ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 141–156

THE K-ADMISSIBILITY OF $2A_6$ AND $2A_7$

BY

WALTER FEIT

Department of Mathematics, Yale University
Box 2155—Yale Station, New Haven, CT 06520, USA

Dedicated to John Thompson to celebrate his Wolf Prize in Mathematics 1992

ABSTRACT

Let K be a field and let G be a finite group. G is K-admissible if there exists a Galois extension L of K with $G = \mathrm{Gal}(L/K)$ such that L is a maximal subfield of a central K-division algebra. This paper contains a characterization of those number fields which are Q_{16}-admissible. This is the same class of number fields which are $2A_6 = \mathrm{SL}(2,9)$ and $2A_7$ admissible.

1. Introduction

Let L be a finite extension field of the field K; L is K-**adequate** if L is a maximal subfield of a division algebra with center K.

A finite group G is K-**admissible** if $G \simeq \mathrm{Gal}(L/K)$ for some K-adequate Galois extension L of K.

The main result of [3] states that if H is any subgroup of $\mathrm{SL}(2,5)$ which contains a S_2-group, and K is a number field, then H is K-admissible if and only if either $\sqrt{-1} = i \notin K$ or K has at least 2 places over the prime 2. In [6] the same conditions were shown to characterize the number fields K for $H = A_6, A_7$ or D_8, the dihedral group of order 8, to be K-admissible. In this paper we will consider number fields K which satisfy

(*) *Either i and $\sqrt{-2}$ are both not in K or K has at least 2 places over the prime 2.*

The purpose of this paper is to prove the next result.

Received July 9, 1992 and in revised form January 31, 1993

THEOREM A: *Let K be an algebraic number field. The following are equivalent.*

(i) *Q_{16}, the quaternion group of order 16, is K-admissible.*

(ii) *$2A_6 \simeq \mathrm{SL}(2,9)$, the double cover of A_6, is K-admissible.*

(iii) *The double cover $2A_7$ of A_7 is K-admissible.*

(iv) *Condition (*) is satisfied.*

In an earlier paper [2] it was shown that $2A_6$ and $2A_7$ are $\mathbf{Q}$-admissible. This result is of course subsumed under Theorem A, though a different construction was used in [2].

All of these results are initially based on Schacher's criterion [5] which asserts that a number field L is K-adequate if and only if every Sylow group of $\mathrm{Gal}(L/K)$ is contained in the decomposition group for at least 2 places of K. By the Tchebotarev density theorem, only noncyclic Sylow groups need to be considered. Then Mestre's Theorem [4] is used to construct suitable polynomials. The third key result is Serre's Theorem [7], which makes it possible to consider double covers. All of these statements are summarized in [3].

It is not easy to construct a polynomial with Galois group $2A_7$. The smallest possible degree is 240, the minimum index of a subgroup of odd order. As far as I know no one has found a polynomial with Galois group $2A_6$ or $2A_7$ over $\mathbf{Q}$. (I have found one with Galois group $2A_5$ over $\mathbf{Q}$ of degree 24 (on a computer), however the splitting field is not $\mathbf{Q}$-adequate.)

The fact that (i), (ii), or (iii) implies (iv) in Theorem A is not difficult. See Theorem 3.2. The converse is however much more subtle. The essential new difficulty arises in the proof of Theorem 4.6. Let K_2 be the completion of K at some place over 2. Assume that $[K_2 : \mathbf{Q}_2] > 1$. Then Q_{16} is a Galois group over K_2. However, additional conditions are needed to show that there exists an extension of K of $\mathbf{Q}$ with Galois group Q_{16} such that the decomposition group at K_2 is also Q_{16}. For Q_8 the existence of such an extension can be settled fairly easily, see [3, p.10]. The case of Q_{16} is handled in this paper by constructing explicit polynomials. Unfortunately several cases need to be considered separately. This is done in Sections 5-8. Mestre's method is then applied twice, first in Section 9 to construct a quartic, then in Section 11 to construct a polynomial of degree 7, which is used to complete the proof of Theorem A. [6, Corollary 2] is helpful here.

2. Notation

The notation in this paper is standard but we list some of it here to avoid confusion.

If v is a nonarchimedean place of K and a is an integer in K with $a \neq 0$, then $\nu_v(a)$ is the exact power of the prime ideal corresponding to v which divides a. If a, b are integers in K with $ab \neq 0$ then $\nu_v(a/b) = \nu_v(a) - \nu_v(b)$. The completion of K at v is denoted by K_v.

Let E be a field and let $f(x)$ be a monic polynomial in $E[x]$ with distinct roots. Define $\mathrm{Tr}_f(\alpha)$ to be the trace of α in $E[x]/(f(x))$. Then $q_f(\alpha) = \mathrm{Tr}_f(\alpha^2)$ defines a nondegenerate quadratic form over E. If K is a number field, let $w_v(f)$ denote the Hasse invariant of this form at the place v, $(\alpha, \beta)_v$ denotes the Hilbert symbol at v.

Let $\Delta(f)$ denote the discriminant of the polynomial f.

If $a, b \in K^\times$ write $a \sim b$ if $a = bc^2$ for some $c \in K$.

Let D_n, Q_n denote the dihedral group, quaternion group, of order n respectively.

3. Admissibility for local fields

THEOREM 3.1: *Let p be an odd prime and let K_p be a finite extension of $\mathbf{Q}_p$ with residue class field $\mathbf{F}_q$. Let H be a Galois group over K_p and let T be a 2-group contained in H.*

(i) *If $q \equiv 1 \pmod 4$ then T is not a dihedral group (of order at least 8) nor a quaternion group.*
(ii) *If $q \equiv 3 \pmod 8$ then T is not Q_{16}.*

Proof: Replacing K_p by a finite extension it may be assumed that $H = T$. The corresponding field is tamely ramified as q is odd. Hence T is a homomorphic image of $G = \langle x, y \mid x^{-1}yx = x^q\rangle$. Let G_4 be the subgroup of G generated by all 4^{th} powers in G and let $\bar{G} = G/G_4$. Then $\bar{x}^{-1}\bar{y}\bar{x} = \bar{y}^q = \bar{y}$ in Case (i) and so neither a dihedral group of order at least 8 nor a quaternion group can be a homomorphic image of G.

If $q \equiv 3 \pmod 8$ then $\bar{y}$ is not conjugate to $\bar{y}^{-1}$ in $\bar{G} = G/ < y^8 >$. Thus (ii) follows. ∎

THEOREM 3.2: *Let K be an algebraic number field which has only one prime divisor of 2. Assume that either $i = \sqrt{-1} \in K$ or $\sqrt{-2} \in K$. Then none of Q_{16},*

$2A_6$, $2A_7$ *is K-admissible.*

Proof: Let $H = Q_{16}$ or $2A_n$ for $n = 6$ or 7. Suppose that H is K-admissible. Let L be a K-adequate extension of K with $H = \mathrm{Gal}(L/K)$. By Schacher's criterion [5] or [3 ,Theorem 2.1] a S_2-group T of H is contained in the Galois group of at least 2 completions of K. As $|T| > 2$, neither of them can be Archimedean. Hence by assumption one of them, K_p, occurs at an odd prime p. Let $\mathbf{F}_q$ be the residue class field of K_p. If $i \in K$ then $q \equiv 1 \pmod 4$. If $\sqrt{-2} \in K$ then $q \equiv 1$ or $3 \pmod 8$. As T is a quaternion group of order 16, this contradicts Theorem 3.1. ∎

4. The construction of certain polynomials

Let K be a number field. Define $h(x) \in K[x]$ by

$$h(x) = x^4 - 2ax^2 + b, \quad ab \neq 0. \tag{4.1}$$

The following 3 facts are well known. See e.g. [3, Section 5]

$$\Delta(h) = 256b(a^2 - b)^2 \sim b. \tag{4.2}$$

If w_v is the Hasse–Witt invariant of the form $\mathrm{Tr}_h(\alpha^2)$ at the place v then

$$w_v(-2, \Delta(h))_v = (a, -1)_v(b, -2a)_v(a^2 - b, -ab)_v \tag{4.3}$$

for every place v of K.

THEOREM 4.4: *The following are equivalent.*

(i) $h(x)$ *is irreducible with* $\mathrm{Gal}(h(x)/K) \simeq D_8$.

(ii) $b, a^2 - b, b(a^2 - b)$ *are all nonsquares in* K.

For convenience we state here a consequence of Serre's Theorem [7].

THEOREM 4.5: *Let* L *be a splitting field of* $h(x)$ *over* K. *Suppose that* $\mathrm{Gal}(L/K) \simeq D_8$. *The following are equivalent.*

(i) $L \subseteq M$ *with* $\mathrm{Gal}(M/K) \simeq Q_{16}$.

(ii) $w_v(-2, \Delta(h))_v = 1$ *for every place* v *of* K.

Our immediate object is to prove the following result.

THEOREM 4.6: *Assume that (*) of Section 1 is satisfied. There exists a polynomial $h(x)$ as in (4.1) such that the following hold.*

(i) *There exist at least 2 places in K which do not divide 3 so that the decomposition group at each of these is D_8.*

(ii) *$w_v(-2, \Delta(h))_v = 1$ for every place v of K.*

This will be proved in the next 4 sections. The proof is divided into 3 cases as follows.

(I) $i = \sqrt{-1} \notin K$ and $\sqrt{-2} \notin K$.

(II) $i \notin K$, $\sqrt{-2} \in K$.

(III) $i \in K$.

5. 2-adic fields

In this section K is a finite extension of $\mathbf{Q}_2$ such that the index of ramification $e = 2k$ is even. Let K_0 be the maximal unramified subfield of K. Then $[K : K_0] = e = 2k$. Let $\mathbf{F}_q$ be the residue class field of K and let A_0 be the group of all $(q-1)$st roots of unity in K. Let $A = A_0 \cup \{0\}$. Then $A \subseteq K_0$. If π is any prime element in K and θ is an integer in K then

$$\theta = \sum_{0}^{\infty} \alpha_j \pi^j, \qquad \alpha_j \in A. \tag{5.1}$$

Furthermore, the coefficients α_j are uniquely determined by θ. By (5.1)

$$\theta^2 = \sum \alpha_j^2 \pi^{2j} + 2 \sum_{j<s} \alpha_j \alpha_s \pi^{j+s}. \tag{5.2}$$

Hence

$$\theta^2 \equiv \sum_{0}^{k} \alpha_j^2 \pi^{2j} + 2\alpha_0\alpha_1\pi \pmod{\pi^{2k+2}}. \tag{5.3}$$

There exists a unit u with

$$2 = \pi^{2k} u. \tag{5.4}$$

LEMMA 5.5: *If $\alpha \in K_0$ and $\alpha \equiv 0 \pmod{\pi}$ then $\alpha \equiv 0 \pmod{\pi^{2k}}$.*

Proof: Clear as π^{2k} is a prime in K_0. ∎

LEMMA 5.6: *$1+\pi^2$ is not a square in K.*

Proof: If $1+\pi^2=\theta^2$ then (5.3) implies that

$$1+\pi^2=\Sigma\alpha_j^2\pi^{2j}+2\alpha_0\alpha_1\pi \pmod{\pi^{2k+2}}.$$

Hence $\alpha_0=\alpha_1=1$ and $\alpha_j=0$ for $1<j\le k$. Therefore $0\equiv 2\pi \pmod{\pi^{2k+2}}$ which is not the case. ∎

LEMMA 5.7: *Suppose that $\sqrt{-2}\in K$.*

(i) *If $e>2, -(1+\pi^2)$ is not a square in K.*

(ii) *If $e=2$ there exists a prime π_0 such that $-(1+\pi_0^2)$ is not a square in K.*

Proof: Since $\sqrt{-2}\in K$, $u=-v^2$. If $v=\Sigma\gamma_i\pi^i$ for $\gamma_i\in A$, (5.3) yields

$$u\equiv-(\gamma_0^2+\gamma_1^2\pi^2+2\gamma_0\gamma_1\pi) \pmod{\pi^4}. \tag{5.8}$$

Suppose that $\theta^2=-(1+\pi^2)$. As $-1\equiv 1+2+4 \pmod 8$ it follows that

$$-1-\pi^2\equiv(1+2+4)(1+\pi^2)\equiv 1+2+4+\pi^2+2\pi^2 \pmod{\pi^6}. \tag{5.9}$$

(i) By (5.3) and (5.9)

$$1+\pi^2+2\equiv\Sigma\alpha_j^2\pi^{2j}+2\alpha_0\alpha_1\pi \pmod{2\pi^2}.$$

Hence by (5.8)

$$1+\pi^2+\gamma_0^2\pi^{2k}\equiv\Sigma\alpha_j^2\pi^{2j}+2\alpha_0\alpha_1\pi \pmod{2\pi^2}$$

as $\pi^{2k}\equiv-\pi^{2k} \pmod{2\pi^2}$. Thus $\alpha_0=\alpha_1=1$ and $\alpha_j=0$ for $1<j<2k$. Therefore

$$\gamma_0^2\pi^{2k}\equiv\alpha_{2k}^2\pi^{2k}+2\pi \pmod{2\pi^2}$$

and so $\gamma_0^2\equiv\alpha_{2k}^2 \pmod{\pi}$. By Lemma 5.5, $0\equiv 2\pi \pmod{2\pi^2}$ which is not the case.

(ii) By (5.9)

$$-1-\pi^2\equiv 1+2+4+\pi^2+2\pi^2\equiv 1+u\pi^2+u^2\pi^4+\pi^2+u^2\pi^4 \pmod{\pi^6}.$$

As $2\pi^4\equiv 0 \pmod{\pi^6}$ this yields

$$-1-\pi^2\equiv 1-(\gamma_0^2+\gamma_1^2\pi^2)\pi^2+\pi^2 \pmod{\pi^5}. \tag{5.10}$$

Suppose first that $K_0 \neq \mathbf{Q}_2$. Choose $\gamma \in A, \gamma \neq 1$. Let $\pi = \gamma^{-1}\sqrt{-2}$. Hence $2 = -\gamma^2\pi^2$ and $v = \gamma = \gamma_0, \gamma_1 = 0$. Now (5.3) and (5.10) imply

$$1 - \gamma^2\pi^2 + \pi^2 \equiv \alpha_0^2 + \alpha_1^2\pi^2 + 2\alpha_0\alpha_1\pi \pmod{\pi^4}.$$

Therefore $\alpha_0 = 1$ and

$$(5.11) \qquad (1 - \gamma^2 - \alpha_1^2)\pi^2 \equiv 2\alpha_1\pi \pmod{\pi^4}.$$

Hence $1 - \gamma^2 - \alpha_1^2 \equiv 0 \pmod{\pi}$ and so Lemma 5.5 implies that

$$0 \equiv 2\alpha_1\pi \pmod{\pi^4}.$$

Thus $\alpha_1 = 0$ and (5.11) implies that $\gamma^2 \equiv 1 \pmod{\pi}$ which contradicts the choice of γ.

Suppose finally that $K_0 = \mathbf{Q}_2$. Thus $K = \mathbf{Q}_2(\sqrt{-2})$. Let $\pi = \sqrt{-2}(1 + \sqrt{-2})$. Thus $v = (1 + \sqrt{-2})^{-1}$ and so $v \equiv v^{-1} \equiv 1 + \pi \pmod{\pi^2}$. Thus $\gamma_0 = \gamma_1 = 1$ and (5.10) becomes

$$-1 - \pi^2 \equiv 1 - \pi^2 - \pi^4 + \pi^2 \equiv 1 + \pi^4 \pmod{\pi^5}.$$

Therefore (5.3) implies that

$$1 + \pi^4 \equiv \alpha_0^2 + \alpha_1^2\pi^2 + \alpha_2^2\pi^4 + 2\alpha_0\alpha_1\pi + 2\alpha_0\alpha_2\pi^2 \pmod{\pi^5}.$$

Hence $\alpha_0 = 1, \alpha_1 = 0$ and so

$$1 + \pi^4 \equiv 1 + \alpha_2^2\pi^4 + 2\alpha_2\pi^2 \equiv 1 + \alpha_2^2\pi^4 - \alpha_2\pi^4 \pmod{\pi^5}.$$

As $\alpha_2 \in K_0$, $\alpha_2^2 - \alpha_2 = 0$ and so $\pi^4 \equiv 0 \pmod{\pi^5}$ which is not the case. ∎

LEMMA 5.12: *Suppose that $i \in K$ and k is odd. Let $\alpha = 1 + i$. Then $1 + \alpha^2$, $2 + \alpha^2$ and $(1 + \alpha^2)(2 + \alpha^2)$ are all nonsquares in K.*

Proof: Since k is odd $\nu(\alpha)$ is odd. Furthermore $2 + \alpha^2 = 2(1 + i)$ and so $\nu(2 + \alpha^2)$ is odd. Thus neither $2 + \alpha^2$ nor $(1 + \alpha^2)(2 + \alpha^2)$ is a square in K.

Let K_1 be an unramified extension of $\mathbf{Q}_2(i)$. By Lemma 5.6, $1 + \alpha^2$ is not a square in K_1. Therefore $\mathbf{Q}_2(i, \sqrt{1 + \alpha^2})$ is ramified over $\mathbf{Q}_2(i)$. Hence if $\sqrt{1 + \alpha^2} \in K$ then $2|k$ contrary to assumption. ∎

LEMMA 5.13: *Suppose that $i \in K$ and $k \geq 4$. Let $1 - i = \pi^k v$ for a prime π in K. Then $v = \Sigma \gamma_j \pi^j$ with $\gamma_0 \neq 0, \gamma_1 = 0$ and $\gamma_j \in A$ for all j.*

Proof: As v is a unit, $\gamma_0 \neq 0$. By definition $1 - i = \pi^k \Sigma \gamma_j \pi^j$. Thus

$$1 - i - \gamma_0 \pi^k \equiv \gamma_1 \pi^{k+1} \pmod{\pi^{k+2}}. \tag{5.14}$$

Since $k \geq 4, K_0(i, \pi^k)$ is a proper subfield of K. As

$$\frac{1-i}{\pi^k} - \gamma_0 \equiv 0 \pmod{\pi}$$

it follows that

$$\nu(\frac{1-i}{\pi^k} - \gamma_0) > 1.$$

Hence $\gamma_1 = 0$ by (5.14). ∎

LEMMA 5.15: *Suppose that $i \in K$ and $k \geq 4$. Let π be a prime in K. Then $1 + \pi^2, 2 + \pi^2$, and $(1 + \pi^2)(2 + \pi^2)$ are all nonsquares in K.*

Proof: By Lemma 5.6, $1 + \pi^2$ is not a square in k.

Let $1 - i = \pi^k v$. By Lemma 5.13, $v = \Sigma \gamma_j \pi^j$ with $\gamma_j \in A$ and $\gamma_1 = 0$. Since

$$-i = \frac{1}{1 - (1 - i)} = \sum_0^\infty (1 - i)^j$$

it follows that

$$i = -\sum_0^\infty (\pi^k v)^j.$$

By (5.3) this implies that

$$iv^2 = -v^2 \sum_0^\infty (\pi^k v)^j \equiv -v^2 - v^3 \pi^k \equiv v^2 + v^3 \pi^k \pmod{\pi^{2k}}. \tag{5.16}$$

Observe that $2 = i\pi^2 v^2$. Hence

$$2 + \pi^2 = \pi^2(1 + \pi^{2k-2} i v^2).$$

Suppose that $(2 + \pi^2)(1 + \pi^2)$ is a square, then

$$1 + \pi^2 + \pi^{2k-2} i v^2 + \pi^{2k} i v^2 = (1 + \pi^2)(2 + \pi^2)\pi^{-2} = \theta^2.$$

By Lemma 5.13, (5.2) and (5.16)

$$\theta^2 \equiv 1 + \pi^2 + \gamma_0^2\pi^{2k-2} + \gamma_0^2\pi^{2k} \pmod{\pi^{2k+2}}.$$

By (5.3) this implies that

$$1 + \pi^2 + \gamma_0^2\pi^{2k-2} + \gamma_0^2\pi^{2k} \equiv \Sigma\alpha_j^2\pi^{2j} + 2\alpha_0\alpha_1\pi \pmod{\pi^{2k+2}}.$$

Hence $\alpha_0 = \alpha_1 = 1$ and

$$\eta \equiv 1 + \pi^2 + \gamma_0^2\pi^{2k-2} + \gamma_0^2\pi^{2k} - \Sigma\alpha_j^2\pi^{2j} \equiv 2\pi \pmod{\pi^{2k+2}}.$$

Therefore $\nu(\eta) = 2k+1$. However $\eta \in K(\pi^2)$ and so $\nu(\eta)$ must be even contrary to the previous statement.

Suppose that $2+\pi^2$ is a square, then so is

$$1 + \pi^{2k-2}iv^2 = (2+\pi^2)\pi^{-2} = \theta^2.$$

By (5.16) and Lemma 5.13

$$\text{(5.17)} \qquad \begin{aligned} \theta^2 &\equiv 1 + \pi^{2k-2}(v^2 + v^3\pi^k) \equiv 1 + \pi^{2k-2}(\Sigma\gamma_j^2\pi^{2j} + \gamma_0^3\pi^k) \\ &\equiv 1 + \sum_j \gamma_j^2\pi^{2k+2j-2} + \gamma_0^3\pi^{3k-2} \pmod{\pi^{3k}}. \end{aligned}$$

By (5.3)

$$\theta^2 \equiv \Sigma\alpha_j^2\pi^{2j} + 2\sum_{j<s}\alpha_j\alpha_s \quad \pmod{\pi^{3k}}.$$

Hence $\alpha_0 = 1, \alpha_j = 0$ for $1 < j < k-1$ and $\alpha_{k-1} = \gamma_0$. Thus

$$\theta^2 \equiv 1 + \sum_{j\geq k-1} \alpha_j^2\pi^{2j} + 2\gamma_0\pi^{k-1} \pmod{\pi^{3k}}.$$

Therefore

$$\eta \equiv 2\gamma_0\pi^{k-1} \pmod{\pi^{3k}},$$

where

$$\eta = 1 + \Sigma\gamma_j^2\pi^{2k+2j-2} + \gamma_0^3\pi^{3k-2} - 1 - \sum_{j\geq k-1}\alpha_j^2\pi^{2j}.$$

Hence $\nu(\eta) = 3k-1$ is odd, which is impossible as $\eta \in K_0(\pi^2)$. ∎

LEMMA 5.18: *Suppose that $i \in K$, none of $\sqrt{1+i}$, $\omega = \sqrt{i}$, $\sqrt{1-i}$ are in K and $[K : K_0] = 4$. Then $i, 1+i$ and $i(1+i) = -(1-i)$ are nonsquares in K.*

Proof: Clear. ∎

LEMMA 5.19: *Suppose that $i \in K$, π is a prime in K and $[K : K_0] = 4$. Then π, $1-\pi$, $\pi(1-\pi)$ are all nonsquares in K.*

Proof: Clearly π and $\pi(1-\pi)$ are nonsquares in K as they are primes. If $1-\pi = \theta^2$ then (5.2) implies that $1-\pi \equiv \alpha_0^2 \pmod{\pi^2}$, which is not the case. ∎

6. Case I of Section 4

Throughout this section K is an algebraic number field such that $i \notin K$ and $\sqrt{-2} \notin K$.

LEMMA 6.1: *There exist infinitely many rational primes p with $p \equiv 7 \pmod 8$ such that some prime divisor of p in K has odd residue class degree.*

Proof: The Galois closure L of $K(\sqrt{2}, i)$ over $\mathbf{Q}$ is $\hat{K}(\sqrt{2}, i)$ where $\hat{K}$ is the Galois closure of K. If $i \in K(\sqrt{2})$ then $\sqrt{-2} \in K(\sqrt{2})$ and so $K(i) = K(\sqrt{-2})$. Thus $\sqrt{2} = i\sqrt{-2} \in K$ and so $i \in K(\sqrt{2}) = K$ contrary to assumption. Hence there exists $\sigma \in \mathrm{Gal}(L/K(\sqrt{2}))$ with $\sigma(i) = -i$. By the Tchebotarev density theorem there exist infinitely many primes p some of whose divisors in $K(\sqrt{2})$ correspond to σ. Then $p \equiv 3 \pmod 4$ and the residue class degree of the selected divisor of p in $K(\sqrt{2})$, and hence in K, is odd. As $\sqrt{2} \in K(\sqrt{2})$, $p \equiv \pm 1 \pmod 8$. Therefore $p \equiv 7 \pmod 8$. ∎

Proof of Theorem 4.6 in Case (I): By Lemma 6.1 there exist primes $p_1 \neq p_2$ which do not ramify in the Galois closure $\hat{K}$ of K over $\mathbf{Q}$, all of whose divisors have odd residue class degree in K and satisfy $p_j \equiv -1 \pmod 8$ for $j = 1, 2$.

Then $p_1 p_2 \equiv 1 \pmod 8$ and so $p_1 p_2 = \ell^2 + m^2 + n^2$ for $\ell, m, n \in \mathbf{Z}$ such that n is relatively prime $p_1 p_2$. Hence for any place v of K

$$(p_1 p_2 - n^2, -1)_v = (\ell^2 + m^2, -1)_v = 1. \tag{6.2}$$

Let $a = p_1 p_2, b = p_1 p_2 n^2$ and let $h(x) = x^4 - 2ax^2 + b$. Then

$$b \sim p_1 p_2, \qquad a^2 - b = p_1 p_2 (p_1 p_2 - n^2), \qquad b(a^2 - b) \sim (p_1 p_2 - n^2).$$

Let $\{\pi_j\}$ be all the prime divisors of p_1p_2 in K. Let ν_j be the valuation of K corresponding to π_j for all j. As p_1 and p_2 are not ramified in $\hat{K}$, $\nu_j(b)$ and $\nu_j(a^2-b)$ are odd for all j. Since $p \equiv 3 \pmod 4, (-1/p) = -1$ for $p = p_1$ or p_2. As the residue class degree of each π_j is odd this implies that $b(a^2-b) \sim (p_1p_2 - n^2)$ is not a square in the completion K_j of K at ν_j. This proves Theorem 4.6 (i).

Let $w = w_v$ for any place v of K. By (4.3)

$$\begin{aligned} w(-2, \Delta(h)) &= (p_1p_2, -1)(p_1p_2, -2p_1p_2)(p_1p_2(p_1p_2 - n^2), -1) \\ &= (p_1p_2, 2)(p_1p_2 - n^2, -1) = (p_1p_2, 2) \end{aligned}$$

by (6.2). As $p_j \equiv -1 \pmod 8$, $(p_j, 2) = 1$.

7. Case II of Section 4

Let K_1 and K_2 be two completions of K at prime divisors of 2 in K. For $j = 1$, or 2 use Lemmas 5.6 and 5.7 to choose a prime $\pi_j \in K_j$ so that $\pm(1+\pi_j^2)$ are both nonsquares in K_j.

Define $h_j(x) = x^4 - 2a_jx^2 + b_j$ with $a_j = 1$ and $b_j = 1 + \pi_j^2$. Then $a_j^2 - b_j = -\pi_j^2$ and $b_j(a_j^2 - b_j) \sim -(1+\pi_j^2)$. The weak approximation theorem yields the existence of an element π in K such that if $a = 1$ and $b = 1 + \pi^2$ then Theorem 4.4(ii) holds. Furthermore by Krasner's Lemma it may be assumed that Theorem 4.6(i) holds.

Let $w = w_v$ for any place v of K. By (4.3)

$$w(-2, \Delta(h)) = (b, -2)(1-b, -b) = (b, -2)(-\pi^2, 1+\pi^2)(-\pi^2, -1).$$

As $\sqrt{-2} \in K$ and $(-1,-1) = (-1,2) = 1$, Theorem 4.6 (ii) holds.

8. Case III of Section 4

Let K_1 and K_2 be two completions at prime divisors of 2 in K. For $j = 1, 2$ we will first show the existence of elements c_j, u_j, v_j in K_j such that $a_j = c_j^2$, $b_j = 2u_j^2 + v_j^2$ and $h_j(x) = x^4 - 2a_jx^2 + b_j$ has Galois group over K_j isomorphic to D_8. By Theorem 4.4 the latter condition will follow once it is shown that b_j, $a_j^2 - b_j$ and $b_j(a_j^2 - b_j)$ are all nonsquares in K.

Let e_j denote the ramification index of K_j over $\mathbf{Q}_2$. The following cases will be handled separately.

(8.1) $$e_j \equiv 2 \pmod 4.$$

(8.2) $$e_j \equiv 0 \pmod 4 \text{ and } e_j > 4.$$

(8.3) $$e_j = 4 \text{ and none of } \sqrt{1+i}, \sqrt{1-i}, \omega = \sqrt{i} \text{ are in } K.$$

(8.4) $$e_j = 4 \text{ and } \omega = \sqrt{i} \in K.$$

(8.5) $$e_j = 4 \text{ and } \sqrt{1+\varepsilon i} \in K \text{ for } \varepsilon = 1 \text{ or } -1.$$

In Case (8.1), let $a_j = i^2, b_j = 2 + \alpha^2$ in Lemma 5.12.

In Case (8.2), let $a_j = i^2, b_j = 2 + \pi^2$ in Lemma 5.15.

In Case (8.4), let $a_j = 1^2, b_j = \pi$ in Lemma 5.19. Since $\sqrt{-2} \in K$, $(b_j, -2) = 1$ and so $b_j = 2u_j^2 + v_j^2$ for some $u_j, v_j \in K_j$.

For the remaining cases we need the following.

LEMMA 8.6: *Let $\beta = 1 + i$ or $\sqrt{1+\varepsilon i}$ for $\varepsilon = \pm 1$. Then $(\beta, -2) = 1$ and so $\beta = 2u_j^2 + v_j^2$ for some $u_j, v_j \in K_j$.*

Proof: Let $F = \mathbf{Q}(\beta)$. Then β is a unit at any completion other than the completion F_2 of F at the unique place dividing 2. Hence $(\beta, -2)_v = 1$ for any place v other than 2. The result follows from the product formula. ∎

In Case (8.3), let $a_j = 1^2, b_j = 1 + i$ in Lemma 5.18 and use Lemma 8.6.

In Case (8.5), let $a_j = 1^2, b_j = \sqrt{1+\varepsilon i}$ in Lemma 5.19 and use Lemma 8.6.

The weak approximation theorem and Krasner's Lemma imply the existence of elements $c, u, v \in K$ such that if $a = c^2$, $b = 2u^2 + v^2$ and if $h(x) = x^4 - 2ax^2 + b$ then Theorem 4.6 (i) holds.

Let $w = w_v$ for any place v of K. By (4.3)

$$w(-2, \Delta(h)) = (b, -2)(1 - b, -c^2)$$

As $b = 2u^2 + v^2, (b, -2) = 1$. As $-1 = i^2$ this yields Theorem 4.6 (ii).

9. The polynomial $f(x)$

THEOREM 9.1: *Let K be a number field which satisfies condition (*) of Section 1. Then there exists a quartic polynomial $f(x) \in K(x)$ such that the following hold.*

(i) $\mathrm{Gal}(f(x)/K) \simeq \Sigma_4$.

(ii) *There exist two places v_1, v_2 of K such that the decomposition group at each of these is D_8.*

(iii) *If w is the Hasse invariant of the form q_f over K at any place then $w(-2, \Delta(f)) = 1$.*

Proof: Let $h(x)$ be the polynomial defined by Theorem 4.6. Let $h_1(x) = h(x)x$. Let v_1, v_2 be two places of K such that the decomposition group at these places is D_8. By [6, Corollary 2] there exists an H-general polynomial $P(x)$ such that if α_j are the roots of $h_1(x)$ and β_j are the roots of $P(x)$, then after a possible rearrangement $K(\alpha_j) = K(\beta_j)$ for all j. Thus $\Delta(P) \sim \Delta(h_1)$. By Mestre's Theorem [4] or [3, Section 4] there exists a polynomial $F_T(x) = P(x) - TQ(x)$, where T is an indeterminate, such that $\mathrm{Gal}(F_T(x)/K(T)) \simeq \Sigma_5$ and the quadratic forms q_{F_T} and q_P are equivalent over $K(T)$. By [3, Lemma 6.3] there exists $t \in K$ such that $\mathrm{Gal}(F_t(x)/K) \simeq \Sigma_5$ and the decomposition group at v_1 and v_2 is D_8. Hence $F_t(x)$ has a root in the completion K_j of K at v_j. Furthermore a splitting field of F_t can be imbedded in a field M with $\mathrm{Gal}(M/K) \simeq \Sigma_5^+$ by Serre's Theorem [7] or [3, Section 3]. Now the existence of $f(x)$ follows from either [3, Lemma 6.6] or [1, Theorem 4]. ∎

THEOREM 9.2: *Let $f(x)$ be the polynomial defined in Theorem 9.1. Then there exist places v_3 and v_4 of K distinct from v_1 and v_2 such that v_j has residue class degree 3 over K, a rational prime over v_j is greater than 7 and $-3\Delta(f)$ is a nonzero square in the residue class field corresponding to v_j for $j = 3, 4$.*

Proof: Let σ be an element of order 3 in the Galois group of $f(x)(x^2 + 3\Delta(f))$ over K. The result follows from the Tchebotarev density theorem. ∎

10. A cubic polynomial $g(x)$

The notation of Section 9 is used in this section. Let $\Delta = \Delta(f)$.

THEOREM 10.1: *There exists a cubic polynomial $g(x)$ with the following properties.*

(i) $\Delta(g) \sim \Delta$.

(ii) *A rational prime over v_j is greater than 7 and g has ramification index 3 at v_j for $j = 3$ and 4.*

(iii) *g has a root at the completion K_j of K at v_j for $j = 1, 2$.*

Proof: By Theorem 9.1

$$\nu_1(\Delta) > 0, \qquad \nu_2(\Delta) > 0. \tag{10.2}$$

Thus by Theorem 9.2 there exist algebraic integers $s, \alpha, \beta \in K$ so that

$$s = 27\alpha^2 + \beta^2 \Delta$$

and

$$\nu_1(s) = \nu_2(s) = 0, \qquad \nu_3(s) = \nu_4(s) = 1,$$

where ν_j is the valuation corresponding to v_j. Thus also $\nu_j(\alpha) = 0$ for $j = 1, 2$. Then

$$4s^3 = 27(2s\alpha)^2 + (2s\beta)^2\Delta.$$

Define

$$g(x) = x^3 - sx + 2s\alpha.$$

Then

$$\Delta(g) = 4s^3 - 27(2s\alpha)^2 = (2s\beta)^2\Delta \sim \Delta.$$

Thus (i) holds. The Newton polygons imply that (ii) holds.

Let π be a prime in K_j for $j = 1$ or 2. Substitute 3α in $g(x)$ and $g'(x)$ and -6α in $g(x)$. By (10.2) this yields

$$g(x) \equiv (x - 3\alpha)^2(x + 6\alpha)(mod\ \pi).$$

Since $3\alpha \not\equiv -6\alpha(mod\ \pi)$ as $\nu_j(3) = \nu_j(\alpha) = 0$, Hensel's Lemma implies (iii). ∎

11. The proof of Theorem A

The fact that Condition (i), (ii) or (iii) of Theorem A implies (iv) follows from Theorem 3.2.

(iv) $\Rightarrow$ (i). This follows from Theorem 4.6.

Before proceeding we need the next result.

LEMMA 11.1: *Suppose that K is a number field which satisfies condition (*) of Section 1. Then there exists a monic polynomial $F(x) \in K[x]$ of degree 7 and 4 places v_1, v_2, v_3, v_4 of K such that the following hold.*

(i) $\mathrm{Gal}(F(x)/K) \simeq A_7$

(ii) *The decomposition group at v_1 and v_2 is D_8.*

(iii) *The decomposition group at v_3 and v_4 has order divisible by 9.*

(iv) *$F(x)$ has a root at the completion K_j of K at v_j for $j = 1, 2, 3, 4$.*

(v) *If v is a place of K and w_v is the Hasse invariant of the form q_F over K_v then $w_v = 1$.*

Proof: Let $f(x)$ be defined in Theorem 9.1 and let $g(x)$ be defined in Theorem 10.1. By [6, Corollary 2] there exists an H-general polynomial $P(x)$ such that if α_j are the roots of $f(x)g(x)$ and β_j are the roots of $P(x)$, then after a possible rearrangement $K(\alpha_j) = K(\beta_j)$ for all j. By Theorem 10.1 (i) $\Delta(P) \sim \Delta(f)\Delta(g) \sim 1$. By Mestre's Theorem [4] or [3, Section 4] there exists a polynomial $F_T(x) = P(x) - TQ(x)$, where T is an indeterminate, such that $\mathrm{Gal}(F_T(x)/K(T)) \simeq A_7$ and the quadratic forms q_{F_T} and q_P are equivalent over $K(T)$. By [3, Lemmas 6.3 and 6.6] there exists $t \in K$ so that if $F(x) = F_t(x)$ then $\mathrm{Gal}(F(x)/K) \simeq A_7$ and (ii) and (iii) are satisfied.

Let G_j be the decomposition group at v_j. If $j = 1$ or 2 then $G_j \simeq D_8$ and so $G_j \subseteq A_6$. Hence (iv) is satisfied in this case. If $j = 3$ or 4 the extension is tamely ramified as the prime corresponding to v_j is greater than 7. Thus G_j is a meta-cyclic subgroup of A_7 which contains a S_3-group of A_7. Hence $|G_j| = 9$. Therefore $G_j \subseteq A_6$ and (iv) is also satisfied in this case.

Let v be a place of K and let $w = w_v$. Then

$$w(F) = w(P) = w(f)w(g)(\Delta(f), \Delta(g)) = w(f)w(g)(-1, \Delta),$$

where $\Delta = \Delta(f) \sim \Delta(g)$.

By Theorem 9.1 $w(f) = (-2, \Delta)$. Furthermore $w(g) = (2, \Delta)$ for any cubic by Serre's Theorem, see e.g. [2, Lemma 3.13]. Therefore

$$w(F) = (-2, \Delta)(2, \Delta)(-1, \Delta) = 1. \quad \blacksquare$$

Lemma 11.1 and Serre's Theorem show that (iv) implies (iii) in Theorem A. Thus (iv) implies (ii) by Lemma 11.1 and either [3, Lemma 6.6] or [1, Theorem 4]. This completes the proof of Theorem A.

References

[1] B. Fein and M. Schacher, *$\mathbf{Q}$-admissiblity questions for alternating groups*, J. Algebra **142** (1991), 360–382.

[2] W. Feit, *The $\mathbf{Q}$-admissibility of $2A_6$ and $2A_7$*, to appear.

[3] P. Feit and W. Feit, *The K-admissibility of* SL(2,5), Geometriae Dedicata **36** (1990), 1–13.

[4] J.-F. Mestre, *Extensions reguliéres de $\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_n$*, J. Algebra **131** (1990), 483–496.

[5] M. Schacher, *Subfields of division rings*, J. Algebra **9** (1968), 451–477.

[6] M. Schacher and J. Sonn, *K-Admissibility of A_6 and A_7*, J. Algebra **145** (1992), 333–338.

[7] J.-P. Serre, *L'invariant de Witt de la forme $Tr(x^2)$*, Comment. Math. Helv. **59** (1984), 651–676.