ACTA ARITHMETICA
LXIV.1 (1993)

# Some remarks on the $S$-unit equation in function fields

by

Umberto Zannier (Venezia)

**Introduction.** Let $k$ be an algebraically closed field of zero characteristic, $K$ a function field in one variable over $k$, of genus $g$. For $n \geq 2$, $u_1, \ldots, u_n \in K$ not all zero, we define the projective height as usual:

$$H(u_1, \ldots, u_n) = -\sum_v \min(v(u_1), \ldots, v(u_n)) \tag{1}$$

where $v$ (normalized so that $v(K^*) = \mathbb{Z}$) runs over all places of $K/k$.

In [10] R. C. Mason proved essentially the following result ([1]), fundamental for his analysis of norm form equations over function fields.

*Let $u_1, \ldots, u_n \in K$ $(n \geq 3)$ be such that $u_1 + \ldots + u_n = 0$ but no proper nonempty subset of the $u_i$'s is made of elements linearly dependent over $k$. Then*

$$H(u_1, \ldots, u_n) \leq 4^{n-2}(\#S + 2g - 2) \tag{2}$$

*where $S$ is the set of places of $K$ where some $u_i$ is not a unit.*

(Actually Mason's Lemma 2 in [10] is stated differently, since he deals with the inhomogeneous equation $u_1 + \ldots + u_n = 1$.)

The work of Mason generalized his previous result with $n = 3$ (see [9]) which he had used to solve effectively certain classical diophantine equations over function fields. In that case, however, he had obtained the constant factor 1 in place of 4.

In the meantime J. F. Voloch, in [16], was led to consider similar questions and, by methods different from Mason's, obtained results which easily implied ([2]) that, under the above conditions,

$$H(u_1, \ldots, u_n) \leq \binom{n-1}{2}(\#S + 2g - 2). \tag{3}$$

---

([1]) In fact announced already in [8].

([2]) This remark appears in [3].

Shortly afterwards W. D. Brownawell and D. Masser [3], independently of Voloch, obtained some improvements of (2) in different directions and stated explicitly (3) as Corollary 1 to Theorem A.

In [10] Mason also remarked that his inequality was true under the weaker hypothesis that no proper nonempty subsum of the $u_i$ vanished. In fact, in [3] the authors prove a result (Theorem B) which immediately implies that with this restriction, and if moreover the $u_i$ are not all constant, then (3) holds ([3]).

The first purpose of this note is to show that, under such conditions, (3) holds in the more precise form

$$H(u_1,\dots,u_n) \le \binom{\mu}{2}(\#S + 2g - 2) \tag{4}$$

where $\mu$ is the dimension of the vector space spanned by the $u_i$ over $k$.

Our proof, following [3], will make essential use of Wro/nskians. We shall, however, need to make a subsequent induction work, a result which, even in case $\mu = n-1$, is not entirely contained in (3) (though only slightly different). Namely, we shall prove the following

THEOREM 1. *Let $a_1,\dots,a_n \in K$ be $S$-units ([4]) such that $\sum_{i\in\Gamma} a_i \neq 0$ for every nonempty $\Gamma \subset \{1,\dots,n\}$. Put $b = a_1 + \dots + a_n$. Then*

$$\sum_{v\in S}(v(b) - \min v(a_i)) \le \binom{\mu}{2}(\#S + 2g - 2)$$

*where $\mu = \dim \sum ka_i$.*

(Now, unlike the previous statements, $b$ is not necessarily an $S$-unit.)

Inequality (4) will be shown to follow at once.

In some cases one may further improve upon (4). We have in fact

THEOREM 2. *Let $a_1,\dots,a_n \in K$ be $S$-units spanning a $k$-vector space of dimension $\mu < n$. Assume also that any $\mu$ of the $a_i$ are linearly independent over $k$. Then*

$$H(a_1,\dots,a_n) \le \frac{1}{n-\mu}\binom{\mu}{2}(\#S + 2g - 2)\,.$$

Later we shall briefly discuss, as in [3], some questions connected with "extremal examples", i.e. cases when (3), say, holds as an equality.

After quoting some new examples due to J. Browkin and J. Brzeziński we shall concentrate on the simplest nontrivial case, i.e. $n = 3$: we shall show that extremal examples correspond to coverings of the Riemann sphere

---

([3]) Both Theorems A and B of [3] are actually more precise than (3) since they also take into account, for each place in $S$, the number of the $u_i$ which are units at that place.

([4]) That is, $v(a_i) = 0$ for $v \notin S$.

ramified only above $\{0, 1, \infty\}$. We have in fact the following observation (essentially a recollection and reformulation of known facts, however):

THEOREM 3. *Let the equation $a + b = 1$, where $a, b \in K - k$, represent an "extremal example". Then the only places of $k(a)$ ramified in $K$ are (at most) $0, 1, \infty$, and conversely. In particular, given the genus $g$ of $K$ and given $\#S$, there are only finitely many essentially distinct such equations.*

(By essentially distinct we mean "distinct up to isomorphisms of $K$ over $k$". For instance two extremal examples $a + b = 1$, $a^* + b^* = 1$ where $a, b, a^*, b^* \in k(t)$ are considered "essentially equal" if $a(t) = a^*(\lambda(t))$ and $b(t) = b^*(\lambda(t))$ where $\lambda$ is a suitable fractional linear transformation.)

Some particular cases of this phenomenon, when $K = k(t)$ has genus zero, had already been noticed in dealing with finite homography groups: see [1] for a detailed account, also in connection with hypergeometric differential equations. In this context other cases arise in the analysis of Lamé's operators with finite monodromy group (see [4]).

After the proof of Theorem 3 we shall sketch in Remarks 1 and 2 a combinatorial interpretation (in terms of the cycle decomposition of certain permutations) of the number of "essentially distinct extremal examples". This method will yield in particular an existence proof for extremal examples with given genus $g$ and given $\#S$, a question left partially unanswered in [3].

Proof of Theorem 1. We first treat the case $\mu = n$, and follow [3]. We let $z$ be a nonconstant element of $K$ and define, for $a_1, \dots, a_n \in K$, the Wrońskian

$$W = W(a_1, \dots, a_n) = \det(a_i^{(j)}), \quad i = 1, \dots, n, \ j = 0, \dots, n-1,$$

the $a_i^{(j)}$ denoting derivatives with respect to $z$. (Actually in [3] the equivalent logarithmic Wrońskian is used.)

Since $a_1, \dots, a_n$ are linearly independent over the constant field $k$ of the derivation $d/dz$, $W$ does not vanish.

Now let $v$ be any place of $K$ and choose a local parameter $t_v$ at $v$. Also let $h = h_v$ be an index such that $v(a_h) = \min v(a_i)$.

We have

$$W(a_1, \dots, a_n) = W(a_1, \dots, a_{h-1}, b, a_{h+1}, \dots, a_n). \tag{5}$$

We shall use several times Lemma 2 of [3]. For the reader's convenience we restate it here in our own notation as

LEMMA 1. *For $n \geq 3$ let $f_1, \dots, f_n$ be elements of $K$ linearly independent over $k$, and for a place $v$ and an integer $\nu$ with $0 \leq \nu \leq n$ suppose that at*

*least $\nu$ of the $f_i$'s are units at $v$. Then*

$$v(W(f_1,\dots,f_n)) \geq -\binom{n}{2}v(dz/dt_v) - \left(\binom{n}{2} - \binom{\nu}{2}\right) + \sum_{i=1}^{n} v(f_i).$$

By this lemma applied with $a_1,\dots,a_{h-1},b,\dots,a_n$ in place of $f_1,\dots,f_n$ and with $\nu = 0$ the following inequality holds:

$$\begin{aligned} v(W) + \binom{n}{2}v(dz/dt_v) + \binom{n}{2} &\geq \sum_{i\neq h} v(a_i) + v(b) \\ &= \sum_{i=1}^{n} v(a_i) + (v(b) - \min v(a_i))\,. \end{aligned}$$

Now sum over $v \in S$. Since the $a_i$ are $S$-units we have $\sum_{v\in S} v(a_i) = 0$ for $i = 1,2,\dots,n$, whence

$$\sum_{v\in S}(v(b) - \min v(a_i)) \leq \binom{n}{2}\#S + \sum_{v\in S}\left\{v(W) + \binom{n}{2}v(dz/dt_v)\right\}. \tag{6}$$

On the other hand, if $v \notin S$, by the same Lemma 1 applied with $a_1,\dots,a_n$ in place of $f_1,\dots,f_n$ and with $\nu = n$ (now $a_1,\dots,a_n$ are units at $v$) we get

$$v(W) + \binom{n}{2}v(dz/dt_v) \geq 0 \quad \text{for } v \notin S$$

whence

$$\sum_{v}\left\{v(W) + \binom{n}{2}v(dz/dt_v)\right\} \geq \sum_{v\in S}\left\{v(W) + \binom{n}{2}v(dz/dt_v)\right\}. \tag{7}$$

Now it suffices to use (6) and to recall that

$$\sum_{v} v(W) = 0, \qquad \sum_{v} v(dz/dt_v) = 2g-2\,. \tag{8}$$

To deal with the general case we argue by induction on $n$, the case $n = 1$ being trivial.

Let $a_1,\dots,a_\mu$ be a basis for $ka_1+\dots+ka_n$ and set, renumbering indices if necessary,

$$b = a_1 + \dots + a_n = \sum_{i=1}^{\nu}\gamma_i a_i, \qquad \text{where } \gamma_1\dots\gamma_\nu \neq 0\,; \tag{9}$$

here $1 \leq \nu \leq \mu$.

If $\nu = \mu$ or if $\mu = n$ the theorem follows at once from the particular case treated above: in fact, each $a_i$ is a linear combination with coefficients in $k$ of $a_1,\dots,a_\mu$, whence

$$\min_{1\leq i\leq \mu} v(a_i) = \min_{1\leq i\leq n} v(a_i) \tag{10}$$

and we could apply the previous result with $\gamma_1 a_1, \dots, \gamma_\mu a_\mu$ in place of $a_1, \dots, a_n$.

So assume $1 \le \nu < \mu < n$. By the inductive assumption applied to (9) we get

$$\sum_{v \in S} \{v(b) - \min_{1 \le i \le \nu} v(a_i)\} \le \binom{\nu}{2} (\#S + 2g - 2)\,. \tag{11}$$

We now construct recursively a finite sequence $\{\mu_h\}$ of integers such that

(i) $\mu_0 = \nu$, $\mu_h > \mu_{h-1}$ for $h \ge 1$,
(ii) $\max\{\mu_h\} = \mu$,
(iii) there is a renumbering of the indices $\nu + 1, \dots, \mu$ such that

$$\sum_{v \in S} \{v(b) - \min_{1 \le i \le \mu_h} v(a_i)\} \le \binom{\mu_h}{2} (\#S + 2g - 2)\,.$$

Clearly this construction, in view of (ii) and of (10), will complete the proof.

The first step, namely the construction of $\mu_0$, is just (11). Assume $\mu_0, \dots$ $\dots, \mu_h$ constructed. For any index $j$ we have

$$a_j = \sum_{i=1}^{\mu} \lambda_{i,j} a_i = \sum_{i=1}^{\mu_h} \lambda_{i,j} a_i + \sum_{i=\mu_h+1}^{\mu} \lambda_{i,j} a_i = T_j + U_j$$

say, the $\lambda_{i,j}$ being suitable elements of $k$.

If $\mu_h = \mu$, as already observed, we are done, so assume $\mu_h < \mu$. We contend that, for some $j$, both $T_j$ and $U_j$ are nonzero. In fact, assume the contrary. Then either $U_j = 0$ or $a_j = U_j$. Equation (9) clearly implies $\sum_{j=1}^{n} U_j = 0$ (since $\mu_h + 1 \ge \nu + 1$), whence

$$\sum_{U_j \ne 0} a_j = 0\,. \tag{12}$$

The set $\Gamma = \{j : U_j \ne 0\}$ is, however, nonempty: in fact, $\mu_h < \mu$ and thus $\mu \in \Gamma$. Equation (12) would now contradict our assumptions.

Pick then $j_0$ such that both $T_{j_0}$ and $U_{j_0}$ are nonzero. Certainly $j_0 > \mu$.

Renumber the indices $\mu_h + 1, \dots, \mu$ to write

$$U_{j_0} = \sum_{i=\mu_h+1}^{\mu_{h+1}} \lambda_{i,j_0} a_i \tag{13}$$

where

$$\lambda_{i,j_0} \ne 0 \quad \text{for } \mu_h + 1 \le i \le \mu_{h+1}\,. \tag{14}$$

These requirements define $\mu_{h+1}$ and clearly $\mu \ge \mu_{h+1} > \mu_h$.

Apply the induction assumption to $T_{j_0}$ in place of $b$ and $a_{j_0}, -\lambda_{i,j_0}a_i$ $(\mu_h+1 \le i \le \mu_{h+1})$ in place of $a_1,\dots,a_n$.

The assumptions are in fact satisfied, for

$$T_{j_0} = a_{j_0} + \sum_{i=\mu_h+1}^{\mu_{h+1}} -\lambda_{i,j_0}a_i \tag{15}$$

and moreover no nonempty subsum of the right hand side vanishes since $T_{j_0} \neq 0$, since the $a_i, 1 \le i \le \mu$, are linearly independent and since (14) holds. Setting

$$B = \{j_0\} \cup \{\mu_h+1,\dots,\mu_{h+1}\},$$

we obtain

$$\sum_{v\in S}\{v(T_{j_0}) - \min_{i\in B} v(a_i)\} \le \binom{\mu_{h+1}-\mu_h+1}{2}(\#S+2g-2). \tag{16}$$

Adding this inequality to (iii) above (the one obtained for $b, a_1,\dots,a_{\mu_h}$) and putting $A=\{1,\dots,\mu_h\}$ yields

$$\begin{aligned}\sum_{v\in S}\{v(b)+v(T_{j_0}) - \min_{i\in A} v(a_i) - \min_{i\in B} v(a_i)\} &\\ \le \left\{\binom{\mu_h}{2} + \binom{\mu_{h+1}-\mu_h+1}{2}\right\}(\#S+2g-2) &\\ \le \binom{\mu_{h+1}}{2}(\#S+2g-2).&\end{aligned} \tag{17}$$

We must now deal with the left hand side. Observe that, since

$$T_{j_0} = a_{j_0} - \sum_{i=\mu_h+1}^{\mu_{h+1}} \lambda_{i,j_0}a_i = \sum_{i=1}^{\mu_h}\lambda_{i,j_0}a_i$$

we have, for any $v$,

$$v(T_{j_0}) \ge \max\{\min_{i\in B} v(a_i), \min_{i\in A} v(a_i)\},$$

whence each term in the sum on the left of (17) is bounded below by

$$v(b) - \min_{i\in A\cup B} v(a_i) \ge v(b) - \min_{1\le i\le \mu_{h+1}} v(a_i),$$

completing the verification of (i), (iii) for $h+1$ in place of $h$ (in case $\mu_h < \mu$), and thus finishing the proof of Theorem 1.

Corollary. *If $u_1+\ldots+u_n = 0$ but no proper subsum of the $u_i$ vanishes, then, provided the $u_i$ are $S$-units, inequality* (4) *holds.*

P r o o f. Apply Theorem 1 with $n-1$ in place of $n$, with $b=-u_n$ and with $a_i=u_i$, the assumptions being clearly satisfied. We get

$$\sum_{v\in S}\{v(u_n)-\min_{1\le i\le n-1}v(u_i)\}\le\binom{\mu}{2}(\#S+2g-2)\,.$$

On the other hand, if $v\notin S$, then $v(u_i)=0$ for $i=1,\dots,n$, whence the range of summation in the left hand side may be extended to all $v$.

To get the Corollary it now suffices to use the equations

$$\sum_v v(u_n)=0\quad\text{ and }\quad\min_{1\le i\le n-1}v(u_i)=\min_{1\le i\le n}v(u_i)\,,$$

the last one following from the basic assumption $u_n=-\sum_{i=1}^{n-1}u_i$.

P r o o f o f T h e o r e m 2. Let $W$ denote the Wrońskian of any $\mu$ of the $a_i$ and observe that the value $v(W)$ does not depend on such a choice: in fact, since any $\mu$ of the $a_i$ form a basis for the $k$-linear span of $a_1,\dots,a_n$, the quotient of any two such determinants is a nonzero constant.

Let $v\in S$. Assume, renumbering indices if necessary, that

$$v(a_1)\ge v(a_2)\ge\ldots\ge v(a_n)=\min v(a_i)=m_v\,,\quad\text{say}\,.$$

Since $a_1,\dots,a_\mu$ are linearly independent over $k$, $a_n$ is their linear combination with constant coefficients, whence

$$m_v=v(a_n)\ge\min_{1\le i\le\mu}v(a_i)=v(a_\mu)\ge m_v$$

and so

$$v(a_i)=m_v\quad\text{ for }\mu\le i\le n\,.\tag{18}$$

Also, by the remark made at the beginning and by Lemma 1 applied with $a_1,\dots,a_\mu$ in place of $f_1,\dots,f_n$ and with $\nu=0$ we have

$$v(W)=v(W(a_1,\dots,a_\mu))\ge-\binom{\mu}{2}(v(dz/dt_v)+1)+\sum_{i=1}^{\mu}v(a_i)\,,$$

whence, by (18),

$$v(W)+\binom{\mu}{2}(v(dz/dt_v)+1)\ge\sum_{i=1}^{n}v(a_i)-(n-\mu)m_v\,.$$

Summing this inequality over $v\in S$ and using (7) and (8) we obtain the desired result.

**Extremal examples.** Let us restrict ourselves to the case $\mu=n-1$ of the Corollary (one of the results in [3]). In [14] J. H. Silverman, after giving a new proof for the case $n=3$, observes that it is best possible, if $g=0$, for every value of $\#S$. In [3] the authors give examples with $n=3$, any $g\ge0$

and infinitely many values of $\#S$. (For a combinatorial method of proving the existence of examples with given $g$ and $\#S$ see Remark 2 below.) They also remark that, when $n > 3$, $\binom{n-1}{2}$ cannot be replaced with $n-3$.

Now J. Browkin and J. Brzeziński in [2] have examples which show that (at least when $g = 0$), $\binom{n-1}{2}$ cannot be replaced with $2n-5-\varepsilon$ for any value of $\#S$ and any $\varepsilon > 0$. In particular, the coefficient $\binom{n-1}{2}$ is best possible even for $n = 4$.

Another question which one can ask is to characterize extremal examples, if there are any. Theorem 3 is a first observation in that direction.

P r o o f o f T h e o r e m 3. (We shall practically repeat the proof for the case $n = 3$.) For $v$ a place of $K$ we calculate $v(da/dt_v)$ according to four possibilities:

(i) $v(a) < 0$. Now $v(a) = v(b)$ and $v(da/dt_v) = v(a) - 1$.
(ii) $v(a) > 0$. In this case $v(b) = 0$ and again $v(da/dt_v) = v(a) - 1$.
(iii) $v(b) > 0$. Now $v(a) = 0$ and $v(da/dt_v) = v(-db/dt_v) = v(b) - 1$.

These cases correspond to all $v \in S$. Also observe that we may combine (i)–(iii) in a single formula, viz.

$$v(da/dt_v) = \max(v(a), v(b)) - 1 = v(a) + v(b) - \min(v(a), v(b)) - 1 \tag{19}$$

for all $v \in S$.

The remaining case is thus

(iv) $v \notin S$, i.e. $v(a) = v(b) = 0$. If $p$ is the place of $k(a)$ below $v$ then $p \neq \infty$ and $a - p$ (we identify $p$ with an element of $k$) is a local parameter at $p$ in $k(a)$. We may write $a - p = t_v^{e_v}\varrho$ where $e_v$ is the ramification index over $p$ and $\varrho \in K$ is a unit at $v$. Differentiating with respect to $t_v$ we obtain

$$v(da/dt_v) = e_v - 1\,. \tag{20}$$

Now using (19) and (20) in the formula $\sum_v v(da/dt_v) = 2g-2$ and recalling that

$$\sum_v v(a) = \sum_v v(b) = 0, \qquad \min(v(a), v(b)) \leq 0 \qquad (\text{since } a + b = 1)$$

we get

$$H(a, b, 1) = \#S + 2g - 2 - \sum_{v \notin S}(e_v - 1)\,.$$

This shows that we have an extremal example iff $e_v = 1$ for all $v \notin S$, namely iff $K/k(a)$ is unramified outside $S$.

To obtain the first part of Theorem 3 it thus suffices to remark again that a place $v$ of $K/k$ lies in $S$ if and only if either $v(a) < 0$ or $v(a) > 0$, or $v(1-a) > 0$, i.e. if and only if $v$ lies above one of the places $\infty, 0, 1$ of $k(a)$.

For the second part we use the Lefschetz principle to assume $k = \mathbb{C}$ and follow mainly M. Fried's paper [5]. Let $n = [K : k(a)]$.

We consider the inclusion $k(a) \subset K$ as an $n$-sheeted covering

$$a : \Sigma_1 \to \Sigma$$

of Riemann surfaces of genera resp. $g, 0$, unramified except above $\{0, 1, \infty\}$. Let $p \in \Sigma - \{0, 1, \infty\} = \mathbb{C} - \{0, 1\}$ and let $\{\zeta_1, \dots, \zeta_n\}$ be the fiber above $p$. Then it is well known that we have a transitive representation

$$\sigma : \pi_1(\mathbb{C} - \{0, 1\}) \to S_n = \{\text{permutations on } \zeta_1, \dots, \zeta_n\}\,. \tag{21}$$

(Given a closed path $P$ through $p$ in $\mathbb{C} - \{0, 1\}$ the permutation $\sigma(P)$ assigns to $\zeta_i$ the end point of a lifting of $P$ starting at $\zeta_i$. See [5], p. 43, or [12], §58, and the related references for more details.)

Also, let $a_* \in K_*$ be such that $n = [K_* : k(a_*)]$ and consider the corresponding covering $a_* : \Sigma_{1*} \to \Sigma_*$ as above, also supposed to be unramified except above the places $0, 1, \infty$ of $\Sigma_*$ (so the equation $a_* + (1 - a_*) = 1$ gives another extremal example with the same degree $n$). Assume, moreover, that the associated representation $\sigma_*$ is isomorphic to $\sigma$ (i.e. $\sigma_* = \tau\sigma\tau^{-1}$ for some bijection $\tau : \{\zeta_1, \dots, \zeta_n\} \to \{\zeta_{1*}, \dots, \zeta_{n*}\}$). There is a canonical covering $\phi : \Sigma_* \to \Sigma$ of degree 1 associated with the canonical isomorphism $k(a) \cong k(a_*)$. Then, clearly, letting $\sigma_{**}$ be the representation associated with the composite covering $\phi \circ a_* : \Sigma_{1*} \to \Sigma$, we also have $\sigma_{**} \cong \sigma_* \cong \sigma$. In this situation the proof of Lemma 6, p. 44 of [5] (which extends at once to our case) shows that there exists an analytic isomorphism $l : \Sigma_1 \to \Sigma_{1*}$ such that

$$\phi \circ a_* \circ l = a\,.$$

(Alternatively to [5] one can use standard topological theory of covering spaces to construct first a homeomorphism $\tilde{l}$ defined *only outside the ramification points*. In our setting, $\tilde{l}$ becomes automatically analytic and may be extended to an analytic isomorphism $l$ as above, by the classical theory of Riemann surfaces.)

If $L : K_* \to K$ denotes the isomorphism corresponding to $l$ this equation is equivalent to $a = L(a_*)$, so, according to our definition, the two "extremal examples" are in fact the same.

Hence "essentially distinct" examples of the same degree $n$ correspond to distinct isomorphism classes of representations (21), which are clearly finite in number, $\pi_1(\mathbb{C} - \{0, 1\})$ being a free group generated by two elements.

Since $\#S$ and $g$ determine the degree $n$ (just use $n = H(a, b, 1) = \#S + 2g - 2!$), Theorem 3 follows.

R e m a r k 1. It is well known (see for instance [15]) that the Galois group of the normal closure of $K$ over $k(a)$ is isomorphic to the image of $\sigma$ (which is

classically referred to as the "monodromy group"). Also, let $P_0, P_1$ be clockwise oriented nonintersecting circles around $0, 1$ resp. Then their homotopy classes generate $\pi_1(\mathbb{C} - \{0,1\})$. Moreover, the cycle lengths in the canonical decomposition of $\sigma(P_0), \sigma(P_1)$ and their product are the ramification indices over $0, 1, \infty$ resp. (observe that the product of the homotopy classes of $P_0, P_1$ is the class of a small circle around $\infty$ in the Riemann sphere $\Sigma$).

That the ramification indices correspond to the cycle lengths is stated for instance in Lemma 5, p. 44 of [5] or in [4]. It may be proved for example by recalling that near a ramified point $\zeta$ above 0, say, local coordinates may be chosen in such a way that the covering map is equivalent to $z \to z^e$ in a neighborhood of $\zeta$, where $e$ is the ramification index. If we assume, as we may without loss of generality, that $P_0$ is sufficiently small, the action of $\sigma(P_0)$ on points near $\zeta$ becomes explicit, namely it is the action of an $e$-cycle.

R e m a r k 2. Using [12], §58, pp. 198–200 (see also the construction in [4] and the related references, or [15]) one proves the existence, for any given transitive representation $\sigma$ as in (21), of an associated $n$-sheeted covering $\Sigma_1$ of the Riemann sphere as above ([5]). The book [12] furnishes the topological construction. That the resulting space is actually a Riemann surface is a classical theorem in the theory: *Every compact ramified covering of the Riemann sphere is the Riemann surface of an algebraic function $w$ of the independent complex variable $z$* ([6]).

This covering corresponds to an "extremal example" with $K$ of genus $g$ precisely if $\Sigma_1$ is of genus $g$. By the Hurwitz genus formula this is equivalent to a certain relation among the ramification indices above $0, 1, \infty$ (see formula (22) below), which in turn correspond, by Remark 1, to the cycle lengths of certain permutations $\omega_0, \omega_1, \omega_0\omega_1$ related to the given representation of $\pi_1(\mathbb{C} - \{0,1\})$. Counting the number of essentially distinct extremal examples with given $\#S$ and given $g$ is thus reduced to a purely combinatorial problem about cycle decompositions in $S_n$ (where $n = \#S + 2g - 2$). Namely, we must count the number of pairs of elements in $S_n$, up to conjugation, which generate a transitive subgroup and are such that their cycle lengths satisfy a certain relation together with the cycle lengths of their product, namely formula (23) below.

To outline the method, let $e_i, e_j^*, e_k^{**}$ be the cycle lengths in the canonical decomposition of the permutations $\omega_0, \omega_1, \omega_0\omega_1$ resp., assuming that these generate a transitive group in $S_n$. By Remark 1 and the Hurwitz genus

([5]) This statement seems to be well known, as M. Fried states on p. 43 of [6], even if it is not easy to locate a complete proof in the literature.

([6]) This statement appears in [15], p. 496. For a proof see for instance Siegel's book [13].

formula the genus $g$ of our covering is given by ([7])

$$2g-2=-2n+\sum(e_i-1)+\sum(e_j^*-1)+\sum(e_k^{**}-1)\,. \tag{22}$$

If we let $h_0, h_1, h_\infty$ resp. be the number of cycles belonging to the above permutations, the last formula gives

$$h_0+h_1+h_\infty=n+2-2g\,. \tag{23}$$

To find permutations as above which satisfy this equation is equivalent to proving the existence of an extremal example with $K$ of genus $g$ and with $\#S$ given by the common value of the sides of the equation. It is trivially checked that, setting $\omega_0=(1,\dots,n)$, $\omega_1=(1,\dots,2g+1)$ where $n>2g$, we obtain such an instance, since

$$(1,\dots,n)\circ(1,\dots,2g+1)=(1,3,\dots,2g+1,2,4,\dots,2g+2,2g+3,\dots,n).$$

(For a purely algebraic approach to some of the above topological questions, as remarked in [5], one can see [7], especially [8, Cor. 6.9, p. 6.7].)

As recalled in the introduction interesting examples arise from the study of finite groups of linear fractional transformations: in this way one obtains indeed all cases when $K=k(t)$ is Galois over $k(a)$. A complete list is given in [2].

Also, it is perhaps worth mentioning that another instance, relevant both in the context of Ritt's second Theorem (see [11], p. 26, Lemma 6) and in the theme of [5] (see Lemma 12), appears in connection with Chebyshev polynomials.

I would like to thank Professor A. Schinzel for his kind attention, generous encouragement and indication of several references. I also wish to thank Dr. B. Chiarellotto for useful conversations in which he pointed out to my attention papers [4], [15] and the book [12].

## References

[1] F. Baldassarri and B. Dwork, *On second order linear differential equations with algebraic solutions*, Amer. J. Math. 101 (1979), 42–76.

[2] J. Browkin and J. Brzezi/nski, *Some remarks on the abc-conjecture*, Math. Comp., to appear.

[3] W. D. Brownawell and D. Masser, *Vanishing sums in function fields*, Math. Proc. Cambridge Philos. Soc. 100 (1986), 427–434.

[4] B. Chiarellotto, *On Lamé operator with finite monodromy group*, Trans. Amer. Math. Soc., to appear.

[5] M. Fried, *On a conjecture of Schur*, Michigan Math. J. 17 (1970), 41–55.

([7]) The formula which follows appears, even in a more general form, on p. 43 of [6].

[6] M. Fried, *On a theorem of Ritt and related diophantine problems*, J. Reine Angew. Math. 264 (1973), 40–55.
[7] W. Fulton, *Fundamental Group of a Curve*, Archives of the Princeton University Mathematics Library, 1966.
[8] R. C. Mason, *Equations over function fields*, in: Number Theory, Noordwijkerhout 1983, Lecture Notes in Math. 1068, Springer, 1984, 149–157.
[9] —, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge Univ. Press, 1984.
[10] —, *Norm form equations I*, J. Number Theory 22 (1986), 190–207.
[11] A. Schinzel, *Selected Topics on Polynomials*, Univ. of Michigan Press, 1982.
[12] H. Seifert and W. Threlfall, *Lehrbuch der Topologie*, Teubner, Leipzig 1932.
[13] C. L. Siegel, *Topics in Complex Function Theory*, Vol. I, Interscience Publ., New York 1969.
[14] J. H. Silverman, *The S-unit equation over function fields*, Math. Proc. Cambridge Philos. Soc. 95 (1984), 3–4.
[15] M. Tretkoff, *Algebraic extensions of the field of rational functions*, Comm. Pure Appl. Math. 24 (1971), 491–497.
[16] J. F. Voloch, *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat. 16 (1985), 29–39.

IST. UNIV. ARCH. D.S.T.R.
S. CROCE, 191
30135 VENEZIA
ITALY

*Received on 13.7.1992*
*and in revised form on 16.10.1992* (2280)