ACTA ARITHMETICA
LXXI.2 (1995)

On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's Existence Theorem

by

Umberto Zannier (Venezia)

1. Introduction. In [Dav] H. Davenport, solving in the affirmative part of a conjecture stated in [BCHS], proved the following theorem about the distance between squares and cubes of polynomials with complex coefficients:

Let f, g be polynomials with complex coefficients. Then either $f^3 = g^2$, or $\deg(f^3 - g^2) \geq \frac{1}{2}\deg f + 1$.

(Actually Davenport remarked that the method would yield a more general result, which he stated explicitly.) The remaining half of the conjecture, namely the existence of pairs of distinct polynomials f^3, g^2 with arbitrarily large degrees, and satisfying the bound with equality, remained open. (In [BCHS] examples appear with $\deg f = 6, 10$, and Davenport gave an example with $\deg f = 16$.)

The result partly motivated M. Hall's conjectural formulation of an analogous statement concerning rational integers instead of polynomials. In his paper [Ha], Hall also wrote down examples, of small degrees, when the above theorem holds with equality (see p. 185), and a characterization for them, in terms of the roots of f and g is a particular case of a criterion due to M. Langevin (see [La], Thm. 1 and the examples at p. 3). Other examples of attainment of Davenport's bound were found by S. Uchiyama and M. Yorinaga in [U-Y]; in that paper the authors also sketch some computational shortcuts useful to find such cases of equality. They do not, however, prove the full original conjecture that equality occurs for infinitely many values of the degrees.

Davenport's theorem, as remarked for instance in [Lang, p. 48], follows at once from the so called *abc theorem for function fields* of R. C. Mason [Ma], applied in the genus zero case, and the cases of equality become "extremal examples" for Mason's inequality. In [Za] such examples were shown to correspond to coverings of the Riemann sphere, unramified except above

$0, 1, \infty$ ([1]). (Such coverings are quite remarkable, especially after Belyi's Theorem; see [Gr] or [S-V].) Accordingly, a combinatorial criterion was given for the existence of examples with prescribed degree and monodromy: this is Riemann's Existence Theorem (see Section 2 below). As a consequence, for given degree, the number of "essentially distinct" extremal examples was shown to be finite. Also, this approach allowed us to prove the existence (in zero characteristic) of extremal examples of arbitrary genus g and degree $n \geq 2g-2$, a question left partially unanswered by Brownawell and Masser in [B-M].

The purpose of this paper is to exploit the criterion of [Za] to complete the proof of the [BCHS] conjecture, showing the existence of equality cases for Davenport's Theorem for any positive integer n, and f, g of degrees $2n, 3n$ resp. We shall show in Section 5 that the solutions fall into finitely many families which correspond to trees on $2n$ points, with each degree equal to either 1 or 3 (their number will be estimated in an appendix), each tree being assigned certain orientations around each vertex. We shall in fact first carry out in Section 4 a similar investigation on more general extremal cases of the *abc* theorem, producing an existence result (Theorem 1) for distinct polynomials F, G with roots of prescribed multiplicities and $\deg(F-G)$ as small as possible (as in (6) of Section 4).

An interesting question in this context is whether these constructions may be realized over the rationals, say. (This fits into the theory of the field of definition of what Grothendieck called *dessins d'enfant*—see [Gr] or [S-V]). When this is the case one may obtain numerical inequalities close to the conjecturally optimal ones, just by specializing the variable to positive integers. Corresponding for instance to Davenport's Theorem, there is Hall's conjecture ([Ha], p. 175) stating that $|x^3 - y^2| > C|x|^{1/2}$, C being some positive absolute constant. Suppose now to have polynomials f, g with integral coefficients and degrees $3n, 2n$ resp., such that $\deg(f^3 - g^2) = n+1$. Then, as Hall himself remarks, setting $x = f(t), y = g(t)$, we would get, for large integers t, the existence of integers x, y with

$$0 < |x^3 - y^2| \ll |x|^{1/2+1/(2n)}.$$

In this case anyway, no matter how large n may be, this statement is superseded by Danilov's result [Dan] (a part of Hall's conjecture) that $|x^3 - y^2| \leq 0.97|x|^{1/2}$ for infinitely many integers x (in fact Schinzel has shown that one may take $54/(25\sqrt{5})$ in place of 0.97; see [Sie], p. 105). Still, Danilov's identity, based on solutions of a Pell equation, produces exponen-

([1]) In fact Vojta [Vo] had previously noticed a connection between the *abc* and ramification above $0, 1, \infty$. This was used by Elkies (Duke Math. J. Internat. Res. Notes 7 (1991), 95–109) to deduce an effective Falting's Theorem from the numerical *abc*.

tially growing sequences of such x's, while the above identity gives, when it exists, polynomial behaviour.

We cannot, however, prove that such identities may be realized over the rationals for infinitely many n (and in fact some of the considerations of Section 6 and Section 7—as well as the computations carried out in [U-Y]—somewhat suggest this might well be false). We only give a criterion, valid also for analogues of Davenport's result, which establishes the realizability over the rationals of extremal examples provided the underlying combinatorial structure is essentially unique. The method of proof is a very simple instance of descent, and provides in any case a bound on the degree of a number field where the construction can be realized. Analogues of it have being used to realize over $\mathbb{Q}(T)$ certain Galois groups, provided the so-called *rigidity condition* (in some respects analogous to what we require) is satisfied (see [Se1], Ch. 8, and the related references).

To my knowledge no analogue of Riemann's Theorem is known in positive characteristic, so we cannot apply our methods in that case. However, in Section 7 we shall prove the possibility of lifting coverings considered in Section 4, unramified outside $0, 1, \infty$, from an algebraic closure $\mathcal{F}_p$ of $\mathbb{F}_p$ to the maximal unramified extension of $\mathbb{Q}_p$. Also, the isomorphism class of the lifting depends only on the class of the reduction. A consequence is that the number of isomorphism classes mod p cannot be greater than over $\mathbb{C}$. (Our proofs will be simple and direct.) When good reduction is possible in the same class of a covering defined over a number field L, for various prime numbers, we shall show that it is possible to find a covering in the same class, with good reduction simultaneously at all such primes, and defined over the Hilbert class field of L. We shall also show how the existence of examples mod p bounds the ramification in the field generated by zeros and poles of the cover, over L.

In the course of this investigation we came across the observation that Riemann Existence Theorem combined with the Riemann–Hurwitz formula immediately implies an inequality for the total number of disjoint cycles in the canonical decomposition of certain permutations (see (2) of Section 3). When only three permutations appear, the equality cases may be thought of as a combinatorial counterpart of extremal examples of the *abc* theorem. P. M. Neumann kindly informed us that such inequality had in fact been noticed by several authors. Topological proofs were given by D. Singerman [Sin], for the case $r = 3$, and by R. Ree ([Ree]) generally. More direct proofs were given later by W. Feit, R. Lyndon and L. L. Scott [FLS] and by M. Conder and J. McKay [CMK]. Since this inequality naturally appears in the context of the present paper, we have thought to be not out of place to present here a proof of it, which to our knowledge is new, and is completely direct and elementary, involving no considerations of topology or graph theory.

2. Riemann's Existence Theorem. Before giving precise statements and proofs we briefly recall, for the sake of completeness, some classical facts about Riemann's Existence Theorem, and their relation to extremal cases of *abc*.

Let X be a compact Riemann surface of genus g, and let $\phi : X \to \mathbb{P}^1$ be an n-sheeted covering, ramified (possibly) only above some of the (distinct) points $p_1, \dots, p_r$. Let $z \in \mathbb{P}^1 - \{p_1, \dots, p_r\}$ and let $\{\zeta_1, \dots, \zeta_n\}$ be the fiber above z. We then have a transitive representation (the monodromy representation)

$$\sigma : \pi_1(\mathbb{P}^1 - \{p_1, \dots, p_r\}) \to S_n \ (= \{\text{permutations on } \zeta_1, \dots, \zeta_n\}) \tag{1}$$

constructed as follows: given a closed path $\mathcal{P}$ through z in $\mathbb{P}^1 - \{p_1, \dots, p_r\}$, the permutation $\sigma(\mathcal{P})$ sends ζ_i to the end point of a lifting of $\mathcal{P}$ starting at ζ_i (this of course depends only on the homotopy class of $\mathcal{P}$).

Two such representations σ, σ^* are considered equivalent if $\sigma^*(\mathcal{P}) = \tau\sigma(\mathcal{P})\tau^{-1}$ for some $\tau \in S_n$ and all paths $\mathcal{P}$ as above. A basic fact is that *two coverings ϕ, ϕ^* as above are isomorphic (namely $\phi^* = \phi \circ \psi$ for some automorphism ψ of X) if and only if the associated representations are equivalent*. This assertion is part of Riemann's theorem; a proof of a particular case (which extends at once) appears as Lemma 6, p. 44 of [Fr1]; see also [Fr2], p. 25 or [Za], p. 95.

Choose now, once and for all, loops $\mathcal{P}_1, \dots, \mathcal{P}_r$ in $\mathbb{P}^1 - \{p_1, \dots, p_r\}$, all through z, any two of which intersect precisely in z, such that their homotopy classes (denoted with the same letters) generate $\pi_1(\mathbb{P}^1 - \{p_1, \dots, p_r\})$ and satisfy $\mathcal{P}_1 \dots \mathcal{P}_r = \mathrm{id}$. There are of course many such choices, but we normalize them similarly to [Fr2], p. 25, namely by requiring that $\mathcal{P}_i$ consists of three parts: a path from z to some point p_i' "very near" to p_i, then a small (i.e. containing only p_i as a ramification point) oriented circle around p_i back to p_i', then back to z along the same path as before (of course we must never go through any ramification point). Given a covering $\phi : X \to \mathbb{P}^1$ as above we thus get permutations $\sigma_i := \sigma(\mathcal{P}_i), i = 1, \dots, r$, with the following properties:

(i) $\sigma_1 \dots \sigma_r = 1$,

(ii) the subgroup Γ of S_n generated by $\sigma_1, \dots, \sigma_r$ (the monodromy group) is transitive,

(iii) if $\sigma_1^*, \dots, \sigma_r^*$ are the analogous permutations associated with another covering $\phi^* : X \to \mathbb{P}^1$, then the coverings are isomorphic if and only if $\sigma_i^* = \tau\sigma_i\tau^{-1}$ for some $\tau \in S_n$ and $i = 1, \dots, r$.

Such permutations $\sigma_1, \dots, \sigma_r$ are called a *description of the branch cycles* of the covering. They depend, apart from the covering itself, on the choice of the base point z, on the choice of loops $\mathcal{P}_i$ as above, and on the naming

of the fiber above z. In [Fr2], it is shown (see Lemma 1.1, p. 28) that, if τ_i is another description of the branch cycles corresponding to the same cover, then the conjugacy class of σ_i in G is the same as the one of $\gamma\tau_i\gamma^{-1}$, for some $\gamma \in S_n$. In particular, σ_i has the same cycle decomposition type as τ_i. One finds that

(iv) the cycle lengths in the canonical decomposition of σ_i correspond to the ramification indices above p_i.

In fact, near a ramified point $\widetilde{p}_i$ above p_i, local coordinates may be chosen to make the covering map equivalent to $x \to x^e$ near 0, where e is the ramification index. Then the action of lifting a sufficiently small circle near $\widetilde{p}_i$ is that of an e-cycle (see also [Za], p. 96); since σ_i is conjugate to such a permutation, the assertion follows.

A fundamental fact is that, given the above structure on $\mathbb{P}^1$ (namely the point z, the p_i's and the associated loops), and given permutations $\sigma_1, \dots, \sigma_r$ satisfying (i) and (ii),

(v) there exist a compact Riemann surface X and a covering $\phi : X \to \mathbb{P}^1$ unramified except possibly above some p_i, of degree n, such that σ_i is its description of the branch cycles corresponding to the given loops $\mathcal{P}_i$.

This is the remaining part of Riemann's Existence Theorem for covers of $\mathbb{P}^1$, a particular case of the statement in [Fr2], p. 25. See also [Ch], Remark 2 in [Za], or [Tr]. For a somewhat different approach see [Se1], Thms. 7.5, 7.6.

For later reference we recall a particular case of Lemma 2.2, p. 32 of [Fr2], stating that

(vi) the subgroup $C = \{\tau \in S_n : \tau\sigma_i\tau^{-1} = \sigma_i \ \forall i\}$ is isomorphic to the automorphism group of the covering.

3. The Ree–Singerman inequality. For a permutation $\sigma \in S_n$, product of disjoint cycles $\lambda_1, \dots, \lambda_h$ ([2]) of lengths $l_1, \dots, l_h$ resp., we set $\mathrm{ind}(\sigma) := \sum(l_i - 1) = n - h$.

Let ϕ, X be as above and let $\sigma_1, \dots, \sigma_r$ be a description of the branch cycles. Fact (iv) above combined with the Riemann–Hurwitz formula gives, for the genus g of X, the equality

$$2g - 2 = -2n + \sum \mathrm{ind}(\sigma_i) = -2n + \sum (n - h_i),$$

where h_i is the number of disjoint cycles in the canonical decomposition of σ_i. Since $g \geq 0$ we get

$$\sum h_i \leq (r-2)n + 2. \tag{2}$$

([2]) We also count cycles of length 1.

By (v) the permutations σ_i are subject only to (i) and (ii) and otherwise arbitrary. (2) becomes thus a purely combinatorial statement, the inequality referred to in the introduction. As announced, we now present a new, completely direct proof of it.

From now on we agree that permutations act on the right of integers.

We prove the following (equivalent) statement about transpositions.

PROPOSITION 1. *Let $t_1, \dots, t_m$ be transpositions in S_n such that*:

(i) $t_1 t_2 \dots t_m = 1$,

(ii) *for each nonempty proper subset A of $\{1, \dots, n\}$ there exists j such that t_j moves both A and its complement in $\{1, \dots, n\}$.*

Then $m \geq 2(n-1)$.

Proof. We argue by induction on n, the case $n = 2$ being trivial. If $t = (n, \mu)$ is some t_j moving n, we change (possibly) the situation according to the following rules:

(R1) If either $j = 1$ or if t_{j-1} moves n, then we leave everything for the moment unchanged.

(R2) If $t_{j-1} = (a, b)$ with $\{a, b\} \cap \{n, \mu\} = \emptyset$ we move t_j and t_{j-1} using $t_{j-1} t_j = t_j t_{j-1}$.

(R3) If $t_{j-1} = (a, \mu)$ where $a \neq n$ we use the identity $(a, \mu)(n, \mu) = (n, a)(a, \mu)$ to replace t_{j-1}, t_j resp. with $(n, a), (a, \mu)$.

It is verified at once that application of each rule leaves (i) and (ii) unchanged. Even m remains unaltered, and the same holds for the number k of transpositions moving n (by (ii), $k \geq 1$). Plainly, with a suitable iteration of this procedure, we shall be able to "move" on the left all the transpositions moving n, and to assume without loss of generality that $t_1, \dots, t_k$ move n, while none of $t_{k+1}, \dots, t_m$ does.

Now, if two consecutive ones of $t_1, \dots, t_k$ are of type $(n, a), (n, b)$ with $a \neq b$, we replace them resp. with $(n, b), (a, b)$, which is possible in view of the identity $(n, a)(n, b) = (n, b)(a, b)$. Such a substitution replaces k with $k - 1$ and leaves m, (i) and (ii) unchanged. Iteration of such procedures leaves us with a situation where $t_1 = \dots = t_h = (n, a)$, while $t_{h+1}, \dots, t_m$ do not move n (since (ii) is still valid, we have $h > 0$). If $h > 2$, we simply omit t_1 and t_2. This makes both h and m smaller, but leaves (i) and (ii) unchanged. So, since we are proving a lower bound for m, we may assume that $h = 1$ or 2. However, $h = 1$ is impossible in view of $t_1 \dots t_m = 1$. Assume then $h = 2$. Plainly $t_3 \dots t_m = 1$, while $t_3, \dots, t_m \in S_{n-1}$.

We show that $t_3, \dots, t_m$ satisfy (i) and (ii), but with $n - 1$ in place of n. (i) has just being shown. To prove (ii) let A^* be a proper nonempty subset of $\{1, \dots, n-1\}$ and let B denote its complement with respect to $\{1, \dots, n-1\}$. By symmetry we may assume that $a \in A^*$. Assume that none

of t_j, $3 \le j \le m$, moves both A^* and B. In this case none of the t_j, $1 \le j \le n$, moves both $A := A^* \cup \{n\}$ and B, contrary to the assumption (ii) for the original transpositions. The inductive assumption applied to $t_3, \dots, t_m$ gives $m - 2 \ge 2(n-2)$, i.e. $m \ge 2(n-1)$, as required. ∎

Also, from Proposition 1(i) it follows immediately that m is even.

Now let $\sigma_1, \dots, \sigma_r \in S_n$ be permutations generating a transitive subgroup and such that $\sigma_1 \dots \sigma_r = 1$, and let h_i denote, as above, the number of disjoint cycles of σ_i. Since a cycle of length l may be written as the product of $l-1$ transpositions, σ_i may be written as the product of $\mathrm{ind}(\sigma_i) = n - h_i$ transpositions. To the total set of such transpositions, ordered in an obvious manner, we may apply the above proposition, assumption (ii) being a consequence of transitivity. So $\sum(n - h_i) \ge 2n - 2$, which gives (2) (in fact, (2) applied to the transpositions t_i implies Proposition 1).

4. Attained lower bounds for $\deg(F-G)$**.** Recall Mason's *abc* theorem for polynomials (we assume throughout that only complex coefficients are involved):

If a, b, c are coprime polynomials such that $a - b = c$, and $n > 0$ is the maximum of their degrees, then $n+1$ does not exceed the number of distinct roots of abc.

Let now F, G be *distinct* polynomials of exact degree n and assume that F has precisely h distinct roots of prescribed multiplicities $\mu_1, \dots, \mu_h$, while G has exactly k roots with multiplicities $\nu_1, \dots, \nu_k$. Here μ_i, ν_j are prescribed sequences of positive integers with

$$n = \sum_{i=1}^{h} \mu_i = \sum_{j=1}^{k} \nu_j. \tag{3}$$

We seek a lower bound for $\deg(F - G)$. Let $D = (F, G)$, and let l be the number of distinct roots of D. Apply Mason's inequality to $a = F/D$, $b = G/D$, $c = a - b$, the assumptions being clearly fulfilled. The product abc has at most $h + k - l + \deg c$ distinct roots, while both a, b have degree $n - \deg D$, so

$$\deg(F - G) = \deg c + \deg D \ge n - h - k + l + 1 \ge n - h - k + 1 \tag{4}$$

and equality may occur only if F, G are coprime, i.e. $l = 0$, if $F - G$ has distinct roots, and if

$$n + 1 \ge h + k. \tag{5}$$

Assume now that all the multiplicities μ_i, ν_j are divisible by a positive integer δ. Then $F = f^\delta$, $G = g^\delta$, where f, g satisfy the same assumptions of F, G above, but with n/δ in place of n, and with μ_i/δ (resp. ν_j/δ) in place of

μ_i (resp. ν_j). Now $F-G=\prod_{\zeta^\delta=1}(f-\zeta g)$. All factors but one have degree n/δ, while the degree of the remaining factor may be estimated by (4) as being at least $\max\{0, n/\delta-h-k+1\}$. In conclusion,

$$\deg(F-G)\geq \max\left(n\frac{\delta-1}{\delta}, n-h-k+1\right). \tag{6}$$

(This covers also Davenport's generalization, given as (4) in [Dav].) The argument shows also that the bound may be attained if and only if the corresponding bound may be attained with f,g in place of F,G and μ_i/δ, ν_j/δ in place of μ_i, ν_j. We shall show that this will always be the case.

THEOREM 1. *Let positive integers μ_i, ν_j satisfying* (3) *be given. Then there exist polynomials F,G having μ_i, resp. ν_j as the sequences of multiplicities of their roots, satisfying* (6) *with equality.*

Proof. We proceed by induction on n, the case $n=1$ being trivial.

Assume first that

$$n/\delta-h-k+1\geq 0, \tag{7}$$

and that there is equality in (6), so we have an extremal example of Mason's inequality, and consider the covering

$$\phi:\mathbb{P}^1\to\mathbb{P}^1$$

where $\phi=F/G$ has degree n, since $(F,G)=1$. By Theorem 3 of [Za] (or even by a calculation using the Riemann–Hurwitz formula), the covering is ramified possibly only above $0,1,\infty$. The ramification indices over 0 are the μ_i, over ∞ they are the ν_j, and over 1 they are a sequence of $(n-h-k+1)$ 1's (corresponding to the distinct roots of $F-G$), plus one index equal to $h+k-1$ (which corresponds to the root $t=\infty$ of $F(t)/G(t)-1$, counted with multiplicity $h+k-1$). By the same Theorem 3 of [Za], if the covering (4) is unramified except (possibly) above $0,1,\infty$, then we have an extremal example, the multiplicities of the roots of F,G corresponding to the ramification indices above $0,\infty$ resp., and the multiplicities of the roots (in $\mathbb{P}^1$) of $F(t)/G(t)-1$ corresponding to the ramification indices above 1: observe that any root $t=\beta$ of $F(t)/G(t)-1$ may be sent to $t=\infty$ by means of a linear fractional transformation (i.e. an automorphism of $\mathbb{P}^1$), which leaves the other properties unchanged. To realize our construction it will suffice, in view of (iv) and (v) of Section 2 (applied with $r=3$ and p_1,p_2,p_3 equal to $0,\infty,1$ resp.), to find permutations $\sigma_1,\sigma_2,\sigma_3\in S_n$ such that

(A) $\sigma_1\sigma_2\sigma_3=1$, the identity permutation,
(B) the subgroup of S_n generated by σ_i, $i=1,2$, is transitive,
(C) σ_1 is a product of disjoint cycles of lengths $\mu_1,\dots,\mu_h$,
(D) σ_2 is a product of disjoint cycles of lengths $\nu_1,\dots,\nu_k$,

(E) σ_3 (or, equivalently, the product $\sigma_1\sigma_2$) is a product of a cycle of length $h + k - 1$ with $n - h - k + 1$ trivial cycles of length 1.

Observe that when (A)–(E) are satisfied, we have a case of equality in the Ree–Singerman inequality ((2) of Section 3). Observe also that, by this same inequality, (E) may be replaced by the apparently weaker

(E′) $\sigma_1\sigma_2$ has at least $n - h - k + 1$ fixed points.

In fact, if the σ_i satisfy (A)–(D), (E′), then σ_3 has at least $n - h - k + 1$ trivial cycles, so, by the Ree–Singerman inequality, only one more cycle may appear in its canonical decomposition, whence (E) is also satisfied.

We now proceed to show that the construction may be realized under the additional assumption $\delta = 1$. If this is not the case, the inductive assumption applies immediately (by the remark following (6)).

Consider the smallest multiplicity, say, $\mu = \mu_1$. We may assume that $\nu_r > \mu$ for some r. If not, then we choose ν_1 in place of μ_1. Now, if $\mu_i = \nu_1$ for all i, we have (since $\delta = 1$) $\mu_i = 1 = \nu_j$ for all i, j, whence $n = 1$, a trivial case. Otherwise $\mu_i > \nu_1$ for some i, so our assumption would hold by reversing the role of μ_i, ν_j.

We show first that, for some r such that $\nu_r > \mu$, the construction may be realized, but with $n - \mu = n'$, say, in place of n, with $\mu_2, \ldots, \mu_h$ in place of $\mu_1, \ldots, \mu_h$, and with the multiplicities ν_j unchanged, except that ν_r is replaced by $\nu_r - \mu$ (so h is replaced by $h-1$ while k remains unchanged). For $\nu_r > \mu$ let δ_r be the g.c.d. of the new sequence of multiplicities just defined. To prove our assertion it suffices, in view of the inductive hypothesis, to show that, for some r as above,

$$n'/\delta_r + 1 \geq (h - 1) + k. \tag{8}$$

Assume $\delta_r = 1$ for some r. If $\mu = 1$, inequality (8) follows then from (7). If $\mu > 1$, observe that $h, k \leq n/\mu$, whence (8) is implied by $(n-\mu)(\mu-2) \geq 0$, which holds.

If some $\nu_s = \mu$ then certainly $\delta_r = 1$, for in this case δ_r divides $\delta = 1$.

So we may assume that $\nu_r > \mu$ and that $\delta_r > 1$ for all $r = 1, \ldots, k$. It is immediately verified that the g.c.d. of any two δ_r's is a divisor of $\delta = 1$, so the δ_r's are pairwise coprime, whence their product divides μ_i for all $i \geq 2$. In particular,

$$h - 1 \leq \frac{n'}{\delta_1 \ldots \delta_k}. \tag{9}$$

If $k = 1$, (8) follows. Otherwise, observe that $\delta_1\delta_2$ divides ν_j for $j > 2$, while $\delta_1 \leq \nu_1 - \mu$, $\delta_1 \leq \nu_2$. Hence $n' \geq (k - 2)\delta_1\delta_2 + 2\delta_1$, or

$$k - 1 \leq \frac{n'}{\delta_1\delta_2} + 1 - \frac{2}{\delta_2}.$$

Combining this inequality with (9) we get

$$h+k-2 \le 2\frac{n'}{\delta_1\delta_2}+1-\frac{2}{\delta_2} \le \frac{n'}{\delta_1},$$

proving (8) with $r=1$.

By induction we may thus assume to have permutations $\sigma_i^* \in S_{n'}$, $i=1,2$, such that

(B*) they generate a transitive subgroup of $S_{n'}$,
(C*) σ_1^* is a product of disjoint cycles of lengths $\mu_2,\dots,\mu_h$,
(D*) σ_2^* is a product of disjoint cycles of lengths $\nu_1-\mu,\nu_2,\dots,\nu_k$,
(E$'^*$) $\sigma_1^*\sigma_2^*$ has at least (hence exactly) $n'-h-k+2$ fixed points.

We define $\sigma_i \in S_n$, $i=1,2$, as follows: σ_1 is defined just as the product of σ_1^* by the cycle $(n'+1,\dots,n)$, of length μ. To define σ_2 consider a cycle α of σ_2^* of length $\nu_1-\mu$. We may write, without loss of generality, $\alpha=(1,2,\dots,\nu_1-\mu)$, where 1 is not a fixed point of $\sigma_1^*\sigma_2^*$. In fact, not every element moved by α may be left fixed by $\sigma_1^*\sigma_2^*$, for otherwise α would be a disjoint cycle of σ_1^*, contradicting condition (B*). Define then σ_2 as the product of the same disjoint cycles as σ_2^*, but with α replaced by $\beta=(n,n-1,\dots,n'+1,1,2,\dots,\nu_1-\mu)$, a cycle of length ν_1.

The cycle β allows the sets $\{1,\dots,n'\}$ and $\{n'+1,\dots,n\}$ to "communicate", so condition (B) above is satisfied by σ_1, σ_2. Also, conditions (C) and (D) hold by construction. Finally, let us count the number of fixed points of $\sigma_1\sigma_2$. Since 1 is not fixed by $\sigma_1^*\sigma_2^*$, every fixed point of $\sigma_1^*\sigma_2^*$ is fixed also by $\sigma_1\sigma_2$. Moreover, the points $n'+1,\dots,n-1$ are also fixed by $\sigma_1\sigma_2$, giving a total of $(n-\mu)-(h-1)-k+1+(\mu-1)=n-h-k+1$ fixed points (at least). So (E$'$) is satisfied.

We shall now deal with the remaining case $n/\delta+1<h+k$. We have seen that δ may be assumed to be 1, so suppose

$$\varrho := h+k-n-1>0. \tag{10}$$

We must prove the existence of polynomials F, G as above, such that $F-G$ is a nonzero constant.

We shall use again Riemann's Existence Theorem, but with four ramified points. We start from a combinatorial construction, simpler to obtain than the previous one. We now seek permutations $\sigma_1,\sigma_2,\sigma_3 \in S_n$ such that

(I) the cycle decomposition of σ_1 is of type $\mu_1,\dots,\mu_h$,
(II) the cycle decomposition of σ_2 is of type $\nu_1,\dots,\nu_k$,
(III) the cycle decomposition of σ_3 consists of precisely $2n+1-h-k$ cycles,
(IV) the σ_i generate a transitive subgroup of S_n.

We first establish the following easy

LEMMA 1. *If* (10) *is true, there exist permutations* σ_1, σ_2 *satisfying* (I), (II) *and generating a subgroup of* S_n *with at most* $h + k - n$ *orbits.*

P r o o f. We argue by induction on n, the statement being true (in fact empty) if $n = 1$. If either σ_1 or σ_2 is the identity the lemma is clear. So assume that both h, k are less than n and that the lemma has been proved up to $n-1$. Since $\varrho > 0$ either some μ_i or some ν_j equals 1. Suppose $\mu_1 = 1$ and $\nu_1 > 1$. By induction there exist σ_1', σ_2' satisfying (I) and (II), but with μ_1 omitted and ν_1 replaced by $\nu_1 - 1$, and generating a subgroup of S_{n-1} with at most $(h-1) + k - (n-1) = h + k - n$ orbits. Define σ_1 just by adding the trivial cycle (n) to the cycle decomposition of σ_1', and σ_2 by inserting n anywhere in a cycle of σ_2' of length $\nu_1 - 1$, and taking unchanged the remaining cycles of σ_2'. It is immediately verified that such permutations work. ∎

Coming back to the requirements (I), (II), (III), (IV), take first σ_1, σ_2 as in the lemma. Let a be the number of orbits of the subgroup they generate, and pick integers $x_1, \dots, x_a$, one from each orbit. Since $a \le h + k - n$, there exist positive integers $l_1, \dots, l_{2n-h-k}$ such that $\sum l_i = n - a$. Define σ_3 as the product of the cycle $(x_1, \dots, x_a)$ with other $2n - h - k$ arbitrary cycles of lengths $l_1, \dots, l_{2n-h-k}$. Plainly also (III) and (IV) are satisfied.

Put now $\sigma_4 := (\sigma_1\sigma_2\sigma_3)^{-1}$, and apply the Ree–Singerman inequality to such four permutations, the assumptions being satisfied, in view of (IV). The total number of cycles is $h + k + (2n - h - k + 1) + x = 2n + 1 + x$, where x is the number of cycles of σ_4. Since that quantity cannot exceed $2n + 2$ we have $x = 1$, so σ_4 is an n-cycle.

By Riemann's Existence Theorem there exists a compact Riemann surface X and a covering $\phi : X \to \mathbb{P}^1$ of degree n, unramified except above $0, 1, \infty, \alpha$ (here α is any complex number different from $0, 1, \infty$) such that the ramification indices above $0, \infty, \alpha, 1$ correspond *respectively* to the cycle lengths of $\sigma_1, \sigma_2, \sigma_3, \sigma_4$. A calculation with the Riemann–Hurwitz formula (or the fact that the Ree–Singerman inequality is in fact an equality) shows that the covering is of genus zero. So ϕ is a rational function of a variable t, of the form $\phi = F/G$, where F, G are polynomials in t with maximum degree equal to n. The ramification indices over 0 are the multiplicities of F and, by the above, the cycle lengths of σ_1, namely the μ_i. So, this condition is satisfied, and the same holds for the multiplicities of the roots of G. Also, the roots (in $\mathbb{P}^1$) of $\phi - 1$ correspond to the cycle lengths of σ_4, namely there is only one such root, which (as before) may be assumed to be $t = \infty$ (i.e. by means of a linear fractional transformation, which leaves the sets of multiplicities unchanged): this means that $t = \infty$ is a root of multiplicity n of $(F - G)/G$, namely $F - G$ is a (nonzero) constant (the proof shows that

we may also require a root of any given multiplicity $\leq h+k-n$ for the polynomial $F-\alpha G$). This proves Theorem 1 completely. ∎

To a certain extent we may find all polynomials in question, in some cases (see also [Za], Thm. 3). Assume for instance that $\delta = 1$, and that $h+k \leq n+1$. Then, as we have seen, if F, G satisfy (6) with equality, then the covering of $\mathbb{P}^1$ by itself given by F/G is ramified possibly only above $0, 1, \infty$. By (iii) of Section 2 two such coverings are isomorphic if and only if they have conjugate descriptions of the branch cycles. Such descriptions are clearly finite in number, whence there exist finitely many couples (F_i, G_i), $i = 1, \ldots, r$, of polynomials as above, such that, if also F, G are as above, then

$$\frac{F(t)}{G(t)} = \frac{F_i(\gamma(t))}{G_i(\gamma(t))} \tag{11}$$

for some i and some transformation $\gamma(t) = (at+b)/(ct+d)$. The fact that ∞ is the only multiple root of both $F/G-1$, F_i/G_i-1, implies that γ must fix ∞, namely we may assume $\gamma(t) = at+b$. In particular, the solutions form a two-parameter family.

The situation is somewhat different when $h+k > n+1$: now we have also α at our disposal. In fact, the condition that the covering must have genus zero amounts to $h+k = n+1+\sum_{i=1}^{s}(n-c_i)$, the sum running over all ramification points, different from $0, 1, \infty$, of the covering given by F/G, the c_i being the number of points in the corresponding fibers. So, if $h+k-n$ is large, we shall have many choices both for the number s and for the ramification points themselves. In our construction we have made the simple choice $s = 1$.

It may also be of some interest (also in connection with the next two sections) to discover when nontrivial automorphisms of the covering exist, and to describe them. Assume again $\delta = 1$ and $n+1 \geq h+k$. Any automorphism is represented by a linear fractional transformation, which must fix ∞ (which is the only ramified point above 1), and so is of the form $\gamma(t) = at+b$. The group of automorphisms is thus cyclic ($\gamma \to a$ is an isomorphism). After a translation we may assume that it is generated by $\gamma(t) = at$. We must have equations

$$F(at) = \lambda F(t), \qquad F(at) - G(at) = \lambda(F(t) - G(t))$$

for some λ. Comparing highest coefficients we get $a^n = \lambda = a^{h+k-1}$. Moreover, the order q of a must divide the degree n. So $\lambda = 1$.

Not both F, G can have the root 0. Assume $F(0) \neq 0$, the other case being symmetrical. The map $\xi \to a\xi$ stabilizes the set of roots of F, preserving also the corresponding multiplicities. Since 0 is not a root, each orbit has order q. In particular $q \mid h$. Also, the sequence of multiplicities may be

partitioned into h/q subsequences, each made of q equal elements. Let μ_i^*, $1 \le i \le h/q$, be the new sequence, so the μ_i are the μ_i^*, each counted q times. If also $G(0) \neq 0$, then $q \mid k$, which is impossible, in view of $q \mid h + k - 1$. So $G(0) = 0$.

The above argument may now be repeated on the roots different from 0. The sum of the respective multiplicities must be divisible by q, so since this holds also for the total sum n, the multiplicity of 0, say ν_k, is a multiple $q\nu^*$ of q. The remaining multiplicities ν_j, $1 \le j \le k-1$, may be partitioned as above into $(k-1)/q$ blocks of q elements, each element equal to ν_j^*, say, $1 \le j \le (k-1)/q$. Both F and G are polynomials in $t^q = u$, say, so, setting $F(t) = F^*(u)$, $G(t) = G^*(u)$ we see that F^*, G^* are a solution for the corresponding problem, but with h/q (resp. $1 + (k-1)/q$) in place of h (resp. k), and the μ_i^* (resp. ν^* and the ν_j^*) in place of the μ_i (resp. the ν_j).

It would be nice if some simple necessary and sufficient condition existed to guarantee, more generally than in Theorem 1, the attainment of bounds given by the *abc*, when the multiplicities of the roots of all $F, G, F - G$ are given. The above result gives the case when $F - G$ has only one multiple root. Again, Riemann's Existence Theorem reduces the general question to a purely combinatorial problem, equivalent to the existence of certain extremal cases of the Ree–Singerman inequality.

5. Davenport's bound. Retaining the notation of the previous section, assume that all μ_i are divisible by 3 and that all the ν_j are even. Then $h \le n/3, k \le n/2$, so $n - h - k + 1 \ge n/6 + 1$. Putting $F = f^3, G = g^2$ we get Davenport's bound. It may be attained only if n is a multiple of 6, and h, k equal respectively $n/3, n/2$, i.e. if $\mu_i = 3, \nu_j = 2$, $\forall i, j$; in particular, neither f nor g can have multiple roots. If these conditions are satisfied, Theorem 1 guarantees the existence of f, g. The considerations of the previous section show that, given $n = 6n'$, the solutions fall into finitely many two-parameter families, as in more general cases.

We now investigate the situation in this case with little more detail. As shown in the previous section, examples amount to finding permutations σ_1, σ_2 such that

(i) σ_1 is a product of $2n'$ disjoint 3-cycles (named v_i),
(ii) σ_2 is a product of $3n'$ disjoint transpositions (named e_j),
(iii) σ_1, σ_2 generate a transitive subgroup Γ of S_n,
(iv) $\sigma_1\sigma_2$ has at least (hence exactly) $n' + 1$ fixed points.

Moreover, two examples belong to the same family if and only if the corresponding couples of permutations are conjugate by a same element of S_n. To investigate conditions (i)–(iv) up to conjugation we construct a graph $\mathcal{G}$ on $2n'$ vertices, corresponding to the 3-cycles of σ_1, joining two

vertices v_i, v_j with an edge precisely when there exists a transposition e_l moving some integer in each of the associated 3-cycles v_i, v_j. Condition (iii) is plainly equivalent to the connectedness of $\mathcal{G}$. Let E be the number of edges. These correspond to E transpositions which contribute no fixed points. The remaining transpositions move two integers which must appear in just one of the v's. Each contributes just one fixed point. So (iv) is equivalent to $3n' - E = n' + 1$, or $E = 2n' - 1$. So the number of edges of $\mathcal{G}$ equals the number of its vertices minus 1, i.e. $\mathcal{G}$ is a tree (see [Har], Ch. 4). (A similar construction is possible also in the more general cases covered by Theorem 1. In this particular case, however, the graph theoretic interpretation is more informative than in general.) Observe that the number of edges from each vertex (its degree) must clearly be either 1 or 3.

It may happen that nonconjugate σ_i's give rise to isomorphic trees. To take this into account, to each vertex v of degree 3 we associate a cyclic permutation $o(v)$ of its neighboring vertices as follows: let v correspond to the 3-cycle (a, b, c). Then the three edges correspond, in some order, to transpositions $(a, x), (b, y), (c, z)$. The neighboring vertices correspond then to 3-cycles containing respectively x, y, z, in some order: denote them by v_x, v_y, v_z. Then $o(v)$ will be the 3-cycle (v_x, v_y, v_z). We shall refer to the couple (tree, map o) as a *weighted tree*. There is clearly a notion of isomorphism of weighted trees. Conversely, given a weighted tree on $2n'$ vertices, each of degree 1 or 3, we may construct permutations σ_i as above. The 3-cycles where some fixed point appears correspond to the vertices of the graph having degree 1. Their number x must satisfy $x + 3(2n' - x) = 4n' - 2$, since the sum of the degrees equals the double of the number of edges, whence $x = n' + 1$, in accordance with (iv).

For instance, consider the case $n = 12$, i.e. $n' = 2$. There is only one weighted tree (up to isomorphism) on 4 vertices, v_1, v_2, v_3, v_4, satisfying the above conditions; its three edges connect v_1, say, with the other vertices, say $o(v_1) = (v_2, v_3, v_4)$ (the other choice leading to an isomorphism). Let the vertices correspond to the 3-cycles of σ_1, $(1, 2, 3)$, $(4, 5, 6)$, $(7, 8, 9)$, $(10, 11, 12)$ resp. The last three permutations must contribute a fixed point. So, among the transpositions of σ_2 we choose, say, $(4, 5), (7, 8), (10, 11)$. The remaining transpositions connect v_1 with the other v_i, and may be taken, say, $(1, 6), (2, 9), (3, 12)$. We have $\sigma_1\sigma_2 = (1, 9, 8, 2, 12, 11, 3, 6, 5)(4)(7)(10)$.

A little inspection will also show that isomorphic weighted trees will lead to conjugate permutations σ_i, whence

PROPOSITION 2. *The number of "essentially distinct" examples of equations* $\deg(f^3 - g^2) = n' + 1$, *where* $\deg f = 2n'$, *equals the number of non-isomorphic weighted trees on* $2n'$ *vertices, such that each vertex has degree* 1 *or* 3.

(For an estimation of the number of such weighted trees see the Appendix.)

Here examples given by $(f, g), (f_*, g_*)$ are considered "essentially equal" if, as in (11) of Section 4, they belong to the same family, i.e.

$$f_*^3(t) = a^{-6n} f^3(at + b), \qquad g_*^2(t) = a^{-6n} g^2(at + b)$$

for some complex numbers a, b.

Let us classify the automorphisms, according to the remarks in the previous section. Their group may be assumed to be generated by $t \to at$. The order q of a must divide 2 or 3.

First case: $a = -1$. Now n' is necessarily odd, f is even while g is odd, namely, setting $u = t^2$, $f(t) = f_1(u)$, $g(t) = tg_1(u)$, our equation becomes

$$f_1^3(u) - ug_1^2(u) := h_1(u), \qquad \deg h_1 = (n' + 1)/2. \tag{12}$$

We have obtained another extremal example of the *abc* theorem, to which our previous methods could also be applied directly. Again, the examples give rise to trees, the vertices being associated with the 3-cycles which, as above, correspond in turn to the roots of f: now the tree is on $n' = \deg f_1$ vertices. Inspection shows that, for $n' > 1$, there is precisely one vertex of degree 2, all other vertices having degree 1 or 3. When this type of automorphism exists, the original graph, associated with the original Davenport's equation, exhibits obviously a spectacular symmetry. "One half" of it (but first omitting one edge) gives the new graph. As before, nonconjugate permutations may lead to isomorphic trees. To take this into account, adjoin to the tree a distinguished vertex v and the edge from v to the vertex of degree 2. We thus obtain again a tree with each vertex of degree 1 or 3, and, as before, we may define a weight on it. The isomorphism class of the weighted tree (which now has a distinguished vertex of degree 1) so defined describes completely the σ_i's up to conjugation.

Second case: $a^2 + a + 1 = 0$. Now $n' \equiv 2 \pmod 3$, whence $f(at) = af(t)$, $g(at) = g(t)$. Setting $u = t^3$ we obtain $f(t) = tf_1(u)$, $g(t) = g_1(u)$. The original assumption becomes

$$uf_1^3(u) - g_1^2(u) = h_1(u), \qquad \deg h_1 = (n' + 1)/3. \tag{13}$$

Even here we have still another extremal example. Again we may construct a graph, now on $(2n' - 1)/3$ vertices, which turns out to have the same properties as the one considered in the first case; namely it is a tree, and, when $n' > 2$, every vertex has degree ≤ 3, and there is precisely one vertex of degree 2. If an automorphism of order 3 exists, then the original graph, when placed properly in the plane, will be invariant under a rotation of $2\pi/3$, and the new graph may be easily deduced from it. As in the first case,

we may add a distinguished vertex and an edge (to the vertex of degree 2), to define a weight.

It is to be remarked that the coverings corresponding to both equations (12) and (13) never have nontrivial automorphisms.

Automorphisms could also be studied via (iv) of Section 2, which states that their group corresponds to the centralizer of Γ in S_n (the proof given by Fried, referred to above, gives an explicit description of this).

Another question is to calculate the monodromy group Γ. We can make the following observation:

Remark 1. *If $5n'-1$ is a prime number then $\Gamma = A_n$.*

In fact, in this case Γ is primitive: the group being transitive, the orders of sets of imprimitivity can be assumed all equal, to c, say. The $5n'-1$-cycle $\sigma_1\sigma_2$ would induce a nontrivial (otherwise $5n'-1 \mid 6n'$) cycle of order dividing $5n'-1$. This implies easily $c=1$. Now a theorem of Jordan (see [Wie], p. 39) implies that Γ equals S_n or A_n. Since, however, both σ_1 and σ_2 are even in this case, we get the statement. We do not know if, in case no automorphisms exist, always Γ is S_n or A_n.

We conclude this section by mentioning another possible approach to an existence proof, directly related to Davenport's proof of the lower bound. We briefly recall how this works. We may clearly assume f, g to be monic. If $\deg(f^3-g^2) \le n'$, then the first $5n'-1$ elementary symmetric functions of the roots of f^3 and of g^2 coincide. Since the form $x_1^s+\ldots+x_k^s$ is, for s a natural number, a polynomial in the first s symmetric functions of the x_i, we would get, letting $\xi_1,\ldots,\xi_{2n'}$, $\eta_1,\ldots,\eta_{3n'}$ be the distinct roots of f and g resp.,

$$3\sum \xi_i^s - 2\sum \eta_j^s = 0, \qquad 0 \le s \le 5n'-1. \tag{14}$$

It is easy to see that this implies that the same equation would hold for all $s \ge 0$, implying $f^3 = g^2$.

The same argument shows that attainment of Davenport's lower bound with $\deg f = 2n'$, amounts to the existence of ξ_i, η_j, $1 \le i \le 2n'$, $1 \le j \le 3n'$, such that, denoting by u_s the left hand side of (14),

$$u_s = 0, \qquad 0 \le s \le 5n'-2, \qquad u_{5n'-1} \ne 0. \tag{15}$$

By the Nullstellensatz such quantities exist if and only if the form $u_{5n'-1}$ is not contained in the radical of the ideal generated by the u_s, $1 \le s \le 5n'-2$. So we have to decide whether some power of a certain form lies in a given ideal. We may formulate the question more generally: given complex numbers $c_1,\ldots,c_m$, put $u_s = c_1x_1^s+\ldots+c_mx_m^s$. Determine then the minimal positive integer q such that u_q lies in the radical of the ideal generated by the u_i for $i<q$. The question seems not obvious in general. Theorem 1 is

equivalent to certain special cases. On the other hand, there seems not to be an analogous formulation of general extremal examples of *abc* (especially in the case of positive genus).

6. A rationality criterion. We come back to the situation of Theorem 1, retaining that notation: we assume μ_i, ν_j are sequences of integers satisfying (3), and consider polynomials F, G of degree n, with roots of multiplicities μ_i, resp. ν_j. Assume for simplicity that $\delta = 1$ and that $n + 1 \geq h + k$. Theorem 1 implies then the existence of such F, G satisfying $\deg(F - G) = n + 1 - h - k$. Moreover, the proof showed that the covering $F/G : \mathbb{P}^1 \to \mathbb{P}^1$ is ramified only above 0, 1, ∞. Recall also that such coverings correspond to permutations σ_1, σ_2, σ_3 satisfying (A)–(E) of Section 4, isomorphic covers corresponding to conjugate (by the same element) permutations. We try to prove the existence of a "small" field containing the coefficients of such F, G.

First we remark that, given such a cover $\phi = F/G$, we may replace it with an isomorphic one, associated moreover with F, G with algebraic coefficients. This is a particular case of Theorem 7.7, p. 70 of [Se1], but may also be proved directly with the following simple continuity argument. The field $\mathcal{L}$ generated by the roots of F, G, which we may assume monic, is a finite extension of $\overline{\mathbb{Q}}(x_1, \ldots, x_d)$, where $\overline{\mathbb{Q}}$ denotes the field of algebraic numbers, and the x_i are complex numbers, algebraically independent over $\overline{\mathbb{Q}}$. Let η be such that $\mathcal{L} = \overline{\mathbb{Q}}(x_1, \ldots, x_d)(\eta)$, and let $H(\eta, x_1, \ldots, x_d) = 0$ be the minimal equation for η over $\overline{\mathbb{Q}}(x_1, \ldots, x_d)$. The roots c_l are of the form $c_l = A_l(\eta, x_1, \ldots, x_d)$, where $A_l \in \overline{\mathbb{Q}}(x_1, \ldots, x_d)[\eta]$. By the continuity of the roots (applied to the polynomial H), for any $\varepsilon > 0$ we can find algebraic numbers $\alpha_1, \ldots, \alpha_d$ and ξ such that $|\alpha_i - x_i| < \varepsilon$, $|\xi - \eta| < \varepsilon$, and $H(\xi, \alpha_1, \ldots, \alpha_d) = 0$. Put $\beta_l = A_l(\xi, \alpha_1, \ldots, \alpha_d)$, the substitution being defined for small ε. Also, we may assume, by taking ε small, that $c_l \neq c_m$ implies $\beta_l \neq \beta_m$. Let F^*, G^* denote the polynomials obtained by replacing the c_l with the β_l. F^*, G^* will still be monic of degree n, and, since all the root-multiplicities and the degree of the difference remain unchanged ($\deg(F^* - G^*)$ could only be lowered, which is impossible), we get another extremal example of *abc*, corresponding to the cover $\phi^* = F^*/G^*$, also unramified except above $0, 1, \infty$. Let $\mathcal{P}$ be some path used to get the description of branch cycles, as in Section 2. If ε is small enough, liftings of $\mathcal{P}$ by ϕ and ϕ^* starting in "near" points will be as near as wanted. In particular, the end points will be near. But then the liftings induce equal permutations (provided "near" points in the fibers above z have been labelled with the same integer), so the same description of branch cycles. It follows that the covers, having also the same ramifications, are isomorphic ((iii) of Section 2).

Let now $\mathcal{T}$ denote the equivalence class (i.e. up to conjugation) of a triple of permutations σ_i, satisfying (A)–(E) of Section 4. Let $\Gamma(\mathcal{T})$ be the equivalence class (up to conjugation) of the group generated by the σ_i in S_n. Sometimes we shall, by abuse of language, denote with the same letters both the group and its equivalence class. Let $\mathcal{T}_1$ be such a triple, and set $\Gamma = \Gamma(\mathcal{T}_1)$. Define

$$S = \{\mathcal{T} : \Gamma(\mathcal{T}) = \Gamma\} = \{\mathcal{T}_1, \dots, \mathcal{T}_D\}, \qquad D = \#S.$$

PROPOSITION 3. *Assume that the centralizer of Γ in S_n is trivial* ([3]). *Then there exist polynomials F, G as above such that the covering defined by F/G has $\mathcal{T}_1$ as a description of the branch cycles, and such that their coefficients lie in a number field K with $[K : \mathbb{Q}] \le D$.*

P r o o f. By the above remark there exist polynomials F, G satisfying the usual conditions, with coefficients in a number field L, say, such that the covering defined by their quotient ϕ has the required description of branch cycles. We may clearly assume L normal over $\mathbb{Q}$. Let Ω be the Galois group. Consider, for $g \in \Omega$, the covering defined by $g\phi = gF/gG$. The polynomials gF, gG have the same sequences of root-multiplicities, and the degree of their difference is also $n-h-k+1$. This covering is also unramified outside 0, 1, ∞. Let $\mathcal{T}$ be its description of the branch cycles. If F, $G \in L[t]$, then the monodromy group Γ is the Galois group of the normal closure of $\mathbb{C}(t)$ over $\mathbb{C}(\phi)$ (see [Tr]). The isomorphism g may be extended to the normal closure of $\mathbb{C}(t)$ over $\mathbb{C}(g\phi)$, proving that $\Gamma(\mathcal{T}) = \Gamma$, so $\mathcal{T} \in S$. Let Δ be the subgroup of Ω formed with those g such that $\mathcal{T} = \mathcal{T}_1$ (it is a subgroup, since the defining condition amounts to an isomorphism of the covers given by ϕ and $g\phi$). Clearly Δ has index $\le D$ in Ω. Let K be the fixed field of Δ.

For $g \in \Delta$ the coverings defined by ϕ and by $g\phi$ are isomorphic, whence, by (11) of Section 4 and the subsequent remarks, there exists a transformation γ_g of the form $\gamma_g(t) = a_g t + b_g$ such that

$$(g\phi) \circ \gamma_g = \phi. \tag{16}$$

Observe that $a_g, b_g \in L$. In fact, if h is any automorphism of $\overline{\mathbb{Q}}$ over L, we have, by (16), $(hg\phi) \circ (h\gamma_g) = h\phi$, whence $(g\phi) \circ (h\gamma_g) = \phi$. Comparing with (16) we see that $(h\gamma_g) \circ \gamma^{-1}$ is an automorphism of the cover, whence the identity, in view of our assumptions. So any such h fixes γ_g, proving our assertion.

Let $g, h \in \Delta$. Apply h to (16), obtaining $(hg\phi) \circ (h\gamma_g) = h\phi$, whence

$$(hg\phi) \circ (h\gamma_g) \circ \gamma_h = h\phi \circ \gamma_h = \phi. \tag{17}$$

([3]) That is, the cover has no nontrivial automorphism.

Writing equation (16) with hg in place of g and comparing with (17) we obtain, in view of the fact that ϕ has no nontrivial automorphisms,

$$\gamma_{hg} = (h\gamma_g) \circ \gamma_h, \tag{18}$$

the familiar cocycle equation.

Let $\Sigma = \{\gamma(t) = at + b : a \in L^*, b \in L\}$. Then Σ is a group under composition and we have an exact sequence

$$\{0\} \to L^+ \to \Sigma \to L^* \to \{1\},$$

commuting with the action of Δ (the second arrow being $b \to t + b$, and the third $at + b \to a$), whence an exact sequence

$$\{0\} = H^1(\Delta, L^+) \to H^1(\Delta, \Sigma) \to H^1(\Delta, L^*) = \{0\}.$$

(Of course also the familiar "Poincaré series" argument would equally do.)

So there exists $\gamma \in \Sigma$ such that

$$\gamma_g = (g\gamma)^{-1} \circ \gamma \quad \forall g \in \Delta.$$

Using this equation in (16) we easily get

$$(g\phi) \circ ((g\gamma)^{-1}) = \phi \circ (\gamma^{-1}) \quad \forall g \in \Delta,$$

i.e. $\phi \circ (\gamma^{-1})$ has coefficients in K. The polynomials $F \circ (\gamma^{-1})$ and $G \circ (\gamma^{-1})$, multiplied by a suitable nonzero constant, clearly solve our problem. ∎

R e m a r k 2. When nontrivial automorphisms (of order q) exist (so Proposition 3 cannot be applied), we have seen in Section 4 that the extremal example "comes" from another one, by setting, after a suitable translation, $F^*(t^q) = F(t)$, $G^*(t^q)$. So the result may be applied to construct first F^*, G^*.

R e m a r k 3. A question which seems of some interest is the following: to find effective estimates for the height of the algebraic coefficients that one can obtain in this way (in terms of the σ_i's, say). It would suffice to do that (together with some estimate for the degree of L) for the original ϕ introduced at the beginning of the proof. Similar, more general, questions could be asked in connection with the realizability of covers of $\overline{\mathbb{Q}}$-varieties over $\overline{\mathbb{Q}}$ (see Thm. 7.7, p. 70 of [Se1]).

R e m a r k 4. Observe that the proof shows that, if $g\phi$ is isomorphic to ϕ for g running in a subgroup Σ of Ω, then ϕ may be found with coefficients in the fixed field. Suppose then that, for $i = 1, 2$, the cover given by ϕ_i (as in the proposition) has coefficients in a number field L_i, and that ϕ_1, ϕ_2 are isomorphic. Let L be the normal closure of $L_1 L_2$. Then $g\phi_1$ is isomorphic to ϕ_1 both when g fixes L_1 and when g fixes L_2. The subgroup generated by such elements has $L_1 \cap L_2$ as fixed field. In other words, there is a minimal field of definition for the coefficients of coverings of the above type.

An obvious corollary of Proposition 3 is that, if $D = 1$ for some Γ as above, the construction may be realized over the rationals. As recalled in the Introduction, this requirement is analogous to part of the so-called rigidity condition for a family of conjugacy classes in a group (see [Se1], Ch. 8). Unfortunately, D is usually large. Take for instance Davenport's case, and assume that $5n' - 1$ is a prime. Then, as observed in Remark 1, every relevant triple of permutations generates the group A_n. So in this case D is the number introduced in Proposition 2, which grows rapidly with n' (see the Appendix). This fact also seems to indicate, in absence of some other, not obvious, reason, that polynomials with rational coefficients realizing Davenport's bound will hardly be found for all large n'. It would be nice to settle this question. (In this connection one may recall that there are, also in low degree, extremal examples of *abc*, not realizable over $\mathbb{Q}$. See [S-V], p. 212, or the examples in [U-Y].)

In any case, when no nontrivial automorphisms exist, D does not exceed the number D' of weighted trees appearing in Proposition 2. It is easy to see that $D' = 1$ for $n' = 1, \dots, 4$, and $D' = 4$ for $n' = 5$. When nontrivial automorphisms exist, we cannot apply directly Proposition 3, but we may follow Remark 2, using the reduction obtained in the previous section, namely looking at equations (12) or (13), instead of at Davenport's. So let D'' be the number of nonisomorphic weighted trees on $m + 1$ vertices, each of degree 1 or 3 and with one distinguished vertex of degree 1. m must be odd. We have $D'' = 1$ for $m = 1, 3$, while $D'' = 2$ for $m = 5$. So equation (12) will be realized over the rationals when $n' = 1, 3$, and equation (13) when $(2n' - 1)/3 = 1, 3$, namely $n' = 2, 5$. Correspondingly, we may realize Davenport's bound over $\mathbb{Q}$ when $n' = 1, \dots, 5$. When $n' = 5$, of the four nonisomorphic cases, one comes from equation (13) (and has rational coefficients), two from equation (12) (they shall be either defined over the rationals or conjugate in a quadratic extension), while the last one will have no nontrivial automorphism. This implies that the corresponding group Γ has trivial centralizer, and so is not isomorphic to the groups corresponding to the other three cases. So, even now the construction will be possible over $\mathbb{Q}$ (but does not appear in the quoted literature), leading to two nonisomorphic examples with rational coefficients when $n' = 5$. This somewhat justifies *a priori* the examples of Hall (pp. 181, 183, 185 of [Ha]). Also, his examples (4.27), (4.28) are isomorphic, namely they belong to the same family, in the sense of (11) of Section 4. When $n' = 7$, equation (12) admits 5 nonisomorphic possibilities: in fact, the corresponding example in [U-Y], p. 225, is defined over a number field of degree 5. When $n' = 11$, the weighted trees corresponding to equation (13) correspond to the ones coming from (12) with $n' = 7$. So, again 5 is a bound for the degree of a field of definition. However, this time the example in [U-Y] has degree only 3. It would be interesting

to carry out further computations to get numerical data to be compared to the above theoretical bounds. The most practical approach, from the computational point of view, seems, as in [U-Y], to look at equation (12) (or (13)). This is in turn equivalent to the fact that $f_1 g_1 + 2ug_1' f_1 - 3ug_1 f_1'$ is a nonzero constant (being equal to $g_1^{-1}(h_1' f_1 - 3h_1 f_1')$).

As remarked, some of the cases covered by Theorem 1 correspond to covers of $\mathbb{P}^1$ unramified outside $0, 1, \infty$. With such covers one may associate what Grothendieck called "dessins d'enfant" (see [Gr] or [S-V]). It may be proved for instance that, permuting suitably $0, 1, \infty$, the *dessin* of a Davenport covering is just the tree introduced in Proposition 2 (but with loops adjoined at the vertices of degree 1); we may also recover the weight $o(v)$ by the orientation of the edges touching v, induced by a prescribed orientation of the Riemann sphere. It would be nice to treat the above questions from such a point of view. G. Jones and D. Singerman ([J-S]) have analyzed the theory using hypermaps, and Professor Jones has observed that such an approach could probably lead to an even simpler proof of Theorem 1.

7. The mod p case. As far as we know no analogue of Riemann's Theorem is known in positive characteristic, and we cannot prove in this case the existence of attained bounds, as in Section 4, for general given multiplicities. However, something can be said about the lifting of examples from positive characteristic. These facts will enable us (especially with the use of a reasonable, though strong, unproved assumption), to derive some new conclusion about the question of rationality. We shall limit ourselves to the lifting of coverings, unramified outside $0, 1, \infty$, described by (a part of) Theorem 1. We shall refer to them as (μ, ν)-coverings.

Let $\mathcal{F}_p$ be an algebraic closure of $\mathbb{F}_p$, K_p be the maximal unramified extension of $\mathbb{Q}_p$, with valuation ring $\mathcal{O}_p$, and algebraic closure $\overline{K}_p$. v will denote the p-adic valuation, extended to $\overline{K}_p$. We shall denote reduction from $\mathcal{O}_p$ to $\mathcal{F}_p$ by $[-]$.

Let $\overline{F}$, $\overline{G}$ be monic polynomials over $\mathcal{F}_p$, of degree n and roots of multiplicities μ_i $(i = 1, \dots, h)$, ν_j $(j = 1, \dots, k)$ resp. We assume that the g.c.d. of all these numbers is 1, and that $n+1 \geq h+k$. It may be shown (following for instance Mason's proof) that the bound of Section 4 for $\deg(\overline{F} - \overline{G})$ remains true, provided $\overline{F}$, $\overline{G}$ are linearly independent over $\mathcal{F}_p(x^p)$ or, equivalently, provided they are coprime. For later reference we recall the argument.

Let $\overline{F} - \overline{G} = \overline{H}$. Put

$$\overline{F}(t) = \prod (t - \overline{\xi}_i)^{\mu_i}, \qquad \overline{G}(t) = \prod (t - \overline{\varrho}_j)^{\nu_j}.$$

Put also (and a similar notation will be adopted throughout)

$$\overline{P}(t) = \prod (t - \overline{\xi}_i), \qquad \overline{P}_i(t) = \frac{\overline{P}(t)}{t - \overline{\xi}_i},$$

$$\overline{Q}(t) = \prod (t - \overline{\varrho}_j), \qquad \overline{Q}_j(t) = \frac{\overline{Q}(t)}{t - \overline{\varrho}_j},$$
$$\overline{F}(t) = \overline{P}(t)\overline{R}(t), \qquad \overline{G}(t) = \overline{Q}(t)\overline{S}(t).$$

Differentiating $\overline{F} - \overline{G} = \overline{H}$ we get $\overline{R}(\sum \mu_i \overline{P}_i) - \overline{S}(\sum \nu_j \overline{Q}_j) = \overline{H}'$. Multiply the first equation by $\sum \nu_j \overline{Q}_j$, the second by $\overline{Q}$ and subtract, getting

$$\overline{R}\Big(\overline{Q}\sum \mu_i \overline{P}_i - \overline{P}\sum \nu_j \overline{Q}_j\Big) = \overline{H}'\overline{Q} - \overline{H}\Big(\sum \nu_j \overline{Q}_j\Big).$$

The common value of the two sides divides the Wrońskian of $\overline{F}$ and $\overline{G}$, so, by our assumption, it cannot be zero. Being divisible by $\overline{R}$, its degree is at least $n - h$, and we get the desired lower bound for $\overline{H}$.

Assume now that the lower bound is attained, so we have an extremal example mod p. From the above we see, moreover, that

$$\overline{Q}\sum \mu_i \overline{P}_i - \overline{P}\sum \nu_j \overline{Q}_j = c \tag{19}$$

is a nonzero constant. In particular, $\overline{P}$ and $\overline{Q}$ are coprime and have no multiple root. Also, observe that this prevents p to divide $(h+k-1)\prod \mu_i \prod \nu_j$, namely the product of the various ramification indices of the associated covering ([4]); in other words, the ramification of the function fields extension is tame.

We shall show that we may lift to K_p, namely find $\xi_i, \varrho_j \in K_p[t]$ such that $[\xi_i] = \overline{\xi}_i$, $[\varrho_j] = \overline{\varrho}_j$, and such that, defining F, G in the obvious way, $\deg(F - G) = n - h - k + 1$, i.e. we shall lift the covering to another one with the same ramification type.

As remarked by M. Fried in [Fr1], p. 45, the existence of such liftings was shown to be possible for general coverings by W. Fulton in his thesis [Fu], with proofs which "*rely heavily on the work of Grothendieck...*". In the same paper Fried asks for simpler proofs, valid at least in certain special cases. In fact in our case an elementary and direct method suffices (a simple version of Hensel's principle in fact). It is quite possible that this may be fairly generalized: the construction of unramified coverings as those considered in the present paper amounts (if one forgets the monodromy, but only takes into account the conditions on the ramification indices) to finding a point in a certain Zariski open subset of an algebraic set (in our case defined on equating the first $h + k - 1$ coefficients of F, G, as polynomials in the indeterminate roots of F and G, the open subset being given by $(F, G) = 1$, namely the resultant of F, G must be nonzero). If the point is nonsingular, then Hensel's principle is applicable and a lifting may be found. This is the

([4]) If $p \mid \mu_1$, say, then evaluating at ξ_1 gives a contradiction. Also, comparing leading coefficients in the previous equation we get easily $c = -l(h+k-1)$, where l is the leading coefficient of $\overline{H}$.

principle of the present method. However, we shall work directly with the involved polynomials instead of the associated algebraic set. (This seems to extend with few modifications to the lifting of general covers of genus zero.)

By a similar direct method we shall also show that the isomorphism class of the lifting depends only on the class of its reduction. We begin with the following

LEMMA 2. *Let V_m denote the space of polynomials of degree $\le m$ over $\mathcal{F}_p$, and let $\overline{F}$, $\overline{G}$ be as above. Define $\phi : \mathcal{F}_p^h \times \mathcal{F}_p^k \times V_{n-h-k} \to V_{n-1}$ by*

$$\phi(\delta_i, \eta_j, \gamma) = \overline{R}\Big(\sum \delta_i \mu_i \overline{P}_i\Big) - \overline{S}\Big(\sum \eta_j \nu_j \overline{Q}_j\Big) - \gamma(t).$$

Then the kernel of ϕ is one-dimensional, generated by $(1, \dots, 1, \dots, \overline{H}')$.

P r o o f. Let δ_i, η_j, γ lie in the kernel. Then $\overline{R}(\sum \delta_i \mu_i \overline{P}_i) - \overline{S}(\sum \eta_j \nu_j \overline{Q}_j) = \gamma$. Multiplying by $\overline{Q}$ and using the equation $\overline{S}\,\overline{Q} = \overline{R}\,\overline{P} - \overline{H}$ to substitute for $\overline{S}\,\overline{Q}$ we get $\overline{R}(\overline{Q}\sum \delta_i \mu_i \overline{P}_i - \overline{P}\sum \eta_j \nu_j \overline{Q}_j) = \overline{Q}\gamma - \overline{H}\sum \eta_j \nu_j \overline{Q}_j$. The right hand side has degree $\le n - h$ and is divisible by $\overline{R}$, whence $\overline{Q}\sum \delta_i \mu_i \overline{P}_i - \overline{P}\sum \eta_j \nu_j \overline{Q}_j$ is a constant, c' say. Multiply (19) by c'/c and subtract. We get $\overline{Q}(\sum(\delta_i - (c'/c))\mu_i \overline{P}_i) = \overline{P}(\sum(\eta_j - (c'/c))\nu_j \overline{Q}_j)$. So $\sum(\delta_i - (c'/c))\mu_i \overline{P}_i$ is a multiple of $\overline{P}$, whence must be zero. Evaluating at $\overline{\xi}_i$ we get $\delta_i = (c'/c)$ for all i. Similarly $\eta_j = (c'/c)$ for all j, and the lemma follows. ∎

We now prove the existence of a lifting. Assume we have found, for a certain $m \ge 1$, elements of $\mathcal{O}_p$, $\xi_i^{(m)}$, $\varrho_j^{(m)}$ with $\bmod p$ reductions $\overline{\xi}_i$, $\overline{\varrho}_j$ resp., and a polynomial H_m over $\mathcal{O}_p$ of degree $n - h - k + 1$ such that, defining F_m, G_m in an obvious way, we have $F_m - G_m = H_m + p^m r_m$ for some polynomial r_m (of degree $\le n - 1$), also with coefficients in $\mathcal{O}_p$. We seek $\xi_i^{(m+1)}$, $\varrho_j^{(m+1)}$ in the form

$$\xi_i^{(m+1)} = \xi_i^{(m)} - p^m \delta_i, \qquad \varrho_j^{(m+1)} = \varrho_j^{(m)} - p^m \eta_j \tag{20}$$

with undetermined $\delta_i, \eta_j \in \mathcal{O}_p$. We get, with an obvious notation,

$$F_{m+1} - G_{m+1}$$
$$\equiv H_m + p^m\Big(R_m\Big(\sum \delta_i \mu_i P_{i,m}\Big) - S_m\Big(\sum \eta_j \nu_j Q_{j,m}\Big) + r_m\Big) \pmod{p^{m+1}}.$$

By counting dimensions, Lemma 2 implies that the map ϕ is surjective, so there exist $\delta_i, \eta_j \in \mathcal{O}_p$ and a polynomial $\gamma \in \mathcal{O}_p[t]$ such that $R_m(\sum \delta_i \mu_i P_{i,m}) - S_m(\sum \eta_j \nu_j Q_{j,m}) - \gamma \equiv -r_m \pmod p$, where γ has degree $\le n-h-k$. Defining $H_{m+1} = H_m + p^m \gamma$ we have realized the same construction for $m+1$ in place of m, where moreover (20) and $H_{m+1} \equiv H_m \pmod{p^m}$ hold. Since the construction is clearly possible for $m = 1$, it is possible for all m. Setting $\xi_i = \lim \xi_i^{(m)}$, and similarly for η_j, H, where the last limit is taken coefficientwise in the p-adic convergence, gives the required lifting.

We now show that the isomorphism class of the lifting depends only on the isomorphism class of its reduction. It will suffice to prove that two liftings with the same reduction are isomorphic. Let, for $i = 1, 2$, $r_i := F_i/G_i$ be such liftings, where F_i, G_i are monic polynomials with roots in $\mathcal{O}_p$. Put $H_i = F_i - G_i$. Let λ_i be the leading coefficient of H_i, and set $\omega = \lambda_1/\lambda_2$. We have $\omega \equiv 1 \pmod p$. Since p does not divide $h + k - 1$ the equation $x^{h+k-1} = \omega$ has its roots in K_p. Let λ be one such root which is congruent to 1 (mod p). Put $\widetilde{F}_1(t) = \lambda^{-n} F_1(\lambda t)$, $\widetilde{G}_1(t) = \lambda^{-n} G_1(\lambda t)$. We have $\widetilde{H}_1(t) = \lambda^{-n} H_1(\lambda t)$, and so the leading coefficient of $\widetilde{H}_1$ equals the leading coefficient of H_2. Since $\lambda \equiv 1 \pmod p$ the reduction is preserved, and clearly also the isomorphism class. So we may assume from the beginning that H_1, H_2 have equal leading coefficients.

Drop the subscript 2, and put $F(t) = \prod (t - \xi_i)^{\mu_i}$ and similarly for G.

We construct by induction on m linear polynomials $\alpha_m(t) = t + a_m$ such that $F_1 \circ \alpha_m = \prod (t - \xi_i + p^m \delta_i)^{\mu_i}$, $G_1 \circ \alpha_m \equiv \prod (t - \xi_i + p^m \delta_i)^{\mu_i}$, where δ_i and η_j lie in $\mathcal{O}_p$, and such that $a_{m+1} \equiv a_m \pmod{p^m}$. Defining $a = \lim a_m$, $\alpha(t) = t + a$, we shall have $r_1 \circ \alpha = r_2$, as required.

For $m = 1$ we just take $a_1 = 0$. Assume a_m constructed. Replacing F_1 (resp. G_1) by $F_1 \circ \alpha_m^{-1}$ (resp. $G_1 \circ \alpha_m^{-1}$), we may assume

$$F_1 = \prod (t - \xi_i + p^m \delta_i)^{\mu_i}, \qquad G_1 = \prod (t - \xi_i + p^m \delta_i)^{\mu_i}.$$

We get

$$H_1 \equiv H_2 + p^m \Big(R\Big(\sum \delta_i \mu_i P_i \Big) - S\Big(\sum \eta_j \nu_j Q_j \Big) \Big) \pmod{p^{m+1}}.$$

The H_i having equal leading coefficients, the polynomial $R(\sum \delta_i \mu_i P_i) - S(\sum \eta_j \nu_j Q_j)$ has a reduction (mod p) of degree $\le n - h - k$, whence, by Lemma 2, $\delta_i = b + p\delta_i'$, $\eta_j = b + p\eta_j'$, for some $b, \delta_i', \eta_j' \in \mathcal{O}_p$. This means that $F_1(t) = \prod (t + p^m b - \xi_i + p^{m+1} \delta_i')^{\mu_i}$, and similarly for G_1. This completes the proof. ∎

Remark 5. The same arguments work if we start with any algebraically closed field k of characteristic p, instead of $\mathcal{F}_p$, and consider liftings to $W(k)$, the *Witt vector ring* introduced by Theorem 3, p. 45 of [Se2].

Let $s(t) = F/G$, where $F, G \in K_p[t]$ are monic, be a covering as above. We say it has *good reduction* (mod p) if $F, G \in \mathcal{O}_p[t]$, and if moreover $[s] \notin \mathcal{F}_p(t^p)$ (or, equivalently, if the reduced covering has the same degree). We have the following

Lemma 3. *For $i = 1, 2$, let s_i be coverings as above, with good reduction, and such that $s_1(t) = s_2(at + b)$, for some a, b in $\overline{K}_p$. Then a is a unit in $\mathcal{O}_p$, while $v(b) \ge 0$.*

P r o o f. We have, with an obvious notation,

$$a^n F_1(t) = F_2(at+b), \qquad a^n G_1(t) = G_2(at+b).$$

Replacing if necessary s_1 with s_2, and the transformation $t \to at+b$ with its inverse, we may assume $v(a) \geq 0$. If $v(b) < 0$ then, since F_2 is monic and lies in $\mathcal{O}_p[t]$, we have $v(F_2(b)) = nv(b) < 0$, contradicting the first equation. So $v(b) \geq 0$. Now, if $v(a) > 0$, reduction of the above equations would give $[F_2]([b]) = [G_2]([b]) = 0$, which is impossible since, in view of the fact that s_2 has good reduction, $[F_2]$ and $[G_2]$ have no common root. ∎

The lemma shows in particular that coverings in the same isomorphism class, both with good reduction, have in fact isomorphic reductions. In view of this and the above results we may state the following

PROPOSITION 4. *There is a* 1-1 *correspondence between the isomorphism classes of (μ, ν)-coverings of degree n over $\mathcal{F}_p$ and the isomorphism classes of the same coverings over K_p, such that some representative of the class has good reduction.*

Since every finitely generated field of characteristic zero can be embedded in $\mathbb{C}$, this shows in particular that there cannot be more isomorphism classes over $\mathcal{F}_p$ than the number of classes over the complex numbers (given by Proposition 2 in combinatorial terms, for Davenport's coverings).

R e m a r k 6. Given a (μ, ν)-covering s over K_p, with good reduction, we may find an isomorphic one, also over K_p and with good reduction, where moreover the coefficients are algebraic numbers. This may be proved for instance by the same continuity argument given before Proposition 3, Section 5. The only modification required consists first in imbedding the field generated by the coefficients of s in $\mathbb{C}$, and then in choosing the algebraic numbers α_i, ξ (appearing in that argument) sufficiently near to the x_i and η, even with respect to the p-adic absolute value, which is certainly possible by the weak approximation theorem. The covering so defined will have all the required properties.

We shall assume from now on that the automorphism group of the coverings considered is trivial. The discussion of automorphisms and Remark 3 above allow us to reduce the general case to this one.

Let now r be a (μ, ν)-covering of degree n, with coefficients in a number field L. We let $\mathcal{P}$ be a prime ideal of L above p and unramified above it, and imbed L in its completion $L_{\mathcal{P}}$ at $\mathcal{P}$, which is a subfield of K_p. Assume there is a covering s, in the same class of r, defined over K_p ([5]) and having

([5]) Throughout the paper by a *cover defined over a field L* we mean that there exists a rational function in $L(t)$ defining a cover isomorphic to the given one. This is not always quite equivalent with the usual definition, as given in [Fr2].

good reduction. Let $s(t) = r(\alpha(t))$, where $\alpha(t) = at + b$, with a, b algebraic over K_p. Since our coverings have only the trivial automorphism we see that α must be invariant under automorphisms of $K_p(a, b)$ over K_p, whence actually $a, b \in K_p$.

From Lemma 3 we see that, if s_1, $\alpha_1 : t \to a_1 t + b_1$ have the same properties, then $v(a_1) = v(a)$ and $v(b - b_1) \geq v(a)$, and, conversely, if a_1, b_1 have these properties, then $r \circ \alpha_1$ too has good reduction.

Let $\sigma \in \mathrm{Gal}(K_p | L_{\mathcal{P}})$. Then $\sigma s = r(\sigma\alpha)$ has good reduction, whence, in particular, $v(b - \sigma b) \geq v(a) = e$, say. Let $x = b/p^e$. Then

$$\sigma x - x \in \mathcal{O}_p \quad \forall \sigma. \tag{21}$$

Lemma 4. *Under* (21) *there exists an algebraic integer* $y \in L$ *and an integer* c *such that* $x - y/p^c \in \mathcal{O}_p$.

Proof. We may assume $v(x) < 0$ (otherwise $y = 0$ does). We argue by induction on $-v(x)$. Let $c = -v(x) > 0$, and set $x' = p^c x \in \mathcal{O}_p$, $\xi = [x]$. The assumption gives $x' - \sigma x' \in p\mathcal{O}_p$, whence $\xi = \sigma\xi$. So ξ lies in the residue field of $L_{\mathcal{P}}$, whence, for some algebraic integer y_0 in L, $x' \equiv y_0 \pmod{p}$. So $-v(x - y_0/p^c) \leq c - 1$. Since $x - y_0/p^c$ satisfies the same assumption, the proof is finished by induction. ∎

The lemma shows that, replacing a with p^e, b with yp^{e-c}, in fact we may take $a, b \in L$, so there is some covering defined over L, with good reduction at $\mathcal{P}$.

For a (μ, ν)-covering defined over L, let Φ be the set of prime ideals of L such that

(i) If $\mathcal{P} \in \Phi$ then $\mathcal{P}$ is unramified over $\mathbb{Q}$.

(ii) Embedding L in K_p through the completion at $\mathcal{P}$, there exists a covering over K_p in the same class of r and having good reduction at p.

Observe that Φ contains all but a finite number of prime ideals.

This set depends of course on the class of the covering and on L. We could make it independent of L by choosing it as the smallest field of definition (see Remark 4).

Proposition 5. *Let* r *be a* (μ, ν)*-covering defined over* L, *and let* $\mathcal{P} \in \Phi$. *Then* $\mathcal{P}$ *is unramified in the extension of* L *generated by the poles and zeros of* r.

Proof. By replacing r with an isomorphic covering defined over L, we may assume that it has good reduction at $\mathcal{P}$. Writing $r = F/G$ for monic F, G we have seen that the distinct roots of F, G must have distinct reductions for the reduced covering to be still of degree n. Then the inertia group is trivial, proving what we want. ∎

We now would like to find a covering in the same class as r and having good reduction simultaneously at as many primes as possible, and still defined over L. Let, for $\mathcal{P} \in \Phi$, $r(a_{\mathcal{P}}t + b_{\mathcal{P}})$ have good reduction at $\mathcal{P}$, where $a_{\mathcal{P}}, b_{\mathcal{P}} \in L$. Let $e_{\mathcal{P}} = v_{\mathcal{P}}(a_{\mathcal{P}})$, an integer depending only on $\mathcal{P}$ and r. We remark that, since r itself has good reduction at all but finitely many primes, we may take $e_{\mathcal{P}} = b_{\mathcal{P}} = 0$ for all but finitely many primes. Let $a, b \in L$. In order for $r(at+b)$ to have good reduction at $\mathcal{P}$ it is necessary and sufficient that

(i) $v_{\mathcal{P}}(a) = e_{\mathcal{P}}$, and
(ii) $v(b - b_{\mathcal{P}}) \geq e_{\mathcal{P}}$.

If we wanted such conditions to hold for *all* primes in Φ, the ideal class of $I(\Phi) := \prod_{\mathcal{P}\in\Phi} \mathcal{P}^{e_{\mathcal{P}}}$ would be equal to an ideal class generated by ideals outside Φ. Conversely, this is a sufficient condition for the existence of a, b such that (i) and (ii) hold for all primes in Φ. In fact, once a has been found satisfying (i), we may find b satisfying (ii) by the Strong Approximation Theorem (see [Ca-Fr], p. 67); in fact, there are primes outside Φ (for instance those dividing some ramification index of the covering), so we may forget what happens at that prime.

Let $\mathcal{G} = \mathcal{G}(L)$ be the ideal class group of L, and $\mathcal{G}_\Phi$ the subgroup generated by prime ideals *not* in Φ. It is natural to define $\mathcal{C} \in \mathcal{G}/\mathcal{G}_\Phi$ as the image of the class of $I(\Phi)$ in the quotient group. We can find simultaneous good reduction if and only if $\mathcal{C}$ is trivial. More generally, we can find simultaneous good reduction at all primes in a set $S \subset \Phi$ if and only if $\mathcal{C}$ becomes trivial in $\mathcal{G}/\mathcal{G}_S$.

If L' is a finite extension of L, unramified above Φ, then it is at once verified that the invariants so far defined, namely Φ, $e_{\mathcal{P}}$, $I(\Phi)$, $\mathcal{C}$, are compatible with the embedding $L \subset L'$, in the sense that Φ' consists of the primes of L' above some prime in Φ, that, for $\mathcal{Q}|\mathcal{P}$, $e_{\mathcal{Q}} = e_{\mathcal{P}}$, and $\mathcal{C}'$ is obtained by taking the injection

$$\frac{\mathcal{G}(L)}{\mathcal{G}_\Phi(L)} \to \frac{\mathcal{G}(L')}{\mathcal{G}_{\Phi'}(L')}.$$

As a consequence of these remarks we obtain

PROPOSITION 6. *There exists a covering in the same class of r, and having good reduction at all primes above Φ, defined over the Hilbert class field L^* of L.*

The proof follows at once, by recalling that L^* is unramified over L, and moreover each ideal of L becomes principal in L^*.

We may improve sometimes on Proposition 5. Let r have coefficients in L and good reduction at primes above $S \subset \Phi$. Since the covering is unramified outside $0, 1, \infty$, the discriminant of the polynomial $P(t, \lambda) := F(t) - \lambda G(t)$ with respect to t is of the form $c\lambda^a(1 - \lambda)^b$. Take, say, $\lambda \notin \{0, 1\}$. The reduction of P (mod $\mathcal{P}$) cannot have double roots (since the reduction too

is unramified outside $0, 1, \infty$), so c can have nonzero order only at primes not lying above S. This of course bounds the primes dividing the discriminant for all given λ. We can see this as a refinement (in our quite particular situation) of the affine Chevalley–Weil Theorem, which, in our case, simply states that primes which ramify in the field generated by the roots of $P(t, \lambda_0)$ divide $c'\lambda_0(1-\lambda_0)$ for *some* fixed c'.

So, if we can prove that the (μ, ν)-covering may be realized over $\mathcal{F}_p$ in as many isomorphic ways as over $\overline{\mathbb{Q}}$, for many primes p, we shall obtain arithmetical information about the ramification introduced by poles and zeros of r. Take for instance the coverings described in Section 5, first case, which lead to attained Davenport's bounds. It seems reasonable that primes $p \geq 5$ should not impose any particular restriction on the existence of as many isomorphism classes as those possible over $\overline{\mathbb{Q}}$. A consequence would be for instance that r could not have 6 distinct rational roots (or poles) (otherwise two of them would be congruent mod 5). Also, the prime factors of the discriminants of the involved polynomials would divide $6(5n'-1)$.

These considerations put further restrictions on the realizability of examples over the rationals, and perhaps in some cases could be used to bound from below the degree of the minimal field of definition.

Some caution is, however, necessary in assuming the existence of (many) examples mod p. Take for instance $n = 4$ and $(3, 1)$ as sequence of ramification indices above all of $0, 1, \infty$ (with monodromy given for instance by the permutations $(1, 2, 3), (2, 1, 4), (4, 3, 2)$). Now, although 2 does not divide the indices, no such covering is possible over $\mathcal{F}_2$; or take $(1, 1, 6)$ to be the sequence of both μ, ν, so $n = 8$, $h = k = 3$. Now the construction is easily seen to be impossible in characteristic 7. We give the simple argument, also because it may be fairly generalized in an obvious way. If the construction is possible, we may write

$$q_1 l_1^6 - q_2 l_2^6 = h,$$

where the q_i are quadratic monic polynomials, the l_i are linear, and monic, and h has exact degree 3. Multiplying the equation by $l_1 l_2$ we see that the polynomial $q_1(t)l_2(t)l_1(0)^7 - q_2(t)l_1(t)l_2(0)^7 - h(t)l_1(t)l_2(t)$ is divisible by t^7, whence it must vanish, since each term has degree at most 5. This, however, contradicts the fact that the q_i, l_j are pairwise coprime.

The obvious generalization of this argument leads, however, to inelegant necessary conditions on the ramifications indices. In fact, I do not have, nor know about, any simple general conjecture about a necessary and sufficient condition to guarantee that examples exist mod p. (Perhaps a sufficient condition is that p divides neither the ramification indices nor the order of the monodromy group.)

Appendix. As announced I give an estimate, found together with Professor R. Dvornicich, for the number D' of weighted trees in the statement of Proposition 2. No doubt it is not new. However, we were not able to find a reference. So, for the sake of completeness we give a (very sketchy) argument.

It will be convenient to count first the number F_n of rooted weighted trees (up to isomorphism) on $2n$ vertices of degrees 1 or 3, and the root of degree 1. (We recall that a *rooted tree* is a tree with a distinguished vertex, its *root*.) Let v be the vertex joined to the root. In an obvious way the root *originates* (after one edge) two new weighted trees (both having v as root), again with each vertex of degree 1 or 3. We may consider such a new couple of trees to be an *ordered* couple, corresponding to the cycle attached to v. The following recurrence formula is then easy to prove: for $n \geq 2$, we have

$$F_n = \sum_{i+j=n} F_i F_j.$$

Also, we have clearly $F_0 = 0$, $F_1 = 1$. These facts at once imply the following identity for the generating function $F(x) = \sum F_n x^n$:

$$F(x) = x + F^2(x),$$

which gives

$$F(x) = \frac{1}{2}(1 - \sqrt{1 - 4x}),$$

whence we find the "Catalan" numbers

$$F_n = (-1)^{n-1}\frac{1}{2}4^n\binom{1/2}{n} = \frac{\binom{2n}{n}}{2(2n-1)} \sim cn^{-3/2}4^n,$$

for a certain nonzero constant c.

Now, some nonisomorphic rooted weighted trees may become isomorphic as (non-rooted) weighted trees, but this accounts for a factor at most $2n$. In conclusion, we have

$$n^{-5/2}4^n \ll D' \ll n^{-3/2}4^n.$$

Added in proof (February 1995)**.** Recently the volume *The Grothendieck Theory of Dessins d'Enfants*, edited by L. Schneps, London Math. Soc. Lecture Note Ser. 200, Cambridge Univ. Press, 1994, has appeared. This contains many results connected with the topic of the present paper, and very detailed constructions connected with Riemann's Existence Theorem (see e.g. the first paper by Leila Schneps). In particular, I have learned from the paper of Birch that the conjecture appearing before the present Appendix (concerning the primes dividing neither the ramification indices nor the order of the monodromy group) had in fact been proved by W. Fulton and later by S. Beckmann (*Ramified primes in the field of moduli of ramified coverings of curves*, J. Algebra 125 (1989), 236–255), using different techniques. Still, to my knowledge no criterion is known for dealing with all primes not dividing the ramification indices.

References

[BCHS] B. J. Birch, S. Chowla, M. Hall, Jr., and A. Schinzel, *On the difference* $x^3 - y^2$, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 65–69.

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

[Ca-Fr] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

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

[CMK] M. Conder and J. McKay, *A necessary condition for transitivity of a finite permutation group*, Bull. London Math. Soc. 20 (1988), 235–238.

[Dan] L. Danilov, *Letter to the editor*, Mat. Zametki 36 (1971), 103–107 (in Russian).

[Dav] H. Davenport, *On* $f^3(t) - g^2(t)$, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 86–87.

[FLS] W. Feit, R. Lyndon and L. L. Scott, *A remark about permutations*, J. Combin. Theory Ser. A 18 (1975), 234–235.

[Fr1] M. Fried, *On a conjecture of Schur*, Michigan Math. J. 17 (1970), 41–55.

[Fr2] —, *Fields of definition of function fields and Hurwitz families—Groups as Galois groups*, Comm. Algebra 5 (1977), 17–82.

[Fu] W. Fulton, *The fundamental group of a curve*, Archives of the Princeton Mathematical Library, 1966.

[Gr] A. Grothendieck, *Esquisse d'un programme*, preprint, 1984.

[Ha] M. Hall, Jr., *The Diophantine equation* $x^3 - y^2 = k$, in: Computers in Number Theory, A. O. L. Atkin and B. J. Birch (eds.), Proc. Oxford 1969, Academic Press, 1971, 173–198.

[Har] F. Harary, *Graph Theory*, 3rd ed., Addison Wesley, 1972.

[J-S] G. Jones and D. Singerman, *Maps, hypermaps and triangle groups*, preprint Univ. of Southampton, July 1993.

[Lang] S. Lang, *Number Theory III*, Encyclopaedia Math. Sci. 60, Springer, 1991.

[La] M. Langevin, *Cas d'égalité pour le Théorème de Mason et applications de la conjecture* (*abc*), C. R. Acad. Sci. Paris 317 (1993), 441–444.

[Ma] R. C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge Univ. Press, 1984.

[Ree] R. Ree, *A theorem on permutations*, J. Combin. Theory Ser. A 10 (1971), 174–175.

[Se1] J. P. Serre, *Topics in Galois Theory*, Course at Harvard University, Fall 1988 (Notes by H. Darmon).

[Se2] —, *Corps locaux*, Hermann, Paris, 1968.

[S-V] G. B. Shabat and V. A. Voevodsky, *Drawing curves over number fields*, in: The Grothendieck Festschrift, vol. III, Progr. Math. 88, Birkhäuser, 1990, 199–227.

[Sie] W. Sierpiński, *Elementary Theory of Numbers*, edited by A. Schinzel, 2nd ed., North-Holland, 1988.

[Sin] D. Singerman, *Subgroups of Fuchsian groups and finite permutation groups*, Bull. London Math. Soc. 2 (1970), 319–323.

[Tr] M. Tretkoff, *Algebraic extensions of the field of rational functions*, Comm. Pure Appl. Math. 24 (1971), 491–497.

[U-Y] S. Uchiyama and M. Yorinaga, *On the difference* $f^3(x) - g^2(x)$, Tsukuba J. Math. 6 (1982), 215–230.

[Vo] P. Vojta, *Diophantine Approximation and Value Distribution Theory*, Lecture Notes in Math. 1239, Springer, 1987.

[Wie] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

[Za] U. Zannier, *Some remarks on the S-unit equation in function fields*, Acta Arith. 64 (1993), 87–98.

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

Received on 13.9.1993
and in revised form on 14.9.1994 (2487)