ACTA ARITHMETICA
LXII.4 (1992)

Arithmetic properties of periodic points of quadratic maps

by

Patrick Morton (Wellesley, Mass.)

1. Introduction. Iterating polynomial maps gives a convenient way of finding extensions of $\mathbb{Q}$ whose Galois groups are subgroups of special imprimitive groups known as wreath products, as has been shown by Odoni ([o1], [o2]). Subgroups of wreath products occur as Galois groups not only for the iterates studied by Odoni, but also for the algebraic number fields generated by the periodic points of a polynomial map (see [m1] and [vh]). In particular, studying periodic points of iterated maps over a number field leads naturally to some parametrized families of polynomials with special Galois groups. One of the purposes of this paper is to illustrate this by investigating the algebraic and number-theoretic properties of periodic points of order 3 of a quadratic map over an arbitrary field κ whose characteristic is different from 2. The investigation shows that the arithmetic properties of these periodic points are related to an interesting curve of genus 4. This is part of a larger project to study the Galois groups of periodic points of arbitrary polynomial maps. (See [m1] and [pa].)

Thus, let $\sigma(x)$ be a polynomial over a field κ, and denote by $\sigma^n(x)$ the n-fold iteration of σ with itself:

$$\sigma^0(x) = x\,, \qquad \sigma^{n+1}(x) = \sigma(\sigma^n(x))\,, \qquad n \geq 0\,.$$

Then $\sigma^n(x) - x$ factors over κ as

$$\sigma^n(x) - x = \prod_{d\,|\,n} \Phi_{d,\sigma}(x)\,,$$

where the polynomial $\Phi_{n,\sigma}(x)$ is defined using the Möbius function μ:

$$\Phi_{n,\sigma}(x) = \prod_{d\,|\,n} (\sigma^d(x) - x)^{\mu(n/d)}\,.$$

The polynomial $\Phi_{n,\sigma}(x)$ has *among* its roots all the periodic points of σ of exact order n in an algebraic closure of κ; usually these are all the roots of $\Phi_{n,\sigma}(x)$, e.g. when $\Phi_{n,\sigma}(x)$ has no multiple roots. The degree of $\Phi_{n,\sigma}(x)$ is

equal to

$$\deg \Phi_{n,\sigma}(x) = \sum_{d\,|\,n} \mu(n/d)(\deg \sigma)^d\,,$$

and the splitting fields $\Sigma_{n,\sigma}$ of these polynomials $\Phi_{n,\sigma}(x)$ are the fields whose Galois groups are computed in [m1] and [pa]. (Also see [vh].)

In [m1] it is proved that

$$\Phi_{n,\sigma}(x)\,|\,\Phi_{n,\sigma}(\sigma(x))\,, \tag{1}$$

which implies that the map σ permutes the roots of $\Phi_{n,\sigma}(x)$, and that these roots fall into distinct orbits under σ. This is a well-known result in the classical case, when $\kappa = \mathbb{C}$ or $\mathbb{R}$.

This raises the following

QUESTION. *Are the elements of an orbit algebraic conjugates over the base field* κ?

The answer to this question is *no* in general, since, for example, if $\sigma(x) = x^2 - 29/16$, we have

$$\Phi_{3,\sigma}(x) = \left(x + \frac{7}{4}\right)\left(x + \frac{1}{4}\right)\left(x - \frac{5}{4}\right)\left(x^3 + \frac{1}{4}x^2 - \frac{41}{16}x + \frac{23}{64}\right). \tag{2}$$

However, the answer to the above question is *yes* "generically". This means that if $\overline{\sigma}(x) = x^k + a_1x^{k-1} + \ldots + a_k$ is a "generic" polynomial over $\mathbb{Q}$ with coefficients a_i which are algebraically independent variables over $\mathbb{Q}$, then the divisibility relation $\bar{f}(x)\,|\,\bar{f}(\overline{\sigma}(x))$ holds for all irreducible factors $\bar{f}$ of $\Phi_{n,\bar{\sigma}}(x)$ over $\mathbb{Q}(a_1, a_2, \ldots, a_k)$. (For the proof see [m1].) In general, the roots of an irreducible factor f of $\Phi_{n,\sigma}(x)$ consist of complete orbits if and only if

$$f(x)\,|\,f(\sigma(x))\,. \tag{3}$$

In this paper I will first use the elementary theory of function fields to consider this question in detail when σ is quadratic and $n = 3$. In this case $\deg \Phi_{3,\sigma}(x) = 6$, and using (1) it is easy to see that the set of degrees of the irreducible factors of $\Phi_{3,\sigma}(x)$ can only be one of the following: $\{6\}$, $\{3,3\}$, $\{1,1,1,3\}$, $\{1,1,1,1,1,1\}$, $\{2,2,2\}$. Furthermore, it is clear that if two polynomials σ_1 and σ_2 are related by

$$\sigma_1 = \ell \circ \sigma_2 \circ \ell^{-1}\,,$$

where ℓ is a linear polynomial in $\kappa[x]$, then the corresponding Φ-polynomials will factor in the same way (as long as these polynomials have no multiple roots). We will call such pairs of polynomials *equivalent*, or *linearly conjugate*, pairs.

On the basis of extensive calculations over $\mathbb{Q}$ it appears that the factorization types $\{1,1,1,1,1,1\}$ and $\{2,2,2\}$ *never occur*. I will prove this

fact in Section 3. A consequence is that for every quadratic polynomial σ over $\mathbb{Q}$, at least one of the orbits of roots of $\Phi_{3,\sigma}(x)$ consists of algebraic conjugates over $\mathbb{Q}$. In addition, each of the factorization types $\{6\}$, $\{3,3\}$, $\{1,1,1,3\}$ occurs for infinitely many classes of polynomials over $\mathbb{Q}$.

The argument will show that the factorization of $\Phi_{3,\sigma}(x)$ over $\mathbb{Q}$ depends on several diophantine conditions. We first state

THEOREM 1. *Let κ be a field whose characteristic is different from 2. If $\sigma(x)$ is a quadratic polynomial in $\kappa[x]$ for which $\Phi_{3,\sigma}(x)$ factors as a product of three irreducible quadratics, then either*:

(i) *$\sigma(x)$ is equivalent to x^2, the polynomial x^3-x^2-2x+1 splits in κ and -7 is not a square in κ; or*

(ii) *the equation*

$$\delta^2 = 4\alpha(\alpha+1)(\alpha^2-3\alpha+4) \tag{4}$$

has solutions in κ other than $(\alpha,\delta)=(0,0)$, $(-1,0)$, $(1,\pm 4)$, for which the number d given by

$$d = \frac{\alpha^2-1-(3\alpha^2-2\alpha-9)\beta}{\beta^3-\beta^2}\,, \tag{4'}$$

with

$$\beta = \frac{-4\alpha^3+2\alpha^2+6\alpha+\delta}{-8(\alpha^3-\alpha^2-2\alpha+1)} \neq 0\,, \tag{4''}$$

is not a square in κ.

If $\beta=1$ in (4''), then instead of (4') we have $d=(11\pm\sqrt{17})/2$, corresponding to the solutions $(\alpha,\delta)=((1\pm\sqrt{17})/2, \pm 2(1\pm\sqrt{17}))$ of (4).

In case (ii), *$\sigma(x)$ is equivalent over κ to the polynomial $x^2-(d+28)/16$.*

Conversely, if the conditions of (i) *or* (ii) *hold, then $\Phi_{3,\sigma}(x)$ factors as a product of three irreducible quadratic polynomials over κ.*

The curve defined by equation (4) is rationally equivalent to the curve

$$E: Y^2 = 4X^3-11X^2+8X\,, \tag{5}$$

an elliptic curve of rank 0 over $\mathbb{Q}$, whose only rational solutions are $(0,0)$, $(1,\pm 1)$, $(2,\pm 2)$. (See [cm], where the same curve occurs in the context of coding theory, and [a], Table 1, curve 14A.) Consequently, the curve (4) has only the rational solutions listed in the theorem. Furthermore, every quadratic polynomial $\sigma(x)$ in $\kappa[x]$ not equivalent to x^2, for which $\Phi_{3,\sigma}(x)$ factors as a product of three irreducible quadratics, gives rise to a solution (X,Y) of (5) with $X\neq 0,1,2$.

THEOREM 2. (a) *If κ is an algebraic number field, then $\Phi_{3,\sigma}(x)$ splits into linear factors for at most finitely many equivalence classes of quadratic polynomials over κ.*

(b) *For any algebraic number field* κ, *the factorization types* $\{6\}$, $\{3,3\}$, $\{1,1,1,3\}$ *occur as the degree sets of the irreducible factors of* $\Phi_{3,\sigma}(x)$ *for infinitely many inequivalent quadratic polynomials.*

(c) *Over an arbitrary field* κ, $\Phi_{3,\sigma}(x)$ *has linear or cubic factors if and only if* $\operatorname{disc}\Phi_{3,\sigma}(x)$ *is a square in* κ; *this holds if and only if* $\sigma(x)$ *is linearly conjugate to* x^2+a, *where* $a=-(s^2+7)/4$ *for some* s *in* κ.

The same result holds for any global field κ whose characteristic is different from 2.

As noted above, Theorems 1 and 2 can be sharpened when the base field is $\kappa=\mathbb{Q}$.

THEOREM 3. *Over* $\mathbb{Q}$, $\Phi_{3,\sigma}(x)$ *never has irreducible quadratic factors and never splits completely*, *when* σ *is a quadratic polynomial. For any quadratic polynomial* σ *over* $\mathbb{Q}$, $\Phi_{3,\sigma}(x)$ *has at least one orbit of roots* (*under* σ) *consisting of algebraic conjugates over* $\mathbb{Q}$. *Moreover*, $\Phi_{3,\sigma}(x)$ *is reducible over* $\mathbb{Q}$ *if and only if* σ *is linearly conjugate to* x^2+a, *where* $a=-(s^2+7)/4$ *for some rational number* s.

Compare this theorem and Theorem 2(b) with Theorem II of Narkiewicz [n], which shows that the factorization type $\{1,1,1,3\}$ does *not* occur for any monic quadratic polynomial $\sigma(x)$ with *integral* coefficients over $\mathbb{Q}$ (or over an imaginary quadratic field with conductor >4).

Over number fields other than $\mathbb{Q}$, $\Phi_{3,\sigma}(x)$ can have quadratic factors. As an example of this take $\kappa=\mathbb{Q}(\sqrt{3})$ and

$$\sigma(x)=x^2-1-\frac{11\sqrt{3}}{24},$$

so that

$$\Phi_{3,\sigma}(x)=\left(x^2+2x+\frac{18-5\sqrt{3}}{24}\right)\left(x^2-\frac{1+\sqrt{3}}{2}x+\frac{12-5\sqrt{3}}{24}\right)\times\left(x^2-\frac{1-\sqrt{3}}{2}x-\frac{18+23\sqrt{3}}{24}\right).$$

This example comes from the solution $(3/2,\ \sqrt{3}/2)$ in $\kappa=\mathbb{Q}(\sqrt{3})$ of equation (5). It is easy to see that the factors of $\Phi_{3,\sigma}(x)$ do not satisfy (3), so that the elements of the two orbits of roots in this example are *not* algebraic conjugates over $\mathbb{Q}(\sqrt{3})$. (In general, a factor f of $\Phi_{n,\sigma}(x)$ can only satisfy (3) if $\deg f$ is divisible by n.)

In fact, there are infinitely many inequivalent polynomials $\sigma(x)$ over $\mathbb{Q}(\sqrt{3})$ for which $\Phi_{3,\sigma}(x)$ factors as a product of quadratics, since the point $(3/2,\sqrt{3}/2)$ has infinite order on (5). (See [si], p. 220, Theorem 7.1.) The same holds for any number field κ (or global field with characteristic $\neq 2$)

over which the rank of the curve (5) is positive (see the remarks following Theorem 5 below).

Another such field is $\mathbb{Q}(\sqrt{17})$, since the point $((7+\sqrt{17})/8, (-1+\sqrt{17})/4)$ on (5) also has infinite order; this point corresponds to the point $((1+\sqrt{17})/2, 2+2\sqrt{17})$ on (4) mentioned in Theorem 1(ii).

We prove Theorems 1 and 2 by studying the polynomial $\Phi_{3,\sigma}(x)$ for $\sigma(x) = x^2 + y$ over the field $\kappa(y)$. This involves no loss of generality since every quadratic polynomial is equivalent over κ (when $\operatorname{char}\kappa \neq 2$) to a polynomial of this form. Thus we let

$$\begin{aligned}(6)\quad f(x,y) = \Phi_{3,\sigma}(x) &= x^6 + x^5 + (3y+1)x^4 + (2y+1)x^3 \\ &\quad + (3y^2+3y+1)x^2 + (y^2+2y+1)x + y^3 + 2y^2 + y + 1 \\ &= y^3 + (2+x+3x^2)y^2 + (1+2x+3x^2+2x^3+3x^4)y \\ &\quad + 1 + x + x^2 + x^3 + x^4 + x^5 + x^6\,,\end{aligned}$$

and define the algebraic function field

$$K = \kappa(x,y)\,, \qquad \text{where} \qquad f(x,y) = 0\,.$$

We show that f is absolutely irreducible over κ (assuming $\operatorname{char}\kappa \neq 2$) and that K has genus 0. More precisely, we have

THEOREM 4. *If* $\operatorname{char}\kappa \neq 2$, *the curve* $f(x,y) = 0$ *is rational, with parameter*

$$(7)\qquad t = 1 + 2y + 2x + 2x^2\,,$$

where

$$(8)\qquad x = \frac{t^3 + t^2 - t + 7}{4(t^2-1)}$$

and

$$(9)\qquad y = -\frac{t^6 - 2t^5 + 11t^4 + 20t^3 + 23t^2 - 18t + 29}{16(t^2-1)^2}\,.$$

(Note: (i) for x and y on the curve (6) the value of t in (7) is never ± 1;

(ii) $t = 0$ gives the polynomial $\sigma(x) = x^2 - 29/16$ in (2);

(iii) Narkiewicz's Theorem II in [n], referred to above, implies that the value of y in (9) is never a rational integer when t is in $\mathbb{Q}$.)

Now let N be the normal closure of $K/\kappa(y)$. The following result holds for N.

THEOREM 5. *If* $\operatorname{char}\kappa \neq 2$, *then the genus* g *of the function field* N *is*

$$g = \begin{cases} 4 & \text{if } \operatorname{char}\kappa \neq 7, \\ 1 & \text{if } \operatorname{char}\kappa = 7. \end{cases}$$

$N = \kappa(t,u)$ has generators t, u (t is the quantity defined in Theorem 4) which satisfy the equation

$$(10)\qquad h(t,u) = (t^2-1)u^3 + (t^3-2t^2-9t+2)u^2 - 9(t^2-1)u - (t^3-2t^2-9t+2) = 0\,.$$

This equation is symmetric in t and u and absolutely irreducible. The Galois group of $N/\kappa(y)$ has order 18:

$$(11)\qquad \mathrm{Gal}(N/\kappa(y)) \cong \mathbb{Z}/3\mathbb{Z} \;\dot{\sim}\; \mathbb{Z}/2\mathbb{Z}\,,$$

the wreath product of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

Theorems 1 and 2 will follow from Theorems 4 and 5 by considering the way the prime divisors of $\kappa(y)$ split in subfields of N. The fact that N has genus 4 whenever κ is a number field, together with Faltings' theorem [fa], will give Theorem 2(a), since every σ for which $\Phi_{3,\sigma}(x)$ splits completely over κ yields a κ-rational point on (10). Theorem 2(b) is an easy consequence of Hilbert's irreducibility theorem.

In Section 3 we show that the only $\mathbb{Q}$-rational solutions of (10) are $(t,u) = (\pm1,\pm1)$, by showing that N has degree 2 over a subfield which is elliptic and computing the $\mathbb{Q}$-rational prime divisors of this elliptic subfield. In fact, there is an automorphism π of $N/\kappa(y)$ which simply switches t and u, and the fixed field N_π of π is elliptic (see §3, Lemma 6):

$$N_\pi = \kappa(X,Y)\,, \qquad \text{where} \qquad Y^2 = 4X^3 - 11X^2 + 8X\,.$$

Thus N_π is defined by the curve (5). This gives another way of looking at Theorem 1. Essentially, $f(x,a)$ factors into a product of quadratics if and only if the numerator divisor of $y-a$ in $\kappa(y)$ lies below a κ-rational prime divisor of N_π which is inert in N/N_π. Moreover, σ induces an automorphism on N_π which corresponds to a translation on the elliptic curve defining N_π by the point $(1,1)$, a point of order 3.

This computation implies that the function field $N/\mathbb{Q}$ has exactly 9 prime divisors with degree 1 over $\mathbb{Q}$ (see §3). We use this fact to complete the proof of Theorem 3.

The second, related, object we investigate is the Galois group of $\Phi_{3,\sigma}(x)$, as $\sigma(x) = x^2+a$ varies over quadratic polynomials in $\kappa[x]$ for which $\Phi_{3,\sigma}(x)$ is irreducible. (If $\Phi_{3,\sigma}(x)$ is reducible over κ its Galois group is either 1, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.) We prove the following result for an arbitrary field κ with $\mathrm{char}\,\kappa \neq 2$ or 7.

THEOREM 6. *Let $\sigma(x) = x^2 + a$, and assume that $\Phi_{3,\sigma}(x)$ is irreducible over κ* ($\mathrm{char}\,\kappa \neq 2$ *or* 7). (*This is equivalent to $a \neq -(s^2+7)/4$ for s in κ and that the conditions of Theorem* 1 *do not hold.*) *Let $\Sigma_{3,\sigma}$ be the splitting*

field of $\Phi_{3,\sigma}(x)$ *over* κ *and* $\Gamma_{3,\sigma} = \mathrm{Gal}(\Sigma_{3,\sigma}/\kappa)$. *Then exactly one of the following situations holds*:

(i) *a is given by*

$$a = \frac{-2z+3}{8} - \frac{w}{8(z-4)} = \frac{-2z^2+11z-12-w}{8(z-4)}\,, \tag{12}$$

where $(z,w) \neq (\infty,\infty)$, $(4,0)$ *is a* κ*-rational point on the elliptic curve*

$$E' : w^2 = 4z^3 - 35z^2 + 120z - 176 = (z-4)(4z^2-19z+44)\,, \tag{13}$$

and $\Gamma_{3,\sigma} \cong \mathbb{Z}/6\mathbb{Z}$;

(ii) *for some value of* $\xi \neq -7, -11$ *in* κ,

$$a = -\frac{\xi^3+29\xi^2+243\xi+559}{16(\xi+7)(\xi+11)} \tag{14}$$

and $\Gamma_{3,\sigma} \cong S_3$;

(iii) *neither* (i) *nor* (ii) *hold and* $\Gamma_{3,\sigma} \cong \mathbb{Z}/3\mathbb{Z} \,\dot{\sim}\, \mathbb{Z}/2\mathbb{Z}$, *the wreath product of* $\mathbb{Z}/3\mathbb{Z}$ *with* $\mathbb{Z}/2\mathbb{Z}$.

Together with equation (6), the conditions of Theorem 6 give three parametrized families of sixth degree polynomials whose Galois groups over κ are the three groups listed above.

THEOREM 7. *Let* κ *be a number field* (*or a global field with characteristic different from* 2 *or* 7).

(a) *For both groups* $\Gamma = S_3$ *and* $\mathbb{Z}/3\mathbb{Z} \,\dot{\sim}\, \mathbb{Z}/2\mathbb{Z}$ *there are infinitely many inequivalent quadratic maps* σ *for which the Galois group of* $\Phi_{3,\sigma}(x)$ *over* κ *is isomorphic to* Γ.

(b) *Let* ϕ *be the isogeny* $\phi : E \to E'$ *from the curve* E *defined by* (5) *to the curve* E' *in* (13), *given by*

$$\phi(X,Y) = \left(\frac{X^3-4X+4}{(X-1)^2},\, Y\frac{X^3-3X^2+4X-4}{(X-1)^3}\right) = (z,w)\,.$$

Let $E(\kappa)$ *denote the group of points on* E *which are defined over* κ.

(i) *If* $\phi(E(\kappa)) = E'(\kappa)$, *then there are no quadratic maps* σ *in* $\kappa[x]$ *for which* $\Gamma_{3,\sigma} \cong \mathbb{Z}/6\mathbb{Z}$;

(ii) *if* $\phi(E(\kappa)) \neq E'(\kappa)$, *and the rank of* $E(\kappa)$ *is zero*, *then there are at most finitely many inequivalent quadratic maps* σ *for which* $\Gamma_{3,\sigma} \cong \mathbb{Z}/6\mathbb{Z}$;

(iii) *if* $\phi(E(\kappa)) \neq E'(\kappa)$, *and the rank of* $E(\kappa)$ *is positive*, *then there are infinitely many inequivalent quadratic maps* σ *for which* $\Gamma_{3,\sigma} \cong \mathbb{Z}/6\mathbb{Z}$.

The curve E' in (13) is 3-isogenous to the curve (5) and has only the $\mathbb{Q}$-rational solutions $(4,0)$, $(5,\pm 7)$, $(12,\pm 56)$ (see curve 14C in Table 1 of [a]). The field $\kappa = \mathbb{Q}$ satisfies condition (b)(ii) of Theorem 7, a fact which leads to part (a) of the following result (see §4).

THEOREM 8. *Let $\sigma(x) = x^2 + a$ be a quadratic polynomial in $\mathbb{Q}[x]$ for which $a \neq -(s^2+7)/4$ for s in $\mathbb{Q}$. Then $\Phi_{3,\sigma}(x)$ is irreducible and the group* $\mathrm{Gal}(\Phi_{3,\sigma}(x)/\mathbb{Q})$ *is*

(a) *the cyclic group $\mathbb{Z}/6\mathbb{Z}$, iff $a = 0, -7/2$;*

(b) *the symmetric group S_3, iff a is given by the formula in* (ii) *of Theorem* 6; *and*

(c) *the full wreath product $\mathbb{Z}/3\mathbb{Z} \dot{\wr} \mathbb{Z}/2\mathbb{Z}$, otherwise.*

Cases (b) *and* (c) *both occur for infinitely many values of a.*

In case (a) of Theorem 8, the two polynomials with cyclic Galois groups over $\mathbb{Q}$ are

$$\Phi_{3,x^2}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \quad \text{(conductor 7)}\,,$$

$$\Phi_{3,x^2-7/2}(x) = x^6 + x^5 - \frac{19}{2}x^4 - 6x^3 + \frac{109}{4}x^2 + \frac{25}{4}x - \frac{167}{8} \quad \text{(conductor 28)}\,.$$

(The last polynomial generates the real subfield of the field of 28th roots of unity.) An example with Galois group S_3 over $\mathbb{Q}$ is

$$\Phi_{3,x^2-1/8}(x) = x^6 + x^5 + \frac{5}{8}x^4 + \frac{3}{4}x^3 + \frac{43}{64}x^2 + \frac{49}{64}x + \frac{463}{512}$$

(corresponding to $\xi = -3$ in (14)), a polynomial with discriminant $-2^{-7} \cdot 3^6 \cdot 13^3$. Almost any choice for σ will give a polynomial with group $\mathbb{Z}/3\mathbb{Z} \dot{\wr} \mathbb{Z}/2\mathbb{Z}$. For example, $\sigma(x) = x^2 + 1$ gives

$$\Phi_{3,x^2+1}(x) = x^6 + x^5 + 4x^4 + 3x^3 + 7x^2 + 4x + 5\,,$$

a polynomial of discriminant $-3^6 \cdot 11^3$.

A field satisfying condition (b)(iii) of Theorem 7 is $\kappa = \mathbb{Q}(\sqrt{-11})$, since the point $(2, 2\sqrt{-11})$ on E' has infinite order and is not in $\phi(E(\kappa))$ (see §4). Thus $\mathbb{Z}/6\mathbb{Z}$ occurs as the Galois group of $\Phi_{3,\sigma}(x)$ over $\mathbb{Q}(\sqrt{-11})$ for infinitely many inequivalent quadratic maps.

I do not know an example of a number field κ satisfying condition (b)(i). Thus the question remains open: are there number fields for which *no* polynomial $\Phi_{3,\sigma}(x)$ has Galois group $\mathbb{Z}/6\mathbb{Z}$? By [si], p. 298, Theorem 4.2, condition (b)(i) holds if and only if the ϕ-Selmer group $S^{(\phi)}(E/\kappa)$ *equals* the Tate–Shafarevich group $Ш(E/\kappa)[\phi]$, i.e. if and only if *no* non-trivial homogeneous space in $S^{(\phi)}$ is globally solvable.

It is very clear by now that the prime 7 plays a special role in the Galois theory of $\Phi_{3,\sigma}(x)$. When the characteristic of κ is 7, N is an elliptic function field, a fact which leads to some interesting connections between the third order periodic points corresponding to *different* quadratic maps! In this case we have the following results. For the proofs of Theorems 9–11, see [m2].

THEOREM 9. *If* $\operatorname{char}\kappa = 7$, *then the field* N *has generators* Z, Δ *satisfying*

$$\Delta^2 = (Z-1)(Z+1)(Z-2)\,, \tag{15}$$

and

$$t, u = \frac{-Z^2}{Z^2-2} \pm \frac{2(Z+2)}{(Z-1)(Z^2-2)}\Delta\,,$$

where t *goes with the upper sign and* u *with the lower. The map* $(x,y) \to (\sigma(x), y)$ *of* $\kappa(x,y)/\kappa(y)$ *is induced by the automorphism*

$$\tau_3 : (t,u) \to \left(\frac{t+3}{-t+1}, \frac{u-3}{u+1}\right)$$

of N, *and* τ_3 *coincides with translation by the point* $-(3,1)$ *on the curve* (15):

$$\tau_3 : (Z,\Delta) \to (Z,\Delta) - (3,1)\,;$$

the point $(3,1)$ *has order* 3 *on* (15).

In the situation of Theorem 9, let P_a be the set of primes of $N\overline{\kappa}/\overline{\kappa}$ which divide the numerator of $y - a$, for a given a in the algebraic closure $\overline{\kappa}$ of κ (where $\operatorname{char}\kappa = 7$). If $a = \infty$, let P_∞ be the set of poles of y in $N\overline{\kappa}/\overline{\kappa}$.

THEOREM 10. (a) *The sets* P_a, *for* $a \neq 0, \infty$, *coincide with the minimal sets* P *of prime divisors of* $N\overline{\kappa}/\overline{\kappa}$ *which do not contain any of the prime divisors of* N *of degree* 1 *over the prime field* $\mathbb{F}_7$ *and which are invariant under the operations*

$$\widetilde{p} \to -\widetilde{p}, \quad \widetilde{p} \to \widetilde{p} + \widetilde{p}_3, \quad \widetilde{p} \to \psi(\widetilde{p}) + \widetilde{p}_1 \qquad (\widetilde{p} \in P)\,. \tag{16}$$

Here ψ *is the automorphism* $\psi : (Z,\Delta) \to (2Z-3, \Delta)$ *of* (15) *and* $\widetilde{p_1}$, $\widetilde{p_3}$ *are the prime divisors corresponding to the points* $(1,0)$ *and* $(3,1)$ *on* (15) (*of orders* 2 *and* 3, *respectively*). *The addition in* (16) *corresponds to the addition of points on* (15).

(b) *For all values* $a \neq 0$ *in* $\overline{\kappa}$, *the map* $\sigma(x) = x^2 + a$ *has periodic points of exact order* 3. *The sets of periodic points* (*of order* 3) *of quadratic maps over* $\overline{\kappa}$ *correspond* 1-1 *to the sets of points* $P = P_a$ *on* (15) *which do not contain points defined over* $\mathbb{F}_7$.

It turns out that there are natural relationships between the sets P_a which arise from the structure of the curve (15), and in particular, from the way $G = \operatorname{Gal}(N\overline{\kappa}/\overline{\kappa}(y))$ sits inside the automorphism group A of $N\overline{\kappa}/\overline{\kappa}$. G is contained in the subgroup $\overline{G}$ of A (of order 72), which is generated by the automorphisms $\psi : (Z,\Delta) \to (2Z-3,\Delta)$ and $\pi : (Z,\Delta) \to (Z,-\Delta)$ of (15), together with the automorphisms τ in A which correspond to translation by points of (15) defined over $\mathbb{F}_7$:

$$\tau : (Z,\Delta) \to (Z,\Delta) - (a,b) \qquad (a,b \in \mathbb{F}_7)\,.$$

Denoting by $\overline{G}P_a$ the set of all images of primes in P_a by elements of $\overline{G}$, the following result holds. To state it let τ_2 be the automorphism corresponding to translation by the point $(2,0)$.

THEOREM 11. *The set* $\overline{G}P_a = \bigcup_{i=1}^4 P_{a_i}$, *where* $a_1 = a$ *and the* a_i *are the roots in* $\overline{\kappa}$ *of the quartic polynomial*

$$\zeta^4 - 2\zeta^3 + 2\zeta^2 - \frac{(a+1)^3(a+2)}{a}\zeta + 2 = 0 \qquad (a \neq 0, \infty)\,.$$

The a_i *may also be determined by the values of* $\{y, \psi(y), \psi^2(y), \tau_2(y)\}$ *modulo a prime divisor* $\widetilde{p}$ *in* P_a, *and are rational expressions in the* Z*-coordinate of the point on* (15) *corresponding to* $\widetilde{p}$ (*see* [m2]). *Moreover, the sets* $\overline{G}P_a$ *can be added*:

$$\overline{G}P_a + \overline{G}P_b = \bigcup_c \overline{G}P_c \qquad \text{for any } a, b \text{ in } \overline{\kappa} \cup \{\infty\}\,,$$

for suitable values c. *In general*, 72 *values of* c *arise in this way from a given pair* a, b.

In addition, $\overline{G}P_0 = \overline{G}P_\infty = P_0 \cup P_\infty$, *and* $\overline{G}P_0 + \overline{G}P_a = \overline{G}P_a$, *for any* a. (*The set* P_∞ *consists of the nine prime divisors whose* Z*-coordinates on* (15) *are* ∞, 0, ± 1, ± 3, *while* P_0 *consists of the three points on* (15) *with* Z*-coordinates* ± 2.)

The results of Theorems 10 and 11 raise the question: are there similar results for arbitrary characteristic which involve the Jacobian variety of the curve (10)?

Finally, the parametrization $\phi(t) = (x(t), y(t))$ of $f(x,y) = 0$ given by (8) and (9) also leads to some interesting insights about the real algebraic curve C defined by f in (6). From Theorem 4 and the discussion in Section 2 (see (17)) follows

THEOREM 12. *The real curve* $C : f(x,y) = 0$ *has three connected components* C_i $(i = 1, 2, 3)$, *which are defined as the images under* $\phi(t) = (x(t), y(t))$ (*see* (8), (9)) *of the respective intervals* $I_1 = (-\infty, -1)$, $I_2 = (-1, 1)$, $I_3 = (1, \infty)$. *These components are cyclically permuted by the map*

$$t \to m(t) = -(t+3)/(t-1)\,.$$

If $\phi(t) \in C_i$, *then* $\phi(m(t)) \in C_{i+1}$ (*subscripts read modulo* 3). *Each of the curves* C_i *is asymptotic to the curve* $y = -x^2$ *as* $t \to \pm\infty, \pm 1$.

The polynomials $\Phi_{3,\sigma}(x)$ can also be used to give an elementary characterization of the cyclic cubic extensions of any field which does *not* contain the cube roots of unity. See [m3].

One remark on notation: prime divisors in the fields $\kappa(y)$, $\kappa(t)$, N, N_π will be denoted respectively by $\mathfrak{p}$, $\overline{p}$, $\widetilde{p}$, q (or $\widetilde{q}$), while p will be used for prime divisors in the field $\kappa(\eta)$ introduced in Section 2.

In further papers I will use similar techniques to consider the possible groups which can occur as the Galois group of an irreducible $\Phi_{n,\sigma}(x)$ of small degree.

I would like to thank Pratiksha Patel for the extensive calculations which suggested the results concerning linear and quadratic factors in Theorem 3 (see [pa]). The work in this paper was partially supported by an NSF grant and the University of Arizona, and partially by a Brachman–Hoffman fellowship from Wellesley College.

2. The function fields K and N. We first verify that $f(x,y) = \Phi_{3,\sigma}(x)$ is irreducible.

LEMMA 1. *If* $\operatorname{char}\kappa \neq 2$, *then* $f(x,y)$ *is irreducible in* $\kappa[x,y]$. *In particular*, $f(x,y)$ *is absolutely irreducible over* κ. *If* $\operatorname{char}\kappa = 2$, *and* κ *contains the finite field of order* 8, *then*

$$f(x,y) = (y + x^2 + x + c)(y + x^2 + x + c^2)(y + x^2 + x + c^4)\,,$$

where $c^3 + c + 1 = 0$.

P r o o f. If f is reducible over κ, then since f is cubic as a polynomial in y and y is integral over $\kappa[x]$, there must be a root of (6) of the form $y = p(x)$, $p(x) \in \kappa[x]$. From (6) it is clear that $p(x)$ can only be quadratic. Putting $y = ax^2 + bx + c$ in for y in $f(x,y)$ then gives

$$\begin{aligned}(ax^2 + bx + c)^3 + (2 + x + 3x^2)(ax^2 + bx + c)^2 \\ +(1 + 2x + 3x^2 + 2x^3 + 3x^4)(ax^2 + bx + c) \\ +1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = 0\,.\end{aligned}$$

Comparing coefficients of x^6 gives $(a+1)^3 = 0$ and so $a = -1$. Considering the constant term gives $c^3 + 2c^2 + c + 1 = 0$. Note that the coefficients of x^4 and x^5 are identically zero on setting $a = -1$, and the coefficients of x^3 and x^2 become

$$\begin{aligned}x^3 &: b^3 + b^2 - b - 1 = (b-1)(b+1)^2 = 0\,,\\ x^2 &: 3b^2c + 2bc + 2b^2 - 4c + 2b + 3c = 0\,.\end{aligned}$$

Putting $b^2 = 1$ in the second equation gives $2(b+1)c = 2(b-1)$, which does hold in characteristic 2 but not otherwise. The statements of the lemma follow.

For the remainder of this section we assume $\operatorname{char}\kappa \neq 2$. By Lemma 1 the function field $K = \kappa(x,y)$ has degree 6 over $\kappa(y)$ and degree 3 over $\kappa(x)$. If we set$t = 1 + 2(y + x + x^2)$,then a straightforward calculation shows that the formulas of Theorem 4 hold. Thus K is rational.

We can verify the formula for y somewhat more elegantly by using properties of the map $\sigma(x) = x^2 + y$. By results of [m1] we know that σ permutes the roots of $f(x, y)$, i.e. if (x, y) satisfies $f(x, y) = 0$, then so does $(x^2 + y, y)$. Furthermore, we know that this map

$$\sigma : (x, y) \to (x^2 + y, y)$$

must be an automorphism of $K/\kappa(y)$ from the fact that $\sigma^3(x) = x$. Hence

$$\sigma^{-1} = \sigma^2 : (x, y) \to ((x^2 + y)^2 + y, y)\,.$$

Now compute the action of σ on t:

$$\sigma(t) = \sigma(1 + 2(y + x + x^2)) = 2y^2 + (4x^2 + 4)y + 2x^4 + 2x^2 + 1\,.$$

A straightforward calculation shows that this last expression equals $\frac{t+3}{1-t}$, and so

$$\sigma(t) = \frac{t+3}{1-t}\,, \qquad \sigma^2(t) = \frac{t-3}{t+1}\,. \tag{17}$$

Since σ has order 3 and fixes $\kappa(y)$, K is cubic over the fixed field F of σ, $K = F(t)$, and $[F : \kappa(y)] = 2$.

Now set

$$\eta = t + \sigma(t) + \sigma^2(t) = (t^3 - 9t)/(t^2 - 1)\,. \tag{18}$$

Then $\eta \in F$, and in terms of x and y we have

$$\begin{aligned}\eta &= t + \frac{t+3}{1-t} + \frac{t-3}{t+1} \\ &= (2y + 2x^2 + 2x + 1) + \{2y^2 + (4x^2 + 4)y + 2x^4 + 2x^2 + 1\} \\ &\quad + \{2y^2 + (4x^2 + 2)y + 2x^4 + 2x + 1\} \\ &= 4\{y^2 + 2(x^2 + 1)y + x^4 + x^2 + x\} + 3\,.\end{aligned}$$

Hence

$$\left(\frac{\eta - 1}{2}\right)^2 = [2y^2 + 4(x^2 + 1)y + 2(x^4 + x^2 + x) + 1]^2 = -4y - 7\,, \tag{19}$$

$$y = \frac{-1}{16}(\eta^2 - 2\eta + 29)\,, \tag{19$'$}$$

and η is quadratic over $\kappa(y)$. It follows that $F = \kappa(y, \eta) = \kappa(\eta)$. Therefore $K = \kappa(t, \eta) = \kappa(t)$ is indeed rational. The formula (9) for y follows easily from (18) and (19′).

Now consider the normal closure N of $K/\kappa(y)$. If x' is a root of $f(x, y)$ in N, not in the σ-orbit of x, then $\kappa(x', y) \cong \kappa(x, y)$ and $N = \kappa(y, x, x')$. To determine a parametrizing variable for $\kappa(x', y)$, note that the conjugate η' of η over $\kappa(y)$ is $\eta' = 2 - \eta$. If π is an automorphism of $N/\kappa(y)$ which takes η to η' then without loss of generality we may take

$$x' = \pi(x)\,, \qquad u = \pi(t)\,. \tag{20}$$

Note that $\pi(x)$ is not in the σ-orbit of x. If it were then it would follow that $\pi(x) = \sigma(x)$ or $\sigma^2(x)$, and π would coincide with one of the maps σ or σ^2 on K, which is not the case since σ fixes $\kappa(\eta)$ and π does not.

It follows that $\kappa(x', y) = \kappa(u)$, where

$$\frac{u^3 - 9u}{u^2 - 1} = 2 - \eta = -\frac{t^3 - 2t^2 - 9t + 2}{t^2 - 1}\,, \tag{21}$$

and the root x' is obtained from u by the formula

$$x' = \frac{u^3 + u^2 - u + 7}{4(u^2 - 1)}\,.$$

From (21) we see that u satisfies the equation

$$u^3 + (\eta - 2)u^2 - 9u + 2 - \eta = 0 \tag{22}$$

which must be irreducible over $\kappa(\eta)$ since the conjugate equation

$$t^3 - \eta t^2 - 9t + \eta = 0\,, \tag{23}$$

being the equation satisfied by t over $\kappa(\eta)$, is irreducible. Putting in the expression for η from (18) gives the equation satisfied by u over $\kappa(t)$:

$$\begin{aligned} h(t,u) = {} & (t^2 - 1)u^3 + (t^3 - 2t^2 - 9t + 2)u^2 \\ & - 9(t^2 - 1)u - (t^3 - 2t^2 - 9t + 2) = 0\,. \end{aligned} \tag{24}$$

We have $N = \kappa(t, u)$, but at the moment it is not clear that u is not contained in $\kappa(t)$, or equivalently, whether t, u generate disjoint extensions over F. To show that this is the case we prove that there is a prime divisor of $\kappa(\eta)$ which ramifies in $\kappa(t)$ but not in $\kappa(u)$. In what follows we use the symbol $\cong$ to denote equality of divisors, as in [h1].

Lemma 2. *If $\eta^2 + 27 \cong a/p_\infty^2$ and $\eta^2 - 4\eta + 31 \cong b/p_\infty^2$ in $\kappa(\eta)$, where p_∞ is the denominator divisor (pole) of η, then the discriminants d_t and d_u of the extensions $\kappa(t)/\kappa(\eta)$ and $\kappa(u)/\kappa(\eta)$ are, respectively,*

$$d_t \cong a^2\,, \qquad d_u \cong b^2\,.$$

Proof. First note that the η-discriminants of the minimal polynomials (23) and (22) of t and u over $\kappa[\eta]$ are

$$\operatorname{disc}(t) = (\eta^2 + 27)^2\,, \qquad \operatorname{disc}(u) = ((2 - \eta)^2 + 27)^2 = (\eta^2 - 4\eta + 31)^2\,.$$

It is easily checked that p_∞ is unramified in $\kappa(t)$ and $\kappa(u)$. For example, setting $t = 1/v$ and $\eta = 1/\beta$ in (23) gives that

$$v^3 - 9\beta v^2 - v + \beta = 0\,,$$

and reducing this equation modulo p_∞ yields

$$v^3 - 9\beta v^2 - v + \beta \equiv v^3 - v \equiv v(v - 1)(v + 1) \pmod{p_\infty}\,,$$

showing that p_∞ splits completely in $\kappa(t)$. The same obviously holds for $\kappa(u)$.

If $\operatorname{char}\kappa \neq 3$, then neither η^2+27 nor $\eta^2-4\eta+31$ has a multiple root in κ, so a and b are either primes of degree 2 in $\kappa(\eta)$ or products of two primes of degree 1. If $\operatorname{char}\kappa = 3$, then the primes dividing $a \cong (p_0)^2$ and $b \cong (p_{-1})^2$ are wildly ramified. In any case d_t and d_u must both have degree 4 in $\kappa(\eta)$ in order for the genus formulae

$$0 = g_{\kappa(t)} = \tfrac{1}{2}\deg d_t - 2\,, \qquad 0 = g_{\kappa(u)} = \tfrac{1}{2}\deg d_u - 2$$

to hold. (See [h1], p. 457.) This proves the lemma.

LEMMA 3. *$\kappa(t)$ and $\kappa(u)$ are linearly disjoint over $F = \kappa(\eta)$.*

Proof. If some prime divisor p of F divides η^2+27 and $\eta^2-4\eta+31$, then p divides the difference $(\eta^2+27)-(\eta^2-4\eta+31) = 4\eta-4$. Hence $\eta-1$ would have to be a common factor of both polynomials. This happens if and only if $\operatorname{char}\kappa = 7$. In that case

$$\eta^2+27 = \eta^2-1 = (\eta+1)(\eta-1)\,,$$
$$\eta^2-4\eta+31 = \eta^2-4\eta+3 = (\eta-3)(\eta-1)\,.$$

Thus even in this case there is a prime divisor which ramifies in $\kappa(t)$ but not in $\kappa(u)$, and vice versa. The statement of the lemma follows.

COROLLARY. *The equation $h(t,u) = 0$ in (24) is irreducible (and therefore absolutely irreducible) in $\kappa[t,u]$, for any field κ whose characteristic is different from 2.*

Lemma 3 implies that $[\kappa(t,u) : \kappa(\eta)] = 9$ and $[N : \kappa(y)] = 18$. Since N is the splitting field of $\Phi_{3,\sigma}(x)$ over $\kappa(y)$, results of [m1] show that $G = \operatorname{Gal}(N/\kappa(y))$ is isomorphic to a subgroup of the wreath product $\mathbb{Z}/3\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. This proves (11), since the latter group has order 18.

We now compute the genus of N. Assume first that $\operatorname{char}\kappa \neq 3, 7$. In this case the ramification for each prime p dividing b must be 3 from $\kappa(t)$ to N, by Lemma 2. Hence the discriminant d_N of $N/\kappa(t)$ is

$$d_N \cong b^2 \qquad \text{in } \kappa(t).$$

Since $\deg_t b = 3\deg_\eta b = 6$, we have

$$g_N = \tfrac{1}{2}\deg d_N - 2 = 4$$

by the Hurwitz genus formula ([h1], p. 457). Note that this is consistent with the fact that the minimal polynomial of u over $\kappa(t)$ is $h(t,u)$ and the discriminant of h as a polynomial in u is

$$\operatorname{disc}_t h(t,u) = 4(t^6-4t^5+13t^4+40t^3+19t^2-36t+31)^2 = 4(d(t))^2\,.$$

Since $\operatorname{disc} d(t) = -2^{34} \cdot 3^9 \cdot 7^2$, $d(t)$ has distinct roots when $\operatorname{char} \kappa \neq 3, 7$ and is irreducible over $\mathbb{Q}$.

If $\operatorname{char} \kappa = 3$ or 7, then $d(t)$ has multiple roots:

$$d(t) \equiv (t^3 + t^2 + 2)^2 \pmod 3,$$
$$d(t) \equiv (t+2)^3(t^3 + 4t^2 + 5t + 3) \pmod 7.$$

If $\operatorname{char} \kappa = 3$, then as above, the prime divisors of $p_{-1} \cong (\eta + 1)p_\infty$ must be wildly ramified in $N/\kappa(t)$. The Dedekind discriminant theorem ([h1], pp. 431, 449) implies that $(p_{-1})^3$ divides d_N. But *only* the primes which divide p_{-1} can be ramified in $N/\kappa(t)$. Since $\deg d_N$ must be even (in $\kappa(t)$), $\deg_t p_{-1} = 3 \deg_\eta p_{-1} = 3$, and prime divisors of p_{-1} are conjugate over $\kappa(\eta)$, we must have $d_N = (p_{-1})^r$ for some $r \geq 4$. But the formula for $\operatorname{disc} h(t, u)$ shows that $\deg_t d_N \leq 12$, so that $\deg_t d_N = 12$ and $g_N = 4$, as before.

If $\operatorname{char} \kappa = 7$, then we have

$$d_t \cong (p_1 p_{-1})^2, \qquad \text{where } p_1 p_{-1}/p_\infty^2 \cong (\eta - 1)(\eta + 1),$$
$$d_u \cong (p_1 p_3)^2, \qquad \text{where } p_1 p_3/p_\infty^2 \cong (\eta - 1)(\eta - 3)$$

in $\kappa(\eta)$. Hence $d_N \cong (p_3)^2 \cdot \overline{p}^a$, for some $a \geq 0$, where $p_1 \cong \overline{p}^3$ in $\kappa(t)$. Note that

$$\eta \equiv 1 \pmod{p_1} \Rightarrow t \equiv -2 \pmod{\overline{p}},$$

by (23). Setting $z = t + 2$ and $zw = u + 2$ in (24) and dividing by z^3 gives

$$0 = h(z - 2, zw - 2)/z^3 = (3 + 3z + z^2)w^3 + (3 + 3zw + z^2w^2).$$

Considering the last equation modulo $\overline{p}$ and using $z \equiv 0 \pmod{\overline{p}}$ gives

$$0 \equiv 3w^3 + 3 \equiv 3(w+1)(w+2)(w+4) \pmod{\overline{p}},$$

so that $\overline{p}$ is unramified in $N/\kappa(t)$. This implies that $d_N \cong (p_3)^2$ and

$$g_N = \tfrac{1}{2} \deg_t d_N - 2 = 3 - 2 = 1.$$

Hence N is an elliptic function field in characteristic 7.

This completes the proof of Theorem 5.

3. The factorization of $f(x, a)$. We will now use the results of Section 2 to investigate the factorization of the polynomial $\Phi_{3,\sigma}(x) = f(x, a)$, when $\sigma(x) = x^2 + a$ for given value of a in κ. To consider the factorization of $f(x, a)$ for a specific value of a we need to look at the corresponding prime divisor $\mathfrak{p}_a$, where

$$y - a \cong \frac{\mathfrak{p}_a}{\mathfrak{p}_\infty} \qquad \text{in } \kappa(y).$$

By Dedekind's classical result (see [h1], p. 288), if $\mathfrak{p}_a$ does not divide $\mathfrak{p}_\infty$ or the discriminant of $f(x, y)$ (considered over $\kappa[y]$), the factors of $f(x, y) \equiv$

$f(x,a)$ modulo $\mathfrak{p}_a$ correspond one-to-one to the prime divisors of $\mathfrak{p}_a$ in the field $\kappa(x,y)=\kappa(t)$. Note that

$$\operatorname{disc}_y f(x,y) = -(4y+7)^3(16y^2+4y+7)^2\,,$$

so we only need to exclude the values $a=-7/4, (-1\pm 3\sqrt{-3})/8$. We also note that to these values correspond the factorizations

$$\Phi_{3,x^2-7/4}(x) = \left(x^3+\frac{1}{2}x^2-\frac{9}{4}x-\frac{1}{8}\right)^2$$

and

$$\Phi_{3,x^2+(-1+3\sqrt{-3})/8}(x) = \left(x+\frac{1-\sqrt{-3}}{4}\right)^3\left(x^3+\frac{1+3\sqrt{-3}}{4}x^2+\frac{-7+9\sqrt{-3}}{8}x-\frac{14+3\sqrt{-3}}{8}\right).$$

The above factors are irreducible over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-3})$, respectively. If either of the above cubics is reducible over κ, they must split completely into linear factors (since their roots make up an orbit of the map σ). For all other values of a in κ, $f(x,a)$ will not have multiple factors.

(i) Quadratic factors and the proof of Theorem 1.First suppose $f(x,a)$ is a product of irreducible quadratic polynomials over κ. Then the three prime divisors $\overline{p}$ of $\mathfrak{p}_a$ in $\kappa(t)$ all have degree 2, so that the residue class field $\kappa(t) \pmod{\overline{p}}$ is a quadratic extension of κ. Moreover, the residue class field of $\kappa(\eta) \pmod{\overline{p}}$ must also have degree 2 over κ since $\kappa(t)/\kappa(\eta)$ is normal and primes in $\kappa(t)$ can only have inertial degree 1 or 3 relative to $\kappa(\eta)$. Thus $\mathfrak{p}_a$ is inert in $\kappa(\eta)/\kappa(y)$ and splits into three primes in $\kappa(t)/\kappa(\eta)$. The relation (19) shows that

$$y\equiv a\,,\qquad \eta\equiv 1\pm 2\sqrt{-4a-7}=1+\sqrt{d}\pmod{\mathfrak{p}_a}\,,$$

where $d=4(-4a-7)$ is not a square in κ.

The fact that $\mathfrak{p}_a$ splits completely in $\kappa(t)/\kappa(\eta)$ implies that the congruence

$$t^3-\eta t^2-9t+\eta\equiv 0 \pmod{\mathfrak{p}_a}$$

must have three distinct roots in $\kappa(\sqrt{d})$ (see (23)). Hence the equation

$$t^3-(1+\sqrt{d})t^2-9t+(1+\sqrt{d})=0 \tag{25}$$

must have roots of the form $\alpha+\beta\sqrt{d}$, where α,β are in κ. Putting $\alpha+\beta\sqrt{d}$ in for t in (25) and setting coefficients of 1, $\sqrt{d}$ equal to 0, we get

$$\begin{aligned}&\alpha^3-\alpha^2-9\alpha+1+d(3\alpha\beta^2-\beta^2-2\alpha\beta)=0\,,\\ &3\alpha^2\beta-2\alpha\beta-\alpha^2-9\beta+1+d(\beta^3-\beta^2)=0\,.\end{aligned} \tag{26}$$

Now multiply through in each equation by the opposite coefficient of d and subtract; this gives, after simplifying and collecting coefficients of β,

$$0 = \beta^3(-4\alpha^3 + 4\alpha^2 + 8\alpha - 4) + \beta^2(4\alpha^3 - 2\alpha^2 - 6\alpha) + \beta(-\alpha^3 + \alpha)\,.$$

If $\beta = 0$, then $\alpha^2 = 1$ and $\alpha^3 = 9\alpha$ by (26), impossible since $\operatorname{char}\kappa \neq 2$. Thus we may divide through by β to obtain

$$0 = Q(\alpha,\beta) = \beta^2(-4\alpha^3+4\alpha^2+8\alpha-4)+\beta(4\alpha^3-2\alpha^2-6\alpha)-\alpha^3+\alpha\,. \tag{27}$$

This equation has the solution β in κ, so either the coefficient of β^2 is zero, in which case α is a solution to

$$\alpha^3 - \alpha^2 - 2\alpha + 1 = 0\,, \tag{28}$$

or the discriminant Δ of $Q(\alpha,\beta)$ must be a square.

First consider (28). To each solution α of (28) there is a unique solution (α,β) of (27), unless the coefficient of β is also zero. But the resultant of the two coefficients (of β and β^2) is

$$R(\alpha^3 - \alpha^2 - 2\alpha + 1, 2\alpha(2\alpha^2 - \alpha - 3)) = 56\,,$$

so both coefficients can be zero only if $\operatorname{char}\kappa = 7$. In this case we also have

$$\alpha^3 - \alpha^2 - 2\alpha + 1 = (\alpha+2)^3 \pmod 7\,,$$

so $\alpha = 2$, and then $Q(\alpha,\beta) = \alpha - \alpha^3 = 2 - 1 = 1 \neq 0$.

If (28) holds and $\operatorname{char}\kappa \neq 7$, then $\beta = (\alpha-1)/(4\alpha-6)$. If $\beta \neq 1$, i.e. $\alpha \neq 5/3$, then d can found from the second equation in (26):

$$d = -\frac{4(2\alpha-3)^2(\alpha^2+3)}{(\alpha-1)(3\alpha-5)} = -\frac{4\cdot 7(\alpha-1)(3\alpha-5)}{(\alpha-1)(3\alpha-5)} = -28\,,$$

since the expression $(2\alpha-3)^2(\alpha^2+3)$ reduces modulo the cubic $\alpha^3-\alpha^2-2\alpha+1$. Note that $d=-28$ also satisfies the first equation in (26) since

$$\alpha^3-\alpha^2-9\alpha+1-28(3\alpha\beta^2-\beta^2-2\alpha\beta) = \frac{4(\alpha^2-3\alpha+4)(\alpha^3-\alpha^2-2\alpha+1)}{(2\alpha-3)^2}\,.$$

As long as -28 is not a square in κ, then for $-28 = 4(-4a-7)$, i.e. $a=0$, $f(x,0)$ will factor into three irreducible quadratics over κ. In the excluded case, if $\alpha = 5/3$ and $\beta = 1$, then from (28) the characteristic of κ must be 13 and $d = 164/9 = -2$. Hence $\alpha = 0 \pmod{13}$, giving the same solution as before. Indeed, we have

$$\begin{aligned} f(x,0) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ &\equiv (x^2+3x+1)(x^2+5x+1)(x^2+6x+1) \pmod{13}\,. \end{aligned}$$

If (28) does not hold then (27) is a quadratic equation and $\operatorname{disc} Q = \Delta$ is a square in κ:

$$\delta^2 = \Delta = 4\alpha^4 - 8\alpha^3 + 4\alpha^2 + 16\alpha = 4\alpha(\alpha+1)(\alpha^2-3\alpha+4)\,; \tag{29}$$

this is the same as equation (4). Note the solutions $(\alpha,\delta)=(0,0)$, $(-1,0)$, both of which lead to $\beta=0$, a case we showed above to be impossible. Also, the solution $(\alpha,\delta)=(1,\pm 4)$ gives $\beta=0$ or 1, both of which are impossible by (26).

Setting $\lambda=1/\alpha+1$ and $\mu=(\lambda-1)^2\delta/2$, (29) becomes

$$\mu^2=\lambda(4\lambda^2-11\lambda+8)\,, \tag{30}$$

which is the equation of an elliptic curve over κ, if the quadratic $4\lambda^2-11\lambda+8$ has distinct roots; this is the case if and only if $\operatorname{char}\kappa\neq 7$ (the discriminant is -7).

The diophantine equation (30) has the solutions $(\lambda,\mu)=(0,0)$, $(1,\pm 1)$, $(2,\pm 2)$ and the solution "at infinity", $(\lambda,\mu)=(\infty,\infty)$. These correspond, respectively, to the solutions

$$\begin{aligned}
&\lambda=0 \;\Rightarrow\; (\alpha,\beta)=(-1,0)\,,\\
&\lambda=1 \;\Rightarrow\; \alpha=\infty\,,\\
&\lambda=2 \;\Rightarrow\; (\alpha,\beta)=(1,0)\text{ or }(1,1)\,,\\
&\lambda=\infty \;\Rightarrow\; (\alpha,\beta)=(0,0)
\end{aligned}$$

of (27).

It follows that a solution to (26) must yield a solution in κ to (29), and hence to (30), other than one of these solutions. Over $\mathbb{Q}$ these are the *only* solutions of (30) (see [cm]). Thus the only rational values of α that give solutions to (29) are $\alpha=0,\pm 1$.

The second equation in (26) gives formula $(4')$ for d in case $\beta\neq 1$. Then both equations in (26) hold and $f(x,a)$ does factor as a product of quadratics when d is not a square in κ.

If $\beta=1$, then (26) and (27) give

$$\alpha=(1\pm\sqrt{17})/2\,,\quad d=(11\pm\sqrt{17})/2\,,$$

and for these values of α we have $\delta=\pm(2\pm 2\sqrt{17})$ in (29). Then from $4(-4a-7)=d$ we get the values$a=-(67\pm\sqrt{17})/32$,for which $f(x,a)$ does indeed factor as a product of quadratics, whenever $\sqrt{17}\in\kappa$ but $\sqrt{d}\notin\kappa$.

This completes the proof of Theorem 1.

(ii) Proof of Theorem 2. For the proof of Theorem 2, note that $f(x,a)$ splits into distinct linear factors over κ if and only if the prime divisor $\mathfrak{p}_a$ in $\kappa(y)$ splits into primes of the first degree in $K=\kappa(t)$, which is the case if and only if $\mathfrak{p}_a$ splits into primes of the first degree in the normal closure N of $\kappa(t)/\kappa(y)$. Thus any a for which $f(x,a)$ splits into linear factors yields a first degree prime divisor of N over κ, i.e. a κ-rational point on the curve (10). In fact, such a point can be obtained from (7) and the

corresponding equation for u, i.e.

$$t = 1 + 2a + 2\beta + 2\beta^2\,, \qquad u = 1 + 2a + 2\beta' + 2(\beta')^2\,,$$

where β, β' are roots of $f(x,a)$ belonging to different orbits under σ. Part (a) of Theorem 2 follows immediately from Faltings' theorem [fa] and the fact that N has genus 4.

To prove part (b), we note that $f(x,a)$ is certainly irreducible for infinitely many values of a in κ, since κ is hilbertian and $f(x,y)$ is irreducible in x and y. (See [fj] or [s], p. 179.) Thus the factorization type $\{6\}$ occurs infinitely often. Furthermore, if $t \neq \pm 1$ is an element of κ, then (9) gives a value for $y = a$ for which $f(x,a)$ has three roots in κ, namely the values x, $\sigma(x)$, and $\sigma^2(x)$, where x is defined by (8). Since $f(x,a)$ can split for at most finitely many values of a in κ, it follows that almost all of these values give the factorization type $\{1,1,1,3\}$.

It remains to show that the factorization type $\{3,3\}$ occurs infinitely often, and to prove part (c). For this we need the following lemma.

LEMMA 4. *Let κ be an arbitrary field with* $\operatorname{char}\kappa \neq 2$. *For a given a in κ, $f(x,a)$ has a cubic factor, irreducible or not, if and only if the discriminant of $f(x,a)$ is a square in κ. In this case $a = -(s^2+7)/4$, for some s in κ. For the polynomial $\sigma(x) = x^2 - \frac{1}{4}(s^2+7)$, $f(x,a) = \Phi_{3,\sigma}(x)$ factors as*

$$\Phi_{3,\sigma}(x) = g(x,s)g(x,-s)\,, \tag{31}$$

where

$$g(x,s) = x^3 + \tfrac{1}{2}(1-s)x^2 - \tfrac{1}{4}(s^2+2s+9)x + \tfrac{1}{8}(s^3+s^2+7s-1)\,. \tag{32}$$

The polynomial $g(x,s)$ is absolutely irreducible over $\kappa[x,s]$.

Proof. If $f(x,a)$ has a cubic factor, then $f(x,a) = g_1 g_2$, where the g_i are cubic and monic. Without loss of generality $f(x,a)$ has no multiple roots. If one of the g_i is irreducible, its roots must be permuted among themselves by σ. Suppose this were not the case, so that for some root α of g_1, $\sigma(\alpha)$ is a root of g_2. Then g_2 is also irreducible since roots of $f(x,a)$ in the same orbit generate the same field over κ. Since g_1 is irreducible, $\sigma(\alpha)$ is a root of g_2 for *all* roots α of g_1. If $\sigma^2(\alpha)$ were a root of g_1, then $\sigma^3(\alpha)$ would be a root of g_2, impossible since $\sigma^3(\alpha) = \alpha$. Hence $\sigma^2(\alpha)$ must be a root of g_2, implying that σ must permute the roots of g_2, and therefore those of g_1, since σ is 1-1 on the roots of $f(x,a)$. This contradiction establishes the claim.

Now it follows that a root of an irreducible g_i generates a cyclic cubic extension of κ, hence that $\operatorname{disc} g_i$ is a square in κ. If both g_i are reducible then they must both have linear factors, and it follows easily that both polynomials factor completely into linear factors. If one is irreducible and one not, then the reducible g_i certainly factors into linear factors. In any

case a reducible g_i has three roots in κ, and its discriminant is a square in κ by definition. Thus in all cases, $\operatorname{disc} g_i$ is a square in κ, whence the same assertion follows for

$$\operatorname{disc} f(x,a) = \operatorname{disc} g_1 g_2 = \operatorname{disc} g_1 \operatorname{disc} g_2 R(g_1,g_2)^2 .$$

Conversely, if $\operatorname{disc} f(x,a) = -(4a+7)^3(16a^2+4a+7)^2$ is a square in κ and $f(x,a)$ does not have multiple roots, then $-4a-7 = s^2$ for some s in κ. If $\operatorname{disc} f(x,a) = 0$, then either $a = (-1 \pm 3\sqrt{-3})/8$ or $-7/4$, both of which have the form $-(s^2+7)/4$. The formula (31) is now easily checked.

The irreducibility of $g(x,s)$ follows from an argument similar to the proof of Lemma 1 in Section 2.

Now we can complete the proof of Theorem 2(b) using (31), (32), and the irreducibility of $g(x,s)$ over $\kappa[x,s]$. Hilbert's irreducibility theorem ([s], p. 179) shows that there are infinitely many values of s in the algebraic number field κ (even in $\mathbb{Z}$) for which $g(x,s)$ and $g(x,-s)$ are simultaneously irreducible over κ. For such s, $f(x,-(s^2+7)/4)$ factors into two irreducible cubics.

In certain algebraic number fields we can give some explicit values of s for which $g(x,s)$ and $g(x,-s)$ are simultaneously irreducible.

LEMMA 5. *Let κ be an algebraic number field in which the prime 2 is unramified and has only first degree prime factors. If $s \equiv 1 \pmod 2$ in κ, then $g(x,s)$ is irreducible over κ.*

Proof. If $g(x)$ is reducible over κ, note that its roots α_1, α_2, α_3 are algebraic integers in κ, since the coefficients of $g(x,s)$ in (32) are algebraic integers. Hence

$$(s^2+s+7)^2 = \operatorname{disc} g(x,s) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$$

implies that each term $\alpha_i - \alpha_j$ is $\equiv 1 \pmod 2$. But this is impossible since$\alpha_1 - \alpha_3 = (\alpha_1-\alpha_2) + (\alpha_2-\alpha_3)$.

(iii) Proof of Theorem 3.Most of the assertions of Theorem 3 follow from what we have already shown. The last assertion is a consequence of Lemma 4 since $\Phi_{3,\sigma}(x)$ is reducible over $\mathbb{Q}$ if and only if it has cubic factors (the factorization type $\{2,2,2\}$ does not occur). The first two assertions will be proved if we show that the factorization type $\{1,1,1,1,1,1\}$ never occurs. To do this we compute the $\mathbb{Q}$-rational prime divisors of the function field $N/\mathbb{Q}$.

We start by determining the fixed field N_π of the automorphism π defined in Section 2. Because the defining equation (24) is symmetric in t and u we may assume π simply switches t and u. We perform the computation for an arbitrary field κ.

LEMMA 6. *The fixed field N_π of π is given by $N_\pi = \kappa(X,Y)$, where*

$$X = \frac{2+\zeta}{\zeta}\,, \qquad Y = \frac{\upsilon(\zeta-2)-(3\zeta+2)}{\zeta^2}\,, \tag{33}$$

with $\zeta = t+u$, $\upsilon = tu$, and

$$Y^2 = 4X^3 - 11X^2 + 8X\,. \tag{34}$$

Thus N_π has genus 1 when $\kappa = \mathbb{Q}$: its $\mathbb{Q}$-rational torsion group consists of the prime divisors corresponding to the solutions $(X,Y) = (\infty,\infty)$, $(0,0)$, $(1,\pm1)$, $(2,\pm2)$ of (34).

P r o o f. First of all, it is clear that $N_\pi = \kappa(\upsilon,\zeta)$ since π simply switches t and u and t and u are the roots of the polynomial $T^2 - \zeta T + \upsilon = 0$ over $\kappa(\upsilon,\zeta)$. To determine the relation between ζ and υ, rewrite (24) in terms of the elementary symmetric polynomials ζ and υ:

$$\upsilon^2(\zeta-2) - \upsilon(6\zeta+4) - (\zeta^3 - 2\zeta^2 - 9\zeta + 2) = 0\,. \tag{35}$$

Multiplying through in this equation by $\zeta - 2$, completing the square and using (33) gives the relation (34). Note that (34) coincides with equation (5), so the last statement of the lemma is a fact we have mentioned already. (A proof is given in [cm].)

Now consider a $\mathbb{Q}$-rational prime divisor $\widetilde{p}$ of $N/\mathbb{Q}$. Then $\widetilde{p}$ lies over a $\mathbb{Q}$-rational prime divisor $\widetilde{q}$ of N_π. From (33) we have

$$\zeta = \frac{2}{X-1}\,, \qquad \upsilon = \frac{\zeta^2 Y + 3\zeta + 2}{\zeta - 2} = \frac{2 - X - X^2 - 2Y}{(X-1)(X-2)}\,. \tag{36}$$

If the divisor $\widetilde{q}$ corresponds to $(X,Y) = (\infty,\infty)$, then $(\zeta,\upsilon) = (0,-1)$, whence $(t,u) = (1,-1)$ or $(-1,1)$. If $\widetilde{q} \leftrightarrow (0,0)$, then $(\zeta,\upsilon) = (-2,1)$ and $(t,u) = (-1,-1)$. If $\widetilde{q} \leftrightarrow (2,-2)$, then $\zeta = 2$ and υ is integral for $\widetilde{q}$. Putting $u = 2 - t$ in (10) gives easily that $(t,u) = (1,1)$. Thus $(0,0)$ and $(2,-2)$ are ramified in N/N_π. For the remaining rational points $\widetilde{q}$ of N_π, corresponding to the solutions $(1,\pm1)$ and $(2,2)$ of (34), at least one of ζ and υ, and therefore at least one of t and u, is non-integral for $\widetilde{q}$. Thus $(t,u) = (\pm1,\pm1)$ are the only rational solutions to equation (10).

As before, if $f(x,a)$ factors into linear factors over $\mathbb{Q}$, then the prime divisor $\mathfrak{p}_a$ ($a \neq \infty$ or $-7/4$) of $\kappa(y)$ splits completely in N, and its prime divisors in N are $\mathbb{Q}$-rational. Furthermore, t and u are integral for these prime divisors $\widetilde{p}$ (cf. (19), (22) and (23)) and modulo $\widetilde{p}$ must, by the last paragraph, give one of the solutions $(\pm1,\pm1)$ of (10). But the parenthetical remark following Theorem 4 shows that this is impossible. This completes the proof of Theorem 3.

This argument shows that all the $\mathbb{Q}$-rational primes of $N/\mathbb{Q}$ must divide $\mathfrak{p}_\infty$. Since $\mathfrak{p}_\infty$ ramifies in $\kappa(\eta)/\kappa(y)$ but splits in $\kappa(t)/\kappa(\eta)$ and $\kappa(u)/\kappa(\eta)$,

it must have ramification index 2 in N and 9 distinct prime divisors, all of degree 1, in N. Hence N has exactly 9 $\mathbb{Q}$-rational prime divisors.

4. The Galois group of $f(x,a)$. In this section we prove Theorem 6 and derive the diophantine conditions which determine what the Galois group of $f(x,a)$ over κ will be for a specific value of a in κ. We begin with the following well-known lemma.

LEMMA 7. *Let $\mathfrak{p}_a$ be the numerator divisor of $y-a$ and $\widetilde{p}$ a prime divisor of $\mathfrak{p}_a$ in N/κ not ramified over $\mathfrak{p}_a$. If G_z is the decomposition group of $\widetilde{p}$ in $G = \mathrm{Gal}(N/\kappa(y))$, then*

$$\mathrm{Gal}(f(x,a)/\kappa) \cong G_z\,.$$

Proof. If $N_{\tilde{p}}$ is the completion of N with respect to the divisor $\widetilde{p}$, then $N_{\tilde{p}}$ is an extension of $\kappa(y)_{\mathfrak{p}_a}$ of degree $f_{\tilde{p}}$ with Galois group G_z. (See [h3], Ch. 1, §3.) If, moreover, $\overline{N}$ and $\overline{\kappa(y)}$ denote the residue class fields of N and $\kappa(y)$ modulo $\widetilde{p}$ and $\mathfrak{p}_a$, respectively, then

$$\mathrm{Gal}(\overline{N}/\overline{\kappa(y)}) \cong \mathrm{Gal}(N_{\tilde{p}}/\kappa(y)_{\mathfrak{p}_a}) \cong G_z\,.$$

(See [h1], pp. 198–199.) But for us $\overline{N}$ is the splitting field of $f(x,a)$ over $\overline{\kappa(y)} = \kappa$, which proves the claim.

In order to make use of this lemma recall the characterization of the fixed field N_z of the group G_z : N_z is the largest extension of $\kappa(y)$ in which the prime divisor lying below $\widetilde{p}$ has degree 1 over $\mathfrak{p}_a$. To determine $\mathrm{Gal}(f(x,a)/\kappa)$ we therefore need to find the maximal subfields N_z of N in which $\mathfrak{p}_a$ has a prime divisor of degree 1. Then $\mathrm{Gal}(N/N_z)$ is the group we want. (Note: the fields N_z will all be conjugate under G, so it does not matter which maximal field N_z we use.)

The next step is to determine generators and genus of each subfield of $N/\kappa(y)$. Denote by H the subgroup of G that fixes $\kappa(\eta)$. Then $H \cong Z_3 \times Z_3$ and we may write the automorphisms in H as (σ^i, σ^j), where the first component acts on t and the second acts on u. For the automorphism π as defined in Section 3(iii), we have

$$G = H\langle\pi\rangle, \qquad G/H \cong \langle\pi\rangle\,, \tag{37}$$

and

$$\pi(\sigma^i, \sigma^j)\pi = (\sigma^j, \sigma^i)\,. \tag{38}$$

Since we are considering only the case in which $f(x,a)$ is irreducible we need to know the subgroups of G which have order divisible by 6. There are five:

$$G, \qquad J_1 = \langle(\sigma, \sigma^{-1}), \pi\rangle \text{ (normal in } G \text{ and isomorphic to } S_3)\,,$$

and the three conjugate subgroups

$$J_2 = \langle(\sigma,\sigma),\pi\rangle, \quad \langle(\sigma,\sigma),(\sigma,\sigma^{-1})\pi\rangle, \quad \langle(\sigma,\sigma),(\sigma^{-1},\sigma)\pi\rangle$$
$$\text{(all isomorphic to } \mathbb{Z}/6\mathbb{Z})\,.$$

We work with J_1 and J_2. Denote the corresponding fixed fields by N_1 and N_2.

LEMMA 8. *Assume the characteristic of* κ *is different from* 2, 3 *or* 7.

(a) *The genus of* N_1 *is* 0. *The fixed field* N_- *of* $\langle(\sigma^{-1},\sigma)\rangle$ *has degree* 2 *over* N_1 *and genus* 2.

(b) *The genus of* N_2 *is* 1. *The fixed field* N_+ *of* $\langle(\sigma,\sigma)\rangle$ *has degree* 2 *over* N_2 *and genus* 2.

Proof. Recall from Sections 2 and 3 that the only primes of $\kappa(y)$ which ramify in N are $\mathfrak{p}_\infty$, $\mathfrak{p}_{-7/4}$ and the prime divisors of $\mathfrak{p}'$, where $\mathfrak{p}'$ is the numerator divisor of $16y^2+4y+7$. (If $\operatorname{char}\kappa \neq 3$, $\mathfrak{p}'$ is either prime or a product of two primes, while if $\operatorname{char}\kappa = 3$, $\mathfrak{p}'$ is a square of a prime.) By (19), $\mathfrak{p}_{-7/4} \cong (p_1)^2$ in $\kappa(\eta)$ and p_1 is unramified in $N/\kappa(\eta)$. The same holds for $\mathfrak{p}_\infty$. Further, $\mathfrak{p}'$ is unramified in $\kappa(\eta)/\kappa(y)$, and it is easy to see that $\mathfrak{p}' \cong ab$, where a and b are the divisors of $\kappa(\eta)$ defined in Lemma 2.

We prove the lemma by considering the ramification of these primes in each of the fields N_*.

(a) N_1 is normal over $\kappa(y)$ of degree 3. Therefore $\mathfrak{p}_\infty$, $\mathfrak{p}_{-7/4}$ are unramified in N_1, but must ramify in N_-/N_1. Hence the prime divisors of $\mathfrak{p}'$ must ramify in N_1, so that the discriminant of $N_1/\kappa(y)$ is $d_1 \cong (\mathfrak{p}')^2$, and the genus of N_1 is

$$g(N_1) = \tfrac{1}{2}\deg(\mathfrak{p}')^2 - 2 = 0\,.$$

By Lemma 2 the ramification indices in $N/\kappa(\eta)$ of the primes dividing a and b in $\kappa(\eta)$ must be 3. Hence none of these primes ramify in N_-/N_1; it follows that the discriminant of N_-/N_1 is $d_- \cong \mathfrak{p}_\infty\mathfrak{p}_{-7/4}$, and $g(N_-) = \frac{1}{2}\deg_{N_1}(\mathfrak{p}_\infty\mathfrak{p}_{-7/4}) - 1 = 2$.

(b) Consider the field N_+ first. N_+ has degree 3 over $\kappa(\eta)$ and is normal over $\kappa(y)$. I claim the prime divisors of a and b are all ramified in $N_+/\kappa(\eta)$. For example, consider a prime divisor p of a in $\kappa(\eta)$. If p were unramified in N_+, it would also be unramified in $N_+\kappa(u) = N$, which is false by Lemma 2. It follows that N/N_+ is unramified and hence that $g(N_+) = 2$ by the relative genus formula for N/N_+ ([h1], p. 462):

$$4 = g(N) = 3g(N_+) + \tfrac{1}{2}\deg_N\delta - 2 = 3g(N_+) - 2\,.$$

(δ is the relative different of N/N_+.) Now the prime divisors of $\mathfrak{p}'$ must all have ramification index 3 in $N_+/\kappa(y)$ and therefore also in $N_2/\kappa(y)$. Furthermore, $\mathfrak{p}_\infty$ and $\mathfrak{p}_{-7/4}$ must ramify in N_2. If not, they are unramified in the normal closure of $N_2/\kappa(y)$, which is N_+, impossible since N_+ contains

$\kappa(\eta)$. On the other hand, a prime divisor of either $\mathfrak{p}_\infty$ or $\mathfrak{p}_{-7/4}$ can only have ramification index 2 in N_2. It follows that the discriminant of $N_2/\kappa(y)$ is $d_2 \cong (\mathfrak{p}')^2\mathfrak{p}_\infty\mathfrak{p}_{-7/4}$, whence

$$g(N_2) = \tfrac{1}{2}\deg(\mathfrak{p}')^2\mathfrak{p}_\infty\mathfrak{p}_{-7/4} - 2 = 1\,.$$

This completes the proof of Lemma 8.

Remarks. 1. The arguments in Lemma 8 imply that both extensions N/N_+ and N/N_- are unramified. This is also clear from the relative genus formula ([h1], p. 462).

2. The conclusions of Lemma 8 are also valid when $\operatorname{char}\kappa = 3$. For N_1, N_2 and N_- this will be clear from the computations which follow (see Lemmas 10 and 11). For N_+ this follows from the first part of the argument in (b).

Now we determine generators for N_2. We first give the action of the automorphism (σ,σ) on the field N_π of Lemma 6, in terms of the elliptic curve (34). For the remainder of this section assume that $\operatorname{char}\kappa \neq 2$ or 7.

Lemma 9. *On N_π the automorphism (σ,σ) coincides with the automorphism τ which corresponds to translation by the point $(1,1)$ on* (34):

$$\begin{aligned}(39)\quad \tau(X,Y) &= (X,Y)+(1,1)\\ &= \left(\frac{2X^2-5X+4-Y}{2(X-1)^2},\ \frac{2X^3-5X^2+X+4+(X-3)Y}{2(X-1)^3}\right).\end{aligned}$$

Proof. That τ is an automorphism of N_π follows from well-known results in the theory of elliptic curves. (See [h2], II. The explicit expressions for $\tau(X)$ and $\tau(Y)$ follow from the addition formula on (34); see [si], pp. 58–59.) Furthermore, (σ,σ) is also an automorphism of N_π since (σ,σ) commutes with π. By means of the equations

$$\begin{aligned}(\sigma,\sigma)(\zeta) &= \frac{t+3}{1-t}+\frac{u+3}{1-u} = \frac{6-2\zeta-2\upsilon}{1-\zeta+\upsilon}\,,\\ (\sigma,\sigma)(\upsilon) &= \frac{t+3}{1-t}\cdot\frac{u+3}{1-u} = \frac{9+3\zeta+\upsilon}{1-\zeta+\upsilon}\,,\end{aligned}$$

and the formulas (33) and (36), a straightforward calculation proves the lemma.

We also note the formula

$$\begin{aligned}(40)\quad (\sigma^{-1},\sigma^{-1})(X,Y) &= \tau^{-1}(X,Y) = (X,Y)-(1,1)\\ &= \left(\frac{2X^2-5X+4+Y}{2(X-1)^2},\ \frac{-2X^3+5X^2-X-4+(X-3)Y}{2(X-1)^3}\right).\end{aligned}$$

Remark. If $\kappa = \mathbb{Q}$, the fact that (σ,σ) and τ have the same fixed field inside N_π can be seen on purely theoretical grounds, without any calculation.

The fixed field of (σ,σ) inside N_π is N_2, a field of genus 1. By Deuring [d] (p. 206, 3.) any subfield of N_π of genus 1 is the fixed field of a group of translation automorphisms of N_π. In our case this group of translation automorphisms must correspond to points of order 3 on (34), which can only be $(1,\pm1)$. The translation automorphisms corresponding to these two points are just τ and τ^{-1}.

Now we can compute N_2. On setting $z=\operatorname{trace}_{N_2}(X)$ and $w=\operatorname{trace}_{N_2}(Y)$, equations (39) and (40) easily give

$$\begin{aligned} z &= \operatorname{trace}_{N_2}(X) = \frac{X^3-4X+4}{(X-1)^2}\,, \\ w &= \operatorname{trace}_{N_2}(Y) = Y\frac{X^3-3X^2+4X-4}{(X-1)^3}\,. \end{aligned} \tag{41}$$

LEMMA 10. (a) *The field $N_2=\kappa(z,w)$, where z and w satisfy*

$$w^2 = 4z^3-35z^2+120z-176 = (z-4)(4z^2-19z+44)\,. \tag{42}$$

(b) *In terms of z and w we have*

$$y = \frac{-2z+3}{8} - \frac{w}{8(z-4)} = \frac{-2z^2+11z-12-w}{8(z-4)}\,, \tag{43}$$

$$z^3+8(y-1)z^2+(16y^2-44y+19)z-(64y^2-48y+20)=0\,. \tag{44}$$

P r o o f. (a) Equation (42) follows easily from (34). That z and w generate N_2 can be seen by a simple degree calculation:

$$[N_\pi:\kappa(z,w)] = [N_\pi:\kappa(X)][\kappa(X):\kappa(z)]/[\kappa(z,w):\kappa(z)] = 6/2 = 3\,.$$

Since z and w lie in N_2 the assertion follows.

(b) From (19′), (17), (21), (39) and (40) we have

$$\begin{aligned} 16y+29 = \eta(2-\eta) &= \left(t\frac{t+3}{1-t}\cdot\frac{t-3}{1+t}\right)\left(u\frac{u+3}{1-u}\cdot\frac{u-3}{u+1}\right) \\ &= \upsilon\cdot(\sigma,\sigma)\upsilon\cdot(\sigma^2,\sigma^2)\upsilon \\ &= \frac{2-X-X^2-2Y}{(X-1)(X-2)}\cdot\frac{-3X+2X^2-(X-2)Y}{X(X-1)} \\ &\quad\times\frac{2-7X+4X^2-XY}{(X-1)(X-2)} \\ &= -\frac{X(X-2)(4X^3-35X^2+54X-19)}{X(X-1)^2(X-2)} \\ &\quad+\frac{2(X-1)(X^2-X+2)Y}{X(X-1)^2(X-2)}\,. \end{aligned} \tag{45}$$

Using (41) gives

$$\begin{aligned}-16y-29 &= \frac{X(X-2)^2(4X^3-35X^2+54X-19)+2w(X-1)^4}{X(X-1)^2(X-2)^2}\\ &= \frac{4X^3-35X^2+54X-19}{(X-1)^2}+\frac{2w(X-1)^2}{X(X-2)^2}\\ &= 4z-35+\frac{2w}{z-4}\,,\end{aligned}$$

from which (43) follows. Finally, equation (42) and the relation $w=(-2z-8y+3)(z-4)$ imply (44).

The fact that N_2 is a subfield of N_π means that the curve (42) is 3-isogenous to (34) ([si], Ch. III, §4). Thus the ranks of the respective groups of κ-rational points on (34) and (42) are the same (when κ is a number field), so that (42) has a finite number of $\mathbb{Q}$-rational solutions. By the Lutz–Nagell theorem ([si], p. 221) the solutions in $\mathbb{Q}$ of (42) are

$$(z,w)=(4,0),\ (5,\pm7),\ (12,\pm56)\,. \tag{46}$$

The $\mathbb{Q}$-rational points of (34) lie above the points $(z,w)=(\infty,\infty)$ and $(4,0)$.

We turn now to the calculation of N_1.

Lemma 11. (a) *The field* $N_1=\kappa(\xi)$, *where*

$$\xi=-\mathrm{trace}_{N_1}\upsilon=\frac{4X^2-17X+22+2Y}{X-2}\,, \tag{47}$$

$$y=-\frac{\xi^3+29\xi^2+243\xi+559}{16(\xi+7)(\xi+11)}\,. \tag{48}$$

(b) *The fixed field* N_- *of* $\langle(\sigma^{-1},\sigma)\rangle$ *is given by* $N_-=\kappa(\xi,\eta)$, *where*

$$\left(2(\xi+7)(\xi+11)\left(\frac{\eta-1}{2}\right)\right)^2=(\xi+7)(\xi+11)(\xi^3+\xi^2-261\xi-1597)\,. \tag{49}$$

Proof. (a) First use (36) to compute the trace of υ to the field N_1:

$$\begin{aligned}\mathrm{trace}_{N_1}\upsilon &= tu+\frac{t+3}{1-t}\cdot\frac{u-3}{u+1}+\frac{t-3}{t+1}\cdot\frac{u+3}{1-u}\\ &= \frac{\upsilon^3-\upsilon\zeta^2-6\zeta^2+45\upsilon-18}{\upsilon^2-\zeta^2+2\upsilon+1}=-\frac{4X^2-17X+22+2Y}{X-2}=-\xi\,.\end{aligned}$$

If o^2 is the pole divisor of X in N_π, and $X-2\cong\frac{q_2q_{-2}}{o^2}$, where $Y\equiv-2\pmod{q_{-2}}$, then the pole divisor of ξ is o^2q_2, so that

$$[N_\pi:\kappa(\xi)]=\deg(o^2q_2)=3\,.$$

This implies that $\kappa(\xi) = N_1$. The expression (48) follows from (45) and (47) by expanding $-16y - 29$ into a continued fraction whose partial quotients are polynomials in ξ.

(b) The assertions of (b) follow from Galois theory and equation (19), which, together with (48), gives

$$\left(\frac{\eta - 1}{2}\right)^2 = -4y - 7 = \frac{\xi^3 + \xi^2 - 261\xi - 1597}{4(\xi + 7)(\xi + 11)}\,.$$

Thus N_- is a hyperelliptic function field.

The κ-rational points on N_π lie above the respective points

$$\begin{aligned}(X, Y) &= (\infty, \infty), (2, 2) \to \xi = \infty\,,\\ (X, Y) &= (0, 0), (1, 1) \to \xi = -11\,,\\ (X, Y) &= (1, -1), (2, -2) \to \xi = -7\,,\end{aligned}$$

of N_1. These points are conjugate under the automorphisms of $N_1/\kappa(y)$, which are

$$(\xi \to \xi), \qquad \left(\xi \to -\frac{11\xi + 93}{\xi + 7}\right) \quad \text{and} \quad \left(\xi \to -\frac{7\xi + 93}{\xi + 11}\right).$$

(i) Proof of Theorem 6.We first note that if $f(x, a) = \Phi_{3,\sigma}(x)$ is irreducible, then by Lemma 7, $\mathfrak{p}_a$ cannot lie below a first degree prime divisor of N_π (or any of the subfields of N conjugate to N_π), N_- or N_+. (N has degree < 6 over each of these fields.) Thus, in the notation of Lemma 7, $G_z = G$, J_1, or one of the groups conjugate to J_2, which we may take to be J_2. If $G_z = J_2$, then $\mathfrak{p}_a$ has a first degree prime divisor in N_2, so part (i) of Theorem 6 follows from Lemma 10 and the fact that y is not integral for the prime divisors of N_2 corresponding to the points (∞, ∞), $(4, 0)$ on (42). If $G_z = J_1$, part (ii) of Theorem 6 follows in the same way from Lemma 11. The final case $G_z = G$ corresponds to part (iii) of Theorem 6.

(ii) Proof of Theorem 7(a).To prove part (a) we need to prove the existence of infinitely many values of a in κ for which $G_z = G$ or J_1. Consider the group G first. From (19′), (44) and (48) the three equations

$$\begin{gathered}\eta^2 - 2\eta + 29 + 16y = 0\,,\\ z^3 + 8(y - 1)z^2 + (16y^2 - 44y + 19)z - (64y^2 - 48y + 20) = 0\,,\\ \xi^3 + 29\xi^2 + 243\xi + 559 + 16y(\xi + 7)(\xi + 11) = 0\,,\end{gathered}$$

are irreducible in η, z and ξ, respectively (and even absolutely irreducible). Thus there are infinitely many values of $y = a$ for which the three equations are simultaneously irreducible over κ, when κ is any global field with characteristic different from 2. For these values of a, there are no κ-rational prime divisors in any of the fields $\kappa(\eta)$, N_2 or N_1 lying above $\mathfrak{p}_a$, since η, z and ξ must be integral for any such prime divisor. It follows that $G_z = G$

for these $\mathfrak{p}_a$, since there can be no κ-rational prime divisors over $\mathfrak{p}_a$ in any overfield of $\kappa(\eta)$, N_2 or N_1, either.

Now consider the group J_1. From (47) and (34) the irreducible equation satisfied by X over the field $\kappa(\xi)$ is

$$16X^3 - (8\xi + 120)X^2 + (\xi^2 + 34\xi + 269)X - 2(\xi^2 + 22\xi + 121) = 0\,.$$

Also, equation (49) shows that $N_- = \kappa(H, \xi)$ with

$$H^2 - (\xi + 7)(\xi + 11)(\xi^3 + \xi^2 - 261\xi - 1597) = 0\,.$$

By Hilbert's irreducibility theorem there are infinitely many values of $\xi \neq -7$, -11, for which both of these equations are irreducible over κ. If for any of these values ξ, q_ξ is the corresponding prime divisor of $\kappa(\xi)$, then q_ξ does not lie below a κ-rational prime divisor of N_π (or any of its conjugate fields), or of N_-. By (48) each of these values of ξ yields a value of $y = a$ in κ for which $G_z = J_1$. This completes the proof of Theorem 7(a).

(iii) Proof of Theorem 7(b).By (41) and (42) a prime divisor q of N_2 of degree 1 (over κ) lies below a prime divisor $\widetilde{q}$ of N_π of degree 1 if and only if the image of the point $\widetilde{Q}$ corresponding to $\widetilde{q}$ on (34) under the isogeny ϕ (defined in Theorem 7) is the point Q corresponding to q on (42). If $\phi(E(\kappa)) = E'(\kappa)$, it follows that J_2 is not the decomposition group of any prime divisor of $\mathfrak{p}_a$ in N. This proves (i). If $\phi(E(\kappa)) \neq E'(\kappa)$, then there are prime divisors q of N_2, of degree 1 over κ, which do not lie below any first degree prime divisor of N_π. This holds for any prime divisor corresponding to a point Q in a non-trivial coset of $E'(\kappa)/\phi(E(\kappa))$, since ϕ is a homomorphism from $E(\kappa)$ to $E'(\kappa)$. If $E(\kappa)$ has rank 0, each of these cosets is finite, and (since $E'(\kappa)$ is also finite) there are at most finitely many first degree prime divisors of N_2. If $E(\kappa)$ has positive rank, each of these cosets is infinite (ϕ has a finite kernel). Furthermore, at most finitely many of the prime divisors corresponding to points in a coset of $E'(\kappa)/\phi(E(\kappa))$ can lie below a first degree prime divisor of N_+, by Faltings' theorem and Lemma 8(b). Lemma 7 now shows that $\mathrm{Gal}(f(x,a)/\kappa) = \mathbb{Z}/6\mathbb{Z}$ for infinitely many distinct values of a in κ. This completes the proof of Theorem 7.

Note that the point $Q = (2, 2\sqrt{-11})$ has infinite order in $E'(\mathbb{Q}(\sqrt{-11}))$, since for example

$$4Q = \left(\frac{-2^3 \cdot 5 \cdot 491}{11 \cdot 29^2}, \frac{2^2 \cdot 7 \cdot 17 \cdot 53 \cdot 883\sqrt{-11}}{11^2 \cdot 29^3}\right).$$

(See Theorem 7.1 on p. 220 of [si].) Furthermore, $Q \neq \phi(\widetilde{Q})$ for any $\widetilde{Q}$ in $E(\mathbb{Q}(\sqrt{-11}))$, since the equation

$$0 = X^3 - 4X + 4 - 2(X-1)^2 = X^3 - 2X^2 + 2\,,$$

obtained by setting $z = 2$ in (41), is irreducible over $\mathbb{Q}(\sqrt{-11})$. (It is Eisenstein for the prime ideal (2) of $\mathbb{Q}(\sqrt{-11})$.) Thus the field $\mathbb{Q}(\sqrt{-11})$ satisfies condition (b)(iii) of Theorem 7, as we claimed in the introduction.

(iv) Proof of Theorem 8. Theorem 8 is a consequence of Theorems 3, 6 and 7, and the fact that (13) has only the rational points listed in (46). For this note that the rational points on (13) other than (∞, ∞) and $(4, 0)$ yield the respective values

$$(5, 7),\ (12, -56) \to y = -7/4\,,$$
$$(5, -7) \to y = 0\,,$$
$$(12, 56) \to y = -7/2\,,$$

for y, by (43). The value $-7/4$ does not work here since $f(x, -7/4)$ is reducible (see §3). Also, $f(x, 0)$ and $f(x, -7/2)$ are irreducible over $\mathbb{Q}$, so Theorem 6(i) implies that both polynomials have the Galois group $\mathbb{Z}/6\mathbb{Z}$.

Finally, note that (14) can represent a value of a of the form $-(s^2+7)/4$ for at most finitely many rational values of ξ. If $a = -(s^2+7)/4$ is given by (14), then $\mathfrak{p}_a$ must have a first degree prime divisor in $\kappa(\eta)$ and in N_1 and therefore (since both fields are normal over $\kappa(y)$) also in the compositum $N_1\kappa(\eta) = N_-$, a field of genus 2.

References

[a] *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer, 1975.

[cm] A. R. Calderbank and P. Morton, *Quasi-symmetric* 3*-designs and elliptic curves*, SIAM J. Discrete Math. 3 (1990), 178–196.

[d] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg 14 (1941), 197–272.

[fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[fj] M. Fried and M. Jarden, *Field Arithmetic*, Ergeb. Math. Grenzgeb. 11, Springer, 1980.

[h1] H. Hasse, *Zahlentheorie*, Akademische Verlagsgesellschaft, Berlin 1969.

[h2] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III*, J. Reine Angew. Math. 175 (1936), 55–62, 69–88, 193–208.

[h3] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg 1967.

[m1] P. Morton and P. Patel, *The Galois theory of periodic points of iterated polynomial maps*, Wellesley College, 1992.

[m2] P. Morton, *Periodic points of quadratic maps in characteristic* 7, Wellesley College, 1992.

[m3] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory, to appear.

[n] W. Narkiewicz, *Polynomial cycles in algebraic number fields*, Colloq. Math. 58 (1989), 151–155.

[o1] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. 51 (1985), 385–414.
[o2] R. W. K. Odoni, *Realising wreath products of cyclic groups as Galois groups*, Mathematika 35 (1988), 101–113.
[pa] P. Patel, *Topics in Computational Galois Theory*, Honors thesis, Wellesley College, 1991.
[s] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, 1982.
[si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer, 1986.
[vh] F. Vivaldi and S. Hatjispyros, *Galois theory of periodic orbits of rational maps*, Nonlinearity 5 (1992), 961–978.

DEPARTMENT OF MATHEMATICS
WELLESLEY COLLEGE
WELLESLEY, MASSACHUSETTS 02181 U.S.A. E-mail: PMORTON@LUCY.WELLESLEY.EDU

Received on 13.9.1991 (2171)