HT90 and "simplest" number fields

Kurt Foster

Abstract

A standard formula (1) leads to a proof of HT90, but requires proving the existence of θ such that $\alpha \neq 0$, so that $\beta = \alpha/\sigma(\alpha)$.

We instead impose the condition (M), that taking $\theta = 1$ makes $\alpha = 0$. Taking $n = 3$, we recover Shanks's simplest cubic fields. The "simplest" number fields of degrees 3, 4, 5, and 6, Washington's cyclic quartic fields, and a certain family of totally real cyclic extensions of $\mathbb{Q}(\cot(\pi/4m))$ also have primitive elements which are *units* satisfying this condition.

Further investigation of (M) for $n = 4$ leads to an elementary algebraic construction of a 2-parameter family of octic polynomials with "generic" Galois group ${}_8T_{11}$. Imposing an additional algebraic condition on these octics produces a new family of cyclic quartic extensions. This family includes the "simplest" quartic fields and Washington's cyclic quartic fields as special cases.

We obtain more detailed results on our octics when the parameters are algebraic integers in a number field. In particular, we identify certain sets of special units, including exceptional sequences of 3 units, and give some of their properties.

1 Introduction

Hilbert's Theorem 90 (See, e.g. [16]) characterizes elements β of norm 1 in a cyclic extension $L/\mathbf{k}$ of degree n with Galois group $G = \langle\sigma\rangle$; one has

$$\mathcal{N}_{L/\mathbf{k}}(\beta) = 1 \text{ if, and only if, } \beta = \alpha/\sigma(\alpha) \text{ for some } \alpha \in L. \qquad \text{(HT90)}$$

"If" is obvious. The usual proof of "only if " uses the formula

$$\alpha = \theta + \sigma(\theta)\beta + \sigma^2(\theta)\beta\sigma(\beta) + \ldots + \sigma^{n-1}(\theta)\beta\sigma(\beta)\cdots\sigma^{n-2}(\beta). \qquad (1)$$

If $\mathcal{N}_{L/\mathbf{k}}(\beta) = 1$, this formula makes $\alpha/\sigma(\alpha) = \beta$ a formal identity. One has to show that $\alpha \neq 0$ for some $\theta \in L$ to complete the proof.

In [6], Chapter XI, Theorem 2 there is a constructive proof of (HT90) for $n = 2$. It actually exhibits a nonzero α: Substituting $\theta = 1$ gives the simplified formula

$$\alpha = 1 + \beta.$$

This gives a nonzero α unless $\beta = -1$, and this case is handled separately.

We note that $\theta = 1$ is the *only* nonzero value guaranteed to be in *every* field. We make this choice for arbitrary n. We assume $L/\mathbf{k}$ is a finite Galois extension with Galois group G, and $\sigma \in G$ is of order n. We impose the condition on $r \in L$ that

$$1 + r + r\sigma(r) + \ldots + r\sigma(r)\cdots\sigma^{n-2}(r) = 0. \tag{M}$$

We call (M) the *Murphy condition*. As the condition is stated, $L/\mathbf{k}$ need not be cyclic. This is simply because for all we know, L^σ could be a *proper* extension of $\mathbf{k}$. This in fact happens in §4, even with the additional conditions in Eq. (1.3).

The following formal properties are immediate:

Proposition 1.1. *Let* $\mathbf{k}$, L, σ, r *and* n *satisfy* (M). *Then*

(a) (M) *holds if* r *is replaced by* $\sigma^i(r)$, $1 \le i \le n-1$.

(b) $r\sigma(r)\cdots\sigma^{n-1}(r) = 1$.

Proof. For (a), apply σ^i to (M). For (b), apply σ to (M), multiply by r, and subtract (M). □

If $\mathbf{k}(r)/\mathbf{k}$ is cyclic of degree n and r is an *algebraic integer* satisfying (M), $\mathbf{k}(r)$ has elements z with an unusual property (see the end of §2). By Prop. 1.1(b), such r are *units*, which we call *Murphy's units*.

We take as a simple example the case $n = 3$. Then (M) becomes

$$1 + r + r\sigma(r) = 0. \tag{M3}$$

Solving for $\sigma(r)$ and repeatedly applying σ, treating it as a field automorphism, we obtain the expressions

$$\sigma(r) = \frac{-r-1}{r},\ \sigma^2(r) = \frac{-1}{r+1},\ \sigma^3(r) = r. \tag{C3}$$

$$\text{Setting } r + \sigma(r) + \sigma^2(r) = A,\ A \in \mathbf{k} \tag{Tr3}$$

and clearing fractions, we find that any r for which (M3) and (Tr3) hold is a zero of

$$p(x) = x^3 - Ax^2 - (A+3)x - 1, \text{ for some } A \in \mathbf{k}. \tag{P3}$$

By Proposition 2.3, *every* cyclic cubic field extension has a defining polynomial of this form. However, if we take $\mathbf{k} = \mathbb{Q}$ and $A \in \mathbb{Z}$, $p(x)$ is irreducible (mod 2), so this restriction on the parameter produces a family of cyclic cubic fields in which 2 remains inert, which is clearly *not* true of all cyclic cubic fields. In [33], D. Shanks called the fields defined by (P3) with $A \in \mathbb{Z}$ the "simplest" cubic fields. Certain families of cyclic number fields of degrees 4, 5, and 6 have subsequently been dubbed "simplest." They, too, have defining polynomials whose zeroes are units satisfying (M). We have the following result:

Proposition 1.2. *Let* $\mathbf{k}$ *be a field,* $t \in \mathbf{k}$*. In each of the following cases,* $\sigma(x) \pmod{P(x)}$ *makes* (M) *a formal identity, with* n *equal to the degree of* $P(x)$*.*

a) $P(x) = x^3 - tx^2 - (t+3)x - 1, \sigma(x) = (-x-1)/x;$

b) $P(x) = x^4 - tx^3 - 6x^2 + tx + 1, \sigma(x) = (-x-1)/(x-1);$

c) $P(x) = x^4 + (t^2+2t+4)x^3 + (t^3+3t^2+4t+6)x^2$
$+ (t^3+t^2+2t+4)x + 1,$
$\sigma(x) = (-x^3 + (-t^2-2t-4)x^2 + (-t^3-3t^2-4t-5)x$
$- t^3 - t^2 - 2t - 2)/t;$

d) $P(x) = x^5 - t^2x^4 - (2t^3+6t^2+10t+10)x^3$
$- (t^4+5t^3+11t^2+15t+5)x^2 + (t^3+4t^2+10t+10)x - 1,$
$\sigma(x) = ((-t-1)x^4 + (t^3+2t^2+3t+3)x^3$
$+ (t^4+4t^3+9t^2+14t+8)x^2 + (-t^4-7t^3-19t^2-29t-19)x$
$+ (-t^4-6t^3-16t^2-20t-9))/(t^3+5t^2+10t+7);$ *and*

e) $P(x) = x^6 - 2tx^5 - (5t+15)x^4 - 20x^3 + 5tx^2 + (2t+6)x + 1,$
$\sigma(x) = (-2x-1)/(x-1).$

Proof. For (a), (b), and (e), the fact that (M) becomes a formal identity is easily checked by hand. The others can be checked with symbolic algebra software. The author (with Phil Carmody's guidance) used Pari-GP. □

Remarks. The term "formal identity" means that substituting $\sigma(x)$ and its compositional powers $\pmod{P(x)}$ into (M) gives a quotient of polynomials in which $P(x)$ divides the numerator. For the $\sigma(x)$ which are independent of t in (a), (b), and (e), one can make the stronger statement that (M) actually evaluates to 0 at any x for which all the terms in the sum are defined.

Shanks's 1974 paper [33] seems to be the first to refer to certain families of number fields as "simplest." The polynomials in (a) had previously appeared in H. Cohn's 1956 paper [5]. They yield explicit systems of independent units, a property which Shanks sought. When this system is fundamental, the regulator is very small. A great deal of research has been done on these cubics.

In [40], L.C. Washington extended Uchida's work in [38], to force class numbers divisible by n in the "simplest" cubic fields, and used elliptic curves to describe the 2-Sylow subgroup of their class groups, and to exhibit explicit quartic extensions of these fields.

In [28], Patrick Morton gave a parameterization of cyclic cubic fields based on automorphism polynomials, and obtained Shanks's simplest cubics by change of parameter. Robin Chapman simplified Morton's proofs in [2].

E. Thomas proved in [37] that if r is a zero of a Shanks's simplest cubic, then $\langle r, r+1\rangle$ is a system of fundamental units for the order $\mathbb{Z}[r]$.

The property that r and $r+1$ are both units makes $r, r+1$ an *exceptional sequence* in the sense of Lenstra [20]: a finite sequence $r_1, \ldots, r_k$ of units, the difference of any two of which is also a unit (and $r_2 - r_1 = 1$) . This generalizes Nagell's definition of *exceptional units* in [30]. D. Buell and V. Ennola studied the only other family of totally real cubic fields with exceptional units in [1].

The polynomials in (b) were constructed in [9], while those in (e) were introduced (in a slightly different form) in [8]. The quintics in (d) are of the form $-f(-x)$ where $f(x)$ is one of the quintics introduced by E. Lehmer in [19]. She observed in this paper that the zeroes of the cubic polynomials in [33] and the quartic and sextic polynomials in [9] and [8] are, in the case of a prime conductor, integer translates of Gaussian periods, and obtained quintic units with the same property. In [32] (Appendix), R. Schoof and L.C. Washington proved that the integer-translates property characterizes the "simplest" fields of degrees 2, 3, and 4 with prime conductor. In [17], A. Lazarus applied the term "simplest" to these fields of degrees 2 to 6, as well as to a family of octic fields constructed by Y.Y. Shen in [34].

In Proposition 4.17 we show that for $t \in \mathbf{k} - \{0, -2\}$, the polynomial $P(x)$ in (c), which falls out from (M) and the conditions in Eq. (1.3) with $n = 4$, defines the same extension as the polynomial

$$f_t(x) = x^4 - t^2x^3 - (t^3 + 2t^2 + 4t + 2)x^2 - t^2x + 1 \tag{1.1}$$

which L.C. Washington constructed in [41]. In [29], Patrick Morton proved the equivalence of these fields with cyclic quartic fields whose Galois groups have a quadratic (rather than cubic) generating automorphism polynomial.

In [33] Shanks also proposed "simplest" quadratic fields defined by the polynomials $x^2 = ax + 1$, $a \in \mathbb{Z}$. These quadratic fields have a special significance with respect to (M). For if $v^2 - tv - 1 = 0$, $t \in \mathbb{Z} - \{0, -2\}$, the cyclic quartic field L defined by $f_t(x)$ contains v, and if $G(L/\mathbb{Q}) = \langle\sigma\rangle$, we have

$$1 + v + v\sigma(v) + v\sigma(v)\sigma^2(v) = 1 + v + (-1) + (-1)v = 0. \tag{1.2}$$

That is, quadratic units of norm -1 (unlike those of norm $+1$), satisfy (M) with $n = 4$ when embedded in a cyclic quartic field (such as a Washington's cyclic quartic field). We give a generalization of this phenomenon based on (M), in the remarks following Proposition 2.3.

The "simplest" number fields of degrees 3, 4, and 6 were studied further by G. Lettl, A. Pethő, and P. Voutier in [21] and [22]. A. Lazarus studied the unit groups and class numbers of the "simplest" quartic fields in [17].

L. C. Washington used coverings of modular curves in [41] to construct his family of cyclic quartic fields. He observed that the "simplest" fields of degree 2, 3, 4, 5, and 6 can be constructed by the same method. (See [7] with regard

to Emma Lehmer's quintics.) He further observed that in all these cases, the coverings have genus 1. In contrast, the cyclic sextic fields constructed by O. Lecacheux in [18], use a covering of genus 2.

In [26], S. Louboutin obtained explicit formulas for powers of Gaussian sums attached to the "simplest" fields of degrees 2 to 6, and used them to give efficient computations of their class numbers.

In §3, we construct a 1-parameter family of polynomials of degree n in $\mathbb{Q}(\cot(\pi/n))[x]$, whose zeroes are permuted cyclically by a linear fractional transformation λ of compositional order n for each $n > 1$, generalizing a construction in [34]. When $n = 4m$, $\sigma = \lambda^{-1}$ makes (M) a formal identity.

For $n > 3$ we cannot simply "solve" (M) for σ as we did in (C3); but we would like to obtain as general an algebraic map of compositional order n as possible, that makes (M) a formal identity. So, we impose purely algebraic conditions which always hold when $\mathbf{k}(r)/\mathbf{k}$ is cyclic of degree n with $G = \langle\sigma\rangle$:

$$\sum_{i=0}^{\frac{n}{d}-1} \sigma^i \left(\prod_{j=0}^{d-1} \sigma^{\frac{jn}{d}}(r) \right) \in \mathbf{k}, \text{ for each divisor } d \text{ of } n. \tag{1.3}$$

These conditions do not depend on the choice of cyclic generator for $\langle\sigma\rangle$ but (as mentioned after Proposition 1.2), do admit extensions in which L^σ is a *proper* extension of $\mathbf{k}$.

In §4.1, using only (M) for $n = 4$, the condition that the map σ fixes the ground field elementwise, the conditions (1.3), and elementary algebra, we obtain a linear fractional map (C4) for σ, and a 2-parameter family of defining octics $T(m, A, x)$, $m, A \in \mathbf{k}$, with "generic" Galois group $G \cong {}_8T_{11}$ (see below). We let $L/\mathbf{k}$ denote the splitting field of $T(m, A, x)$.

$L/\mathbf{k}$ contains (§4.4) the elementary Abelian extension $E = \mathbf{k}(s, w, y)/\mathbf{k}$, where $s^2 = m^2 - 4$, $w^2 = (m + 2 + A)^2 - 4(m - 2)$, and $y^2 = A^2 - 4(m - 2)$. When $[E : \mathbf{k}] = 8$, $G \cong {}_8T_{11}$, and E contains 7 quadratic extensions of $\mathbf{k}$. In Theorem 4.14 we describe the subgroups of ${}_8T_{11}$ fixing each of these.

The description of the Galois group is greatly facilitated by the fact that the *related* octics $T(m, A, x)$ and $T(m, -m-2-A, x)$ have the same splitting field over $\mathbf{k}$ (Theorem 4.13). When $[L : \mathbf{k}] = 8$, at least one of these octics is a defining polynomial for the splitting field.

The cyclic quartics for which our map σ makes (M) a formal identity with $n = 4$, occur in *pairs*. They are the quartic factors of $T(m, A, x)$ in $\mathbf{k}(sw)[x]$, so typically define cyclic quartic extensions of $\mathbf{k}(sw)$, not of $\mathbf{k}$. But when $sw \in \mathbf{k}$, they are in $\mathbf{k}[x]$, and we call them *Murphy's twins*. They "generically" define distinct cyclic quartic extensions of $\mathbf{k}$, both containing $\mathbf{k}(s)$. The "simplest" quartic fields and Washington's cyclic quartic fields are "degenerate" cases (with $\mathbf{k} = \mathbb{Q}$) for which $s = 0$ and $w = 0$, respectively. In these cases the "twins" are identical. We construct other "Murphy's twins" extensions of $\mathbb{Q}$ in §6.3 using standard results on norms from real quadratic fields.

By "collapsing" other quadratic extensions of $\mathbf{k}$ in E, we construct families of polynomials defining normal octic extensions with $G \cong D_8(8)$, Q_8, and $C_4 \times C_2$, and quartics with $G \cong D_4$ and V_4.

The "generic" Galois group ${}_8T_{11}$ is an order-16 transitive subgroup of A_8; ${}_8T_{11} \cong$ GAP small group $\langle 16, 13\rangle$. It has one maximal subgroup $\cong Q_8$ (quaternion group), three $\cong D_4$, and three $\cong C_4 \times C_2$. It has presentation

$$\langle a, b, c\rangle : \ a^4 = b^2 = c^2 = 1, ab = ba, \ ac = ca, \ (bc)^2 = a^2.$$

It is also known as the "almost extraspecial group of order 16." Derek Holt ([14]) described almost extraspecial p-groups as *central products*. A central product is an "amalgamated product" (see [10]), in which the subgroups being identified are in the centers of the factors. In this particular case,

$${}_8T_{11} \cong C_4 \vee D_4 \cong C_4 \vee Q_8.$$

When $\mathbf{k} = \mathbb{Q}$ and $m, A \in \mathbb{Z}$, there are (§6.5) explicit sets of 3 independent units. If $T(m, A, x)$ defines one or more number fields whose units groups have rank 3, these can produce rather small regulators.

Our octics produce (Propositions 5.3 and 5.4) some unusual sets of units and associates. Specifically (Proposition 5.3(b)), if $m, A \in \mathcal{O}_{\mathbf{k}}$ for a number field $\mathbf{k}$, and $m-2 \in \mathcal{O}_{\mathbf{k}}^{\times}$, then each zero of $T(m, A, x)$ is part of an *exceptional sequence of three units*; that is, three units, the difference of any two of which is also a unit. In particular, $T(1, A, x)$ and $T(3, A, x)$, $A \in \mathbb{Z}$, are one-parameter families in $\mathbb{Q}[x]$ whose zeroes have this property. An infinite subfamily of $T(3, A, x)$ gives (Eqs. (6.3a) - (6.4b)) "Murphy's twins" cyclic quartic fields with exceptional sequences of three units. We also obtain (Eq. (6.5)) a unit index formula which may be of interest.

The terms "exceptional units," "exceptional sequences," and "cliques" (of units) arose as follows: In [30], Nagell called either of two units whose sum is 1, *exceptional units*. In [20], Lenstra used finite sequences of algebraic integers, the difference of any two of which is a unit, to construct Euclidean fields. He observed that by applying an appropriate affine transformation, the first two terms of the sequence become 0 and 1, and any further terms become exceptional units. Thus, Lenstra's sets generalize the concept of exceptional units. In [24], A. Leutbecher and J. Martinet called them *exceptional sequences*. In [23], Leutbecher entitled Section 1 "The graph of exceptional units." This applied an idea of Győry, that defining two elements of a commutative ring R as being "connected" when their difference is a unit, induces a graph structure on R (see, e.g. [25], reference [G3]). Leutbecher and G. Niklasch used the graph-theoretic term "cliques" in this context in [25].

2 Basic formal properties

Proposition 1.1 gave some very simple formal properties implied by (M). We give several more. The first of these applies to non-Abelian extensions.

Proposition 2.1. *Let $L/\mathbf{k}$ be a finite Galois extension with Galois group G, and assume $\sigma \in G$, r,and n satisfy* (M). *If $\gamma \in C_G(\langle\sigma\rangle)$, then* (M) *holds for $\gamma(r)$.*

Proof. Since $\gamma\sigma = \sigma\gamma$, we have $\gamma(\sigma^i(r)) = \sigma^i(\gamma(r))$ for all i. □

Next, (M) does not depend on the choice of generator for $\langle\sigma\rangle$.

Proposition 2.2. *Assume $\mathbf{k}$, L, r, σ, and $n > 2$ satisfy* (M). *If $1 \le k < n$, $(k, n) = 1$, $\eta = \sigma^k$, and $y_k = r\sigma(r)\cdots\sigma^{k-1}(r)$, then*

$$1 + y_k + y_k\eta(y_k) + \ldots + y_k\eta(y_k)\cdots\eta^{n-2}(y_k) = 0.$$

Proof. The proof is left as an exercise. □

The y_k are zeroes of the degree-n polynomials

$$f_k(x) = \prod_{i=1}^{n}(x - \sigma^i(y_k)). \tag{2.1}$$

We thus obtain a set of $\varphi(n)$ polynomials. Mutually inverse generators of $\langle\sigma\rangle$ give polynomials with mutually reciprocal zeroes.

Examples. Applying Eq. (2.1) to $f_1(x) = P(x)$ and σ as in Proposition 1.2(d), we obtain the alternate defining polynomial

$$f_2(x) = x^5 + (t^3 + 3t^2 + 5t + 5)x^4 - (t^4 + 3t^3 + 7t^2 + 5t + 5)x^3$$
$$- (t^4 + 5t^3 + 17t^2 + 25t + 25)x^2 - (2t^2 + 5t + 10)x - 1.$$

Eq. (2.1) gives $f_2(x)$, $f_3(x) = -x^5 f_2(1/x)$, and $f_4(x) = -x^5 f_1(1/x)$ in addition to $f_1(x)$.

The zeroes of the octic polynomials studied by Y.Y. Shen in [34],

$$P(a, x) = x^8 - ax^7 - 28x^6 + 7ax^5 + 70x^4 - 7ax^3 - 28x^2 + ax + 1,\ a \in \mathbb{Z},$$

are permuted cyclically by the compositional powers of the algebraic map

$$\sigma : x \mapsto (-\xi x - 1)/(x - \xi),\ \text{taking } \xi \pmod{\xi^2 - 2\xi - 1}.$$

It may be verified directly that (M) with $n = 8$ is a formal identity for the compositional powers of this algebraic map. Shen showed that $P(a, x)$ defines cyclic octic fields when $a^2 + 64 \in 2\mathbb{Z}^2$, and investigated the properties of these

fields. For such a, $P(a,x)$ is irreducible in $\mathbb{Q}[x]$ but *not* in $\mathbb{Q}(\xi)[x]$. In this case, the *automorphism* defined by σ maps ξ to $-1/\xi$, so its compositional powers occur in a different order than those of the algebraic map. If we assume that $\mathbf{k} = \mathbb{Q}(\xi)$, $a \in \mathcal{O}_{\mathbf{k}}$, and $P(a,x)$ is irreducible in $\mathbf{k}[x]$, then it defines a cyclic octic extension of $\mathbf{k}$ with Galois group $\langle\sigma\rangle$, and its zeroes are *units* which satisfy (M) with $n = 8$. The coefficients of $f_3(x)$ and $f_5(x)$ as in Eq. (2.1) are not formally in $\mathbb{Z}[a]$; for instance, the coefficient of x^5 in $f_3(x)$ is $(12a^2 + 768)\xi + a^3 - 12a^2 + 57a - 768$.

From Proposition 1.1(b) and HT90, we see that if $L/\mathbf{k}$ is cyclic of degree n with Galois group $\langle\sigma\rangle$, any r for which (M) holds is of the form $\alpha/\sigma(\alpha)$, $\alpha \in L$. If $\alpha = 1/z$, we have $r = \sigma(z)/z$. Substituting this expression into (M), the products in each term telescope, giving

$$(z + \sigma(z) + \ldots + \sigma^{n-1}(z))/z = 0.$$

The numerator is $\mathbf{Tr}_{L/\mathbf{k}}(z)$. Thus, in a cyclic extension, an element which satisfies (M) is of the form $\sigma(z)/z$ where z is *in the kernel of the trace*. For cyclic extensions of degree $n > 2$, primitive elements of this form always exist.

Proposition 2.3. *Let $L/\mathbf{k}$ be a cyclic extension of degree n with $G = \langle\sigma\rangle$. If $n > 2$, there is $r \in L$ with $L = \mathbf{k}(r)$ for which* (M) *holds.*

Proof. The kernel of the trace from L to $\mathbf{k}$ is a $\mathbf{k}$-vector subspace V of L of dimension $n - 1$. The distinct elements $\sigma(z)/z$, $z \in V - \{0\}$, correspond in an obvious way to the 1-dimensional $\mathbf{k}$-subspaces of V.

If $\mathbf{k}$ is a finite field with q elements, the number of such subspaces is

$$(q^{n-1} - 1)/(q - 1) = 1 + q + \ldots + q^{n-2}.$$

The formula (see, for example, [3], Exercise 13 for Chapter 3) for the number of primitive elements in a degree-n extension of a finite field shows that the number of nonzero *non*primitive elements in L is less than

$$1 + q + \ldots + q^{n/\ell},$$

where ℓ is the least prime factor of n. If $n > 2$, the number of distinct elements $\sigma(z)/z$, $z \in V - \{0\}$, is thus too large for them all to be non-primitive.

Now suppose $\mathbf{k}$ is infinite and $n > 2$. Let $d \mid n$, $d > 1$, and suppose $z \in V$ with $\sigma(z)/z = w \in F$, where F is the intermediate field with L/F of degree d. Then $\mathcal{N}_{F/\mathbf{k}}(w) = \sigma^{n/d}(z)/z = W$; $\mathcal{N}_{L/\mathbf{k}}(W) = W^n = 1$; there are at most n such W. The distinct values of $\sigma^{n/d}(z)/z$ correspond to one-dimensional F-vector subspaces of L; these are n/d-dimensional $\mathbf{k}$-vector spaces. Now $n/d < n - 1$ for $d > 1$ and $n > 2$. Thus, the values $r = \sigma(z)/z$, $z \in V$, for which $\mathbf{k}(r) \neq L$, correspond to the 1-dimensional subspaces of a finite union of *proper* $\mathbf{k}$-subspaces of V. It is well-known that when $\mathbf{k}$ is infinite, no $\mathbf{k}$-vector space is a finite union of proper subspaces, and the result follows. □

Remarks. If $r = \sigma(z)/z$ satisfies (M), then in Proposition 2.2, $y_k = \sigma^k(z)/z$.

When the ground field $\mathbf{k}$ contains an mth root of unity $\zeta \neq 1$, $F = \mathbf{k}(r)$ is a cyclic extension of degree d, and $\mathcal{N}_{F/\mathbf{k}}(r) = \zeta$, then embedding F in a cyclic extension of degree md over $\mathbf{k}$ forces r to satisfy (M) with $n = md$, as occurs in Eq. (1.2) with $m = 2$ and $\zeta = -1$.

If $\mathbf{k}$ is a number field and r is a "Murphy's unit," we may take z so its σ-conjugates are *associate algebraic integers in the kernel of the trace.* Among cyclic cubic extensions of $\mathbb{Q}$, only Shanks's simplest cubic fields possess such z. If $P(r) = 0$ in Prop. 1.2(a), $r = \sigma(z)/z$ for $z = 2r^2 - (2t+1)r - t - 4$. Noting that $(t^2+3t+9)^2 = \mathrm{disc}(x^3 - tx^2 - (t+3)x - 1)$, we have

$$z^3 - (t^2+3t+9)z + t^2 + 3t + 9 = 0.$$

3 Shen's polynomials

In [34], Y.Y. Shen constructed polynomials of 2-power degree, generalizing the 1-parameter family of defining polynomials for the octic fields he investigated. His construction used linear fractional transformations of the form

$$\lambda : x \mapsto \frac{\xi x - 1}{x + \xi} \text{ defined by the matrix } \begin{pmatrix} \xi & -1 \\ 1 & \xi \end{pmatrix}, \ \xi = \cot(\pi/2^k). \tag{3.1}$$

The results in this section are thus very similar to those in [31], but our results are less general. We restrict our parameter to the complex field $\mathbb{C}$. This allows us to "cheat" by invoking a periodic transcendental meromorphic function (the cotangent), and to exploit the fact that the linear transformation in Eq. (3.1) corresponds to adding a division point to the argument of this function. Our approach also differs in that we begin with well-known polynomials, rather than a linear transformation. We later restrict our parameter further to algebraic integers in $K = \mathbb{Q}(\cot(\pi/n))$. This produces polynomials of degree n in $K[x]$ whose irreducible factors all have the same degree $d \mid n$. If d is a proper divisor of n, the "rescaled" polynomial of degree n/d splits into linear factors in $K[x]$ (Prop. 3.4).

Here, we generalize Shen's construction to polynomials of degree n for all $n > 1$. We take

$$Q_n(x) = \Re((x+i)^n) \text{ and } V_n(x) = \Im((x+i)^n). \tag{3.2}$$

Clearly

$$Q_n(x) = \sum_{0 \le 2k \le n} (-1)^k \binom{n}{2k} x^{n-2k} \ , \ V_n(x) = \sum_{0 \le 2k < n} (-1)^k \binom{n}{2k+1} x^{n-2k-1}$$

so $Q_n(x)$ is monic of degree n, and $V_n(x)$ is of degree $n-1$, with leading coefficient n. There is also the very useful formula

$$Q_n(\cot(\theta))/V_n(\cot(\theta)) = \cot(n\theta) \text{ for all } n \in \mathbb{Z}^+. \tag{3.3}$$

The gcd of the coefficients of $V_n(x)$ is $2^{v_2(n)}$, where $n/2^{v_2(n)}$ is an odd integer. The proof is left as an exercise.

Definition 3.1. With $Q_n(x)$ and $V_n(x)$ as in Eq. (3.2), and $n \in \mathbb{Z}^+$, set

$$P_n(a,x) = Q_n(x) - \frac{a}{2^{v_2(n)}} V_n(x). \tag{3.4}$$

Then $P_n(a,x)$ is monic of degree n. For $0 \le k \le n$, the coefficient of x^{n-k} is in $\mathbb{Z}$ if k is even, and in $\mathbb{Z} \cdot a$ if k is odd.

Clearly $V_{2n}(x) = 2Q_n(x)V_n(x)$, so $V_{2^t}(x) = 2^t Q_1(x)Q_2(x)\cdots Q_{2^{t-1}}(x)$ for $t \in \mathbb{Z}^+$ by induction. Thus, when $n = 2^t$, $P_n(a,x)$ coincides with the degree-2^t polynomial constructed in [34].

The following properties are easily obtained:

Proposition 3.1. *Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{C}$.*

(a) If $a \neq \pm 2^{v_2(n)} i$, $P_n(a,x)$ has n distinct zeroes $x = \cot(\theta)$ for which $\cot(n\theta) = a/2^{v_2(n)}$. The zeroes are real if a is real. If $\cot(\theta_1)$ is one of them, all are given by $\cot(\theta_1 + k\pi/n)$, $0 \le k \le n-1$.

(b) The discriminant of $P_n(a,x)$ is $n(2^{n-2-2v_2(n)}n)^{n-1}(a^2+4^{v_2(n)})^{n-1}$.

(c) If $P_n(a,\cot(\theta)) = 0$, then $Q_k(\cot(\theta)) - \cot(k\theta)V_k(\cot(\theta)) = 0$ for $k \in \mathbb{Z}^+$.

(d) If $P_n(a,\cot(\theta)) = 0$ and $D \mid n$, $P_{n/D}(a/2^{v_2(D)}, x) = 0$ for

$$x = \cot(D\theta + kD\pi/n),\ 0 \le k \le n/D - 1.$$

Proof. For (a), use Eq. (3.3). Except for $\pm i$, $\cot(n\theta)$ assumes all complex values, including all real values for $\theta \in (0, \pi/n)$, and is periodic with period π/n.

For (b), $\operatorname{disc}(P_n(a,x)) = f(a) \in \mathbb{Z}[a]$. By construction, $P_n(a,x) = (x \mp i)^n$ when $a = \pm 2^{v_2(n)} i$. By (a), $f(a)$ has no linear factors in $\mathbb{C}[a]$ other than $a \pm 2^{v_2(n)} i$, so is a constant multiple of $(a^2+4^{v_2(n)})^{n-1}$. Taking $a = 0$, we see the constant is the discriminant of $Q_n(x)$ divided by $4^{(n-1)v_2(n)}$. The identity $Q_n'(x) = nQ_{n-1}(x)$ aids in evaluating the discriminant of $Q_n(x)$.

Finally, (c) and (d) follow easily from Eq. (3.3). □

We recover the following well-known identities by comparing the coefficient of x^{n-1} and the constant term of $P_n(a,x)$ with the formula $\cot(n\theta) = a/2^{v_2(n)}$ in Proposition 3.1(a). They are valid if $n\theta$ is not an integer multiple of π.

$$\text{If } n \in \mathbb{Z}^+, \text{ then } \sum_{k=0}^{n-1} \cot(\theta + k\pi/n) = n\cot(n\theta). \tag{3.5a}$$

$$\text{If } n \in \mathbb{Z}^+ \text{ is odd, then } \prod_{k=0}^{n-1} \cot(\theta + k\pi/n) = (-1)^{(n-1)/2}\cot(n\theta). \tag{3.5b}$$

Let $n > 1$, $x = \cot(\theta)$ and $\xi = \cot(\pi/n)$. Then the map

$$T:\ \cot(\theta) \mapsto \cot(\theta + \pi/n) \text{ becomes } \lambda:\ x \mapsto \frac{\xi x - 1}{x + \xi}. \tag{3.6}$$

Since T has compositional order n, so does λ. Using Eq. (3.3) and Proposition 3.1(a), we have

$$\sum_{k=0}^{n-1} \lambda^{(k)}(x) = nQ_n(x)/V_n(x), \tag{3.7}$$

where $\lambda^{(k)}$ is the k^{th} compositional power of λ. Also,

Corollary 3.2. *Let $n \in \mathbb{Z}$, $n > 1$, and $a \in \mathbb{C}$. If $\xi = \cot(\pi/n)$, the zeroes of $P_n(a,x)$ are permuted cyclically by the linear fractional map λ in* Eq. (3.6).

Proof. If $a \neq \pm 2^{v_2(n)}i$, this just restates Proposition 3.1(a). If $a = \pm 2^{v_2(n)}i$, the n-fold zero $\pm i$ of $P_n(a,x) = (x \mp i)^n$ is fixed by λ. □

Now, let $n \in \mathbb{Z}$, $n > 1$ and $K = \mathbb{Q}(\cot(\pi/n))$. It is easily shown that $K = \mathbb{Q}(2\cos(2\pi/N))$ where $N = \operatorname{lcm}(n,4)$. We have the following result:

Theorem 3.3. *Let $n \in \mathbb{Z}$, $n > 1$, $K = \mathbb{Q}(\cot(\pi/n))$, and $\alpha \in \mathcal{O}_K$.*

(a) The zeroes of $P_n(\alpha,x)$ are algebraic integers (units, if n is even).

(b) $P_n(\alpha,x)$ determines a totally real extension L of K.

(c) There is a divisor d of n such that, if $f(x)$ is any irreducible factor of $P_n(\alpha,x)$ in $K[x]$, $f(x)$ has degree d.

(d) If $f(x)$ and $d \mid n$ are as in (c)*, then $G(L/K) = \langle\sigma\rangle$, where the restriction of σ to the zeroes of $f(x)$ is given by $\lambda^{(n/d)}$, λ as in* Eq. (3.6).

Proof. For (a), $P_n(\alpha, x)$ is a monic polynomial in $\mathcal{O}_K[x]$ by Definition 3.1. If n is even, the constant term is $(-1)^{n/2}$.

For (b), the zeroes of $P_n(\alpha, x)$ are all real by part (a) of Proposition 3.1. Since K is totally real, the zeroes of $P_n(\alpha', x)$ are also all real, for each conjugate α' of α.

For (c), let $P_n(\alpha, r) = 0$. By Corollary 3.2, the rest of the zeroes are given by $\lambda^{(k)}(r)$, $1 \le k \le n-1$, λ as in Eq. (3.6). Now λ is defined by a matrix in $\mathbf{PGL}_2(K)$, so all zeroes of $P_n(\alpha, x)$ determine the *same* extension of K. Thus, its irreducible factors in $K[x]$ all have the same degree.

For (d), let $f(x)$ be a monic irreducible factor of $P_n(\alpha, x)$ in $K[x]$, and $d \mid n$ its degree. Let $f_k(x) = (x + \cot(k\pi/n))^d f(\lambda^{(k)}(x))$ "made monic" (divided by its lead coefficient).

If $f_{j+k}(x) = f_j(x)$, clearly $\lambda^{(k)}$ has compositional order d at most. So $f(x) = f_0(x)$, $f_1(x), \ldots, f_{n/d-1}(x)$ are all distinct, and $f_{n/d}(x) = f(x)$. The rest is now self-evident. □

The integer d in Theorem 3.3(c) has some additional properties:

Proposition 3.4. *Let n, α, and $P_n(\alpha, x)$ be as in* Theorem 3.3*, with d as in* Theorem 3.3(c)*.*

(a) If $P_n(\alpha, \cot(\theta)) = 0$, then $\cot(d\theta) \in K$.

(b) $P_{n/d}(\alpha/2^{v_2(d)}, x)$ splits into linear factors in $K[x]$.

(c) d is the least positive integer for which (a) *and* (b) *hold.*

Proof. Let $f(x)$ be the minimum polynomial for $\cot(\theta)$ in $K[x]$. By Theorem 3.3(d), the zeroes of $f(x)$ are $\cot(\theta + k\pi/d)$, $0 \le k < d$. By the identity in Eq. (3.5a), the sum of these zeroes is $d\cot(d\theta)$, proving (a). Since $f(x)$ is irreducible in $K[x]$, the formula in Prop. 3.1(c) shows that d is the least positive integer with this property, and exhibits $f(x)$. By the formula in Prop. 3.1(d), the zeroes of $P_{n/d}(\alpha/2^{v_2(d)}, x)$ are $\cot(d\theta + k\pi d/n)$, $0 \le k < n/d$. These are all in K because the cotangents of both summands of the argument are in K.

□

When $4 \mid n$, $\langle\lambda\rangle$ has generators which make (M) a formal identity.

Proposition 3.5. *Let λ be as in* Eq. (3.6)*, $m \in \mathbb{Z}^+$, and $n = 4m$. If*

$$S(x) = 1 + x + x\lambda^{-1}(x) + x\lambda^{-1}(x)\lambda^{-2}(x) + \ldots + x\lambda^{-1}(x)\cdots\lambda^{-(4m-2)}(x),$$

then $S(x) \equiv 0$; that is, if $\sigma^k(r) = \lambda^{-k}(r)$, (M) *becomes a formal identity.*

Proof. $S(x)$ is a rational function, which clearly has a partial fraction decomposition of the form

$$S(x) = A + Bx + \sum_{k=1}^{4m-2} \frac{c_k}{(x - \cot(k\pi/4m))},$$

where $A, B, c_k \in \mathbb{Q}(\cot(\pi/4m))$. Using $\lambda^{2m}(x) = -1/x$, we find

$$B = \sum_{k=0}^{2m-1} \prod_{j=1}^{k} (-\cot(j\pi/4m)).$$

Since $\cot(\pi/2 - \theta) = 1/\cot(\theta)$, the terms of index k and $2m-1-k$ are equal and opposite. Thus $B = 0$, so $S(x)$ is bounded as $x \to \infty$.

Now $\lambda^{-(4m-1)}(x) = \lambda(x)$. Using $\lambda^{j+2m}(x) = -1/\lambda^j(x)$, we find that $\lambda(x)S(x) = S(\lambda(x))$. Letting $x \to \infty$, we see $S(\lambda(x))$ remains bounded as $\lambda(x) \to \cot(\pi/4m)$, so $c_1 = 0$. Then, $\lambda^{(k)}(x)S(\lambda^{k-1}(x)) = S(\lambda^{(k)}(x))$, giving $c_k = 0$ for $1 \le k \le 4m-2$. Thus, $S(x) = A$, a constant. Substituting $x = i$, which is fixed by λ, we find $S(i) = 0$. □

Next, we evaluate the sums in Eq. (1.3) with $\sigma = \lambda$. If d (and hence n) is even, the factors in each term occur in negative-reciprocal pairs, so the sum is $(-1)^{d/2}(n/d)$. If d is odd, we use Eq. (3.5b) to evaluate each term, then Eq. (3.5a) to add them; the result is $(-1)^{(d-1)/2}na/(d \cdot 2^{v_2(n)})$.

Let $n = 4m$, $a \in \mathbb{Z}$. Since $\cot(\pi/n) \in \mathbb{Q}(r, \lambda(r))$ if $P_n(a, r) = 0$, the splitting field of $P_n(a, x)$ over $\mathbb{Q}$ has degree divisible by $\varphi(2m)$. If $\mathbb{Q}(r)/\mathbb{Q}$ is normal of degree n, then $\varphi(2m) \mid 4m$. The degree d of the irreducible factors of $P_n(a, x)$ in $K[x]$ divides $4m/\varphi(2m)$. If $n = 2^t$, $t \ge 4$, then $d \mid 4$, and it can be shown using Prop. 3.4(b), that $\mathbb{Q}(r)/\mathbb{Q}$ is a normal extension of degree $n = 2^t$ only if $a = \pm n$ and $\mathbb{Q}(r) = \mathbb{Q}(2\cos(\pi/4n))$, or if $n = 16$ and $a = \pm 16 \cdot 239$.

4 The condition (M) with $n = 4$

Assuming that (M) and the conditions in Eq. (1.3) hold, and that the map σ fixes the ground field $\mathbf{k}$ elementwise, we only need elementary algebra, treating σ as a field isomorphism as needed, to produce a complete description of σ as an algebraic map, in terms of two parameters m and A in $\mathbf{k}$.

4.1 The formal construction

When $n = 4$, (M) becomes

$$1 + r + r\sigma(r) + r\sigma(r)\sigma^2(r) = 0. \tag{M4}$$

The condition of Eq. (1.3) with $d = 2$ is

$$r\sigma^2(r) + \sigma(r)\sigma^3(r) = m \in \mathbf{k}.$$

By Proposition 1.1, $r\sigma(r)\sigma^2(r)\sigma^3(r) = 1$, so taking $r\sigma^2(r) = u$, we have

$$\sigma(u) = u^{-1}, \text{ where} \tag{4.1a}$$

$$u^2 - mu + 1 = 0,\ m \in \mathbf{k}. \tag{4.1b}$$

Substituting u for $r\sigma^2(r)$ in (M4), solving for $\sigma(r)$, repeatedly applying σ, and keeping in mind Eq. (4.1a), we obtain the expressions

$$\sigma(r) = \frac{-r-1}{r+u},\ \sigma^2(r) = \frac{u}{r},\ \sigma^3(r) = \frac{-u^{-1}r-1}{r+1},\ \sigma^4(r) = r. \tag{C4}$$

The product of the four expressions in (C4) is 1 as required by Proposition 1.1. The expression for $\sigma^2(r)$ is of the same form as that for a "relative" unit in a cyclic quartic extension, as given in [41], §2. These expressions are also strikingly similar to those in [23], §1.1.

Because of Eq. (4.1a), for the map σ to fix $\mathbf{k}$ elementwise it is necessary that either

$$m = \pm 2 \text{ or } m^2 - 4 \notin \mathbf{k}^2. \tag{4.2}$$

Substituting (C4) into the condition in Eq. (1.3) with $d = 1$,

$$r + \frac{-r-1}{r+u} + \frac{u}{r} + \frac{-u^{-1}r-1}{r+1} = A,\ A \in \mathbf{k}. \tag{Tr4}$$

Clearing fractions and collecting terms, we find that r is a zero of

$$p(x) = x^4 + (u - u^{-1} - A)x^3 + ((2-A)u - A - 4)x^2 + (u^2 - 1 - Au)x + u^2 \tag{Q4}$$

where $m, A \in \mathbf{k}$, and Eqs. (4.1b) and (4.2) hold. By Eq. (4.2), $p(x) \in \mathbf{k}[x]$ only if $m = \pm 2$. We treat those cases first.

4.2 The cases $m = \pm 2$

If $m = 2$ then $u = 1$, the formal expressions for $\sigma(r)$ and $\sigma^3(r)$ become -1, and we obtain

$$p(x) = (x+1)^2(x^2 - (A+2)x + 1).$$

In this case the transformation σ is *not* a field automorphism of order 4, but if $(A+2)^2 - 4 \notin \mathbf{k}^2$, the quadratic factor is irreducible in $\mathbf{k}[x]$, and the expression $1/r$ for $\sigma^2(r)$ does define an automorphism of order 2. The change of parameter $A \leftarrow -4 - A$ changes the signs of the zeroes of the quadratic factor.

If $m = -2$ then $u = -1$, and the expressions in (C4) become

$$\sigma(r) = \frac{-r-1}{r-1},\ \sigma^2(r) = -\frac{1}{r},\ \sigma^3(r) = \frac{r-1}{r+1},\ \text{ and } \sigma^4(r) = r. \tag{C4$'$}$$

Substituting $u = -1$ into Equation (Q4) gives

$$p(x) = x^4 - Ax^3 - 6x^2 + Ax + 1. \tag{Q4$'$}$$

Apart from parameter name, this is the $P(x)$ in Proposition 1.2(b) for the "simplest" quartic fields. If $\mathbf{k} = \mathbb{Q}$ and $A \in \mathbb{Z}$, $p(x)$ is irreducible in $\mathbb{Z}[x]$ unless $A \in \{-3, 0, 3\}$. In general, $p(x)$ is irreducible in $\mathbf{k}[x]$ when $A^2 + 16 \notin \mathbf{k}^2$. The Galois group acts on the zeroes as in (C4$'$). The polynomials $f_1(x) = p(x)$ and $f_3(x)$ in Proposition 2.2, are related by the change of parameter $A \leftarrow -A$.

4.3 Fundamental identities when $m^2 - 4 \notin \mathbf{k}^2$

When $m^2 - 4 \notin \mathbf{k}^2$, however, the $p(x)$ in (Q4) is *not* in $\mathbf{k}[x]$. Conjugating the coefficients in $\mathbf{k}(u)/\mathbf{k}$ gives a polynomial $\bar{p}(x) \neq p(x)$. Assuming σ is a field automorphism, and $p(r) = 0$, $\sigma(r)$ is a zero of $\bar{p}(x)$ rather than of $p(x)$. But *that* would imply an *algebraic* relation between $\bar{p}((-x-1)/(x+u))$ and $p(x)$. And there is indeed such a relation:

Theorem 4.1. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$, and u, $p(x)$ and $\bar{p}(x)$ be as above. Then*

$$(x+u)^4\, \bar{p}\left(\frac{-x-1}{x+u}\right) = (m-2)p(x).$$

Proof. Straightforward polynomial algebra. □

Although $p(x) \notin \mathbf{k}[x]$, clearly

$$T(m, A, x) = p(x)\bar{p}(x) \tag{4.3}$$

is a monic octic formally in $\mathbb{Z}[m, A][x]$ (thus in $\mathbf{k}[x]$ when $m, A \in \mathbf{k}$), with constant term 1. Theorem 4.1 gives two important properties of $T(m, A, x)$:

Corollary 4.2. *Let m, A, and $p(x)$ be as above.*

(a) $p(x)$ and $\bar{p}(x)$ have the same splitting field L over $\mathbf{k}(u)$, which is the splitting field of $T(m, A, x)$ over $\mathbf{k}$.

(b) $\operatorname{disc}(T(m, A, x)) \in \mathbf{k}^2$.

Proof. Adjoining to $\mathbf{k}(u)$ either the zero r of $p(x)$, or the zero $(-r-1)/(r+u)$ of $\bar{p}(x)$, define the *same* extension of $\mathbf{k}(u)$. The join of the extensions defined by all the zeroes thus gives the same splitting field for both quartics.

For (b), a standard formula (see, for instance, [3], Corollary 3.3.6) gives

$$\mathrm{disc}(T(m,A,x)) = \mathrm{disc}(p(x))\mathrm{disc}(\bar{p}(x))[\mathrm{Res}(p(x),\bar{p}(x))]^2.$$

The arguments of the resultant are interchanged by conjugation in $\mathbf{k}(u)/\mathbf{k}$, but also by 4 (evenly many) row interchanges of the Sylvester's matrix, which leaves its determinant unchanged. Therefore, the resultant is in $\mathbf{k}$.

If we differentiate the identity in Theorem 4.1, evaluate at the zeroes of $p(x)$, and multiply, we obtain $\mathrm{disc}(p(x)) = u^6\mathrm{disc}(\bar{p}(x))$. The discriminants are conjugate in $\mathbf{k}(u)/\mathbf{k}$ and u has norm 1, so $\mathrm{disc}(p(x)) = cu^3$ for some $c \in \mathbf{k}$. Thus, $\mathrm{disc}(p(x))\mathrm{disc}(\bar{p}(x)) = c^2 \in \mathbf{k}^2$, and the proof is complete. □

The situation is further simplified by the fact that $p(x)$ is a generalized reciprocal polynomial:

Lemma 4.3. *If $m, A \in \mathbf{k}$, $u^2 - mu + 1 = 0$, and $p(x)$ is as in* (Q4)*, then*

$$\frac{p(x)}{x^2} = \frac{p\,(u/x)}{(u/x)^2}.$$

Proof. Straightforward polynomial algebra. □

We use Lemma 4.3 to split $p(x)$ into quadratic factors.

Lemma 4.4. *With $p(x)$ as in* Eq. (Q4) *and $Y = x + u/x$,*

(a) $p(x) = x^2F(Y)$, where $F(Y) = Y^2 + (-A + u - u^{-1})Y - A - 4 - Au$.

(b) $\mathrm{disc}(F(Y)) = (m + 2 + A)^2 - 4(m - 2)$.

(c) If $F(Y) = (Y - \alpha)(Y - \beta)$, then

$$p(x) = q_1(x)q_2(x) = (x^2 - \alpha x + u)(x^2 - \beta x + u).$$

(d) Let $Q_1 = q_1(-1) = 1 + \alpha + u$, $Q_2 = q_2(-1) = 1 + \beta + u$. Then

(i) $\mathrm{disc}(x^2 - \alpha x + u) = \alpha^2 - 4u = Q_1(Q_1 + Q_2u - 2(u + 1))$.

(ii) $\mathrm{disc}(x^2 - \beta x + u) = \beta^2 - 4u = Q_2(Q_2 + Q_1u - 2(u + 1))$.

Proof. Straightforward polynomial algebra. □

We then have

Proposition 4.5. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$, and $L/\mathbf{k}$ the splitting field of $T(m, A, x)$. Then $[L:\mathbf{k}]$ divides* 16.

Proof. Since $p(x)$ splits into quadratic factors in a quadratic extension (at most) of its coefficient field $\mathbf{k}(u)$, its splitting field over $\mathbf{k}(u)$ has degree dividing 8, and $\mathbf{k}(u)$ has degree 2 over $\mathbf{k}$. Corollary 4.2(a) then gives the result. □

4.4 The quadratic and quartic factors of $T(m, A, x)$

Note that $\mathrm{disc}(F(Y)) \in \mathbf{k}$ in Lemma 4.4(b), even though $F(Y) \notin \mathbf{k}[Y]$. The quadratic factors $q_1(x)$ and $q_2(x)$ of $p(x)$ in Lemma 4.4(c) (and, obviously, the corresponding factors of $\bar{p}(x)$) are in $\mathbf{k}(s, w)[x]$, where

$$s^2 = (m^2 - 4) \text{ and } w^2 = ((m + 2 + A)^2 - 4(m - 2)) = \mathrm{disc}(F(Y)). \quad (4.4)$$

Solving $F(Y) = 0$ by quadratic formula, we find the quadratic factors of $T(m, A, x)$ in $\mathbf{k}(s, w)[x]$ are

$$q_1(x) = x^2 + (-A + s - w)x/2 + (m + s)/2 \quad (4.5a)$$
$$q_2(x) = x^2 + (-A + s + w)x/2 + (m + s)/2, \quad (4.5b)$$
$$q_3(x) = x^2 + (-A - s + w)x/2 + (m - s)/2 \text{ , and} \quad (4.5c)$$
$$q_4(x) = x^2 + (-A - s - w)x/2 + (m - s)/2. \quad (4.5d)$$

These choices give $q_1(x)q_2(x) = p(x)$ and $q_3(x)q_4(x) = \bar{p}(x)$. By regrouping the $q_i(x)$ in pairs, we see that $T(m, A, x)$ splits into quartic factors in $\mathbf{k}(s)[x]$, $\mathbf{k}(sw)[x]$, and $\mathbf{k}(w)[x]$, namely

$$P_s(x) = p(x) = q_1(x)q_2(x) \text{ and } \bar{P}_s(x) = \bar{p}(x) = q_3(x)q_4(x), \quad (4.6a)$$
$$P_{sw}(x) = q_1(x)q_3(x) \text{ and } \bar{P}_{sw}(x) = q_2(x)q_4(x), \text{ and} \quad (4.6b)$$
$$P_w(x) = q_1(x)q_4(x) \text{ and } \bar{P}_w(x) = q_2(x)q_3(x). \quad (4.6c)$$

We have the following refinement of Theorem 4.1:

Lemma 4.6. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$, and notation as above. Then*

a) $(x + u)^2 \, q_3\left(\dfrac{-x - 1}{x + u}\right) = q_3(-1)q_1(x)$;

b) $\mathrm{disc}(q_1(x))\mathrm{disc}(q_3(x)) = ((u - 1)\mathrm{disc}(q_3(x))/q_3(-1))^2$;

c) $(u - 1)\mathrm{disc}(q_3(x))/q_3(-1) = ((m + A - 2)s + (2 - m)w)/2$.

Proof. For (a), there clearly must be an algebraic relation between $q_1(x)$ and either $q_3((-x-1)/(x+u))$ or $q_4((-x-1)/(x+u))$. By Eqs. (4.5a) and (4.5c), the coefficient of x^3 in $q_1(x)q_3(x)$ is $-A$ in agreement with (Tr4). Routine though tedious algebra completes the verification.

For (b), differentiate (a), evaluate at the zeroes, and multiply.

Finally, (c) may be verified algebraically. □

Remarks. The substitution $w \leftarrow -w$ replaces $(q_1(x), q_3(x))$ with $(q_2(x), q_4(x))$ in (a) – (c). Multiplying (a) by its counterpart gives Theorem 4.1.

To formulate s (and thus u and σ) in $\mathbf{k}[x] \pmod{T(m,A,x)}$, we write

$$P_s(x) = p(x) = \mathcal{A}(x)s + \mathcal{B}(x) \text{ where } \mathcal{A}(x), \mathcal{B}(x) \in \mathbf{k}[x], \text{ and take} \tag{4.7a}$$
$$s \equiv -\mathcal{B}(x)/\mathcal{A}(x) \pmod{T(m,A,x)}, \text{ if } \mathrm{Res}(\mathcal{A}(x), T(m,A,x)) \neq 0. \tag{4.7b}$$

Similarly, writing

$$P_w(x) = \mathcal{C}(x)w + \mathcal{D}(x) \text{ where } \mathcal{C}(x), \mathcal{D}(x) \in \mathbf{k}[x], \text{ we can take} \tag{4.8a}$$
$$w \equiv -\mathcal{D}(x)/\mathcal{C}(x) \pmod{T(m,A,x)} \text{ if } \mathrm{Res}(\mathcal{C}(x), T(m,A,x)) \neq 0. \tag{4.8b}$$

We can express these resultants in terms of the "monster" resultant norm

$$\mu = \mathrm{Res}(q_1(x), q_3(x))\mathrm{Res}(q_2(x), q_4(x)). \tag{4.9}$$

Direct calculation (using plenty of computing power) gives the results

$$\mathrm{Res}(\mathcal{A}(x), T(m,A,x)) = (m-2)^2\mu^2/256, \text{ and} \tag{4.10a}$$
$$\mathrm{Res}(\mathcal{C}(x), T(m,A,x)) = \mu^2/256. \tag{4.10b}$$

Lemma 4.7. *Let $m, A \in \mathbf{k}$, and either $m = \pm 2$ or $m^2 - 4 \notin \mathbf{k}^2$, with $q_1(x), q_3(x)$ as in* Eqs. (4.5a)–(4.5d) *and μ as in* Eq. (4.9)*. Then,*

$$\mu \neq 0 \text{ unless}$$

$(m, A) = (2, -4)$*;* $(-2, 4i)$ *or* $(-2, -4i)$ *if* $-1 \in \mathbf{k}^2$*; or* $(2/3, -4/3)$ *if* $-2 \notin \mathbf{k}^2$*.*

Proof. If $\mathrm{Res}(q_1(x), q_3(x)) = 0$, then $q_1(x)$ and $q_3(x)$ have a common factor in $\mathbf{k}(s,w)[x]$, which is also a factor of every $\mathbf{k}(s,w)$-linear combination of $q_1(x)$ and $q_3(x)$. Using Lemma 4.6, we see that $q_u(x) = x^2 + (1+u)x + 1$ or $\bar{q}_u(x) = x^2 + (u^{-1}+1)x + 1$ has the same common factor, because any common zero of $q_1(x)$ and $q_3(x)$ is a fixed point of (at least) one of the linear fractional transformations $\sigma(x)$ or $\sigma^3(x)$ in Eq. (C4).

There can be no common factor of degree ≥ 1 unless $\{q_1(x), q_u(x), q_3(x)\}$ or $\{q_1(x), \bar{q}_u(x), q_3(x)\}$ is a linearly dependent set in the $\mathbf{k}(s,w)$ vector space V with basis $\{1, x, x^2\}$. Let $v = (q_1(x), q_u(x), q_3(x)) \in V^3$, and let M be the 3×3 matrix whose i,j entry is the coefficient of x^{3-j} in v_i. The entries of v are linearly dependent in V when the "test value" $\mathbf{tv} = \mathrm{Det}(M)$ is 0. Tedious algebra gives

$$\mathbf{tv} = (-2m - A)s/2 + (m-2)w/2 - (m^2-4)/2.$$

If $m = 2$, all three terms are 0. In this case, we have $w^2 = (A+4)^2$. Taking $w = A+4$ and $s = 0$ we obtain $q_1(x) = x^2 - (A+2)x + 1$ and $q_3(x) = (x+1)^2$, as in §4.2, and $\gcd(q_1(x), q_3(x)) = 1$ unless $(m, A) = (2, -4)$.

If $m = -2$, then $s = 0$, and we obtain $w = m + 2 = 0$. But $w^2 = A^2 + 16$ when $m = -2$, so $A = \pm 4i$. These give $q_1(x) = q_3(x) = (x \mp i)^2$.

If $m \neq \pm 2$, then $s \notin \mathbf{k}$. If $(-2m - A) \neq 0$, then $(-2m - A)s/2 \notin \mathbf{k}$. Then $\mathbf{tv} \notin \mathbf{k}$ unless $(2m - A)s/2 + (m - 2)w/2 = 0$. But then $\mathbf{tv} \neq 0$ since $m \neq \pm 2$.

So if $m \neq \pm 2$, $\mathbf{tv} \neq 0$ unless $A = -2m$. Again $w = m + 2$, but also $w^2 = (m + 2 + (-2m))^2 - 4(m - 2) = m^2 - 8m + 12$. The two conditions on w are only satisfied simultaneously when $m = 2/3$ and $A = -4/3$. The substitution $(s, w) \leftarrow (-s, -w)$ changes v to $v' = (q_3(x), \bar{q}_u(x), q_1(x))$ and gives a "test value" $\mathbf{tv}'$ which is 0 for exactly the same (m, A). The argument for $\mathrm{Res}(q_2(x), q_4(x))$ is the same. If $m = 2/3$, $m^2 - 4 \notin \mathbf{k}^2$ when $-2 \notin \mathbf{k}^2$. □

Remark. Direct calculation shows that

$$\mathbf{tv} \cdot \mathbf{tv}' = (2 - m)\mathrm{Res}(q_1(x), q_3(x)).$$

Lemma 4.8. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$, and s and w as in* Eq. (4.4)*. If $T(m, A, r) = 0$, then $\mathbf{k}(s, w) \subset \mathbf{k}(r)$.*

Proof. We may take $r \equiv x \pmod{T(m, A, x)}$. Since $m \neq \pm 2$, s and w are given by Eqs. (4.7b) and (4.8b) unless $(m, A) = (2/3, -4/3)$, by Lemma 4.7. This case may be verified directly. □

Proposition 4.9. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$. Then $P_w(x)$ and $\bar{P}_w(x)$ have the same splitting field over $\mathbf{k}(w)$.*

Proof. This follows from an argument similar to that in Corollary 4.2, using Lemma 4.8. □

Brute-force algebra gives the simple expressions

$$\mathrm{disc}(q_1(x))\mathrm{disc}(q_2(x)) = (A^2 - 4(m - 2)) \cdot (u - 1)^2, \tag{4.11a}$$

$$\mathrm{Res}(q_1(x), q_2(x)) = w^2 u, \tag{4.11b}$$

$$\mathrm{disc}(q_1(x))\mathrm{disc}(q_4(x)) = (A^2 - 4(m - 2)) \cdot Q_1^2, \text{ and} \tag{4.11c}$$

$$\mathrm{Res}(q_1(x), q_4(x)) = s^2 Q_1 = (m^2 - 4)Q_1, \tag{4.11d}$$

where $Q_1 = q_1(-1) = (m + 2 + A + w)/2$ is as in Lemma 4.4(d).

From Eqs. (4.11a) and (4.11c), we see that the splitting field of $T(m, A, x)$ contains $\mathbf{k}(y)$, where

$$y^2 = A^2 - 4(m - 2). \tag{4.12}$$

We have the following result:

Proposition 4.10. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$. The zeroes of $T(m, A, x)$ are simple unless $w^2 y^2 = 0$ or $(m, A) = (2/3, -4/3)$.*

Proof. Eqs. (4.11a) – (4.11d) show that if $m \neq \pm 2$, $w^2 \neq 0$, and $y^2 \neq 0$, then none of the $q_i(x)$ have repeated factors, and $\mathrm{Res}(q_i(x), q_j(x)) \neq 0$ unless $\{i, j\} = \{1, 3\}$ or $\{2, 4\}$. For these, apply Lemma 4.7. □

When $w^2 = 0$, $q_1(x) \equiv q_2(x)$ and $q_3(x) \equiv q_4(x)$, so $P_w(x) \equiv P_{sw}(x)$ and $T(m, A, x) = P_{sw}^2$ in $\mathbf{k}[x]$. We deal with this case in §4.7. We see from Lemma 4.6(a) and its counterpart for $q_2(x)$ and $q_4(x)$, that except for the four pairs (m, A) in Lemma 4.7, if $y^2 \neq 0$ the zeroes of $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ are simple, and the linear fractional transformation σ in Eq. (C4) (defined via Eq. (4.7b)) permutes the zeroes of each cyclically.

The expression in Lemma 4.6(c) for a square root of the discriminant norm leads to an irreducibility criterion for $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ in $\mathbf{k}(sw)[x]$.

Theorem 4.11. *Let $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$. Then*

(a) $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ are both irreducible in $\mathbf{k}(sw)[x]$ if and only if

$$[\mathbf{k}(s, w) : \mathbf{k}(sw)] = 2 \text{ and } A^2 - 4(m-2) \neq 0.$$

(b) If $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ are irreducible in $\mathbf{k}(sw)[x]$, they define cyclic quartic extensions of $\mathbf{k}(sw)$. In each case, the action of the Galois group on the zeroes is given by (C4)*, defined via* Eq. (4.7b)*.*

Proof. First, $P_{sw}(x) = q_1(x)q_3(x)$ in $\mathbf{k}(s, w)[x]$, so is reducible in $\mathbf{k}(sw)[x]$ if $\mathbf{k}(sw) = \mathbf{k}(s, w)$. So suppose $[\mathbf{k}(s, w) : \mathbf{k}(sw)] = 2$. Conjugation in $\mathbf{k}(s, w)/\mathbf{k}(sw)$ changes the sign of the square root of $\mathrm{disc}(q_1(x))\mathrm{disc}(q_3(x))$ in Lemma 4.6(c), so neither $\mathrm{disc}(q_1(x))$ nor $\mathrm{disc}(q_3(x))$ is a square in $\mathbf{k}(s, w)$ unless their product is 0. Similarly for $q_2(x)$, $q_4(x)$ and $\bar{P}_{sw}(x)$. Multiplying these square roots gives $(m-2)(A^2 - 4(m-2))$ as a square root of $\mathrm{disc}(q_1(x))\mathrm{disc}(q_2(x))\mathrm{disc}(q_3(x))\mathrm{disc}(q_4(x))$. Now $m \neq 2$ by hypothesis, so if $A^2 - 4(m-2) \neq 0$, both $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ are irreducible in $\mathbf{k}(sw)[x]$. But if $A^2 - 4(m-2) = 0$, at least one of $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ has a repeated factor, so is reducible in $\mathbf{k}(sw)[x]$.

Part (b) follows from the discussion after Eqs. (4.11a)–(4.11d). □

We then obtain an irreducibility criterion for $T(m, A, x)$:

Corollary 4.12. *Let $m, A \in \mathbf{k}$. Then $T(m, A, x)$ is irreducible in $\mathbf{k}[x]$ if and only if $[\mathbf{k}(s, w) : \mathbf{k}] = 4$.*

Proof. Clearly, $T(m, A, x)$ is irreducible in $\mathbf{k}[x]$ if and only if $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ are irreducible in $\mathbf{k}(sw)[x]$ (which requires $[\mathbf{k}(s, w) : \mathbf{k}(sw)] = 2$), and $[\mathbf{k}(sw) : \mathbf{k}] = 2$. We only need to show that, if $A^2 - 4(m-2) = 0$, then $[\mathbf{k}(s, w) : \mathbf{k}] < 4$. This is trivial if $m = 2$. Otherwise, $A \neq 0$, so we can write

$$w^2 = (m+2)(m+2+2A) = (2s/A)^2(A/2+2)^2 \in (\mathbf{k}(s))^2.$$

□

4.5 Pairs of related octics

Eqs. (4.4) and (4.11a)-(4.11d) show the splitting field of $T(m, A, x)$ contains $E = \mathbf{k}(s, w, y)$, where

$$s^2 = m^2 - 4,\ w^2 = (m + A + 2)^2 - 4(m - 2),\ \text{and}\ y^2 = A^2 - 4(m - 2).$$

Note that $A \leftarrow -m - 2 - A$ has compositional order 2, and interchanges w^2 and y^2. [This formula gives the changes of parameter in §4.2.] We call $T(m, A, x)$ and $T(m, -m - 2 - A, x)$ *related* octics. We have the following result:

Theorem 4.13. *Let $m, A \in \mathbf{k}$, and $s^2 = m^2 - 4 \notin \mathbf{k}^2$. Then $T(m, A, x)$ and $T(m, -m - 2 - A, x)$ have the same splitting field over $\mathbf{k}$.*

Proof. We consider the corresponding quadratic factors

$q_1(x) = x^2 + (-A + s - w)x/2 + (m + s)/2$ as in Eq. (4.5a), and
$\psi_1(x) = x^2 + (m + 2 + A + s - y)x/2 + (m + s)/2$ with y as in Eq. (4.12).

If $w^2y^2 \neq 0$, Eqs. (4.11a), (4.11c), and Lemma 4.6 show that the $q_i(x)$ all define the *same* extension of E. Similarly for the corresponding $\psi_i(x)$. Greatly facilitated by the substitution $A = -(m+2)/2 + \mathbf{v}$ and Phil Carmody's guidance with Pari-GP, we found an algebraic square root of $\mathrm{disc}(q_1(x))\mathrm{disc}(\psi_1(x))$ in E, namely

$$c_0 + c_1 s + c_2 w + c_3 y + c_4 sw + c_5 sy + c_6 wy + c_7 swy,\ \text{where}$$

$c_0 = (3m^2 - 20m + 12 + 4\mathbf{v}^2)/16$, $c_1 = (m - 6)/4$, $c_2 = (-3m + 2 + 2\mathbf{v})/8$,
$c_3 = (-3m + 2 - 2\mathbf{v})/8$, $c_4 = -1/4$, $c_5 = -1/4$, $c_6 = -1/4$, and $c_7 = 0$.

If $w^2 = 0$, at least one of $\mathrm{disc}(q_1(x))\mathrm{disc}(\psi_1(x))$ and $\mathrm{disc}(q_1(x))\mathrm{disc}(\psi_2(x))$ will be nonzero unless $y^2 = 0$ also. (Replacing $\psi_1(x)$ with $\psi_2(x)$ has the effect of replacing y with $-y$ in the algebraic square root.) But $w^2 = y^2 = 0$ only when $m = 6$ and $A = -4$, for which the two related octics are identical, $T(6, -4, x) = (x^2 - 2x - 1)^4$. □

4.6 The Galois group of $T(m, A, x)$

We can now prove the main results about the splitting field $L/\mathbf{k}$ of $T(m, A, x)$.

Theorem 4.14. *Let $m, A \in \mathbf{k}$, and $[E:\mathbf{k}] = 8$ where $E = \mathbf{k}(s, w, y)$. Then*

(a) $T(m, A, x)$ is irreducible in $\mathbf{k}[x]$ with Galois group $G \cong {}_8T_{11}$.

(b) The fixed field of the quaternion subgroup is $\mathbf{k}(swy)$.

(c) *The fixed fields of the subgroups* $\cong D_4$ *are* $\mathbf{k}(s)$, $\mathbf{k}(w)$, *and* $\mathbf{k}(y)$.

(d) *The fixed fields of the subgroups* $\cong C_4 \times C_2$ *are* $\mathbf{k}(sw)$, $\mathbf{k}(sy)$, *and* $\mathbf{k}(wy)$.

Proof. $T(m, A, x)$ is irreducible in $\mathbf{k}[x]$ by Corollary 4.12. If $L/\mathbf{k}$ is its splitting field, then $E \subset L$, $[L : \mathbf{k}] \mid 16$ by Proposition 4.5, and L contains a C_4 extension of $\mathbf{k}[sw]$ by Theorem 4.11, so $L \neq E$. Thus $|G| = 16$, and $G \subset A_8$ by Corollary 4.2(b). This narrows the possibilities for G to ${}_8T_9$, ${}_8T_{10}$, and ${}_8T_{11}$. Of these, only ${}_8T_{11}$ has a quaternion subgroup.

Let H be the subgroup of G fixing $\mathbf{k}(swy)$. Then $|H| = 8$. Since the $q_i(x)$ remain irreducible in $E[x]$, it follows that $P_s(x)$, $P_{sw}(x)$, and $P_w(x)$ remain irreducible in $\mathbf{k}(s, swy)[x]$, $\mathbf{k}(sw, swy)[x]$, and $\mathbf{k}(w, swy)[x]$, respectively. By Lemma 4.6 and Eqns. (4.11a) and (4.11c), their discriminants are not squares in the coefficient fields, and L is normal of degree 4 over each, so

$$G(L/\mathbf{k}(s, swy)) \cong G(L/\mathbf{k}(sw, swy)) \cong G(L/\mathbf{k}(w, swy)) \cong C_4.$$

Now the elements of order 4 in these groups can only map $q_1(x)$ to $q_2(x)$, $q_3(x)$, and $q_4(x)$, respectively. Thus, H has 6 elements of order 4, so $H \cong Q_8$, proving (a) and (b). By Corollary 4.2, $G(L/\mathbf{k}(s)) \cong D_4$. By Proposition 4.9, $G(L/\mathbf{k}(w)) \cong D_4$ also; and $G(L/\mathbf{k}(y)) \cong D_4$ (use the related octic), establishing (c). The other three maximal subgroups of ${}_8T_{11}$ are $\cong C_4 \times C_2$, so (d) follows by the Galois correspondence. □

Remarks. The degree of $E/\mathbf{k}$ can be determined by testing whether s^2, w^2, y^2, s^2w^2, s^2y^2, w^2y^2, and $s^2w^2y^2$ are squares in $\mathbf{k}$.

When $[E : \mathbf{k}] = 8$, the factors $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ of $T(m, A, x)$ define the fixed fields of a conjugacy class of order-2 subgroups of G. The corresponding factors of the related octic define the fixed fields of a *different* conjugacy class of order-2 subgroups.

Taking $\sqrt{a} = sw$, $\sqrt{b} = sy$, $\sqrt{c} = s$, and $d = \mathrm{disc}(q_1(x))$ in [27], Appendix, we have $\mathrm{disc}(q_1(x))\mathrm{disc}(q_2(x)) = \mathrm{k}_a$, $\mathrm{disc}(q_1(x))\mathrm{disc}(q_3(x)) = \mathrm{k}_c$, and $\mathrm{disc}(q_1(x))\mathrm{disc}(q_4(x)) = \mathrm{k}_{ac}$. Using Eqs. (4.11a), (4.11c), and Lemma 4.6, the obstruction $(a, b)(c, c)$ to Galois group $\mathbf{DC} \cong {}_8T_{11}$ then evaluates to 1.

Corollary 4.15. *Let* $m, A \in \mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$, $[E : \mathbf{k}] = 4$ *where* $E = \mathbf{k}(s, w, y)$, *and* $L/\mathbf{k}$ *the splitting field of* $T(m, A, x)$. *Then* $[L : \mathbf{k}] = 8$, *and*

$$G(L/\mathbf{k}) \cong \begin{cases} Q_8, \text{ if } swy \in \mathbf{k}, \\ D_4 \cong D_8(8), \text{ if } w \in \mathbf{k} \text{ or } y \in \mathbf{k}, \text{ and} \\ C_4 \times C_2, \text{ if } sw \in \mathbf{k}, \ sy \in \mathbf{k}, \text{ or } wy \in \mathbf{k}. \end{cases}$$

Proof. At least one of the related octics is irreducible in $\mathbf{k}[x]$ by Corollary 4.12, and the rest is clear from Theorem 4.14. □

We formulate the condition $w \in \mathbf{k}$ (disregarding $[E:\mathbf{k}]$) by taking

$$m \in \mathbf{k},\ d \in \mathbf{k}^\times,\ A = -m-2-d-(m-2)/d, \text{ and } w = (m-2)/d-d. \quad (4.13)$$

Substituting into Eq. (4.6c), we obtain

$$P_w(x) = x^4+(m+2d+2)x^3+((d+2)m+d^2+2d+2)x^2+((d+1)m+2)x+1. \quad (4.14)$$

If $[E:\mathbf{k}] = 4$, the related octic has Galois group $D_8(8)$, and is a defining polynomial for the splitting field L, while $P_w(x)$ as in Eq. (4.14) and $\bar{P}_w(x)$ are quartics in $\mathbf{k}[x]$ with $G \cong D_4$ which define the same conjugacy class of (non-normal) quartic subfields of L. Note that replacing d by $(m-2)/d$ interchanges $P_w(x)$ and $\bar{P}_w(x)$. If $d = (m-2)/d = t$, then $P_w(x) = \bar{P}_w(x) = P_t(x)$ as in §4.7. We give two other "degenerate" cases of Eqs. (4.13) and (4.14). In both cases, the "generic" Galois group is V_4.

When $d = -2$, $A = -m-2-A$, and $w^2 = y^2 = (m-6)^2/4$. By Eqs. (4.11c) and (d), $\mathrm{disc}(P_w(x)) \in \mathbf{k}^2$. We find $L = \mathbf{k}(\sqrt{(m-2)^2-16}, \sqrt{(m-4)^2-4})$. We have $A = -m-2-A$ for the pair $(m, A) = (2/3, -4/3)$ in Lemma 4.7 .

If $d = -1$ then $A = -3$, and $\mathrm{disc}(P_w(x)) \in \mathbf{k}^2$ when $m = 4-t-t^2$, $t \in \mathbf{k}$. In this case, $L = \mathbf{k}(\sqrt{t^2-4}, \sqrt{(t+1)^2-4})$.

If $swy \in \mathbf{k}$ or $wy \in \mathbf{k}$ and $[E:\mathbf{k}] = 4$, the related octics are distinct defining polynomials for the splitting field. We do not have a complete description of either $swy \in \mathbf{k}$ or $wy \in \mathbf{k}$. With respect to m, $\mathrm{Res}(w^2, y^2) = (A+4)^2(A^2+16)$. Taking $A = -4$, we find:

Proposition 4.16. *Let $t \in \mathbf{k}$.*

(a) If $[\mathbf{k}(\sqrt{t^2+4}, \sqrt{t^2-4}) : \mathbf{k}] = 4$, then the related octics $T(2-t^2, -4, x)$ and $T(2-t^2, t^2, x)$ are both irreducible in $\mathbf{k}[x]$, with $G \cong C_4 \times C_2$.

(b) If $[\mathbf{k}(\sqrt{t^2+4}, \sqrt{t^2+8}) : \mathbf{k}] = 4$, then the related octics $T(-t^2-2, -4, x)$ and $T(-t^2-2, t^2+4, x)$ are both irreducible in $\mathbf{k}[x]$, with $G \cong Q_8$.

Proof. One simply has to check that in both (a) and (b), the elementary Abelian 2-extension of $\mathbf{k}$ is $E = \mathbf{k}(s, w, y)$, that $wy \in \mathbf{k}$ in (a), and $swy \in \mathbf{k}$ in (b). □

Remarks. Taking $A = \pm 4i$ and $m = t^2 + 2 \mp 8i$ for $t \in \mathbb{Z}[i]$, $T(m, A, x)$ and the related octic are "typically" a pair of defining polynomials for a $C_4 \times C_2$ extension of $\mathbb{Q}(i)$ ($wy \in \mathbf{k}$).

With respect to A, $\mathrm{Res}(w^2, y^2) = (m-2)^2(m-6)^2$. Taking $m = 6$, we find that if $A = 8a_n - 4$ where $a_n + b_n\sqrt{2} = (3+\sqrt{2})^n$, the octics $T(6, A, x)$ and $T(6, -8-A, x)$ are pairs of defining polynomials for a family of quaternion fields reminiscent of the cyclic octic fields in [34].

If $sw \in \mathbf{k}$ and $[\mathbf{k}(s, y) : \mathbf{k}] = 4$, $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ are "Murphy's twins" in $\mathbf{k}[x]$, and define distinct cyclic quartic extensions of $\mathbf{k}$. The related octic is a defining polynomial for their join. We deal with Murphy's twins for $\mathbf{k} = \mathbb{Q}$ and $m, A \in \mathbb{Z}$, in §6.3.

4.7 Washington's cyclic quartic fields

We close this section with a discussion of the "degenerate" case $w^2 = 0$. It produces the polynomials $P(x)$ in Proposition 1.2(c). These give alternate defining polynomials for the cyclic quartic fields constructed by L.C. Washington in [41] when $\mathbf{k} = \mathbb{Q}$ and $t \in \mathbb{Z} - \{0, -2\}$.

Very early on, Phil Carmody drew the author's attention to examples of $T(m, A, x)$, $m, A \in \mathbb{Z}$, $m \neq \pm 2$, with repeated factors in $\mathbb{Z}[x]$. It was this observation that originally led us to consider the case $w^2 = 0$. As when $s^2 = 0$, $T(m, A, x)$ is again the square of a quartic in $\mathbf{k}[x]$.

If $m = t^2 + 2$, then $4(m-2) = 4t^2$, and $w = 0$ when $A = -t^2 - 4 \pm 2t$. To choose the $\pm$ sign, we substitute into the formulas in Lemma 4.4(d); we find that $Q_1 = Q_2 = \pm t$, and

$$\operatorname{disc}(q_1(x)) = \operatorname{disc}(q_2(x)) = t(t \mp 2)(u+1), \text{ whence} \tag{4.15}$$

$$\operatorname{disc}(q_1(x))\operatorname{disc}(q_3(x)) = t^2(t \mp 2)^2(t^2+4). \tag{4.16}$$

Taking $A = -t^2 - 4 - 2t$ gives $\operatorname{disc}(q_1(x))\operatorname{disc}(q_3(x)) = t^2(t+2)^2(t^2+4)$, the same form as the product of the discriminants of the quadratic factors of the quartics in [41]. Then $T(t^2+2, -t^2-2t-4, x) = P_t^2(x)$, where

$$P_t(x) = x^4 + (t^2+2t+4)x^3 + (t^3+3t^2+4t+6)x^2 + (t^3+t^2+2t+4)x + 1, \tag{4.17}$$

the $P(x)$ in Proposition 1.2(c). By Theorem 4.11, $P_t(x)$ is irreducible in $\mathbf{k}[x]$ when $t \in \mathbf{k}$, $t^2 + 4 \notin \mathbf{k}^2$, and $t \neq -2$.

Next, we relate the $P_t(x)$ to the cyclic quartics

$$f_t(x) = x^4 - t^2x^3 - (t^3 + 2t^2 + 4t + 2)x^2 - t^2x + 1 \tag{4.18}$$

in [41]. Clearly $f_t(x)$ is a reciprocal polynomial; if $f_t(\rho) = 0$ then the element of order 2 in the Galois group maps ρ to $1/\rho$. Similarly, the element σ^2 of order 2 in the Galois group of $P_t(x)$ maps a zero r to u/r. With $m = t^2 + 2$, we have $u^2 - (t^2+2)u + 1 = 0$, and $u = v^2$ where $v^2 - tv - 1 = 0$. Then $\sigma^2(r/v) = 1/(r/v)$, so r/v is a zero of a reciprocal polynomial. By formulating u and σ as rational expressions (mod $P_t(x)$), and using Pari-GP to bludgeon the algebra into submission, we find that

$$u \equiv -x^3 - (t^2+2t+3)x^2 - (t^3+2t^2+3t+3)x - 1 \pmod{P_t(x)}. \tag{4.19}$$

Taking $v = (u-1)/t$, we find that r/v is in fact a zero of $f_t(x)$.

Proposition 4.17. *If $t \in \mathbf{k} - \{0, -2\}$, $P_t(x)$ and $f_t(x)$ define the same extension of $\mathbf{k}$.*

Proof. Eq. (4.19) and $v = (u-1)/t$ give $f_t(x/v) \equiv 0 \pmod{P_t(x)}$, where

$$x/v \equiv (x^3 + (t^2+t+3)x^2 + (t^2+t+3)x + 1)/t^2 \pmod{P_t(x)}, \text{ if } t \neq 0.$$

Reformulating $v \pmod{f_t(x)}$, we have $P_t(xv) \equiv 0 \pmod{f_t(x)}$, where

$$xv \equiv (-x^2 + (t^2+t)x - 1)/(t+2) \pmod{f_t(x)}, \text{ if } t \neq -2.$$

Both transformations are defined when $t \in \mathbf{k} - \{0, -2\}$, and the result follows. □

Remarks. The related octic $T(t^2+2, 2t, x)$ has the repeated factor $(x^2 - tx - 1)^2$. The cofactor is a quartic which defines the same extension of $\mathbf{k}$ as $P_t(x)$.

5 $T(m, A, x)$ and number field extensions

We now apply the preceding results when $\mathbf{k}$ is a number field and $m, A \in \mathcal{O}_{\mathbf{k}}$, when the zeroes of $T(m, A, x)$ are units. We continue to assume that u is defined via Eq. (4.7b).

If $m^2 - 4 \notin \mathbf{k}^2$ and $w^2 y^2 \neq 0$, the zeroes of $T(m, A, x)$ are all simple by Proposition 4.10. We have the following result:

Theorem 5.1 (Real and complex zeroes)**.** *Let* $\mathbf{k}$ *be a number field,* $\mathbf{k} \subset \mathbb{R}$*,* $m, A \in \mathcal{O}_{\mathbf{k}}$*,* $m^2 - 4 \notin \mathbf{k}^2$*. Then the number of real zeroes of* $T(m, A, x)$ *is*

(a) None, if $s^2 < 0$ *or* $w^2 < 0$*;*

(b) Four, if $s^2 > 0$*,* $w^2 > 0$*, and* $y^2 < 0$*;*

(c) Eight, if $m < -2$*;*

(d) Eight , if $m > 2$*,* $w^2 > 0$*,* $y^2 > 0$*, and*

$$\left|(A+4)^2 + mA(A+4) + A^2\right| > 16; \text{ and}$$

(e) None, if $m > 2$*,* $w^2 > 0$*,* $y^2 > 0$*, and*

$$\left|(A+4)^2 + mA(A+4) + A^2\right| < 16,$$

i.e. if $2 < m < 6$ *and* $-m - 2 + 2\sqrt{m-2} < A < -2\sqrt{m-2}$.

Proof. For (a), $\mathbf{k}(s, w) \subset \mathbf{k}(r)$, so $\mathbf{k}(r) \not\subseteq \mathbb{R}$ for each zero r, by Lemma 4.8.

For (b), $\mathbf{k}(s, w) \subset \mathbb{R}$, so $q_i(x) \in \mathbb{R}[x]$. Now, $\operatorname{disc}(q_3(x))$ has the same sign as $\operatorname{disc}(q_1(x))$ by Lemma 4.6(b), while $\operatorname{disc}(q_2(x))$ and $\operatorname{disc}(q_4(x))$ have the opposite sign by Eqs. (4.11a) and (4.11c).

For (c), if $m < -2$ then $E = \mathbf{k}(s, w, y) \subset \mathbb{R}$, so the $\operatorname{disc}(q_i(x))$ all have the same sign. Here $u < 0$, so by Lemma 4.4(d), $\operatorname{disc}(q_1(x)) > 0$.

If $m > 2$, $w^2 > 0$, and $y^2 > 0$, then again the $\operatorname{disc}(q_i(x))$ all have the same sign, but here $u > 0$. Again using Lemma 4.4(d), $\operatorname{disc}(q_1(x))$ and $\operatorname{disc}(q_2(x))$ are both > 0 or both < 0, according as whether $|\alpha\beta| > 4u$ or $|\alpha\beta| < 4u$. By Lemma 4.4(a), $\alpha\beta = A + 4 + Au$. Multiplying by the corresponding conditions for $q_3(x)$ and $q_4(x)$ gives (d) and (e). □

Remarks. Suppose $m, A \in \mathbb{R}$. If $m < 2$ (in particular, when $s^2 < 0$), then $w^2 > 0$ and $y^2 > 0$. Since $\mathrm{Max}(|A|, |-m-2-A|) \geq |(m+2)/2|$, we have $\mathrm{Max}(w^2, y^2) \geq (m-6)^2/4 \geq 0$, so w^2 and y^2 cannot both be negative.

The cases $w^2 < 0$ and $y^2 < 0$ correspond to related octics. Thus, if $m > 2$ and A is such that $w^2 y^2 < 0$, one of the two related octics has signature $(0, 4)$ and the other has signature $(4, 2)$.

Suppose $T(m, A, x)$ is irreducible with $G \cong {}_8T_{11}$. Then the fixed field of complex conjugation is non-normal over $\mathbf{k}$ in cases (a) and (b). In case (e), the fixed field of complex conjugation is the elementary Abelian extension $E/\mathbf{k}$.

If $m^2 - 4 \notin \mathbf{k}^2$, $T(m, A, x)$ can have repeated zeroes only if $w = 0$ or $y = 0$. If $w = 0$ we have $T(t^2+2, -t^2-2t-4, x) = P_t^2(x)$ as in §4.7. The case $y = 0$ corresponds to the related octic $T(t^2+2, 2t, x)$. Assuming $\mathbf{k} \subset \mathbb{R}$, the following result allows us to deal with real and complex repeated zeroes.

Theorem 5.2. *Let $\mathbf{k} \subset \mathbb{R}$, $t \in \mathcal{O}_\mathbf{k}$, and $T(t^2+2, -t^2-2t-4, x) = P_t^2(x)$ as in §4.7. Then $P_t(x)$ has 4 real zeroes if $|t+1| > 1$, and none if $|t+1| < 1$.*

Proof. In §4.7, the choice $A = -t^2-2t-4$ makes $\mathrm{disc}(q_1(x)) = t(t+2)(u+1)$ in Eq. (4.15). Also in §4.7, $u = v^2$ where $v^2 - tv - 1 = 0$. Thus, $u + 1 \geq 1$, so $\mathrm{disc}(q_1(x))$ has the same sign as $t(t+2) = (t+1)^2 - 1$. □

The following result depends only on the fact that the zeroes of $T(m, A, x)$ are units when m and A are algebraic integers. We let $\sim$ indicate associates.

Proposition 5.3 (Exceptional sequences)**.** *Let $\mathbf{k}$ be a number field, $m, A \in \mathcal{O}_\mathbf{k}$, $m^2 - 4 \notin \mathbf{k}^2$, and $T(m, A, r) = 0$. Then*

(a) $r + 1 \sim r + u$ in $\mathbf{k}(r)$.

(b) If $m - 2 \in \mathcal{O}_\mathbf{k}^\times$, then $r, r+1, r+u$ is an exceptional sequence of three units.

Proof. For part (a), $\sigma(r) = (-r-1)/(r+u)$ is a zero of $T(m, A, x)$, hence is a unit. For part (b), use $P_s(-1) = \bar{P}_s(-1) = m-2$ and $(u-1)^2 = (m-2)u$. □

We obtain additional units and associates when m, A, and $w \in \mathcal{O}_\mathbf{k}$. The following result does *not* require that $[E : \mathbf{k}] = 4$.

Proposition 5.4 ("Constellations" of units and associates)**.** *Let $\mathbf{k}$ be a number field, $m, d \in \mathcal{O}_\mathbf{k}$, $d \mid m-2$, and A, w and $P_w(x)$ as in* Eqs. (4.13) *and* (4.14)*. If $P_w(r) = 0$, then*

(a) $r + 1 \sim r + u \sim r + 1 + d$, and $r \sim r + 1 + d + u \sim 1$.

(b) If $d \in \mathcal{O}_\mathbf{k}^\times$, then all the quantities in (a) *are units.*

Proof. In this case, $q_1(x) = x(x+1+d) + u(x+1) = x(x+1+d+u) + u$, giving (a). For (b), note that in Eq. (4.14), $P_w(-1) = d^2$. Thus, if $d \in \mathcal{O}_\mathbf{k}^\times$, $r + 1 \sim 1$, and the result follows. □

6 Extensions of $\mathbf{k} = \mathbb{Q}$

We let $\mathbf{k} = \mathbb{Q}$ and $m, A \in \mathbb{Z}$. For $|m|, |A + (m+2)/2| \leq 10^4$, a simple numerical sweep found that $[E : \mathbb{Q}] = 8$ for over 95% of pairs (m, A). So it appears that for $m, A \in \mathbb{Z}$, $T(m, A, x)$ "typically" produces non-normal octic fields whose normal closures over $\mathbb{Q}$ have Galois group $G \cong {}_8T_{11}$.

6.1 Real and complex fields

The only $(m, A) \in \mathbb{Z} \times \mathbb{Z}$ to which Theorem 5.1(e) applies, is $(4, -3)$. Here, $A = -(m+2)/2$, the "degenerate" case $d = -2$ of Eq. (4.14); we have $G \cong V_4$ and $L = \mathbb{Q}(\zeta_{12})$. The only $t \in \mathbb{Z}$ for which $|t + 1| < 1$ as in Theorem 5.2 is $t = -1$. In this case, $L = \mathbb{Q}(\zeta_5)$.

Apart from these cases, assuming $m \neq \pm 2$, by Theorem 5.1 the splitting field of $T(m, A, x)$ is totally real for $m, A \in \mathbb{Z}$ unless $s^2 < 0$ ($m = -1$, 0, or 1); or, $m > 2$ and $w^2 < 0$ or $y^2 < 0$. Now $y^2 < 0$ requires that $A^2 < 4(m-2)$, so non-real fields are relatively rare. When $[E : \mathbb{Q}] < 8$, they are even less common. We have the following result:

Theorem 6.1. *Let $m, A \in \mathbb{Z}$, $s^2w^2y^2 \neq 0$, L the splitting field of $T(m, A, x)$.*

(a) If $yw \in \mathbb{Z}$, then L is totally real unless $(m, A) = (1, -4)$, $(1, 1)$, or $(4, -3)$.

(b) If $swy \in \mathbb{Z}$, then L is totally real.

(c) If $m \in \mathbb{Z}$, $d \in \mathbb{Z}$, $d \mid m - 2$, $d^2 \leq |m - 2|$, and A and $P_w(x)$ are as in Eqs. (4.13) *and* (4.14)*, then L is totally real unless $(m, d) = (-1, \pm 1)$, $(0, \pm 1)$, $(1, \pm 1)$, $(4, -1)$, or $(m, -1)$ with $m > 4$.*

(d) If $sw \in \mathbb{Z}$, then L is totally real unless $(m, A) = (7, -4)$ or $(7, 1)$.

Proof. For (a) and (b), one simply checks the criteria of Theorem 5.1, keeping in mind that w^2 and y^2 cannot both be negative. For (c), we have $w^2 > 0$, and if $4 \leq d^2 \leq |m - 2|$, $|(m-2)/d + d| \leq |(m+2)/2|$, so $y^2 \geq (m-6)^2/4$.

For (d), we have the "polynomial square root" identity

$$s^2w^2 = (m^2 + Am + 2A + 4)^2 - 4A(A + 4)m - 8(A^2 + 4A + 8).$$

The "remainder" $-4A(A+4)m-8(A^2+4A+8)$ is even, so if s^2w^2 is a perfect square, its square root differs from $m^2 + Am + 2A + 4$ by an even integer $2k$. Now here, L is totally real unless $m > 2$ and $A^2 < 4(m - 2)$. This makes the remainder so small, we only need to consider the cases $-4 < A < 0$ and $0 \leq k \leq 4$. The only ones where $sw \in \mathbb{Z}$ and $s^2w^2y^2 \neq 0$ have $k = 1$, namely $(m, A) = (7, -4)$ and $(7, 1)$. □

We note that $(m,d) = (4,-2)$ defines the same pair $(m,A) = (4,-3)$ as $(m,d) = (4,-1)$ in (c).

The only cases where $L/\mathbb{Q}$ is Abelian and non-real are $(m,A) = (3,-3)$ or $(3,-2)$ ($L = \mathbb{Q}(\zeta_5)$); $(4,-3)$ ($L = \mathbb{Q}(\zeta_{12})$); $(1,-4)$ or $(1,1)$ ($L = \mathbb{Q}(\zeta_{15})$); $(7,-4)$ or $(7,-5)$ ($L = \mathbb{Q}(\zeta_{20})$); and $(7,1)$ or $(7,-10)$ ($L \subset \mathbb{Q}(\zeta_{95}), [L:\mathbb{Q}] = 8$). The cases $(m,A) = (7,-4)$ and $(7,1)$ give "Murphy's twins." In both cases, the splitting field of one is $\mathbb{Q}(\zeta_5)$, while that of the other is the real subfield of L. The $C_4 \times C_2$ cyclotomic field $\mathbb{Q}(\zeta_{16})$ is "left out," although its real subfield is the splitting field of $P_t(x)$ for $t = 2$.

All quaternion fields defined by $T(m,A,x)$ for $m, A \in \mathbb{Z}$ are totally real, by Theorem 6.1(b).

6.2 Special units

We have $\mathbb{Z}^\times = \{-1,1\}$, so Propositions 5.3(b) and 5.4(b) only apply with $m \in \{1,3\}$ and $d \in \{-1,1\}$, respectively.

The 1-parameter family $T(1,A,x), A \in \mathbb{Z}$, produces fields which are totally imaginary by Theorem 5.1(a), and with exceptional sequences of three units by Proposition 5.3(b). We have $[E:\mathbb{Q}] = 8$ except for $A \in \{-3,0\}$ or $\{-4,1\}$, when $[E:\mathbb{Q}] = 4$. Eq. (4.13) gives $A = -3$ when $d = -1$; the quartic factors $P_w(x) = x^4 + x^3 + 2x^2 + 2x + 1$ and $\bar{P}_w(x) = x^4 + 5x^3 + 8x^2 + 4x + 1$ of $T(1,-3,x)$, both have the minimum quartic discriminant (See [15]) of 117. The related octic, $T(1,0,x) = x^8 - 3x^6 + 3x^5 + 14x^4 + 15x^3 + 9x^2 + 3x + 1$, is a defining polynomial for the splitting field, the Hilbert Class Field of $\mathbb{Q}(\sqrt{-39})$.

Both related octics $T(1,-4,x)$ and $T(1,1,x)$ are irreducible in $\mathbb{Z}[x]$, with $G \cong C_4 \times C_2$, by Proposition 4.16(a) with $t = 1$. The splitting field is $\mathbb{Q}(\zeta_{15})$.

The 1-parameter family $T(3,A,x)$, $A \in \mathbb{Z}$, also produces fields with exceptional sequences of three units. But these fields are totally real, except when $A \in \{-6,1\}$, $\{-5,0\}$, $\{-4,-1\}$, or $\{-3,-2\}$. Since $4(m-2) = 4$ for $m = 3$, $w^2 \notin \mathbb{Z}^2$ and $y^2 \notin \mathbb{Z}^2$ unless $w^2y^2 = 0$. It is also not hard to check that with $m = 3$ and $A \in \mathbb{Z}$, $w^2y^2 \notin \mathbb{Z}^2$ and $s^2w^2y^2 = 5w^2y^2 \notin \mathbb{Z}^2$ unless $w^2y^2 = 0$. Thus, $[E:\mathbb{Q}] = 8$ unless either $5w^2 \in \mathbb{Z}^2$ or $5y^2 \in \mathbb{Z}^2$. Taking $5w^2 \in \mathbb{Z}^2$ gives a family of "Murphy's twins" (See Eqs. (6.3a) - (6.4b)). These define a family of cyclic quartic fields which (apart from $\mathbb{Q}(\zeta_5)$) are real, contain $\mathbb{Q}(\sqrt{5})$, and have exceptional sequences of three units by Proposition 5.3(b).

Using Pari-GP, we checked $T(m,A,x)$ for small values of m and A against the octic fields with small discriminants listed in the tables of [4]. We found that $T(3,-6,x)$, $T(1,-2,x)$, and $T(1,-14,x)$ all define the two conjugate octic fields of minimum discriminant for signature $(0,4)$ and $G \cong_8 T_{11}$. Each of these polynomials gives exceptional sequences of 3 units in those fields.

If $m, d \in \mathbb{Z}$, $m \neq \pm 2$, $d \mid m-2$, and r is a zero of $P_w(x)$ given by Eqs. (4.13) and (4.14), $\sigma(r) = (-r-1)/(r+u)$ is a unit in $\mathbb{Q}(r)$. When $d \neq -1$, this allows us to exhibit a system of three independent units for the field $\mathbb{Q}(r)$

when this is a totally real quartic field. The values $d = -1$ and $d = 1$ give the 1-parameter families

$$P_w(x) = x^4 + mx^3 + (m+1)x^2 + 2x + 1, \text{ and} \tag{6.1a}$$

$$P_w(x) = x^4 + (m+4)x^3 + (3m+5)x^2 + (2m+2)x + 1, \tag{6.1b}$$

respectively, to which Proposition 5.4(b) applies. If r is a zero of Eq. (6.1b), then (with u defined via Eq. (4.7b)) r, $r+1$, $r+2$, $r+u$, and $r+2+u$ are all units.

6.3 Murphy's twins

If $m, A \in \mathbb{Z}$ and $sw \in \mathbb{Z}$, the "Murphy's twins" $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ define cyclic quartic number fields when the conditions of Theorem 4.11 hold, and (with u and σ defined via Eq. (4.7b)) their zeroes are units satisfying (M) with $n = 4$. We give a description of "Murphy's twins" cyclic quartic fields having a given quadratic subfield, based on standard results about norms from real quadratic fields. We show that any quadratic field which is contained in *some* cyclic quartic field, is a subfield of infinitely many "Murphy's twins" cyclic quartic fields.

Let $d > 1$ be a squarefree integer, $K = \mathbb{Q}(\sqrt{d})$, and assume that $m \in \mathbb{Z}$, $m^2 - 4 = dN^2$, $N \in \mathbb{Z}$. Then $(m + N\sqrt{d})/2$ is a unit of norm 1 in $\mathcal{O}_K$, so m and N are (to within sign) generalized Lucas and Fibonacci numbers, respectively, which we describe as follows.

Let $\varepsilon > 1$ be the fundamental unit of K, and $\bar{\varepsilon}$ its conjugate. Let

$$\varepsilon^n = \frac{L_n + F_n(\varepsilon - \bar{\varepsilon})}{2}, \text{ where } L_n, F_n \in \mathbb{Z}. \tag{LF}$$

The properties in [11], Theorem 179, where $d = 5$, and L_n and F_n are the Lucas and Fibonacci numbers, easily generalize to any squarefree $d > 1$. We have $\mathbb{Q}(\sqrt{m^2-4}) = \mathbb{Q}(\sqrt{d})$ when $m = \pm L_n$, where n is arbitrary if $\mathcal{N}(\varepsilon) = +1$, but n must be *even* if $\mathcal{N}(\varepsilon) = -1$.

Now we want $w^2 = dY^2$ for some $Y \in \mathbb{Z}$. Taking $X = m + A + 2 \in \mathbb{Z}$, we may express this as $(X + Y\sqrt{d})/2 = \pi \in \mathcal{O}_K$, $\mathcal{N}(\pi) = m - 2$. Then $X^2 + (m-2)^2 = d(N^2 + Y^2)$, so d is the sum of two squares, as expected if K is contained in a cyclic quartic field. We have the following result:

Proposition 6.2. *Let $d > 1$ be squarefree, $d = a^2 + b^2$, $K = \mathbb{Q}(\sqrt{d})$, L_n and F_n as in* Eq. (LF)*. There are infinitely many m such that $\mathbb{Q}(s) = K$, for which there are infinitely many $A \in \mathbb{Z}$ such that $T(m, A, x) = P_{sw}(x)\bar{P}_{sw}(x)$ in $\mathbb{Z}[x]$.*

Proof. If $\mathcal{N}(\varepsilon) = -1$, then for any $j \in \mathbb{Z}$, we obtain $sw \in \mathbb{Z}$ by taking

$$m = L_{2k},\ X + Y\sqrt{d} = 2(\varepsilon^{2k} - 1)\varepsilon^{2j-1}, \text{ and } A = -m - 2 \pm X.$$

If $\mathcal{N}(\varepsilon) = +1$, choose n and the $\pm$ sign so that $u = \pm\varepsilon^n \equiv 1 \pmod{a\mathcal{O}_K}$. Then $(u-1)/a \in \mathcal{O}_K$, so $sw \in \mathbb{Z}$ for any $j \in \mathbb{Z}$, if

$$m = \pm L_n, X + Y\sqrt{d} = 2((u-1)/a)(b - \sqrt{d})\varepsilon^j, \text{ and } A = -m - 2 \pm X.$$

□

Remark. The condition $\mathcal{N}(\pi) = m - 2$ may well have other solutions than those given in Proposition 6.2.

Thus, there are "Murphy's twins" cyclic quartic fields containing $\mathbb{Q}(\sqrt{d})$ whenever $d > 1$ is squarefree and the sum of two squares. But if d is even, and $K = \mathbb{Q}(\sqrt{d})$ has $\mathcal{N}(\varepsilon) = +1$, K is *not* a subfield of any of Washington's cyclic quartic fields (their quadratic subfields all have $\mathcal{N}(\varepsilon) = -1$), or (as is easily shown) of any "simplest" quartic fields. The smallest such d is 34.

The only non-real Murphy's twins cyclic quartic field is $\mathbb{Q}(\zeta_5)$, which occurs when $(m, A) = (3, -3)$, $(3, -2)$, $(7, -4)$, and $(7, 1)$.

We can make $P_{(sw)'}(x) = x^4 P_{sw}(1/x)$ as per Proposition 2.2, with parameter $m' = m$, the same square root s of $m^2 - 4$, and $(sw)' = s \cdot w'$, specifying A' and w' by

$$\frac{m + 2 + A' + w'}{2} = \left(\frac{m + 2 + A - w}{2}\right)\left(\frac{m + s}{2}\right), \text{ that is} \tag{6.2a}$$

$$A' = \frac{m^2 + mA - 4 - sw}{2} \text{ and } w' = \frac{(m + A + 2)s - mw}{2}. \tag{6.2b}$$

Of course, $(m, A', -s, -w')$ gives the same $P_{(sw)'}(x)$ as (m, A', s, w'). Note, however, that if $sw \neq 0$, $P_{sw}(x)$ and $\bar{P}_{sw}(x)$ produce different values of A'. For the $P_t(x)$ in §4.7, $A' = -t^3 - t^2 - 2t - 4$ and $(sw)' = -t^5 - 4t^3$ give $P_{(sw)'}(x) = x^4 P_t(1/x)$.

The case $m = 3$ is particularly simple. Here, $d = 5$, $\varepsilon = \tau$, the "golden ratio," and $(X + Y\sqrt{5})/2$ has norm $m - 2 = 1$. We take $X = L_{2j}$. With $A = -5 + L_{2j}$ and $sw = 5F_{2j}$, we obtain

$$P_{sw}(x) = x^4 + (5 - L_{2j})x^3 + (9 - 5F_{2j-1})x^2 + (5 - L_{2j-2})x + 1 \text{ and} \tag{6.3a}$$

$$\bar{P}_{sw}(x) = x^4 + (5 - L_{2j})x^3 + (9 - 5F_{2j+1})x^2 + (5 - L_{2j+2})x + 1. \tag{6.3b}$$

With $A = -5 - L_{2j}$ and $sw = 5F_{2j}$, we obtain

$$P_{sw}(x) = x^4 + (5 + L_{2j})x^3 + (9 + 5F_{2j+1})x^2 + (5 + L_{2j+2})x + 1 \text{ and} \tag{6.4a}$$

$$\bar{P}_{sw}(x) = x^4 + (5 + L_{2j})x^3 + (9 + 5F_{2j-1})x^2 + (5 + L_{2j-2})x + 1. \tag{6.4b}$$

As suggested by Eq. (6.2a), in both families $x^4 P_{sw}(1/x)$ is obtained by taking $\bar{P}_{sw}(x)$ and shifting the index.

As mentioned in §6.2, the cyclic quartic fields given by Eqs. (6.3a)-(6.4b) have exceptional sequences of three units r, $r+1$, $r+u$ as per Proposition 5.3(b). The zeroes of the related octics also give exceptional sequences of three units, which are generally of degree 8 over $\mathbb{Q}$.

It is easy to show that for a given m, there can be only finitely many $A \in \mathbb{Z}$ for which either y^2 or y^2w^2 is a perfect square. Consequently, for a given m there can be only finitely many A yielding Murphy's twins which do *not* have distinct cyclic quartic splitting fields. The octics with $(m, A) = (-3, -4)$, $(-7, 8)$, and $(-66, 13)$, are the only examples we know where $s^2w^2y^2 \neq 0$ and the "twins" have the *same* C_4 splitting field.

6.4 The cases $[L:\mathbb{Q}] = 8$ when $wy \in \mathbb{Z}$, $swy \in \mathbb{Z}$, and $w \in \mathbb{Z}$

We apply Proposition 4.16 to the cases $wy \in \mathbb{Z}$ and $swy \in \mathbb{Z}$ by taking $t \in \mathbb{Z}^+$. In (a), we have $[E:\mathbb{Q}] = 4$ when $t \neq 2$; and in (b), $[E:\mathbb{Q}] = 4$ when $t > 1$. Clearly t^2-4 and t^2+4 are both squarefree for a positive proportion of $t \in \mathbb{Z}^+$; likewise for t^2+4 and t^2+8, so these families of $C_4 \times C_2$ and Q_8 number fields are infinite. The family of quaternion fields mentioned in the Remarks after Proposition 4.16 may also be shown to be infinite.

When $m, d \in \mathbb{Z}$, $m \neq \pm 2$, and $d \mid m-2$ in Eqs. (4.13) and (4.14), it is not hard to show that $P_w(x)$ is irreducible in $\mathbb{Z}[x]$ unless $d = -2$ and $m = 6$. Apart from the special cases described after Eqs. (4.13) and (4.14), the only instances we know where $P_w(x) \in \mathbb{Z}[x]$ has $G \ncong D_4$ are $(m, A) = (-3, 5)$, $(-7, -3)$ and $(-66, 51)$. In these instances, $s^2y^2 \in \mathbb{Z}^2$, and $G \cong C_4$. The related octics are the 3 instances mentioned in §6.3 in which the "twins" both define the *same* C_4 field.

6.5 Regulator formulas

Let $\mathbf{k} = \mathbb{Q}$, and $m, A \in \mathbb{Z}$. If $T(m, A, r) = 0$ and $F = \mathbb{Q}(r)$, then $\mathcal{O}_F^\times$ has rank 3 if F has signature $(0, 4)$ or $(4, 0)$. We show that in most such cases, the system $\langle \zeta, \varepsilon, r, \sigma(r) \rangle$ has rank 3, where $\langle \zeta \rangle$ is the torsion units in F, ε is the fundamental unit of a real quadratic subfield of F, $\sigma(r)$ is as in Eq. (C4) with u as per Eq. (4.7b). The regulator formulas are similar to those in [17] and [41].

In the following three results (which we state without proof), by Theorem 4.11 we can treat σ as a field isomorphism. Checking that the $\ln^2()$ values are not both 0, is left as an exercise for the reader.

Proposition 6.3. *Let $m \in \{-1, 0, 1\}$, $(m, A) \neq (-1, -3)$, $(-1, 1)$, $(0, -3)$, $(0, -1)$, or $(1, -3)$. Let $\varepsilon > 1$ be the fundamental unit of $\mathbb{Q}(w)$ and $\langle \zeta \rangle$ the torsion units in $\mathbb{Q}(r)$. Then*

$$\mathrm{Reg}\langle \zeta, \varepsilon, r, \sigma(r) \rangle = 16 \ln(\varepsilon) \left(\ln^2 |r| + \ln^2 |\sigma(r)| \right) \neq 0.$$

Proposition 6.4. *Let $m > 2$ and $(m+2+A)^2 < 4(m-2)$. Let $\varepsilon > 1$ be the fundamental unit of $\mathbb{Q}(s)$ and $\langle\zeta\rangle$ the torsion units in $\mathbb{Q}(r)$. Then*

$$\mathrm{Reg}\langle\zeta, \varepsilon, r, \sigma(r)\rangle = 4\ln(\varepsilon)\left(\ln^2\left|r^2/u\right| + \ln^2\left|\sigma(r)^2 u\right|\right) \neq 0.$$

Proposition 6.5. *Let $|m| > 2$. Assume $T(m, A, x) = P_{sw}(x)\bar{P}_{sw}(x)$ in $\mathbb{Z}[x]$, $(m, A) \neq (3, -2)$ or $(3, -3)$. Let $\varepsilon > 1$ be the fundamental unit of $\mathbb{Q}(s)$. If $T(m, A, r) = 0$, $[\mathbb{Q}(r):\mathbb{Q}] = 4$, and $\mathbb{Q}(r)$ is real, then*

$$\mathrm{Reg}\langle -1, \varepsilon, r, \sigma(r)\rangle = \frac{1}{2}\ln(\varepsilon)\left(\ln^2\left|r^2/u\right| + \ln^2\left|\sigma(r)^2 u\right|\right) \neq 0.$$

For $P_w(x)$ as in Eqs. (4.13) and (b), $\sigma(r)$ is a unit in $\mathbb{Q}(r)$, but it is *not* an algebraic conjugate of r. In this case we have the following result:

Proposition 6.6. *Let $m, d \in \mathbb{Z}$, $d \mid m-2$, $d \neq -1$, $d^2 \leq |m-2|$. Let $P_w(x)$ be as in* Eqs. (4.13) and (b). *Assume $P_w(x)$ is irreducible with signature $(4, 0)$, and $\varepsilon > 1$ is the fundamental unit of $\mathbb{Q}(s)$. Then up to a factor of $(1 + O(|d/m-2|)) = (1 + O(1/\sqrt{|m-2|}))$,*

$$\mathrm{Reg}\langle -1, \varepsilon, r, \sigma(r)\rangle \approx$$
$$2\ln(\varepsilon)\left|\ln^2|m-2| + \ln\left|(d+1)^2/d\right|\ln|m-2| - \ln|d|\ln|d+1|\right|.$$

Proof. With $R = 1/(m-2)$, we can express the zeroes of $x^2 - mx + 1$ or $x^2 - (1/R+2)x + 1$ as formal power series in R, $u_1 = 1/R + 2 - R + 2R^2 + \ldots$ and $u_2 = R - 2R^2 + \ldots$, which converge for $|m-2| > 4$.

Taking $q_1(x) = x^2 + (1 + d + u_1)x + u_1$, with a zero $r_1 \approx -1$, we obtain a formal series for r_1 with terms $p_k(d)R^k$, where $p_k(d) \in \mathbb{Z}[d]$ has degree k. This gives a series for $\sigma(r_1) = -(r_1+1)/(r_1+u_1)$. Now $P_w(x) = q_1(x)q_4(x)$, where $q_4(x) = x^2 + (d+1+u_2)x + u_2$, which has a zero $r_3 \approx -d-1$. (The coefficient of R^k in the series for r_3 has a power of $d+1$ in the denominator.) Using ε, r_1, $\sigma(r_1)$; $\varepsilon' = \pm\varepsilon^{-1}$, r_3, $\sigma(r_3) = -(r_3+1)/(r_3+u_2)$; and ε, $r_2 = u_1/r_1$, $\sigma(r_2) = u_2/\sigma(r_1)$ to form the regulator determinant then gives the result. □

Remarks. When $d = -1$ the quartic fields defined by the $P_w(x)$ in Eq. (6.1a) are totally real when $m < -2$, but $r+1, r+u \in \langle -1, \varepsilon, r\rangle$, so $\langle -1, \varepsilon, r, \sigma(r)\rangle$ has rank 2 at most. When $m = 4 - t - t^2$, $t \in \mathbb{Z}$, $t > 2$, and $G = V_4$, the fundamental units of the 3 quadratic subfields of the splitting field give 3 independent units.

Now $\sigma(r) = (-r-1)/(r+u) = -(r+1)^2/rq_1(-1)$. Thus, $r+1$ and $r+u$ are both units precisely when $q_1(-1) = (m + A + 2 + w)/2$ is a *unit*. With $\mathbf{k} = \mathbb{Q}$ and $m, A \in \mathbb{Z}$, we then find that $q_1(-1) \in \langle\zeta, \varepsilon\rangle$, so

$$[\langle\zeta, \varepsilon, r, r+1\rangle : \langle\zeta, \varepsilon, r, \sigma(r)\rangle] = 2, \text{ when } q_1(-1) = \pm 1, \text{ or } m - 2 = \pm 1 \quad (6.5)$$

This gives a "one-half" regulator in Proposition 6.3 when $m = 1$; in Proposition 6.4 when $m = 3$ and $A = -6$, -5, or -4; for the quartics in Eqs. (6.3a) - (6.4b); and for the quartics in Eq. (6.1b).

The regulators in Propositions 6.3–6.6 can be extremely small. We estimate the "one-half" regulator $R_1 = \mathrm{Reg}\langle \zeta, \varepsilon, r, r+1\rangle$ for infinite families with $\varepsilon = \tau$, the "golden ratio;" this makes the factor $\ln(\varepsilon)$ as small as possible.

When $m = 1$, $A \in \mathbb{Z}$, $A \neq -3$, and $T(1, A, r) = 0$, $F = \mathbb{Q}(r)$ is a totally imaginary octic field. Here $y^2 = A^2+4$. By Eq. (4.11c), if A^2+4 is squarefree, $\Delta(F/\mathbb{Q}) = (\Delta(\mathbb{Q}(s, w)/\mathbb{Q}))^2(A^2 + 4)^2$. Taking $A = L_{2j-1} - 3$ makes $\varepsilon = \tau$. Then, refining $r \approx -1$ gives, assuming $(L_{2j-1} - 3)^2 + 4$ is squarefree,

$$R_1 = \frac{1}{2}\ln(\tau)\ln^2\left(\frac{1}{15^4}\Delta(F/\mathbb{Q})\right)\left(1 + O\left(1/|A|\right)\right). \tag{6.6}$$

Let F be a real cyclic quartic field given by Eq. (6.3a). Using Lemma 4.4(d), $\mathrm{disc}(q_1(x))\mathrm{disc}(q_3(x)) = 5(F_{2j-1} - 2)^2$. Refining $r \approx -1$, and using Proposition 6.5, we find that if $F_{2j-1} - 2$ is squarefree and prime to 10, then

$$R_1 = \frac{1}{4}\ln(\tau)\ln^2\left(\frac{1}{5^2}\Delta(F/\mathbb{Q})\right)\left(1 + O\left(1/j^2\right)\right). \tag{6.7}$$

Replacing $F_{2j-1} - 2$ with $F_{2j-1} + 2$, and assuming this is squarefree and prime to 10, we again obtain Eq. (6.7) for the real cyclic quartic fields given by Eq. (6.4b).

Using Proposition 6.6 and Eq. (4.11c), we obtain an estimate asymptotically equal to that in Eq. (6.7) for the non-normal quartic fields defined by Eq. (6.1b), taking $m = L_{2j}$, a Lucas number of even index, if $4L_{2j}^2 + 9$ is squarefree.

The regulator estimates in Eqs. (6.6) and (6.7) are comparable to the lower bound in [35], for totally imaginary octic fields with a real quadratic but not a real quartic subfield, or for real quartic fields with a quadratic subfield.

We do not know that the squarefreeness conditions are satisfied infinitely often, but we do not know any reason to assume otherwise. The numbers $F_{2j-1} \pm 2$ are always the product of a Fibonacci number and a Lucas number whose indexes differ by 3, but the squarefreeness question for these is also open.

In [41], Washington obtains a lower bound for the regulators of the cyclic quartic fields defined by $f_t(x)$ which proves the system of 3 units he gives is fundamental when t, $t+4$, and t^2+4 are squarefree, except when $t = 1$. The system in Proposition 6.5 for $P_t(x)$ has the same regulator. In the case $t = 1$, the system $\langle -1, \tau, r, r+1\rangle$ for Eqs. (6.4a) and (b) with $j = 0$ is fundamental.

7 Concluding remarks

The condition (M) provides a conceptual unification of all families of number fields previously dubbed "simplest." It also enabled us to re-derive both the "simplest" quartic fields and Washington's cyclic quartic fields by elementary methods, and to place both families together in a larger context.

For purely algebraic purposes, the substitution $A \leftarrow -(m+2)/2 + \mathbf{v}$ used in the proof of Theorem 4.13 may be useful.

However, more sophisticated methods than used here would surely be required to construct algebraic maps σ satisfying (M) for $n > 4$. More powerful techniques would probably also refine and elaborate some of our results considerably, particularly those in §6.5. Those wanting to to investigate class number or unit index questions might want to read [8], [9], [17], [26], [12] and [13] first.

We note that (M) and its σ-conjugates can be viewed as a system of n constraints which may limit the relative sizes of $r, \sigma(r), \ldots, \sigma^{n-1}(r)$. This might help account for the previously-noted feature of small regulators in "simplest" cyclic number fields of low degree. In this regard, the factorization of the "circulant" matrix determinant (see, for example, Lemma 5.26 in [39]) might be of interest.

We chose the variable names s and w prior to learning about the "simplest" quartic fields or Washington's cyclic quartic fields. The fact that the conditions $s = 0$ and $w = 0$ turned out to produce the "simplest" quartic fields and Washington's cyclic quartic fields respectively, is a coincidence that absolutely delights the author.

While investigating Eq. (C4), we noticed that $f : x \mapsto (-x-1)/(x+u)$ has compositional order 10 when $u^2 + 3u + 1 = 0$. The compositional powers $f^{(3)}$ and $f^{(7)}$ make (M) a formal identity with $n = 10$. With $K = \mathbb{Q}(\sqrt{5})$,

$$\sum_{k=0}^{9} f^{(k)}(x) = 2(A + Bu),\ A, B \in \mathbb{Z}$$

produces a family of totally real C_{10} extensions of K defined by units whose conjugates satisfy (M), and which have exceptional sequences of *four* units. The normal closure over $\mathbb{Q}$ has "generic" Galois group ${}_{20}T_{53}$.

Acknowledgements

Without Phil Carmody's willingness to perform many Pari-GP calculations, this work would hardly have begun; and his subsequent guidance in using the software was most useful in completing it. My thesis advisor Leon McCulloh gave indispensable advice and assistance with the submission process,

and pointed out simplifications of some of the arguments. Jürgen Klüners suggested rational rather than integer parameter values, and using Magma to compute Galois groups of 1-parameter families of polynomials. Derek Holt's description of ${}_8T_{11}$ as a central product, and Laurent Bartholdi's use of GAP were instrumental in understanding ${}_8T_{11}$ and ${}_{20}T_{53}$. H. W. Lenstra, jr. and Gerhard Niklasch provided historical context and specific references for the terminology and applications of exceptional units.

The members of the North Dakota NMBRTHRY listserv supplied more helpful suggestions and calculations than I can list here. Claus Fieker provided very helpful guidance about ${}_8T_{11}$. Franz Lemmermeyer, Attila Pethő, Siman Wong and Volker Ziegler provided useful bibliographic references. Duncan Buell, Kok Seng Chua and Odile Lecacheux sent papers. Duncan Buell, George Gras, Patrick Morton, and Lawrence Washington sent papers, and also helped clarify the origins of the bestowal of sobriquet "simplest" on number fields. To them, and to many others, my heartfelt thanks. I hope the ideas and results presented here will in some measure repay their generosity.

References

[1] D. A. Buell and V. Ennola, *On a parameterized family of quadratic and cubic fields*, J. Number Theory **54** (1995), 134–148.

[2] Robin J. Chapman,*Automorphism Polynomials in Cyclic Cubic Extensions*, J. Number Theory **61**, (1996) 283–291

[3] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin *et al* 1993

[4] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Tables of octic fields with a quartic subfield*, Math. Comp. **68** (1999) 1701-1716

[5] H. Cohn, *A device for generating fields of even class number*, Proc. Amer. Math. Soc., **7** (1956) 595–598.

[6] Harvey Cohn, *Advanced Number Theory*, Dover, New York 1980. Originally published in 1962 as *A Second Course in Number Theory* by John Wiley and Sons

[7] H. Darmon, *Note on a polynomial of Emma Lehmer*, Math. Comp. **56** (1991), 795-800

[8] M. N. Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1977) 179–182

[9] M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques reeles de degré 4 de* $\boldsymbol{Q}$, Publ Math. Fac. Sci. Bensacon **2** (1977/8) 1–26, 1–53

[10] Marshall Hall, Jr., *The Theory of Groups*, Macmillan, New York, 1959

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, New York, 1988

[12] Helmut Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, In Mathematische Abhandlungen, pages 285-379, Walter de Gruyter, Berlin, 1975, Originally published 1950.

[13] ———, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

[14] Derek Holt, private communications

[15] Loo Keng Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin, Heidelberg, New York, English edition 1982

[16] Serge Lang, *Algebra*, Addison-Wesley, revised 1971

[17] A. J. Lazarus, *On the Class Number and Unit Index of Simplest Quartic Fields*, Nagoya Math J. **121** (1991) 1–13

[18] O. Lecacheux, *Unités d'une famille de corps cycliques réels de degré 6 liès à la courbe modulaire* $X_1(13)$, J. Number Theory **31** (1989), 54-63

[19] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541.

[20] H. W. Lenstra, Jr., *Euclidean number fields of large degree*, Invent. Math. **38** (1977) 237–254

[21] G. Lettl, A. Pethő, and P. Voutier, *Simple Families of Thue Inequalities*, Trans. Amer. Math. Soc. **351** (1999) 1871–1894

[22] ———, *On the arithmetic of simplest sextic fields and related Thue equations*, In *Number Theory*, K. Győry, A.Pethő and V.T. Sós Eds., Walter de Gruyter GmbH & Co., Berlin-New York, 1998, pp. 331–348.

[23] A. Leutbecher, *Euclidean fields having a large Lenstra constant*, Ann. Inst. Fourier Grenoble **35** (1985) 83–106

[24] A. Leutbecher and J. Martinet, *Lenstra's constant and Euclidean number fields*, *Astérisque* **94** (1982) 87–131

[25] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields.* In *Number Theory*, Proc. Jour. Arith., Ulm, 1987. Ed. H. P. Schlickewei and E. Wirsing, 150–178. *Lecture Notes in Mathematics* 1380, Springer-Verlag, New York *et al* 1989

[26] S. R. Louboutin, *Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields*, Math. Comp. **76** (2007), 455-473

[27] J. Mináč and T. L. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137** (1991), 1–11.

[28] P. Morton, *Characterizing Cyclic Cubic Extensions by Automorphism Polynomials.* J. Number Theory, **49** (1994) 183-208

[29] ———, *Arithmetic properties of periodic points of quadratic maps, II* Acta Arithmetica LXXXVII.2 (1998)

[30] T. Nagell, *Sur un type particulier d'unités algébriques*, Arkiv f. Matem **8** #18 (1969), 163–164

[31] Yuichi Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2215–2218.

[32] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (182) (1988), 543–556

[33] D. Shanks, *The Simplest Cubic Fields*, Math. Comp. **28** (1974) 1137–1152

[34] Y. Y. Shen, *Unit Groups and Class Numbers of Real Cyclic Octic Fields*, Trans. Amer. Math Soc. **326** (1991) 179–209

[35] J. H. Silverman, *An inequality relating the regulator and the discriminant of a number field*, J. Number Theory **19** (1984), 437-442

[36] B. K. Spearman and K. S. Williams, *Normal integral bases for Emma Lehmer's parametric family of cyclic quintics*, J. Théor. Nombres Bordeaux **16** (2004), 215-220

[37] E. Thomas, *Fundamental units for orders in certain cubic number fields*, J. Reine Angew. Math. **310** (1979), 33–55.

[38] Kôji Uchida, *Class numbers of cubic cyclic fields*, J. Math. Soc. Japan **26** (3) (1974)

[39] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate texts in Math., vol. 83, Springer-Verlag, New York, 1982.

[40] _____, *Class Numbers of the Simplest Cubic Fields*, Math. Comp., **48**, (177) (Jan., 1987), 371-384

[41] _____, *A Family of Cyclic Quartic Fields Arising from Modular Curves*, Math. Comp. **57** (1991), 763-775

Kurt Foster
601 Columbia Court
Colorado Springs, CO 80904
E-mail address: drsardonicus@earthlink.net