Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

R. Dvornicich
U. Zannier

Fields containing values of algebraic functions

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 21, nº 3 (1994), p. 421-443
<http://www.numdam.org/item?id=ASNSP_1994_4_21_3_421_0>

Fields Containing Values of Algebraic Functions

R. DVORNICICH - U. ZANNIER

Introduction

The present paper takes its starting point in the celebrated Hilbert's Irreducibility Theorem (from now on H.I.T.) the simplest case of which states:

Let $F \in \mathbb{Q}[X,Y]$ be an irreducible polynomial. Then, for infinitely many natural numbers n, $F(n,Y)$ is irreducible in $\mathbb{Q}[Y]$.

Many proofs and generalizations of this result in many different directions are known (Hilbert himself proved a version valid for several polynomials and variables); see for example the books [11], [14], [17], [19] and the related references or, for a survey of more recent work, [8].

There is for instance a quantitative version which we state in a weak form, sufficient for a later application in the present paper.

Namely, set $d = \deg_Y F$ and

$$N(T) = \#\{n \in \mathbb{N} : n \leq T,\ \ F(n,Y) \text{ is reducible over } \mathbb{Q}\}. \tag{1}$$

Then, provided $d > 1$, we have the estimate

$$N(T) \ll T^{\beta} \tag{2}$$

for some $\beta = \beta(F) < 1$. (In fact much more is known. For instance one can take $\beta = \frac{1}{2}$, independently of F. See [10] or [19] for even more precise statements.)

We can restate H.I.T. as the assertion that the roots of $F(n,Y) = 0$ have degree d over $\mathbb{Q}$ for infinitely many $n \in \mathbb{N}$ or even, letting θ be an algebraic function solution of $F(X,\theta(X)) = 0$, we may say that the degree over $\mathbb{Q}$ of the values of θ at infinitely many rational integers n equals the degree of θ over $\mathbb{Q}(X)$.[1]

[1] Of course the value of an algebraic function at n is not well defined. However in this case, as well as in what follows, it turns out that the choice of the "branch" makes no difference.

Pervenuto alla Redazione il 17 Febbraio 1993 e in forma definitiva il 26 Aprile 1994.

In this context the following problem seems natural to us: *To determine, or estimate, the degree obtained adjoining to* $\mathbb{Q}$ *many values of type* $\theta(n)$. In other words we ask how independent are the values of an algebraic function at rational integral arguments. The problem is clearly capable of generalizations. However in the present paper we shall discuss only the basic case just mentioned.

We shall prove some results concerning the order of magnitude, for $n \to \infty$, of the degree over $\mathbb{Q}$ of fields of type

$$k(n) = \mathbb{Q}(\theta_1, \dots, \theta_n) \tag{3}$$

for a prescribed sequence $\{\theta_j\}$ satisfying $F(j, \theta_j) = 0$.

Actually we shall first give some simple result for an analogous "functional problem"; namely, given a field Γ, assumed to be of characteristic zero, we shall consider the degree over $\Gamma(X)$ of the fields

$$k_*(n) = \Gamma(X, \psi(X), \dots, \psi(X + n - 1)) \tag{4}$$

$\psi(X + h)$ being a root of $F(X + h, Y) = 0$.

The interest of these fields in connection with the previous problem may be motivated as follows: if F has rational coefficients and ρ is a suitable primitive element for $k_*(n)$ over $\mathbb{Q}(X)$ then the values $\rho(j)$ (see footnote (1)) lie in the composite field $L \cdot k(n + j)$ for some choice of the sequence $\{\theta_j\}$ and for some fixed algebraic number field L independent of n, so, at least in principle, using some explicit version of H.I.T. one may get lower bounds for $[k(m) : \mathbb{Q}]$ from a knowledge of the degree of ρ over $\mathbb{Q}(X)$. This idea may in fact be carried out to prove at least the result $[k(m) : \mathbb{Q}] \to \infty$ for all sequences $\{\theta_j\}$ as above, if $D > 1$ and F is absolutely irreducible.(2) Although we shall obtain much more about $k(n)$, we have included some results about $k_*(n)$ as well.

One easily proves that, even assuming F to be absolutely irreducible, the degree $D_*(n) = [k_*(n) : \Gamma(X)]$ may be sometimes substantially smaller than the obvious upper estimate d^n; to construct such examples let $\psi_1(X)$ be of degree $d_1 > 1$ over $\Gamma(X)$ and put $\psi(X) = \psi_1(X) + c\psi_1(X + 1)$, where $c \in \Gamma$ is such that ψ is a primitive element for $\Gamma(X, \psi_1(X), \psi_1(X + 1))$ over $\Gamma(X)$. Then, easily

$$[k_*(n + 1) : k_*(n)] \leq d_1 < d \tag{5}$$

where $d = [\Gamma(X, \psi(X)) : \Gamma(X)]$, whence $D_*(n) \ll d_1^n$.(3)

(2) Such qualitative estimate may also be obtained directly from the version of Hilbert's theorem valid for polynomials over general number fields; in fact, under the above assumptions, there exists, given any n, a natural number $n' > n$ such that $F(n', Y)$ is irreducible over $k(n)$. Then $k(n')$ contains $k(n)$ properly.

(3) The construction may be generalized to obtain algebraic functions ψ of arbitrarily large degree d and such that $D_*(n) \ll 2^n$ (consider for instance $\psi_h(X) = \sqrt{X} + \sqrt{X+1} + \dots + \sqrt{X+h}$), substantially a best possible bound.

However we shall see in Theorem 1 (b) that we always have exponential growth.

In the numerical case the behaviour of $D(n) = \min[k(n) : \mathbb{Q}]$, where the minimum is taken over all sequences $\{\theta_j\}$ as above, is still further from the upper bound d^n, as we can see in a most simple class of examples, namely setting $F(X,Y) = Y^d - X$, where $d \geq 2$.

Now we have

$$(6) \qquad k(n) \subset \mathbb{Q}(\varsigma, p^{\frac{1}{d}},\ p \text{ prime},\ p \leq n)$$

where $\varsigma = \exp \dfrac{2\pi i}{d}$, whence

$$(7) \qquad D(n) \ll d^{\pi(n)} \ll d^{(1+\epsilon)\frac{n}{\log n}}$$

for any $\epsilon > 0$.

These examples are essentially the best possible, since an estimate

$$(8) \qquad D(n) \gg c^{\frac{n}{\log n}} \qquad c = c(F) > 1 \text{ for } d > 1$$

will be shown to hold generally.

Moreover we shall produce a class of polynomials F such that $D(n)$ has exponential growth.

Our results are the following:

THEOREM 1. (a) *Let $F \in \Gamma[X,Y]$ be irreducible. Then there exists a finite set $S_F \subset \Gamma$ such that, if $N_1, \ldots, N_k \in \Gamma$ satisfy $N_i - N_j \notin S_F$ for $i \neq j$, then*

$$[\Gamma(X, \psi(X+N_1), \ldots, \psi(X+N_k)) : \Gamma(X)] = d^k.$$

(b) *For distinct $N_1, \ldots, N_k$ we have*

$$[\Gamma(X, \psi(X+N_1), \ldots, \psi(X+N_k)) : \Gamma(X)] \geq 2^{k-1}d,$$

provided $d > 1$.

Here $\psi(X+h)$ is any root of $F(X+h, Y) = 0$.

In the more interesting numerical case we have:

THEOREM 2. (a) *For all absolutely irreducible $F \in \mathbb{Q}[X,Y]$ of degree in Y greater than 1 we have the estimate*

$$D(n) \gg c^{\frac{n}{\log n}}$$

where $c > 1$ depends only on F.

(b) *Assume the discriminant $\Delta(X)$ of the splitting field of F over $\mathbb{Q}(X)$ (with respect to $\mathbb{Q}[X]$) has an irreducible factor (over $\mathbb{Q}$) of degree 2 or 3. Then*

$$D(n) \gg c^n$$

for some $c = c(F) > 1$.

We conjecture that in Theorem 2 (b) "degree 2 or 3" may be replaced by "degree ≥ 2". Without such an assumption the result does not hold in full generality, in view of the above examples.

Professor A.Schinzel has formulated an interesting and more precise conjecture, which we cannot prove at present even in the most simple nontrivial cases. Namely

$D(n)$ should have exponential growth except when:

(i) *$\Delta(X)$ splits into linear factors over $\mathbb{Q}$.*

(ii) *The splitting field $\tilde{\Sigma}$ of $F(X,Y)$ over $\overline{\mathbb{Q}}(X)$.*[4] *is an abelian extension of $\overline{\mathbb{Q}}(X)$.*

By applying Kummer Theory it is easy to see that (i) and (ii) imply that the splitting field Σ of $F(X,Y)$ over $\mathbb{Q}(X)$ is contained in a finite extension of $\mathbb{Q}(X)$ obtained as a composite of fields of type $L(\rho)$, where L is a number field and $\rho^h = l(X)$ for some positive integer h and some linear polynomial $l(X) \in \mathbb{Q}[X]$, so we would practically reduce to the simple examples mentioned before.

As remarked above our methods, which are based on the concept of ramification used as a tool to distinguish different fields, are inadequate to attack such a problem: even assuming deep conjectures from the theory of the distribution of power free values of polynomials (whose significance in our setting shall be clear from the proof of Theorem 2), which would enable us to remove the restriction on degrees in Theorem 2 (b), new ideas seem to be required to deal with the "algebraic part" of Schinzel's conjecture. While revising the present paper the authors have however obtained some progress in this direction; the results will appear in a forthcoming paper.

We remark that Theorem 2 (a) remains valid for polynomials over number fields, and that the assumption about absolute irreducibility may be weakened to "*The absolutely irreducible factors of F have degree ≥ 2*". However the proofs of these more general results do not require ideas different from those already occurring here, so we have preferred not to discuss them for the sake of simplicity.

It is perhaps worth mentioning that the results obtained here appeared in a preliminary version several years ago, as a preprint of the University of Pisa [9], which has been quoted by P. Debes in his survey [8]. For a number of reasons, including the hope of getting substantial improvements, the publication of a final version has been delayed up to now.

[4] From now on a bar denotes algebraic closure.

Finally, in the appendix, we shall show how the method of proof of Theorem 2 can be applied to the effective solution of a diophamtine problem, namely, the problem of finding the integers m for which $F(m, Y)$ splits into linear factors in $\mathbb{Q}[Y]$. This problem was however solved by Belotserkovski (Bilu).

Throughout the paper the letters m, n will denote natural numbers, while p will stand for a prime number.

1. - Auxiliary results

We first briefly recall the definition and main properties of the discriminant. For details and proofs see any book on Algebraic Number Theory e.g. [6] or [18].

Let A be a Dedekind domain, K be its quotient field, L be a finite separable extension of K of degree d and finally let B be the integral closure of A in L.

Let $W = \{w_1, \dots, w_d\}$ be a d-tuple of elements of L and define the "discriminant of W" as

$$D(W) = D_{L/K}(W) = \det(\sigma_i w_j)^2$$

the σ_i being the isomorphisms of L over K in some algebraic closure.

From the formula $D(W) = \det(\mathrm{Tr}(w_i w_j))$ it follows that $D(W) \in K$. Moreover it may be easily seen that the principal fractional ideal $AD(W) \subset K$ depends only on the module $\sum Aw_j$ and is the zero ideal if and only if the w_i are linearly dependent over K.

Now specialize to the case when A is principal. (We shall use the present concepts only when A is either $\mathbb{Z}$ or $\Gamma[X]$ for Γ a field. For the general case see for instance [18]). In this situation B is a free A-module of rank d. Define then the "discriminant of L" (with respect to A) as

$$\Delta(L) = AD(W) \quad \text{where} \quad B = \oplus_{i=1}^{d} Aw_i$$

Recall that if P is a prime ideal in A, P is said to be "ramified" in B (or in L) if in the factorization

$$PB = Q_1^{e_1} \dots Q_s^{e_s} \qquad e_i = e(Q_i|P)$$

where the Q_i are distinct prime ideals in B, at least one of the ramification indices e_i is > 1.

We recall the following classical results in a Lemma, where all the discriminants involved are taken with respect to A.

LEMMA 1.1. (i) *If P is a prime ideal in A then P ramifies in L if and only if it divides $\Delta(L)$.*

(ii) *If $K \subset L \subset M$ then the prime divisors of $\Delta(L)$ divide $\Delta(M)$.*

(iii) *The prime divisors of $\Delta(LM)$, where $K \subset L \cap M$ divide the product $\Delta(L)\Delta(M)$.*

Take in particular $A = \Gamma[X]$ and $F \in \Gamma[X,Y]$ an absolutely irreducible polynomial. (Here Γ is, as above, a field of characteristic zero.) Define L as the extension of $\Gamma(X)$ determined by a root of F. The discriminant $\Delta(L)$ is generated by a polynomial with coefficients in Γ; we may assume it to be monic and unambiguously denote it with the same symbol $\Delta(L)$. From the absolute irreducibility of F it follows that such polynomial remains unchanged if we replace Γ by its algebraic closure $\overline{\Gamma}$.

We also recall from the classical theory of function fields (see for instance [1]) that the prime ideals of $\overline{\Gamma}B$, which is the integral closure of $\overline{\Gamma}[X]$ in $\overline{\Gamma}L$, correspond to the finite places of $\overline{\Gamma}L$, i.e. those not lying above the place ∞ of $\overline{\Gamma}(X)$.

Assume $d = \deg_Y F > 1$ i.e. $L \neq \Gamma(X)$. Then we have the following well known result (whose short proof is recalled for the reader's convenience). It is the analogue of Minkowsky's theorem stating the existence of ramified primes in all number rings but $\mathbb{Z}$.

LEMMA 1.2. *$\Delta(L)$ is nonconstant, i.e. there exists at least one ramified finite place of L.*

PROOF. By the above remarks we may work over $\overline{\Gamma}(X)$ and replace L by $\overline{\Gamma}L$, the extension of $\overline{\Gamma}(X)$ determined by a root of F.

From the Hurwitz genus formula we have, letting g be the genus of L,

$$2d + 2g - 2 = \sum_{v}(e_v - 1) = \sum_{v \not| \infty}(e_v - 1) + \sum_{v | \infty}(e_v - 1)$$

Now $g \geq 0$ while the second summation on the right is trivially bounded by $d - 1$ whence

$$d - 1 \leq \sum_{v \not| \infty}(e_v - 1)$$

Since $d > 1$ we get the Lemma and even more.

In the sequel we shall need the following classical result from the analytic theory of algebraic numbers. It appears as Corollary 1 to Theorem 8 in Ch.8 of [6].

LEMMA 1.3. *Let $f \in \mathbb{Z}[X]$ have exactly s distinct irreducible factors over the rationals. Then, letting for a prime p, $n(p)$ be the number of solutions of the congruence $f(n) \equiv 0 \pmod{p}$, $n \in \mathbb{F}_p$, we have the asymptotic formula*

$$\sum_{p \leq x} n(p) \sim s \frac{x}{\log x}$$

The following simple estimate will be useful in a moment:

LEMMA 1.4. *Let g be an irreducible quadratic polynomial with rational integral coefficients. Then, for large x,*

$$E_g(x) = \#\{p \geq x : g(m) \equiv 0 \ (\operatorname{mod} p^2) \textit{ has a solution } 0 \leq m \leq p\} \ll \log x.$$

PROOF. $g(m) \equiv 0 \ (\operatorname{mod} p^2)$, $0 \leq m \leq p$ implies $g(m) = kp^2$ where k is bounded independently of m. Multiplying by $4a$ where a is the leading coefficient of g and changing variables we get an equation

$$m_*^2 - 4akp^2 = A$$

where m_* is an integer and where A is a fixed integer which is not a square in view of the irreducibility of g.

For every fixed $k \neq 0$ classical Pell's equation theory (see for instance [15]) gives the desired estimate while for $k = 0$ we have no solution, and the result follows. □

REMARK. It can be shown (see the proof of Theorem 2 (b)) that if $g \in \mathbb{Z}[X]$ is an irreducible polynomial of degree ≥ 2 then

$$(1) \qquad \#\{p \geq x, \ p | g(m) \text{ for some } m \leq x\} \gg x.$$

It shall be clear in the sequel that to prove the conjecture stated immediately after Theorem 2 we would need the estimate

$$(2) \qquad \#\{p \geq x, \ p || g(m) \text{ for some } m \leq x\} \gg x.$$

When $\deg g = 2$ this follows immediately from (1) combined with Lemma 1.4. When $\deg g = 3$ we may still deduce (2) from (1) by using the following Theorem of Hooley on square-free values of polynomials.

HOOLEY'S THEOREM. *Let $g(X)$ be a cubic irreducible polynomial with integer coefficients, T be a fixed real number and define*

$$E(T, x) = \#\{m \leq x : \forall \text{ primes } p > T, \ p^2 \nmid g(m)\}$$

Then $E(T, x) \sim c(T)x$ when $x \to \infty$, where $c(T) \to 1$ when $T \to \infty$.

In fact Hooley's result in [12] is stated for $T = 1$ with an explicit formula for $c(1)$ in terms of the number of solutions of congruences of the form $g(m) \equiv 0$ $(\operatorname{mod} p^2)$. However his proof leads to the present Theorem with practically no changes: it is only necessary to introduce the parameter T and otherwise follow strictly Hooley's arguments. We omit details for simplicity, Hooley's proof being quite involved.

To see why this result combined with (1) implies (2) for cubic irreducible polynomials observe that, for large x,

$$\#\{p : \exists m \leq x,\ p^2|g(m)\} \leq \pi(x) + \#\{p : p > x, \exists m \leq x,\ p^2|g(m)\} \leq$$
$$\leq \mathrm{o}(x) + \#\{m \leq x : \exists p > x,\ p^2|g(m)\} = x - E(x,x) + \mathrm{o}(x)$$

since, for $m \leq x$, there exists at most one prime $p > x$ whose square divides $g(m)$, g being a cubic polynomial.

Observe that the definition directly implies that $E(T,x)$ is a non-decreasing function of T (for fixed x), so, for any given T we have, for large x, $x - E(x,x) \leq x - E(T,x) = (1 - c(T))x + \mathrm{o}(x)$. Since T is arbitrary and since $c(T) \to 1$ we deduce $x - E(x,x) = \mathrm{o}(x)$ and the resulting asymptotic inequality, combined with (1), clearly proves (2).

The general case of arbitrary degree, which, as remarked above, would give a corresponding improvement of Theorem 2 (b) seems quite deep, in any case not available in the existing literature.

To prove (1) we shall use a result of Nagell [16].

LEMMA 1.5. *Let $g \in \mathbb{Z}[X]$ be irreducible of degree at least two. Let x be a large real number and, for a natural number $m \leq x$ set $g(m) = A(m)B(m)$ where $A(m)$, $B(m)$ are the factors of $g(m)$ formed with the prime numbers $\leq x$ and $> x$ respectively. Then:*

$$\sum_{m\leq x} \log A(m) \leq x \log x + \mathrm{O}(x).$$

We state one more result about field extensions of finite degree. It is certainly well known but for the sake of completeness we give a short proof.

For F/K a finite degree extension denote by F_* the normal closure of F over K.

LEMMA 1.6. *Let A, B be finite extensions of K such that $A_* \cap B_* = K$. Then*

$$[AB : K] = [A : K][B : K].$$

PROOF. One needs to prove that $[AB : A] = [B : K]$. Let $b \in B$ be a primitive element of the extension B/K and P be its irreducible (monic) polynomial over K. If $P = QR$ with Q, R monic polynomials in $A[Y] \setminus A$, there exists at least one coefficient of Q or R in $A \setminus K$. This coefficient also lies in B_*, which contradicts $A \cap B_* = K$. □

2. - Proof of Theorem 1

Let L be the splitting field of F over $\Gamma(X)$. Define $\Delta(L)$ to be the discriminant taken with respect to $\Gamma[X]$ and let S_F be the set of differences of the roots of a generator $G(X)$, say, for $\Delta(L)$ which, by Lemma 1.2, is a nonconstant polynomial with coefficients in Γ.

Also, for a finite extension M of $\Gamma(X)$ let M_* denote its normal closure over $\Gamma(X)$.

From Lemma 1.6 it follows immediately that for the proof of Theorem 1 (a) it suffices to show that

$$\Gamma(X, \psi(X+N_i))_* \cap \prod_{j \neq i} \Gamma(X, \psi(X+N_j))_* = \Gamma(X).$$

Assume the contrary. Then the above intersection is a proper extension of $\Gamma(X)$ whence, in view of Lemma 1.2, its discriminant is generated by a nonconstant polynomial $\delta(X)$, say. By Lemma 1.1 (ii) the linear factors of $\delta(X)$ divide both the discriminants of $\Gamma(X, \psi(X+N_i))_*$ and of $\prod_{j \neq i} \Gamma(X, \psi(X+N_j))_*$.

Now, the discriminant of $\Gamma(X, \psi(X+N_i))_*$ is immediately seen to be generated by $G(X+N_i)$. In particular, by Lemma 1.1 (iii) the factors of $\Delta\left(\prod_{j \neq i} \Gamma(X, \psi(X+N_j))_*\right)$ divide $\prod_{j \neq i} G(X+N_j)$.

On the other hand, by the very definition of S_F the polynomials $G(X+N_i)$ and $\prod_{j \neq i} G(X+N_j)$ are coprime, a contradiction which proves part (a) of our Theorem.

The proof of part (b) is entirely analogous, but requires a preliminary observation. If A is a subset of Γ, we say that an element $\alpha \in \Gamma$ lies in the convex hull of A if $\alpha = \sum r_i a_i$ where $a_i \in A$ and r_i are non-negative rational numbers with sum 1. Then

Let R, $S \subset \Gamma$ be finite sets. Assume that $r \in R$ does not lie in the convex hull of $R - \{r\}$. Then

$$S + r \not\subset \bigcup_{\rho \in R - \{r\}} (S + \rho).$$

In fact assume the contrary; then we may write, letting $s_1 \in S$,

$$s_1 + r = s_2 + \rho_1, \quad \text{for some } s_2 \in S, \rho_1 \in R - \{r\}$$

$$s_2 + r = s_3 + \rho_2, \quad \text{for some } s_3 \in S, \rho_2 \in R - \{r\}$$

and so on. Sooner or later we shall obtain $s_u = s_{u+k}$ for some nonzero k whence, summing the equations corresponding to $u, \ldots, u+k-1$, we get

$$kr = \rho_u + \ldots + \rho_{u+k-1},$$

a contradiction.

To apply this to the proof of Theorem 1 (b) set $R = \{-N_1, \ldots, -N_k\}$, $S = \{\alpha : G(\alpha) = 0\}$ where G has been defined above.

Choose an index i such that $-N_i$ does not belong to the convex hull of $R - \{-N_i\}$: this is certainly possible as we can for instance embed $\mathbb{Q}(R)$ in $\mathbb{C}$ and so look at the elements of R as complex numbers, in which case the assertion holds. Apply then the above proposition with $r = -N_i$.

We obtain that, for at least one root β of $G(x + N_i)$, we have

$$\prod_{j \neq i} G(\beta + N_j) \neq 0.$$

From this we may deduce, arguing as in the proof of part (a), that

$$\Gamma(X, \psi(X + N_i))_* \not\subset \prod_{j \neq i} \Gamma(X, \psi(X + N_j))_*$$

and Theorem 1 (b) follows at once by induction on k. □

3. - Proof of Theorem 2

PROOF OF PART (a). Let $L(j)$ be the splitting field over $\mathbb{Q}$ of the polynomial $F(j, Y)$. We shall first prove a lower bound for

$$\tilde{D}(n) = [\tilde{k}(n) : \mathbb{Q}]$$

where $\tilde{k}(n)$ is the composite of the fields $L(j)$ for $1 \leq j \leq n$.

H.I.T. will then be applied to deduce our original statement.

To obtain such a lower bound we shall construct many values of m such that $L(m)$ is not contained in $\tilde{k}(m-1)$.

Using the results stated in Lemma 1.1 it will be sufficient to produce values of m such that $\Delta(L(m))$ – the discriminant of $L(m)$ with respect to $\mathbb{Z}$ – has at least one prime factor not dividing $\Delta(\tilde{k}(m-1))$.

On the other hand the prime factors of $\Delta(\tilde{k}(m-1))$ are just the primes dividing some $\Delta(L(j))$, $1 \leq j \leq m-1$, by Lemma 1.1 (iii).

In conclusion we must investigate the prime factors of $\Delta(L(m))$, i.e. the rational primes which ramify in $L(m)$.

Let Σ be a splitting field for $F(X, Y)$ over $\mathbb{Q}(X)$ and let $G(X)$ be a generator for the discriminant of Σ (with respect to $\mathbb{Q}[X]$): we may assume that G is a polynomial with coprime rational integral coefficients. Also, in view of Lemma 1.2, we may assume $G(X)$ is nonconstant.

Now, it is natural to assume the existence of some relation between $\Delta(L(m))$ and $G(m)$, the specialization of the discriminant of Σ.[5] At first sight

[5] A result which, as a particular case, has implications in this direction is the "*Chevalley - Weil Theorem*". It appears for instance in [14], p. 44 or in [19], p. 50. In fact the affine version of it, mentioned in [19], implies our Lemma 3.1 below.

one could even attempt to parametrize $\Delta(L(m))$ for instance with $G(m)$ itself, or try to parametrize some integral basis for the integers of $L(m)$ with the specialization of an integral basis for the integers of Σ (over $\mathbb{Q}[X]$).

In fact there is such a relation, but it does not hold for all m. To see this consider for instance the simple case when $F(X,Y) = Y^2 - X$. We have $\Sigma = \mathbb{Q}(\sqrt{X})$, $G(X) = X$, but, if for instance $m = s^2$, then $L(m) = L(s^2) = \mathbb{Q}$ and $\Delta((L(m)) = 1$.

We shall show that, however, for many values of m, some of the prime factors of $G(m)$ divide $\Delta(L(m))$, and this will be sufficient for our purposes.

We begin by proving the simpler "inverse property", namely:

LEMMA 3.1. *There exists an integer* $A \neq 0$ *such that*

$$\Delta(L(m))|AG(m) \qquad \textit{for all large } m.$$

PROOF. Preliminary to the main argument we make the following agreement about specializations of algebraic functions. Choose once for all, for each natural number m, a point P_m of the algebraic curve associated to Σ, lying above m.[6] For a function $\xi \in \Sigma$ defined at P_m we put

$$\xi(m) = \xi(P_m)$$

Let $e_1(X), \dots, e_k(X)$ be an integral basis for the integers of Σ over $\mathbb{Q}[X]$.

Since the $e_i(X)$ span Σ over $\mathbb{Q}(X)$ we may write, for each root $\psi_j(X)$ of the equation in Y, $F(X,Y) = 0$,

$$\psi_j(X) = \sum_{i=1}^{k} C_{i,j}(X) e_i(X) \tag{1}$$

where the $C_{i,j} \in \mathbb{Q}(X)$.

If the integer m is large enough all the functions involved are defined at P_m so we may specialize (1) according to the above rule. Since the numbers $\psi_j(P_m)$, $1 \leq j \leq d$, run over the roots of $F(m,Y) = 0$, we conclude that the algebraic numbers $e_i(m)$ generate $L(m)$ over $\mathbb{Q}$.

Define $s = [L(m) : \mathbb{Q}]$ and assume, after renumbering the indices, that $e_1(m), \dots, e_s(m)$ are linearly independent over $\mathbb{Q}$.

Consider the polynomial

$$G^*(X) = \det{}^2(\sigma_j e_i(X)) \tag{2}$$

where σ_j runs through $\mathrm{Gal}(\Sigma/\mathbb{Q}(X))$.

[6] Considering m as a point of $\mathbb{Q}(X)$.

We may assume, replacing the e_i if necessary by suitable constant multiples, that G^* has integral coefficients whence, since G is primitive,

$$G^*(X) = A^*G(X) \qquad \text{for some nonzero } A^* \in \mathbb{Z}$$

Let $\xi(X)$ be a primitive element for Σ over $\mathbb{Q}(X)$ and let $g(X, \xi) = 0$ be its minimal equation. Specializing, as we may, for large m we get

$$g(m, \xi(m)) = 0.$$

The polynomial $g(m, Y)$ has coefficients in $\mathbb{Q}$ whence all the conjugates of $\xi(m)$ lie among its roots, which are the numbers $(\sigma_j\xi)(m)$, $j = 1, \dots, k$.

Let $\rho_1, \dots, \rho_s$ be the automorphisms of $L(m)$ over $\mathbb{Q}$. We may renumber the indices $\{1, \dots, k\}$ so that

$$\rho_i(\xi(m)) = (\sigma_i\xi)(m) \qquad i = 1, \dots, s.$$

Since

$$e_\mu(X) = \sum_{j=0}^{k-1} c_{\mu,j}(X)\xi^j(X) \qquad \mu = 1, \dots, k,$$

for suitable $c_{\mu,j} \in \mathbb{Q}(X)$, we get, for large m

$$\rho_i(e_\mu(m)) = (\sigma_i e_\mu)(m), \quad i = 1, \dots, s, \quad \mu = 1, \dots, k.$$

Let E be the matrix $(\rho_j(e_i(m))) = ((\sigma_j e_i)(m))$ for $1 \leq i \leq k$, $1 \leq j \leq s$. Then, since the $e_i(m)$ may be assumed to be algebraic integers in $L(m)$ (if not this may be achieved by multiplying them by a suitable integer independent of m), every $s \times s$ minor of E is divisible by $\sqrt{\Delta(L(m))}$, in the sense that the quotient is an algebraic integer.

Put $X = m$ in (2) and expand the determinant appearing there, according to Laplace's rule, along the upper $s \times s$ minors. Observe that the first s rows of the corresponding matrix constitute just the matrix E, whence, by the result just proved, we get the lemma. □

We shall now prove a crucial result, namely the above mentioned partial converse of Lemma 3.1.

LEMMA 3.2. *Let p be a prime number dividing $G(m)$. Then, if p is large enough, it divides the product $\Delta(L(m))\Delta(L(m+p))$.*

PROOF. Let $g \in \mathbb{Z}[X]$ be any irreducible factor of $G(X)$.

By Lemma 1.1 (i) $g(X)$, which is a prime of $\mathbb{Q}[X]$, ramifies in Σ.

Since Σ is a normal extension of $\mathbb{Q}(X)$ the ramification indices of the prime ideal divisors of $(g(X))$ (in the integral closure B of $\mathbb{Q}[X]$ in Σ) are all equal, as is well known. So we may write

$$g(X)B = \Omega^e \tag{3}$$

where Ω is an ideal in B and where $e \geq 2$.

Let $\omega_1, \dots, \omega_t$ be generators for Ω, normalized in such a way to take algebraic integer values on large rational integers m.[7] Let $B(m)$ be the ring of algebraic integers in $L(m)$ and define $\Omega(m)$ as the ideal in $B(m)$ generated by $\omega_1(m), \dots, \omega_t(m)$.

From (3) we have

$$g(X) = \sum_{(i)} R_{(i)}(X)\omega_1^{i_1}(X)\dots\omega_t^{i_t}(X) \tag{4}$$

where (i) runs over the t-tuples $(i_1, \dots, i_t)$ of natural numbers satisfying $i_1 + \dots + i_t = e$ and where $R_{(i)} \in B\mathrm{I}$.

Let A^* be a nonzero rational integer such that $A^* R_{(i)}(m) \in B(m)$ for all (i) and all large m. (Such an integer clearly exists, for the $R_{(i)}$ satisfy monic equations over $\mathbb{Q}[X]$.)

Specializing formula (4) we then obtain

$$A^* g(m)B(m) \subset \Omega^e(m) \quad \text{for } m > z_0. \tag{5}$$

To obtain an opposite inclusion observe that (3) implies for all (i) as above

$$\omega_1^{i_1}(X)\dots\omega_t^{i_t}(X) = S_{(i)}(X)g(X) \tag{6}$$

where $S_{(i)}(X) \in B$.

Now choose as before a nonzero rational integer A_* such that $A_* S_{(i)}(m) \in B(m)$ for $m > x_0$ and specialize (6) to obtain

$$A_* \Omega^e(m) \subset g(m)B(m). \tag{7}$$

Now let m be an integer and p be a large rational prime such that $p||g(m)$. Then, by (7), $pB(m)|A_*\Omega^e(m)$ and, if p is large enough,

$$pB(m)|\Omega^e(m). \tag{8}$$

Let $\Omega(m) = P_1^{r_1} \dots P_h^{r_h}$ be the prime ideal factorization of $\Omega(m)$ in $B(m)$.

From (8) we obtain that at least one of the P_j, say P_1, is a prime ideal divisor of $pB(m)$.

On the other hand (5) implies that $P_1^{r_1 e}$ divides $A^* g(m)B(m)$ so, if p is larger that A^* this relation forces $P_1^{r_1 e}|g(m)B(m)$.

Now, since P_1 divides p, it cannot divide other rational primes. Also, since $g(m)$ is rational and since p divides $g(m)$ *exactly*, the last relation implies

$$P_1^{r_1 e}|pB(m)$$

so p ramifies in $L(m)$, whence $p|\Delta(L(m))$ by Lemma 1.1 (i).

[7] We adopt the convention described at the beginning of the proof of Lemma 3.1 to define $\omega_i(m)$.

To find primes dividing exactly some value $g(m)$ we use an argument which appears already in [7].

Since $g(X)$ is irreducible it has no common factor with its derivative g' whence we have an equation

$$T(X)g(X) + U(X)g'(X) = c(g) \tag{9}$$

where T, U are polynomials with rational integral coefficients and where $c(g)$ is a nonzero rational integer (which may be taken to be the "discriminant" of g).

Let now p be a sufficiently large prime number dividing $G(m)$. Then p divides some $g(m)$, g being an irreducible factor of G. If $p||g(m)$ the above arguments prove the Lemma. Otherwise $p^2|g(m)$, whence, for $p > \deg g$,

$$g(m+p) = g(m) + pg'(m) + p^2 \frac{g''(m)}{2} + \ldots \equiv pg'(m) \pmod{p^2}.$$

But p cannot divide $g'(m)$ as well, otherwise, by (9), $p|c(g)$, which does not hold if p is large enough.

The last congruence then implies $p||g(m+p)$, and the preceding argument applies with $m+p$ in place of m, proving completely Lemma 3.2. □

REMARK 1. It appears from the proof that "sufficiently large" can be made explicit in terms of the magnitude of the coefficients of the polynomial F.

REMARK 2. From the proof of Lemma 3.2 one can get in fact the following more precise statement:

Let $g(X)$ be any irreducible factor of $G(X)$ in $\mathbb{Z}[X]$. Then there exists an integer $e \geq 2$ (the ramification index of g in Σ) with the following property: if p is a sufficiently large rational prime such that

$$\operatorname{ord}_p g(m) \not\equiv 0 \pmod{e}$$

then p ramifies in $L(m)$.

This result could be derived also invoking the Weil's famous decomposition Theorem (see [20] or [14] Ch. 10) which roughly speaking states that the divisor of a rational function on an algebraic curve defined over a number field K determines a corresponding factorization of its values at K-rational points on the curve. We give a brief argument, and refer to the statement appearing in [14], p. 263. We take V to be the nonsingular curve (over the algebraic closure of $\mathbb{Q}$ in Σ) with function field Σ. We take as rational function φ our polynomial g and put $P = P_m$ (as in the beginning of the proof of Lemma 3.1). The divisor of zeros of g is of the form

$$(g)_0 = eD$$

for some positive divisor D, whence all the integers m_W in Lang's statement which are positive are multiples of e. Let p be a prime number and v be an extension to $\overline{\mathbb{Q}}$ of the p-adic valuation on $\mathbb{Q}$. The statement referred to above implies that, for p larger than some number depending only on V,

$$v(g(m)) = ev(\lambda_m)$$

for some $\lambda_m \in L(m)$: in fact the terms $\gamma_i(v)$ vanish by definition for large enough p. Also, all the $\lambda_W(P, v)$ lie in the image of v on $L(m)^*$ for large p, by the construction of the Weil functions. Finally, for large p and W lying above the infinite point of $\mathbb{Q}(X)$, $\lambda_W(P, v)$ vanishes, as may be proved by looking again at the construction of Weil functions (observe for instance that both functions $1/X$, $1/(X+1)$ vanish at each such W, and one at least of them is a v-unit at P_m). This clearly proves what we want.

Using Lemmas 3.1 and 3.2 we may estimate $\tilde{D}(n)$ in the desired way.

Let x be a large real number and set

$$P(x) = \left\{p : \frac{x}{4} < p < \frac{x}{2},\ p|G(m) \text{ for some } m\right\}$$

and

$$j(p) = \inf\{m \geq 0 : p \text{ ramifies in } L(m)\}.$$

From Lemma 3.2 it follows that, if $p \in P(x)$ then we have $j(p) \leq x$.

In fact if $p \in P(x)$ there exists a natural number m such that $m \leq p \leq \frac{x}{2}$ and $p|G(m)$. So we have $m+p \leq x$ and Lemma 3.2 applies since $p \geq \frac{x}{4}$ is very large.

Moreover, from the definition of $j(p)$, it is clear that p does not ramify in any field $L(a)$ for $1 \leq a \leq j(p) - 1$, whence it is still unramified in their compositum $\tilde{k}(j(p) - 1)$, so, in particular,

$$L(j(p)) \not\subset \tilde{k}(j(p) - 1).$$

We then have

$$[\tilde{k}(j(p)) : \tilde{k}(j(p) - 1)] \geq 2$$

whence

$$\tilde{D}(j(p)) \geq 2\tilde{D}(j(p) - 1)$$

and, setting

$$J(x) = \#\{j(p) : p \in P(x)\}$$

we obtain

$$\tilde{D}(x) \geq 2^{J(x)}.$$

To bound $J(x)$ from below observe that, if $p \in P(x)$, then $p|\Delta(L(j(p)))$ and, p being large, Lemma 3.1 implies $p|G(j(p))$.

Set $v = \deg G$. Then $v \geq 1$ by Lemma 1.2.

We contend that, for $m \leq x$,

$$\#\{p \in P(x) : j(p) = m\} \leq v.$$

Indeed every prime counted divides by the above $G(m)$ and is larger than $\frac{x}{4}$, whence the total number N of such primes satisfies $N \leq \left[\frac{\log G(m)}{\log \frac{x}{4}}\right] \leq v$ for large x.

From this inequality we clearly derive

$$J(x) \geq \frac{1}{v}\#P(x).$$

Finally, applying Lemma 1.3 with $f = G$ we obtain

$$\sum_{\frac{x}{4} \leq p \leq \frac{x}{2}} n(p) \sim s \frac{x}{4 \log x}$$

for a certain positive integer s, whence, since $n(p) \leq v$,

$$\#P(x) \geq \frac{x}{5v \log x}$$

for large x, whence

$$J(x) \geq \frac{1}{5v^2} \frac{x}{\log x}$$

thus concluding the proof of Theorem 2 (a) with $\tilde{D}$ in place of D.

To complete the proof of Theorem 2 (a) choose a sequence $\{\theta_j\}$ satisfying $F(j, \theta_j) = 0$ and the corresponding field

$$k(n) = \mathbb{Q}(\theta_1, \dots, \theta_n).$$

We observe at once that

$$\tilde{D}(m) = [\tilde{k}(m) : \mathbb{Q}] = \prod_{j=1}^{m-1} [\tilde{k}(j+1) : \tilde{k}(j)] \leq (d!)^{\tilde{h}(m)} \tag{10}$$

where $d = \deg_Y F$ as usual and

$$\tilde{h}(m) = \#\{j \leq m : \tilde{k}(j+1) \neq \tilde{k}(j)\}.$$

Indeed any factor in the middle term of (10) is clearly bounded by $d!$.

CONTENTION. *If $\tilde{k}(j+1) \neq \tilde{k}(j)$ and $F(j+1, Y)$ is irreducible over $\mathbb{Q}$ then also $k(j+1) \neq k(j)$.*

In fact assume $k(j+1)=k(j)$. Then $\theta_{j+1}\in k(j)$ and, $F(j+1,Y)$ being irreducible, all of its roots must be contained in the normal closure $k_*(j)$ of $k(j)$ over $\mathbb{Q}$. But clearly such a field is contained in $\tilde{k}(j)$, whence $L(j+1)\subset\tilde{k}(j)$ and this means just $\tilde{k}(j+1)=\tilde{k}(j)$.

Setting then

$$h(m)=\#\{j\le m : k(j+1)\ne k(j)\}$$

we get

$$h(m)\ge\tilde{h}(m)-\#\{j\le m : F(j+1,Y)\text{ is reducible}\}.$$

By the quantitative version of H.I.T. recalled in inequality (2) of the Introduction the cardinality on the right is $\ll m^{\beta}$ for some $\beta<1$.

On the other hand by (10) and what has been proved above we have $\tilde{h}(m)\gg\dfrac{m}{\log m}$, whence $h(m)\gg\dfrac{m}{\log m}$ too, the bound holding uniformly in the sequence $\{\theta_j\}$.

Also

$$[k(m):\mathbb{Q}]=\prod_{j=1}^{m-1}[k(j+1):k(j)]\ge 2^{h(m)}$$

and Theorem 2 (a) follows since the bound for $h(m)$ is uniform.

Pproof of Part (b). We first prove formula (1) of Section 1 using Lemma 1.5.

With the notation of that Lemma, let $v=\deg g$. Then $v\ge 2$ by assumption. Elementary estimates show that

$$\sum_{m\le x}\log g(m)\ge vx\log x+O(x)$$

whence

$$\sum_{m\le x}\log B(m)\ge x\log x+O(x).$$

Now, since $\log B(m)\ll\log g(m)\ll\log m\le\log x$, we get

$$\#\{m\le x : B(m)\ne 1\}\gg x$$

Since every prime factor of $B(m)$ is by definition $\ge x$ and since a given prime $p\ge x$ may divide at most v among the $B(m)$, $m\le x$ (since otherwise g would have more than deg g distinct roots mod$p$ which is impossible for large p) we obtain

$$\#\{p\ge x : p|g(m)\text{ for some }m\le x\}\gg x$$

i.e. (1) of Section 1.

Recall now that in Section 1 we have shown, by means of Lemma 1.4 and of Hooley's Theorem, that, for irreducible polynomials g of degree 2 or 3, (1) implies (2) namely

$$\#\{p\ge x : p\|g(m)\text{ for some }m\le x\}\gg x. \qquad (11)$$

Recall also that, by Remark 2 to Lemma 3.2 it follows that, if g is an irreducible factor of G, then, for large x,

(12) If $p > x$ and $p||g(m)$ then p ramifies in $L(m)$.

Combining (11) and (12), Theorem 2 (b) follows by an argument completely similar to the one used for part (a).

REMARK. In analogy with Theorem 2 one may investigate the behaviour of

$$\tilde{D}_S(n) = \left[\prod_{m\in S, m\leq n} L(m) : \mathbb{Q}\right]$$

where S is a sequence of natural numbers.

In this situation, even when S has positive asymptotic density, the estimates of Theorem 2 are no longer generally true.

Define for instance $F(X,Y) = Y^2 - X$ and take

$$S = \{m : p|m \text{ implies } p \leq \sqrt{m}\}$$

One can prove (see [5]) that

$$\#\{s \in S : s \leq x\} \sim (1 - \log 2)x.$$

Also, observe that

$$\prod_{m\in S, m\leq x} \mathbb{Q}(\sqrt{m}) \subset \prod_{p\leq\sqrt{x}} \mathbb{Q}(\sqrt{p})$$

whence

$$\tilde{D}_S(n) \ll c^{\frac{\sqrt{n}}{\log n}}$$

for some $c > 1$.

Anyway the method of proof of Theorem 2 give, for a sequence S of positive upper asymptotic density, the estimate

$$\tilde{D}_S(n) \gg c^{n^\sigma}$$

for some $c > 1$, $\sigma > 0$ and some infinite sequence of n.

We omit details since no new idea is involved.

Appendix

In this Appendix we show how the above methods (in particular the method of proof of Lemma 3.2) can be applied to solve effectively the following diophantine problem:

Let $F(X,Y) \in K[X,Y]$, where K is a number field with ring of integers D. Determine $S = S_F = \{m \in D : F(m,Y)$ splits into linear factors in $K[Y]\}$.

It is easily shown that this problem is equivalent to determining the integral points on irreducible curves $G(X,Y) = 0$ which define a Galois extension of $K(X)$.

We remark that the problem has already been solved by Yu. Belotserkovski in the fundamental case when the splitting field Σ of F over $K(X)$ has positive genus (for the simple genus zero case see [21]). See [3], [4] for general results implying Theorem 3 below; the author gives also explicit estimates for the height of integral points. Even if the result of this Appendix is not new, we nevertheless have decided to include it just to show another application of the idea of considering the specialization of the functional discriminant.

We may assume F to be absolutely irreducible, of degree d^* in Y. We define Γ to be the extension of $K(X)$ determined by a root of $F(X,Y) = 0$. Also, let $\tilde{K}$ be the algebraic closure of K in Σ and let G be the Galois group of Σ over $\tilde{K}(X)$, having order d. Define Δ to be the ring of integers of Σ over $\tilde{K}[X]$. $\mathbb{A}$ will denote the field of algebraic numbers.

We shall prove the following:

THEOREM 3. *Let $F(X,Y) \in K[X,Y]$ be absolutely irreducible and assume that Σ has positive genus. Then the finitely many integers $m \in S$ may be effectively found.*[8]

As remarked before the case of genus zero is dealt with in [21].

PROOF. We give a direct argument, similar to the proof of Lemma 3.2. In this case too Weil's Decomposition Theorem could be applied.

Let $\alpha_1, \dots, \alpha_h \in \mathbb{A}$ be the distinct finite points of $\mathbb{A}(X)$ which ramify in $\mathbb{A}\Sigma$. Enlarging eventually K we may assume $K = \tilde{K}$[9] $\alpha_i \in K$ for all i. Since Σ is a normal extension of $K(X)$ the ramification indices of points lying above α_i are all equal, say to e_i.

Dropping for the moment the subscript i we may write

$$(X - \alpha)\Delta = \Omega^e \tag{13}$$

where Ω is an ideal in Δ, generated by $\omega_1, \dots, \omega_s$, say.

The ω_j satisfy monic equations over $K[X]$, so, multiplying if necessary by a constant, we may assume they satisfy actually monic equations over $D[X]$.

From (13) we derive an expression

$$X - \alpha = \sum_{(i)} R_{(i)} \omega_1^{i_1} \dots \omega_s^{i_s} \tag{14}$$

[8] That S is finite in this case follows at once from Siegel's celebrated Theorem too.

[9] In fact we could assume at once $K = \tilde{K}$. See [21] for the standard argument.

where the summation runs over all s-tuples of natural numbers $(i) = (i_1, \ldots, i_s)$ satisfying $i_1 + \ldots + i_s = e$ and where $R_{(i)} \in \Delta$.

Again from (13) we may write, for all $j = 1, \ldots, s$,

$$\omega_j^e = (X - \alpha)R_j^* \tag{15}$$

where $R_j^* \in \Delta$.

Let B be the finite set of elements of K which, as points of $K(X)$, lie below a pole of some of the functions $\omega_i, R_{(i)}, R_j^*$ above.

Also, for $m \in S - B$, choose a point P_m of Σ above m.[10]

Observe that, in view of the above normalizations, $\omega_i(P_m)$ is an algebraic integer while, for a suitable rational integer $a \neq 0$, independent of m, all the numbers $aR_{(i)}(P_m)$ and $aR_j^*(P_m)$ are algebraic integers.

Observe also that, if T is any element of Σ, then

$$T = Q(X, y_1, \ldots, y_d)$$

where $Q \in K(X)[y_1, \ldots, y_d]$, the y_i being the roots of $F(X, Y) = 0$.

So, if B is large enough to imply that T is defined at P_m we see that $m \in S - B$ implies $T(P_m) \in K$.

Combining this fact with the above we see that, for large enough B and $m \in S - B$,

$$\omega_i(P_m) \in D, \ aR_{(i)}(P_m) \in D, \ aR_j^*(P_m) \in D. \tag{16}$$

Let $m \in S - B$ and take any prime ideal Ξ of D dividing $(m - \alpha)$ but not dividing the above rational integer a.

Multiplying (15) by a and evaluating at P_m we get

$$a\omega_j^e(P_m) = (m - \alpha)(aR_j^*(P_m)).$$

So, if $\Xi^{qe+r} || (m - \alpha)$, where $0 \leq r < e$ we have, by (16), that either $r = 0$ or

$$\Xi^{q+1} | \omega_j(P_m) \quad \text{for all } j. \tag{17}$$

This possibility cannot however happen. In fact assume the contrary, multiply (14) by a and evaluate at P_m. We get

$$a(m - \alpha) = (aR_{(i)}(P_m))\omega_1^{i_1}(P_m) \ldots \omega_s^{i_s}(P_m)$$

whence, by (16), (17) and the fact that Ξ does not divide a,

$$\Xi^{(q+1)e} | (m - \alpha)$$

a contradiction.

[10] As a point of $K(X)$.

So $r = 0$. In other words *every prime ideal outside a finite computable set divides* $(m - \alpha)$ *to a power which is a multiple of* e.

Coming back to our argument write the ideal factorization in D

$$(m - \alpha)D = \Theta\Phi^e \tag{18}$$

where Θ is a fractional ideal which belongs to a finite computable set while $\Phi \subset D$.

We use a well known argument to derive a corresponding numerical equation.

Take ideals Φ^*, Θ^* in the inverse classes of Φ, Θ respectively and having bounded norm. Then the ideals $\Theta^*\Phi^{*e}$, $\Theta\Theta^*$ are clearly principal and of bounded norm, so may be generated by elements respectively θ_1, $\theta_2 \in D$ of bounded height, whence lying in a prescribed finite set. (It is of course understood that all the involved bounds are effective.) Also, the ideal $\Phi\Phi^*$ is clearly principal, generated by ϕ, say.

Multiplying (18) by $\Theta^*\Phi^{*e}$ we get

$$(m - \alpha)D = \left(\frac{\theta_2}{\theta_1}\right)\phi^e D$$

whence

$$m - \alpha = \left(\frac{\theta_2}{\theta_1}\right)\phi^e \mu \tag{19}$$

for some unit μ. Clearly $\mu = \mu^*\nu^e$ where μ^* lies in a finite computable set and ν is a unit. Combining with (18) we thus get

$$m - \alpha = \eta\gamma^e \tag{20}$$

where $\gamma \in D$ and $\eta \in K$ lies in a finite computable set.

Similar equations hold for any α_i, $i = 1, \dots, h$ in place of α, so we have proved the following:

ASSERTION. *There exist finitely many h-tuples* $(\eta_1, \dots, \eta_h) \in K^{*h}$ *such that, for* $m \in S - B$ *at least one of the systems*

$$m - \alpha_i = \eta_i\gamma_i^{e_i} \quad i = 1, \dots, h \tag{21}$$

has a solution with $\gamma_i \in D$ *for all* i.

We now analize the possibilities for the solutions in $m, \gamma_1, \dots, \gamma_h$ of each such system.

If $h \geq 2$ and some $e_i \geq 3$ then the system has only finitely many solutions which may be effectively found: in fact assume $e_1 \geq 3$. Then the first two equations give

$$\gamma_2^{e_2} = \left(\frac{\eta_1}{\eta_2}\right)\gamma_1^{e_1} + \left(\frac{\alpha_2 - \alpha_1}{\eta_1}\right)$$

and Baker's celebrated theorems [2] apply, since $e_2 \geq 2$.

If $h \geq 3$ and all e_i are equal to 2, multiplication of the first three equations gives an equation

$$(m - \alpha_1)(m - \alpha_2)(m - \alpha_3) = \rho\psi^2$$

where $\rho \in K^*$ is fixed and $\psi \in D$. This is an elliptic equation so again its finitely many solutions $(m, \psi) \in D^2$ may be found.

In conclusion the solutions of each system may be found except when either $h = 1$ or $h = e_1 = e_2 = 2$.

We show that each case corresponds to a field Σ of genus zero. In fact apply Hurwitz genus formula to the extension $\mathbb{A}\Sigma$ over $\mathbb{A}(X)$. The extension is still of degree d and the ramification indices remain the same. Hurwitz formula gives

$$2g - 2 = -2d + \sum_{i=1}^{h}(e_i - 1)\frac{d}{e_i} + \sum_{P|\infty}(e(P) - 1)$$

the last sum running over the places above ∞. This term is bounded by $d - 1$, whence

$$2g \leq 1 + \left(h - 1 - \sum_{i=1}^{h}\frac{1}{e_i}\right)d.$$

The right hand side is ≤ 1 in both the above cases, so $g = 0$ or the solutions may be found. This completes the proof. □

We remark that all the entities appearing in the above proof may be effectively calculated in every concrete case.

We wish to thank Professor A. Schinzel for several helpful discussions and comments.

REFERENCES

[1] E. Artin, Algebraic Numbers and Algebraic Functions. Gordon & Breach, New York (1967).

[2] A. Baker, Transcendental Number Theory. Cambridge Univ. Press, Cambridge (1976).

[3] Yu. Belotserkovski (Bilu), *Effective analysis of a new class of Diophantine equations* (Russian). Vestsī Akad. Navuk BSSR, Ser. Fīz.-Math. Navuk **3** (1988), 111-115, (Math. Rev. 89i:11038).

[4] YU. BELOTSERKOVSKI (BILU), *Effective analysis of a new class of Diophantine equations* (Russian). Vestsī Akad. Navuk BSSR, Ser. Fīz.-Math. Navuk, **6** (1988), 34-39, (Math. Rev. 90j:11038).

[5] E. BOMBIERI, Le grand crible dans la théorie analitique des nombres. Astérisque 18, Societé Mathématique de France, Paris (1974).

[6] J.W.S. CASSELS - A. FRÖHLICH, Algebraic Number Theory, Academic Press (1967).

[7] H. DAVENPORT - J. LEWIS - A. SCHINZEL, *Polynomials of certain special types*. Acta Arith. **9** (1964), 107-116.

[8] P. DEBES, *Resultats recents liés au théorème d'irreductibilité de Hilbert*. In: Séminaire de Théorie des Nombres, Paris 1985-86, Progress in Mathematics, vol. 71, Birkhauser.

[9] R. DVORNICICH - U. ZANNIER, *Fields containing values of algebraic functions*. Preprint Univ. Pisa (Novembre 1983).

[10] M. FRIED, *On Hilbert's Irreducibility Theorem*, J. Number Theory **6** (1974), 211-231.

[11] M. FRIED - M. JARDEN, Field Arithmetic. Springer-Verlag (1986).

[12] C. HOOLEY, *Applications of sieve methods to the theory of numbers*. Cambridge Tracts in Mathematics, Cambridge Univ. Press, 1976.

[13] S. LANG, Algebraic Number Theory. Addison Wesley (1970).

[14] S. LANG, Fundamentals of Diophantine Geometry. Springer-Verlag (1983).

[15] L.J. MORDELL, Diophantine equations. Academic Press (1969).

[16] T. NAGELL, *Géneralisation d'un théorème de Tchebycheff*. J. Math. Pures Appl. **4** (1921), 243-356.

[17] A. SCHINZEL, Selected topics on polynomials. Univ. of Michigan Press, Ann Arbor (1982).

[18] J.P. SERRE, Local fields. Springer-Verlag (1979).

[19] J.P. SERRE, Lectures on the Mordell-Weil Theorem. Vieweg (1988).

[20] A. WEIL, *Arithmetic on algebraic varieties*. Annals of Math. **53** (1951), 412-444.

[21] U. ZANNIER, *Note on the effective solution of a certain diophantine problem*. To appear.

Dipartimento di Matematica
Università di Pisa
Via Buonarroti, 2
56127 PISA (ITALY)

D.S.T.R., Ist. Univ. Arch.
S. Croce, 191
30135 VENEZIA (ITALY)