ACTA ARITHMETICA
LXXII.3 (1995)

Fields containing values of algebraic functions II (On a conjecture of Schinzel)

by

R. Dvornicich (Pisa) and U. Zannier (Venezia)

Introduction. The main question considered in the paper [DZ] was the following: given a polynomial $f \in \mathbb{Q}[x,y]$, say absolutely irreducible, and given a sequence $\{\theta_j\}$ satisfying $f(j,\theta_j)=0$, estimate the degree over the rationals of the fields $\mathbb{Q}(\theta_1,\dots,\theta_n)$ as $n \to \infty$.

It was shown (Theorem 2(a)) that, provided $d = \deg_y f > 1$, a lower bound of type $c^{n/\log n}$ holds for large n, where $c > 1$ depends only on f (the simple examples $f(x,y) = y^d - x$ show that the bound is not far from best possible). Also, a sufficient condition for an estimate of type c^n was given (Theorem 2(b)). That condition, which looked somewhat unnatural, was not made more general and complete, due among other things to the lack of certain estimates connected with power free values of polynomials. In that context Professor A. Schinzel formulated an elegant conjecture giving the exact condition for an exponential lower bound to hold: this is stated below (but already appeared in [DZ]). Let us first introduce some notation.

Let Σ denote the splitting field of f over $\mathbb{Q}(x)$ and, for a positive integer m, define $\Sigma(m)$ as the splitting field of the polynomial $f(m,y)$. Let $\mathcal{G}$ be the Galois group of $k\Sigma$ over $k(x)$, k being some number field containing the algebraic closure of $\mathbb{Q}$ in Σ. The function field $k\Sigma$ corresponds to a nonsingular curve $\mathcal{C}$ over k. Let $S(x)$ be a squarefree polynomial whose roots are precisely the finite ramification points of x (viewed as a function on $\mathcal{C}$). It is well known that, in view of our assumptions, S is nonconstant (see Lemma 1.2 in [DZ]), and moreover, since f has rational coefficients, S may also be assumed to have rational integral coefficients. Let $D(n)$ be the degree over $\mathbb{Q}$ of the composite of the fields $\Sigma(j)$ for $1 \le j \le n$. By means of a quantitative version of Hilbert's Irreducibility Theorem it was shown in [DZ] (see Remark 1, p. 21 of the old preprint or the end of the proof of Theorem 2(a) in the published version) that $D(n)$ and the degree of $\mathbb{Q}(\theta_1,\dots,\theta_n)$ have logarithms of the same order of magnitude (their quotient is bounded above and below by positive con-

stants). So it will suffice to consider $D(n)$. Schinzel's conjecture is as follows:

We have $\log D(n) \gg n$ *precisely when not both* (i) *and* (ii) *hold*:

(i) $S(x)$ *has all of its roots rational.*
(ii) $\mathcal{G}$ *is abelian.*

As remarked in [DZ] (in the Introduction to the recent version), Kummer theory (see [La2], p. 218) easily proves that, when both conditions are satisfied, Σ is contained in a finite composite of fields of type $k((x+b)^{1/e})$, $b \in \mathbb{Q}$, for a suitable number field k, whence an estimate $\log D(n) \ll n/\log n$ follows from the prime number theorem. So one half of the statement is easy to prove.

Let us look at the remaining half, namely the lower bound for $\log D(n)$ under the assumption that either (i) or (ii) does not hold. Consideration of polynomials of type $f(x,y) = y^d - S(x)$ (and in any case the proof of Theorem 2 in [DZ], which included the conjecture in case S has some root of degree 2 or 3 over $\mathbb{Q}$) shows that to use the negation of condition (i) one is at once faced with classical problems about the distribution of powerfree values of polynomials (at the moment solved only in quite special cases; see e.g. [Ho]), and conversely (as shown in [DZ]) such results would imply Schinzel's conjecture in all cases when (i) is not true. On the other hand, we have concentrated on what can be said if one assumes that (i) holds, but not (ii), approaching, so to say, the more algebraic part of the problem. Even in this case, we have not been able to settle the question completely. However, moving from the case of a cubic equation (see Remark 2 below for details), we have found arguments which cover a fairly large class of groups. Here is our result.

THEOREM. *Let condition* (i) *hold. Assume, moreover, that there exists a prime* $p \,\|\, \#\mathcal{G}$ *such that* $\mathcal{G}$ *has no normal subgroups of index* p ([1]). *Then* $\log D(n) \gg n$.

(In Remark 3 we shall sketch the proof that, in fact, if the theorem applies, an absolute lower bound holds for large n, namely $\log D(n) \geq ((6\log 2)/\pi^2)n + o(n)$.)

Simple group theoretical arguments combined with Bertrand's postulate will prove the following

COROLLARY. *Under condition* (i), *we have* $\log D(n) \gg n$ *when* $\mathcal{G}$ *is nonabelian of squarefree order, and also when* $\mathcal{G} = S_n$, *or* $\mathcal{G} = A_n$.

Remark 1. Let Ω be a subfield of Σ, normal over $\mathbb{Q}(x)$. We observe that if (i) holds for Σ, then it holds for Ω. Also, if $d(n)$ is defined for Ω

([1]) I.e. $\mathcal{G}$ is not p-nilpotent.

as $D(n)$ is defined for Σ, we have $d(n) \leq D(n)$, so it suffices to prove a lower bound for $d(n)$. This means that in fact it is only necessary that the assumptions apply to some quotient of $\mathcal{G}$ rather than to $\mathcal{G}$ itself.

Proofs. From now on we shall let k be a number field as in the above definitions, containing moreover a primitive pth root of unity. Also, we shall replace $k\Sigma$ with Σ and $k\Sigma(m)$ with $\Sigma(m)$. Throughout we shall let m run through the sequence $\mathcal{M}$ of positive integers such that $\Sigma(m)$ has Galois group $\mathcal{G}$ over k. In view of well known results related to Hilbert's Irreducibility Theorem (see for instance [Sch], Ch. 22 or [Se], Ch. 9), such a sequence contains all but at most $O(\sqrt{T})$ integers in the interval $[0, T]$.

Let now $\sigma \in \mathcal{G}$ be an element of order p, and let Σ_0 be the fixed field of σ. By Kummer theory we have

$$\Sigma = \Sigma_0(\alpha^{1/p})$$

for some $\alpha \in \Sigma_0$, not a pth power in Σ_0 (and the group generated by its image in $\Sigma_0^*/(\Sigma_0^*)^p$ is uniquely determined). We choose such an α to have minimal degree over $k(x)$. Observe that in any case this degree is greater than 1: otherwise $\alpha \in k(x)$, and the field $k(x, \alpha^{1/p})$ would be a Galois extension of $k(x)$ of degree p and contained in Σ, corresponding to a normal subgroup of $\mathcal{G}$ of index p, whose existence violates the assumptions. Let $\Phi = k(x, \alpha)$ and Γ be its Galois closure over $k(x)$. Define $G(x)$ for Γ as $S(x)$ was defined for Σ. Since $\Gamma \subset \Sigma$, G is a divisor of S (in $\mathbb{Q}[x]$), and is also nonconstant, since $\alpha \notin k(x)$.

For an integer m, let P run through all points of $\mathcal{C}$ above m (i.e. such that $x(P) = m$). For all but finitely many m, α, as a function on $\mathcal{C}$, will be defined at all such P's. For such m define $\Phi(P) = k(\alpha(P))$, and let $\Gamma(m)$ be the composite of all such $\Phi(P)$ or, equivalently, $\Gamma(m)$ is the splitting field of $g(m, y)$ over k, where $g(x, \alpha) = 0$ is the minimal equation of α over $k(x)$. In general, for Δ a subfield of Σ containing $k(x)$ one can define $\Delta(P)$, for $P \in \mathcal{C}$, also as the residue field of the valuation (over k) that P induces on Δ.

Observe that, for $m \in \mathcal{M}$, we shall have $\Sigma(m) = \Sigma(P)$ for all P above m, and the definition $\tau(\omega(P)) := (\tau\omega)(P)$ for a rational function $\omega \in \Sigma$, defined at P, will establish the isomorphism beween $\mathrm{Gal}(\Sigma(P) : k)$ and $\mathcal{G}$. (Changing the point P above m has the effect of an inner automorphism of $\mathcal{G}$.) Also, this will induce a 1-1 correspondence, preserving degrees and Galois groups, between the lattices of intermediate fields $k(x) \subset \Delta \subset \Sigma$ and $k \subset \Delta(P) \subset \Sigma(P)$.

In particular, the normal closure of $\Phi(P)$ over k will be $\Gamma(m)$ for $m \in \mathcal{M}$.

LEMMA 1. *There exists p_0 such that if $p \geq p_0$ and p ramifies in $\Gamma(m)$, then $p \,|\, G(m)$.*

This lemma is proved in a direct way in [DZ], Lemma 3.1. It is closely connected to the affine version of the Chevalley–Weil Theorem (see for instance [Se], p. 109; probably a proof can be derived also from the arguments given there). To establish the connection observe that, if $\mathcal{V}$ denotes the affine line deprived of the roots ϱ_i of G, and if S denotes the set of prime divisors of $G(m)$, then m is an S-integral point of $\mathcal{V}$: by this we mean that the functions $x, 1/(x-\varrho_i)$, which generate the affine algebra of $\mathcal{V}$, take S-integral values on m. If ϕ is the morphism of curves corresponding to the inclusion $k(x) \subset \Gamma$, then $\Gamma(m)$ may also be viewed as the field generated by the fiber of ϕ above m. In this way Lemma 1 corresponds to the assertion about ramification made at the beginning of the proof given in [Se]. The only difference is that in our case S depends on m, so a uniform argument would be needed.

LEMMA 2. *There exists p_0 such that if $p \geq p_0$ is a prime such that $p \,\|\, G(m)$, then p ramifies in $\Gamma(m)$.*

This lemma is an immediate corollary of Remark 2, after the proof of Lemma 3.2 in [DZ]. As observed in that paper (where a direct proof is given) it may also be derived from Weil's Decomposition Theorem. In fact, let $l(x)$ be a linear factor of G, thought as a function on the nonsingular curve corresponding to Γ. Its divisor of zeros is of the form eD for some divisor D, where $e \geq 2$ is the ramification index. By Weil's Theorem (see e.g. [La1], p. 263) this implies that the ideal generated by $l(m)$ in the ring of integers of $\Gamma(m)$ is, apart from a set of valuations lying above one of finitely many rational primes, an eth power, whence, if p is large, either $\mathrm{ord}_p l(m)$ is divisible by e or p ramifies in $\Gamma(m)$ (see the recent version of [DZ] for a slightly more detailed argument along these lines, as well as for the above quoted direct proof).

LEMMA 3. *Let $G \in \mathbb{Z}[x]$ be a nonconstant polynomial with all roots rational and simple, and let p_0 be sufficiently large. Then there exists a sequence of distinct natural numbers m_j such that $m_j \ll j$ and $G(m_j) = c_j s_j$, where all prime factors of c_j are $\leq p_0$, and the s_j are pairwise distinct squarefree numbers all of whose prime factors are $> p_0$.*

Proof. For any prime number p, there exists $e = e(p)$ such that, for every $B \in \mathbb{N}$, the number of solutions of the congruence

$$G(m) \equiv 0 \pmod{p^B}$$

does not exceed $e(p)$. (As once remarked by Hooley, this fact was proved independently by Ore and Nagell in 1921. A simple argument in our case is as follows: factor $G(m)$ over $\mathbb{Z}$ as $g\prod_{i=1}^{k}(b_i m - a_i)$, where $(a_i, b_i) = 1$ for all i. The greatest common divisor of any two factors is clearly bounded, whence it follows easily that, if B is large enough and m is a solution of our congruence, then for some index i and some bounded number c, we have

$b_i m - a_i \equiv 0 \pmod{p^{B-c}}$. For $B > c$ it follows that $p \nmid b_i$, whence this congruence has at most p^c solutions mod p^B. Summing over i yields the result.)

Also, there exists p_1 such that, for $p \geq p_1$, $e(p) \leq b = \deg G$. (It suffices that no prime $\geq p_1$ divides the discriminant of G.)

Hence, the number of positive integers $m \leq n$ such that $p^B \mid G(m)$ is $\leq ne(p)/p^B + e(p)$. Observe also that $p^2 \mid G(m)$ implies, for p not dividing the discriminant of G, that p^2 divides some linear factor, whence $p \leq A\sqrt{m}$, for some A (depending of course on G). Let $p_0 > p_1$. Then the sequence $\mathcal{A}$ of positive integers m such that either $p^B \mid G(m)$ for some prime $p \leq p_0$ or $p^2 \mid G(m)$ for some prime $\geq p_0$ intersects the interval $[1, n]$ in at most

$$\sum_{p \leq p_0} n\frac{e(p)}{p^B} + \sum_{p_0 < p \leq A\sqrt{n}} n\frac{b}{p^2} + O(\sqrt{n}) = n(\lambda_1 + \lambda_2) + O(\sqrt{n}),$$

integers, where $\lambda_1 = \sum_{p \leq p_0} e(p)/p^B$, $\lambda_2 = \sum_{p_0 < p \leq A\sqrt{n}} b/p^2$. We have $\lambda_2 \leq \sum_{p_0 < p} b/p^2 \leq b/p_0$. Choose $p_0 > \max(p_1, 2b)$, and then choose B so large that $\lambda_1 < 1/4$, say. Then $\lambda_1 + \lambda_2 \leq 3/4$, whence the complementary sequence $\widetilde{\mathcal{A}}$ contains at least $\frac{1}{4}n + O(\sqrt{n})$ integers in the interval $[1, n]$. By definition we may write, for $m \in \widetilde{\mathcal{A}}$,

$$G(m) = c(m)s(m)$$

where $c(m)$ is made with primes up to p_0, each taken with an exponent $\leq B$, while $s(m)$ is squarefree, and made only with primes $> p_0$, or $s(m) = 1$. Since $c(m)$ has a finite number, say H, of possibilities, each $s(m)$ can appear at most bH times. So, taking a subsequence such that each $s(m)$ appears exactly once, this will contain at least $\frac{1}{4bH}n + O(\sqrt{n})$ integers in $[1, n]$, proving the lemma. ∎

Such simple results have been well known since long ago; for instance, Professor Schinzel has pointed out to us Nagell's paper [Na]. For the sake of completeness we have included a proof.

By the above remarks concerning the density of $\mathcal{M}$ it is clear that we may also assume that the sequence $\mathcal{B} = \{m_j\}$ in the statement of Lemma 3 is contained in $\mathcal{M}$.

We may write $\Sigma_0 = k(x, \xi)$ for some primitive element ξ, which we may assume, for all j, to be defined at each point P of $\mathcal{C}$ lying above $m_j \in \mathcal{B}$ (in the sense that $x(P) = m_j$).

We begin by choosing inductively points P_j above m_j. Assume P_j is constructed for $1 \leq j \leq h$ in such a way that, setting

$$F_h = k(\xi(P_1), \ldots, \xi(P_h)) \tag{1}$$

we have

$$p \nmid [F_h : k]. \tag{2}$$

We contend that P_{h+1} may be found with the same properties. We are indebted to Yuri Bilu for the following argument, which simplifies our previous proof. Let $X = \{\xi(P) : P \in \mathcal{C},\ x(P) = m_{h+1}\}$ be the set of values of ξ at points lying above m_{h+1}. Then $\mathrm{Gal}(\overline{k}/k)$ ([2]) acts on X (in fact, it acts transitively by our choice of the sequence $\mathcal{M}$). Also, $\#X = [\Sigma : k(x)]$ is not divisible by p. In particular, at least one orbit X_0 of the action of the subgroup $\mathrm{Gal}(\overline{k}/F_h)$ on X has cardinality not divisible by p. Choosing P_{h+1} such that $\xi(P_{h+1}) \in X_0$ we get our contention.

The following result will be crucial.

LEMMA 4. *Let Λ, Ω be subfields of Σ such that $\Lambda \supset \Phi = k(x, \alpha)$ and $k(x) \subset \Omega \subset \Lambda$. Assume also that $p \nmid [\Omega : k(x)]$. Let $\mathcal{N}$ denote the norm from Λ to Ω. Then either $\mathcal{N}(\alpha)$ is a p-th power in Ω, or $[\Omega : k(x)] \geq [k(x, \alpha) : k(x)]$.*

Remark 2. As a simple and basic instance, which motivated the more general method, consider f of degree 3 in y such that $\mathcal{G} = S_3$, and take $p = 3$. We may assume $f(x, y) = y^3 - 3by - 2c$, where $b, c \in \mathbb{Q}(x)$, and we let $k = \mathbb{Q}\big(\exp\big(\frac{2}{3}\pi i\big)\big)$. Set $a = c^2 - b^3$. Then Cardano's formulae show that the splitting field Σ of f over $k(x)$ is $k(x, (c+\sqrt{a})^{1/3})$ $(= k(x, (c-\sqrt{a})^{1/3}))$. The field Σ_0 in this case is $k(x, \sqrt{a})$, while $\alpha = c + \sqrt{a}$. Observe that the norm of α from Σ_0 to $k(x)$ is b^3, the cube of a rational function. This fact corresponds to the conclusion of Lemma 4, taking $\Omega = k(x)$, $\Lambda = \Sigma_0 = k(x, \sqrt{a})$.

Proof of Lemma 4. Put $\beta = \mathcal{N}(\alpha)$, and assume β is not a pth power in Ω. Then $[\Omega(\beta^{1/p}) : \Omega] = p$. Since β is a product of conjugates of α, which are all pth powers in Σ, we have $\beta^{1/p} \in \Sigma$.

Let $\mathcal{H} \subset \mathcal{G}$ be the Galois group of the extension Σ/Ω. In view of our assumptions, $\mathcal{H}$ has order divisible by p, and thus contains an element τ of order p. Let $\widetilde{\Sigma}_0$ be the fixed field of τ. This field contains Ω and has degree p below Σ. Since the order of $\mathcal{G}$ is not divisible by p^2, we see that p does not divide $[\widetilde{\Sigma}_0 : \Omega]$. In particular, $\beta^{1/p} \notin \widetilde{\Sigma}_0$, whence

$$\widetilde{\Sigma}_0(\beta^{1/p}) = \Sigma. \tag{3}$$

Since the order of $\mathcal{G}$ is not a multiple of p^2 and since all p-Sylow are conjugate, we deduce that $\widetilde{\Sigma}_0$ is a field conjugate to Σ_0, say $\Sigma_0 = \delta\widetilde{\Sigma}_0$ for some $\delta \in \mathcal{G}$. Let $\alpha_* = \delta\beta \in \Sigma_0$. Then (3) implies

$$\Sigma_0(\alpha_*^{1/p}) = \Sigma. \tag{4}$$

By minimality we find that the degree of α_* over $k(x)$, which equals the degree of β over $k(x)$, is at least the degree of α over $k(x)$. Since, however, $\beta \in \Omega$, we get the second alternative in the conclusion of the lemma. ∎

([2]) A bar denotes algebraic closure.

For all pairs of subfields Ω, Λ of Σ such that the first alternative of the lemma applies, let $\mathcal{N}\alpha = \beta^p$ be the corresponding equation. Omitting if necessary a finite number of terms from our sequence $\{m_j\}$, we may assume that each such function β is, for all j, defined at each point of $\mathcal{C}$ above m_j.

Put $\alpha_h = \alpha(P_h)$ and $\xi_h = \xi(P_h)$. We have

$$\Sigma(m_h) = k(\xi_h)(\alpha_h^{1/p}) \subset F_h(\alpha_h^{1/p}). \tag{5}$$

Assume that h is such that

$$\Sigma(m_h) \subset \Sigma(m_1) \dots \Sigma(m_{h-1}). \tag{6}$$

The field on the right is contained in $F_h(\alpha_1^{1/p}, \dots, \alpha_{h-1}^{1/p})$ so, by (5) and by Kummer theory, applied with base field F_h, we must have

$$\alpha_h = \prod_{i=1}^{h-1} \alpha_i^{a_i} \phi^p \tag{7}$$

for suitable integers a_i and $\phi \in F_h$.

We shall take the norm of (7) to $k(\alpha_h)$. Put, for $i < h$,

$$A = k(\alpha_h, \alpha_i) \cap \Gamma(m_i) \quad \text{and} \quad B = k(\alpha_h) \cap \Gamma(m_i).$$

Then, N denoting the norm map, we have

$$N_{k(\alpha_h)}^{k(\alpha_h,\alpha_i)}(\alpha_i) = N_B^A(\alpha_i). \tag{8}$$

In fact, the restriction $\mathrm{Gal}(k(\alpha_h)\Gamma(m_i) : k(\alpha_h)) \to \mathrm{Gal}(\Gamma(m_i) : B)$ is an isomorphism.

Since $m_i \in \mathcal{M}$ the fields A, B will correspond, under the identification of functional and numerical Galois groups obtained by specializing at P_i, to fields Λ, Ω resp., intermediate between $k(x)$ and Σ, and satisfying the assumptions of Lemma 4. In fact, $k(\alpha_i)$ (which is $\Phi(P_i)$) is contained in A, and also $B \subset A$, whence $\Phi \subset \Lambda$ and $\Omega \subset \Lambda$. Also, since $k(\alpha_h) \subset F_h$, we have $p \nmid [B : k]$, whence $p \nmid [\Omega : k(x)]$. In fact, the correspondence preserves degrees. This also implies that, if the second alternative of Lemma 4 held, then

$$[B : k] \geq [k(\alpha_i) : k].$$

But $[B : k] \leq [k(\alpha_h) : k] = [\Phi : k(x)] = [k(\alpha_i) : k]$, the last equalities being valid since both m_i, m_h belong to $\mathcal{M}$. We deduce that equality would hold throughout, whence

$$B = k(\alpha_h) \subset \Gamma(m_i).$$

Since $\Gamma(m_i)$ is normal over k, the normal closure of $k(\alpha_h)$ over k, which is $\Gamma(m_h)$, is contained in $\Gamma(m_i)$. But they have the same degree over k, since $m_i, m_h \in \mathcal{M}$, whence $\Gamma(m_h) = \Gamma(m_i)$. In particular, these fields must have the same ramified rational primes. Now we have $G(m_i) = c_i s_i$ and $G(m_h) = c_h s_h$ with c_i, c_h, s_i, s_h as in Lemma 3, and $s_i \neq s_h$. Assume $s_h \nmid s_i$

(the other case being symmetrical) and pick a prime q dividing s_h but not s_i (this exists since both are squarefree). Since $q \geq p_0$ and since $q \,\|\, G(m_h)$, Lemma 2 implies that q ramifies in $\Gamma(m_h)$. If q were ramified in $\Gamma(m_i)$, then Lemma 1 would imply $q \,|\, G(m_i)$, which is false.

We conclude that the first alternative of Lemma 4 must hold, whence

$$\mathcal{N}(\alpha) = \beta^p$$

for some $\beta \in \Omega$. Specializing this equation at P_i, which is possible in view of the remarks following the proof of Lemma 4 about the β's arising in this way, we get

$$N_B^A(\alpha_i) = \beta(P_i)^p,$$

where now $\beta(P_i) \in B$. Using (8) we also get

$$N_{k(\alpha_h)}^{k(\alpha_h,\alpha_i)}(\alpha_i) = \beta(P_i)^p.$$

But the norm from F_h to $k(\alpha_h)$ is a power of $N_{k(\alpha_h)}^{k(\alpha_h,\alpha_i)}(\alpha_i)$, whence

$$N_{k(\alpha_h)}^{F_h}(\alpha_i) = \delta_i^p$$

for some $\delta_i \in k(\alpha_h)$, and this holds for all $i < h$. Taking the norm of (7) from F_h to $k(\alpha_h)$ then implies that $\alpha_h^{[F_h:k(\alpha_h)]}$ is the pth power of some element of $k(\alpha_h)$. However, $[F_h : k]$ is not divisible by p, so α_h itself is a pth power in $k(\alpha_h)$. But α_h cannot be a pth power even in $\Sigma_0(P_h)$ (which contains $k(\alpha_h)$ since $\alpha \in \Sigma_0$), otherwise $\Sigma_0(P_h) = \Sigma_0(P_h)(\alpha_h^{1/p}) = \Sigma(P_h)$, which does not hold since $m_h \in \mathcal{M}$, and since $\Sigma_0 \neq \Sigma$. This shows that, for all h, (6) is impossible. So

$$[\Sigma(m_1) \dots \Sigma(m_h) : \Sigma(m_1) \dots \Sigma(m_{h-1})] \geq 2$$

(in fact $\geq p$), whence $D(m_h) \geq 2^h$. Since, however, $m_h \ll h$, we get the desired exponential estimate. This concludes the proof. ∎

R e m a r k 3. We have made no effort to optimize the constant implicit in $\log D(n) \gg n$, or even the value $\mu = \liminf(\log D(n))/n$. This will depend on the density of the sequence $\{m_i\}$ constructed in Lemma 3, which in turn certainly depends on the basic data, in general. However, by a slightly different construction μ can be shown to be bounded below by a positive absolute constant. We only give a sketch of the argument. The proof of Lemma 3 shows the following, by making p_0 bigger if necessary:

For all $\lambda < 1$ and for sufficiently large p_0 there exists a sequence $\{m_i\}$ of asymptotic density at least λ such that $G(m_i) = c_i s(m_i)$, where each prime power appearing in c_i is of type q^b with $q \leq p_0$ and $b \leq B = B(\lambda)$, and where each $s(m_i)$ is squarefree and has only prime factors $> p_0$.

Now it suffices to choose a subsequence as dense as possible and such that the corresponding $s(m_i)$ are pairwise distinct: the rest of the above proof will work in the same way. Assume that $m < n$ are elements of the sequence with $s(m) = s(n)$. Then we have an equation

$$cG(m) = c'G(n) \tag{9}$$

where c, c' have the same form as the c_i, and so have finitely many possibilities, leading to a finite number of diophantine equations (9).

Assume $b = \deg G > 1$. At this point one could invoke Siegel's celebrated theorem ([La1], Ch. 8, or [Se], Ch. 7) and show that, for each equation, the solutions form a "thin" set. In this case, however, an elementary argument suffices. Let $\beta \in \mathbb{Q}$ be such that the second coefficient of $G(x-\beta) = G_*(x)$, say, vanishes, and write

$$G_*(x) = a_0x^b + a_2x^{b-2} + \ldots + a_b, \quad a_i \in \mathbb{Q}, \quad a_0 \neq 0. \tag{10}$$

Also, put $\omega = c/c'$, a positive rational number which we suppose fixed. Now, (9) reads $cG_*(m+\beta) = c'G_*(n+\beta)$, and from (10) we get

$$|a_0||(n+\beta)^b - (m+\beta)^b\omega| \ll n^{b-2},$$

whence, for the positive real bth root of ω we have

$$|(n+\beta) - \omega^{1/b}(m+\beta)| \ll 1/n, \tag{11}$$

where the implied constant depends only on G_*. If $a := \omega^{1/b} > 0$ is rational, this shows that the left hand side of (11) is zero for large n so, if there were infinitely many solutions we would have $cG_*(x) = c'G_*(ax)$ identically. By (10), $(c - c'a^h)a_{b-h} = 0$ for all h, whence $a_i = 0$ for $i > 0$, a contradiction, since G has only simple roots and degree > 1. If $\omega^{1/b}$ is irrational, then the rationals $(n+\beta)/(m+\beta)$ form a sequence of good approximations to $\omega^{1/b}$. Now it is easily proved that the admissible m's belong to a sequence of zero asymptotic density (in fact, the difference between consecutive elements plainly tends to ∞). To sum up, omitting a finite number of sequences of zero asymptotic density from our original sequence, we may assume that, for all possible values of c, c', (9) is unsolvable. This clearly proves the assertion when $b \geq 2$.

The case of linear G remains. Now the function field extension $\Gamma/k(x)$ has just one finite ramified point. It is known (and easily proved by the Hurwitz genus formula) that Γ has genus zero, whence it must be of type $k((rx-s)^{1/e})$, where $r \neq 0, s$ and $e > 1$ are integers. Write $r = (r,s)r_1, s = (r,s)s_1$ and consider the sequence $\mathcal{B}$ of the integers m such that $r_1m - s_1$ is squarefree. It is well known (and easily proved) that $\mathcal{B}$ contains asymptotically $\geq (6/\pi^2)n + o(n)$ elements in the interval $[1,n]$. Distinct elements in the sequence give rise to distinct fields $\Gamma(m)$, and this suffices for the above proof to work.

In this way one gets the bound $\mu \geq (6/\pi^2)\log p$.

Proof of Corollary. Let us begin with the case of $g := \#\mathcal{G}$ square-free. If the assumptions of the Theorem are satisfied for at least one prime p the proof is finished. Otherwise, for each $p \mid g$, there exists a subgroup $\mathcal{H}_p$ normal in $\mathcal{G}$, of index p.

Observe that, if $\mathcal{H}$ and $\mathcal{K}$ are normal subgroups of $\mathcal{G}$, of coprime indices m, n resp., then $\mathcal{H} \cap \mathcal{K}$ has index mn. (In fact, its index in $\mathcal{H}$ is $\leq m$, whence its index in $\mathcal{G}$ is at most mn. On the other hand, this index is divisible by both m, n.)

It follows inductively that, letting q run through primes, the subgroup

$$\bigcap_{q \mid g,\, q \neq p} \mathcal{H}_q = \mathcal{S}(p)$$

has order p, and is normal. Thus each p-Sylow is normal and cyclic, whence $\mathcal{G}$ is cyclic, contradicting the assumption that the group is nonabelian. (In any case we have already remarked that, for abelian $\mathcal{G}$, and if (i) holds, then $\log D(n) \ll n/\log n$.)

Let now $n \geq 3$ and $\mathcal{G} = S_n$. By Bertrand's postulate there exists a prime p with $n/2 < p \leq n$. Clearly $p \parallel n!$. It is also well known that the only normal proper subgroup of S_n is A_n, so again the assumptions of the theorem are satisfied for at least one p. Similarly in the case of A_n.

References

[DZ] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, preprint Univ. Pisa n. 44, novembre 1983; Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 21 (1994), 421–443.

[Ho] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Math., Cambridge Univ. Press, 1976.

[La1] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[La2] —, *Algebra*, 7th ed., Addison-Wesley, 1977.

[Na] T. Nagell, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 179–194.

[Sch] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982.

[Se] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, Vieweg, 1988.

DIPARTIMENTO DI MATEMATICA
VIA BUONARROTI, 2
56127 PISA, ITALY
E-mail: DVORNIC@GAUSS.DM.UNIPI.IT

IST. UNIV. ARCH. VENEZIA D.S.T.R.
S. CROCE, 191
30135 VENEZIA, ITALY
E-mail: ZANNIER@DIMI.UNIUD.IT

Received on 9.3.1994
and in revised form on 16.7.1994 (2573)