ISRAEL JOURNAL OF MATHEMATICS, Vol. 31, No. 1, 1978

FROBENIUS GALOIS GROUPS OVER QUADRATIC FIELDS

BY
JACK SONN

ABSTRACT
There exists a quadratic field $\mathbf{Q}(\sqrt{D})$ over which every Frobenius group is realizable as a Galois group.

1. Introduction

A Frobenius group is a finite transitive permutation group in which every element different from 1 has at most one fixed point, and some element different from 1 has a fixed point. Our main result is that there exist infinitely many quadratic fields $\mathbf{Q}(\sqrt{D})$ such that every Frobenius group is realizable as the Galois group of an extension of $\mathbf{Q}(\sqrt{D})$, where $\mathbf{Q}$ denotes the field of rational numbers. From the proof it appears likely that the result holds for $\mathbf{Q}$ as well as for quadratic fields. Indeed, we will show that given any number field k, every Frobenius group is a Galois group over k provided that SL(2, 5) and one other nonsolvable group of order 240 are Galois groups over k. Here and in the rest of this paper, we will say G is a Galois group over k if there exists a Galois extension K/k with Galois group $G(K/k)$ isomorphic to G.

Let k be a field, $\tilde{k}$ its separable closure. An *embedding problem over* k is given by a finite Galois extension K/k, together with an epimorphism $f: E \to G(K/k)$ with E a finite group. A *solution* to this embedding problem is given by a homomorphism $g: G(\tilde{k}/k) \to E$ such that fg is the natural restriction map $\operatorname{res}(\tilde{k}/K)$: $G(\tilde{k}/k) \to G(K/k)$. If g is surjective, then the fixed field of its kernel is a Galois extension L of k containing K with $G(L/k) \simeq E$.

Received June 30, 1977

2. Reduction to two special groups

Let G be a Frobenius group. By Frobenius' theorem [5, p. 179], the set of all elements of G with no fixed points, together with the identity, form a normal subgroup M of G, the *Frobenius kernel* of G. If H is the subgroup of G fixing some given point, then H has order prime to M, and $HM = G$, hence G is a split extension of M by H. H is called a *Frobenius complement* of G.

THEOREM 2.1. (Thompson [11]; see [5, p. 184.) *The Frobenius kernel of a Frobenius group is nilpotent.*

THEOREM 2.2. (Shafarevich [9].) *Let k be a number field, and let an embedding problem be given by $(K/k, f\colon E \to G(K/k))$, where f is a split epimorphism whose kernel is nilpotent of order prime to the order of $G(K/k)$. Then the embedding problem has a surjective solution.*

By a split epimorphism f we mean that there exists a monomorphism $s\colon G(K/k) \to E$ such that fs is the identity map. From Theorems 2.1, 2.2 we obtain

COROLLARY 2.3. *If the Frobenius complement of a Frobenius group G is a Galois group over a number field k, then so is G.*

If a Frobenius group G is solvable, then it is a Galois group over every number field k [10]. We therefore assume from now on that G, and hence its Frobenius complement H, are not solvable.

THEOREM 2.4. (Zassenhaus [5, theor. 18.6].) *Let H be a nonsolvable Frobenius complement. Then H contains a subgroup of index 1 or 2 of the form $Z \times \mathrm{SL}(2,5)$, where Z is the semidirect product of two cyclic groups C_m and C_n of orders m, n respectively, and m and n are relatively prime to each other and to 2, 3, 5. Here $\mathrm{SL}(2,5)$ denotes the group of 2×2 matrices of determinant one over the field of 5 elements.*

Clearly Z is a normal subgroup of H of order prime to its index, hence H is the semidirect product of Z by a complementary subgroup B.

LEMMA 2.5. *If B is a Galois group over a number field k, then so is H.*

PROOF. Let K/k be a Galois extension with $G(K/k) \simeq B$. Z is the semidirect product of its normal subgroup C_n, say, by C_m. Since m, n are relatively prime, C_n is normal in H. m is prime to the order of B, so H/C_n is the semidirect product of Z/C_n by $H/Z \simeq B$, hence by a theorem of Scholz [6],

K/k can be embedded into an extension K_1/k with $G(K_1/k) \simeq H/C_n$. By the same argument, K_1/k can be embedded into an extension L/K with $G(L/k) \simeq H$.

By Corollary 2.3 and Lemma 2.5, the problem is reduced to groups of type B. A Sylow 2-subgroup of a Frobenius complement H is either cyclic or generalized quaternion [8, p. 356], hence the same is true for B. If $H \simeq Z \times \mathrm{SL}(2,5)$, then $B \simeq \mathrm{SL}(2,5)$. Otherwise, B contains a subgroup B' of index 2 isomorphic to $\mathrm{SL}(2,5)$, in which case a Sylow 2-subgroup of B is the generalized quaternion group Q_{16} of order 16 (generated by x, y, with defining relations $x^8 = y^4 = 1$, $x^4 = y^2$, $y^{-1}xy = x^{-1}$).

Lemma 2.6. *There is exactly one group B whose Sylow 2-subgroups are generalized quaternion, and which contains a subgroup B' of index 2 isomorphic to* $\mathrm{SL}(2,5)$.

Proof. Since the center $C(Q_{16})$ of Q_{16} has order 2, as does $C(B')$, it follows that $C(B)$ has order 2, and all these centers are identical. Now $B/C(B)$ contains $B'/C(B) \simeq \mathrm{PSL}(2,5) \simeq A_5$, the simple group of order 60, as a subgroup of index 2. Hence [2, p. 176] $B/C(B)$ is either S_5 or $C_2 \times A_5$, where C_n denotes a cyclic group of order n. But the latter is impossible, by comparison of the Sylow 2-subgroups. Therefore $B/C(B) \simeq S_5$, so B is a central extension

$$1 \to C_2 \to B \to S_5 \to 1$$

so S_5 by C_2.

Let $H^2(G, A)$ denote the second cohomology group of a group G over a G-module A with trivial action. The Schur multiplier $H^2(S_5, \mathbf{C}^*)$ of S_5 [2, 25.12] has order two, where $\mathbf{C}^*$ is the multiplicative group of the complex number field $\mathbf{C}$. The short exact sequence

$$0 \to \mathbf{Z}/2\mathbf{Z} \to \mathbf{C}^* \xrightarrow{2} \mathbf{C}^* \to 1$$

yields the cohomology sequence

$$H^1(S_5, \mathbf{C}^*) \to H^2(S_5, \mathbf{Z}/2\mathbf{Z}) \to H^2(S_5, \mathbf{C}^*).$$

The two outer groups have order two, hence $H^2(S_5, \mathbf{Z}/2\mathbf{Z})$ has order at most four. In fact the order is exactly four, since there are four nonisomorphic group extensions of S_5 by $\mathbf{Z}/2\mathbf{Z}$. Two are the direct product and the pullback of the maps $C_4 \to C_2 \leftarrow S_5$, and the other two are exhibited by Schur in [7], exactly one of which has generalized quaternion Sylow-2-subgroup. It is the subgroup of $\mathrm{GL}(2, 5^2)$ generated by $\mathrm{SL}(2,5)$ and the matrix

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$$

where u is a primitive eighth root of unity in the field of 5^2 elements. q.e.d.

SL(2, 5) is in fact a Frobenius complement [5, p. 205], and it is easy to show, using the example of [5, p. 205] that B is also a Frobenius complement.

From the preceding discussion we have:

THEOREM 2.7. *Let k be a number field such that* SL(2, 5) *and the group B of Lemma* 2.6 *are Galois groups over k. Then every Frobenius group is a Galois group over k.*

3. Frobenius Galois groups over quadratic fields

LEMMA 3.1. *Let k be a number field, K/k an unramified extension with $G(K/k) \simeq A_5$, in which all real primes of k split completely. Then K/k can be embedded into a Galois extension L/k with $G(L/k) \simeq$ SL(2, 5). Similarly, let K_1/k be an unramified extension with $G(K_1/k) \simeq S_5$, in which all real primes split completely. Then K_1/k can be embedded into a Galois extension L_1/k with $G(L_1/k) \simeq B$, where B is the extension of S_5 in Lemma* 2.6.

By an unramified extension K/k we mean that all finite primes of k are unramified in K.

PROOF. An unramified extension K/k, in which all real primes of k split completely, is "tolerant with respect to 2," in the sense of Neukirch [4, p. 86]. The lemma follows immediately from [4, corol. 5.4] with the observation that all solutions to the embedding problems of Lemma 3.1 are necessarily surjective.

Let S_n and A_n denote the symmetric and alternating groups of degree n.

THEOREM 3.2. *For any $n \geqq 3$, there exist infinitely many imaginary quadratic fields $\mathbf{Q}(\sqrt{D})$, $D \in \mathbf{Z}$, each of which has an unramified Galois extension with Galois group A_n and an unramified Galois extension with Galois group S_n.*

PROOF. This theorem is essentially a corollary to a theorem proved independently by Uchida [12] and Yamamoto [13]. The following is proved in [12]. Let l be a prime number satisfying $l \equiv 1 \pmod{n-1}$. Choose an integer $b \equiv 0 \pmod{l}$ and prime to $n-1$. Then choose an integer a so that a is congruent to a primitive root mod l, $(a, nb) = 1$ and a large enough so that $X^n - aX + b$ has no rational root (there are only finitely many integral a for which $X^n - aX + b$ has a rational root). Then the splitting field K of $X^n - aX + b$ over $\mathbf{Q}$ has Galois group S_n over $\mathbf{Q}$ and is unramified over $\mathbf{Q}(\sqrt{D})$, where

$$D = D(a, b) = (-1)^{\frac{1}{2}n(n-1)}(n^n b^{n-1} - (n-1)^{n-1} a^n)$$

is the discriminant of $X^n - aX + b$. To prove that infinitely many quadratic fields $\mathbf{Q}(\sqrt{D})$ arise in this way, it is then proved that given any prime p not dividing $ln(n-1)$, a and b can be chosen as above so that, in addition, D is divisible by p but not by p^2. We need the following sharper version of this last fact. *Given any squarefree integer r, relatively prime to $ln(n-1)$, a and b can be chosen as above so that, in addition, for every prime p dividing r, D is divisible by p but not by p^2.* Our argument is a refinement of that in [12]. Choose $b \equiv n - 1 \pmod{r}$ and as before, $b \equiv 0 \pmod{l}$,$(b, n-1) = 1$. Since $(r, n) = 1$, we can choose a_1 so that $a_1 \equiv n \pmod{r}$, a_1 congruent to a primitive root mod l, $(a_1, nb) = 1$ and a_1 large enough so that $X^n - a_1X + b$ has no rational roots. Then $D_1 = D(a_1, b)$ is divisible by r. If $p^2 \mid D_1$ for some prime $p \mid r$, write $r = r_1r_2$, where r_1 is the product of the primes which divide r and whose squares divide D_1. Now replace a_1 by $a = a_1 + nblr_1r_2^2$. Then a has all the properties of a_1, and for every prime $p \mid r$, $p \mid D$, $p^2 \nmid D$, where $D = D(a, b)$.

Now let $X^n - aX + b$ be a trinomial satisfying the conditions of the Uchida–Yamamoto theorem. Let K be its splitting field, D its discriminant. By choice of a and b, D is prime to $ln(n-1)$. Let r_0 be the product of the prime divisors of D, let q be a prime not dividing $Dln(n-1)$, and set $r = qr_0$. It follows from the preceding discussion that there is another trinomial $X^n - a'X + b'$ whose discriminant D' is divisible by r but not by the square of any prime dividing r, and in addition, its splitting field K', like K, has Galois group S_n over $\mathbf{Q}$, and is unramified over $\mathbf{Q}(\sqrt{D'})$. We observe that a' can be chosen so that D' is negative.

Let us verify that $\mathbf{Q}(\sqrt{D'})$ satisfies the requirements of the theorem. First, $K'/\mathbf{Q}(\sqrt{D'})$ is unramified with Galois group A_n. Secondly, since $\mathbf{Q}(\sqrt{D'}) \cap K = \mathbf{Q}$, $K(\sqrt{D'})/\mathbf{Q}(\sqrt{D'})$ has Galois group S_n. Moreover, $K/\mathbf{Q}(\sqrt{D})$ is unramified, hence so is $K(\sqrt{D'})/\mathbf{Q}(\sqrt{D}, \sqrt{D'})$. But $\mathbf{Q}(\sqrt{D}, \sqrt{D'})/\mathbf{Q}(\sqrt{D'})$ is unramified, hence $K(\sqrt{D'})$ is unramified over $\mathbf{Q}(\sqrt{D'})$. The process of going from D to D' can be iterated, hence there are infinitely many imaginary quadratic fields satisfying the requirements of the theorem. This completes the proof.

THEOREM 3.3. *There are infinitely many imaginary quadratic fields over each of which every Frobenius group is a Galois group.*

PROOF. The theorem follows immediately from Theorem 2.7, Lemma 3.1, and Theorem 3.2.

EXAMPLE. $X^5 - X + 1$ has Galois group S_5 over $\mathbf{Q}$ and is unramified over

$Q(\sqrt{D_0}) = 2869 = 19 \times 151$ [3, p. 121]. Taking $l = 5$, $r = 3 \times 19 \times 151 = 8607$, we can take $b = 25{,}825 = 5^2 \times 1033$, $a_1 = 51{,}647$. $D_1 = D(51{,}647;\ 25{,}825)$ is divisible by 3^2, 19, 151 and not by 19^2 or 151^2. Hence if we replace a_1 by

$$\begin{aligned} a &= a_1 + nblr_1r_2^2 \\ &= 51{,}647 + 5^2 \times 25{,}825 \times 3 \times 19^2 \times 151^2 \\ &= 15{,}942{,}730{,}013{,}522 \end{aligned}$$

then $D = D(a, b)$ satisfies the conditions of Theorem 3.3, i.e. every Frobenius group is a Galois group over $\mathbf{Q}(\sqrt{D})$.

Acknowledgement

I am grateful to Dr. David Chillag for helpful information on Frobenius groups.

Note added in proof, April 1978. The author has just succeeded in realizing SL(2, 5) and B over $\mathbf{Q}$; thus every Frobenius group is realizable over $\mathbf{Q}$.

References

1. J. Dieudonné, On the automorphisms of the classical groups, Mem. Amer. Math. Soc. **2** (1951), 1–95.
2. B. Huppert, *Endliche Gruppen* I, Springer-Verlag, Berlin, 1967.
3. S. Lang, *Algebraic Number Theory*, Addison-Wesley, New York, 1970.
4. J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.
5. D. Passman, *Permutation Groups*, Benjamin, New York, 1968.
6. A. Scholz, *Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoissche Gruppe*, Math. Z. **30** (1929), 332–356.
7. J. Schur, *Untersuchungen über die Darstellung endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.
8. W. R. Scott, *Group Theory*, Prentice-Hall, New Jersey, 1964.
9. I. R. Shafarevich, *On the problem of imbedding fields*, Transl. Amer. Math. Soc., Ser. 2, **4** (1956), 151–183.
10. I. R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Transl. Amer. Math. Soc., Ser. 2, **4** (1956), 185–237.
11. J. Thompson, *Finite groups with fixed point free automorphisms of prime order*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 578–581.
12. K. Uchida, *Unramified extensions of quadratic number fields*, II, Tôhoku Math. J. **22** (1970), 220–224.
13. Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

Faculty of Mathematics
Technion—Israel Institute of Technology,
Haifa, Israel