$. 

8
References

[1] James Ax. On the undecidability of power series fields. *Proc. Amer. Math. Soc.*, 16:846, 1965.

[2] Raf Cluckers, Jamshid Derakshan, Eva Leenknegt, and Angus Macintyre. Uniformly defining valuation rings in henselian valued fields with finite and pseudo-finite residue field. *arXiv:1306.1802v1*, 2013.

[3] Jan Denef and Hans Schoutens. On the decidability of the existential theory of $\mathbb{F}_p[[t]]$. *Fields Inst. Commun.*, 33:43–60, 2003.

[4] Jochen Koenigsmann. Elementary characterization of fields by their absolute galois group. *Siberian Adv. Math.*, 14:16–42, 2004.

[5] Angus Macintyre. On definable subsets of $p$-adic fields. *J. Symbolic Logic*, 41:605–610, 1976.

[6] Alexander Prestel. Algebraic number fields elementarily determined by their absolute Galois group. *Israel J. Math.*, 73(2):199–205, 1991.

[7] Alexander Prestel and Martin Ziegler. Model-theoretic methods in the theory of topological fields. *J. Reine Angew. Math.*, 299 (300):318–341, 1978.

Will Anscombe
Lincoln College, Turl Street, Oxford OX1 3DR, UK
anscombe@maths.ox.ac.uk

Jochen Koenigsmann
Mathematical Institute, 24-29 St Giles, Oxford OX1 3LB, UK
koenigsmann@maths.ox.ac.uk