A note on universal Hilbert sets

Yuri Bilu

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI/95-52

A note on universal Hilbert sets

By *Yuri Bilu* at Bonn

1 Introduction

Let $F(X,Y) \in \mathbf{Q}[X,Y]$ be a polynomial with rational coefficients and $\mathcal{G}(F)$ its Galois group over $\mathbf{Q}(X)$. For any $h \in \mathbf{Q}$ denote by $\mathcal{G}_h(F)$ the Galois group of $F(h,Y)$ over $\mathbf{Q}$. (By the *Galois group of a polynomial* we mean the Galois group of its splitting field.) The classical *Hilbert irreducibility theorem* [7] states that for infinitely many $h \in \mathbf{Z}$ the group $\mathcal{G}_h(F)$ is isomorphic to $\mathcal{G}(F)$ (see [6, 10, 16] for modern expositions). In particular, if $F(X,Y)$ is irreducible over $\mathbf{Q}$ then for infinitely many $h \in \mathbf{Z}$ the specialization $F(h,Y)$ is an irreducible over $\mathbf{Q}$ polynomial in Y.

Of course, the set of $h \in \mathbf{Z}$ with this property depends on the polynomial F.

Gilmore and Robinson [8] proved the existence of an infinite set $\mathcal{H} \subset \mathbf{Z}$ with the following property: for *any* $F(X,Y) \in \mathbf{Q}[X,Y]$, the group $\mathcal{G}_h(F)$ is isomorphic to $\mathcal{G}(F)$ for all but finitely many $h \in \mathcal{H}$. Such sets will be referred to as *universal Hilbert sets.* (Gilmore and Robinson do not state this result explicitly, but it definitely follows from their Theorem 2.1, see [6], Ch. 14, Exercise 2.)

The argument of Gilmore and Robinson was non-constructive. Sprindžuk [18] obtained a very explicit construction of a universal Hilbert set. He proved that such is the set

$$\left\{h_m = \left[\exp\sqrt{\log\log m}\right] + m!\,2^{m^2} : m = 3,\,4,\,\ldots\right\}.$$

(As usual, $[x]$ is the largest integer not exceeding x.) Sprindžuk proves that for any $F(X,Y) \in \mathbf{Q}[X,Y]$, one can effectively compute $m_0 = m_0(F)$ such that $\mathcal{G}_{h_m}(F) \cong \mathcal{G}(F)$ for all $m \ge m_0$. See also [19, 5].

Yasumoto [21] obtained a general sufficient condition for an infinite set $\mathcal{H} \subset \mathbf{Z}$ to be universal Hilbert. He showed that this condition is satisfied for the sets $\{2^m p_m\}$ (where p_m is the m-th prime) and $\{2^m\,(m^3+1)\}$, which are thereby universal Hilbert.

The sequences of Sprindžuk and Yasumoto grow exponentially, and, in particular, they have asymptotic density 0. In this note we give a very simple (constructive) proof of the following result.

Theorem 1.1 *There exists a universal Hilbert set $\mathcal{H} \subset \mathbf{Z}$ of asymptotic density* 1.

Recall that the *asymptotic density* of a set $A \subset \mathbf{Z}$ is

$$\mathrm{d}A \overset{\mathrm{def}}{=} \lim_{N\to\infty} \frac{|A \cap [-N,\,N]|}{2N}$$

provided that the limit exists. (We denote by $|S|$ the cardinality of the finite set S.)

Yasumoto [21] introduced a weaker notion of *μ-irreducibility set*, μ being a positive integer. An infinite set $\mathcal{H} \subset \mathbf{Z}$ is a *μ-irreducibility set* if for any irreducible polynomial

$F(X,Y) \in \mathbf{Q}[X,Y]$ with $\deg_X F(X,Y) \le \mu$ the polynomial $F(h,Y)$ is irreducible for all but finitely many $h \in \mathcal{H}$. For any μ he gave [22] an explicit construction of a μ-irreducibility set of polynomial growth; for instance, such is the set $\left\{m^{4d} + m^{4d-4}\right\}$ with $d = (\mu!)!$.

Our second result is an explicit universal Hilbert set with polynomial growth.

Theorem 1.2 *The set*

$$\left\{h_m = \left[\log\log|m|\right] + m^3 : m = \pm 3,\ \pm 4,\ \ldots\right\} \tag{1}$$

is universal Hilbert.

Acknoledgements. This work was done during the author's post-doctoral stage in Max-Planck-Institute für Mathematik. I am grateful to Prof. F. Hirzebruch and MPI für Mathematik for their kind invitation and excellent working conditions.

I would like to thank S. Suter for helpful remarks and Prof. P. Roquette for drawing my attention to the work of Yasumoto.

2 Hilbert irreducibility theorem

For any polynomial $F(x,y) \in \mathbf{Q}[X,Y]$ put

$$R(F) = \{h \in \mathbf{Z} : \mathcal{G}_h(F) \not\cong \mathcal{G}(F)\}\ . \tag{2}$$

We say that $\mathrm{M} \subset \mathbf{Z}$ is *a singular set of the first type* if $\mathrm{M} = \mathrm{M}_g = g(\mathbf{Z}) \cap \mathbf{Z}$ for some polynomial $g(T) \in \mathbf{Q}(T)$ of degree at least 2.

We say that $\mathrm{M} \subset \mathbf{Z}$ is *a singular set of the second type* if

$$\mathrm{M} = \mathrm{M}_{(K,g_1,g_2)} = \left\{g_1(\eta) + g_2(\eta^{-1}) : \eta \text{ is a unit in } K\right\} \cap \mathbf{Z}$$

where K is a number field and g_1 , $g_2 \in K(T)$ are non-constant polynomials.

We use Hilbert irreducibility theorem in the following form.

Theorem 2.1 *The set $R(F)$ is contained in a union of a finite set* M *and finitely many singular sets, the corresponding polynomials g and triples (K, g_1, g_2) being effectively constructible in terms of F. The cardinality of the finite set* M *can be effectively estimated in terms of F.*

(We do not claim that the set M can be effectively constructed.)

The proof of this theorem is implicit in [16], Ch. 9, especially Section 9.7 and Exercise 2. We include some details for the sake of completeness.

We deal with pairs (C, x), where C is a projective curve defined and irreducible over $\mathbf{Q}$ (but may be reducible over $\overline{\mathbf{Q}}$), and $x \in \mathbf{Q}(C)$ is non-constant and satisfies $[\mathbf{Q}(C) : \mathbf{Q}(x)] \ge 2$. For such a pair put

$$\mathrm{M}_{(C,x)} = x\left(C(\mathbf{Q})\right) \cap \mathbf{Z}\,.$$

Lemma 2.2 ([16], Section 9.2, Proposition 2) *The set $R(F)$ is contained in a union of an effectively constructible finite set and finitely many sets of the type* $\mathrm{M}_{(C,x)}$, *the corresponding pairs (C,x) being effectively constructible as well.*

In view of this, Theorem 2.1 is a consequence of the following lemma.

Lemma 2.3 *Let (C,x) be as above.*

(a) *If C is reducible over $\overline{\mathbf{Q}}$ then the set $\mathrm{M}_{(C,x)}$ is finite and can be effectively determined.*

Now suppose that C is irreducible over $\overline{\mathbf{Q}}$.

(b) *If $\mathbf{g}(C) \geq 1$ or x has at least three distinct poles then the set $\mathrm{M}_{(C,x)}$ is finite and its cardinality can be effectively estimated.*

(c) *If $\mathbf{g}(C) = 0$ and x has exactly two distinct poles, then $\mathrm{M}_{(C,x)}$ is contained in the union of finitely many singular sets of the second type, the corresponding triples (K, g_1, g_2) being effectively constructible.*

(d) *If $\mathbf{g}(C) = 0$ and x has exactly one pole, then $\mathrm{M}_{(C,x)}$ is contained in a singular set of the first type, the corresponding polynomial g being effectively constructible.*

Proof (a) As follows from the consideration of the Galois action, any rational point on C should belong to its any absolutely irreducible component. Any two components have finitely many intersections, which can be effectively found. Thus, even the set $C(\mathbf{Q})$ is finite and can be effectively determined. This completes the proof.

(b) This is classical Siegel's theorem on integral points [17, 10, 13, 16]. In fact, more information on the effectivity is available than it is stated. Namely, in the case $\mathbf{g} = 1$ and in the case $\mathbf{g} = 0$ *and x has at least three poles* the set $\mathrm{M}_{(C,x)}$ can be effectively determined [16], Ch. 8, see also [1, 9, 15, 11, 2]. In the case $\mathbf{g} \geq 2$ the cardinality of the set $C(\mathbf{Q})$ can be effectively estimated [4], Section 6.6 and [3].

(c) Let P_1 and P_2 be the two distinct poles of x and K a number field such that both P_1 and P_2 are defined over K. Then there exist $t \in K(C)$ such that $(t) = P_1 - P_2$. We have $x = \tilde{g}_1(t) + \tilde{g}_2(t^{-1})$, where $\tilde{g}_1(T)$ and $\tilde{g}_2(T)$ are non-constant polynomials with coefficients in K. Let $P_0 \in C(\mathbf{Q})$ be such that $x(P_0) \in \mathbf{Z}$. Both t and t^{-1} are integral over the ring $\mathbf{Q}[x]$. Therefore there exist only finitely many possibilities for the fractional ideal $(t(P_0))$ of the field K. In the other terms, $t(P_0)$ is a unit of K times a non-zero number from a finite effectively computable set. Therefore $\mathrm{M}_{(C,x)}$ is contained in the union of finitely many singular sets $\mathrm{M}_{(K,g_1,g_2)}$, where $g_1(T) = \tilde{g}_1(\alpha T)$ and $g_2(T) = \tilde{g}_2(\alpha^{-1}T)$, with α from the finite set referred to in the previous phrase.

(d) In this case there is $t \in \mathbf{Q}(C)$ such that $\mathbf{Q}(C) = \mathbf{Q}(t)$ and t has the same pole as x. This t is integral over the ring $\mathbf{Q}[x]$. Multiplying it by an appropriate integer, we may assume that it is integral over $\mathbf{Z}[x]$. We have $x = g(t)$, where $g(T) \in \mathbf{Q}[T]$ and $\deg g = [\mathbf{Q}(C) : \mathbf{Q}(x)] \geq 2$. If P_0 is as in the proof of (c), then $t_0 = t(P_0)$ is an integer and $x(P_0) = g(t_0)$. Therefore $\mathrm{M}_{(C,x)} \subset \mathrm{M}_g$. The proof is complete.

(As one can easily see, the field K in the proof of (c) can be assumed to be real quadratic, and the polynomials g_1 and g_2 of the same degree; we do not need this additional information.)

As a direct consequence of Theorem 2.1 we have

Corollary 2.4 *Given an irreducible polynomial $F(x,y) \in \mathbf{Z}[x,y]$, there exists an effective constant $c(F)$ such that for any $N \geq 1$ we have*

$$\Big|R(F) \cap [-N,\, N]\Big| \leq c(F)\sqrt{N}\,. \tag{3}$$

(See [16], Section 9.7 and Ch. 13 for more general results.)

The corollary will be sufficient for Theorem 1.1, but the proof of Theorem 1.2 will require the full strength of Theorem 2.1.

3 Proof of Theorem 1.1

For any $F(X,Y) \in \mathbf{Q}[X,Y]$ put

$$R'(F) = \{h \in R(F) \colon |h| \geq N(F)\}\ ,$$

where $N(F) \geq 1$ is to be defined later.

Further, put

$$R = \bigcup_{F \in \mathbf{Q}[X,Y]} R'(F)\,, \qquad \mathcal{H} = \mathbf{Z} \setminus R\,.$$

Clearly, $\mathcal{H}$ is a universal Hilbert set. We shall show that $\mathbf{d}\mathcal{H} = 1$ under an appropriate definition of $N(F)$.

Let $c(F)$ be the constant defined in Corollary 2.4. Fix a numbering F_1 , F_2 , ... of the polynomials $F(X,Y) \in \mathbf{Q}[X,Y]$ and put

$$N_k = N(F_k) = \max\left(k,\, \big(c(F_1) + \cdots + c(F_k)\big)^4\right)$$

(in fact, 4 can be replaced by $2+\varepsilon$ for any $\varepsilon > 0$). Now fix $N \geq 1$. Then $N_k \leq N < N_{k+1}$ for some k. We have

$$[-N\,,\, N] \cap R = [-N\,,\, N] \cap \left(\bigcup_{1 \leq i \leq k} R'(F_i)\right) \subseteq [-N\,,\, N] \cap \left(\bigcup_{1 \leq i \leq k} R(F_i)\right)\,.$$

Therefore

$$|[-N\,,\, N] \cap R| \leq \big(c(F_1) + \cdots + c(F_k)\big)\sqrt{N} \leq N_k^{1/4}\sqrt{N} \leq N^{3/4}\,. \tag{4}$$

Thus, the asymptotic density of R is 0. Therefore the asymptotic density of $\mathcal{H}$ is 1. The theorem is proved.

Remark 3.1 Note that the presented proof is *constructive* in the following sense. If $\mathcal{H} = \{\ldots < h_{-2} < h_{-1} < h_0 = 0 < h_1 < h_2 < \ldots\}$, then h_m and h_{-m} can be effectively computed for the given m (when the numbering $F_1, F_2, \ldots$ is fixed). Indeed, we deduce from (4) that

$$2h_m + 1 - h_m^{3/4} \leq \left|\mathcal{H} \cap [-h_m\,,\, h_m]\right| \leq h_m + 1 + m\,.$$

Therefore $h_m - h_m^{3/4} \leq m$, which immediately yields $h_m \leq 4m$. By induction, we may suppose that h_{m-1} is already found. Now h_m is the minimal integer h in the interval $[h_{m-1} + 1\,, 4m]$ with the following property: for all polynomials F_k with $N_k \leq h$ we have $h \notin R(F_k)$. This allows to find h_m in finitely many steps, because $N_k \geq k$ by definition. Similarly one finds effectively h_{-m}.

Moreover, as in Sprindžuk's case, for any $F \in \mathbf{Q}[X, Y]$ we can find effectively such $m_0 = m_0(F)$ that $\mathcal{G}_{h_m}(F) = \mathcal{G}(F)$ when $|m| \geq m_0$. Say, put $m_0(F) = [N(F)] + 1$. Then $|m| \geq m_0$ yields $|h_m| \geq |m| > N(F)$, and $h_m \notin R(F)$ by the construction.

4 Proof of Theorem 1.2

Let K be a number field. Recall the definition of the *height* of an affine vector $\underline{\alpha} = (\alpha_1 : \ldots : \alpha_n) \in K^n$:

$$H_K(\underline{\alpha}) \overset{\text{def}}{=} \prod_v \Big(\max(1, |\alpha_1|_v\,, \ldots, |\alpha_n|_v)\Big)^{[K_v : \mathbf{Q}_v]}\,,$$

the product being over all valuations of K, normalized to extend standard valuations of $\mathbf{Q}$.

The height of a polynomial is, by definition, the height of the vector of its coefficients. For a rational number $\alpha = \frac{p}{q}$ with $(p, q) = 1$ we have $H_{\mathbf{Q}}(\alpha) = \max(|p|\,, |q|)$.

Lemma 4.1 *Let K be a number field, $\mathcal{O} = \mathcal{O}_K$ its ring of integers, $g(T) \in \mathbf{K}(T)$ a separable polynomial of degree $\nu \geq 2$ and $n \geq 3$. Then any solution $(u\,, t) \in \mathcal{O} \times \mathcal{O}$ of the equation $u^n = g(t)$ satisfies*

$$\max\Big(H_K(u)\,, H_K(t)\Big) \leq \exp\Big(c(K, n, \nu) H_K(g)^{c(n.\nu)}\Big)\,.$$

Proof See Voutier [20] or Poulakis [12]. The proofs are heavily based on Baker's theory of linear forms in the logarithms. Poulakis obtains the exponent $c(n, \nu, d)$, depending also on the degree $d = [\mathbf{K} : \mathbf{Q}]$, but this would suffice for our purposes as well.

Lemma 4.2 *Let $g(T) \in \mathbf{Q}[T]$ be a polynomial of degree at least two. Then the equation*

$$u^3 + \Big[\log\log|u|\Big] = g(t)$$

has finitely many solutions $u\,, t \in \mathbf{Z}$.

Proof For sufficiently large $|u|$ the polynomial $g_u(T) = g(T) - \Big[\log\log|u|\Big]$ is separable and

$$H_{\mathbf{Q}}(g_u) \leq c_1(g)\log\log|u|\,.$$

Therefore, given a solution $(u, t) \in \mathbf{Z} \times \mathbf{Z}$ with u sufficiently large, we have

$$|u| = H_{\mathbf{Q}}(u) \leq \exp\left(\Big(\log\log|u|\Big)^{c_2(g)}\right) \leq c(g, \varepsilon)|u|^{\varepsilon}$$

for any $\varepsilon > 0$. This gives an upper bound for $|u|$. The proof is complete.

Lemma 4.3 *Let $g(T) \in \mathbf{C}(T)$ and k a positive integer. Suppose that $g(0) \neq 0$. Then the polynomial $g(T,z) = g(T) + zT^k$ is separable for all but finitely many $z \in \mathbf{C}$.*

Proof The discriminant $D(Z)$ of $g(T,Z)$ is a polynomial in Z and $g(T,z)$ is separable when $D(z) \neq 0$. Thus, it suffices to prove that $D(Z) \not\equiv 0$.

If $D(Z) \equiv 0$ then $g(T,Z)$ is not separable over the field $\mathbf{C}(Z)$. In particular, it is reducible over $\mathbf{C}(Z)$. By Gauss lemma, it is reducible over the ring $\mathbf{C}[Z]$. We have $g(T)+ZT^k = G_1(T,Z)G_2(T,Z)$, and one of G_1 and G_2 is of degree 0 in Z. This means that the polynomials $g(T)$ and T^k should have a common root, which contradicts to $g(0) \neq 0$. This completes the proof.

Lemma 4.4 *Let K be a number field, $\mathcal{O}^* = \mathcal{O}_K^*$ its group of units and g_1, $g_2 \in K(T)$ non-constant polynomials. Then the equation*

$$u^3 + \left[\log\log|u|\right] = g_1(\eta) + g_2(\eta^{-1}) \tag{5}$$

has finitely many solutions in $u \in \mathbf{Z}$ and $\eta \in \mathcal{O}^*$.

Proof Let ξ, $\eta_1, \dots, \eta_r$ generate the group $\mathcal{O}^*$ and $L = K\left(\sqrt[3]{\xi}, \sqrt[3]{\eta_1}, \dots, \sqrt[3]{\eta_r}\right)$. Put

$$g_u(T) = T^{\deg g_2}\left(g_1(T) + g_2(T) - \left[\log\log|u|\right]\right).$$

By Lemma 4.3 the polynomial $g_u(T)$ is separable for sufficiently large $|u|$. We have $\deg g_u(T) = \deg g_1 + \deg g_2 \geq 2$, and for sufficiently large $|u|$

$$H_L(g_u) \leq \left(\log\log|u|\right)^{c_1(g_1,g_2,K)}.$$

For any $\eta \in \mathcal{O}^*$ one of the cubic roots $\sqrt[3]{\eta}$ belongs to L. Therefore for any solution $(u,\eta) \in \mathbf{Z} \times \mathcal{O}^*$ of (5) we obtain a solution $(w,t) \in \mathcal{O}_L \times \mathcal{O}_L$ of the equation

$$w^3 = g_u(t),$$

putting $w = u\left(\sqrt[3]{\eta}\right)^{\deg g_2}$ and $t = \eta$.

By Lemma 4.1, for sufficiently large $|u|$ we have

$$\max\left(|\eta|, |\eta^{-1}|\right) \leq H_L(\eta) \leq \exp\left(\left(\log\log|u|\right)^{c_2(g_1,g_2,K)}\right).$$

(Here $|\dots|$ is a fixed archimedean valuation of the field L.) Substituting this to (5), we obtain an estimate $|u| \leq c(g_1,g_2,K,\varepsilon)|u|^\varepsilon$ for any $\varepsilon > 0$. This completes the proof.

Theorem 1.2 is an immediate consequence of Lemma 4.2, Lemma 4.4 and Theorem 2.1.

Remark 4.5 Of course, the set (1) is just an example. In fact, $\left[\log\log|m|\right]$ can be replaced by any other integral-valued function $\psi(m)$ such that $\psi(m) \to \infty$ when $m \to \infty$ and $\psi(m) \ll \left(\log|m|\right)^\varepsilon$ for any $\varepsilon > 0$. Further, instead of $|m|^3$ one can take $A|m|^n$ with fixed integers $A \neq 0$ and $n \geq 3$. Moreover, in view of a result of Schinzel and Tijdeman [14], one can construct a "two-parametric" universal Hilbert set

$$\{\psi(m) + m^n : m, n \in \mathbf{Z}, \quad |m| \geq 2, \quad n \geq 3\}$$

where the integral-valued function $\psi(m)$ can be written explicitly.

Also, as usual, the ring $\mathbf{Z}$ can be replaced by the ring of integers (or S-integers) of an arbitrary number field.

Remark 4.6 Unlike Sprindžuk, we can only claim the existence of $m_0(F)$ for any polynomial F such that $\mathcal{G}_{h_m}(F) = \mathcal{G}(F)$ for all $m \geq m_0$. We cannot find m_0 effectively, because we have no effective upper bound for the integers from the set M in Theorem 2.1. This is also the case for Yasumoto sequences.

References

[1] *A. Baker, J. Coates,* Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* **67** (1970), 592–602.

[2] *Yu. Bilu,* Effective analysis of integral points on algebraic curves, Israel J. Math., **90** (1995), 235–252.

[3] *E. Bombieri,* The Mordell Conjecture Revisited, Ann. Sc. Nor. Sup. Pisa, Cl. Sci., S. IV **17** (1990), 615–640; Errata-Corrigendum: **18** (1991), 473.

[4] *G. Faltings, G. Wustholz et al.,* Rational points, Aspects of Math. **E6**, Third Edition, Vieweg, Braunschweig 1992.

[5] *M. D. Fried,* On the Sprindžuk-Weissauer approach to universal Hilbert subsets, Israel J. Math. **51** (1985), 347–363.

[6] *M. D. Fried, M. Jarden,* Field Arithmetic, Erg. Math. Grenz. **11**, Springer, 1986.

[7] *D. Hilbert,* Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, J. reine und angew. Math. **110** (1892), 104–129.

[8] *P.C. Gilmore, A. Robinson,* Mathematical consideration of the relative irreducibility of polynomials, Can. J. Math **7** (1955), 483–489.

[9] *S.V. Kotov, L.A. Trellina,* S-ganze Punkte auf elliptischen Kurven, J. reine und angew. Math. **306** (1979), 28–41.

[10] *S. Lang,* Fundamentals of Diophantine Geometry, Springer, 1983.

[11] *D. Poulakis,* Points entiers sur les courbes de genre 0, Colloquium Math. **66** (1993), 1–7.

[12] *D. Poulakis,* Solutions entières de l'équation $Y^m = f(x)$. Sém. Th. Nom. Bordeaux **3** (1991), 187–199.

[13] *A. Robinson, P. Roquette,* On the Finiteness Theorem of Siegel and Mahler Concerning Diophantine Equations, J. Number Theory **7** (1975), 121–176.

[14] *A. Schinzel, R. Tijdeman,* On the equation $y^m = P(x)$, Acta Arithm. **31** (1976), 199–204.

[15] *W.M. Schmidt,* Integer points on curves of genus 1, Compositio Math. **81** (1992), 33–59.

[16] *J.-P. Serre* Lectures on the Mordell-Weil theorem, Aspects of Math. **E15**, Vieweg, Braunschweig 1989.

[17] *C.L. Siegel,* Über einige Anwendungen Diophantischer Approximationen, Abh. Preuss Akad. Wiss. Phys.-Math. Kl., 1929, Nr. 1.

[18] *V.G. Sprindžuk,* Diophantine equations with unknown prime numbers (Russian), Trudy MIAN SSSR **158** (1981), 180–196; *English transl.:* Proc. Steklov Inst. Math. 1983, Issue 4, 197–214.

[19] *V.G. Sprindžuk,* Arithmetic specializations in polynomials, J. reine und angew. Math. **340** (1983), 26–52.

[20] *P.M. Voutier,* An Upper Bound for the Size of Integral Solutions to $Y^m = f(X)$, J. Number Theory, to appear.

[21] *M. Yasumoto* Hilbert Irreducibility Sequences and Nonstandard Arithmetic, J. Number Theory **26** (1987), 274–285.

[22] *M. Yasumoto* Algebraic extensions in nonstandard models and Hilbert's irreducibility theorem, J. Symbolic Logic **53** (1988), 470–480.

Max-Planck-Institut für Mathematik
Gottfried-Claren-Strasse 26
53225 Bonn GERMANY.