Comment.Math.Univ.Carolin. 58,3 (2017) 267–273

Semifields and a theorem of Abhyankar

Vítězslav Kala

Abstract. Abhyankar proved that every field of finite transcendence degree over $\mathbb{Q}$ or over a finite field is a homomorphic image of a subring of the ring of polynomials $\mathbb{Z}[T_1, \dots, T_n]$ (for some n depending on the field). We conjecture that his result cannot be substantially strengthened and show that our conjecture implies a well-known conjecture on the additive idempotence of semifields that are finitely generated as semirings.

Keywords: Abhyankar's construction; semiring; semifield; finitely generated; additively idempotent

Classification: 12K10, 13B25, 16Y60

1. Introduction

A classical fact says that if a field is finitely generated as a ring, then it is finite — in other words, no infinite field is a homomorphic image of the ring of polynomials $\mathbb{Z}[T_1, \dots, T_n]$. Surprisingly, Abhyankar in 2011 proved the following theorem saying that this is not true when we consider fields as factors of subrings of $\mathbb{Z}[T_1, \dots, T_n]$.

Theorem 1.1 ([1, Proposition 1.2]). *Let F be a field of finite transcendence degree over $\mathbb{Q}$ or over a finite field $\mathbb{F}_q$. Then there is a ring $B \subset A = \mathbb{Z}[T_1, \dots, T_n]$ (for a suitable n) and a maximal ideal I of B such that $F \simeq B/I$.*

For example, there is a subring $B \subset \mathbb{Z}[T_1, T_2]$ and an epimorphism $B \twoheadrightarrow \mathbb{Q}$, described in Section 2 below.

Rings B that arise from Abhyankar's construction have several unusual properties. The goal of this short note is to explore them and to study the (im)possibility of a generalization and a connection to the theory of semirings.

Just to recall, by a *semiring* $S(+, \cdot)$ we here mean a set S with addition $+$ and multiplication $\cdot$ that are both commutative and associative, and such that multiplication distributes over addition. A semiring $S(+, \cdot)$ is a *semifield* if moreover $S(\cdot)$ is a group (such a structure is also occasionally called a parasemifield [2], [7]; note that unlike our definition, sometimes a semifield is defined to have a zero element). A semiring is *additively idempotent* if $a + a = a$ for all $a \in S$.

DOI 10.14712/1213-7243.2015.216

The author was partly supported by the Czech Science Foundation GAČR, grant 17-04703Y.

Semirings are a very natural generalization of rings that has been widely studied, not only from purely algebraic perspective, but also for their applications in cryptography, dequantization, tropical mathematics, non-commutative geometry, and the connection to logic via MV-algebras and lattice-ordered groups [2], [3], [4], [5], [6], [15], [16], [17], [18], [19], [20], and [21]. We refer the reader to the aforementioned works for further history and references.

Particularly important and interesting are the problems of classifying various classes of semirings. In order to classify all ideal-simple (commutative) semirings [2], one needs to study the following conjecture that extends the above-mentioned classical result on fields that are finitely generated as rings:

Conjecture 1.2 ([2]). *Every semifield which is finitely generated as a semiring is additively idempotent.*

A lot of progress has already been made on Conjecture 1.2: building on the results from [9], [10], the conjecture was proved for the case of two generators in [7]. Recently, additively idempotent semifields that are finitely generated as semirings were classified [8] using their correspondence with lattice-ordered groups. This result then provides new tools for attacking the conjecture in the case of more generators [11]. Some partial results have also been obtained for a generalization of this problem to divisible semirings (instead of semifields) [12], [13], [14].

In this short note we consider the connection between semirings, semifields and rings. The basic construction is that of the difference ring $S-S$ of a semiring S. If S is additively cancellative (i.e., $a+c=b+c$ implies $a=b$ for all $a,b,c\in S$), we can define $S-S$ as the set of all (formal) differences $s-t$ of elements of S with addition and multiplication naturally extended from the semiring. The fact that S is additively cancellative ensures that $S-S$ is well-defined and that $S\subset S-S$.

The situation is much more complicated in the case of semifields that might violate Conjecture 1.2 — it is easy to show that they cannot be additively cancellative. In fact, more generally assume that we have a finitely generated semiring S that contains the semifield of positive rational numbers $\mathbb{Q}^+$. Then we know that S is not additively cancellative [10, Proposition 1.18], and so the difference ring $S-S$ is not well-defined. One could instead consider the Grothendieck ring $G(S)$, but we still would not have $S\subset G(S)$.

However, we can proceed somewhat less directly: S is finitely generated, and so it is a factor of the polynomial semiring $\mathbb{N}[T_1,\dots,T_n]$. Let $\varphi:\mathbb{N}[T_1,\dots,T_n]\twoheadrightarrow S$ be the defining surjective homomorphism. $\mathbb{Q}^+\subset S$ is additively cancellative, and so we can consider the difference ring $B:=\varphi^{-1}(\mathbb{Q}^+)-\varphi^{-1}(\mathbb{Q}^+)\subset\mathbb{Z}[T_1,\dots,T_n]$ and extend φ to a surjection $B\twoheadrightarrow\mathbb{Q}$. The existence of such a B is purely a ring-theoretic statement. If such a B did not exist, we would have obtained a contradiction with the existence of S. However, precisely such rings were constructed by Abhyankar [1], and so this naïve approach fails.

Despite the fact that this attempt does not work, there are finer ways of translating the problem to the setting of rings. As our main result, we show in Theorem 3.1 that the existence of a semifield which is finitely generated as a semiring and not additively idempotent (i.e., one violating Conjecture 1.2) implies the existence of a ring which would contradict the following conjecture.

Conjecture 1.3. *The following situation cannot happen: Let $A = \mathbb{Z}[T_1, \dots, T_n]$. There exists a subring B of A and an ideal I of B such that*

(a) $QF(B) = \mathbb{Q}(T_1, \dots, T_n)$ *(QF denotes the quotient field).*
(b) $IA = A$.
(c) *Let* $A^+ = \mathbb{N}[T_1, \dots, T_n]$. *Then there is $\ell_0 \in A^+$ such that for all $a \in A^+$ and all $\ell = \ell_0 + a \in A$, we have if $h(\ell) = 0$ for some $h(X) \in B[X]$, then $h(X) \in I[X]$.*
(d) $\mathbb{Q} \subset B/I$.

The significance of the conditions above will become clear from the proof of Theorem 3.1 below. Let us only remark here that Abhyankar's rings from Theorem 1.1 satisfy (a), (b), and (d), but not (c).

Condition (c) in the conjecture does not look very natural from ring-theoretic point of view. However, we are not even aware of whether the conjecture holds when we replace (c) by

(c') *For all $\ell \in A$ we have that if $h(\ell) = 0$ for $h(X) \in B[X]$, then $h(X) \in I[X]$.*

It seems plausible to expect that this Conjecture 1.3 is in fact equivalent to Conjecture 1.2. This is certainly an interesting direction for future research.

2. Abhyankar's construction

Abhyankar's construction and the proof of Theorem 1.1 are fairly involved, being based on the notion of blow-up from algebraic geometry, which is also used in the resolution of singularities of algebraic varieties. Hence we refer the reader to the original paper for details; let us just illustrate the construction with an explicit example of a ring with a surjection onto $F = \mathbb{Q}$, in which case we can take $n = 2$.

Example 2.1. We have $A = \mathbb{Z}[T_1, T_2]$. Define $B = \mathbb{Z}[f_2, f_3, \dots]$ and a homomorphism $\varphi : B \twoheadrightarrow \mathbb{Q}$ by

$f_2 = T_1 T_2$
$f_{n+1} = (n f_n - 1) T_2$
$\varphi(f_n) = \frac{1}{n}$.

Then simply let $I = \ker \varphi$ and we have $\mathbb{Q} \simeq B/I = \operatorname{Im} \varphi$.

Note that not only the condition (d), but also the conditions (a) and (b) of Conjecture 1.3 are satisfied in this case. However, (c) is far from being true. Similarly, this example can be modified to give counterexamples to versions of Conjecture 1.3 with other conditions omitted.

It is also trivial to observe that the homomorphism φ cannot be extended to A: If $\psi : A \twoheadrightarrow \mathbb{Q}$ was such an extension, then we would have

$$\frac{1}{n+1} = \psi(f_{n+1}) = \psi(n f_n - 1)\psi(T_2) = (n\psi(f_n) - 1)\psi(T_2) = 0,$$

a contradiction.

A similar construction works generally (for other fields of finite transcendence degree over $\mathbb{Q}$ or $\mathbb{F}_p$). However, the proof given in [1] is not very elementary, it uses local rings, blow-ups, etc. It is an interesting question whether it is possible to give an elementary proof.

Details are given in the first three sections of [1], especially see Proposition 3.1.

3. Outline of the proof

In this section we prove the following Theorem 3.1. Along the way we collect and review various useful properties of semifields extending and generalizing [7].

Theorem 3.1. *Conjecture* 1.3 *implies Conjecture* 1.2.

Throughout the rest of this section we will assume that Conjecture 1.2 does not hold and construct a counterexample to Conjecture 1.3. Let us start by recalling a few basic definitions and facts on semifields.

Suppose that S is a semifield which is n-generated as a semiring and not additively idempotent. Then it is not hard to see that $\mathbb{Q}^+ \subset S$ (see e.g. [10, Lemma 2.2]). Consider the natural pre-order on S defined by $a \leq b$ if $b = a + c$ for some $c \in S$ and let $P = \{s \in S | \exists q, r \in \mathbb{Q}^+ : q \leq s \leq r\}$. By [10, Proposition 3.11], P is an additively cancellative semifield, and so we can also define its difference ring $P - P$. Using these notions we now attach to S the objects from Conjecture 1.3:

Definition 3.2. Let $A = \mathbb{Z}[T_1, \ldots, T_n]$, $A^+ = \mathbb{N}[T_1, \ldots, T_n]$, and let $\varphi : A^+ \twoheadrightarrow S$ be the surjective semiring homomorphism that sends the variables T_i to the generators of S.

Let $B^+ = \varphi^{-1}(P) \subset A^+$, extend φ to $\varphi^\pm : B = B^+ - B^+ \twoheadrightarrow P - P$, and define $I = \ker \varphi^\pm$, an ideal of B.

Note that since P is additively cancellative, $\varphi^\pm$ is a well-defined surjective ring homomorphism. Thus we have constructed the objects from Conjecture 1.3 and just need to check they have all the required properties. Condition (d) is clear (since $\mathbb{Q}^+ \subset P$) and (b) follows easily.

Proposition 3.3. *Let $f, g \in A^+$. If $\varphi(f) = \varphi(g)$ then $f - g \in IA$.*
Therefore $IA = A$.

Proof: S is a semifield, and so there is $h \in A^+$ such that $\varphi(gh) = 1$. Then also $\varphi(fh) = 1$ and $f - g = (1 - gh)f + (fh - 1)g \in IA$.

Now by [10, Proposition 3.14], there is an $\ell \in A^+$ such that $\varphi(\ell) + 1 = \varphi(\ell)$. Then $\varphi(\ell + 1) = \varphi(\ell)$, and so by the first part, $1 = (\ell + 1) - \ell \in IA$.

Since IA is an ideal in A, we have $IA = A$. □

To prove (a) and (c), we need to consider a certain subsemiring Q of S and its properties.

Theorem 3.4 (Properties of Q, summary of various statements from [7] and [10])**.** *Let $Q = \{s \in S | \exists q \in \mathbb{Q}^+ : s \leq q\}$. Then the following hold.*

(a) *If $a_1 + \cdots + a_n \in Q$, then $a_i \in Q$ for each i. Hence $\varphi^{-1}(A)$ is generated by monomials as an additive semigroup.*

(b) *$a \in Q$ if and only if $qA \in Q$ for all $q \in \mathbb{Q}^+$.*

(c) *$Q + \mathbb{Q}^+ = P$.*

Let $\mathcal{C}$ be the "cone" of Q, $\mathcal{C} = \{(u_1, \ldots, u_n) \in \mathbb{N}_0^n | \varphi(T_1^{u_1} \cdots T_n^{u_n}) \in Q\} \subset \mathbb{N}_0^n$. (If $u = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$, we sometimes write just $T^u := T_1^{u_1} \cdots T_n^{u_n}$.)

(d) *$\mathcal{C}$ is a pure semigroup, i.e., if $a \in \mathcal{C}$, $k \in \mathbb{N}$ and $a/k \in \mathbb{N}_0^n$, then $a/k \in \mathcal{C}$.*

Definition 3.5. Let dim $\mathcal{C}$ denote the smallest dimension of a linear subspace of $\mathbb{R}^n$ which contains $\mathcal{C}$.

Lemma 3.6. (a) *$\dim \mathcal{C} = n$.*

(b) *There exists $u \in \mathcal{C}$ s.t. $u + (1, 0, \ldots, 0)$, $u + (0, 1, 0, \ldots, 0), \ldots$, $u + (0, \ldots, 0, 1) \in \mathcal{C}$.*

Proof: Take $f = T_1 + \cdots + T_n$ and let $g \in A^+$ be such that $\varphi(fg) = 1$. Write $g = \sum c_i T^{u^{(i)}}$, where $c_i \in \mathbb{N}, u^{(i)} \in \mathbb{N}_0^n$. Thus $\varphi(fg) \in Q$, and so (by Theorem 3.4(a)) $u^{(1)} + (1, 0, \ldots, 0)$, $u^{(1)} + (0, 1, 0, \ldots, 0), \ldots, u^{(1)} + (0, \ldots, 0, 1)$ are n linearly independent vectors in $\mathcal{C}$. Hence $\dim \mathcal{C} = n$. □

Lemma 3.7. *If $u \in \mathcal{C}$, then $\varphi(1 + T^u) \in P$.*

Proof: This follows just from Theorem 3.4(c). □

Now we are ready to show that the condition (a) of Conjecture 1.3 is satisfied.

Proposition 3.8. *$QF(B) = \mathbb{Q}(T_1, \ldots, T_n)$.*

Proof: By Lemma 3.7 we have $1 + T^u \in B^+$ for all $u \in \mathcal{C}$. Since also $1 \in B^+$, we see that $T^u \in B$ for all $u \in \mathcal{C}$.

By Lemma 3.6(b) we have $u+(1, 0, \ldots, 0), u+(0, 1, 0, \ldots, 0), \ldots, u+(0, \ldots, 0, 1) \in \mathcal{C}$ for some u. Thus $T^{\text{any of these vectors}} \in B$. Since also $T^u \in B$, we see that $QF(B) \ni T_1 = T^{(1,0,\ldots,0)} = \frac{T^{u+(1,0,\ldots,0)}}{T^u}$. Similarly we see that all other generators $T_i \in QF(B)$, concluding the proof. □

It remains only to show the condition (c).

Proposition 3.9. *There is $\ell_0 \in A^+$ such that for all $a \in A^+$ and all $\ell = \ell_0 + a \in A$ we have: if $\ell = f/g$ for $f, g \in B$, then $f, g \in I$.*

More generally, let ℓ be as above. If $h(\ell) = 0$ for $h(X) \in B[X]$, then $h(X) \in I[X]$.

Proof: Consider $L = \{\ell \in A^+ | \varphi(\ell) + 1 = \varphi(\ell)\}$. L is non-empty by [10, Proposition 3.14]. Clearly $L + A^+ \subset L$. Hence if we take $\ell_0 \in L$, then every $\ell = \ell_0 + a$ (for $a \in A^+$) lies in L. Also note that $\varphi(\ell) + p = \varphi(\ell)$ for all $\ell \in L$ and $p \in P$.

Take now any $\ell \in L$ and assume that $\ell = f/g$ for some $f, g \in B$ (note that by Proposition 3.8 such f, g exist for each ℓ). We have $f, g \in B$, so there are $f_1, f_2, g_1, g_2 \in B^+$ such that $f = f_1 - f_2, g = g_1 - g_2$. Then $\ell g_1 + f_2 = \ell g_2 + f_1$.

Since $\ell \in L$ and $\varphi(f_i), \varphi(g_i) \in P$, we have $\varphi(\ell g_1 + f_2) = \varphi(\ell g_1)$ and $\varphi(\ell g_2 + f_1) = \varphi(\ell g_2)$. Hence $\varphi(\ell g_1) = \varphi(\ell g_2)$, and so $\varphi(g_1) = \varphi(g_2)$. But then also $\varphi(f_1) = \varphi(f_2)$.

Hence $f, g \in I$ as needed.

Proof of the second part is essentially the same. Write $h = f - g$ with $f, g \in B^+[X]$. Then $\varphi(f(\ell)) = \varphi(g(\ell))$. As before, this implies that we can remove the constant terms from the equality and divide by ℓ. We get a new equality of polynomials of the same form and we can proceed inductively till we get that the $\varphi(f), \varphi(g)$ have the same degree and equal leading coefficients. Then we can again proceed inductively and show that in fact all coefficients of $\varphi(f), \varphi(g)$ are equal, which means that $\varphi(f) - \varphi(g) = 0$, and so $h = f - g \in I[X]$. □

References

[1] Abhyankar S.S., *Pillars and towers of quadratic transformations*, Proc. Amer. Math. Soc. **139** (2011), 3067–3082.

[2] El Bashir R., Hurt J., Jančařík A., Kepka T., *Simple commutative semirings*, J. Algebra **236** (2001), 277–306.

[3] Busaniche M., Cabrer L., Mundici D., *Confluence and combinatorics in finitely generated unital lattice-ordered abelian groups*, Forum Math. **24** (2012), 253–271.

[4] Di Nola A., Gerla B., *Algebras of Lukasiewicz's logic and their semiring reducts*, Contemp. Math. **377** (2005), 131–144.

[5] Di Nola A., Lettieri A., *Perfect MV-algebras are categorically equivalent to abelian ℓ-groups*, Studia Logica **53** (1994), 417–432.

[6] Golan J.S., *Semirings and Their Applications*, Kluwer Academic, Dordrecht, 1999.

[7] Ježek J., Kala V., Kepka T., *Finitely generated algebraic structures with various divisibility conditions*, Forum Math. **24** (2012), 379–397.

[8] Kala V., *Lattice-ordered groups finitely generated as semirings*, J. Commut. Alg., to appear, 16 pp., `arxiv:1502.01651`.

[9] Kala V., Kepka T., *A note on finitely generated ideal-simple commutative semirings*, Comment. Math. Univ. Carolin. **49** (2008), 1–9.

[10] Kala V., Kepka T., Korbelář M., *Notes on commutative parasemifields*, Comment. Math. Univ. Carolin. **50** (2009), 521–533.

[11] Kala V., Korbelář M., *Idempotence of commutative semifields*, preprint, 16 pp.

[12] Kepka T., Korbelář M., *Conjectures on additively divisible commutative semirings*, Math. Slovaca **66** (2016), 1059–1064.

[13] Korbelář M., Landsmann G., *One-generated semirings and additive divisibility*, J. Algebra Appl. **16** (2017), 1750038, 22 pp., DOI: 10.1142/S0219498817500384

[14] Korbelář M., *Torsion and divisibility in finitely generated commutative semirings*, Semigroup Forum, to appear; DOI: 10.1007/s00233-016-9827-4

[15] Leichtnam E., *A classification of the commutative Banach perfect semi-fields of characteristic 1. Applications*, to appear in Math. Ann., DOI: 10.1007/s00208-017-1527-1.

[16] Litvinov G.L., *The Maslov dequantization, idempotent and tropical mathematics: a brief introduction*, `arXiv:math/0507014`.

[17] Monico C.J., *Semirings and semigroup actions in public-key cryptography*, PhD Thesis, University of Notre Dame, USA, 2002.

[18] Mundici D., *Interpretation of AF C^*-algebras in Łukasiewicz sentential calculus*, J. Funct. Anal. **65** (1986), 15–63.

[19] Weinert H.J., *Über Halbringe und Halbkörper I*, Acta Math. Acad. Sci. Hungar. **13** (1962), 365–378.

[20] Weinert H.J., Wiegandt R., *On the structure of semifields and lattice-ordered groups*, Period. Math. Hungar. **32** (1996), 147–162.
[21] Zumbrägel J., *Public-key cryptography based on simple semirings*, PhD Thesis, Universität Zürich, Switzerland, 2008.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Praha 8, Czech Republic

Universität Göttingen, Mathematisches Institut, Bunsenstrasse 3-5, 37073 Göttingen, Germany

E-mail: vita.kala@gmail.com

(*Received* March 13, 2017, *revised* May 16, 2017)