PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 115, Number 4, AUGUST 1992

THE AUTOMORPHISM GROUP OF A FUNCTION FIELD

MANOHAR MADAN AND MICHAEL ROSEN

(Communicated by William Adams)

ABSTRACT. Let k be an algebraically closed field, K a function field in one variable over k, and G a nontrivial finite group. It is proven that there exist infinitely many Galois extensions L/K such that $\mathrm{Gal}(L/K)$ is isomorphic to G, and $\mathrm{Gal}(L/K) = \mathrm{Aut}_k(L)$. This extends to arbitrary characteristic, a result first proven in the case $k = \mathbb{C}$ by Greenberg in 1974.

INTRODUCTION

In 1974, Greenberg published a result which showed that every finite group occurs as the automorphism group of a compact Riemann surface [Gr]. In fact, his result is more precise.

Theorem (L. Greenberg). *Let K be a function field in one variable over $\mathbb{C}$, and G a nontrivial finite group. Then there exists a Galois extension L/K such that $\mathrm{Gal}(L/K)$ is isomorphic to G, and $\mathrm{Gal}(L/K) = \mathrm{Aut}_{\mathbb{C}}(L)$, the full automorphism group of L over $\mathbb{C}$.*

Greenberg uses analytic methods, but it makes sense to ask if the theorem remains true when $\mathbb{C}$ is replaced by an arbitrary algebraically closed field k. If G is assumed to be abelian, and $K = k(T)$, this was shown by Valentini and Madan [Va-Mad]. This was generalized by D'Mello and Madan to the case of solvable groups [D'M-Mad]. Subsequently, Madden and Valentini showed every finite group G occurs as the full automorphism group of a function field L/k, but without controlling the genus of the fixed field of G [Madd-Va]. In 1984, Stichtenoth showed the full strength of Greenberg's theorem was valid over any algebraically closed field if one makes the additional assumption that the genus of K is at least two [St2]. It is the purpose of this paper to show that this restriction is not necessary. Namely, we will prove

Theorem. *Let K be a function field in one variable over an algebraically closed constant field k, and let G be a nontrivial finite group. There exist infinitely many Galois extensions L/K such that $\mathrm{Gal}(L/K)$ is isomorphic to G, and $\mathrm{Gal}(L/K) = \mathrm{Aut}_k(L)$.*

Received by the editors November 8, 1990 and, in revised form, January 17, 1991.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14H99.
The second author was partially supported by a grant from the National Science Foundation.

0002-9939/92 $1.00 + $.25 per page

In order to prove this completely general result, we will use tools developed by these earlier authors, and, when the characteristic of k is positive, make crucial use of some results of Harbater on mock covers of curves. Our proof itself, however, is new and somewhat simpler than the proofs of these earlier results, even in the case $k = \mathbb{C}$.

1. Preparatory results

In this section we assemble some of the tools we will need for our proof. Throughout the rest of the paper, k will denote an algebraically closed field, and function field will mean a function field in one variable over k. If K is such a function field, g_K will denote its genus. The following version of the Castelnuovo-Severi inequality, and its corollary, comes from [St1, Madd-Va].

Proposition 1. *Let L be a function field, and E and F be two subfields of finite index. If $L = EF$, then*

$$g_L \leq [L: E]g_E + [L: F]g_F + ([L: E] - 1)([L: F] - 1).$$

Corollary. *Let L/K be an extension of function fields. Suppose that for every intermediate extension $K \subset M \subset L$, with $M \neq K$, $g_M > [M: K]^2 + 2[M: K](g_K - 1) + 1$. Then, for every $\sigma \in \mathrm{Aut}_k(L)$, we have $\sigma(K) = K$.*

Proof of Corollary. If $\sigma \in \mathrm{Aut}_k(L)$ is such that $\sigma(K) \neq K$, let M be the compositum of K and $\sigma(K)$. Applying the proposition to M and its two subfields K and $\sigma(K)$ shows $g_M \leq [M: K]^2 + 2[M: K](g_K - 1) + 1$, which contradicts the hypothesis.

We will later use the corollary in the following way. We will construct an extension L/K such that every intermediate extension is ramified at many primes. By the Riemann-Hurwitz genus formula, the genus of all intermediate fields will be large. Using the corollary, this shows that every automorphism of L induces an automorphism of K. We will then rigidify the situation so that every such automorphism of K must be the identity. To achieve this rigidification the following proposition will be of use. It is a small generalization of a result in [Va-Mad].

Proposition 2. *Let K be a function field of genus g, and $T = \{P_1, P_2, \ldots, P_t\}$ a set of primes of K with $t > 2g + 3$. Then, for all but finitely many primes Q, the set $T' = T \cup \{Q\}$ has the property that the identity is the only element of $\mathrm{Aut}_k(K)$ which maps T' into itself.*

Proof. According to Satz 9 of [Sch], a nontrivial automorphism of K has at most $2g + 2$ fixed points. It follows that an automorphism is determined by its action on $2g + 3$ primes.

Define $\Gamma = \{\sigma \in \mathrm{Aut}_k(K) \mid |\sigma T \cap T| \geq t - 1\}$. Since $t - 1 \geq 2g + 3$ it follows easily that Γ is finite. For each $\gamma \in \Gamma$, γ not the identity, let W_γ be the set of primes Q, not in T, such that either $\gamma Q = Q$, or $\gamma Q \in T$. We claim $|W_\gamma| \leq 2g + 3$. Suppose $|W_\gamma| > 2g + 3$. Since γ is not the identity, it can fix at most $2g + 2$ primes. Thus there exist Q and Q' in W_γ such that γQ and $\gamma Q'$ are in T. Since $|\gamma T \cap T| \geq t - 1$, either γQ or $\gamma Q'$ is in $\gamma t \cap T$, and so either Q or Q' is in T. This is a contradiction.

Let W be the union of all the W_γ for $\gamma \in \Gamma$. We have shown that W is a finite set. Let Q be a prime not in $W \cup T$, and set $T' = T \cup \{Q\}$. Suppose $\sigma \in \mathrm{Aut}_k(K)$ maps T' into itself. Then $|\sigma T \cap T| \geq t - 1$, and either $\sigma Q = Q$ or $\sigma Q \in T$. If σ were not the identity, the first condition would show $\sigma \in \Gamma$ and the second condition would contradict the choice of Q. Thus σ must be the identity.

Proposition 3. *Let p be the characteristic of k. Let G be a finite group with more than two elements and otherwise arbitrary order if $p = 0$, and of order prime to p if $p \neq 0$. Let $H_1, H_2, \ldots, H_t$ be cyclic subgroups of G which generate G. Let $T = \{P_1, P_2, \ldots, P_t\}$ be a set of primes of K, and Q, not in T, another prime of K. Then, after possibly replacing H_t with another nontrivial cyclic group, there is a Galois extension L/K and an isomorphism $\rho\colon \mathrm{Gal}(L/K) \to G$ such that for each i, $1 \leq i \leq t$, we have $\rho^{-1}(H_i)$ is the ramification group of some prime of L lying above P_i. Moreover, $T' = T \cup \{Q\}$ is the full set of primes of K ramified in L.*

Proof. If $p = 0$, let F be the Galois group of the maximal Galois extension of K unramified outside of T'. If $p \neq 0$, let F be the Galois group of the maximal prime-to-p Galois extension of K unramified outside of T' (the tame fundamental group). In both cases F is topologically generated by $2g + t + 1$ elements $a_1, b_1, \ldots, a_g, b_g, c_1, \ldots, c_t, c_{t+1}$ subject to the one relation

$$[a_1, b_1] \cdots [a_g, b_g] c_1 c_2 \cdots c_t c_{t+1} = e.$$

When $p = 0$, this is classical. When $p \neq 0$ this is a theorem of Grothendieck (see Popp [P]). Define a homomorphism $\overline{\rho}$ from F to G by sending each a_i and b_i to e, each c_i to a generator h_i of H_i for $i = 1, 2, \ldots, t$, and c_{t+1} to $(h_1 h_2 \cdots h_t)^{-1}$. Suppose h_t has order greater than two. By replacing h_t by an appropriate power of h_t if necessary, we can assume $h_1 h_2 \cdots h_t \neq e$. If the order of h_t is two, and $h_1 h_2 \cdots h_t = e$, then $\{h_1, h_2, \cdots, h_{t-1}\}$ already generate G. Replace h_t by any element $g_t \in G$ different from itself and e, and H_t by $\langle g_t \rangle$. This is possible because we are assuming G has more than two elements. Thus, in all cases we can assume that $h_1 h_2 \cdots h_t \neq e$. Let $N \subset F$ be the kernel of $\overline{\rho}$, and L the fixed field of N. Then, $F/N \cong \mathrm{Gal}(L/K)$ and $F/N \cong G$. Let $\rho\colon \mathrm{Gal}(L/K) \to G$ be the isomorphism induced by $\overline{\rho}$. The assertions about $\rho^{-1}(H_i)$ and T' follow from the general theory.

Remark 1. Let $G = \langle g \rangle$ be a group with two elements, and T and T' sets of primes of K as in the statement of Proposition 3. Suppose t is odd. Then there is a separable quadratic extension L of K such that T' is the full set of primes of K ramified in L. To see this, using the notation of the proof, send each a_i and b_i to e, and each c_i to g for $i = 1, 2, \ldots, t$, and c_{t+1} to $(g^t)^{-1} = g$. Then, L is the fixed field of the kernel of this homomorphism. If t is even this construction fails, as indeed it must, since a tamely ramified quadratic extension must have an even number of ramified primes by the Riemann-Hurwitz genus formula.

Remark 2. It is important to notice that it is not necessary to assume the groups H_i are distinct so long as, in their totality, they generate G. We will use this remark later.

Proposition 1, 2, and 3 are all that will be needed to prove the theorem except in the case where $p \neq 0$ and p divides $|G|$. To deal with this case some further background will be called upon.

2. The main result

We now come to the proof of the theorem. We will prove a special case first. The proof of the special case contains the main idea and is free from certain technicalities.

Theorem′. *Let K be a function field over k. Let p be the characteristic of k. If $p = 0$, let G by any nontrivial finite group. If $p \neq 0$, let G be a nontrivial group of order prime to p. Then, there exist infinitely many Galois extensions L/K such that* $\mathrm{Gal}(L/K)$ *is isomorphic to G, and* $\mathrm{Gal}(L/K) = \mathrm{Aut}_k(L)$.

Proof. Let g be the genus of K and n the order of G. Let $s = 2(n+g)^2$. Let $H_1, \ldots, H_r$ be a set of nontrivial cyclic subgroups of G which generate G. Set $t = sr$ and let $T = \{P_1, \ldots, P_t\}$ be a set of t primes of K. Finally, find a prime Q of K, Q not in T, such that any $\sigma \in \mathrm{Aut}_k(K)$ which maps $T' = T \cup \{Q\}$ into itself is the identity. This is possible by Proposition 2.

Assume G has more than two elements. By Proposition 3, we can find a Galois extension L/K and an isomorphism $\rho\colon \mathrm{Gal}(L/K)$ to G with the following properties

(i) For each i with $1 \leq i \leq r$, $\rho^{-1}(H_i)$ is the ramification group of some prime above P_j for $j = (i-1)s+1, \ldots, is$. (It is here that we use the remark that the H_i in Proposition 3 need not be distinct.)

(ii) T' is the full set of primes of K ramified in L.

We claim that $\mathrm{Gal}(L/K) = \mathrm{Aut}_k(K)$. Let $M \neq K$ be an intermediate extension. M cannot be fixed by all the groups $\rho^{-1}(H_i)$, since these generate $\mathrm{Gal}(L/K)$. It follows that there are at least s primes in K which ramify in M. A short computation, using the Riemann-Hurwitz genus formula, shows that $g_M > n^2 + 2n(g_k - 1) + 1$, and so the hypotheses to the corollary of Proposition 1 are satisfied. It follows that every automorphism $\sigma \in \mathrm{Aut}_k(L)$ induces an automorphism of K. Such an automorphism must induce a permutation of the ramification set $T' = T \cup \{Q\}$. By Proposition 2, and the choice of Q, this shows that σ is the identity on K.

To deal with the remaining case where $|G| = 2$, let t be an odd integer, $t > 4g_K + 3$, and $T = \{P_1, P_2, \ldots, P_t\}$ a set of distinct primes of K. By the first remark following Proposition 3, for any prime Q of K not in T, we can find a separable quadratic extension L/K ramified precisely above the set $T' = T \cup \{Q\}$. Choose Q to satisfy the conclusion of Proposition 2. Since $|T'| = t+1 > 4g_K + 4$, one finds that $g_L > 4 + 4(g_K - 1) + 1$, and so by the corollary to Proposition 1 every automorphism $\sigma \in \mathrm{Aut}_k(L)$ induces an automorphism of K. This induced automorphism must permute the ramification set T', and so, using Proposition 2 once more, σ must be the identity on K. This completes the proof.

To prove our theorem in complete generality, we will use some results of Harbater on mock covers of algebraic curves. These will enable us to imitate the proof of Theorem′in the remaining case where p, the characteristic of k, is positive and p divides the order of G.

Let G be a given finite group. One can find nontrivial cyclic subgroups $H_1, H_2, \ldots, H_r$, each of prime power order, which generate G. Let X be a smooth projective curve, and $K = k(X)$ the field of rational functions on X. The main theorem will follow from the following two propositions.

Proposition 4. *Let s be a positive integer. There is a Galois cover $Y \to X$ with group G and the property that for each i, $1 \leq i \leq r$, there are at least s points of X over which there is a point of Y having H_i as ramification group.*

Proposition 5. *Let s be a positive integer. Let a cover $Y \to X$ be given which is Galois with group G. Suppose that $T = \{P_1, P_2, \ldots, P_t\}$ is the branch locus, and that for each i, $1 \leq i \leq r$, there are at least s points in T above which H_i occurs as a ramification group. Let Q be a point of X not in T. Finally, suppose p divides n. Then, there is a cover $Z \to X$ such that*

(a) *$Z \to X$ is Galois with group G, and with branch locus $T' = \{P_1, P_2, \ldots, P_t, Q\}$.*
(b) *For each i, $1 \leq i \leq r$, there are at least s points of X over which there is a point in Z having H_i as ramification group.*

The proof of Proposition 4 is essentially contained in the first section of [Ha2], *Mock covers and Galois extensions*, which builds on the earlier paper [Ha1], *Deformation theory and the fundamental group.* We sketch the idea. Let $t = sr$, and find a covering of X by t affine open sets U_j which is not redundant, i.e., for every j, U_j is not covered by $\{U_i | i \neq j\}$. For each j, choose a point $P_j \in U_j$ which is not in $\bigcup_{i \neq j} U_i$. For $j = (i-1)s+1, \ldots, is$ find a standard mock cover of U_j which is ramified only above P_j with ramification group H_i. Let $e_i = |H_i|$. By taking n/e_i disjoint copies of these standard mock covers and labeling the sheets in the obvious way with the elements of the group G we can find a G-mock cover of each U_i ramified only above P_i. Now let j vary from 1 to t and patch these covers over the intersections $U_k \cap U_1$. This is easily done since all these mock covers are trivial over these intersections. We have now described a G-mock cover over X with branch locus $\{P_1, \ldots, P_t\}$ with the further property that each H_i, $i = 1, 2, \ldots, r$, is the ramification group above at least s points. Harbater shows how to deform this mock cover into an actual Galois cover with Galois group G. The branch locus can move in this deformation, and even increase in size, but the property that each H_i is the ramification group above at least s primes is preserved. The details are given in [Ha2, Proposition 1.2, and its corollaries]. The discussion there assumes X is the affine line, but the methods work equally well with X a smooth, projective curve.

To prove Proposition 5 one uses the same idea. Let H be a subgroup of G of order p. Let $A^1(k)$ be the affine line, and let $k[x]$ be the ring of regular functions on it. The Artin-Schreier equation, $z^p - x^{p-1}z = t$ defines a family of covers of A^1 whose fiber at $t = 0$ is a mock cover ramified only at the origin with ramification group cyclic of order p. Pulling this back one constructs a (connected) mock cover of a neighborhood V of Q ramified only above Q with ramification group H. By taking n/p disjoint copies of this, one constructs a G-mock cover of V which is ramified only above Q. On $U = X - \{Q\}$ consider

the restriction of the given cover $Y \to X$. We have a family of deformations over V which reduces to our G-mock cover over V at $t = 0$, and we consider the trivial family of deformations of our given cover over U. One special feature of the Artin-schreier construction is that the point Q does not move in the deformation. So if we can patch, deform, and specialize we can construct the desired cover $Z \to X$. This can be done, but since we are working with an actual cover over U at $t = 0$, instead of a mock cover, the details of the patching are more delicate. This is carried out in [Ha3]. Proposition 6 of that paper is virtually identical to our Proposition 5.

We are now in a position to prove our main theorem. If p does not divide n, then the result has already been proven (Theorem′). So assume p divides n.

Let g be the genus of X, n the order of the group G, and set $s = (n+g)^2$. By Proposition 4, there is a field $L = K(Y)$ which is a Galois extension of $K = k(X)$ with group G, and such that each subgroup H_i is the ramification group of at least $s = (n+g)^2$ primes of L. Let T be the branch locus of $Y \to X$ and choose a point $Q \in X$ to satisfy the conclusion of Proposition 2. Now use Proposition 5, and replace $L = k(Y)$ by $L' = K(Z)$. As before, L'/K is Galois with group G. Using (b) of Proposition 5, and the corollary to Proposition 1 as in the proof of Theorem′, we see that every $\sigma \in \mathrm{Aut}_k(L')$ induces an automorphism of K. The branch locus of L'/K is the union of T and $\{Q\}$. Since σ restricted to K must permute the branch locus, the choice of Q shows that σ must be the identity on K. This completes the proof of the theorem.

Acknowledgment

We would like to extend our thanks to Professor S. Abhyankar for pointing out an error in an earlier version of this paper.

References

[D'M-Mad] J. G. D'Mello and M. L. Madan, *Algebraic function fields with solvable automorphism group in characteristic p*, Comm. Algebra **11** (1983), 1187–1236.

[Gr] L. Greenberg, *Maximal groups and signatures*, Discontinuous Groups and Riemann Surfaces (L. Greenberg, ed.), Ann. of Math. Stud., no. 79, Princeton Univ. Press, Princeton, NJ, 1974, pp. 207–226.

[Ha1] D. Harbater, *Deformation theory and the tame fundamental group*, Trans. Amer. Math. Soc. **262** (1980), 399–415.

[Ha2] ——, *Mock covers and group extensions*, J. Algebra **91** (1984), 281–293.

[Ha3] ——, *Formal patching and adding branch points*, preprint.

[Madd-Va] D. J. Madden and R. C. Valentini, *The group of automorphisms of algebraic function fields*, J. Reine Angew. Math. **343** (1983), 162–168.

[P] H. Popp, *Fundamentalgruppen algebraische Mannigfaltigkeiten*, Lecture Notes in Math.,vol. 176, Springer-Verlag, Berlin, Heidelberg, and New York, 1970.

[Sch] H. L. Schmid, *Uber die Automorphismen eines algebraischen Funktionenkörper von Primzahlcharacteristik*, J. Reine Angew. Math. **179** (1938), 5–15.

[St1] H. Stichtenoth, *Die Ungleichung von Castelnuovo*, J. Reine Angew. Math. **348** (1984), 197–202.

[St2] H. Stichtenoth, *Zur Realisierbarkeit endlichen Gruppen als Automorphismengruppen algebraischer Funktionenkörper*, Math. Z. **187** (1984), 221–225.

[Va-Mad] R. C. Valentini and M. L. Madan, *Automorphism groups of algebraic function fields*, Math. Z. **176** (1981), 39–52.

Department of Mathematics, Ohio State University, Columbus, Ohio 43210

Department of Mathematics, Brown University, Providence, Rhode Island 02912