ISRAEL JOURNAL OF MATHEMATICS, Vol. 68, No. 1, 1989

ALGEBRAIC FUNCTION FIELDS OF ONE VARIABLE OVER FINITE FIELDS ARE STABLE

BY

WULF-DIETER GEYER†

Mathematisches Institut, Universität Erlangen — Nürnberg, Bismarckstr. 1½, 852 Erlangen, FRG

ABSTRACT

It is shown that any algebraic curve C over a finite field has a separable cover of some degree n over the projective line $\mathbf{P}_1$ such that the geometric Galois group of the Galois hull of $C \mid \mathbf{P}_1$ is the full symmetric group S_n.

§0. Statement of results

In this note, the following will be shown:

PROPOSITION. *Let $K \mid \mathbf{F}_q$ be a field of algebraic functions of one variable, i.e. a finitely generated regular extension of transcendence degree one. Let $\tilde{\mathbf{F}}_q$ denote the algebraic closure of $\mathbf{F}_q$. Then there exists an (arbitrary large) integer n and an element $x \in K$ such that $K \mid \mathbf{F}_q(x)$ is separable of degree n and $\mathrm{Gal}(\tilde{K} \mid \tilde{\mathbf{F}}_q(x)) = S_n$, where $\tilde{K}$ is the normal closure of $K\tilde{\mathbf{F}}_q \mid \tilde{\mathbf{F}}_q(x)$.*

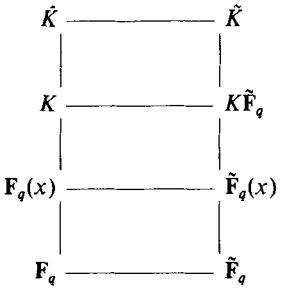
REMARK 1. Let $\hat{K}$ be the normal closure of $K \mid \mathbf{F}_q(x)$, so $\tilde{K} = \hat{K}\tilde{\mathbf{F}}_q$. Since S_n is the maximal Galois group of a polynomial of degree n, from the proposition it follows that

$$\mathrm{Gal}(\hat{K} \mid \mathbf{F}_q(x)) = \mathrm{Gal}(\tilde{K} \mid \tilde{\mathbf{F}}_q(x)).$$

Especially, $\hat{K} \mid \mathbf{F}_q$ is a regular extension. Therefore the function field $K \mid \mathbf{F}_q$ is called *stable*, cf. [4], p. 222.

† This work was partially supported by a grant from G.I.F. (German Israeli Foundation for Scientific Research and Development).

Received March 31, 1989



REMARK 2. In the form of Remark 1 the proposition was first shown by Madan and Madden in [7]. But their proof missed the case of char $K = 2$. In the following proof their ideas are used, but the construction and the means used are simplified, e.g. by replacing the theorems of Marggraf and Manning on multiple transitive groups by an older and easier theorem of Jordan.

REMARK 3. The proposition in case of conservative curves over infinite fields k has been handled (see [3] and [5]) using the ramification structure of $K \mid k(x)$, showing there is an x such that the geometric ramification is of the simplest possible type $(2,1,\ldots,1)$ over any ramified point of the line. This cannot be done over a finite field k. Therefore decomposition groups are used, to get the Galois group large.

§1. Decomposition groups

For the convenience of the reader, some basic facts on decomposition groups are recalled, which refine the standard definitions (cf. e.g. [4], p. 15). In this section the following situation is fixed: Let $L \mid K$ be a separable extension of fields of degree n, say $L = K(y_1)$, given by some irreducible polynomial

$$g(X) = \prod_{i=1}^{n} (X - y_i) \in K[X].$$

Let $\hat{L} = K(y_1, y_2, \ldots, y_n)$ be the Galois hull of $L \mid K$. We look at $G = \mathrm{Gal}(\hat{L} \mid K)$ as a permutation group $\mathrm{Gal}(g \mid K)$ on the set $\{y_1, y_2, \ldots, y_n\}$ of roots of g. Let $\mathfrak{p}$ be a discrete valuation of K with residue field $K(\mathfrak{p})$. It decomposes in L into

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$$

with residue degrees $[L(\mathfrak{P}_i) : K(\mathfrak{p})] = f_i$, and we assume (as is the case in all usual situations) that

$$\sum_{i=1}^{r} e_i f_i = n.$$

Then the decomposition above corresponds to a decomposition

$$g = g_1 \cdot \cdots \cdot g_r \qquad \text{with irreducible } g_i \in K_\mathfrak{p}[X]$$

of the polynomial g over the $\mathfrak{p}$-adic completion $K_\mathfrak{p}$ of K with $\deg g_i = e_i f_i$.† We call

$$G_\mathfrak{p} := \mathrm{Gal}(g \mid K_\mathfrak{p})$$

the *decomposition group* of $L \mid K$ at the place $\mathfrak{p}$. Of course, it is a subgroup of G as permutation group. Let $\hat{L}_{\mathfrak{P}_i}$ be the Galois hull of $L_{\mathfrak{P}_i} \mid K_\mathfrak{p}$, i.e. the decomposition field of g_i over $K_\mathfrak{p}$. Then the composite of all fields $\hat{L}_{\mathfrak{P}_i}$ is isomorphic to the completion of $\hat{L}$ at any extension of $\mathfrak{p}$ to $\hat{L}$.

REMARK. The local Galois groups

$$G_{\mathfrak{P}_i} := \mathrm{Gal}(g_i \mid K_\mathfrak{p}) \cong \mathrm{Gal}(\hat{L}_{\mathfrak{P}_i} \mid K_\mathfrak{p})$$

are also called the decomposition groups of $L \mid K$ at the place $\mathfrak{P}_i$. If $L = \hat{L}$ is Galois over K, then the groups

$$\mathrm{Gal}(\hat{L}_{\mathfrak{P}_i} \mid K_\mathfrak{p}) = \{\sigma \in G;\ \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$$

form a family of conjugate subgroups of G, isomorphic to $G_\mathfrak{p}$; but $G_{\mathfrak{P}_i}$ is not a subgroup as permutation group, since it operates only on the roots of g_i. But in the non-Galois case, the groups $G_{\mathfrak{P}_i}$ are only factor groups of $G_\mathfrak{p}$, and not necessarily subgroups of G.

In the proof of the proposition the following facts on decomposition groups are used, which rely on simple facts about extensions of local fields, cf. [6], §14:

FACT 1. *Let $K(\mathfrak{p})$ be finite. If $e_1 = e_2 = \cdots = e_r = 1$, i.e. if $\mathfrak{p}$ is unramified in $L \mid K$, then $G_\mathfrak{p}$ is a cyclic group, generated by a permutation consisting of r disjoint cycles of length $f_1, f_2, \ldots, f_r$.*

† If y_1 is appropriately chosen, then $g_i \bmod \mathfrak{p}$ is the e_i-th power of an irreducible polynomial of degree f_i over the residue class field $K(\mathfrak{p})$. We are not going to use this fact, which is important for computations but has one complication: As Dedekind ([2], pp. 404–406) 1871 remarked, it may be possible that one cannot choose y_1 simultaneously for all g_i, due to the existence of 'ausserwesentliche Diskriminantenteiler.' By Hensel's methods (see e.g. [6], §21, §25) the standpoint of completions gives a more complete picture than Kummer's congruential standpoint.

PROOF. Since the residue field $K(\mathfrak{p})$ is finite, the Galois group of any unramified extension of $K_\mathfrak{p}$ is generated by the corresponding Frobenius, which permutes the roots of each g_i cyclically.

FACT 2. *Let $K(\mathfrak{p})$ be finite. If $e_1 = 1$, i.e. $\mathfrak{P}_1$ is unramified in $L \mid K$, if f_1 is odd and prime to f_i for all $i > 1$, and if $e_i \leqq 2$ for all i, then $G_\mathfrak{p}$ contains an f_1-cycle.*

PROOF. If $e_i = 2$, then $L_{\mathfrak{P}_i}$ is a quadratic extension of the unramified extension $K_\mathfrak{p}^{(f_i)}$ of degree f_i of $K_\mathfrak{p}$. Then $\hat{L}_{\mathfrak{P}_i}$ is the composite of the quadratic extensions of $K_\mathfrak{p}^{(f_i)}$ conjugate to $L_{\mathfrak{P}_i} \mid K_\mathfrak{p}^{(f_i)}$ over $K_\mathfrak{p}$. Therefore $G_{\mathfrak{P}_i}$ has exponent $2f_i$. Now take any $\sigma \in G_\mathfrak{p}$ which induces the Frobenius on g_1. Then σ^N with

$$N = 2 \cdot \operatorname{lcm}\{f_2, \ldots, f_r\}$$

is an f_1-cycle.

FACT 3. *Let the residue field $K(\mathfrak{p})$ be algebraically closed of characteristic p ($= 0$ or $\neq 0$). If all e_i are prime to p, then $G_\mathfrak{p}$ is a cyclic group, generated by a permutation consisting of r disjoint cycles of length $e_1, e_2, \ldots, e_r$.*

PROOF. All tamely ramified extensions of $K_\mathfrak{p}$ are cyclic, generated by the corresponding root of any prime element. So the same argument works as in the proof of Fact 1.

§2. Proof of the Proposition

Step 1. *Find prime divisors of $K \mid \mathbf{F}_q$*

By the Riemann hypothesis the number P_r of prime divisors of degree r in $K \mid \mathbf{F}_q$ is asymptotically

$$P_r = \frac{q^r}{r} + O(q^{r/2}) \qquad (r \to \infty)$$

cf. [4], p. 41. Therefore there is an r_0 such that

$$P_r > 0 \qquad \text{if } r \geqq r_0. \tag{1}$$

Now choose an odd prime number $l_0 \geqq \max(r_0, 2g - 1, g + 1)$, where g is the genus of $K \mid \mathbf{F}_q$, and choose a larger prime l of the form

$$l = l_0 + 2u, \quad u > r_0, \quad u \equiv 1 \bmod 2. \tag{2}$$

By (1) choose prime divisors $\mathfrak{P}$, $\mathfrak{Q}$ of K with

$$\deg \mathfrak{P} = u, \qquad \deg \mathfrak{Q} = l_0.$$

Step 2. *Find the function* x

Let α be an element of a normal base of $\mathbf{F}_{q^u} \mid \mathbf{F}_q$ and t be a prime element of $\mathfrak{P}$. Then choose a function x such that

$$x \equiv \frac{1}{\alpha}\left(\frac{1}{t^2} + \frac{1}{t}\right) \mod \mathfrak{P}^0, \tag{3}$$

$$x \equiv 0 \mod \mathfrak{Q}^{-1}, \tag{4}$$

and x integral at all places $\neq \mathfrak{P}, \mathfrak{Q}$. The obstruction to these congruences is the differential module $\Omega(\mathfrak{P}^0\mathfrak{Q})$, cf. [1], Chap. II. Because $\deg \mathfrak{Q} = l_0 > 2g - 2$, this module vanishes. The dimension of the affine space of solutions of (3) and (4) is, by the theorem of Riemann–Roch,

$$\dim L(\mathfrak{Q}) = l_0 + 1 - g \geqq 2$$

whereas the space of solutions of (3) and $x \equiv 0 \mod \mathfrak{Q}^0$ has at most dimension 1. So there are solutions x with $\operatorname{ord}_{\mathfrak{Q}} x = -1$, i.e. the divisor of x is

$$(x) = \frac{\mathfrak{A}}{\mathfrak{P}^2\mathfrak{Q}} \tag{5}$$

for some integral divisor $\mathfrak{A}$ of degree $2u + l_0 = l$, prime to $\mathfrak{P}$ and $\mathfrak{Q}$. If $\operatorname{char} K \neq 2$, the equation (5) is sufficient for the following. The more precise congruence (3) is only necessary if $\operatorname{char} K = 2$. From (5) it follows that $K \mid \mathbf{F}_q(x)$ is a separable extension of prime degree l.

Step 3. *Show that* $G = \operatorname{Gal}(\hat{K} \mid \mathbf{F}_q(x)) \geqq A_l$

The pole $\mathfrak{p}$ of x in $\mathbf{F}_q(x)$ resp. $\tilde{\mathbf{F}}_q(x)$ splits in K resp. $K\tilde{\mathbf{F}}_q$ as

$$\mathfrak{p} = \mathfrak{P}^2\mathfrak{Q} \qquad \deg \mathfrak{P} = u, \quad \deg \mathfrak{Q} = l_0,$$

$$= \mathfrak{P}_1^2\mathfrak{P}_2^2 \cdots \mathfrak{P}_u^2\mathfrak{Q}_1 \cdots \mathfrak{Q}_{l_0} \qquad \text{(splitting in } K\tilde{\mathbf{F}}_q\text{)}.$$

We look at G as a subgroup of the symmetric group S_l. Since G is transitive of prime degree, it is primitive. The decomposition group $G_{\mathfrak{p}}$ contains from the factor $\mathfrak{Q}$ of $\mathfrak{p}$ an l_0-cycle (Fact 2 in §1). By a theorem of C. Jordan from 1873 (see [8], Theorem 13.9), a primitive subgroup of S_l containing an l_0-cycle with l_0 prime and $l_0 < l - 2$ has to contain the alternating group A_l.

Step 4. *Show that* $\tilde{G} = \operatorname{Gal}(\tilde{K} \mid \tilde{\mathbf{F}}_q(x)) = S_l$

Since A_l is a simple group and $\operatorname{Gal}(\tilde{\mathbf{F}}_q \mid \mathbf{F}_q)$ is abelian, from step 3 it follows

that $\tilde{G} \supseteqq A_l$. To show the claim of step 4, which is the claim of the proposition, one has to find an odd permutation in $\tilde{G}$. For this let us look at the ramified prime divisors $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_u$.

If char $K \neq 2$, the decomposition group $\tilde{G}_\mathfrak{p}$ contains a product of u transpositions (Fact 3 in §1), which is an odd permutation.

If char $K = 2$, the decomposition group $\tilde{G}_\mathfrak{p}$ has to be determined more carefully. From the ramification structure of $\mathfrak{p}$ in $K\tilde{\mathbf{F}}_q \mid \tilde{\mathbf{F}}_q(x)$, one only gets that $\tilde{G}_\mathfrak{p}$ is some subgroup of $(\mathbf{Z}/2\mathbf{Z})^u$. From (3) one gets

$$\alpha x = \frac{1}{t^2} + \frac{1}{t} + \sum_{i=0}^{\infty} a_i t^i \qquad (a_i \in \mathbf{F}_{q^u}). \tag{6}$$

We choose a new prime element τ of $K_\mathfrak{P}$ instead of t such that the above equation becomes

$$\tau^{-2} + \tau^{-1} = \alpha x + a_0. \tag{7}$$

This can be done by substituting

$$\tau^{-1} = t^{-1} + \sum_{j=1}^{\infty} b_j t^j \qquad (b_j \in \mathbf{F}_{q^u})$$

into (7) and comparing with (6), which gives equations

$$a_{2n-1} = b_{2n-1}, \quad a_{2n} = b_{2n} + b_n^2 \qquad (n \in \mathbf{N})$$

which recursively determine the coefficients b_j.

On the quadratic equation (7) for $K_\mathfrak{P}$ over $\mathbf{F}_{q^u}((x^{-1}))$ operates the Frobenius of $\mathbf{F}_{q^u} \mid \mathbf{F}_q$, giving conjugate equations

$$\tau_i^{-2} + \tau_i^{-1} = \alpha^{q^i} x + a_0^{q^i} \qquad (1 \leqq i \leqq u) \tag{8}$$

which generate the quadratic extensions $(K\tilde{\mathbf{F}}_q)_{\mathfrak{P}_i} \mid \tilde{\mathbf{F}}_q((x^{-1}))$. Since the α^{q^i} are $\mathbf{F}_2$-independent as normal base over $\mathbf{F}_q$, the equations (8) generate by Artin–Schreier theory linearly independent quadratic extensions of $\tilde{\mathbf{F}}_q((x^{-1}))$. Therefore the decomposition group $\tilde{G}_\mathfrak{p}$ is isomorphic to the full group $(\mathbf{Z}/2\mathbf{Z})^u$, generated by u disjoint transpositions. Especially, $\tilde{G}$ contains odd permutations, and therefore $\tilde{G} = S_l$. This ends the proof of the proposition.

References

1. C. Chevalley, *Introduction to the Theory of Algebraic Function Fields of One Variable*, Am. Math. Soc., New York, 1951.

2. R. Dedekind, *Gesammelte mathematische Werke III*, Vieweg, Braunschweig, 1932.

3. M. Fried and M. Jarden, *Diophantine properties of subfields of* **Q**, Am. J. Math. **100** (1978), 653–666.

4. M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.

5. W.-D. Geyer and M. Jarden, *On stable fields in positive characteristic*, Geom. Dedic. **29** (1989), 335–376.

6. H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin, 1949.

7. M. L. Madan and D. J. Madden, *On the theory of congruence function fields*, Commun. Algebra **8** (1980), 1687–1697.

8. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York–London, 1964.