DIVISION ALGEBRAS WITH $\mathrm{PSL}(2, q)$-GALOIS MAXIMAL SUBFIELDS

ELIZABETH S. ALLMAN AND MURRAY M. SCHACHER

Abstract. If G is a finite group and k is a field, then G is k-*admissible* if there exists a G-Galois extension L/k such that L is a maximal subfield of a k-division algebra. We prove that $\mathrm{PSL}(2, 7)$ is k-admissible for any number field which either fails to contain $\sqrt{-1}$ or which has two primes lying over the dyadic prime. In addition, $\mathrm{PSL}(2, 11)$ is shown to be admissible over $\mathbb{Q}$ or any number field k with at least two extensions of the dyadic prime. Indeed, there exist infinitely many linearly disjoint admissible extensions for these groups.

1. Introduction

A famous theorem of Albert-Brauer-Hasse-Noether states that every central simple algebra over a global field is a cyclic algebra. Thus every division algebra D over a global field has a cyclic Galois maximal subfield and D is a crossed product algebra for this cyclic group. This beautiful theorem leaves unexplored the structure of other subfields of D.

If G is a finite group and k is a field, then G is k-*admissible* if there exists a G-Galois extension L/k such that L is a maximal subfield of a k-division algebra. Interestingly, in [2], the authors prove that for a Galois extension of fields L/k, there exists a rational function field $K = k(t_1, \ldots, t_m)$ in m variables so that LK is a maximal subfield of a K-division algebra. In general, a sharp upper bound on the number of variables m needed is hard to determine. If k is a number field, the authors calculate a respectable upper bound determined from the lengths of minimal cyclic series for the Sylow subgroups of G. In particular, if $k = \mathbb{Q}$ and G is a Sylow metacyclic finite group that occurs as a Galois group over $\mathbb{Q}$, then $m = 1$. Thus, any such group is immediately admissible over $\mathbb{Q}(t)$. This leads to the strange conclusion that there are groups G that are known to be $\mathbb{Q}(t)$-admissible, but whose

The authors thank MSRI for office space, funding, and stimulating lectures during fall 1999 when the ideas in this article first arose. Murray Schacher gratefully acknowledges the support of NSA grant MDA 904-97-1-0060.

$\mathbb{Q}$-admissibility status is unknown. $\mathrm{PSL}(2,7)$ is the group of smallest order in this odd situation.

In this paper we show the $\mathrm{PSL}(2,7)$ is, indeed, admissible over the rational numbers and, more generally, admissible over any number field that fails to contain a square root of minus one or contains two primes lying over the dyadic prime. Since the 2-Sylow subgroup of $\mathrm{PSL}(2,7)$ is the dihedral group of order eight, D_8, it is natural that the conditions on a number field k so that $\mathrm{PSL}(2,7)$ is k-admissible are precisely the same as for the admissibility of $\mathrm{SL}(2,5)$, A_6, and A_7, [3], [12]. We prove additionally that $\mathrm{PSL}(2,11)$ is admissible over $\mathbb{Q}$ and are indebted to Walter Feit for extending this result to show that $\mathrm{PSL}(2,11)$ is admissible for a certain class of number fields k. We conjecture that $\mathrm{PSL}(2,11)$ is admissible over any number field k.

There are two well-known approaches to proving that a finite group is admissible. In [10], Saltman proves that if a finite group has a generic extension then it is possible to solve local to global lifting problems. As a result, if certain local conditions are met and a group G has a generic extension over k, then G is k-admissible. Unfortunately, it is quite difficult to prove the existence of a generic extension.

The other tack is to find explicit polynomials, usually with parameters, and argue that it is possible to specialize these parameters in such a way that certain arithmetic criteria are met and the Galois group $G \cong \mathrm{Gal}(f(x)/k)$ is, in fact, admissible over k. This method is more concrete, but it requires methods for realizing Galois groups over fields such as $\mathbb{Q}(t)$. The difficulty is that $\mathrm{PSL}(2,7)$ has not been realized as a Galois group over $\mathbb{Q}$ very often and $\mathrm{PSL}(2,11)$ even less so.

The earliest example of a $\mathrm{PSL}(2,7)$-polynomial is attributed to Trinks [14] in 1968 in his unpublished thesis: $x^7 - 7x + 3$. Another such trinomial, $x^7 - 154x + 99$, was given by Erbach, Fisher, and McKay [1] in 1979. LaMacchia [5] in 1980 is the first to give a family of polynomials in two parameters that have Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(t_1,t_2)$. Just recently, in 1999, Smith [13] gave a new family of polynomials with Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(t)$. With a bit of effort, it is possible to extend Smith's result to a family with Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(t_1,t_2)$. Examples of $\mathrm{PSL}(2,11)$-Galois polynomials are given by LaMacchia, Malle-Matzat, and Ward [6], [8], [13].

In [11], Schacher gives an arithmetic criterion for a finite group to be k-admissible over a number field k.

Proposition 1. [11] *A finite group G is k-admissible if and only if there is a G-Galois extension L/k such that for each prime p dividing*

$[L : k]$ *there are at least two primes* $\mathfrak{p}$ *of* k *such that the decomposition group* $\mathrm{Gal}(L_{\mathfrak{p}}/k_{\mathfrak{p}})$ *contains a* p*-Sylow subgroup of* G.

Unfortunately, the polynomials above fail the test for admissibility.

Recently, however, G. Malle has given multi-parameter families of polynomials with Galois groups $\mathrm{PSL}(2,7)$ and $\mathrm{PSL}(2,11)$ over $\mathbb{Q}(t_1, \ldots, t_n)$. These polynomials provide a proof of admissibility.

We used the software packages Maple V and GP/Pari in our investigations. Pari sports an impressive list of number theoretic functions and we used it to factor polynomials p-adicly.

In this paper, a $\sqrt{-1}$*-free field* means a number field k not containing a square root of minus one; $\sqrt{-1} \notin k$. By *infinitely often*, we mean there exists a sequence of fields $L_1, \ldots, L_n, \cdots$ with L_{n+1} disjoint from the compositum of the first n. For example, Hilbert's existence theorem states that any finite group is realizable as a Galois group over $\mathbb{C}(t)$ infinitely often. We write $\mathrm{PSL}(2,q)$ to refer to $\mathrm{PSL}(2,7)$ and $\mathrm{PSL}(2,11)$ simultaneously. Finally, $\mathfrak{O}_k$ denotes the ring of integers in a number field k and k_p the completion of k at a prime p.

2. Preliminaries

We begin by recording some results of Malle.

Proposition 2 (Malle [7]). *The polynomials*

$$\begin{aligned} f_2(a,b,t,x) =&(x^4 - 2(b+2)x^2 + 4bx - a)(x^3 + 2(b-1)x^2 \\ &+ (a + b^2 - 4b)x - 2a) + tx^2(x-2) \end{aligned}$$

and

$$\begin{aligned} f_3(a,b,c,t,x) &= x^7 - ((c-2)a + 2b + c)x^6 + (-(b-4)(c-1)a^2 \\ &+ ((c-2)b^2 + (2c^2 - 5c + 4)b - 2c^2)a + b(2bc + 2c^2 + b^2))x^4 \\ &+ ((2c^2 - 1)(b-4)a^2 + ((-2c^2 + c + 2)b^2 + (5c^2 + 2c - 4)b - 4c^2)a \\ &- (c+1)b^3 - c(2c+3)b^2 + c^2 b)x^3 + ((c^2 + 3c - 1)(4-b)a^2 \\ &+ ((3c-2)b^2 - 2(c^2 + 4c - 2)b + 4c^2)a + b(b^2 + 3bc - c^2))cx^2 \\ &+ (2abc - 8ac + ab - 4a - b^2 + 2bc)ac^2 x - a^2(b-4)c^3 \\ &+ tx^2(x-c)(x^2 - bx + b) \end{aligned}$$

have Galois group $\mathrm{PSL}(2,7)$ *over* $\mathbb{Q}(a,b,t)$ *and* $\mathbb{Q}(a,b,c,t)$ *respectively.*

In addition, the polynomial

$$\begin{aligned} f(a,t,x) = {} & (x^5 + 2(a-4)x^4 - 4(a-5)x^3 - 2(a^2-3a+8)x^2 \\ & + (2a-1)^2x - 2a^2)(x^6 + 2(-3+5a)x^5 + (32a^2-24a+11)x^4 \\ & + 2(16a^3+15a^2+9a-4)x^3 + 2(2a+1)(20a^2-4a+1)x^2 \\ & - 16a^2(2a^2+7a+2)x + 32a^4) + t(x^3)(x-1)^2 \end{aligned}$$

has Galois group $\mathrm{PSL}(2,11)$ *over* $\mathbb{Q}(a,t)$.

We quote an additional result of Malle that is used to verify the calculation of the Galois groups of multi-parameter polynomials. The reader is directed to [9] for more details.

Lemma 1 (Malle [7]). *Let k be a field of characteristic zero and $f(t_1,\ldots,t_n,t)(x) \in k(t_1,\ldots,t_n,t)[x]$ absolutely irreducible. Assume that $k(t_1,\ldots,t_n)$ is algebraically closed in the splitting field of f. Let $a_1,\ldots,a_n \in k$ such that the stem fields of $f(t_1,\ldots,t_n,t)(x)$ over $k(t_1,\ldots,t_n,t)$ and of $f(a_1,\ldots,a_n,t)(x)$ over $k(t)$ have the same number of ramification points with respect to t. Then the Galois groups of*

$$f(t_1,\ldots,t_n,t)(x) \quad \textit{and} \quad f(a_1,\ldots,a_n,t)(x)$$

coincide.

One practical consequence of this lemma is that after specializing $t_1,\ldots,t_n$ to elements of a field k, the Galois group of $f(a_1,\ldots,a_n,t,x)$ over $k(a_1,\ldots,a_n,t)$ remains unchanged, provided the discriminant of f, a polynomial in t, has the same degree in t as it did prior to the specialization.

We exploit the geometric nature of the Galois groups to prove that $\mathrm{PSL}(2,q)$ is admissible. Indeed, we prove the remarkable result that if $\mathrm{PSL}(2,q)$ is admissible for some specialization of the parameters $t_1,\cdots,t_n$, then $\mathrm{PSL}(2,q)$ is admissible infinitely often. With this proposition in hand, our job remains to exhibit explicit admissible polynomials.

Proposition 3. *Let $f(t_1,\ldots,t_n,x) \in k(t_1,\ldots,t_n)[x]$ be a polynomial with geometric Galois group G over $k(t_1,\ldots,t_n)$, k a number field. Suppose that for the specializations $t_1 \to a_1,\cdots,t_n \to a_n$ with $a_i \in k$, the polynomial $f(a_1,\ldots,a_n,x)$ is k-admissible with Galois group G. Then the field k has infinitely many linearly disjoint G-admissible field extensions.*

Proof. Only the induction step needs to be proved. Let K be the compositum of disjoint k-admissible fields $K_1,\ldots,K_n$, each with Galois group G. Then $\mathrm{Gal}(K/k) \cong G^n$ and by Hilbert's Existence theorem, there exists a new extension L/k with Galois group G that is linearly disjoint from K. Let $a_i' \in k$ denote the specializations so that L is the splitting field of the polynomial $f(a_1', \dots, a_n', x)$.

For each non-trivial Sylow subgroup S of G, choose two primes q_1, q_2 of k such that S occurs as a subgroup of the local Galois group of $f(a_1, \dots, a_n, x)$ over k_{q_j}, $j = 1, 2$. For each proper subgroup H of G, fix a prime $\mathfrak{p}$ of K that does not split completely in KL^H and let p be the restriction of $\mathfrak{p}$ to k. We may assume that p is distinct from the previously chosen primes. Let $q_1, \dots, q_r, p_1, \dots, p_s$ be a complete list of these primes of k. By repeated use of the Chinese remainder theorem, we can choose elements $b_1, \cdots, b_n \in k$ so that for each $i = 1, \dots, n$,

$$
\begin{aligned}
b_i &\equiv a_i \bmod (q_j)^m, \quad j = 1, \dots r \\
b_i &\equiv a_i' \bmod (p_j)^m, \quad j = 1, \dots s
\end{aligned}
$$

where m is a large positive integer. Indeed, choose m so large that $f(b_1, \dots, b_n, x)$ determine the same splitting fields over the k_{q_j} and k_{p_j} as $f(a_1, \dots, a_n, x)$ and $f(a_1', \dots, a_n', x)$ respectively. Let K_{n+1} be the splitting field of $f(b_1, \dots, b_n, x)$ over k.

Since $f(b_1, \dots, b_n, x)$ is a specialization of a geometric polynomial with Galois group G and each Sylow subgroup of G occurs as a local Galois group, the Galois group of K_{n+1}/k is the full group G. Moreover, by construction, K_{n+1} is k-admissible since the b_i were chosen so that each Sylow subgroup S of G occurs locally over two primes of k. Suppose now, for the sake of contradiction, that K_{n+1} is not linearly disjoint from K. Then $K \cap K_{n+1} = (K_{n+1})^H$ for some proper subgroup H of G. Let p be the prime of k that corresponds to H from above. Since K is normal, K_p must be the splitting field of $(K_{n+1})_p^H$. But this is impossible since $f = f(a_1', \dots, a_n', x)$ and $f(b_1, \dots, b_n, x)$ are close p-adicly and p was chosen so that f did not split in K_p. $\square$

3. PSL$(2,7)$-Galois Maximal Subfields

In this section, we prove the main theorem for PSL$(2,7)$: if k is a number field satisfying one of the following:

(1) k is a $\sqrt{-1}$-free field or
(2) $\sqrt{-1} \in k$ and the rational prime (2) has at least two extensions in k,

then there are infinitely many crossed product k-division algebras with Galois group PSL$(2,7)$. In fact, these conditions are necessary and sufficient. We give the proof in two parts: we employ the family of polynomials f_3 to argue for $\sqrt{-1}$-free number fields and the polynomials f_2 in the remaining case.

We thank Malle who, in personal communications, kindly shared details of the proof of Proposition 2 by supplying a rational change of variable $t = \frac{g(Y)}{h(Y)}$ so that f_3 factored as a product of a cubic and quartic polynomial. Our goal is to determine a choice of parameters a, b, c, t maintaining $\mathrm{PSL}(2,7)$ as the Galois group of f_3 while requiring that D_8 is contained as a subgroup of two local Galois groups. We present the choice of parameters as a fait-accompli; however, we comment that hours of Maple computations were necessary to discover the right choice. Since our polynomials are specializations of Malle's polynomial $f_3(a,b,c,t,x)$, it is necessary to prove that our polynomials retain $\mathrm{PSL}(2,7)$ as their Galois group. We do this in a series of lemmas.

Lemma 2. *In the Malle polynomial $f_3(a,b,c,t,x) \in \mathbb{Q}(a,b,c,t)[x]$, set $t = \left(\frac{b(592-552b+549b^2)}{12(4+3b)^2} + ub\right)$. Then the resulting polynomial $f_3(a,b,c,u,x)$ has Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(a,b,c,u)$.*

Proof. The substitution $t = \left(\frac{b(592-552b+549b^2)}{12(4+3b)^2} + ub\right)$ is an invertible change of variable. By Proposition 2, $\mathrm{PSL}(2,7)$ remains the Galois group. $\square$

We next prove that for particular specializations of the parameters a, b, c the resulting polynomial $f_3(u,x)$ has Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(u)$.

Lemma 3. *For $a = b$, $b \neq 0$ or 4, and $c = 1$, the polynomials $f_3(u,x)$ have Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(u)$.*

Proof. The polynomial $f_3(a,b,c,u,x)$ over $\mathbb{Q}(a,b,c,u)$ has six ramification points with respect to u. After making the prescribed specializations for a and c, the leading term of the discriminant of f_3 with respect to u is $16b^{16}(b-4)^2u^{10}$. The leading term does not disappear for any choice of $b \neq 0$ or 4. Thus, $f_3(u,x)$ over $\mathbb{Q}(u)$ and $f_3(a,b,c,u,x)$ over $\mathbb{Q}(a,b,c,u)$ both have six ramification points including infinity with respect to u. By Lemma 1, $f_3(u,x)$ has Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(u)$. $\square$

Remark. Malle's proof ([7], Theorem 4.3) is more general than the current setup; he argues that $f_3(a,b,c,t,x)$ has Galois group $\mathrm{PSL}(2,7)$ over $\mathbb{Q}(a,b,c,t)$. His argument can be adapted to give an alternative proof that $\mathrm{PSL}(2,7)$ remains the Galois group of $f_3(u,x)$ with the particular choice of parameters above. The polynomial $f_3(u,x)$ is irreducible since if we set $b = 1$ and $u = 1$, the resulting polynomial is irreducible mod 11. Setting $u = 0$, f_3 factors as the product of an irreducible cubic and an irreducible quartic. Thus, the Galois group of $f_3(u,x)$ has a subgroup of index 7 with orbits of length 3 and 4 on the seven points and has group order divisible by $3 \cdot 4 \cdot 7$. PSL$(2,7)$ is the only such transitive subgroup of S_7.

Proposition 4. *(Statement over $\mathbb{Q}$.) Suppose b is exactly divisible by two distinct primes, both greater than 3 and congruent to $3 \bmod 4$. Then for $a = b$, $c = 1$, the polynomials $f_3(u,x)$ are $\mathbb{Q}$-admissible for any choice of u in the Hilbert set of f_3.*

Proof. The order of PSL$(2,7)$ is 168, $|\operatorname{PSL}(2,7)| = 168 = 2^3 \cdot 3 \cdot 7$ and the only non-cyclic Sylow subgroup of PSL$(2,7)$ is the 2-Sylow subgroup D_8. By density considerations, the cyclic 3- and 7-Sylow subgroups of PSL$(2,7)$ occur as local Galois groups over an infinite number of primes of k. Thus, by Proposition 1, it suffices to show that the dihedral group D_8 is contained as a subgroup of the local Galois group G_p for at least two rational primes p.

For the choice of parameters $a = b$, $c = 1$, the polynomial $f_3 = f_3(b,u,x) = f_3(u,x)$ is:

$$\begin{aligned} f_3(u,x) = x^7 &- (b+1)x^6 + ((-b^2+b-2)b + b(2b+2+b^2))x^4 \\ &+ ((b-4)b^2 + (b^2+3b-4)b - 2b^3 - 5b^2 + b)x^3 \\ &+ (3(4-b)b^2 + (b^2-6b+4)b + b(b^2+3b-1))x^2 \\ &+ (2b^2 - 10b)bx - (b-4)b^2 \\ &+ tx^2(x-1)(x^2-bx+b), \end{aligned}$$

with $t = \left(\frac{b(592-552b+549b^2)}{12(4+3b)^2} + ub\right) = b\left(\frac{(592-552b+549b^2)}{12(4+3b)^2} + u\right)$

Expanding, we have:

$$\begin{aligned} f_3(u,x) = x^7 &+ (-b-1)x^6 + tx^5 + (-t - tb + 3b^2)x^4 \\ &- b(-2t+6b+3)x^3 - b(-9b+b^2-3+t)x^2 \\ &+ 2b^2(b-5)x - (b-4)b^2 \end{aligned}$$

and $f_3(u,x)$ has Galois group PSL$(2,7)$ over $\mathbb{Q}(u)$ by Lemma 3.

Let p_1, p_2 be distinct rational primes satisfying the hypotheses of the proposition. In examining the coefficients of f_3, we find that the Newton polygon of f_3 at p_j, $j = 1,2$, consists of segments joining $(0,2)$, $(2,1)$, $(6,0)$ and $(7,0)$. Thus, over the local field $\mathbb{Q}_{p_j}$, f_3 must factor as the product of a quadratic, a quartic, and a linear polynomial.

Moreover, since the slope of the segment corresponding to the quartic polynomial q is $\frac{-1}{4}$, the splitting field of q must be ramified with $4 \mid e$.

Adjoining a root of q to the local field $\mathbb{Q}_{p_j}$ gives rise to a totally and tamely ramified extension k_{p_j}; specifically, k_{p_j} is obtained by adjoining a fourth root of a prime element of $\mathbb{Q}_{p_j}$. Since $\sqrt{-1} \notin \mathbb{Q}_{p_j}$, the splitting field of q over $\mathbb{Q}_{p_j}$ is $k_{p_j}(i)$ and q has Galois group D_8 over $\mathbb{Q}_{p_j}$. By Proposition 1, $\mathrm{PSL}(2,7)$ is $\mathbb{Q}$-admissible for any u in the Hilbert set of $f_3(u,x)$. $\square$

We pause at this time to give an example of a $\mathbb{Q}$-admissible polynomial f_3. If we take $b = 7 \cdot 11$ and $u = 1$, then the specialized polynomial

$$f_3(7\cdot 11, x) = x^7 - 78x^6 + 17787x^4 - 35805x^3 - 402941x^2 + 853776x \\ - 432817 + \frac{298437293}{662700}x^2(x-1)(x^2-77x+77)$$

is $\mathrm{PSL}(2,7)$-Galois and $\mathbb{Q}$-admissible.

The previous result extends seamlessly to $\sqrt{-1}$-free number fields.

Proposition 5. *Suppose k is a number field and $\sqrt{-1} \notin k$. Then $\mathrm{PSL}(2,7)$ is k-admissible.*

Proof. By the Chebotarev density theorem, there are infinitely many primes $\mathfrak{p}_j$ of k that remain inertial in the extension $k(i)$ of k. Choose two of these primes $\mathfrak{p}_j$, $j = 1, 2$, that are unramified over $\mathbb{Q}$. Then, if p_j is the contraction of $\mathfrak{p}_j$ to $\mathbb{Z}$, $p_j \equiv 3 \bmod 4$ and we may assume $p_j > 3$. For $p_j \mid b$, let $f_3(b,x)$ be a $\mathbb{Q}$-admissible polynomial arising from Proposition 4 whose splitting field over $\mathbb{Q}$ is linearly disjoint from k. Such a polynomial exists by Proposition 3. Since $k_{\mathfrak{p}_j}$ is an unramified extension of $\mathbb{Q}_{p_j}$, the Newton polygon of f_3 at $\mathfrak{p}_j$ shows that the splitting field of f_3 over $k_{\mathfrak{p}_j}$ is ramified with $4 \mid e$. Since $\sqrt{-1} \notin k_{\mathfrak{p}_j}$, the local Galois groups $G_{\mathfrak{p}_j}$ contain D_8 as a subgroup and f_3 is k-admissible. By Hilbert irreducibility, $\mathrm{PSL}(2,7)$ is k-admissible for any u in the Hilbert set of f_3 over k. $\square$

Next we show that $\mathrm{PSL}(2,7)$ is k-admissible over number fields that have two extensions over the rational prime (2). For this we use an elementary exercise from [4], p. 53.

Lemma 4. *Let $g(x) = x^4 + px^2 + q$ be irreducible over a field K of characteristic different from 2. If neither q nor $q(p^2 - 4q)$ is a square in K, then the Galois group of $g(x)$ is the dihedral group of order 8, D_8.*

We apply Lemma 4 in the following situation:

Lemma 5. *Suppose k is a number field and the rational prime (2) has two extensions $\mathfrak{p}_1$, $\mathfrak{p}_2$ in k. Then there exists an element $a \in \mathfrak{O}_k$ such that $g(x) = x^4 - 4x^2 - a$ has Galois group D_8 over the complete fields k_{p_j}, $j = 1, 2$.*

Proof. For $j = 1, 2$, let s_j be the valuation of 2 at $\mathfrak{p}_j$, $\nu_{\mathfrak{p}_j}(2) = s_j$, and suppose $a_j \in \mathfrak{p}_j^{2s_j+1} \setminus \mathfrak{p}_j^{2s_j+2}$. By the Chinese Remainder theorem, there exists an $a \in k$ such that $a \equiv a_j \bmod \mathfrak{p}_j^{2s_j+2}$. Notice that $\nu_{\mathfrak{p}_j}(-a) = 2s_j + 1$ and $\nu_{\mathfrak{p}_j}(-4) = 2s_j$. Since $s_j > 0$, the Newton polygon of $g(x)$ consists of a single segment joining $(0, 2s_j + 1)$ to $(4, 0)$ and $g(x)$ is irreducible. Since the valuation $\nu_{\mathfrak{p}_j}(-a)$ is odd, $-a$ is not a square in k_{p_j}. The valuation $\nu_{\mathfrak{p}_j}(-a(16 + 4a)) = \nu_{\mathfrak{p}_j}(-4a(4 + a))$ is equal to $6s_j + 1$ and so $-a(16 + 4a)$ is not a square in k_{p_j}. Lemma 4 completes the proof. ☐

Proposition 6. *Suppose k is a number field satisfying $\sqrt{-1} \in k$ and the rational prime (2) has at least two extensions $\mathfrak{p}_1$, $\mathfrak{p}_2$ in k. Then* PSL$(2, 7)$ *is k-admissible.*

Proof. Let $r \in (\mathfrak{p}_1\mathfrak{p}_2)^n$ where n is a large positive integer whose value will be determined later. In the polynomial f_2, set $t = ur$ where u is a new indeterminate. Note that $f_2(a, b, t, x)$ and $f_2(a, b, u, x)$ have the same Galois group over the fields $k(a, b, t)$ and $k(a, b, u)$ respectively, since $t \to ur$ is a rational change of variable.

Let $a_k \in \mathfrak{O}_k$ be an element satisfying Lemma 5 and let $b_k \in \mathfrak{O}_k$ be an element satisfying

$$b_k \equiv 0 \bmod (\mathfrak{p}_1\mathfrak{p}_2)^n.$$

We argue that $f_2(a_k, b_k, u, x)$ is k-admissible with Galois group PSL$(2, 7)$ for any u in the Hilbert set of f_2.

The discriminant of $f_2(a, b, u, x)$ is a polynomial in u with leading term $l = 16384a^2r^8u^8$ of degree 8. Since l does not vanish under the specializations $a \to a_k$ and $b \to b_k$, the Galois group of $f_2(a_k, b_k, u, x)$ is PSL$(2, 7)$ over $k(u)$ by Lemma 1.

Since the Hilbert sets of a number field k contain arithmetic progressions, there is a $u_k \in \mathfrak{O}_k$ such that $f_2(a_k, b_k, u_k, x)$ is PSL$(2, 7)$-Galois over k. If we take $n \in \mathbb{Z}$ large enough, then b_k and $u_k r$ are so close to 0 in the p-adic topologies that, by Krasner's Lemma, $f_2(a_k, b_k, u_k, x)$ and $(x^4 - 4x^2 - a_k)(x^3 - 2x^2 + a_k x - 2a_k)$ determine the same splitting field over k_{p_j}, $j = 1, 2$. By Lemma 5, $x^4 - 4x^2 - a_k$ has Galois group D_8 over the local field k_{p_j}. We conclude that PSL$(2, 7)$ is k-admissible. ☐

We now prove the main theorem:

Theorem 1. *Suppose k is a number field satisfying one of the following:*

(1) k is a $\sqrt{-1}$-free field or

(2) $\sqrt{-1} \in k$ and the rational prime (2) has at least two extensions in k

then $\mathrm{PSL}(2,7)$ *is k-admissible infinitely often. The converse holds also: if* $\mathrm{PSL}(2,7)$ *is k-admissible, then k is a number field satisfying (1) or (2) above.*

Proof. If k is a number field satisfying the hypotheses of the theorem, then there exist infinite many linearly disjoint $\mathrm{PSL}(2,7)$-admissible extensions by combining the results of Propositions 3, 4, 5, and 6.

For the converse, we remark that it is well known that the 2-Sylow subgroup of $\mathrm{PSL}(2,7)$, D_8, is realizable as a Galois group over at least two complete local fields k_{p_j} if and only if k satisfies (1) or (2) above [12]. All other p-Sylow subgroups of $\mathrm{PSL}(2,7)$ are cyclic. $\square$

4. $\mathrm{PSL}(2,11)$-Galois Maximal Subfields

We next consider the simple group $\mathrm{PSL}(2,11)$.

Theorem 2. *The group* $\mathrm{PSL}(2,11)$ *is $\mathbb{Q}$-admissible infinitely often.*

Proof. Let $f(a,t,x)$ be the polynomial with Galois group $\mathrm{PSL}(2,11)$ from Proposition 2. By Proposition 3, it is enough to find explicit specializations of a and t into the rational numbers so the resulting polynomial is $\mathbb{Q}$-admissible with Galois group $\mathrm{PSL}(2,11)$. To this end, set $a = t = 7776 = 2^5 \cdot 3^5$. Then

$$\begin{aligned} f(x) = x^{11} &+ 93298x^{10} + 3143308111x^9 + 45118654799960x^8 \\ &+ 233870049535820927x^7 - 233949029487266662x^6 \\ &- 363906143256326155095 7x^5 + 4548522834423181952600x^4 \\ &+ 14153280659533276298981858x^3 - 4245438150379723790503526 4x^2 \\ &+ 4244892224502288821413478 4x - 14148730862126934905585664. \end{aligned}$$

The discriminant of $f(x)$ is a huge integer that is divisible by $2^{104} \cdot 3^{82}$. Over the local fields $\mathbb{Q}_2$ and $\mathbb{Q}_3$, $f(x)$ has an irreducible quartic factor. This was verified using Pari's number theoretic function *factorpadic* with a degree of precision 120. (The precision level of 120 was chosen somewhat arbitrarily; we just needed a level greater than the degree of the prime 2 dividing the discriminant.)

The order of $\mathrm{PSL}(2,11)$ is $|\mathrm{PSL}(2,11)| = 660 = 2^2 \cdot 3 \cdot 5 \cdot 11$ and the 2-Sylow subgroup is the Klein 4-group V_4. Since $f(x)$ has an irreducible quartic factor 2- and 3-adicly, the local Galois groups have order divisible by 4. In addition, this means the group order of $G = \mathrm{Gal}(f(x)/\mathbb{Q})$

is divisible by 4. If we factor $f(x)$ mod the primes 7, 11, and 19, then $f(x)$ has factors of order 11, 5 and 3 respectively. We conclude that the Galois group G is a subgroup of $\mathrm{PSL}(2,11)$ that is divisible by $2^2 \cdot 3 \cdot 5 \cdot 11$ and must be the full group $\mathrm{PSL}(2,11)$. By Proposition 1, $\mathrm{PSL}(2,11)$ is $\mathbb{Q}$-admissible. $\square$

Recently, Walter Feit has pointed out a simplification of our argument above. His argument has the advantage that it generalizes to a class of number fields k. We thank him for suggesting the proofs below.

Example. In the $\mathrm{PSL}(2,11)$-Galois polynomial $f(a,t,x)$, set $a = 72$ and $t = 36$. The resulting polynomial $f(x)$ is $\mathbb{Q}$-admissible.

Proof. With the choice of parameters above, we have

$$\begin{aligned} f(x) = {} & x^{11} + 850x^{10} + 261007x^9 + 34226696x^8 + 1624602047x^7 \\ & - 1686352102x^6 - 246915510409x^5 + 306018599936x^4 + 9233249273030x^3 \\ & - 27312858540288x^2 + 26936633327616x - 8916100448256. \end{aligned}$$

$f(x)$ has an irreducible factor of degree 4 over the local fields $\mathbb{Q}_2$ and $\mathbb{Q}_3$. Thus, the Galois group G of $f(72,36,x)$ is a subgroup of $\mathrm{PSL}(2,11)$ with order divisible by $44 = 4 \cdot 11$ and if $G \cong \mathrm{PSL}(2,11)$, then $\mathrm{PSL}(2,11)$ is $\mathbb{Q}$-admissible. Since the normalizer of an 11-Sylow subgroup of $\mathrm{PSL}(2,11)$ has order 55, any subgroup of G of order divisible by 44 must be the full group $\mathrm{PSL}(2,11)$. $\square$

Remark. Feit argues that the local degrees over $\mathbb{Q}_2$ and $\mathbb{Q}_3$ are divisible by 4, without using Pari, as follows: after making the variable substitution $x = y + 1$ in $f(72,36,x)$, a Newton polygon shows that the splitting field of $f(72,36,x)$ over $\mathbb{Q}_2$ has ramification index divisible by 4. Factoring $f(72,36,x) \bmod 3$ shows that the residue class degree over $\mathbb{Q}_3$ is divisible by 2. Suppose u generates the unramified quadratic extension of $\mathbb{Q}_3$; specifically, u satisfies $u^2 - u - 1 = 0$. Let $g(y) = f(72,36,y+u)$. Examining the coefficients mod 9 gives:

$$g(y) = y^{11} + \cdots + (4+5u)y^3 + (3+6u)y^2 + (3+6u)y,$$

and the Newton polygon of $g(y)$ has a segment joining $(1,1)$ to $(3,0)$. Thus, the ramification index over $\mathbb{Q}_3(u)$ is divisible by 2. We conclude that the local degree of the splitting field of $f(72,36,x)$ over $\mathbb{Q}_3$ is divisible by 4, as desired.

Feit uses the same variable substitution $x \to y + 1$ to argue, more generally, that $\mathrm{PSL}(2,11)$ is admissible over any number field in which the prime (2) has at least two extensions. We supply the details in the following theorem.

Theorem 3. *Suppose k is a number field and the rational prime* (2) *has at least two extensions in k. Then* PSL(2, 11) *is k-admissible infinitely often.*

Proof. Let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be distinct primes of $\mathfrak{O}_k$ lying over (2) with uniformizing parameters π_1, π_2. Let $f(a,t,x)$ be the PSL(2, 11)-Galois polynomial of Proposition 2 and set $a = 2$. If we make the substitution $x = y + 1$ and examine the coefficients mod 4, we find

$$f(2,t,y) = y^{11} + \cdots + \\ y^6 + (t+2)y^5 + (3t+2)y^4 + (3t+2)y^3 + (t+2)y^2 \mod 4.$$

If the prime (2) is unramified in k, set $t = 4u$ where u is a new indeterminate. If (2) ramifies in k, set $t = \pi_1\pi_2 + 4u$ with u a new indeterminate. With these choices for t, the Newton polygon of $f(2,t,y)$ has a segment of length 4 and the ramification index at $\mathfrak{p}_j$ is divisible by 4. Thus, if u is any integer in the Hilbert set of $f(2,t,y) = f(2,4u,y)$, then PSL(2, 11) is k-admissible. Since Hilbert sets contain arithmetic progressions, such a $u \in \mathfrak{O}_k$ exists. By Proposition 3, PSL(2, 11) is k-admissible infinitely often. □

5. Reflections

We strongly suspect that PSL(2, 11) is admissible for any number field k. All our investigations suggest this and we can give busloads of explicit examples of PSL(2, 11)-admissible polynomials. However, the general proof eludes us at this time.

The interesting question of the existence of a generic extensions for PSL(2, 7) and PSL(2, 11) remains open. We hope it is settled soon.

Elizabeth S. Allman
Department of Mathematics
University of Southern Maine
eallman@usm.maine.edu

Murray M. Schacher
Department of Mathematics
UCLA
mms@math.ucla.edu

References

1. D. Erbach, J. Fisher, and J. McKay, *Polynomials with $PSL(2,7)$ as Galois group*, J. Number Theory **11** (1979), no. 1, 69 – 75.
2. B. Fein, D. Saltman, and M. Schacher, *Crossed products over rational function fields*, J. Algebra **156** (1993), no. 2, 454 – 493.
3. P. Feit and W. Feit, *The K-admissibility of $SL(2,5)$*, Geom. Dedicata **36** (1990), no. 1, 1 – 13.
4. I. Kaplansky, *Fields and rings*, Chicago lectures in mathematics, University of Chicago Press, 1969.
5. S. LaMacchia, *Polynomials with Galois group $PSL(2,7)$*, Comm. Algebra **8** (1980), no. 10, 983 – 992.
6. ______, *Polynomials with Galois group $PSL(2,11)$*, Comm. Algebra **9** (1981), no. 6, 613 – 625.
7. G. Malle, *Some multi-parameter polynomials with given Galois group*, J. Symbolic Comput., to appear.
8. G. Malle and B. H. Matzat, *Realisierung von Gruppen $PSL_2(F_p)$ als Galoisgruppen uber $\mathbb{Q}$*, Math. Ann. **272** (1985), no. 4, 549 – 565.
9. ______, *Inverse Galois theory*, Springer-Verlag, Berlin, 1999.
10. D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. in Math. **43** (1983), no. 3, 250 – 283.
11. M. Schacher, *Subfields of division rings, I*, J. Algebra **9** (1968), 451 – 477.
12. M. Schacher and J. Sonn, *k-admissibility of A_6 and A_7*, J. Algebra **145** (1992), no. 2, 333–338.
13. G.W. Smith, *Some polynomials over $\mathbb{Q}(t)$ and their Galois groups*, Math. Comp. **69** (2000), no. 230, 775 – 796.
14. W. Trinks, *Ein Beispiel eines Zahlkorpers mit der Galoisgruppe $PGL(3,2)$ uber $\mathbb{Q}$*, manuscript Univ. Karlsruhe, 1968.
15. E. Weiss, *Algebraic number theory*, Chelsea Publishing Company, New York, 1963.