BOLETIM
DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

Bol. Soc. Bras. Mat., Vol. 20, No. 1, 55-59

Some Galois groups over number fields

Walter Feit

Abstract. Some conditions are stated which imply that certain finite groups are Galois groups over some number fields and related fields.

1. Introduction

Let K be an algebraic number field (i.e. $[K:Q] < \infty$) and let t be an indeterminate over K. An algebraic extension L of $K(t)$ is regular if K is algebraically closed in L.

Let G be a finite group. In this work I want to discuss the question of when any, or all, of the following assertions are true.

(1.1) *G is the Galois group of a regular extension of $K(t)$.*

(1.2) *There exist infinitely many fields E_i with $K \subseteq E_i \subseteq \overline{K}$ such that $\mathrm{Gal}(E_i/K) \simeq G$ and $E_i \cap E_j = K$ for $i \neq j$. (Here $\overline{K}$ is an algebraic closure of K).*

(1.3) *G is the Galois group of an extension field of every number field which contains K.*

(1.4) *G is the Galois group of an extension of K.*

In this sequence each assertion implies the next. The first implies the second by Hilbert's irreducibility theorem, the other implications are straighforward.

Observe that if any of the assertions (1.1)-(1.3) is true for a field K then it is true for any finite extension of K. Thus in each case the strongest statement is the case $K = \mathbb{Q}$.

There is no finite group for which any of these assertions is known to be false for $K = \mathbb{Q}$. In recent years much progress has been made in proving some or all of these assertions for a variety of finite groups. The object of this work is to discuss some of these results. An excellent survey of these topics can be found in [11]. For a more detailed treatment, see [9].

Received 10 June 1988.

2. Rigidity and some consequences

Rigidity and related concepts and their connection with the construction of Galois groups are due to Belyi [2], Fried [5], Matzat [8] and Thompson [13]. I will state only a special case of their results here.

Let C_1, C_2, C_3 be conjugacy classes of the finite group G. Define

$$A = A_G(C_1, C_2, C_3) = \{(x_1, x_2, x_3) \mid x_i \in C_i, \quad x_1x_2x_3 = 1\}.$$

$$\mathbb{Q}(C_1, C_2, C_3) = \{\mathbb{Q}(\chi_n(x_i)) \mid i = 1,2,3; \quad n = 1,2,\ldots\},$$

where $\{\chi_n\}$ is the set of irreducible characters of G.

If $y \in G$ and $(x_1, x_2, x_3) \in A$ then $(x_1^y, x_2^y, x_3^y) \in A$. Thus G acts as a permutation group on A.

Definition. $A = A_G(C_1, C_2, C_3)$ is *rigid* if

(i) $A \neq \varnothing$

(ii) G acts transitively on A

(iii) If $(x_1, x_2, x_3) \in A$ then $G = \langle x_1, x_2, x_3 \rangle$.

If in addition $\mathbb{Q}(C_1, C_2, C_3) = \mathbb{Q}$ then A is said to be *rationally rigid*.

Observe that if A is rigid then G acts faithfully on A if and only if the center of G is $\langle 1 \rangle$.

The next result shows the relevance of this concept.

Theorem 2.1. *Let G be a finite group with center of order 1. Let C_1, C_2, C_3 be conjugacy classes of G such that $A_G(C_1, C_2, C_3)$ is rigid. Let $\mathbb{Q}(C_1, C_2, C_3) = K$. Then there exists a regular extension L of $K(t)$ with*

$$\mathrm{Gal}(L/K(t)) \simeq G.$$

Furthermore at most 3 points in $K(t)$ ramify in L.

The conclusion of Theorem 2.1 asserts that (1.1) and hence (1.2), (1.3), (1.4) is true for G. Theorem 2.1 is a special case of results proved by all the authors mentioned at the beginning of this section. However the various generalizations can be a bit technical and won't be discussed here.

Let F_0 be a function field of genus g_0 over the complex numbers and let F be a finite extension of F_0 with $[F : F_0] = n$. Let g be the genus of F. The following fundamental formula is due to Hurwitz:

$$2g - 2 = n(2g_0 - 2) + \sum(e_i - 1),$$

where P_i ranges over all ramified places in F and e_i is the corresponding index of ramification.

The next result is proved by using Hurwitz's formula in conjunction with

Theorem 2.1. See [4] or [9], p. 372.

Theorem 2.2. *Let G be a finite group with center of order 1. Let $H \lhd G$ with $|G : H| = 2$ or 3. Let $C_1 \neq \{1\}$, C_2, C_3 be conjugacy classes of G with $C_2, C_3 \not\subseteq H$ such that $A_G(C_1, C_2, C_3)$ is rigid. Let K and L be as in Theorem 2.1 and let $K(t) \subseteq M \subseteq L$ where M corresponds to H. Then $M \approx K(t)$ and H is a Galois group over M.*

Thompson [13] used Theorem 2.1 to show that the monster is rationally rigid, and hence is the Galois group of a regular extension of $\mathbb{Q}(t)$. Since then several authors have investigated the various sporadic simple groups, see [6], [7]. Quite recently H. Pahlings in unpublished work has almost completed this work. It is now known that if G is a sporadic simple group, $G \not\approx M_{23}$, then (2.1) holds for G with $K = \mathbb{Q}$. If $G \approx M_{23}$ then (2.1) holds for G with $K = \mathbb{Q}(\sqrt{-23})$.

Let $H \simeq A_6$ or A_7 or a sporadic simple group such that 3 divides the order of the Schur multiplier of H. Then there is a unique covering group $\tilde{H}$ of H with center of order 3. In each of these cases there exists a group G with a center of order 1, such that $\left|G : \tilde{H}\right| = 2$. The existence of G is proved by inspection. By using recent results of Pahlings, as well as earlier known results [6], [7], and Theorems 2.1 and 2.2 it can be shown that in each case $\tilde{H}$ satisfies (2.1) with $K = \mathbb{Q}$. See [4]. This is perhaps surprising since rigidity only applies to groups with trivial center, yet it can be used to handle these groups $\tilde{H}$ with center of order 3.

3. Serre's theorem and some consequences

Let $n \geq 4$. Then there exists a nonsplit exact sequence

$$\langle 1 \rangle \to \mathbb{Z} \to \tilde{A}_n \to A_n \to \langle 1 \rangle$$

where $\mathbb{Z}$ has order 2 and $\tilde{A}_n$, the double cover of A_n, is unique up to isomorphism. If G is a transitive subgroup of A_n, let $\tilde{G}$ denote the inverse image of G in $\tilde{A}_n$. The following result is a special case of a theorem of Serre [10].

Theorem 3.1. *Let $\mathrm{char}\, K \neq 2$. Let $f(x)$ be an irreducible separable monic polynomial over K of degree n and let $F = K(\theta)$ for a root θ of $f(x)$. Assume that the discriminant of $f(x)$ is a square in K. Let E be a splitting field of $f(x)$. Thus $G = \mathrm{Gal}(E/K)$ acting on the roots of $f(x)$ is a subgroup of A_n. Let T be the trace from F to K and let w be the Witt invariant of the quadratic form $T(x^2)$. Then the following are equivalent.*

(i) *There exists a Galois extension M of K with $E \subset M$ and $\mathrm{Gal}(M/K) \approx \tilde{G}$.*

(ii) $w = 1$.

As an example of how this result may be used I will show that $\tilde{A}_8$ is the Galois group of a regular extension of $\mathbb{Q}(t)$.

It is known that there exist polynomials $f(x) = x^8 + ax + b$ over $K = \mathbb{Q}(t)$ whose splitting field is a regular extension of $\mathbb{Q}(t)$ with Galois group A_8. Let θ be a root of $f(x)$. Then $\{\theta^i \mid 0 \le i \le 7\}$ is a basis of F over K and $T(\theta^i) = 0$ for $1 \le i \le 6$. Thus the subspace spanned by $\theta, \theta^2, \theta^3$ is a totally isotropic space orthogonal to 1. Hence $F = H \perp V_1 \perp V_2$, where V_1 is spanned by 1 and H is the direct sum of 3 hyperbolic planes. Therefore T is equivalent to the diagonal form $[1, -1, 1, -1, 1, -1, 8, c]$. Since T has square discriminant $c = -8c_0^2$, and so $w = 1$.

The argument above is due to Serre [10]. A minor variation shows that (2.1) with $K = \mathbb{Q}(t)$ is true for $G = \tilde{A}_{8k}$. By using similar polynomials it can be shown that (1.1) is true for $\tilde{A}_n$ in the following cases (see [12], [14]):

$n \equiv 0$ or $1 \pmod 8$;

$n \equiv 2$ and n is the sum of two squares;

$n \equiv 3 \pmod 8$ and $n = x_1^2 + x_2^2 + x_3^2$ with $(n, x_1) = 1$.

Similar results can be proved for the two double covers of symmetric groups.

By using generalized Laguerre polynomials it can be shown that $\tilde{A}_5$ satisfies (1.1) with $K = \mathbb{Q}$, while $\tilde{A}_6$ and $\tilde{A}_7$ satisfy (1.2) with $K = \mathbb{Q}$. See [3] and some unpublished results of J.-F. Mestre.

By making use of the duality theorem of Tate and the argument of Section 2 it can also be shown that there exist algebraic number fields K_n for $n = 6, 7$ such that (1.2) is satisfied for $6A_n$ with $K = K_n$. Here $6A_n$ is the universal central extension of A_n. See [4].

It should be emphasized that Serre's theorem does not cover all central extensions with a center of order 2. For instance if $p > 3$ is a prime then $\mathrm{SL}(2,p)$ is the universal central extension of the simple group $\mathrm{PSL}(2,p)$. If 16 divides the order of $G = \mathrm{PSL}(2,p)$, and G is a transitive subgroup of A_n then $\tilde{G} \approx \mathbb{Z}_2 \times \mathrm{PSL}(2,p)$. Hence one can never find extensions with Galois group $\mathrm{SL}(2,p)$ by using Serre's theorem.

In fact very little is known about the groups $\mathrm{SL}(2,q)$ with q a prime power. The results mentioned above imply that $\mathrm{SL}(2,5) \simeq \tilde{A}_5$ satisfies (1.1) with $K = \mathbb{Q}$ and $\mathrm{SL}(2,9) \simeq \tilde{A}_6$ satisfies (1.2) with $K = \mathbb{Q}$. Recently Zeh-Marschke has shown that $\mathrm{SL}(2,7)$ is a Galois group over $\mathbb{Q}$. No group $\mathrm{SL}(2,q)$ with q odd, $q > 3$, $q \neq 5, 7, 9$ is known to be a Galois group over $\mathbb{Q}$.

By using the results of [1], the author and J.-F. Mestre have also shown that

$\tilde{M}_{12}$, satisfies (1.2) with $K = \mathbb{Q}$.

References

1. Bayer, P., Llorente, P., and Vila, N., *$\tilde{M}_{12}$ comme group de Galois sur $\mathbb{Q}$*, C. R. Acad. Sc. Paris t. **303,** Série **I** (1986), 277-280..
2. Belyi, G. V., *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izvestia, AMS Translation **14** (1980), 247-256.
3. Feit, W., *$\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields*, J. Algebra **104** (1986), 231-260.
4. ———, *Some finite groups with nontrivial centers which are Galois groups*, Proceedings of the 1987 Singapore Conference, Walter de Gruyter, Berlin – New York.
5. Fried, M., *Fields of definition of function fields and Hurwitz families-Groups as Galois groups*, Comm. Alg. **5** (1977), 17-82.
6. Hoyden-Siedersleben, G. and Matzat, B. H., *Realisierung sporadischer einfacher Gruppen als Galoisgruppen uber Kreisteilungskorpern*, J. Algebra **101** (1986), 273-285.
7. Hunt, D. C., *Rational rigidity and the sporadic groups*, J. of Algebra **99** (1986), 577-592.
8. Matzat, B. H., *Konstruktion von Zahl-und Funktionenkorpern mit vorgegebener Galoisgruppe*, J. reine angew. Math. **349** (1984), 179-220.
9. Matzat, B. H., *Konstruktive Galoistheory*, Lect. Notes on Math. **1284** (1987). Springer-Verlag
10. Serre, J.-P., *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), 651-676.
11. ———, *Groupes de Galois sur $\mathbb{Q}$*, Seminaire Bourbaki (1987-88) **689**.
12. Sonn, J., *Double covers of the alternating and symmetric groups as Galois groups over number fields*, To appear.
13. Thompson, J. G., *Some finite groups which appear as* $\mathrm{Gal}(L/K)$ *where* $K \subseteq \mathbb{Q}(\mu_n)$, J. Algebra **89** (1984,), 437-499.
14. Vila, N., *On central extensions of A_n as Galois group over $\mathbb{Q}_n$*, Arch. Math. (Basel) **44** (1985), 424-437.

Walter Feit
Yale University
Department of Mathematics
New Haven, CT 06520