ACTA ARITHMETICA
112.4 (2004)

Sums of values of a rational function

by

Bjorn Poonen (Berkeley, CA)

1. Introduction. Lagrange proved that every nonnegative integer is a sum of four integer squares. Waring claimed that for each $k \geq 1$, there exists $n \geq 1$ such that every nonnegative integer is a sum of n nonnegative kth powers. Hilbert proved this, and later the circle method was developed to give a simpler approach to this and other such questions. Analogues over number fields are known. There is also the easier problem which asks for representations of an integer as

$$\sum_{i=1}^{n} x_i^k - \sum_{i=n+1}^{n+n'} x_i^k$$

when n and n' are large relative to k. See the beginning of the book [Vau97] for an introduction to some of these problems.

Each of these results for integers implies its analogue for rational numbers. This paper studies what happens when the function $f(x) = x^k$ is replaced by an arbitrary rational function $f(x)$. The problem can be generalized further by considering number fields instead of $\mathbb{Q}$, but already over $\mathbb{Q}$ the problem seems very difficult (see Section 5).

Our two main theorems give partial answers to these questions:

Theorem 1.1. *Suppose K is a finite extension of $\mathbb{Q}$. Let $f \in K(x)$ be a nonconstant rational function with all poles in $K \cup \infty$. Then for $n \gg 1$ and all $c \in K$, there exist $x_1, \ldots, x_{2n} \in K - \{$poles of $f\}$ such that*

$$\sum_{i=1}^{n} f(x_i) - \sum_{i=n+1}^{2n} f(x_i) = c.$$

Theorem 1.2. *Keep the hypotheses of Theorem* 1.1 *and assume in addition that f has at most* 3 *poles*, *all of which are simple. Then for $n \gg 1$*

2000 *Mathematics Subject Classification*: Primary 11P05; Secondary 11D68.

Key words and phrases: Waring's Problem.

This research was supported by NSF grant DMS-9801104, and a Packard Fellowship.

and all $c \in K$, there exist $x_1, \dots, x_n \in K - \{$poles of $f\}$ such that

$$\sum_{i=1}^{n} f(x_i) = c.$$

Conjecture 1.3. Theorem 1.2 holds even for f having more than 3 poles, provided that all the poles are simple and in $K \cup \infty$.

To give a glimpse of the main ideas of the paper, let us sketch a proof of Theorem 1.1 in the case that $K = \mathbb{Q}$ and all poles of f are simple and in $\mathbb{Q}$. We will find a "generic" solution, that is, we will find $g_1, \dots, g_{n+n'} \in \mathbb{Q}(x)$ such that

$$\sum_{i=1}^{n} f(g_i(x)) - \sum_{i=n+1}^{n+n'} f(g_i(x)) = x.$$

Then by specializing x we can represent any rational number in the desired form. (Actually, a further trick is needed to force $n = n'$ and to represent the rational numbers at which the g_i have poles, but let us ignore these technicalities for now.) To find the g_i, we let

$$S := \Big\{ \sum_{i=1}^{n} f(g_i(x)) - \sum_{i=n+1}^{n+n'} f(g_i(x)) \,\Big|\, n, n' \geq 0,\ g_i \in \mathbb{Q}(x) \text{ and } \deg g_i = 1 \Big\} \subset \mathbb{Q}(x)$$

and let P_1 be the set of $\gamma \in S$ such that all poles of γ lie in $\mathbb{Z}$ (they are automatically simple). Each $\gamma \in P_1$ has the form

$$\gamma(x) = \sum_{i=1}^{s} \frac{a_i}{x - r_i} + b,$$

where the r_i are distinct integers, $a_i \in \mathbb{Q}^*$, and $b \in \mathbb{Q}$. The trick is to associate to γ the Laurent polynomial

$$\overline{\gamma} := \sum_{i=1}^{s} a_i T^{r_i} \in \mathbb{Q}[T, T^{-1}],$$

and let $M := \{\overline{\gamma} \mid \gamma \in P_1\}$ [1]. Clearly M is an additive subgroup of $\mathbb{Q}[T, T^{-1}]$; moreover, since the operations $\gamma(x) \mapsto \gamma(x \pm 1)$ map P_1 into itself, M is a $\mathbb{Z}[T, T^{-1}]$-submodule, and $\mathbb{Q} \cdot M$ is an ideal of $\mathbb{Q}[T, T^{-1}]$. With a little work, one shows that for each $\alpha \in \overline{\mathbb{Q}}^*$ there exists a Laurent polynomial in $\mathbb{Q} \cdot M$ not vanishing at α, so that by the Hilbert Nullstellensatz, $\mathbb{Q} \cdot M$ is the unit ideal. (Here we used the Nullstellensatz only for $\mathbb{A}^1 - \{0\}$, but when we prove our theorem for number fields other than $\mathbb{Q}$, we will apply it to

[1] A. Okounkov pointed out to me that up to some normalizations, $\overline{\gamma}(T)$ is the Fourier transform of $\gamma(x)$!

$(\mathbb{A}^1-\{0\})^n$.) The inclusion $1 \in \mathbb{Q}\cdot M$ means that some function $a/x+b$ with $a \neq 0$ belongs to S. Substituting the inverse fractional linear transformation into x shows that x itself belongs to S, completing the proof.

Remark 1.4. Without the assumption that the poles of f are in $K \cup \infty$, Theorems 1.1 and 1.2 can fail. See Section 5.

Question 1.5. Do Theorems 1.1 and 1.2 hold for arbitrary fields K? Probably both can fail.

We now outline the structure of the paper. Section 2 uses Hensel's Lemma to prove an analogous (but much easier) result over p-adic fields; this is not needed for the global results, but helps motivate the discussion in Section 5. Sections 3 and 4 prove Theorems 1.1 and 1.2, respectively. Section 5 raises questions about the number field case not yet addressed by our results. Finally, Section 6 discusses potential implications for diophantine definability.

2. Sums over p-adic fields

Proposition 2.1. *Suppose that $[K_v : \mathbb{Q}_p] < \infty$ for some finite prime p. Let $f \in K_v(x)$ be nonconstant. Then there exists $c \in K_v$ and an open additive subgroup G of K_v such that for all sufficiently large n,*

$$\{f(t_1)+\ldots+f(t_n) \mid t_1,\ldots,t_n \in K_v\} = nc+G.$$

Remark 2.2. The open additive subgroups of $\mathbb{Q}_p$ are $\mathbb{Q}_p$ and $p^n\mathbb{Z}_p$ for $n \in \mathbb{Z}$. For other local fields K_v, there are others, such as $\mathbb{Z}_p + p^n\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of K_v.

Proof of Proposition 2.1

Case 1: *f has a pole at some point $P \in \mathbb{P}^1(K_v)$.* Expand f in a Laurent series in a uniformizer t at P. Let ε be the coefficient of t^{-r}, where r is the order of the pole. By scaling f, we may assume that $\varepsilon = 1$. There is a power series $g = t + \ldots \in K_v[[t]]$ such that $g^{-r} = f$ and g converges for sufficiently small t. By Hensel's Lemma, the set of values taken by g on any neighborhood of 0 contains a neighborhood of 0. Thus every sufficiently large rth power in K_v is a value of f. Next we must show that there exists n such that any $\gamma \in K_v$ is a sum of large rth powers. To accomplish this, first use Hensel's Lemma to write $0 = \alpha_1^r + \ldots + \alpha_n^r$ for some $n \geq 1$ and $\alpha_1,\ldots,\alpha_n \in K_v^*$. Let $\beta_i = M\alpha_i$ for some $M \in K_v$ much larger than γ, and use Hensel's Lemma to replace β_1 by some $\widetilde{\beta}_1$ closer to β_1 than to 0, such that

$$\widetilde{\beta}_1^r + \beta_2^r + \ldots + \beta_n^r = \gamma.$$

Thus we may take $c = 0$ and $G = K_v$.

Case 2: *f has no poles in $\mathbb{P}^1(K_v)$.* Let $\mathcal{O}$ be the ring of integers in K_v, and let π be a uniformizer. Since f is nonconstant, there exists $\alpha \in K_v$ such that $f'(\alpha) \neq 0$. By Hensel's Lemma, $f(K_v)$ contains a neighborhood of $f(\alpha)$. By considering $f - f(\alpha)$ instead of f, we reduce to the case where $f(\alpha) = 0$. Now $f(K_v)$ contains an open subgroup $H := \pi^r\mathcal{O}$ for some $r \in \mathbb{Z}$. On the other hand, since f has no poles, compactness implies that $f(\mathbb{P}^1(K_v)) \subset \pi^R\mathcal{O}$ for some $R \in \mathbb{Z}$. Let $S_n \subseteq K_v/H$ be the set of cosets that contain $f(t_1) + \ldots + f(t_n)$ for some $t_1, \ldots, t_n$. Since 0 is a value of f, the S_n form an increasing sequence. On the other hand, each S_n is contained in the finite set $\pi^R\mathcal{O}/\pi^r\mathcal{O}$, so there exists n such that $S_N = S_n$ for all $N \geq n$. Since S_n is finite and closed under addition, it is a subgroup of K_v/H. Let G be the union of the cosets in S_n. Then G is an open subgroup of K_v, and all values of f are in G. On the other hand, every element of G is a sum of $n+1$ values of f, by definition of S_n, since we can arrange to have $f(t_{n+1})$ equal to any desired element of H. ■

Corollary 2.3. *Under the hypotheses of Proposition* 2.1, *the values of*

$$f(t_1) + \ldots + f(t_n) - f(t_{n+1}) - \ldots - f(t_{2n})$$

form an open subgroup of K_v.

Analogous results for rational functions in many variables over p-adic fields can be proved in the same way.

3. Sums and differences over number fields. This section is devoted to the proof of Theorem 1.1. The first lemma of this section is a thinly disguised version of Hilbert's Nullstellensatz, as its proof will reveal. Its relevance will become clear in the proof of Lemma 3.2. We fix an integer $d \geq 1$ (which eventually will be taken to be $[K : \mathbb{Q}]$) and for any ring R, we define $R[\mathbf{T}, \mathbf{T}^{-1}] = R[T_1, T_1^{-1}, \ldots, T_d, T_d^{-1}]$. If k is a field and $\mathbf{t} \in (\overline{k}^*)^d$, let $\mathrm{ev}_{\mathbf{t}} : k[\mathbf{T}, \mathbf{T}^{-1}] \to \overline{k}$ denote the evaluation map, which induces $\mathrm{ev}_{\mathbf{t}} : V \otimes_k k[\mathbf{T}, \mathbf{T}^{-1}] \to V \otimes_k \overline{k}$ for any k-vector space V.

Lemma 3.1. *Let V be a finite-dimensional vector space over a field k. If M is a $k[\mathbf{T}, \mathbf{T}^{-1}]$-submodule of $N := V \otimes_k k[\mathbf{T}, \mathbf{T}^{-1}]$ and $M \neq N$, then there exist nonzero $\lambda \in \mathrm{Hom}_{\overline{k}}(V \otimes_k \overline{k}, \overline{k})$ and $\mathbf{t} \in (\overline{k}^*)^d$ such that $\lambda(\mathrm{ev}_{\mathbf{t}}(F)) = 0$ for all $F \in M$.*

Proof. Without loss of generality, we may assume $k = \overline{k}$. Let $A = k[\mathbf{T}, \mathbf{T}^{-1}]$, which is a noetherian ring. Then N is a noetherian A-module, so we may assume M is a maximal proper submodule of N. The A-module homomorphism $A \to N/M$ sending 1 to any $n \in N \setminus M$ must then be surjective, with kernel equal to a maximal ideal $\mathfrak{m}$. Hence $\mathfrak{m}N \subseteq M$. The ring A is the ring of regular functions on the affine variety $(\mathbb{A}^1 \setminus \{0\})^d$, so by Hilbert's Nullstellensatz, $A/\mathfrak{m} \simeq k$ is an isomorphism induced by $\mathrm{ev}_{\mathbf{t}}$

for some point $\mathbf{t} \in (\overline{k}^*)^d$. Since $\mathfrak{m}N \subseteq M \subsetneq N$, the image of M under $\mathrm{ev}_{\mathbf{t}} : N = V \otimes_k A \to V$ is a proper subspace of V, so there exists a nonzero $\lambda \in \mathrm{Hom}_k(V, k)$ such that $\lambda(\mathrm{ev}_{\mathbf{t}}(M)) = 0$, as desired. ■

The main step in the proof of Theorem 1.1 is the following lemma, which gives a representation of the rational function x as a combination of values of f.

LEMMA 3.2. *Suppose $[K : \mathbb{Q}] < \infty$. Let $f \in K(x)$ be nonconstant with all poles in $K \cup \infty$. For some $n, n' \geq 1$, there exist $g_1, \dots, g_{n+n'} \in K(x)$ of degree 1 such that*

$$\sum_{i=1}^{n} f(g_i(x)) - \sum_{i=n+1}^{n+n'} f(g_i(x)) = x.$$

REMARK 3.3. Whenever we write $f(g_i(x))$, there is also the tacit requirement that $g_i(x)$ should not be a constant equal to a pole of f.

Proof of Lemma 3.2. Define

$$S := \Big\{ \sum_{i=1}^{n} f(g_i(x)) - \sum_{i=n+1}^{n+n'} f(g_i(x)) \,\Big|\, n, n' \geq 0,\ g_i \in K(x) \text{ and } \deg g_i = 1 \Big\}$$
$$\subset K(x).$$

We need to show that $x \in S$. Below we will frequently use without mention the easy fact that if $j \in S$, and $g \in K(x)$ is of degree 1, then $j \circ g \in S$.

For $j \in K(x)$, let $m(j)$ denote the maximum order of all poles of j. Since S contains nonconstant rational functions, we may choose a nonconstant $j \in S$ minimizing $m := m(j)$.

CASE 1: *j has a unique pole of order m.* If $m = 1$, then $\deg j = 1$, so $x = j \circ g \in S$, where g is the inverse function of j. If $m > 1$, then by replacing j with $j \circ g$ for some g of degree 1, we may assume that the pole is at ∞. Then $j(x+1) - j(x) \in S$, but $0 < m(j(x+1) - j(x)) = m - 1 < m$, contradicting the definition of j.

CASE 2: *j has more than one pole of order m.* Let $d = [K : \mathbb{Q}]$. Let $\alpha_1, \dots, \alpha_d$ be a $\mathbb{Z}$-basis for the ring of integers $\mathcal{O}_K$ of K. Let P_m be the set of $\gamma \in S$ such that $m(\gamma) \leq m$, and such that all poles of γ of order m are in $\mathcal{O}_K$. By replacing the given j with $j \circ g$ for some g of degree 1, we may assume first that j has no pole at ∞, and then that $j \in P_m$.

Given any $\gamma \in P_m$, write γ as

$$\gamma(x) = \sum_{i=1}^{s} \frac{a_i}{(x - r_i)^m} + \text{(terms with lower order poles)}, \tag{1}$$

where the r_i are distinct elements of $\mathcal{O}_K$ and $a_i \in K^*$, and define the $^-$ operation by

$$\overline{\gamma} := \sum_{i=1}^{s} a_i \mathbf{T}^{\mathbf{k}_i} \in K[\mathbf{T}, \mathbf{T}^{-1}],$$

where each vector of exponents $\mathbf{k}_i = (k_{i1}, \ldots, k_{i,d}) \in \mathbb{Z}^d$ is such that $r_i = k_{i1}\alpha_1 + \ldots + k_{i,d}\alpha_d$. Since P_m is an additive group, so is $M := \{\overline{\gamma} \mid \gamma \in P_m\}$. If $1 \le i \le d$ and $k \in \mathbb{Z}$, and $\tau(x)$ is the polynomial $x - k\alpha_i$, then $\overline{\gamma \circ \tau} = T_i^k \overline{\gamma}$. Thus we arrive at the following key observation:

$$M \text{ is a } \mathbb{Z}[\mathbf{T}, \mathbf{T}^{-1}]\text{-submodule of } K[\mathbf{T}, \mathbf{T}^{-1}].$$

If $\mathbb{Q} \cdot M = K[\mathbf{T}, \mathbf{T}^{-1}]$, then there exists $\gamma \in P_m$ such that $\overline{\gamma} \in \mathbb{Q}^* \subset K[\mathbf{T}, \mathbf{T}^{-1}]$. Then γ has a single pole (at 0) of order m, and we have reduced to Case 1.

Otherwise, if $\mathbb{Q} \cdot M \ne K[\mathbf{T}, \mathbf{T}^{-1}]$, then by Lemma 3.1 applied with $V = K$, $k = \mathbb{Q}$, and $\mathbb{Q} \cdot M$ as M, there exist a nonzero $\lambda \in \operatorname{Hom}_{\overline{\mathbb{Q}}}(K \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}})$ and $\mathbf{t} \in (\overline{\mathbb{Q}}^*)^d$ such that $\lambda(\operatorname{ev}_{\mathbf{t}}(\overline{\gamma})) = 0$ for all $\overline{\gamma} \in M$. Pick a finite extension L of $\mathbb{Q}$ over which λ and $\mathbf{t}$ are defined; i.e., λ maps $K \otimes L$ into L, and $\mathbf{t} \in (L^*)^d$. Replacing λ by an integer multiple, we may assume that λ maps $\mathcal{O}_K \otimes \mathcal{O}_L$ into $\mathcal{O}_L$. Define $a_i, r_i \in K$ so that (1) holds with γ replaced by our given j. For any prime p of $\mathbb{Q}$, let $\mathcal{O}_{K,p}$ (resp. $\mathcal{O}_{L,p}$) denote the subring of K (resp. L) of elements that are integral at all the primes above p. By the Chebotarev Density Theorem, there exists a prime p of $\mathbb{Q}$ such that

(1) p splits completely in K and in L,

(2) for any prime $\mathfrak{p}$ of L above p, the $(\mathcal{O}_L/\mathfrak{p})$-linear functional

$$\lambda_{\mathfrak{p}} : \mathcal{O}_{K,p}/(p) \otimes (\mathcal{O}_L/\mathfrak{p}) \to \mathcal{O}_L/\mathfrak{p} \simeq \mathbb{F}_p$$

induced by λ is *nonzero*,

(3) $\mathbf{t} \in (\mathcal{O}_{L,p}^*)^d$,

(4) $a_i \in \mathcal{O}_{K,p}^*$ and $r_i - r_k \in \mathcal{O}_{K,p}^*$ for all $1 \le i < k \le s$.

(The conditions after the first one exclude only finitely many p.) Fix $\mathfrak{p}$ as in condition (2).

Replacing $j(x)$ by $j(x+c)$ for some $c \in \mathcal{O}_K$, we may assume that $r_1 = p$. Then the other r_i are prime to p, because of condition (4). Let $R = r_1 r_2 \ldots r_s \ne 0$. Then $\eta(x) := p^m j(R/x) \in S$ has poles at R/r_i for $1 \le i \le d$, so $\eta \in P_m$. The coefficient b_i of $(x - R/r_i)^{-m}$ in the partial fraction decomposition of $\eta(x)$ equals the value of

$$p^m \left(x - \frac{R}{r_i} \right)^m \frac{a_i}{(R/x - r_i)^m}$$

at $x = R/r_i$ (which makes sense after terms are cancelled), so

$$b_i = \left(-\frac{p}{r_i}\right)^m \left(\frac{R}{r_i}\right)^m a_i.$$

Since the r_i are in $\mathcal{O}_{K,p}^*$ except for $r_1 = p$, and since $a_i \in \mathcal{O}_{K,p}^*$, each b_i lies in $\mathcal{O}_{K,p}$; in fact, $b_1 \in \mathcal{O}_{K,p}^*$ and $b_i \in p^m\mathcal{O}_{K,p}$ for $2 \le i \le s$. Let $\mu(x) = \eta(x + R/r_1) \in P_m$, to move the pole at R/r_1 to 0. Then

$$\overline{\mu} \equiv b_1 \pmod{p\mathcal{O}_{K,p}[\mathbf{T}, \mathbf{T}^{-1}]}.$$

Since p splits completely in k,

$$\mathcal{O}_{K,p}/(p) \simeq \mathbb{F}_p \times \ldots \times \mathbb{F}_p,$$

and since $b_1 \in \mathcal{O}_{K,p}^*$, b_1 reduces mod p to a vector of elements of $\mathbb{F}_p^*$ on the right. Since $\lambda_{\mathfrak{p}}$ is nonzero, one of the factors on the right (tensored with $\mathcal{O}_L/\mathfrak{p}$), say the ith, is not killed by $\lambda_{\mathfrak{p}}$. Choose $c \in \mathcal{O}_K$ whose image in

$$\mathcal{O}_{K,p}/(p) \simeq \mathbb{F}_p \times \ldots \times \mathbb{F}_p$$

is zero at all coordinates except the ith, and let $\theta(x) = \mu(x/c)$. A short calculation shows that $\theta \in P_m$ and

$$\overline{\theta} \equiv c^m b_1 \pmod{p\mathcal{O}_{K,p}[\mathbf{T}, \mathbf{T}^{-1}]}.$$

Now

$$\mathrm{ev}_{\mathbf{t}}(\overline{\theta}) \equiv c^m b_1 \otimes 1 \pmod{p(\mathcal{O}_{K,p} \otimes \mathcal{O}_L)}.$$

By choice of c, the right hand side is not killed by $\lambda_{\mathfrak{p}}$, so $\lambda(\mathrm{ev}_{\mathbf{t}}(\overline{\theta}))$ cannot possibly be zero. This contradicts the construction of λ and $\mathbf{t}$. ∎

Theorem 3.4. *Let K be a finite extension of $\mathbb{Q}$. Let $f \in K(x)$ be a nonconstant rational function all of whose poles are in $K \cup \infty$. If $n \ge 1$ is sufficiently large, then for any $h \in K(x)$, there exist $g_1, \ldots, g_{2n} \in K(x)$ such that*

$$\sum_{i=1}^{n} f(g_i(x)) - \sum_{i=n+1}^{2n} f(g_i(x)) = h(x).$$

Proof. Find a representation of x as in Lemma 3.2, using n plus terms and n' minus terms. Write $h = h_1 - h_2$, where $h_1, h_2 \in K(x)$ are nonconstant. Substitute h_1 for x in the identity giving x, then substitute h_2 for x in the same identity, and subtract the two equations to obtain a representation of h using $n + n'$ plus terms and $n + n'$ minus terms. We can add pairs of canceling terms to obtain representations with more than $n + n'$ terms of each sign. ∎

To prove Theorem 1.1, apply Theorem 3.4 with $h(x)$ as the constant $c \in K$, and substitute an element of K for x: all but finitely many elements of K will yield a representation of the required form.

4. Sums over number fields. Fix a number field K for this section. If $f, h \in K(x)$, we write $h \preceq f$ to mean that for some $n \geq 1$, there exist $g_1, \ldots, g_n \in K(x)$ of degree 1 such that $\sum_{i=1}^{n} f(g_i(x)) = h(x)$. The set of h such that $h \preceq f$ is closed under addition, and closed under $h \mapsto h \circ j$ for any $j \in K(x)$ of degree 1, so it follows that $\preceq$ is transitive.

LEMMA 4.1. *Suppose f is a nonconstant function in $K(x)$. Suppose that the poles of f are simple and in $K \cup \infty$. If there is a constant function $c \in K$ such that $c \preceq f$, then $x \preceq f$.*

Proof. We are given an identity $\sum_{i=1}^{n} f(g_i(x)) = c$. Let $h(x) = f(g_1(x))$, which is a nonconstant function with poles in $K \cup \infty$ such that $h \preceq f$ and $c - h \preceq f$. Applying Lemma 3.2 to h yields an identity

$$\sum_{i=1}^{n} h(j_i(x)) - \sum_{i=n+1}^{n+n'} h(j_i(x)) = x$$

for some $j_i \in K(x)$ of degree 1. Then

$$\sum_{i=1}^{n} h(j_i(x)) + \sum_{i=n+1}^{n+n'} (c - h(j_i(x))) = x + n'c$$

and each summand on the left is $\preceq f$, so $x + n'c \preceq f$. Substituting $x - n'c$ for x shows that $x \preceq f$. ■

LEMMA 4.2. *If $f \in K(x)$ is nonconstant with ≤ 3 poles, all simple and in $K \cup \infty$, then there is a constant function $c \in K$ such that $c \preceq f$.*

Proof. First suppose that f has ≤ 2 poles. Composing with a degree 1 function, we may assume without loss of generality that the poles are contained in $\{0, \infty\}$, so

$$f(x) = ax + b/x + r$$

for some $a, b, r \in K$. Then $2r = f(x) + f(-x) \preceq f$, and $2r$ is constant.

If f has 3 poles, then we may assume they are 0, 1, and ∞. Then $f(x) + f(-x)$ has 2 poles (at 1 and -1), and $f(x) + f(-x) \preceq f$, so apply the previous paragraph and use transitivity of $\preceq$. ■

Proof of Theorem 1.2. Applying Lemmas 4.1 and 4.2, we see that $x \preceq f$. Thus $\sum_{i=1}^{m} f(g_i(x)) = x$ for some $g_i \in K(x)$ of degree 1. Then $\sum_{i=1}^{m} f(g_i(x)) + \sum_{i=1}^{m} f(g_i(c - x)) = c$. Substitute an element of K for x: all but finitely many choices lead to a representation of c as $\sum_{i=1}^{2m} f(x_i)$ with $x_i \in K$.

To obtain a representation with n terms for $n > 2m$, choose $x_{2m+1}, \ldots, x_n \in K - \{\text{poles of } f\}$ arbitrarily, let $c' = c - \sum_{i=2m+1}^{n} f(x_i)$, and use the previous paragraph to find $x_1, \ldots, x_{2m}$ such that $\sum_{i=1}^{2m} f(x_i) = c'$. ■

5. Local-global questions. Throughout this section K denotes a number field, and $f \in K(x)$ is a nonconstant rational function.

Theorem 1.2 cannot be generalized to all nonconstant f with poles in $K \cup \infty$, since there can be local obstructions at the real places. For instance, if $K = \mathbb{Q}$ and $f(x) = x^2$, then the equation is not solvable when $c < 0$.

Question 5.1. Is it possible that Theorem 1.2 can be extended to the case where f has all poles in $K \cup \infty$ (not necessarily simple), and the highest order pole is of odd order?

Without the assumption that the poles of f are in $K \cup \infty$, even Theorem 1.1 can fail. For example, suppose that $K = \mathbb{Q}$ and $f(x) = 2/(x^2 - 2)$. Local considerations show that

$$f(t) \in R := \{r/s \in \mathbb{Q} \mid r, s \in \mathbb{Z}, \text{ and } s \text{ is a product of primes of the form } 8k \pm 1\}$$

for any $t \in \mathbb{Q}$. If $c \notin R$, then for any n,

$$\sum_{i=1}^{n} f(x_i) - \sum_{i=n+1}^{2n} f(x_i) = c$$

has no solution over K.

Remark 5.2. Nevertheless, there are *some* rational functions having some poles outside $K \cup \infty$ for which the conclusions of Theorems 1.1 and 3.4 still hold. For instance, if $K = \mathbb{Q}$ again, and

$$f(x) = \frac{x}{2} + \frac{1}{x^2 - 2},$$

then although f has poles outside $\mathbb{Q} \cup \infty$, the combination $f(x) - f(-x)$ yields x, from which any other $h \in \mathbb{Q}(x)$ can be obtained. (See the proof of Theorem 3.4 for this last step.)

Local obstructions explain the failure of Theorem 1.1 to generalize to functions such as $f(x) = 2/(x^2 - 2)$. It is natural to ask whether these are the only obstructions to representability of a rational numbers as a sum and difference of a fixed number of values of f. More precisely, one might ask the following:

Question 5.3. For $n \gg 1$ is it true that for each $c \in K$, the equation

$$\sum_{i=1}^{n} f(x_i) - \sum_{i=n+1}^{2n} f(x_i) = c \tag{2}$$

has a solution over K if and only if it has a solution over all completions? Equivalently, if $X_{n,c}$ is the affine variety over K defined by (2) and by the inequalities saying that no x_i is a pole of f, is it true for $n \gg 1$ that for all $c \in K$, the variety $X_{n,c}$ satisfies the Hasse principle?

The analogous question with sums only has a negative answer. For example, if $K = \mathbb{Q}$ and $f(x) = (x^2 - 2)^2$ then methods similar to those used in the proof of Proposition 2.1 show that for $n \geq 5$,

$$f(x_1) + \ldots + f(x_n) = 0$$

has a solution over every completion of $\mathbb{Q}$, while considering the equation over $\mathbb{R}$ shows that it has no solution over $\mathbb{Q}$. One could, however, ask the following:

Question 5.4. Is it true for $n \gg 1$ that for all $c \in K$, if

$$\sum_{i=1}^{n} f(x_i) = c \tag{3}$$

has a solution over every completion of K, and for each real completion K_v the equation $\sum_{i=1}^{n} f(x_i) = c'$ is solvable over K_v for all c' in a *neighborhood* of c, then (3) has a solution over K?

6. Undecidability. A subset $A \subseteq \mathbb{Q}$ is called *diophantine* over $\mathbb{Q}$ if there is a polynomial $g(t, x_1, \ldots, x_n)$ such that

$$A = \{a \in \mathbb{Q} \mid \exists x_1, \ldots, x_n \in \mathbb{Q} \text{ with } g(a, x_1, \ldots, x_n) = 0\}.$$

If $\mathbb{Z}$ were diophantine over $\mathbb{Q}$, then the (known) undecidability of Hilbert's Tenth Problem over $\mathbb{Z}$ would imply the undecidability of Hilbert's Tenth Problem over $\mathbb{Q}$, that is, that there is no general algorithm for deciding whether a variety over $\mathbb{Q}$ has a rational point. See the book [DLPVG00] for a discussion of this and related questions.

Given that it is unknown whether $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, it is natural to ask whether other subrings between $\mathbb{Z}$ and $\mathbb{Q}$ can be proved to be diophantine over $\mathbb{Q}$. If S is the complement of a finite subset in the set of all primes, then the semilocal ring $\mathbb{Z}[S^{-1}]$ is known to be diophantine over $\mathbb{Q}$: this follows from [KR92]. Currently there are no other subsets S for which $\mathbb{Z}[S^{-1}]$ has been proved diophantine over $\mathbb{Q}$.

If Question 5.3 has a positive answer for $K = \mathbb{Q}$ and $f(x) = 2/(x^2 - 2)$, then it would follow that the ring $R = \mathbb{Z}[S^{-1}]$ is diophantine over $\mathbb{Q}$, where S is the set of primes of the form $8k \pm 1$. If Question 5.3 has a positive answer in general, then there would exist subsets S of arbitrarily small positive natural density such that $\mathbb{Z}[S^{-1}]$ is diophantine over $\mathbb{Q}$. One cannot hope to obtain $\mathbb{Z}$ as a finite intersection of subrings arising in this way, however, since if L is the number field generated by the poles of the corresponding rational functions f, then all the primes splitting completely in L will remain invertible in the intersection, and these form a set of primes of positive density, by the Chebotarev Density Theorem.

References

[DLPVG00] J. Denef, L. Lipshitz, T. Pheidas and J. Van Geel (eds.), *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, Amer. Math. Soc., Providence, RI, 2000.

[KR92] K. H. Kim and F. W. Roush, *An approach to rational Diophantine undecidability*, in: Proceedings of Asian Mathematical Conference (Hong Kong, 1990), World Sci., 1992, 242–248.

[Vau97] R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Tracts in Math. 125, Cambridge Univ. Press, Cambridge, 1997.

Department of Mathematics
University of California
Berkeley, CA 94720-3840, U.S.A.
E-mail: poonen@math.berkeley.edu

Received on 28.12.2002 (4435)