JOURNAL OF ALGEBRA **104**, 231–260 (1986)

$\tilde{A}_5$ and $\tilde{A}_7$ Are Galois Groups over Number Fields

WALTER FEIT*

Department of Mathematics, Yale University, New Haven, Connecticut 06520

Received February 15, 1986

TO SANDY GREEN ON HIS 60TH BIRTHDAY

1. INTRODUCTION

Let $n \geqslant 5$ and let $\tilde{A}_n$ denote the double cover of the alternating group A_n.

THEOREM A. *Let $G = \tilde{A}_5$ or $\tilde{A}_7$ and let H be the center of G. There exist infinitely many Galois extensions E_i of $\mathbb{Q}$ with Galois group G such that the subfields L_i corresponding to H are pairwise nonisomorphic.*

This result is a consequence of Theorems 9.6 and 12.2. The proof is an application of a theorem of Serre [12]; see Section 3 for a statement. Certain generalized Laguerre polynomials are constructed whose splitting fields E_i have the property that $\mathrm{Gal}(E_i/\mathbb{Q}) \simeq A_n$ for $n = 5$ or 7 such that the quadratic form $\mathrm{Tr}_{E_i/\mathbb{Q}}(x^2)$ has Witt invariant equal to 1 at every completion of $\mathbb{Q}$ and so Serre's theorem applies.

It is a simple consequence of Theorem A that $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over every number field. In fact a slightly more general result is proved in Section 7, see Theorem 7.3.

The following related result is proved in Section 6.

THEOREM B. *Let $n \equiv 3 \pmod 4$. There exists a Galois extension M_n of $\mathbb{Q}$ with $\mathrm{Gal}(M_n/\mathbb{Q}) \simeq \tilde{A}_n$.*

The major difficulty in the proofs of Theorems A and B concerns the computation of certain Witt invariants. This is done in Section 5. Lemma 5.5 which is essential for the proof may be of independent interest.

Added in proof. T. Orloff has pointed out that an alternative proof of Lemma 5.5 can be given by using the fact that if $p(x)$ is a polynomial of degree at most $m-1$ then $\sum_{k=0}^{m} (-1)^k \binom{m}{k} p(k) = 0$. See, e.g., R. P. Stanley (*MAA Studies in Mathematics* **17**, p. 115). Then Lemma 5.5 follows directly from (5.4), as it can be shown that the coefficient of y^{m-d} in $h_m(y)$ is of the form $p(k)$ for some polynomial p of degree 2d.

* The work in this paper was partly supported by NSF Grant DMS-8512904.

0021-8693/86 $3.00

Sonn [13] proved that $\tilde{A}_5$ is a Galois group over $\mathbb{Q}$. He also used a generalized Laguerre polynomial. I am indebted to John McKay who first drew my attention to Sonn's paper, which suggested the relevance of these polynomials for the proof of Theorem A.

Vila [14–16] has shown that $\tilde{A}_n$ is a Galois group over every number field if $n \equiv 0$ or $1 \pmod 8$, $n \equiv 2 \pmod 8$ and n is a sum of 2 squares, or $n \equiv 3 \pmod 8$ and satisfies another condition (which may always be true.) She has also shown that if K is a number field which contains $\sqrt{-1}$ then $\tilde{A}_n$ is a Galois group over K for all n. Her method of proof is quite different from that given in this paper. She uses Hilbert's irreducibility theorem in conjunction with Serre's theorem. The fields constructed in this paper are totally real, while those constructed by Vila are never totally real. In contrast to her results, the following has not yet been answered.

PROBLEM 1. Let t be an indeterminate. Does there exist a Galois extension M of $\mathbb{Q}(t)$ in which $\mathbb{Q}$ is algebraically closed such that $\mathrm{Gal}(M/\mathbb{Q}(t)) \simeq \tilde{A}_5$ or $\tilde{A}_7$?

$SL_2(5) \simeq \tilde{A}_5$ is a Galois group over every number field by Theorem A.

PROBLEM 2. Let $q > 5$ be an odd prime power. Let K be a number field. Show the existence of a Galois extension M of K with $\mathrm{Gal}(M/K) \simeq SL_2(q)$. Find such an extension for $K = \mathbb{Q}$.

PROBLEM 3. Let $q > 5$ be an odd prime power. Show the existence of a totally real field L which is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq PSL_2(q)$.

Since $SL_2(q)$ has a unique involution, it follows that if M is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \simeq SL_2(q)$ then the subfield of M corresponding to the center of $SL_2(q)$ is totally real. Thus an affirmative answer to Problem 2 would imply an affirmative answer to Problem 3. The converse is of course not true. For instance by using generalized Laguerre polynomials it is easy to construct totally real fields L which are Galois extensions of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_6 \simeq PSL_2(9)$. However, none of these can be embedded in Galois extensions M of $\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \simeq SL_2(9)$.

In handling the case $G \simeq \tilde{A}_7$ in Theorem A it is necessary to use some basic properties of elliptic curves. Also at one point Faltings' theorem is quoted. I am greatly indebted to D. Zagier, with whom I had several illuminating discussions on these topics.

In Sections 13 and 14 the fields constructed in Section 9 are used to show that A_5 and $\tilde{A}_5$ are K-admissible for certain number fields. (K-admissibility is defined in Section 13.)

After seeing an earlier version of this paper, H. Matzat informed me that his student A. Zeh-Marschke has found totally real fields with Galois

groups $PSL_2(7)$ over $\mathbb{Q}$, by specializing some of the polynomials defined by LaMacchia, *Comm. Algebra* **8** (1980), 983–992. This answered a question I had asked. Possibly some of these may lead to fields with Galois groups $SL_2(7)$ over $\mathbb{Q}$.

In view of Vila's results and Theorem A it follows that $\tilde{A}_5$ and $\tilde{A}_n$ for $7 \leqslant n \leqslant 11$ are Galois groups over all number fields. In an earlier version of this paper I raised the obvious question about $\tilde{A}_6$. Serre showed this to J.-F. Mestre and Mestre has now shown that $\tilde{A}_6$ also satisfies the conclusion of Theorem A. His method is similar to that used in this paper. He uses a different set of orthogonal polynomials, the Jacobi polynomials, and is also led to the study of an elliptic curve.

Finally, I wish to thank J.-P. Serre who made several suggestions which provided insight and led to some clarifications and reformulations of the results in this paper.

The notation used in this paper is quite standard. The following should be mentioned:

If p is a prime then v_p denotes the exponential p-adic valuation normalized so that $v_p(p) = 1$.

If $a, b \in Q^\times$ then $a \sim b$ means that $ab = c^2$ for some $c \in \mathbb{Q}$.

2. The Quadratic Form $Q(E)$

Let F be a field and let $f(x)$ be a monic polynomial in $F[x]$. Then $F[x]/(f(x)) \simeq E$, where E is an algebra over F. If $F(x)$ has degree n then E is an n-dimensional vector space over F.

Multiplication by an element γ of E defines a linear transformation on E. Let $T(\gamma)$ denote the trace of this linear transformation. Then $\gamma \to T(\gamma^2)$ defines a quadratic form on E. Denote this form by $Q(E)$ or $Q(f(x))$.

Observe that E is a field if and only if $f(x)$ is irreducible in $F[x]$. Conversely if E is a separable extension of F then $E = F(\theta)$ for some $\theta \in E$. Hence $E \simeq F[x]/(f(x))$, where $f(x)$ is the irreducible monic polynomial in $F[x]$ with $f(\theta) = 0$.

There exists an element Θ in E with $E = F[\Theta]$. Let $f(x) = \prod_{j=1}^{n} (x - \theta_j)$ in an algebraic closure of F. If E is a field we can identify Θ with $\theta = \theta_1$. In any case $T(\Theta^i) = \sum_{j=1}^{n} \theta_j^i$. Furthermore the discriminant of $Q(E)$ is the discriminant of $f(x)$. Thus in particular $Q(E)$ is nondegenerate if and only if $f(x)$ has distinct roots.

Suppose that char $F \neq 2$. Let $B(E)$ be the bilinear form corresponding to $Q(E)$. Then $B(E)(\gamma_1, \gamma_2) = T(\gamma_1 \gamma_2)$.

For any nonnegative integer m define

$$s_m(E) = s_m = \sum_{j=1}^{n} \theta_j^m. \tag{2.1}$$

For $1 \leqslant t \leqslant n$ define the $t \times n$ matrix A_t by

$$A_t = A_t(E) = (\theta_j^{i-1}), \qquad 1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant n. \tag{2.2}$$

(We use the convention that $0^0 = 1$.) Define

$$D_t = D_t(E) = A_t A_t', \tag{2.3}$$

where $'$ denotes the transpose. It follows directly from (2.1), (2.2), (2.3) that

$$D_t = (s_{i+j-2}). \tag{2.4}$$

Define

$$\Delta_t = \Delta_t(E) = \det D_t. \tag{2.5}$$

THEOREM 2.1. *Suppose that for some* θ, $(x-\theta)^{k+1} | f(x)$. *Then for* $1 \leqslant t \leqslant n$,

$$\text{rank of } D_t \leqslant n-k.$$

Proof. There are at most $n-k$ distinct columns in A_t. Hence A_t has rank at most $n-k$. The result follows from (2.3). ∎

THEOREM 2.2. *Suppose that* $\Delta_t \neq 0$ *for* $1 \leqslant t \leqslant n$. *Then* $Q(E)$ *is equivalent over* F *to the form* $a_1 x_1^2 + \cdots + a_n x_n^2$ *where* $a_1 = \Delta_1 = n$ *and*

$$a_t = \Delta_t / \Delta_{t-1} \qquad \text{for} \quad 2 \leqslant t \leqslant n.$$

Furthermore Δ_n *is a discriminant of* $Q(E)$.

Proof. $\{1, \Theta, \ldots, \Theta^{n-1}\}$ is a basis of E and $B(E)(\Theta^i, \Theta^j) = s_{i+j}$, where $\Theta^0 = 1$. Thus $\Delta_1 = n, \Delta_2, \ldots, \Delta_n$ are the principal minors of D_n. ∎

For convenience we state here Newton's identities.

THEOREM 2.3. *Let* $f(x) = x^n - p_1 x^{n-1} + \cdots + (-1)^n p_n$. *Define* $p_j = 0$ *for* $j > n$. *Then*

$$s_k = p_1 s_{k-1} - p_2 s_{k-2} + \cdots + (-1)^k p_{k-1} s_1 + (-1)^{k+1} k p_k$$

for any natural number k.

3. SERRE'S THEOREM

The main results of this paper depend on a theorem of Serre [12]. Before stating what is needed we will give the necessary background, which can for instance be found in [11, Chap. III] or [4, Chap. 9].

Let $p=\infty$ or a prime. Let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ at p. For $a, b \in \mathbb{Q}_p^\times$ let $(a, b)=(a, b)_p=\pm 1$ denote the Hilbert symbol. This has the following properties:

$$(a, b)=(b, a). \tag{3.1}$$

$$(a, bc)=(a, b)(a, c). \tag{3.2}$$

$$(a, -a)=1. \tag{3.3}$$

$$\text{If } ab\neq 0 \text{ and } a+b=1 \text{ } \textit{then } (a, b)=1. \tag{3.4}$$

Furthermore

$$(a, b)_\infty=\begin{cases} -1 & \text{if } a<0 \text{ and } b<0, \\ 1 & \text{otherwise.} \end{cases} \tag{3.5}$$

If p is an odd prime and u, v are p-adic units then

$$(u, v)_p=1, \qquad (u, p)=\left(\frac{u}{p}\right) \quad \text{(the Legendre symbol).} \tag{3.6}$$

Finally, if $a, b \in \mathbb{Q}^\times$ then

$$\prod_p (a, b)_p=1. \tag{3.7}$$

This last statement is equivalent to the quadratic reciprocity law.

The properties (3.1)–(3.6) make it possible to evaluate $(a, b)_p$ for $p\neq 2$ and $a, b \in \mathbb{Q}_p^\times$. For the evaluation of $(a, b)_2$ with $a, b \in \mathbb{Q}_2^\times$ see, for instance [11, p. 39]. This will not be needed here. However, by using (3.7) together with (3.1)–(3.6) it is possible to evaluate $(a, b)_2$ for $a, b \in \mathbb{Q}^\times$.

Let Q be a nondegenerate quadratic form with coefficients in $\mathbb{Q}_p$. Suppose that Q is equivalent to the diagonal form $a_1x_1^2+\cdots+a_nx_n^2$ over $\mathbb{Q}_p$. Define

$$\varepsilon_p(Q)=\prod_{1\leq i<j\leq n} (a_i, a_j)_p.$$

It is known that $\varepsilon_p(Q)$ does not depend on the choice of diagonal form equivalent to Q; $\varepsilon_p(Q)$ is variously known as the Hasse, Witt, or Hasse–Witt invariant.

Let $F=\mathbb{Q}$ and let $Q(E)$ be defined as in Section 2. We will write

$$\varepsilon_p(E)=\varepsilon_p(f(x))=\varepsilon_p(Q(E)) \qquad \text{for all } p.$$

THEOREM 3.1. *Let $F=\mathbb{Q}$. Let $Q(E)$ be defined as in Section 2. Let $\Delta_0(E)=1$. Suppose that $Q(E)$ is nondegenerate and $\Delta_j(E)\neq 0$ for $1\leqslant j\leqslant n$. Then*

$$\varepsilon_p(E)=\left\{\prod_{j=1}^{n}(\Delta_{j-1}(E),\Delta_j(E))_p\right\}\left(-1,\prod_{j=1}^{n-1}\Delta_j(E)\right)_p$$

for all p.

Proof. The definition of $\varepsilon_p(E)$ and Theorem 2.2 imply that

$$\begin{aligned}\varepsilon_p(E)&=\prod_{j=2}^{n}(\Delta_{j-1}(E),\Delta_j(E)/\Delta_{j-1}(E))_p\\&=\prod_{j=2}^{n}(\Delta_{j-1}(E),\Delta_j(E))_p\prod_{j=2}^{n}(\Delta_{j-1}(E),\Delta_{j-1}(E))_p.\end{aligned}$$

By (3.2) and (3.3)

$$\varepsilon_p(E)=\prod_{j=2}^{n}(\Delta_{j-1}(E),\Delta_j(E))_p\left(-1,\prod_{j=2}^{n}\Delta_{j-1}(E)\right)_p.$$

The result follows as $\Delta_0(E)=1$. ∎

Let $n\geqslant 5$. Let A_n denote the alternating group on n letters. Let $\tilde{A}_n$ denote the double cover of A_n. In other words $\tilde{A}_n$ is the group (unique up to isomorphism) such that there exists a nonsplit exact sequence

$$1\to Z\to\tilde{A}_n\to A_n\to 1$$

with $|Z|=2$. If G is a subgroup of A_n let $\tilde{G}$ denote the inverse image of G in $\tilde{A}_n$.

THEOREM 3.2. (Serre [12]). *Let E be a finite extension of $\mathbb{Q}$ and let $\hat{E}$ denote its Galois closure in some algebraic closure. Assume that $\hat{E}$ has square discriminant. Thus $G=\mathrm{Gal}(\hat{E}/\mathbb{Q})\subseteq A_n$, where $n=[E:\mathbb{Q}]$. Suppose that $\tilde{G}$ is a nonsplit extension of G. Then the following are equivalent.*

(i) *There exists a quadratic extension field M of $\hat{E}$ which is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q})\simeq\tilde{G}$.*

(ii) *$\varepsilon_p(E)=1$ for $p=\infty$ or a prime.*

4. GENERALIZED LAGUERRE POLYNOMIALS

Let λ,μ be indeterminates over $\mathbb{Q}$. For any integer j let $c_j=\lambda+j\mu$. Define

$$\begin{aligned}F_n(x,\lambda,\mu)&=x^n-nc_nx^{n-1}+\tbinom{n}{2}c_nc_{n-1}x^{n-2}+\cdots+(-1)^nc_nc_{n-1}\cdots c_1\\&=\sum_{j=0}^{n}(-1)^{n-j}\tbinom{n}{j}\left(\prod_{i=j+1}^{n}c_i\right)x^j.\end{aligned}\tag{4.1}$$

Observe that if $\kappa \neq 0$ then

$$F_n(x, \lambda, \mu) = \kappa^{-n} F_n(x\kappa, \lambda\kappa, \mu\kappa).$$

In particular if $\alpha = \lambda/\mu$ then

$$F_n(x, \lambda, \mu) = \mu^n F_n(x/\mu, \alpha, 1). \tag{4.2}$$

Polya and Szego [8, p. 274] defined the polynomials $F_n(x, \alpha, 1)$ and called them generalized Laguerre polynomials. The case $\alpha = 0$ yields the classical Laguerre polynomials. Schur studied the polynomials $F_n(x, \lambda, \mu)$ and showed that if $\Delta_n(\lambda, \mu)$ denotes the discriminant of $F_n(x, \lambda, \mu)$ then

$$\Delta_n(\lambda, \mu) = \mu^{n(n-1)/2} n! \sum_{i=1}^{n} (ic_i)^{i-1}. \tag{4.3}$$

See [10, p. 229].

If $\gamma_1, \gamma_2 \in \mathbb{Q}(\lambda, \mu)^\times$ write $\gamma_1 \sim \gamma_2$ if $\gamma_1 \gamma_2^{-1}$ is a square in $\mathbb{Q}(\lambda, \mu)$. It follows directly from (4.3) that

$$\Delta_n(\lambda, \mu) \sim \begin{cases} \mu^k \prod_{i=1}^{k-1} (1+2i) \prod_{i=1}^{k} (\lambda + 2i\mu) & \text{if } n = 2k, \\ \mu^k \prod_{i=1}^{k} (1+2i) \prod_{i=1}^{k} (\lambda + 2i\mu) & \text{if } n = 2k+1. \end{cases} \tag{4.4}$$

In particular we see that

$$\Delta_5(\lambda, \mu) \sim 15(\lambda + 2\mu)(\lambda + 4\mu). \tag{4.5}$$

$$\Delta_6(\lambda, \mu) \sim 15\mu(\lambda + 2\mu)(\lambda + 4\mu)(\lambda + 6\mu). \tag{4.6}$$

$$\Delta_7(\lambda, \mu) \sim 105\mu(\lambda + 2\mu)(\lambda + 4\mu)(\lambda + 6\mu). \tag{4.7}$$

$$\Delta_8(\lambda, \mu) \sim \Delta_9(\lambda, \mu) \sim 105(\lambda + 2\mu)(\lambda + 4\mu)(\lambda + 6\mu)(\lambda + 8\mu). \tag{4.8}$$

These formulas of course remain valid if λ and μ are specialized to rational values. Hence we get

$$\Delta_n(1, 1) \sim \begin{cases} 1 & \text{if } n \text{ is odd}, \\ n+1 & \text{if } n \text{ is even}. \end{cases} \tag{4.9}$$

Moreover Schur, [10, p. 227], has shown that $F_n(x, 1, 1)$ is irreducible over $\mathbb{Q}$ with Galois group A_n or the symmetric group Σ_n according to whether $\Delta_n(1, 1)$ is a square in $\mathbb{Q}$ or not.

Among other things, the polynomials $F_n(x, \lambda, \mu)$ satisfy the following recursion formula for $n \geqslant 2$. See [10, p. 229]:

$$F_n(x, \lambda, \mu) = \{x - nc_n + (n-1)\, c_{n-1}\}\, F_{n-1}(x, \lambda, \mu)$$
$$- (n-1)\, \mu c_{n-1} F_{n-2}(x, \lambda, \mu) \tag{4.10}$$
$$= \{x - c_n - (n-1)\mu\} F_{n-1}(x, \lambda, \mu) - (n-1)\, \mu(c_n - \mu)\, F_{n-2}(x, \lambda, \mu).$$

Let $f(x) = F_n(x, \lambda, \mu)$. Let $E = \mathbb{Q}(\lambda, \mu)[x]/(f(x))$. Define

$$A_{n,t}(\lambda, \mu) = A_t(E), \tag{4.11}$$

$$D_{n,t}(\lambda, \mu) = D_t(E), \tag{4.12}$$

$$\Delta_{n,t}(\lambda, \mu) = \Delta_t(E), \tag{4.13}$$

where $A_t(E)$, $D_t(E)$, $\Delta_t(E)$ are defined by (2.2), (2.3), (2.5). We will also write

$$A_{n,t}(\lambda) = A_{n,t}(\lambda, 1), \tag{4.14}$$

$$D_{n,t}(\lambda) = D_{n,t}(\lambda, 1), \tag{4.15}$$

$$\Delta_{n,t}(\lambda) = \Delta_{n,t}(\lambda, 1). \tag{4.16}$$

LEMMA 4.1. *For* $1 \leqslant t \leqslant n$, $\Delta_{n,t}(\lambda, \mu) = \mu^{t(t-1)} \Delta_{n,t}(\lambda/\mu)$.

Proof. By (4.2), $\mu^k s_k(\lambda/\mu, 1) = s_k(\lambda, \mu)$. Thus in the expansion of $\Delta_{n,t}(\lambda, \mu)$ as the determinant of $D_{n,t}(\lambda, \mu)$, each term is $\mu^{2(1+\cdots+t-1)} = \mu^{t(t-1)}$ times the corresponding term in $\Delta_{n,t}(\lambda/\mu)$. ∎

5. THE COMPUTATION OF $\Delta_{n,t}(\lambda)$

The object of this section is to prove the following result.

THEOREM 5.1. *Let* $1 \leqslant t \leqslant n$. *Then*

$$\Delta_{n,t}(\lambda) = n^t (n-1)^{t-1} \cdots (n+1-t)\, c_n^{t-1} c_{n-1}^{t-2} \cdots c_{n+2-t}$$
$$= \prod_{j=n-t+1}^{n} j(jc_j)^{j-(n-t+1)},$$

where $c_j = \lambda + j$.

In case $t = n$ the formula in Theorem 5.1 reduces to (4.3) for $\mu = 1$. Thus Theorem 5.1 may be viewed as a generalization of Schur's formula (4.3).

The proof of Theorem 5.1 will be given in a series of lemmas.

LEMMA 5.2. *s_k is a polynomial in λ for all k and $\Delta_{n,t}(\lambda)$ is a polynomial in λ.*

Proof. Each coefficient of $F_n(x, \lambda, 1)$ is a polynomial in λ. Hence by Newton's identities, Theorem 2.3, each s_k is a polynomial in λ, which implies the result. ∎

Define the polynomials $\Pi_k(y)$ as follows:

$$\Pi_0(y) = 1, \qquad \Pi_k(y) = y(y-1)\cdots(y-k+1). \tag{5.1}$$

Thus Π_k is a polynomial of degree k. By definition

$$f_n(x) = F_n(x, \lambda, 1) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \Pi_k(c_n)\, x^{n-k}.$$

Define

$$g_n(x) = f_n(x + c_n). \tag{5.2}$$

Then

$$\begin{aligned} g_n(x) &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \Pi_k(c_n) \sum_{j=0}^{n-k} \binom{n-k}{j} x^j c_n^{n-k-j} \\ &= \sum_{j=0}^{n} x^j \sum_{k=0}^{n-j} (-1)^k \binom{n}{k} \binom{n-k}{j} c_n^{n-k-j} \Pi_k(c_n) \\ &= \sum_{j=0}^{n} \binom{n}{j} x^j \sum_{k=0}^{n-j} (-1)^k \binom{n-j}{k} c_n^{n-k-j} \Pi_k(c_n). \end{aligned}$$

Therefore

$$g_n(x) = \sum_{j=0}^{n} \binom{n}{j} h_{n-j}(c_n)\, x^j, \tag{5.3}$$

where

$$h_m(y) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} y^{m-k} \Pi_k(y). \tag{5.4}$$

LEMMA 5.3. *For $n \geqslant 2$,*

$$g_n(0) = -(n-1)\, g_{n-1}(1) - (n-1)(c_n - 1)\, g_{n-2}(2).$$

Proof. By (4.10), $f_n(c_n) = -(n-1)\, f_{n-1}(c_n) - (n-1)(c_n - 1)\, f_{n-2}(c_n)$. The result follows from (5.2). ∎

LEMMA 5.4. *For* $n \geqslant 2$,

$$h_n(y) = -(n-1)\sum_{j=0}^{n-1} \binom{n-1}{j} h_j(y-1)$$
$$-(n-1)(y-1)\sum_{j=0}^{n-2} \binom{n-2}{j} h_j(y-2)\, 2^{n-2-j}. \tag{5.5}$$

Proof. Let $y = c_n = \lambda + n$. The equation is a direct consequence of (5.3) and Lemma 5.3. ∎

LEMMA 5.5. *For* $n \geqslant 0$ $h_n(y)$ *is a polynomial of degree at most* $[n/2]$. *Furthermore,* $h_n(c_n)$ *is a polynomial of degree at most* $[n/2]$ *in* λ.

Proof. The second statement is an immediate consequence of the first. The first statement will be proved by induction. Direct computation from (5.4) yields that $h_0(y) = 1$ and $h_1(y) = 0$. Suppose that $n \geqslant 2$. Induction implies that the right-hand side of (5.5) has degree at most the larger of $[(n-1)/2]$ and $[(n-2)/2] + 1$. Since both of these are at most $[n/2]$ the result follows from (5.5). ∎

Remark. By comparing (5.4) and Lemma 5.5 one sees that the vanishing of the coefficients of y^j in $h_n(y)$ for each $j > [n/2]$ yields many identities involving binomial coefficients. These are presumably well known but they do not appear to be obvious. For $n \neq 1$, $h_n(y)$ probably has degree $[n/2]$ but this is not necessary for the results of this paper. Here are the polynomials for the first few values of n:

$$h_0(y) = 1, \qquad h_1(y) = 0, \qquad h_2(y) = -y,$$
$$h_3(y) = -2y, \qquad h_4(y) = 3y^2 - 6y,$$
$$h_5(y) = 20y^2 - 24y, \qquad h_6(y) = -15y^3 + 130y^2 + 120y,$$
$$h_7(y) = -210y^3 + 924y^2 - 720y,$$
$$h_8(y) = 105y^4 - 2380y^3 + 7308y^2 - 5040y,$$
$$h_9(y) = 2520y^4 - 26432y^3 + 64224y^2 - 40320y.$$

Also it follows easily from (5.4) that $h_n(1) = -(n-1)$ for all n.

Let $f_n(x) = \prod_{j=1}^{n}(x - \theta_j)$. Let $\tilde{\theta}_j = \theta_j - c_n$. Then $g_n(x) = \prod_{j=1}^{n}(x - \tilde{\theta}_j)$. Let $\tilde{s}_m = \sum_{j=1}^{n} \tilde{\theta}_j^m$ as in (2.1). Define

$$\tilde{A}_t = (\tilde{\theta}_j^{i-1}), \qquad \tilde{D}_t = \tilde{A}_t \tilde{A}_t', \qquad \tilde{\Delta}_{n,t}(\lambda) = \det \tilde{D}_t$$

for $1 \leqslant t \leqslant n$ as in (2.2), (2.3), and (2.5). Then $\tilde{D}_t = (\tilde{s}_{i+j-2})$ as in (2.4).

LEMMA 5.6. *$\tilde{\Delta}_{n,t}(\lambda) = \Delta_{n,t}(\lambda)$ for $1 \leqslant t \leqslant n$.*

Proof. Since $\tilde{\theta}_j^m = \sum_{i=0}^m \binom{m}{i}(-1)^i \theta_j^{m-i} c_n^i$ it follows that $\tilde{A}_t = XA_t$, where X is a lower triangular matrix with each diagonal entry equal to 1. Thus $\tilde{D}_t = XD_tX'$ and $\det X = 1$. ∎

LEMMA 5.7. *For $1 \leqslant t \leqslant n$, $\Delta_{n,t}(\lambda)$ is a polynomial in λ of degree at most $t(t-1)/2$.*

Proof. We will first show by induction on m that $\tilde{s}_m$ is a polynomial in λ of degree at most $[m/2]$. This is clear for $m = 1$ as $\tilde{s}_1 = n$. If $1 \leqslant k \leqslant m$ then induction and Lemma 5.5 imply that

$$\text{degree of } h_k(c_m)\,\tilde{s}_{m-k} \leqslant \left[\frac{k}{2}\right] + \left[\frac{m-k}{2}\right] \leqslant \left[\frac{m}{2}\right].$$

Thus (5.3) and Newton's identities, Theorem 2.3, imply that the degree of $\tilde{s}_m$ is at most $[m/2]$.

When the determinant $\tilde{\Delta}_{n,t}(\lambda)$ of $\tilde{D}_t$ is expanded, it is a sum of terms of the form $\prod_{i=0}^{t-1} \tilde{s}_{i+\sigma(i)}$, where σ is a permutation of $\{0,\ldots, t-1\}$. By the previous paragraph such a term is a polynomial in λ of degree at most

$$\sum_{i=0}^{t-1} \left[\frac{i+\sigma(i)}{2}\right] \leqslant \frac{1}{2} \sum_{i=0}^{t-1} (i+\sigma(i)) = \sum_{i=0}^{t-1} i = \frac{t(t-1)}{2}.$$

Hence $\tilde{\Delta}_{n,t}(\lambda)$ is a polynomial in λ of degree at most $t(t-1)/2$. The result follows from Lemma 5.6. ∎

LEMMA 5.8. *For $1 \leqslant t \leqslant n$,*

$$\Delta_{n,t}(\lambda) = C \prod_{j=n-t+1}^{n} c_j^{j-(n-t+1)}$$

for some constant $C \in \mathbb{Q}$.

Proof. By Lemma 5.2, D_t is a matrix whose entries are in the principal domain $\mathbb{Q}[\lambda]$. Let $1 \leqslant k \leqslant n$. By (4.1), $f_n(x) \equiv x^k e(x) \pmod{c_k}$ for some polynomial $e(x) \in \mathbb{Q}[\lambda][x]$. Let $\bar{D}_t$ denote the image of D_t in $\mathbb{Q}[\lambda]/(c_k)$. By Theorem 2.1 the rank of $\bar{D}_t$ is at most $n-k+1$. Hence at least $t-(n-k+1)$ elementary divisors of D_t are divisible by c_k. Thus if $k \geqslant n-t+1$ then $c_k^{k-(n-t+1)} | \Delta_{n,t}(\lambda)$. Therefore

$$\Delta_{n,t}(\lambda) = C(\lambda) \prod_{j=n-t+1}^{n} c_j^{j-(n-t+1)}$$

for some polynomial $C(\lambda) \in \mathbb{Q}[\lambda]$.

By Lemma 5.7,

$$\sum_{j=n-t+1}^{n} (j-(n-t+1)) = \sum_{i=1}^{t-1} i = \frac{t(t-1)}{2} \geqslant \text{degree of } \Delta_{n,t}(\lambda).$$

Hence $C(\lambda) = C \in \mathbb{Q}$. ∎

LEMMA 5.9. *Let* $1 \leqslant t \leqslant n$. *Then*

$$\Delta_{n,t}(\lambda) \equiv n^t (n-1)^{t-1} \cdots (n-t+1)(t-1)^{t-1}(t-2)^{t-2} \cdots 2^2 \pmod{c_{n-t+1}}.$$

Proof. By definition $c_j \equiv j-(n-t+1) \pmod{c_{n-t+1}}$. Thus (4.1) implies that

$$\begin{aligned} f_n(x) &\equiv x^n - n(t-1)\, x^{n-1} + \binom{n}{2}(t-1)(t-2)\, x^{n-2} \cdots \\ &\quad + (-1)^{t-1}\binom{n}{t-1}(t-1)!\, x^{n-t+1} \\ &\equiv x^n - n(t-1)\, x^{n-1} + \binom{t-1}{2} n(n-1)\, x^{n-2} \cdots \\ &\quad + (-1)^{t-1} n(n-1) \cdots (n-t+2)\, x^{n-t+1} \\ &\equiv x^{n-t+1} F_{t-1}(x, n-t+1, 1) \pmod{c_{n-t+1}}. \end{aligned}$$

Let $F_{t-1}(x, n-t+1, 1) = \prod_{j=1}^{t-1} (x-\eta_j)$. Then

$$A_t \equiv \begin{pmatrix} 1 & \ldots, & 1, & 1, \ldots, 1 \\ \eta_1 & \ldots, & \eta_{t-1}, & 0 \quad 0 \\ \vdots & & & \vdots \\ \eta_1^{t-1} & \ldots, & \eta_{t-1}^{t-1}, & 0, \ldots, 0 \end{pmatrix} \pmod{c_{n-t+1}}.$$

Define the $t \times t$ matrix A_t^0 by

$$A_t^0 = \begin{pmatrix} 1 & \ldots, & 1 & \sqrt{n-t+1} \\ \eta_1 & \ldots, & \eta_{t-1} & 0 \\ \vdots & & & \vdots \\ \eta_1^{t-1} & \ldots, & \eta_{t-1}^{t-1} & 0 \end{pmatrix}.$$

Then

$$D_t = A_t A_t' \equiv A_t^0 A_t^{0\prime} \pmod{c_{n-t+1}}.$$

Therefore

$$\Delta_{n,t}(\lambda) \equiv (\det A_t^0)^2 \pmod{c_{n-t+1}}. \tag{5.6}$$

By definition,

$$\det A_t^0 = \pm\sqrt{n-t+1}\,\det(\eta_j^i) = \pm\sqrt{n-t+1}\prod_{j=1}^{t-1}\eta_j \det(\eta_j^{i-1}).$$

Thus (5.6) implies that

$$\Delta_{n,t}(\lambda) \equiv (n-t+1)\left(\prod_{j=1}^{t-1}\eta_j\right)^2 \{\det(\eta_j^{i-1})\}^2 \pmod{c_{n-t+1}}. \tag{5.7}$$

By definition,

$$\prod_{j=1}^{t-1}\eta_j = \pm n(n-1)\cdots+(n-t+2).$$

By (4.3),

$$\begin{aligned}\det(\eta_j^{i-1})^2 &= (t-1)!\prod_{i=1}^{t-1}(i(n-t+1+i))^{i-1}\\ &= n^{t-2}(n-1)^{t-3}\cdots(n-t+3)(t-1)^{t-1}(t-2)^{t-2}\cdots 2^2.\end{aligned}$$

Thus (5.7) yields that

$$\Delta_{n,t}(\lambda) \equiv n^t(n-1)^{t-1}\cdots(n-t+1)(t-1)^{t-1}\cdots 2^2 \pmod{c_{n-t+1}}$$

as required. ∎

Proof of Theorem 5.1. Define $e(\lambda)\in\mathbb{Q}[\lambda]$ by

$$e(\lambda) = \prod_{j=n-t+1}^{n} j(jc_j)^{j-(n-t+1)}.$$

Thus

$$e(\lambda) = \prod_{j=n-t+1}^{n} j^{j-(n-t)} \prod_{j=n-t+1}^{n} c_j^{j-(n-t+1)}.$$

By Lemma 5.8,

$$\Delta_{n,t}(\lambda) - e(\lambda) = \left\{C - \prod_{j=n-t+1}^{n} j^{j-(n-t+1)}\right\} \prod_{j=n-t+1}^{n} c_j^{j-(n-t+1)}.$$

By Lemma 5.9, $\Delta_{n,t}(\lambda) - e(\lambda) \equiv 0 \pmod{c_{n-t+1}}$. Hence

$$C - \prod_{j=n-t+1}^{n} j^{j-(n-t+1)} \equiv 0 \pmod{c_{n-t+1}}$$

and so

$$C - \prod_{j=n-t+1}^{n} j^{j-(n-t)} = 0$$

as it is a constant. Thus $\Delta_{n,t}(\lambda) = e(\lambda)$ as required. ∎

6. The Proof of Theorem B

Let n be a natural number and let p be a prime or ∞. Define

$$\varepsilon_p(n) = \varepsilon_p(F_n(x, 1, 1)).$$

THEOREM 6.1. $\varepsilon_p(4m+3) = 1$ *for* $m = 0, 1, \ldots$.

Proof. For $1 \leqslant t \leqslant n$ let $\Delta(n, t) = \Delta_{n,t}(1)$. By Theorem 5.1

$$\Delta(n, t) \sim (n+1)^{t-1}(n+1-t).$$

Let $n = 4m+3$. Then

$$\prod_{t=1}^{n-1} \Delta(n, t) = (n+1)^{(n-1)(n-2)/2} n! \sim (n+1)!, \tag{6.1}$$

$$\Delta(n, 2k-1)\,\Delta(n, 2k+1) \sim (n-2k)(n+2-2k), \tag{6.2}$$

$$\Delta(n, 2k) \sim (n+1)(n+1-2k). \tag{6.3}$$

By (6.2),

$$\prod_{k=1}^{2m+1} \Delta(n, 2k-1)\,\Delta(n, 2k+1) \sim \sum_{k=1}^{2m+1} (n-2k)(n+2-2k) \sim n. \tag{6.4}$$

Therefore (6.2), (6.3), and (6.4) imply that

$$\begin{aligned}
&\prod_{j=1}^{n} (\Delta(n, j-1), \Delta(n, j))_p \\
&\quad = \prod_{k=1}^{2m+1} (\Delta(n, 2k-1)\,\Delta(n, 2k+1), \Delta(n, 2k))_p \\
&\quad = (n, n+1)_p \prod_{k=1}^{2m+1} ((n-2k)(n+2-2k), (n+1-2k))_p \\
&\quad = (n, n+1)_p \prod_{k=1}^{2m+1} ((2k-1)(2k+1), 2k))_p. \qquad (6.5)
\end{aligned}$$

By (3.2) and (3.4)

$$(n, n+1)_p = (-1, n+1)_p(-n, n+1)_p = (-1, n+1)_p.$$

Hence Theorem 3.1, (6.1), and (6.5) imply that

$$\varepsilon_p(n) = (-1, n!)_p \prod_{k=1}^{2m+1} ((2k-1)(2k+1), 2k)_p. \tag{6.6}$$

The result will now be proved by induction on m. Suppose that $m = 0$. Then (6.6) yields that

$$\varepsilon_p(3) = (-1, 6)_p(3, 2)_p.$$

Thus $\varepsilon_p(3) = 1$ if $p \neq 2$ or 3 by (3.5) and (3.6). By (3.6), $(-1, 6)_3 = (3, 2)_3 = -1$ and so $\varepsilon_3(3) = 1$. Hence by (3.7), $\varepsilon_p(3) = 1$ for all p.

By (6.6),

$$\begin{aligned}\varepsilon_p(n)\,\varepsilon_p(n+4) &= (-1, (n+4)(n+3)(n+2)(n+1))_p \\ &\quad \times ((n+4)(n+2), n+3)_p((n+2)n, n+1)_p \\ &= (-1, (n+4)(n+3)(n+2)(n+1))_p(-(n+4), n+3)_p \\ &\quad \times (-(n+2), n+3)_p(-(n+2), n+1)_p(-n, n+1)_p.\end{aligned}$$

By (3.4), $(-a, a+1)_p = 1$. Hence

$$\begin{aligned}\varepsilon_p(n)\,\varepsilon_p(n+4) &= (-1, (n+4)(n+3)(n+2)(n+1))_p \\ &\quad \times (-(n+2), n+1)_p(-(n+4), n+3)_p \\ &= (-1, (n+4)(n+2))_p(n+2, n+1)_p(n+4, n+3)_p \\ &= (n+4, -(n+3))_p(n+2, -(n+1))_p = 1.\end{aligned}$$

Hence $\varepsilon_p(n+4) = \varepsilon_p(n)$ and the result is proved by induction. ∎

Theorem B is now a direct consequence of Theorem 3.2 and the fact that $F_n(x, 1, 1)$ is irreducible over $\mathbb{Q}$ with A_n as Galois group. See (4.9) and the remark following it.

7. A Property of Galois Groups

We will be concerned with finite groups G which have the following properties:

(7.1) *$G = G' \neq \langle 1 \rangle$ and G contains a unique maximal normal subgroup H.*

(7.2) *Let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. There exists infinitely many Galois extensions E_i of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ such that* $\mathrm{Gal}(E_i/\mathbb{Q}) \simeq G$, *and if L_i is the subfield of E_i corresponding to H then $L_i \neq L_j$ for $i \neq j$.*

Clearly the groups $\tilde{A}_n$ for $n \geqslant 5$ satisfy **(7.1)**. It will be shown below, Theorems 9.6 and 12.2, that $\tilde{A}_5$ and $\tilde{A}_7$ also satisfy **(7.2)**

THEOREM 7.3. *Let K be an algebraic number field. Suppose that for $j = 1,..., k$, G_j satisfies* **(7.1)** *and* **(7.2)**. *Then there exists a Galois extension M of K with* $\mathrm{Gal}(M/K) \simeq G_1 \times \cdots \times G_k$.

Proof. Let $\hat{K}$ be the Galois closure of K in $\bar{\mathbb{Q}}$. It suffices to show the existence of a Galois extension N of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ with $N \cap \hat{K} = \mathbb{Q}$ and $\mathrm{Gal}(N/\mathbb{Q}) \simeq G_1 \times \cdots \times G_k$, because in that case $M = NK$ has the required properties.

The existence of N will be proved by induction on k. If $k = 0$ let $N = \mathbb{Q}$. Suppose that $k > 0$. By induction there exists a Galois extension N_0 of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ with $N_0 \cap \hat{K} = \mathbb{Q}$ and $\mathrm{Gal}(N_0/\mathbb{Q}) \simeq G_1 \times \cdots \times G_{k-1}$.

Suppose that E is a Galois extension of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ with $\mathrm{Gal}(E/\mathbb{Q}) \simeq G$. Let L be the subfield of E corresponding to H. Since $N_0\hat{K}$ has only a finite number of subfields, **(7.2)** implies the existence of such an E so that $L \not\subseteq N_0\hat{K}$. Since $L \cap N_0\hat{K}$ is a Galois extension of $\mathbb{Q}$ and G/H is simple, it follows that $L \cap N_0\hat{K} = \mathbb{Q}$. Thus $E \cap N_0\hat{K} = \mathbb{Q}$, since L is the unique minimal Galois subfield of E. This implies that $E \cap N_0 = \mathbb{Q}$ and

$$\begin{aligned}[EN_0\hat{K}:\mathbb{Q}] &= [E:\mathbb{Q}][N_0\hat{K}:\mathbb{Q}] = [E:\mathbb{Q}][N_0:\mathbb{Q}][\hat{K}:\mathbb{Q}] \\ &= [EN_0:\mathbb{Q}][\hat{K}:\mathbb{Q}].\end{aligned}$$

Thus $EN_0 \cap \hat{K} = \mathbb{Q}$. Therefore $N = EN_0$ has the required poperties. ∎

8. SOME PROPERTIES OF NUMBER FIELDS

LEMMA 8.1. *There exists a prime ideal T in $\mathbb{Z}[\sqrt{15}]$ with $(2) = T^2$. Furthermore if I is any fractional ideal in $\mathbb{Q}(\sqrt{15})$ then exactly one of I or TI is principal.*

Proof. The discriminant of $\mathbb{Q}(\sqrt{15})/\mathbb{Q}$ is 60 and so $(2) = T^2$ ramifies. Suppose that $T = (\alpha)$ is principal. Let $\alpha = a\sqrt{15} + b$ with $a, b \in \mathbb{Z}$. Then

$$\pm 2 = N_{\mathbb{Q}(\sqrt{15})/\mathbb{Q}}(a\sqrt{15} + b) = -15a^2 + b^2$$

and so $b^2 \equiv \pm 2 \pmod 5$ which is not the case. Hence T is not principal. The result follows from the fact that $Q(\sqrt{15})$ has class number 2. See, e.g., [1, p. 422]. ∎

THEOREM 8.2. *Let $5 < p_1 < \cdots < p_k$, where $k \geqslant 1$ and each p_i is a prime with $(15/p_i) = 1$. Let $m = \prod_{i=1}^{k} p_i$. Then there exists $\varepsilon = \pm 1$ or ± 2 and integers a, b with $(15a, b) = 1$ such that $\varepsilon m = 15a^2 - b^2$. Furthermore exactly one of the following holds:*

(i) $m \equiv 3 \pmod 4$, $m \equiv -1 \pmod 3$, $m \equiv \pm 1 \pmod 5$, $\varepsilon = 1$.

(ii) $m \equiv 3 \pmod 4$, $m \equiv 1 \pmod 3$, $m \equiv \pm 2 \pmod 5$, $\varepsilon = 2$.

(iii) $m \equiv 1 \pmod 4$, $m \equiv 1 \pmod 3$, $m \equiv \pm 1 \pmod 5$, $\varepsilon = -1$.

(iv) $m \equiv 1 \pmod 4$, $m \equiv -1 \pmod 3$, $m \equiv \pm 2 \pmod 5$, $\varepsilon = -2$.

Proof. Let $1 \leqslant i \leqslant k$. By assumption $(p_i) = P_i Q_i$ for prime ideals $P_i \neq Q_i$ of $\mathbb{Z}[\sqrt{15}]$. Let $I = \prod_{i=1}^{k} P_i$. By Lemma 8.1 either $I = (\alpha)$ or $TI = (\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{15}]$. Thus $N_{\mathbb{Q}(\sqrt{15})/\mathbb{Q}}(\alpha) = \varepsilon m$ for $\varepsilon = \pm 1$ or ± 2. Since no rational prime divides α it follows that $(15a, b) = 1$.

Since $(15/p_i) = 1$, the quadratic reciprocity theorem implies that each p_i must satisfy one of the sets of congruences (i)–(iv). These sets of congruence form a group under multiplication. Hence m must satisfy one of (i)–(iv). By considering $15a^2 - b^2$ modulo 8, 3, and 5 it can be seen that ε must have the value listed in each case. ∎

THEOREM 8.3. *Let m be a square free integer with $m = 15a_0^2 - b_0^2$ with a_0, $b_0 \in \mathbb{Z}$. Then there exist integers a, b such that $m = 15a^2 - b^2$ and*

$$15a^2 + b^2 \not\equiv 0, \pm 1 \pmod 7 \tag{8.1}$$

$$45a^2 - b^2 \not\equiv 0, \pm 1 \pmod{11}. \tag{8.2}$$

Proof. Let N denote the norm $N_{\mathbb{Q}(\sqrt{15})/\mathbb{Q}}$. Let $\omega = \sqrt{15} + 4$. As $N(\omega) = 1$ it follows that $N(\omega\gamma) = N(\gamma)$ for $\gamma \in \mathbb{Q}(\sqrt{15})$. For any integer i let $\alpha\omega^i = a_i\sqrt{15} + b_i$. Then $m = -N(\alpha\omega^i) = -N(\alpha)$. By definition $a_1 = 4a_0 + b_0$ and $b_1 = 15a_0 + 4b_0$. Observe that $\omega^3 \equiv -1 \pmod 7$ and $\omega^5 \equiv -1 \pmod{11}$.

Suppose that $15x^2 + y^2 \equiv 0$ or $\pm 1 \pmod 7$. Then

$$4x^2 + y^2 \equiv \pm 1 \pmod 7. \tag{8.3}$$

The only solutions of (8.3) are the following where $\varepsilon = \pm 1$:

$$(0, \pm 1), \quad (\pm 1, 0), \quad (2\varepsilon, \pm 2), \quad (2\varepsilon, \pm 3), \quad (3\varepsilon, \pm 2). \tag{8.4}$$

Thus if $(x, y) = (a_0, b_0)$ and $(x, y) = (a_1, b_1)$, both satisfy (8.3) then $(a_0, b_0) = (2\varepsilon, -3\varepsilon)$ or $(3\varepsilon, -2\varepsilon)$. In neither of these cases does (a_2, b_2) satisfy (8.3). Therefore there exists i with $1 \leqslant i \leqslant 2$ such that $m = N(\alpha\omega^i) = 15a^2 - b^2$ and (8.1) holds.

Suppose that $45x^2 - y^2 \equiv 0$ or $\pm 1 \pmod{11}$. Then

$$x^2 - y^2 \equiv 0 \text{ or } \pm 1 \pmod{11}. \tag{8.5}$$

The only solutions of (8.5) are the following where $\varepsilon = \pm 1$:

$$(\varepsilon x, \pm x), \quad (0, \pm 1), \quad (\varepsilon, 0), \quad (2\varepsilon, \pm 4), \quad (2\varepsilon, \pm 5), \quad (4\varepsilon, \pm 2), \quad (5\varepsilon, \pm 2). \tag{8.6}$$

Suppose that $(x, y) = (a_0, b_0)$ and $(x, y) = (a_1, b_1)$ both satisfy (8.5). Since m is square free, not both a_0 and b_0 can be divisible by 11. Thus $(a_i, b_i) \neq (0, 0)$ for all i. Hence the only possibilities for (a_0, b_0) are the following:

$$(3\varepsilon, 3\varepsilon), \quad (4\varepsilon, -4\varepsilon), \quad (\varepsilon, 0), \quad (2\varepsilon, 5\varepsilon), \quad (4\varepsilon, 2\varepsilon), \quad (4\varepsilon, -2\varepsilon), \quad (5\varepsilon, 2\varepsilon).$$

Suppose that also (a_2, b_2) satisfies (8.5). Then $(a_0, b_0) = (4\varepsilon, 2\varepsilon)$ or $(5\varepsilon, 2\varepsilon)$. In neither of these case does (a_3, b_3) satisfy (8.5). Therefore there exists j with $0 \leqslant j \leqslant 3$ such that $m = N(\alpha\omega^j) = 15a^2 - b^2$ and (8.2) holds.

Let $s = 10i + 6j$. Then $\omega^s \equiv \pm\omega^i \pmod 7$ and $\omega^s \equiv \pm\omega^j \pmod{11}$. Then $m = N(\alpha\omega^s) = 15a^2 - b^2$ such that (8.1) and (8.2) hold. ∎

9. The Case $n = 5$

Let $p = \infty$ or a prime. Define $\varepsilon_p(\lambda, \mu) = \varepsilon_p(F_5(x, \lambda, \mu))$.

Lemma 9.1. *Let $p = \infty$ or a prime. Let $\lambda, \mu \in \mathbb{Q}^\times$. Then*

$$\varepsilon_p(\lambda, \mu) = (3\mu c_4, \mu c_5)_p (\mu c_2, 2c_3 c_5)_p (-1, 6c_3 c_4)_p.$$

Proof. For $1 \leqslant i \leqslant 5$ let $\Delta_i = \Delta_{5,i}(\lambda, \mu)$. By Lemma 4.1 and Theorem 5.1

$$\begin{aligned} \Delta_1 &\sim 5, \\ \Delta_2 &\sim \mu c_5 \\ \Delta_3 &\sim 15\mu c_4 \\ \Delta_4 &\sim 2c_3 c_5, \\ \Delta_5 &\sim 15c_2 c_4. \end{aligned}$$

By Theorem 3.1, $\varepsilon_p(\lambda, \mu) = (\Delta_1\Delta_3, \Delta_2)_p (\Delta_3\Delta_5, \Delta_4)_p (-1, \Delta_1\Delta_2\Delta_3\Delta_4)_p$. The result follows by substituting the values of Δ_i for $1 \leqslant i \leqslant 5$. ∎

The following notation will be used in the rest of this section.
a, b are natural numbers with $(15a, b) = 1$ and $15a^2 - b^2 > 0$,

$$\mu = \frac{15a^2 - b^2}{2} > 0, \tag{9.1}$$

$$\lambda = 2b^2 - 15a^2. \tag{9.2}$$

By definition

$$c_2 = b^2 \sim 1, \tag{9.3}$$

$$c_3 = \frac{15a^2 + b^2}{2}, \tag{9.4}$$

$$c_4 = 15a^2 \sim 15, \tag{9.5}$$

$$c_5 = \frac{45a^2 - b^2}{2}. \tag{9.6}$$

Thus in particular,

$$c_j > 0 \qquad \text{for} \quad 2 \leqslant j \leqslant 5. \tag{9.7}$$

THEOREM 9.2. *If p is a prime let $v_p = v_p(15a^2 - b^2)$.*

(i) $\varepsilon_\infty(\lambda, \mu) = 1$.

(ii) *Let p be an odd prime such that v_p is even. Then $\varepsilon_p(\lambda, \mu) = 1$.*

(iii) *Let p be an odd prime such that v_p is odd. Then $\varepsilon_p(\lambda, \mu) = (-10/p)$.*

Proof. By Lemma 9.1 and (9.3)–(9.6),

$$\varepsilon_p(\lambda, \mu) = (5\mu, \mu c_5)_p (\mu, 2c_3 c_5)_p (-1, 10c_3)_p. \tag{9.8}$$

Thus (9.7) implies that $\varepsilon_\infty(\lambda, \mu) = 1$. Now let p be an odd prime and write $(\ ,\ ) = (\ ,\ )_p$. By (3.3),

$$(5\mu, \mu c_5) = (5\mu, c_5)(-5, \mu).$$

Repeated application of (3.1), (3.2), and (3.6) to (9.8) yields that

$$\varepsilon_p(\lambda, \mu) = (c_5, 5)(c_3, -\mu)(\mu, -10), (5, -1). \tag{9.9}$$

By (3.3) and (9.6),

$$(c_5, 5) = (2(45a^2 - b^2), 5) = (-2, 5)(1 - 45(a/b)^2, 45(a/b)^2) = (-2, 5).$$

Thus (9.9) becomes

$$\varepsilon_p(\lambda, \mu) = (2, 5)(c_3, -\mu)(\mu, -10). \tag{9.10}$$

By (9.1) and (9.4), $c_3 \equiv -1 \pmod 3$ and $\mu \equiv 1 \pmod 3$. Thus (9.10) implies that $\varepsilon_3(\lambda, \mu) = 1$. Also (9.1) and (9.3) imply that $c_3 \equiv -2b^2 \pmod 5$ and $\mu \equiv 2b^2 \pmod 5$. Thus (9.10) yields that

$$\varepsilon_5(\lambda, \mu) = (2, 5)(2, -10) = (2, -2) = 1.$$

Since $v_3 = v_5 = 0$ the result is proved for $p = 3$ or 5. Suppose that $p > 5$. By (9.10),

$$\varepsilon_p(\lambda, \mu) = (c_3, -\mu)(\mu, -10). \tag{9.11}$$

Suppose that $v_p(c_3) = 1$. Then $15a^2 \equiv -b^2 \pmod{p}$. Thus $\mu \equiv -b^2 \pmod{p}$ and so $v_p = 0$. Therefore

$$(c_3, -\mu) = (p, -\mu) = (b^2/p) = 1.$$

Thus $\varepsilon_p(\lambda, \mu) = 1$ by (9.11). Hence it may be assumed that $p \nmid 10c_3$. Thus (9.11) implies that $\varepsilon_p(\lambda, \mu) = 1$ if v_p is even. Suppose that v_p is odd. By (9.11)

$$\varepsilon_p(\lambda, \mu) = (\mu, -10c_3) = (p, -10c_3). \tag{9.12}$$

By (9.1) and (9.4), $c_3 \equiv b^2 \pmod{\mu}$. Hence (9.12) implies that

$$\varepsilon_p(\lambda, \mu) = (p, -10) = (-10/p). \quad \blacksquare$$

Let $E(\lambda, \mu)$ denote the splitting field of $F_5(x, \lambda, \mu)$.

THEOREM 9.3. *Suppose that $15a^2 - b^2$ is odd, $2c_5$ is not a 5th power and $2c_3$ is not a cube. Then $G = \mathrm{Gal}(E(\lambda, \mu)/\mathbb{Q}) \simeq A_5$.*

Proof. By (9.4) and (9.6), $2c_5$ and $2c_3$ are odd. Since $(15a, b) = 1$, this implies that $(30, 2c_5) = (30, 2c_3) = 1$. By assumption there exists primes $p_1, p_2 > 5$ so that $3 \nmid v_1(c_3)$ and $5 \nmid v_2(c_5)$, where $v_i = v_{p_i}$. Since $v_i(\mu) = 0$ for $i = 1, 2$ it follows that $v_1(c_i) = 0$ for $i \neq 3$, $1 \leqslant i \leqslant 5$, and $v_2(c_i) = 0$ for $1 \leqslant i \leqslant 4$.

Let $v_1 = v_1(c_3)$. The Newton polygon of $F_5(x, \lambda, \mu)$ at p_1 is the lower convex envelope of the points

$$(0, v_1), \quad (1, v_1), \quad (2, v_1), \quad (3, 0), \quad (4, 0), \quad (5, 0).$$

See, e.g., [17, p. 73]. Thus there is a segment from $(0, v_1)$ to $(3, 0)$ of slope $-v_1/3$. Hence 3 divides the ramification index at p_1 and so $3 \| |G|$.

Let $v_2 = v_2(c_5)$. The Newton polygon of $F_5(x, \lambda, \mu)$ at p_2 is the lower convex envelope of the points

$$(0, v_2), \quad (1, v_2), \quad (2, v_2), \quad (3, v_2), \quad (4, v_2), \quad (5, 0).$$

Thus there is a segment from $(0, v_2)$ to $(5, 0)$ of slope $-v_2/5$. Hence 5 divides the ramification index at p_2 and so $5 \| |G|$. Thus $15 \| |G|$. By (4.5), (9.3), and (9.5) $G \subseteq A_5$. Thus $G = A_5$. $\blacksquare$

Define

$$g(x, \lambda, \mu) = F_5(x + c_5, \lambda, \mu). \tag{9.13}$$

By direct computation or by (5.1) and (5.4) this implies that

$$g(x, \lambda, \mu) = x^5 - 10\mu c_5 x^3 - 20\mu^2 c_5 x^2 + 15\mu^2 c_3 c_5 x + 4\mu^3(5c_4 - \mu)\, c_5. \tag{9.14}$$

The splitting field $E(\lambda, \mu)$ of $F_5(x, \lambda, \mu)$ is also a splitting field of $g(x, \lambda, \mu)$ over $\mathbb{Q}$.

THEOREM 9.4. *Let p be a prime such that $(p, 30ab) = 1$ and $v_p(\mu) = 1$. Then $g(x, \lambda, \mu)$ has a root in $\mathbb{F}_p$ and $v_p(\alpha) = \frac{1}{2}$ for the other 4 roots over $\mathbb{Q}_p$. In particular the ramification index of $E(\lambda, \mu)$ at p is even.*

Proof. By (9.1) and (9.4)–(9.6), $v_p(c_3 c_5) = 0 = v_p(5c_4 - \mu)$. Hence the Newton polygon of $g(x, \lambda, \mu)$ at $\mathbb{Q}_p$ is the lower convex envelope of the points

$$(0, 3), \quad (1, 2), \quad (2, 2), \quad (3, 1), \quad (4, \infty), \quad (5, 0).$$

This consists of a segment of slope $-\frac{1}{2}$ from $(1, 2)$ to $(5, 0)$ and a segment of slope -1 from $(0, 3)$ to $(1, 2)$. Thus $g(x, \lambda, \mu)$ has roots α_i for $1 \leqslant i \leqslant 5$ over $\mathbb{Q}_p$ such that $v_p(\alpha_1) = 1$, $v_p(\alpha_i) = \frac{1}{2}$ for $2 \leqslant i \leqslant 5$. The result follows. ∎

THEOREM 9.5. *Let k be an odd natural number. Let $5 < p_1 < \cdots < p_k$, where each p_i is a prime such that*

$$p_i \equiv 3 \pmod 8, \quad p_i \equiv -1 \pmod 3, \qquad p_i \equiv \pm 1 \pmod 5. \tag{9.15}$$

Let $m = \prod_{i=1}^{k} p_i$. Then $m = 15a^2 - b^2$, where a, b are integers which satisfy (8.1) and (8.2). Let λ, μ be defined by (9.1) and (9.2). Then $\mathrm{Gal}(E(\lambda, \mu)/\mathbb{Q}) \simeq A_5$ and there exists a quadratic extension M of $E(\lambda, \mu)$ which is a Galois extension of $\mathbb{Q}$ such that $\mathrm{Gal}(M/\mathbb{Q}) \simeq \tilde{A}_5$. Furthermore the index of ramification of p_i in $E(\lambda, \mu)$ is even for $1 \leqslant i \leqslant k$.

Proof. By (9.14) and quadratic reciprocity $(15/p_i) = 1$ for all i. By (9.14) m satisfies Theorem 8.2(i). Thus Theorems 8.2 and 8.3 imply the existence of a, b with the required properties. By (8.1) and (9.4), $2c_3$ is not a cube. By (8.2) and (9.6), $2c_5$ is not a 5th power. By Theorem 9.3, $\mathrm{Gal}(E(\lambda, \mu)/Q) \simeq A_5$. Since $p_i > 5$ it follows that $(p_i, 30ab) = 1$ for all i. Hence by Theorem 9.4, p_i has an even ramification index in $E(\lambda, \mu)$. By (9.14) and quadratic reciprocity $(-10/p) = (-2/p)(5/p) = 1$. Thus Theorem 9.2 and (3.7) yield that $\varepsilon_p(\lambda, \mu) = 1$ for $p = \infty$ or a prime. The existence of M now follows from Theorem 3.2. ∎

THEOREM 9.6. *The group $\tilde{A}_5$ satisfies (7.1) and (7.2).*

Proof. Clearly $\tilde{A}_5$ satisfies (7.1). By Dirichlet's theorem there exist infinitely many primes which satisfy (9.15). Theorem 9.4 with $k=1$ and $p=p_1$ yields the result. ∎

10. An Elliptic Curve

We will be concerned with the curve given by the equation

$$y^2 = 105x(x^2-4). \tag{10.1}$$

If $X=105x$, $Y=210y$, then (10.1) is equivalent to

$$Y^2 = 4X^3 - (420)^2X. \tag{10.2}$$

The formulas in [7, p. 12] apply to (10.2) to compute the coordinates of sums of points on the curve. Let P correspond to the solution (5, 105) of (10.1). By direct computation one gets the following table:

Point	X	Y	x	y
P	525	$2(105)^2$	5	105
$2P$	$\frac{29^2}{4}$	$\frac{29.41}{4}$	$\frac{29^2}{420}$	$\frac{29.41}{840}$
$3P$	$\frac{21(5885)^2}{(1259)^2}$		$\frac{5(1177)^2}{(1259)^2}$	

(10.3)

Lemma 10.1. *The point P in* (10.3) *has infinite order. Thus* (10.1) *has positive rank.*

Proof. This follows from the Lutz–Nagell theorem [7, p. 55] by (10.3). ∎

It is well known that (10.1) has positive rank. This is equivalent to the fact that 210 is a "congruent" number. See [5].

Theorem 10.2. *Let (x, y) be a solution of* (10.1) *which corresponds to an odd multiple of P. Then there exist $(x_1, x_2, x_3) \in (\mathbb{Q}^\times)^3$ such that*

$$(x-2, x, x+2) = (3x_1^2, 5x_2^2, 7x_3^2). \tag{10.4}$$

In particular there exist infinitely many solutions (x, y) of (10.1) *such that* (10.4) *holds.*

Proof. By (10.2), $(Y/2)^2 = X(X-210)(X+210)$. Let $\overline{\mathbb{Q}^\times}$ be the group $\mathbb{Q}^\times$ modulo the squares. The map which sends a point $(X, Y/2)$

corresponding to a multiple of P onto $(X-210,\ X,\ X+210)$ defines a homomorphism from the rational points on the curve onto a finite subgroup of $\overline{\mathbb{Q}^\times}$. See [7, pp. 101–105]. The inverse image S of $\overline{(315,525,735)}$ in $(\overline{\mathbb{Q}^\times})^3$ contains all odd multiples of P by (10.3) and is infinite by Lemma 10.1. Any point in S has the property that

$$(X-210,\ X,\ X+210)=(315x_1^2,\ 525x_2^2,\ 735x_3^2)$$

for $(x_1, x_2, x_3)\in(\mathbb{Q}^\times)^3$. The result follows as $X=105x$. ∎

LEMMA 10.3. *Let $f(x)\in\mathbb{C}[x]$. Suppose that $f(x)$ has degree $n\geqslant 1$ and $f(x)$ has n distinct roots. Then the genus of the curve given by $y^2=f(x)$ is $[(n-1)/2]$.*

Proof. This is a direct consequence of Hurwitz's genus formula. See, e.g., [6, p. 25]. ∎

The proof of the next result requires Faltings' theorem which asserts that an algebraic curve of genus greater than 1 has only finitely many rational points.

THEOREM 10.4. *Let r be a prime. Let d be an integer with $d\neq 0,\ \pm 2$. Let $B\geqslant 2$ be a real number. Let S be the set of solutions (x, y) of (10.1) such that if p is a prime with $p>B$ then $r\mid v_p(x-d)$. Then S is finite.*

Proof. Let Q be the set of all primes $q\leqslant B$. Let C be the set of all nonzero rational numbers whose numerator and denominator are products of primes in Q such that $-r<v_q(c)<r$ for all $q\in Q$. Thus C is finite.

Let $(x, y)\in S$. Then $x-d=cx_0^r$ for some $c\in C$ and some $x_0\in\mathbb{Q}^\times$. Let $g(x)=f(cx^r+d)$, where $f(x)=105x(x^2-4)$. Then $g(x)$ has degree $3r$ and $g(x)$ has $3r$ distinct roots. By Lemma 10.3, $y^2=g(x)$ has genus $[(3r-1)/2]\geqslant 2$. Thus by Faltings' theorem $y^2=g(x)$ has only finitely many rational solutions. Hence there are only finitely many choices for (x_0, y) and only finitely choices for $(x, y)\in S$ for each $c\in C$. As C is finite so is S. ∎

THEOREM 10.5. *Let $B>5$ be a real number. There exist primes $p_1, p_2>B$ such that the following holds:*

There exists an ordered triple $(x_1, x_2, x_3)\in(\mathbb{Q}^\times)^3$ such that (x, y) is a solution of (10.1) and

$$(x-2,\ x,\ x+2)=(3x_1^2,\ 5x_2^2,\ 7x_3^2). \tag{10.5}$$

Furthermore

$$v_{p_1}(x+1)>0, \qquad 5\nmid v_{p_1}(x+1). \tag{10.6}$$

$$v_{p_2}(x+3)>0, \qquad 7\nmid v_{p_2}(x+3). \tag{10.7}$$

Proof. By Theorems 10.2 and 10.4 there exist primes $p_1, p_2 > B$ and a solution of (10.1) such that (10.5) holds and

$$(v_1(x+d_1), 10) = 1, \qquad (v_2(x+d_2), 14) = 1, \tag{10.8}$$

where $d_1 = 1$, $d_2 = 3$, $v_i = v_{p_i}$ for $i = 1, 2$. It remains to show that $v_i(x+d_i) > 0$.

Suppose on the contrary that $v = v_i(x+d_i) < 0$ for $i = 1$ or 2. Let $x + d_i = a/b$, for a pair of relatively prime integers a, b. If k is an integer with $|k| \leqslant 5$ then $x + d_i + k = (a + bk)/b$. As $p_i > B > 5$, $p_i \nmid (a + bk)$. Hence $v_i(x + d_i + k) = v$. Therefore (10.1) implies

$$2v_i(y) = v_i(y^2) = v_i(x)\, v_i(x+2)\, v_i(x-2) = 3v.$$

Hence $v_i(x + d_i) = v$ is even contrary to (10.8). ∎

11. $\varepsilon_p(F_7(x, \lambda, 1))$

THEOREM 11.1. *Let (x, y) be a solution of* (10.1) *such that* (10.4) *holds. Let $\lambda = x - 4$.* Then

$$\Delta_{7,7}(\lambda) \sim 1, \tag{11.1}$$

$$\varepsilon_p(F_7(x, \lambda, 1)) = 1 \qquad \textit{for} \quad p = \infty \textit{ or } p \textit{ a prime} \tag{11.2}$$

$$\lambda + 2 \sim 3, \qquad \lambda + 4 \sim 5, \qquad \lambda + 6 \sim 7. \tag{11.3}$$

Proof. By (4.7) and Theorem 10.2 (11.1) and (11.3) hold. It remains to verify (11.2). Choose $p = \infty$ or a prime. Let $(\ ,\ ) = (\ ,\ )_p$ and let $\varepsilon = \varepsilon_p(F_7(x, \lambda, 1))$. For $1 \leqslant i \leqslant 7$ let $\Delta_i = \Delta_{7,i}(F_7(x, \lambda, 1))$. By Theorem 3.1,

$$\varepsilon = (\Delta_2, \Delta_1\Delta_3)(\Delta_4, \Delta_3\Delta_5)(\Delta_6, \Delta_5\Delta_7)\Big(-1, \prod_{j=1}^{6} \Delta_j\Big).$$

By Theorem 5.1,

$$\Delta_1 \sim 7, \qquad \Delta_2 \sim 6c_7, \qquad \Delta_3 \sim 35c_6, \qquad \Delta_4 \sim 6c_7c_5,$$
$$\Delta_5 \sim 105c_6c_4, \qquad \Delta_6 \sim 3c_7c_5c_3, \qquad \Delta_7 \sim 1.$$

Thus

$$\varepsilon = (6c_7, 35)(6c_7c_5, 15)(3c_7c_5c_3, 3)(-1, 35c_7c_3).$$

By (3.1)–(3.3) this yields that

$$\varepsilon = (c_7, -7)(c_5, 5)(c_3, -3)(7, -6)(5, -1)(3, 2).$$

By (3.4), $(7, -6) = 1$. By (3.6) and (3.7), $(5, -1) = 1$. Hence

$$\varepsilon = (c_7, -7)(c_5, 5)(c_3, -3)(3, 2). \tag{11.4}$$

Since $c_7 = c_6 + 1 = 7u^2 + 1$, (3.4) yields that

$$(c_7, -7) = (7u^2 + 1, -7u^2) = 1.$$

As $c_3 = c_2 + 1 = 3u^2 + 1$, (3.4) yields that

$$(c_3, -3) = (3u^2 + 1, -3u^2) = 1.$$

Hence (11.4) becomes

$$\varepsilon = (c_5, 5)(3, 2). \tag{11.5}$$

Since $c_5 = c_4 + 1 = 5u^2 + 1$, (3.4) yields that

$$(c_5, 5) = (5u^2 + 1, 5u^2) = (5u^2 + 1, -1) = (c_5, -1). \tag{11.6}$$

As $c_5 = c_2 + 3 = 3u^2 + 3$, (11.5), (11.6), and (3.4) now imply that

$$\varepsilon = (3u^2 + 3, -1)(3, 2) = (3, -2)(u^2 + 1, -1) = (3, -2).$$

By (3.5)–(3.7) this yields that $\varepsilon = 1$. ∎

12. The Case $n = 7$

THEOREM 12.1. *Let $\lambda \in \mathbb{Q}^\times$. Suppose that there exist primes $p_1, p_2 > 7$ so that*

$$v_1(\lambda + 5) > 0, \qquad 5 \nmid v_1(\lambda + 5), \tag{12.1}$$

$$v_2(\lambda + 7) > 0, \qquad 7 \nmid v_2(\lambda + 7), \tag{12.2}$$

where $v_i = v_{p_i}$ for $i = 1, 2$. Let E be the splitting field of $F_7(x, \lambda, 1)$ over $\mathbb{Q}$. Then p_1 and p_2 ramify in E. Furthermore $A_7 \subseteq \mathrm{Gal}(E/\mathbb{Q}) \subseteq \Sigma_7$.

Proof. Let $c_j = \lambda + j$ for $1 \leqslant j \leqslant 7$. Since $p_1, p_2 > 7$ it follows that $v_1(c_j) = 0$ for $j \neq 5$ and $v_2(c_j) = 0$ for $j \neq 7$. Let $v_1 = v_1(c_5)$, $v_2 = v_2(c_7)$. The Newton polygon at p_1 of $F_7(x, \lambda, 1)$ is the lower convex envelope of the points

$$(0, v_1), \quad (1, v_1), \quad (2, v_1), \quad (3, v_1), \quad (4, v_1), \quad (5, 0), \quad (6, 0), \quad (7, 0).$$

Thus there is a segment of slope $-v_1/5$ from $(0, v_1)$ to $(5, 0)$. Hence 5 divides the ramification index at p_1. See, e.g., [17, p. 73]. The Newton polygon at p_2 of $F_7(x, \lambda, 1)$ is the lower convex envelope of the points

$$(0, v_2), \quad (1, v_2), \quad (2, v_2), \quad (3, v_2), \quad (4, v_2), \quad (5, v_2), \quad (6, v_2), \quad (7, 0).$$

Thus there is a segment of slope $-v_2/7$ form $(0, v_2)$ to $(7, 0)$. Hence 7 divides the ramification index at p_2.

Therefore $\mathrm{Gal}(E/\mathbb{Q})$ is a subgroup of Σ_7 whose order is divisible by 35. Thus $A_7 \subseteq \mathrm{Gal}(E/\mathbb{Q})$. ∎

THEOREM 12.2 *Let $B > 7$ be a real number. Choose p_1, p_2, x as in Theorem* 10.5. *Let $\lambda = x - 4$. Let E be the splitting field of $F_7(x, \lambda, 1)$. Then p_1 and p_2 ramify in E and $\mathrm{Gal}(E/\mathbb{Q}) \simeq A_7$. Furthermore, there exists a quadratic extension M of E which is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \simeq \tilde{A}_7$. Thus in particular the group $\tilde{A}_7$ satisfies* **(7.1)** *and* **(7.2)**.

Proof. Theorem 10.5 and (10.1) imply that

$$\lambda + 2 \sim 3, \qquad \lambda + 4 \sim 5, \qquad \lambda + 6 \sim 7 \tag{12.3}$$

$$105(\lambda + 2)(\lambda + 4)(\lambda + 6) = y^2 \tag{12.4}$$

for some $y \in \mathbb{Q}^\times$. By Theorem 10.5, (12.1) and (12.2) are satisfied. By (4.7) and (12.4) $G \subseteq A_7$. Hence $G \simeq A_7$ and p_1 and p_2 ramify in E by Theorem 12.1. The existence of M follows from Theorems 3.2 and 11.1 and (12.3). ∎

13. K-ADMISSIBLE GROUPS

Let $K \subseteq L$ be algebraic number fields. L is *K-adequate* if L is a maximal subfield of a finite dimensional division algebra with center K.

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

The following basic result is proved in [9].

THEOREM 13.1. *Let K be a number field and let L be a Galois extension of K. Let $G = \mathrm{Gal}(L/K)$. The following are equivalent.*

(i) *L is K-adequate.*

(ii) *If p is any prime and P is a S_p-group of G then $P \subseteq \mathrm{Gal}(LK_i/K_i)$ for at least two completions K_1 and K_2 of K.*

The next two results are consequences of Theorem 13.1.

THEOREM 13.2. [9, Theorem 4.1]. *If G is $\mathbb{Q}$-admissible then every Sylow group of G is meta-cyclic.*

THEOREM 13.3. [2, Theorem 1.1]. *If G is K-admissible for every number field K then every Sylow group of G is either cyclic or the direct product of two cyclic groups.*

It is conceivable that A_5 is K-admissible for every number field K. It is known that A_5 is K-admissible if $\sqrt{-1} \notin K$[3]. Also M. Schacher has informed me that in unpublished work D. Saltman has shown that A_5 is K-admissible if $\sqrt{5} \in K$. In Section 14 we give a class of number fields K such that A_5 is K-admissible. A similar result is also proved for $\tilde{A}_5$. In [13] it is shown that $\tilde{A}_5$ in $\mathbb{Q}$-admissible.

THEOREM 13.4. *Let $L \subseteq M$ be Galois extensions of the algebraic number field K such that $G = \mathrm{Gal}(L/K)$ and $\tilde{G} = \mathrm{Gal}(M/K)$. Assume that*

$$\langle 1 \rangle \to Z_2 \to \tilde{G} \to G \to \langle 1 \rangle$$

is a nonsplit exact sequence. Then if L is K-adequate, so is M.

Proof. Let p be a prime and let P be an S_p-group of G. By Theorem 13.1 $P \subseteq \mathrm{Gal}(LK_i/K_i)$ for at least two completions K_1 and K_2 of K.

Suppose that $p \neq 2$. Then P is isomorphic to a S_p-group of $\tilde{G}$. Thus $\mathrm{Gal}(MK_i/K_i)$ contains a S_p-group of $\tilde{G}$ for $i = 1, 2$.

Suppose that $p = 2$. Let T_0 be an S_2-group of $\mathrm{Gal}(MK_i/K_i)$. Then T_0 is mapped onto a S_2-group T of G and $T \subseteq T_0$. Since restriction is injective in cohomology

$$\langle 1 \rangle \to Z_2 \to \tilde{T} \to T \to \langle 1 \rangle$$

is nonsplit. Hence $T_0 = \tilde{T}$. Thus Theorem 13.1 implies that M is K-adequate. ∎

THEOREM 13.5. *Let K be an algebraic number field and let $K \subseteq L \subseteq M$, where L and M are Galois extensions of K with $G = \mathrm{Gal}(L/K) \simeq A_5$ and $\mathrm{Gal}(M/K) \simeq \tilde{A}_5$. Let T be a S_2-group of G. Suppose that there are two completions K_1 and K_2 of K so that $T \subseteq \mathrm{Gal}(LK_i/K_i)$ for $i = 1, 2$. Then L and M are K-adequate.*

Proof. If p is an odd prime then a S_p-group P of A_5 or $\tilde{A}_5$ is cyclic. Thus the Tchebotarev density theorem implies that $P \subseteq \mathrm{Gal}(LK_i/K_i)$ for infinitely many completions K_i of K. Thus L is K-adequate by Theorem 13.1. Hence M is K-adequate by Theorem 3.4. ∎

14. K-ADMISSIBILITY OF A_5 AND $\tilde{A}_5$

LEMMA 14.1. *Let K be an algebraic number field and let $\hat{K}$ be the Galois closure of K in some algebraic closure. Assume that $\sqrt{10} \notin \hat{K}(\sqrt{15})$. Let $5 < p_1 < p_2 < p_3$ where each p_i is a prime which does not ramify in $\hat{K}$ such that the following hold.*

(i) *Let σ_i denote the Frobenius automorphism corresponding to p_i. Then*

$$\langle \sigma_1 \rangle = \langle \sigma_2 \rangle = \mathrm{Gal}(\hat{K}(\sqrt{10}, \sqrt{15})/\hat{K}(\sqrt{15})). \tag{14.1}$$

(ii) *Let $m = p_1 p_2 p_3$. Then $(15/p_3) = 1$ and*

$$m \equiv 3 \pmod 4, \qquad m \equiv -1 \pmod{15}. \tag{14.2}$$

Then $m = 15a^2 - b^2$ such that (8.1) and (8.2) hold. Let μ, λ be defined by (9.1) and (9.2). Then $\mathrm{Gal}(\hat{K}E(\lambda, \mu)/\hat{K}) \simeq A_5$ and $4 | [\hat{K}_i E(\lambda, \mu) : \hat{K}_i]$ for $i = 1, 2$ where $\hat{K}_i$ is the completion of $\hat{K}$ at p_i.

Proof. By (14.1),

$$\sqrt{10} \notin \hat{K}_i, \qquad (15/p_i) = 1 \tag{14.3}$$

for $i = 1, 2$. By Theorems 8.2 and 8.3, a, b, exist with the required properties. By Theorem 9.4, each p_i ramifies in $E(\lambda, \mu)$. By (8.1) and (9.4), $2c_3$ is not a cube. By (8.2) and (9.6), $2c_5$ is not a 5th power. Thus Theorem 9.3 implies that

$$\mathrm{Gal}\,(\hat{K}E(\lambda, \mu)/\hat{K}) \simeq \mathrm{Gal}(E(\lambda, \mu)/E(\lambda, \mu) \cap \hat{K}) \simeq \mathrm{Gal}(E(\lambda, \mu)/\mathbb{Q}) \simeq A_5.$$

Let $G_i = \mathrm{Gal}(\hat{K}_i E(\lambda, \mu)/\hat{K}_i)$ for $i = 1, 2$. By Theorem 9.4, $G_i \subseteq A_4$ and $2 | |G_i|$. Thus either $4 | |G_i|$ or $|G_i| = 2$.

Suppose that the result is false. Then $|G_i| = 2$ for $i = 1$ or 2. Let $\mathbb{Q}_i = \mathbb{Q}_{p_i}$. Hence $[\hat{K}_i E(\lambda, \mu) : \hat{K}_i] = [E(\lambda, \mu)\,\mathbb{Q}_i : \mathbb{Q}_i] = 2$ and so $\hat{K}_i E(\lambda, \mu) = \hat{K}_i(\pi)$, where $\pi^2 = up_i$ for some unit u in $\mathbb{Q}_i$. Let $g(x, \lambda, \mu) = F_5(x + c_5, \lambda, \mu)$. By Theorem 9.4 there exists a unit v of $E(\lambda, \mu)\,\mathbb{Q}_i$ such that $v\pi$ is a root of $g(x, \lambda, \mu)$. By (9.14),

$$0 \equiv g(v\pi, \lambda, \mu) \equiv v^5\pi^5 - 10\mu c_5 v^3\pi^3 + 15\mu^2 c_3 c_5 v\pi \pmod{p_i^3}. \tag{14.4}$$

Let $\mu = dp_i$. Thus $\mu = du^{-1}\pi^2$. Hence (14.4) implies that

$$0 \equiv v^4 - 10\, du^{-1}v^2 c_5 + 15\, d^2 u^{-2} c_3 c_5 \pmod \pi. \tag{14.5}$$

Since v is a unit in $E(\lambda, \mu)\,\mathbb{Q}_i$ there exists a unit $v_0 \in \mathbb{Q}_i$ such that $v \equiv v_0 \pmod \pi$. Therefore (14.5) implies that

$$u^2 v_0^4 - 10\, duv_0^2 c_5 + 15\, d^2 c_3 c_5 \equiv 0 \pmod{p_i}. \tag{14.6}$$

By (9.1), (9.4), and (9.6),

$$c_5 \equiv c_3 \equiv b^2 \pmod \mu.$$

Hence (14.6) implies that

$$u^2v_0^4 - 10\,duv_0^2b^2 + 15\,d^2b^4 \equiv 0 \pmod{p_i}.$$

Therefore $uv_0^2 \equiv 5db^2 \pm db^2\sqrt{10}$. Hence $\sqrt{10} \in \hat{K}$, contrary to (14.3). ∎

THEOREM 14.2. *Let K be an algebraic number field and let $\hat{K}$ denote its Galois closure over $\mathbb{Q}$ in some algebraic closure. If $\sqrt{10} \notin \hat{K}(\sqrt{15})$ then A_5 is K-admissible.*

Proof. By the Tchebotarev density theorem there exist primes p_1 and p_2 which satisfy (14.1). Thus $(15/p_1) = (15/p_2) = 1$ and p_1, p_2 satisfy one of Theorem 8.2(i)–(iv). Hence p_1p_2 satisfies one of these conditions. By Dirichlet's theorem there exists a prime p_3 such that $m = p_1p_2p_3$ satisfies Theorem 8.2(i). Hence p_3 satisfies one of Theorem 8.2(i)–(iv) and so $(15/p_3) = 1$. The result follows from Theorem 13.1 and Lemma 14.1. ∎

THEOREM 14.3. *Let K be an algebraic number field and let $\hat{K}$ denote its Galois closure over $\mathbb{Q}$ in some algebraic closure. If $\sqrt{10} \notin \hat{K}(\sqrt{3}, \sqrt{5}, \sqrt{-2})$ then $\tilde{A}_5$ is K-admissible.*

Proof. Let $F = \hat{K}(\sqrt{5}, \sqrt{3}, \sqrt{-2})$. By the Tchebotarev density theorem there exist primes p_i for $i = 1, 2, 3$ with $5 < p_1 < p_2 < p_3$ such that p_i does not ramify in F for $i = 1, 2, 3$ and such that if σ_i is the Frobenius automorphism of $F(\sqrt{10})$ at p_i then $\langle \sigma_i \rangle = \mathrm{Gal}(F(\sqrt{10})/F)$. Then $\sqrt{10} \notin F_i = F\mathbb{Q}_i$, where $\mathbb{Q}_i$ is the completion of $\mathbb{Q}$ at p_i. Hence the residue class degree of p_i in F is odd. Therefore

$$\left(\frac{-2}{p_i}\right) = \left(\frac{3}{p_i}\right) = \left(\frac{5}{p_i}\right) = 1, \qquad \left(\frac{10}{p_i}\right) = -1.$$

Thus

$$\left(\frac{-1}{p_i}\right) = \left(\frac{-2}{p_i}\right)\left(\frac{5}{p_i}\right)\left(\frac{-1}{p_i}\right) = \left(\frac{10}{p_i}\right) = -1.$$

Hence

$$p_i \equiv 3 \pmod 8, \qquad p_i \equiv -1 \pmod 3, \qquad p_i = \pm 1 \pmod 5.$$

By Theorem 13.1 and Lemma 14.1, $KE(\lambda, \mu)$ is K-adequate and $\mathrm{Gal}(KE(\lambda, \mu)/K) \simeq A_5$. By Theorem 9.5 there exists a Galois extension M of $\mathbb{Q}$ with $E(\lambda, \mu) \subseteq M$ and $\mathrm{Gal}(M/Q) \simeq \tilde{A}_5$. Thus $K \cap M = \mathbb{Q}$ and

$$\mathrm{Gal}(KM/K) \simeq \mathrm{Gal}(M/\mathbb{Q}) \simeq \tilde{A}_5.$$

By Theorem 13.5, KM is K-adequate. ∎

REFERENCES

1. Z. I. BOREVICH AND I. R. SHAFAREVICH, "Number Theory," Academic Press, New York/London, 1966.
2. B. GORDON AND M. SCHACHER, Quartic coverings of a cubic, *in* "Number Theory and Algebra," pp. 97–101, Academic Press, New York/London, 1977.
3. B. GORDON AND M. SCHACHER, The admissibility of A_5, *Number Theory* **11** (1979), 498–504.
4. N. JACOBSON, "Basic Algebra II," Freeman, San Francisco, 1980.
5. N. KOBLITZ, "Introduction to Elliptic Curves and Modular Forms," Springer-Verlag, Berlin/Heidelberg/New York, 1984.
6. S. LANG, "Introduction to Algebraic and Abelian Functions," Addison–Wesley, Reading, Mass., 1972.
7. S. LANG, "Elliptic Curves: Diophantine Analysis," Springer-Verlag, Berlin/Heidelberg/New York, 1978.
8. G. POLYA AND G. SZEGO, "Problems and Theorems in Analysis II," Springer-Verlag, Berlin/Heidelberg/New York, 1976.
9. M. SCHACHER, Subfields of division rings I, *J. Algebra* **9** (1968), 451–477.
10. I. SCHUR, "Collected Works," Vol. III, Springer-Verlag, Berlin/Heidelberg/New York, 1973.
11. J.-P. SERRE, "Cours d'Arithmétique," Presses Univ. France, Paris, 1970.
12. J.-P. SERRE, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment Math. Helv.* **59** (1984), 651–676.
13. J. SONN, $SL(2, 5)$ and Frobenius Galois groups over Q, *Canad. J. Math.* **32** (1980), 281–293.
14. N. VILA, Sur la resolution d'un problème de plongement, Lecture Notes in Math., Vol. 1068, pp. 243–259, Springer-Verlag, New York/Berlin, 1983.
15. N. VILA, Polynomials over Q solving an embedding problem, *Ann. Inst. Fourier (Grenoble)* **35**, 2 (1985), 79–82.
16. N. VILA, On central extensions of A_n as Galois group over $\mathbb{Q}$, *Arch. Math. (Basel)* **44** (1985), 424–437.
17. E. WEISS, "Algebraic Number Theory," Chelsea, New York, 1963.