ACADEMIC PRESS

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Algebra 257 (2002) 244–248

JOURNAL OF Algebra

www.academicpress.com

$SL(2, 11)$ is $\mathbb{Q}$-admissible

Walter Feit

Yale University, Department of Mathematics, PO Box 208283, New Haven, CT 06520-8283, USA

Received 1 March 2002

Communicated by Michel Broué

Dedicated to J.G. Thompson on his 70th birthday

1. Introduction

Let F be an algebraic number field. Let P be a prime ideal in (the ring of integers R of) F and let K be a finite extension of F. Let $P \mid p$, where p is a rational prime. In general it may be difficult to decide whether P ramifies in K, and even more, to compute the ramification index $e(P) = e_P(K/F)$. As this is a local question, there is no loss in replacing F by F_p and K by K_p, the P-adic completions. Then F_p is a finite extension of the p-adic numbers $\mathbb{Q}_p$ and P may be replaced by the prime divisor of p in the ring of integers R_p of F_p. Let $e(K_p/F_p) = e(P)$.

Suppose that N is the splitting field of the monic irreducible polynomial $f(x)$ of degree n in $R[x]$. Let N_p denote the P-adic completion of N. Theorem 1 makes it possible to find $e(N_p/F_p) = e(P)$ in some special situations. This then is applied below to exhibit some $SL(2, 11)$-adequate extensions of $\mathbb{Q}$.

Several polynomials are defined in Section 3 whose splitting field N has $PSL(2, 11)$ as a Galois group over $\mathbb{Q}$, such that N can be embedded in a $\mathbb{Q}$-adequate extension with Galois group $SL(2, 11)$. They are all specializations of Malle's polynomial [M]. It is possible that infinitely many such fields N exist, but a proof of this appears to be beyond known methods. The existence of any one of these polynomials implies

Theorem. *$SL(2, 11)$ is $\mathbb{Q}$-admissible.*

E-mail address: feit@math.yale.edu.

0021-8693/02/$ – see front matter
PII: S0021-8693(02)00523-9

The object of the arguments in Section 4 is to avoid factoring polynomials modulo large primes. However, the referee and J.-P. Serre independently informed me of packages such as KANT and PARI which for the primes and polynomials that arise in this paper can be used to factor the polynomials mod p in a split second. These packages can also be used to compute discriminants of field extensions of some bounded degree, of algebraic number fields, and so can be used here instead of Theorem 1. Since Theorem 1 may be of more general interest, it is included in the paper. In particular, the arguments in Section 4 show that all the computations in this paper can be done by MATHEMATICA on a PC which, for instance, runs at 450 MHz. It should be mentioned that the Shoup algorithm, see [Sh], used in KANT, can be programmed directly in MATHEMATICA and does not take too long to implement. While it is not needed in this paper, it is helpful in providing many more examples of polynomials and fields N with the required properties.

2. A criterion

Let F be a finite extension of $\mathbb{Q}$, let $R, P, f(x), N$ be as in the introduction and let F_p, R_p, N_p denote the P-adic completion in each case. Also P will denote the prime ideal in R or R_p depending on the context. For $a \in F$, $a \neq 0$ let $\nu(a)$ denote the power of P in a (either positive or negative).

By Hensel's Lemma there is a field K with $F \subseteq K \subseteq N$ such that K_p/F_p is unramified and

$$f(x) \equiv \prod_{i=1}^{k} (x - \alpha_i)^{d_i} \mod P, \tag{1}$$

where $\alpha_1, \ldots, \alpha_k$ are local integers in K_p which are distinct mod P for $1 \leqslant i \leqslant k$. Of course P remains prime in K_p. Let $\nu(\beta)$ be the power of P in β for $\beta \in K_p$.

Let $D(f(x))$ denote the discriminant of $f(x)$ over F.

Theorem 1. *Choose an ideal P in R. Assume that $m \geqslant 1$ and the following hold.*

(i) *In* (1) $d_i = 2$ *for* $1 \leqslant i \leqslant m$ *and* $d_i = 1$ *for* $m + 1 \leqslant i \leqslant k$.
(ii) $\nu(D(f(x))) = m$.

Then $e(N_p/F_p)$ is even.

Proof. Let P_1 be a prime ideal in N_p. By Hensel's Lemma

$$f(x) = \prod_{i=1}^{m} (x - \alpha_{i1})(x - \alpha_{i2}) \prod_{i=m+1}^{k} (x - \alpha_{i0}), \tag{2}$$

where $\alpha_{i0} \in K_p$ and $\alpha_{i0} \equiv \alpha_i \bmod P$ for $m+1 \leqslant i \leqslant k$, $(x-\alpha_{i1})(x-\alpha_{i2}) \in K_p[x]$, and $\alpha_{i1} \equiv \alpha_{i2} \equiv \alpha_i \bmod P_1$ for $1 \leqslant i \leqslant m$. By (2),

$$m = v\big(D\big(f(x)\big)\big) = v\left(\prod_{i=1}^{m}(\alpha_{i1}-\alpha_{i2})^2\right). \tag{3}$$

As $(\alpha_{i1}-\alpha_{i2})^2 \in K_p$ and $\alpha_{i1}-\alpha_{i2} \equiv 0 \bmod P_1$, it follows that $(\alpha_{i1}-\alpha_{i2})^2 \equiv 0 \bmod P$. Hence $v((\alpha_{i1}-\alpha_{i2})^2) \geqslant 1$. Thus (3) yields $v((\alpha_{i1}-\alpha_{i2})^2) = 1$ for $1 \leqslant i \leqslant m$. Therefore $K_p(\alpha_{11}-\alpha_{12})$ has ramification index 2 over K_p, and so $e(N_p/F_p)$ is even. □

3. F-admissibility

Let F be an algebraic number field.

A field extension N of F is *F-adequate* if it is the maximal subfield of a central division algebra over F.

A finite group G is *F-admissible* if it is the Galois group of an F-adequate Galois extension of F. The fundamental result needed to show F-admissibility is the following.

Theorem 2 (Schacher [S]). *G is F-admissible if and only if there exists a Galois extension N of F with Galois group G such that for each prime q there are at least two primes P of F so that the decomposition group at P contains a Sylow q-group of G.*

If the Sylow q-group of G is cyclic, in particular, if q does not divide the order of G, the Tchebotarev density Theorem asserts the existence of infinitely many primes at which the decomposition group contains a Sylow q-group of G. So it is sufficient to consider noncyclic Sylow groups. For instance $PSL(2,11)$ and $SL(2,11)$ have cyclic Sylow groups for all odd primes, so only the prime $q=2$ needs to be considered for these groups.

Using Theorem 2 and the 2-parameter family of polynomials $f(a,t,x)$ constructed by Malle, see, e.g., [F] or [M], it was shown in [F] that $PSL(2,11)$ is F-admissible for every algebraic number field F.

To show that $SL(2,11)$ is $\mathbb{Q}$-admissible it is necessary to construct some extensions of $\mathbb{Q}$ with Galois group $SL(2,11)$. The following result is relevant.

Theorem 3 (Böge, see [B] or [K]). *Let N be a Galois extension of $\mathbb{Q}$ with Galois group $PSL(2,11)$. N is embeddable into an extension with Galois group $SL(2,11)$ if and only if the following hold.*

(i) *N is totally real.*

(ii) *For all odd primes p with even ramification index we have that, p has odd residue class degree if and only if $p \equiv 1 \bmod 4$.*

Malle has observed that if $a = -5$ and $-716550 \leqslant t \leqslant -715599$ then $f(-5, t, x)$ is totally real [M]. This can be verified by using Sturm's Theorem. If we set $s = t + 716550$ then $g(s, x) = f(-5, s - 716550, x)$ is totally real for $0 \leqslant s \leqslant 951$. Furthermore,

$$\begin{aligned} g(s,x) \;=\; & x^{11} - 74x^{10} + 1979x^9 - 22442x^8 + 93623x^7 - 68118x^6 \\ & + (s - 512411)x^5 - (2s - 1249730)x^4 + (s - 231088)x^3 \\ & - 2273900x^2 + 2760000x - 1000000. \end{aligned} \tag{4}$$

Direct computation shows that

$$D\big(g(s,x)\big) = 2^{22}5^{14}h(s)^4$$

where

$$h(s) = 21357033124 + 28067951892s - 29543531s^2 + 27s^3.$$

Observe that if $s = u/v$ and $v \not\equiv 0 \bmod 3$ then $h(s) \equiv 1 + s^2 \not\equiv 0 \bmod 3$. Hence 3 does not divide $D(g(s, x))$.

Define the set

$$\begin{aligned} U = \{&26, 176, 191, 213, 263, 281, 288, 296, 321, 373, 421, 456, 463, 501, \\ &513, 548, 796, 823, 836, 863, 916, 928\}. \end{aligned}$$

For each $s \in U$, there are at least two prime divisors $p > 3$ of $h(s)$ with $p \equiv 3 \bmod 4$. Furthermore, each prime divisor of $D(g(s, x))$ greater than five has even ramification index by Theorem 1, and satisfies the conditions of Theorem 3. It is not known whether 5 ramifies for $s \in U$, however for each such s, 5 has odd residue class degree. Hence the conclusion of Theorem 3 shows that a splitting field N of $g(s, x)$ can be embedded in a Galois extension N_0 of $\mathbb{Q}$ with Galois group $SL(2, 11)$.

Let p be a prime, $p \equiv 3 \bmod 4$. As the residue class degree and ramification index are both even, the Sylow 2-group T of the inertia group of N is noncyclic of order 4. A Sylow 2-group of $SL(2, 11)$ is a quaternion group of order 8, and so cannot contain T, this implies that the inertia group of N_0 cannot have T as a Sylow 2-group and so must contain a Sylow 2-group of $SL(2, 11)$. Thus by Theorem 2, N_0 is $\mathbb{Q}$-adequate and $SL(2, 11)$ is $\mathbb{Q}$-admissible.

U consists of integers. However, it is possible to find values of s which are fractions and yield the same result. Here are some (randomly chosen) examples, $s = u/v$ with $u = 939$ and $v \in V$, where

$$V = \{2393, 2693, 3853, 5009, 6709, 8753, 9829, 10453, 10789, 11393\}.$$

The set V consists of primes $p \equiv 1 \bmod 4$. This is a convenience, not a necessity. If p is an odd prime which divides v to the first power, the Newton polygon of $g(939/v, x)$ at p is the convex hull of the set of points

$$\{(i,0) \mid i = 0,1,2\} \cup \{(i,-1) \mid i = 3,4,5\} \cup \{(i,0) \mid 6 \leqslant i \leqslant 11\},$$

and so the ramification index of every prime dividing v is odd, see for instance [W, Proposition 3.1.1]. There is nothing special about "939," various other values of u can be chosen to get similar results. Conceivably there are infinitely many such values of s with $0 \leqslant s \leqslant 951$.

4. Methods of proof

For $s \in U$ and p dividing $D(g(s,x))$, the greatest common divisor of $g(s,x)$ and $g'(s,x) \bmod p$ is a polynomial $g_0(x)$ of degree 4 with distinct roots mod p. Then

$$g(s,x) \equiv g_0(x)^2 g_1(x) \mod p$$

where $g_0(x)$ and $g_1(x)$ are relatively prime mod p and $g_1(x)$ also has distinct roots mod p. If $D(g_i(x))$ is not a square mod p for $i = 0$ or 1 then the Galois group of $g_i(x)$ contains an odd permutation and so contains an element of even order. The quadratic character of $D(g_i(x))$ can be computed in a fraction of a second by using the quadratic reciprocity theorem.

It can also be decided whether the residue class index is odd. This is so if and only if $D(g_0(x))$ and $D(g_1(x))$ are squares mod p and $g_0(x)$ has a root mod p (then $g_0(x)$ has exactly 1 or 4 roots mod p). It is unfortunately not sufficient to show that $D(g_0(x))$ is a square mod p, since the Galois group might contain a product of two disjoint transpositions.

The primes $p \equiv 1 \bmod 4$ which occur for s in U or V are quite small and a command in MATHEMATICA factors $g(s,x) \bmod p$ in a fraction of a second. This shows that the residue class index is odd in all these cases.

References

[B] S. Böge, Witt-Invariante und ein gewisses Einbettungsproblem, J. Reine Angew. Math. 410 (1990) 153–159.
[F] W. Feit, $PSL(2,11)$ is admissible for all number fields, to appear.
[K] J. Klüners, A polynomial with Galois group $SL(2,11)$, J. Symbolic Comput. 30 (2000) 733–737.
[M] G. Malle, Some multi-parameter polynomials with given Galois group, J. Symbolic Comput. 30 (2000) 715–729.
[S] M. Schacher, Subfields of division rings I, J. Algebra 9 (1968) 451–477.
[Sh] V. Shoup, A new polynomial factorization algorithm and its implementation, J. Symbolic Comput. 20 (1995) 363–397.
[W] E. Weiss, Algebraic Number Theory, McGraw–Hill, San Francisco, 1963.