Algebraic conditions for additive functions over the reals and over finite fields

Péter Kutas
Institute for Computer Science and Control, Hungarian Acad. Sci.
kutasp@sztaki.hu

Wednesday 30th August, 2017

Abstract

Let C be an affine plane curve. We consider additive functions $f : K \to K$ for which $f(x)f(y) = 0$, whenever $(x, y) \in C$. We show that if $K = \mathbb{R}$ and C is the hyperbola with defining equation $xy = 1$, then there exist nonzero additive functions with this property. Moreover, we show that such a nonzero f exists for a field K if and only if K is transcendental over $\mathbb{Q}$ or over $\mathbb{F}_p$, the finite field with p elements. We also consider the general question when K is a finite field. We show that if the degree of the curve C is large enough compared to the characteristic of K, then f must be identically zero.

Keywords: Additive functions, Valuation Rings, Finite fields.

Mathematics Subject Classification: 39B22, 39B52, 11G20.

1 Introduction

Let K be field. A function $f : K \to K$ is additive if

$$f(x + y) = f(x) + f(y)$$

holds for every $x, y \in K$. If the characteristic of K is zero then an additive function is also $\mathbb{Q}$-linear [10, Theorem 5.2.1]. For further information on additive functions (and functional equations in general) the reader is referred to [10].

It is well-known that if $K = \mathbb{R}$ then every continuous additive function $f : \mathbb{R} \to \mathbb{R}$ is of the form $f(x) = f(1)x$. However, there exist non-continuous additive functions which behave quite irregularly. Most prominently their graph is dense in the plane. Many similar theorems can be found in [10], however most are of analytic flavour.

The following more algebraic question was posed by Gy. Szabó [12] (motivated by a question of W. Benz [2]): Let $C : x^2 + y^2 = 1$ be the unit circle and suppose that $f : \mathbb{R} \to \mathbb{R}$ is additive and $f(x)f(y) = 0$ whenever $(x, y) \in C$. Does this imply that f is identically zero? The solution was published in a paper [9] by Z. Kominek, L. Reich and J. Schwaiger, where the authors prove that the implication is true. In the same paper the authors also consider different curves (instead of the unit circle), curves of the form $y = p(x)$, where p is a polynomial with rational

coefficients, and the hyperbola $x^2 - y^2 = 1$. In the paper [5] the curves $x^2 - ny^2 = 1$ (where n is a square-free positive integer) are studied. In all cases, the implication that f is identically zero turned out to be true. Moreover, Z. Boros and W. Fechner generalized the unit circle problem to generalized polynomials [4] and in [5] a stability version of the problem is examined. In [5] the case when the curve is $C : xy = 1$ was left open. These previous results suggested that such an f must be identically zero as well.

Another motivation to study this problem comes from the following results. Let f be an additive function such that $f(x)f(\frac{1}{x}) = b$, where b is fixed. If b is negative, then no such function exists. If b is positive, then one can show that f must be continuous [8, Chapter I], thus only the case $b = 0$ was not known before. Interestingly, there exists a non-continuous additive f, for which $f(x)f(\frac{1}{x}) > 0$ for every nonzero x [1], [3].

One of the main results of this paper is that surprisingly there exists an additive $f : \mathbb{R} \to \mathbb{R}$ such that $f(x)f(\frac{1}{x}) = 0$ (when $x \neq 0$) which is not identically zero on $\mathbb{R}$. The example uses the theory of valuations of fields. Moreover, with this technique, we are able to construct a family of curves C, for which the above implication is false.

We also consider the general problem over finite fields. Let C be an absolutely irreducible smooth curve and let $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be an additive function such that $f(x)f(y) = 0$ whenever $(x, y) \in C$. In this setting we are able to prove more general results. Using the classical Hasse-Weil bound on the number of points of a smooth absolutely irreducible curve defined over a finite field, we are able to show that if the degree of the curve is small compared to the characteristic of the field, then f must be identically zero. Our approach can be applied to higher dimensional varieties as well.

The structure of the paper is the following. Section 2 is devoted to preliminaries, it does not contain any new results. We recall basic facts of valuation theory and the Hasse-Weil theorem. Section 3 is devoted to the finite field case, whilst in Section 4 we study the problem over the real numbers.

2 Preliminaries

This section is divided into two subsections. In the first subsection we define some notions and state some theorems concerning algebraic curves over finite fields. In the second subsection, we introduce the concept of valuations of fields.

2.1 Curves over finite fields

The theory of algebraic curves is a vast topic, therefore this subsection is not meant to be a thorough introduction (for more details the reader is referred to [7]). Our goal is to establish a bound on the number of points over a finite field, of a smooth projective curve.

Definition 1. *Let K be a field. An affine (resp. projective) plane curve is an affine (resp. projective) variety of dimension one in $\overline{K}^2$ (resp $\mathbb{P}\overline{K}^2$). Here $\overline{K}$ denotes the algebraic closure of K, and $\mathbb{P}\overline{K}^2$ denotes the projective plane over $\overline{K}$.*

Remark 2. Informally one can think of the following. An affine plane curve (defined over K) is the zero set of an irreducible polynomial $f \in K[x, y]$ in $\overline{K}^2$. A projective plane curve is the zero set of an irreducible homogeneous polynomial $g \in K[x, y, z]$ in $\mathbb{P}\overline{K}^2$, where $\mathbb{P}\overline{K}^2$ denotes the projective plane (over $\overline{K}$).

In this paper we will consider affine curves, however certain theorems are stated in terms of projective curves.

Our main goal is to give a bound on the number of points of a smooth, absolutely irreducible curve. We do not define these notions here, as we will not use their definition. It is enough to note that this is a large (and the most interesting) class of affine curves. For further details the reader is referred to [7]. The bound contains a quantity called the genus of the curve. We do not define the genus here (as it is quite complicated and we do not use it later), the reader is referred to [7, Section 8.3]. We recall the well-known Hasse-Weil theorem [14]:

Fact 3 (Hasse-Weil)**.** *Let p be a prime number and let C be a smooth absolutely irreducible projective curve defined over the finite field $\mathbb{F}_{p^k}$. Let $N(C)$ be the number of points of C in $\mathbb{F}_{p^k}$ and let g be the genus of the curve. Then the following inequality holds:*

$$|N(C) - p^k - 1| \leq 2gp^{\frac{k}{2}}.$$

Fortunately, the genus of the curve can be bounded using the degree of the curve (the degree of its defining polynomial) [6, Section 8.3, Corollary 1]:

Fact 4. *Let C be a smooth projective curve of degree d. Than its genus g satisfies the inequality*

$$g \leq \frac{(d-1)(d-2)}{2}.$$

We conclude the subsection by a fact (which is a consequence of Bézout's theorem [7, Section 5.3]):

Fact 5. *Let C_1 and C_2 be projective curves defined over a field K of degree d_1 and d_2 respectively. Then C_1 and C_2 intersect in at most $d_1 d_2$ points.*

Remark 6. Actually counting multiplicities they intersect in exactly $d_1 d_2$ points over algebraically closed fields.

This fact will be useful for us as we later need a bound on the number of affine points of a smooth curve.

2.2 Valuations

This subsection is based on [6, Chapter 2 and 3]. We define the notion of valuations of a field and state a theorem of Chevalley, about the extensions of valuations. First we recall the notion of an ordered abelian group.

Definition 7. *An abelian group $(\Gamma, +, 0)$ together with a binary relation $\leq$ is called* ordered *if the following conditions hold for all $\gamma, \delta, \lambda \in \Gamma$:*

1. *$\gamma \leq \gamma$,*
2. *if $\gamma \leq \delta$ and $\delta \leq \gamma$ then $\gamma = \delta$,*
3. *if $\gamma \leq \delta$ and $\delta \leq \lambda$ then $\gamma \leq \lambda$,*
4. *either $\gamma \leq \delta$ or $\delta \leq \gamma$,*
5. *$\gamma \leq \delta$ implies that $\gamma + \lambda \leq \delta + \lambda$.*

Example 8. The real numbers with respect to addition form an ordered abelian group.

Definition 9. *Let K be a field and let Γ be an ordered abelian group. Let ∞ be a symbol for which $\infty \geq x$ holds for every $x \in \Gamma$. Then a valuation on K is a function $v : K \to \Gamma \cup \{\infty\}$ with the following properties:*

1. *$v(x) = \infty$ if and only if $x = 0$,*
2. *$v(xy) = v(x) + v(y)$,*
3. *$v(x + y) \geq min(v(x), v(y))$.*

Example 10.

- Every field has the trivial valuation, where $v(x) = 0$, whenever $x \neq 0$.
- Let $K = \mathbb{Q}(t)$, the field of rational functions over $\mathbb{Q}$. Let $f, g \in \mathbb{Q}[t]$. Then
$$v(\frac{f}{g}) = deg(g) - deg(f)$$
is a valuation (the degree of the zero polynomial is $-\infty$).
- Let $K = \mathbb{Q}$ and let p be a prime number. Then every rational number $\frac{a}{b}$ can be written in a form $p^k \frac{a'}{b'}$, where a' and b' are no longer divisible by p. Then $v(\frac{a}{b}) = k$ is a valuation on $\mathbb{Q}$, called the p-adic valuation.

Valuations are a key concept in algebraic number theory. We only need a fraction of the theory. First we observe that elements with nonnegative valuation form a subring with a special property:

Proposition 11. *Let K be a field and let v be a valuation on K. Let $O = \{x \in K | v(x) \geq 0\}$. Then O has the following two properties:*

1. *O is a subring of K.*
2. *For every nonzero element $x \in K$, either x or $\frac{1}{x}$ is in O.*

Proof. We have to show that O is closed under addition and multiplication. Let $x, y \in O$. The second property of a valuation implies that $v(x + y) \geq min(v(x), v(y)) \geq 0$, which proves that O is closed under addition. By the third property of a valuation $v(xy) = v(x) + v(y) \geq 0$, hence O is closed under multiplication. The second part of the statement follows again from the third property. □

This motivates the following definition:

Definition 12. *Let K be a field. Then a subring O is a valuation ring if for every nonzero element $x \in K$ either x or $\frac{1}{x}$ is in O.*

Valuation rings always correspond to valuations, i.e., if O is a valuation ring of K then there exists a valuation on K, such that O consists of those elements whose valuation is nonnegative [6, Proposition 2.1.2]. Valuation rings have a unique maximal ideal (the elements whose valuation is positive). Now we state Chevalley's theorem [6, Theorem 3.1.1.]:

Fact 13 (Chevalley)**.** *Let K be a field and let R be a subring of K with a prime ideal P. Then there exists a valuation ring O of K with maximal ideal M such that $R \subset O$ and $M \cap R = P$.*

A corollary of Fact 13 is that a valuation on a smaller field can be extended to a larger field (however, the value group may grow):

Fact 14. *Let K be a field with a valuation v and let L be an extension of K. Then there exists a valuation w on L such that w restricted to K is v.*

3 Additive functions and curves over finite fields

Throughout the section let p be an odd prime number. We consider additive functions in finite fields with the following property. Let C be a smooth absolutely irreducible curve defined over F_{p^k}. Let f be an additive function on $\mathbb{F}_{p^k}$ such that $f(x)f(y) = 0$ whenever $(x, y) \in C$. The question is whether there exists an f with this property which is not identically zero. First we make some basic observations.

Proposition 15. *Let $\mathbb{F}_{p^k}$ be the finite field with p^k elements, where p is an odd prime. Then an additive function $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ is also an $\mathbb{F}_p$-linear function.*

Proof. We have to show that $f(\lambda x) = \lambda f(x)$, whenever $\lambda \in F_p$. The elements of $\mathbb{F}_p$ can be represented by the residues modulo p, i.e., by the set $\{0, 1, \ldots, p-1\}$. We prove our claim by induction. By the additive property of f we have that $f(0) = f(0) + f(0)$, hence $f(0) = 0$. Thus for $\lambda = 0$ or $\lambda = 1$ we are done. Assume the claim is true for λ, we show it is true for $\lambda + 1$.

$$f((\lambda+1)x) = f(\lambda x + x) = f(\lambda x) + f(x) = \lambda f(x) + f(x) = (\lambda+1)f(x).$$

Thus by induction we are done. □

Remark 16. An easy consequence of this is that the set $H = \{x \in \mathbb{F}_{p^k} |\ f(x) = 0\}$ is an $\mathbb{F}_p$-subspace.

Before we state our main theorem we give a short remark on the number of affine points of a curve.

Remark 17. Assume the curve C has degree d. If one is interested in the number of affine points then one has to subtract d from the lower bound. Indeed, projective points lie on a line, and a line and a degree d curve intersect in at most d points by Fact 5.

Now we are ready to state the main theorem of this section:

Theorem 18. *Let C be a smooth absolutely irreducible affine curve of degree d defined over $\mathbb{F}_{p^k}$. Assume that the following inequality holds:*

$$\frac{p^k + 1 - (d-1)(d-2)p^{\frac{k}{2}} - d}{d} > 2p^{k-1}. \tag{1}$$

Then an additive function $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ for which $f(x)f(y) = 0$ whenever $(x, y) \in C$, is identically zero.

Proof. Consider the following bipartite graph G. The two independent sets S and T are each labelled with the elements of the finite field $\mathbb{F}_{p^k}$. An edge goes from a vertex x to the vertex y in the opposite set if and only if the point (x, y) lies on the curve C. Observe that the number of edges of G is just the number of affine points of C. Since C has degree d, every vertex has degree at most d. The vertices of G corresponding to elements $x \in F_{p^k}$ for which $f(x) = 0$ must cover all the edges of G, otherwise there would be an x and a y such that $f(x)f(y) \neq 0$. Let m be the number of edges of G. Since the degree of every vertex is at most d, one needs at least m/d vertices for covering all the edges of G. As we have noted, the vertices corresponding to elements $x \in \mathbb{F}_{p^k}$ for which $f(x) = 0$ cover all the edges. The number of this vertices is exactly two times the cardinality of the set $H = \{x \in \mathbb{F}_{p^k} | f(x) = 0\}$. Inequality 1 and Fact 3 together imply (considering Remark 17) that the cardinality of H is larger than p^{k-1}. Remark 16 states that H is an $\mathbb{F}_p$-subspace. Since the only $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^k}$ consisting of more than p^{k-1} elements is $\mathbb{F}_{p^k}$ itself, f must be identically zero. □

Remark 19. We conjecture that the 2 on the right hand side of Inequality 1 can be omitted by a more clever construction of the graph G.

The theorem says that if the characteristic of the finite field is large enough compared to the degree of the curve then f must identically zero. For two interesting classes of curves (conics and elliptic curves) we apply Theorem 18 to provide explicit bounds. For the theory of elliptic curves the reader is referred to [11].

Corollary 20. *Let $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be an additive function and let C be a smooth curve. Assume that $f(x)f(y) = 0$ whenever $(x, y) \in C$.*

1. *If C is a conic and $p \geq 5$ then f must be identically zero.*
2. *Let C be an elliptic curve. Then f must be identically zero if one of the following holds:*
   - $p > 13$,
   - $p = 7$ *and* $k > 2$,
   - $p = 11$ *or* $p = 13$ *and* $k > 1$.

Proof. If C is a conic than it has degree 2 and at least $p^k - 1$ points. Thus we have to examine when $\frac{p^k-1}{2} > 2p^{k-1}$ holds. This is equivalent to the inequality

$$p^k - 1 > 4p^{k-1}$$

which holds if $p \geq 5$.

If C is an elliptic curve then we note first that it always has exactly 1 point at infinity. Thus we have to examine when the inequality $\frac{p^k-2p^{\frac{k}{2}}}{3} > 2p^{k-1}$ holds. By rearranging we obtain the inequality

$$(p-6)p^{k-1} - 2\sqrt{p}p^{\frac{k-1}{2}} > 0.$$

If $p - 6 > 2\sqrt{p}$ then the inequality hold for every k since $p^{k-1} \geq p^{\frac{k-1}{2}}$. Since $p - 6 - 2\sqrt{p}$ is a quadratic polynomial in $\sqrt{p}$ it is easy to see that if $p > 13$ then this condition is satisfied. If $p = 7$, then we have to look at $(7-6)7^{k-1} - 2\sqrt{7}p^{\frac{k-1}{2}}$. This will be positive if $7^{\frac{k-1}{2}} > 2\sqrt{7}$ which happens if $k > 2$. A similar calculation shows that if $p = 11$ or $p = 13$ then $k > 1$ suffices. □

Remark 21. We show two examples, when the above conditions are not satisfied and f is not identically zero.

First consider the curve defined over $\mathbb{F}_3$:

$$C : y^2 + 2xy + 2y + x = 0.$$

It is easy to check that it has 2 affine points: $(0, 0)$ and $(0, 1)$. There $f(x) = x$ satisfies the condition and is nonzero.

Now we give an example of an elliptic curve over $\mathbb{F}_5$ for which f can be chosen to be nonzero:

$$C : y^2 = x^3 + 3x + 1.$$

C has three affine points:$(0, 1)$, $(0, 4)$ and $(1, 0)$. Thus $f(x) = x$ is again a suitable choice.

These do not exactly show the tightness of the bounds. However, if the conjecture in Remark 19 is true, then we cannot expect much better examples.

In this section we considered curves, where the degree of the curve is small compared to the characteristic of the field. It would be interesting to study curves where the degree is large compared to the characteristic of the field. Also, it would be even more interesting (and probably not hopeless) to give a complete characterization of those absolutely irreducible smooth curves C for which there exists an additive function $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ such that f is nonzero and $f(x)f(y) = 0$ whenever $(x, y) \in C$. We leave these as open problems.

3.1 Generalizations

One can consider several related problems. The most natural continuation is to ask the following:

Problem 1. *Let $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be an additive function. Let S be an absolutely irreducible smooth surface defined over $\mathbb{F}_{p^k}$. Assume that $f(x)f(y)f(z) = 0$ whenever $(x, y, z) \in S$. Does this imply that f is identically zero?*

The problem can be tackled using the method of Theorem 18. Assume that f is not identically zero, thus there exists an $s \in \mathbb{F}_{p^k}$ such that $f(s) \neq 0$. Now by substituting s into z (or one of the other two variables) we obtain an absolutely irreducible curve (which is smooth) C for which $f(x)f(y) = 0$ if $(x, y) \in C$. If the degree of S was d then the degree of C is at most $\left\lfloor \frac{2d}{3} \right\rfloor$ (by choosing the variable to be substituted in a suitable way). We have obtained the following:

Proposition 22. *Let S be an absolutely irreducible smooth surface of degree d. Let $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be an additive function with the property that $f(x)f(y)f(z) = 0$ whenever $(x, y, z) \in S$. Assume the degree of S is fixed. Then if p is large enough compared to d then f is identically zero.*

Proof. The proof follows from the previous discussion and Theorem 18. □

Similar results can be obtained if we consider smooth varieties of arbitrary (bounded) dimension. Another natural question is the following:

Problem 2. *Let $f : \mathbb{F}_{p^k}^2 \to \mathbb{F}_{p^k}^2$ be an $\mathbb{F}_p$-linear function. Let H be a hypersurface in $\mathbb{F}_{p^k}^4$. Assume that $f(x, y)f(u, v) = 0$ whenever $(x, y, u, v) \in H$. Does this imply that f is identically zero?*

This problem is harder than the previous one and it seems that it cannot be tackled with the above machinery. We leave it as an open problem here.

4 The equation over $\mathbb{R}$

We turn our attention to the curve $C : xy = 1$. In other words we consider additive functions $f : \mathbb{R} \to \mathbb{R}$ for which $f(x)f(\frac{1}{x}) = 0$ (if $x \neq 0$). We show that surprisingly there exists a nonzero additive function with this property. We start with an observation:

Proposition 23. *There exists an additive function $f : \mathbb{R} \to \mathbb{R}$ with the property that $f(x)f(\frac{1}{x}) = 0$ (where $x \neq 0$) if and only if there exists a $\mathbb{Q}$-subspace U of the real numbers such that for every real number x either x or $\frac{1}{x}$ is in U.*

Proof. If f is an additive function with this property, then the set $U = \{x \in \mathbb{R} | f(x) = 0\}$ will suffice. Now consider the reverse direction. Assume such a U is given. Then there exists a Hamel-basis of U which can be extended to a Hamel-basis of $\mathbb{R}$. We set the value of those basis elements to zero which belong to U and all the other values to 1. This shows that f is nonzero and has the desired property. □

Now we give a construction of a nonzero additive function f for which $f(x)f(\frac{1}{x}) = 0$.

Theorem 24. *There exists a non identically zero additive function $f : \mathbb{R} \to \mathbb{R}$ for which $f(x)f(\frac{1}{x}) = 0$ (whenever $x \neq 0$).*

Proof. Let α be a transcendent number over $\mathbb{Q}$. Consider the field $K = \mathbb{Q}(\alpha)$, the field extension of the rational numbers by α. The field K is isomorphic to the field $\mathbb{Q}(t)$, the field of rational functions in one variable. Hence every element of K is the quotient of two polynomials in α and we can define a valuation on K in a similar fashion as in Example 10. Every element of K is a quotient of two polynomials in α thus the valuation is defined as the difference of the degree of the denominator and the numerator. This is well-defined as α is transcendental over $\mathbb{Q}$. This valuation is zero on $\mathbb{Q}$, but nontrivial on K. By Fact 14 the valuation on K can be extended to a valuation w on $\mathbb{R}$. Let O be the valuation ring of w. Then O is a $\mathbb{Q}$-subspace by Proposition 11 and by the fact that the valuation w is zero on $\mathbb{Q}$. Proposition 11 implies that for every nonzero $x \in \mathbb{R}$ either x or $\frac{1}{x}$ is in O. Now Proposition 23 implies the existence of a suitable f. □

Remark 25. Instead of applying Fact 14, Chevalley's theorem (Fact 13) can be applied directly as well. Indeed, let α be a transcendent real number and let S be the set of those numbers in $\mathbb{Q}(\alpha)$ which are rational functions in α with the property that the degree of the denominator is at least as big as the degree of the numerator. Let P be the prime ideal of S consisting of those rational functions in α where the degree of the denominator is strictly larger than the degree of the numerator. Chevalley's theorem states that in this case there exists a valuation ring O of $\mathbb{R}$ which contains S. Thus O satisfies the conditions of Proposition 23 since $\mathbb{Q}$ is contained in S

Remark 26. The valuation described in the proof of Theorem 24 can be constructed explicitly as well. Take a transcendence basis B of $\mathbb{R}$ over $\mathbb{Q}$. Now $\mathbb{R}$ is an algebraic (but not finite) extension of the purely transcendental extension $\mathbb{Q}(B)$. A valuation similar to the degree valuation described in the proof of Theorem 24 (and in Example 10) can be defined on $\mathbb{Q}(B)$ as on $\mathbb{Q}(\alpha)$ (as the elements of $\mathbb{Q}(B)$ are rational functions in infinitely many variables). Finally, there exists a standard procedure to extend valuations to algebraic extensions (see [6]).

The proof also implies that instead of $\mathbb{R}$ any field F which is transcendental over $\mathbb{Q}$ has a nonzero additive function $f : F \to F$ satisfying the property that $f(x)f(\frac{1}{x}) = 0$. Similarly one can show that every field which is transcendental over $\mathbb{F}_p$ has an additive function with the same property. On the other hand Theorem 18 shows that if K is a finite field of odd characteristic then an additive function f satisfying $f(x)f(\frac{1}{x}) = 0$ must be identically 0. This implies that if K is the algebraic closure of a finite field of odd characteristic then such an additive f must be identically zero on K (as finite extensions of finite fields are finite fields also). Thus in the odd characteristic case (let p be the characteristic) one has that an additive function f with the property that $f(x)f(\frac{1}{x}) = 0$ must be identically zero on a field K if and only if K is algebraic over $\mathbb{F}_p$. The next proposition (due to Gábor Ivanyos) shows that the same is true when the characteristic of K is zero.

Proposition 27. *Let K be an algebraic number field and let $f : K \to K$ be an additive function such that for every $x \neq 0$ one has that $f(x)f(\frac{1}{x}) = 0$. Then f is identically zero.*

Proof. Let K be a number field of degree n over $\mathbb{Q}$. Assume that the kernel of f (i.e., the $\mathbb{Q}$-subspace of those $x \in K$ for which $f(x) = 0$) has dimension $l < n$ over $\mathbb{Q}$. We use induction on n. Note that the statement is trivially satisfied if $K = \mathbb{Q}$. Let $x \in K$ be an arbitrary element. We define the set H_x (where $x \in K$) in the following way:

$$H_x = \{k \in \mathbb{N} | f(x^k) = 0\}.$$

Thus H_x is a subset of the natural numbers. By Szemerédi's theorem [13] either H_x or its complement in $\mathbb{N}$ contains an arithmetic progression of length $l+1$ where every element is smaller than $g(l)$ a function depending only on l (meaning it does not depend on x). If H_x contains such an arithmetic progression, then there exists $k, d \in \mathbb{N}$ such that $x^k, x^{k+d}, \ldots, x^{k+ld}$ lie in the kernel of f. Since the dimension of the kernel is l, the elements $x^k, x^{k+d}, \ldots, x^{k+ld}$ are linearly dependent over $\mathbb{Q}$, i.e., there exist $a_0, \ldots, a_l$ rational numbers such that $a_0 x^k + \cdots + a_l x^{k+ld} = 0$. Dividing by x^k leads to

$$a_0 + a_1 x^d + \cdots + a_l x^{ld} = 0.$$

Thus x^d lies in a proper subfield of K. If the complement of H_x contains the arithmetic progression then $(\frac{1}{x})^d$ lies in a proper subfield of K, thus we can conclude that for all x we have that x^d lies in a proper subfield of K. The induction hypothesis implies that there exists a universal D, such that $f(x^D) = 0$ (we may choose $D = g(l)!$) for every $x \in K$.

The map f can be considered as a linear map from $\mathbb{Q}^n$ to $\mathbb{Q}^n$ (by identifying K with $\mathbb{Q}^n$ as a vector space over $\mathbb{Q}$). Consider the tensor product $\mathcal{A} = K \otimes_{\mathbb{Q}} \mathbb{C}$ which is isomorphic to $\mathbb{C}^n$ and contains K as a subfield. The map f extends to $\mathcal{A}$. Then $g : \mathcal{A} \to \mathcal{A}$ defined as $g(x) = f(x^D)$ is a polynomial function which is not identically zero, since the map $x \mapsto x^D$ is surjective and f is not identically zero. On the other hand it must vanish on K which cannot happen as a polynomial function with rational coefficients which vanishes on $\mathbb{Q}^n$ must be identically zero (meaning that each coordinate function must be the zero polynomial). This yields a contradiction. □

Remark 28. It would be interesting to find a proof for Proposition 27 which does not rely on Szemerédi's theorem on arithmetic progressions (maybe just using the fact that for every $x \in K$ there exists a positive integer k for which $f(x^k) = 0$).

Corollary 29. *Let $\overline{\mathbb{Q}}$ be the algebraic closure of the rational numbers. Let $f : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ be an additive function such that for every $x \neq 0$ one has that $f(x)f(\frac{1}{x}) = 0$. Then f is identically zero.*

Proof. Assume that there exists such an f which is not identically zero. Thus there exists an $\alpha \in \overline{\mathbb{Q}}$ such that $f(\alpha) \neq 0$. However, every element in $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$, thus $K = \mathbb{Q}(\alpha)$ is an algebraic number field. Restricting f to K would yield an additive function f' on K which contradicts Proposition 27. □

Now we provide some more curves C for which there exists a non-continuous additive function h such that $h(x)h(y) = 0$ whenever (x, y) lies on the curve C.

Proposition 30. *Let C be an affine curve given by the rational parametrization $C : (f(t), g(\frac{1}{t}))$, where $f, g \in \mathbb{Q}[x]$ are polynomials with rational coefficients. Then there exists a nonzero additive function $h : \mathbb{R} \to \mathbb{R}$ such that $h(x)h(y) = 0$, whenever $(x, y) \in C$.*

Proof. Let v be the valuation defined in Theorem 24. Let

$$f(t) = \sum_{i=0}^{n} a_i t^i,\ g(t) = \sum_{i=0}^{m} a_i t^{-i}.$$

Let O_v be the valuation ring of the valuation v. We set h to be identically zero on O_v and extend it to $\mathbb{R}$ in a fashion that it is not identically zero on $\mathbb{R}$. If $t \in O_v$ then so is $f(t)$ as O_v is a ring which contains $\mathbb{Q}$. If t is not contained in O_v then $\frac{1}{t} \in O_v$ thus $g(\frac{1}{t}) \in O_v$ hence $h(x)h(y) = 0$ whenever $(x, y) \in C$. □

Remark 31. A natural question is whether Proposition 30 holds if $f(x), g(x) \in \mathbb{Q}(x)$ are rational functions where the degree of f is at least zero and the degree of g is at most zero. The answer is negative, as the unit circle ($C : x^2 + y^2 = 1$) admits such a parametrization $C : (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$ but in [9] it is proven that such an h must be identically zero.

Remark 32. Actually the proof of Proposition 30 shows that the following stronger statement is true. Let $\mathcal{H}$ be the family of all those curves which can be parametrized as $(f(t), g(\frac{1}{t}))$. Then there exists a non-continuous additive function h such that $h(x)h(y) = 0$ whenever (x, y) lies on some curve $C \in \mathcal{H}$.

The results of the paper motivate certain questions. Proposition 30 provides a family of curves for which there exist non-continuous additive functions $h : \mathbb{R} \to \mathbb{R}$, where $h(x)h(y) = 0$ if (x, y) lies on the curve. This family include curves of arbitrarily large degree, however they are all rational curves, thus of genus 0. To our knowledge, for genus 1 curves (i.e., elliptic curves) nothing is known. This means that we have no example for an elliptic curve C for which such a nonzero h exists, or which implies that h must be identically zero. Another direction for future investigations could be to study the problem for quadratic functions instead of additive ones. Some investigations have been made in this area, see [5].

Acknowledgement The author would like to thank Zoltán Boros and Lajos Rónyai for their useful remarks and their constant support and also Gábor Ivanyos for helpful suggestions and providing the proof of Proposition 27. Research supported by the Hungarian National Research, Development and Innovation Office - NKFIH.

References

[1] W. Benz: Remark-P178R1, Aequationes Mathematicae, Volume 20, 304 (1980).

[2] W. Benz: Problem 5 in report of Meeting: The Twenty-seventh International Symposium on Functional Equations, Aequationes Mathematicae, Volume 39, 302 (1990).

[3] G. M. Bergman: Problem-P178S1, Aequationes Mathematicae, Volume 23, 312-313 (1981).

[4] Z. Boros, W. Fechner: An alternative equation for polynomial functions, Aequationes Mathematicae, Volume 89, 17-22 (2015).

[5] Z. Boros, W. Fechner, P. Kutas: A regularity condition for quadratic functions involving the unit circle, Publicationes Mathematicae-Debrecen 89.3, 297-306 (2016).

[6] J. A. Engler, A. Prestel: Valued fields; Springer Science and Business Media, 2005.

[7] W. Fulton: Algebraic curves; Université de Versailles, 2005.

[8] P. Kannappan: Functional equations and inequalities with applications; Springer Science and Business Media, 2009.

[9] Z. Kominek, L. Reich, J. Schwaiger: On additive functions fulfilling some additional condition, Sitzungsber. Abt. II 207, 35-42 (1998).

[10] M. Kuczma: Functional equations; John Wiley and Sons Ltd, 1968.

[11] J. H. Silverman: The arithmetic of elliptic curves; Vol. 106. Springer Science and Business Media, 2009.

[12] Gy. Szabó: Problem 20 in report of Meeting: The Thirtieth International Symposium on Functional Equations, Aequationes Mathematicae, Volume 46, 294 (1993).

[13] E. Szemerédi: On sets of integers containing no k elements in arithmetic progression, Acta Arithmetica, Volume 27, 299-345 (1975).

[14] A. Weil: Numbers of solutions of equations in finite fields, Bulletin of the American Mathematical Society, 55(5), 497-508 (1949).