GALOIS GROUPS OF MORI TRINOMIALS AND HYPERELLIPTIC CURVES WITH BIG MONODROMY

YURI G. ZARHIN

Abstract. We compute the Galois groups for a certain class of polynomials over the the field of rational numbers that was introduced by S. Mori and study the monodromy of corresponding hyperelliptic jacobians.

1. Mori polynomials, their reductions and Galois groups

We write $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ for the ring of integers, the field of rational numbers and the field of complex numbers respectively. If a and b are nonzero integers then we write (a, b) for its (positive) greatest common divisor. If ℓ is a prime then $\mathbb{F}_\ell, \mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$ stand for the prime finite field of characteristic ℓ, the ring of ℓ-adic integers and the field of ℓ-adic numbers respectively. If A and B are nonzero integers then we write (A, B) for its greatest (positive) common divisor.

We consider the subring $\mathbb{Z}\left[\frac{1}{2}\right] \subset \mathbb{Q}$ generated by $1/2$ over $\mathbb{Z}$. We have

$$\mathbb{Z} \subset \mathbb{Z}\left[\frac{1}{2}\right] \subset \mathbb{Q}.$$

If ℓ is an odd prime then the principal ideal $\ell\mathbb{Z}\left[\frac{1}{2}\right]$ is maximal in $\mathbb{Z}\left[\frac{1}{2}\right]$ and

$$\mathbb{Z}\left[\frac{1}{2}\right]/\ell\mathbb{Z}\left[\frac{1}{2}\right] = \mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_\ell.$$

If K is a field then we write $\bar{K}$ for its algebraic closure and denote by $\mathrm{Gal}(K)$ its absolute Galois group $\mathrm{Aut}(\bar{K}/K)$. If $u(x) \in K[x]$ is a degree n polynomial with coefficients in K and without multiple roots then we write $\mathfrak{R}_u \subset \bar{K}$ for the n-element set of its roots, $K(\mathfrak{R}_u)$ the splitting field of $u(x)$ and $\mathrm{Gal}(u/K) = \mathrm{Gal}(K(\mathfrak{R}_u)/K)$ the Galois group of $u(x)$ viewed as a certain subgroup of the group $\mathrm{Perm}(\mathfrak{R}_u) \cong \mathbf{S}_n$ of permutations of $\mathfrak{R}_u$. As usual, we write $\mathbf{A}_n$ for the *alternating group*, which is the only index 2 subgroup in the *full symmetric group* $\mathbf{S}_n$.

1.1 (**Discriminants and alternating groups**). We write $\Delta(u)$ for the discriminant of u. We have

$$0 \ne \Delta(u) \in K, \ \sqrt{\Delta(u)} \in K(\mathfrak{R}_u).$$

It is well known that

$$\mathrm{Gal}(K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})) = \mathrm{Gal}(K(\mathfrak{R}_u)/K) \bigcap \mathbf{A}_n \subset \mathbf{A}_n \subset \mathbf{S}_n = \mathrm{Perm}(\mathfrak{R}_u).$$

In particular, the permutation (sub)group $\mathrm{Gal}(K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)}))$ does *not* contain transpositions; $\Delta(u)$ is a *square* in K if and only if $\mathrm{Gal}(u/K)$ lies in the

2010 *Mathematics Subject Classification.* 14H40, 14K05, 11G30, 11G10.

This work was partially supported by a grant from the Simons Foundation (#246625 to Yuri Zarkhin).

alternating (sub)group $\mathbf{A}_n \subset \mathbf{S}_n$. On the other hand, if $\mathrm{Gal}(u/K) = \mathbf{S}_n$ then $\mathrm{Gal}(K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})) = \mathbf{A}_n$.

If n is odd and $\mathrm{char}(K) \ne 2$ then we write C_u for the genus $\frac{n-1}{2}$ hyperelliptic curve

$$C_u : y^2 = u(x)$$

and $J(C_u)$ for its jacobian, which is a $\frac{n-1}{2}$-dimensional abelian variety over K. We write $\mathrm{End}(J(C_u))$ for the ring of all $\bar{K}$-endomorphisms of $J(C_u)$ and $\mathrm{End}_K(J(C_u))$ for the (sub)ring of all its K-endomorphisms. We have

$$\mathbb{Z} \subset \mathrm{End}_K(J(C_u)) \subset \mathrm{End}(J(C_u)).$$

About forty years ago S. Mori [8, Prop. 3 on p. 107] observed that if $n = 2g+1$ is odd and $\mathrm{Gal}(f/K)$ is a *doubly transitive* permutation group then $\mathrm{End}_K(J(C_u)) = \mathbb{Z}$. He constructed [8, Th. 1 on p. 105] explicit examples (in all dimensions g) of polynomials (actually, trinomials) $f(x)$ over $\mathbb{Q}$ such that $\mathrm{Gal}(f/\mathbb{Q})$ is doubly transitive and $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

On the other hand, about fifteen years ago the following assertion was proven by the author [17].

Theorem 1.2. *Suppose that* $\mathrm{char}(K) = 0$ *and* $\mathrm{Gal}(u/K) = \mathbf{S}_n$. *Then*

$$\mathrm{End}(J(C_u)) = \mathbb{Z}.$$

The aim of this note is to prove that in Mori's examples $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_{2g+1}$. This gives another proof of the theorem of Mori [8, Th. 1 on p. 105]. Actually, we extend the class of Mori trinomials with $\mathrm{End}(J(C_f)) = \mathbb{Z}$, by dropping one of the congruence conditions imposed by Mori on the coefficients of $f(x)$. We also prove that the images of $\mathrm{Gal}(\mathbb{Q})$ in the automorphism groups of Tate modules of $J(C_f)$ are *almost* as large as possible.

1.3 (**Mori trinomials).** Throughout this paper, g, p, b, c *are integers that enjoy the following properties* [8].

(i) *The number* g *is a positive integer and* p *is an odd prime. In addition, there is a positive integer* N *such that* $(\frac{p-1}{2})^N$ *is divisible by* g. This means that every *prime* divisor of g is also a divisor of $\frac{p-1}{2}$. This implies that

$$(p, g) = (p, 2g) = 1.$$

It follows that if g is *even* then p is congruent to 1 modulo 4.

(ii) *The residue* b mod p *is a primitive root of* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; in particular, $(b, p) = 1$.

(iii) *The integer* c *is odd and*

$$(b, c) = (b, 2g+1) = (c, g) = 1.$$

This implies that $(c, 2g) = 1$.

S. Mori [8] introduced and studied the monic degree $(2g+1)$ polynomial

$$f(x) = f_{g,p,b,c}(x) := x^{2g+1} - bx - \frac{pc}{4} \in \mathbb{Z}\left[\frac{1}{2}\right][x] \subset \mathbb{Q}[x],$$

which we call a *Mori trinomial*. He proved the following results [8, pp. 106–107].

Theorem 1.4 (Theorem of Mori). *Let* $f(x) = f_{g,p,b,c}(x)$ *be a Mori trinomial. Then:*

(i) *The polynomial $f(x)$ is irreducible over $\mathbb{Q}_2$ and therefore over $\mathbb{Q}$.*
(ii) *The polynomial $f(x) \bmod p \in \mathbb{F}_p[x]$ is a product $x(x^{2g}-b)$ of a linear factor x and an irreducible (over $\mathbb{F}_p$) degree $2g$ polynomial $x^{2g}-b$.*
(iii) *Let $\mathrm{Gal}(f)$ be the Galois group of $f(x)$ over $\mathbb{Q}$ considered canonically as a (transitive) subgroup of the full symmetric group $\mathbf{S}_{2g+1}$. Then $\mathrm{Gal}(f)$ is a doubly transitive permutation group. More precisely, the transitive $\mathrm{Gal}(f)$ contains a permutation σ that is a cycle of length $2g$.*
(iv) *For each odd prime ℓ every root of the polynomial $f(x) \bmod \ell \in \mathbb{F}_\ell[x]$ is either simple or double.*
(v) *Let us consider the genus g hyperelliptic curve*

$$C_f : y^2 = f(x)$$

and its jacobian $J(C_f)$, which is a g-dimensional abelian variety over $\mathbb{Q}$. Assume additionally that c is congruent to $-p$ modulo 4.

Then C_f is a stable curve over $\mathbb{Z}$ and $J(C_f)$ has everywhere semistable reduction over $\mathbb{Z}$. In addition, $\mathrm{End}(J(C_f) = \mathbb{Z}$.

Remarks 1.5. (1) The 2-adic Newton polygon of Mori trinomial $f(x)$ consists of one *segment* that connects $(0,-2)$ and $(2g+1,0)$, which are its only integer points. Now the irreducibility of $f(x)$ follows from Eisenstein–Dumas Criterion [9, Cor. 3.6 on p. 316], [4, p. 502]. It also follows that the field extension $\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}$ is *ramified* at 2.
(2) If $g=1$ then $2g+1=3$ and the only doubly transitive subgroup of $\mathbf{S}_3$ is $\mathbf{S}_3$ itself. Concerning the double transitivity of the Galois group of trinomials of arbitrary degree, see [2, Th. 4.2 on p. 9 and Note 2 on p. 10].
(3) The additional congruence condition in Theorem 1.4(v) guarantees that C_f has stable (even good) reduction at 2 [8, p. 106]. Mori's proof of the last assertion of Theorem 1.4(v) is based on results of [12] and the equality $\mathrm{End}_{\mathbb{Q}}(J(C_f)) = \mathbb{Z}$; the latter follows from the double transitivity of Galois groups of Mori trinomials.

Remark 1.6. Since a cycle of *even* length $2g$ is an *odd* permutation, it follows from Theorem 1.4(iii) that $\mathrm{Gal}(f)$ is *not* contained in $\mathbf{A}_{2g+1}$. In other words, $\Delta(f)$ is *not* a square in $\mathbb{Q}$.

Our first main result is the following statement.

Theorem 1.7. *Let $f(x) = f_{g,p,b,c}(x)$ be a Mori trinomial.*
(i) *If ℓ is an odd prime then the polynomial $f(x) \bmod \ell \in \mathbb{F}_\ell[x]$ has, at most, one double root and this root (if exists) lies in $\mathbb{F}_\ell$.*
(ii) *There exists an odd prime $\ell \ne p$ that $f(x) \bmod \ell \in \mathbb{F}_\ell[x]$ has a double root $\bar{\alpha} \in \mathbb{F}_\ell$. All other roots of $f(x) \bmod \ell$ (in an algebraic closure of $\mathbb{F}_\ell$) are simple.*
(iii) *The Galois group $\mathrm{Gal}(f)$ of $f(x)$ over $\mathbb{Q}$ coincides with the full symmetric group $\mathbf{S}_{2g+1}$. The Galois (sub)group $\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}(\sqrt{\Delta(f)}))$ coincides with the alternating group $\mathbf{A}_{2g+1}$.*
(iiibis) *The Galois extension $\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}(\sqrt{\Delta(f)})$ is ramified at all prime divisors of 2. It is unramified at all prime divisors of every odd prime ℓ.*
(iv) *Suppose that $g>1$. Then $\mathrm{End}(J(C_f)) = \mathbb{Z}$.*

Remark 1.8. Theorem 1.7(iv) was proven by S. Mori under an additional assumption that c is congruent to $-p$ modulo 4 (see Theorem 1.4(v) above).

Remark 1.9. Thanks to Theorem 1.2, Theorem 1.7(iv) follows readily from Theorem 1.7(iii).

Remark 1.10. Let $g > 1$ and suppose we know that $\mathrm{Gal}(f)$ contains a transposition. Now the double transitivity implies that $\mathrm{Gal}(f)$ coincides with $\mathbf{S}_{2g+1}$ (see [15, Lemma 4.4.3 on p. 40]).

Let K be a field of characteristic zero and $u(x) \in K[x]$ be a degree $2g+1$ polynomial without multiple roots. Then the jacobian $J(C_u)$ is a g-dimensional abelian variety over K. For every prime ℓ let $T_\ell(J(C_u))$ be the ℓ-adic Tate module of $J(C_u)$, which is a free $\mathbb{Z}_\ell$-module of rank $2g$ provided with the canonical continuous action

$$\rho_{\ell,u} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J(C_u)))$$

of $\mathrm{Gal}(\mathbb{Q})$ [10, 14, 20]. There is a *Riemann form*

$$e_\ell : T_\ell(J(C_u)) \times T_\ell(J(C_u)) \to \mathbb{Z}_\ell$$

that corresponds to the canonical principal polarization on $J(C_u)$ ([10, Sect. 20], [21, Sect. 1]) and is a nondegenerate (even perfect) alternating $\mathbb{Z}_\ell$-bilinear form that satisfies

$$e_\ell(\sigma(x), \sigma(y)) = \chi_\ell(\sigma) e_\ell(\sigma(x), \sigma(y)).$$

This implies that the image

$$\rho_{\ell,u}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J(C_u)))$$

lies in the (sub)group

$$\mathrm{Gp}(T_\ell(J(C_u)), e_\ell) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J(C_u)))$$

of symplectic similitudes of e_ℓ [18, 19, 21].

Using results of Chris Hall [5] and the author [21], we deduce from Theorem 1.7 the following statement. (Compare it with [18, Th. 2.5] and [19, Th. 8.3].)

Theorem 1.11. *Let $K = \mathbb{Q}$ and $f(x) = f_{g,p,b,c}(x) \in \mathbb{Q}[x]$ be a Mori trinomial. Suppose that $g > 1$.*

Then:

(i) *for all primes ℓ the image $\rho_{\ell,f}(\mathrm{Gal}(\mathbb{Q}))$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(J(C_f)), e_\ell)$.*

ii *Let L be a number field and $\mathrm{Gal}(L)$ be its absolute Galois group, which we view as an open subgroup of finite index in $\mathrm{Gal}(\mathbb{Q})$. Then for all but finitely many primes ℓ the image $\rho_{\ell,f}(\mathrm{Gal}(L))$ coincides with $\mathrm{Gp}(T_\ell(J(C_f)), e_\ell)$.*

The paper is organized as follows. In Section 2 we deduce Theorem 1.11 from Theorem 1.7. In Section 3 we discuss a certain class of trinomials that is related to Mori polynomials. Section 4 deals with discriminants of Mori polynomials. We prove Theorem 1.7 in Section 5.

Acknowledgements. This work was started during my stay at the Max-Planck-Institut für Mathematik (Bonn, Germany) in September of 2013 and finished during the academic year 2013/2014 when I was Erna and Jakob Michael Visiting Professor in the Department of Mathematics at the Weizmann Institute of Science (Rehovot, Israel): the hospitality and support of both Institutes are gratefully acknowledged.

I am grateful to the referee, whose comments helped to improve the exposition.

2. Monodromy of hyperelliptic jacobians

Proof of Theorem 1.11 (modulo Theorem 1.7). By Theorem 1.7(iii), $\mathrm{Gal}(f/\mathbb{Q})$ coincides with the full symmetric group $\mathbf{S}_{2g+1}$. By Theorem 1.7(iv), $\mathrm{End}(J(C_f)) = \mathbb{Z}$. It follows from Theorem 1.7(i) that there is an odd prime ℓ such that $J(C_f)$ has at ℓ a semistable reduction with *toric dimension* 1 [5]. Now the assertion (i) follows from [21, Th. 4.3]. The assertion (ii) follows from [5, Th. 1]. □

3. Reduction of certain trinomials

In order to prove Theorem 1.7(i), we will use the following elementary statement that was inspired by [15, Remark 2 on p. 42] and [8, p. 106]

Lemma 3.1 (Key Lemma). *Let*

$$u(x) = u_{n,B,C}(x) := x^n + Bx + C \in \mathbb{Z}[x]$$

be a monic polynomial of degree $n > 1$ such that $B \neq 0$ and $C \neq 0$.

(1) *If $u(x)$ has a multiple root then n divides B and $(n-1)$ divides C.*
(2) *Let ℓ be a prime that enjoys the following properties.*
   (i) *(B, C) is not divisible by ℓ.*
   (ii) *(n, B) is not divisible by ℓ.*
   (iii) *$(n-1, C)$ is not divisible by ℓ.*

   Suppose that $u(x)$ has no multiple roots. Let us consider the polynomial

$$\bar{u}(x) := u(x) \bmod \ell \in \mathbb{F}_\ell[x].$$

   Then:
   (a) *$\bar{u}(x)$ has, at most, one multiple root in an algebraic closure of $\mathbb{F}_\ell$.*
   (b) *If such a multiple root say, γ, does exist, then ℓ does not divide $n(n-1)BC$ and γ is a double root of $\bar{u}(x)$. In addition, γ is a nonzero element of $\mathbb{F}_\ell$.*
   (c) *If such a multiple root does exist then either the field extension $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}$ is unramified at ℓ or a corresponding inertia subgroup at ℓ in*

$$\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}) = \mathrm{Gal}(u/\mathbb{Q}) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

   is generated by a transposition. In both cases the Galois extension $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}(\sqrt{\Delta(u)})$ is unramified at all prime divisors of ℓ.

Remark 3.2. The discriminant

$$\mathrm{Discr}(n, B, C) := \Delta(u_{n,B,C})$$

of $u_{n,B,C}(x)$ is given by the formula

$$\mathrm{Discr}(n, B, C) = (-1)^{n(n-1)/2} n^n C^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} B^n$$

[3, Ex. 834].

Remark 3.3. In the notation of Lemma 3.1, assume that $\bar{u}(x)$ has *no* multiple roots, i.e., $\Delta(u)$ is *not* divisible by ℓ. Then obviously $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}$ is *unramified* at ℓ. This implies that $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}(\sqrt{\Delta(u)})$ is *unramified* at all prime divisors of ℓ.

Proof of Lemma 3.1. Proof of (1). Since $u(x)$ has a multiple root, its discriminant

$$\Delta(u) = (-1)^{n(n-1)/2} n^n C^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} B^n = 0.$$

This implies that

$$n^n C^{n-1} = \pm (n-1)^{n-1} B^n.$$

Since n and $(n-1)$ are relatively prime, $n^n \mid B^n$ and $(n-1)^{n-1} \mid C^{n-1}$. This implies that $n \mid B$ and $(n-1) \mid C$.

Proof of (2). We have

$$\bar{u}(x) := x^n + \bar{B}x + \bar{C} \in \mathbb{F}_\ell[x]$$

where

$$\bar{B} = B \bmod \ell \in \mathbb{F}_\ell, \ \bar{C} = C \bmod \ell \in \mathbb{F}_\ell.$$

The condition (i) implies that either $\bar{B} \ne 0$ or $\bar{C} \ne 0$. The condition (ii) implies that if $\bar{B} = 0$ then $n \ne 0$ in $\mathbb{F}_\ell$. The condition (iii) implies that if $(n-1) = 0$ in $\mathbb{F}_\ell$ then $\bar{C} \ne 0$ and $n \ne 0$ in $\mathbb{F}_\ell$. We have

$$\Delta(\bar{u}) = (-1)^{n(n-1)/2} n^n \bar{C}^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} \bar{B}^n = 0$$

and therefore

$$n^n \bar{C}^{n-1} = \pm (n-1)^{n-1} \bar{B}^n. \tag{1}$$

This implies that if $(n-1) = 0$ in $\mathbb{F}_\ell$ then $\bar{C} = 0$, which is not the case. This proves that $(n-1) \ne 0$ in $\mathbb{F}_\ell$. On the other hand, if $\bar{B} = 0$ then $\bar{C} \ne 0$ and $n \ne 0$ in $\mathbb{F}_\ell$. Then (1) implies that $\bar{C} = 0$ and we get a contradiction that proves that $\bar{B} \ne 0$. If $n = 0$ in $\mathbb{F}_\ell$ then $n - 1 \ne 0$ in $\mathbb{F}_\ell$ and formula 1 implies that $\bar{B} = 0$, which is not the case. The obtained contradiction proves that $n \ne 0$ in $\mathbb{F}_\ell$. If $\bar{C} = 0$ then formula (1) implies that $\bar{B} = 0$, which is not the case. This proves that ℓ does *not* divide $n(n-1)BC$.

The derivative of $\bar{u}(x)$ is

$$\bar{u}'(x) = nx^{n-1} + \bar{B}.$$

We have

$$x \cdot \bar{u}'(x) - n \cdot \bar{u}(x) = -(n-1)\bar{B}x - n\bar{C}. \tag{2}$$

Suppose $\bar{u}(x)$ has a multiple root γ in an algebraic closure of $\mathbb{F}_\ell$. Then

$$\bar{u}(\gamma) = 0, \ \bar{u}'(\gamma) = 0, \ n \cdot \gamma \cdot \bar{u}'(\gamma) - n \cdot \bar{u}(\gamma) = 0.$$

Using formula (2), we conclude that

$$0 = \gamma \cdot \bar{u}'(\gamma) - n \cdot \bar{u}(\gamma) = -(n-1)\bar{B}\gamma - n\bar{C}, \ \gamma = -\frac{n\bar{C}}{(n-1)\bar{B}} \in \mathbb{F}_\ell.$$

This implies that $\gamma \ne 0$.

Notice that the second derivative $\bar{u}''(x) = n(n-1)x^{n-2}$. This implies that

$$\bar{u}''(\gamma) = n(n-1)\gamma^{n-2} \ne 0.$$

It follows that γ is a *double* root of $\bar{u}(x)$. This ends the proof of (a) and (b).

In order to prove (c), notice that there exists a monic degree $(n-2)$ polynomial $\bar{h}(x) \in \mathbb{F}_\ell[x]$ such that

$$\bar{u}(x) = (x-\gamma)^2 \cdot \bar{h}(x).$$

Clearly, γ is *not* a root of $\bar{h}(x)$ and therefore $\bar{h}(x)$ has no multiple roots and relatively prime to $(x-\gamma)^2$.[1] By Hensel's Lemma, there exist monic polynomials

$$h(x), v(x) \in \mathbb{Z}_\ell[x], \ \deg(h) = n-2, \deg(v) = 2$$

[1] Compare with [11, Lemma 1 on p. 231].

such that

$$u(x) = v(x)h(x)$$

and

$$\bar{h}(x) = h(x) \bmod \ell, \ (x-\gamma)^2 = v(x) \bmod \ell.$$

This implies that the splitting field $\mathbb{Q}_\ell(\mathfrak{R}_h)$ of $h(x)$ (over $\mathbb{Q}_\ell$) is an unramified extension of $\mathbb{Q}_\ell$ while the splitting field $\mathbb{Q}_\ell(\mathfrak{R}_u)$ of $u(x)$ (over $\mathbb{Q}_\ell$) is obtained from $\mathbb{Q}_\ell(\mathfrak{R}_h)$ by adjoining to it two (distinct) roots say, α_1 and α_2 of quadratic $v(x)$. Clearly, $\mathbb{Q}_\ell(\mathfrak{R}_u)$ either coincides with $\mathbb{Q}_\ell(\mathfrak{R}_h)$ or with a certain quadratic extension of $\mathbb{Q}_\ell(\mathfrak{R}_h)$, ramified or unramified. It follows that the inertia subgroup I of

$$\mathrm{Gal}(\mathbb{Q}_\ell(\mathfrak{R}_u)/\mathbb{Q}_\ell) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

is either trivial or is generated by the *transposition* that permutes α_1 and α_2 (and leaves invariant every root of $h(x)$). In the former case $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}$ is unramified at ℓ while in the latter one an inertia subgroup in

$$\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

that corresponds to ℓ is generated by a transposition. However, the permutation subgroup $\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}(\sqrt{\Delta(u)}))$ does not contain transpositions (see Sect. 1.1). This implies that $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}(\sqrt{\Delta(u)})$ is *unramified* at all prime divisors of ℓ. □

Example 3.4. Let us consider the polynomial

$$u(x) = u_{n,-1,-1}(x) = x^n - x - 1 \in \mathbb{Q}[x]$$

over the field $K = \mathbb{Q}$. Here $B = C = -1$ and the conditions of Lemma 3.1 hold for all primes ℓ. It is known that $u(x)$ is irreducible [13], its Galois group over $\mathbb{Q}$ is $\mathbf{S}_n$ [11, Cor. 3 on p. 233] and there exists a prime ℓ such that $u(x) \bmod \ell$ acquires a multiple root [15, Remark 2 on p. 42]. Clearly, the discriminant $\Delta(u) = \mathrm{Discr}(n,-1,-1)$ of $u(x)$ is an *odd* integer and therefore such an ℓ is *odd*. It follows from Lemma 3.1 that $u(x) \bmod \ell$ has exactly one multiple root and its multiplicity is 2.

Let $n = 2g+1$ be an odd integer ≥ 5 and

$$u(x) = u_{2g+1,-1,-1}(x) = x^{2g+1} - x - 1 \in \mathbb{Q}[x].$$

Let us consider the g-dimensional jacobian $J(C_u)$ of the hyperelliptic curve $C_u : y^2 = x^{2g+1} - x - 1$. Since $\mathrm{Gal}(u/\mathbb{Q}) = \mathbf{S}_{2g+1}$, Theorem 1.2 tells us that $\mathrm{End}(J(C_u)) = \mathbb{Z}$. Now the same arguments as in Section 2 prove that:

(i) For all primes ℓ the image

$$\rho_{\ell,u}(\mathrm{Gal}(\mathbb{Q})) \subset \mathrm{Gp}(T_\ell(J(C_u)), e_\ell)$$

is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(J(C_u)), e_\ell)$.

(ii) Let L be a number field and $\mathrm{Gal}(L)$ be its absolute Galois group, which we view as an open subgroup of finite index in $\mathrm{Gal}(\mathbb{Q})$. Then for all but finitely many primes ℓ the image

$$\rho_{\ell,u}(\mathrm{Gal}(L)) \subset \mathrm{Gp}(T_\ell(J(C_u)), e_\ell)$$

coincides with $\mathrm{Gp}(T_\ell(J(C_u)), e_\ell)$.

Corollary 3.5 (Corollary to Lemma 3.1)**.** *Let*

$$u(x) = u_{n,B,C}(x) := x^n + Bx + C \in \mathbb{Z}[x]$$

be a monic polynomial of degree $n > 1$ without multiple roots such that both B and C are nonzero integers that enjoy the following properties.

(i) (B, C) *is either* 1 *or a power of* 2*.*
(ii) (n, B) *is either* 1 *or a power of* 2*.*
(iii) $(n-1, C)$ *is either* 1 *or a power of* 2*.*

Suppose that the discriminant $D = \mathrm{Discr}(n, B, C) = 2^{2M} \cdot D_0$ where M is a nonnegative integer and D_0 is an integer such that

$$D_0 \equiv 1 \bmod 4.$$

Assume also that D is not a square. Then:

(a) *The quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is unramified ar* 2*. For all odd primes ℓ the Galois extension $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}(\sqrt{D})$ is unramified at every prime divisor of ℓ.*
(b) *There exists an odd prime ℓ that enjoys the following properties.*
  (i) *ℓ divides D_0 and*
  $$u(x) \bmod \ell \in \mathbb{F}_\ell[x]$$
  has exactly one multiple root and its multiplicity is 2*. In addition, this root lies in $\mathbb{F}_\ell$.*
  (ii) *The field extension $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}$ is ramified at ℓ and the Galois group*
  $$\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}) = \mathrm{Gal}(u/\mathbb{Q}) \subset \mathrm{Perm}(\mathfrak{R}_u)$$
  contains a transposition. In particular, if $\mathrm{Gal}(u/\mathbb{Q})$ *is doubly transitive then*
  $$\mathrm{Gal}(u/\mathbb{Q}) = \mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$$
  and
  $$\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}(\sqrt{D})) = \mathbf{A}_n.$$

Proof. Clearly, D_0 is *not* a square and

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_0})$$

is a quadratic field. Since D_0 is congruent to 1 modulo 4, the quadratic extension $\mathbb{Q}(\sqrt{D_0})/\mathbb{Q}$ is *unramified* at 2, which proves the first assertion of (a). The conditions of Lemma 3.1(2) hold for all odd primes ℓ. Now the second assertion of (a) follows from Remark 3.3 and Lemma 3.1(2)(c).

Let us start to prove (b). There are nonzero integers S and S_0 such that $D_0 = S^2 S_0$ and S_0 is square-free. Clearly, both S and S_0 are odd. Since

$$D = 2^{2M} \cdot D_0 = 2^{2M} \cdot S^2 S_0 = \left(2^M S\right)^2 S_0$$

is *not* a square, $S_0 \neq 1$. Since S is odd, $S^2 \equiv 1 \bmod 4$. Since $D_0 \equiv 1 \bmod 4$, we obtain that $S_0 \equiv 1 \bmod 4$. It follows that $S_0 \neq -1$. We already know that $S_0 \neq 1$. This implies that there is a prime ℓ that divides S_0. Since S_0 is odd and square-free, ℓ is also odd and ℓ^2 does not divide S_0. Let T be the nonnegative integer such that $\ell^T \mid\mid S$. Then $\ell^{2T+1} \mid\mid 2^{2M} S^2 S_0$, and therefore $\ell^{2T+1} \mid\mid D$. This implies that the quadratic field extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is *ramified* at ℓ. Since

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\mathfrak{R}_u),$$

the field extension $\mathbb{Q}(\mathfrak{R}_u)/\mathbb{Q}$ is also ramified at ℓ. Since $\ell \mid D$, the polynomial

$$u(x) \bmod \ell \in \mathbb{F}_\ell[x]$$

has a multiple root. Now the result follows from Lemma 3.1 combined with Remark 1.10. □

4. Discriminants of Mori trinomials

Let

$$f(x) = f_{g,p,b,c}(x) = x^{2g+1} - bx - \frac{pc}{4}$$

be a Mori trinomial. Following Mori [8], let us consider the polynomial

$$\mathbf{u}(x) = 2^{2g+1} f(x/2) = x^{2g+1} - 2^{2g}bx - 2^{2g-1}pc = u_{n,B,C}(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$$

with

$$n = 2g+1, B = -2^{2g}b, C = -2^{2g-1}pc.$$

Remarks 4.1. (i) Clearly, $f(x)$ and $\mathbf{u}(x)$ have the same splitting field and Galois group. It is also clear that

$$\Delta(\mathbf{u}) = 2^{(2g+1)2g} \cdot \Delta(f) = \left[2^{(2g+1)g}\right]^2 \cdot \Delta(f).$$

In particular, $\Delta(\mathbf{u})$ is *not* a square, thanks to Remark 1.6.

(ii) By Theorem 1.4(i,iii), the polynomial $f(x)$ is irreducible over $\mathbb{Q}$ and its Galois group is *doubly transitive*. This implies that $\mathbf{u}(x)$ is irreducible over $\mathbb{Q}$ and its Galois group over $\mathbb{Q}$ is also *doubly transitive*. (See also Theorem 6.6(i,ii) below.)

(iii) For all g the hyperelliptic curves C_f and $C_{\mathbf{u}}$ are biregularly isomorphic over $\mathbb{Q}(\sqrt{2})$. It follows that the jacobians $J(C_{\mathbf{u}})$ and $J(C_f)$ are also isomorphic over $\mathbb{Q}(\sqrt{2})$. In particular, $\mathrm{End}(J(C_{\mathbf{u}})) = \mathrm{End}(J(C_f))$.

Clearly, the conditions of Lemma 3.1 hold for $u(x) = \mathbf{u}(x)$ for all odd primes ℓ. The discriminant $\Delta(\mathbf{u})$ of $\mathbf{u}(x)$ coincides with

$$\mathrm{Discr}(n,B,C) = (-1)^{(2g+1)2g/2}(2g+1)^{2g+1}[-2^{2g-1}pc]^{2g} + (-1)^{2g(2g-1)/2}(2g)^{2g}[-2^{2g}b]^{2g+1}.$$

It follows that

$$\Delta(\mathbf{u}) = (-1)^g 2^{2g(2g-1)} \left[(2g+1)^{2g+1}(pc)^{2g} - 2^{6g}g^{2g}b^{2g+1}\right].$$

This implies that

$$\Delta(\mathbf{u}) = 2^{2[g(2g-1)]} D_0 \tag{3}$$

where

$$D_0 = (-1)^g \left\{(2g+1)\left[(2g+1)^g(pc)^g\right]^2 - 2^{6g}g^{2g}b^{2g+1}\right\}.$$

Clearly, D_0 is an *odd* integer that is *not* divisible by p. It is also clear that D_0 is congruent to $(-1)^g(2g+1)$ modulo 4 (because every odd square is congruent to 1 modulo 4). This implies that

$$D_0 \equiv 1 \bmod 4 \tag{4}$$

for all g.

5. Proof of Theorem 1.7

Let us apply Lemma 3.1(ii) to

$$\mathbf{u}(x) = 2^{2g+1} f(x/2) = x^{2g+1} - 2^{2g}bx - 2^{2g-1}pc.$$

We obtain that for each odd prime ℓ the polynomial

$$\mathbf{u}(x) \bmod \ell \in \mathbb{F}_\ell[x]$$

has, at most, one multiple root; in addition, this root is double and lies in $\mathbb{F}_\ell$. Applying to $\mathbf{u}(x)$ Corollary 3.5 combined with formulas (3) and (4) of Sect. 4, we conclude that there exists an odd $\ell \ne p$ such that $\mathbf{u}(x) \bmod \ell$ has exactly one multiple root; this root is double and lies in $\mathbb{F}_\ell$. In addition, $\mathrm{Gal}(\mathbf{u}/\mathbb{Q})$ coincides with $\mathbf{S}_{2g+1}$, because it is doubly transitive. Now the assertions (i) and (ii) follow readily from the equality

$$f(x) \bmod \ell = \frac{\mathbf{u}(2x)}{2^{2g+1}} \bmod \ell.$$

that holds for all odd primes ℓ.

By Remarks 4.1, $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(\mathbf{u}/\mathbb{Q})$ and therefore also coincides with $\mathbf{S}_{2g+1}$, which implies (in light of Section 1.1) that $\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}(\sqrt{\Delta(f)})) = \mathbf{A}_{2g+1}$. This proves (iii). Now Remark 1.9 implies that $\mathrm{End}(J(C_f)) = \mathbb{Z}$. This proves (iv). In order to prove (iiibis), first notice that the Galois extension $\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}$ is ramified at 2 (Remark 1.5(1)) while $\mathbb{Q}(\sqrt{\Delta(f)}) = \mathbb{Q}(\sqrt{\Delta(u)})$ is unramified at 2 over $\mathbb{Q}$ in light of formulas (3) and (4) in Sect. 4 (and Corollary 3.5(a)). This implies that $\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}(\sqrt{\Delta(f)})$ is ramified at some prime divisor of 2. Since all the field extensions involved are Galois, $\mathbb{Q}(\mathfrak{R}_f)/\mathbb{Q}(\sqrt{\Delta(f)})$ is actually ramified at *all* prime divisors of 2. This proves the first assertion of (iiibis). The second assertion of (iiibis) follows from Corollary 3.5(a). This proves (iiibis).

6. Variants and Complements

Throughout this section, K is a number field. We write $\mathcal{O}$ for the ring of integers in K. If $\mathfrak{b}$ is a maximal ideal in $\mathcal{O}$ then we write $k(\mathfrak{b})$ for the (finite) residue field $\mathcal{O}/\mathfrak{b}$. As usual, we call $\mathrm{char}(k(\mathfrak{b}))$ the residual characteristic of $\mathfrak{b}$. We write $K_\mathfrak{b}$ for the $\mathfrak{b}$-adic completion of K and

$$\mathcal{O}_\mathfrak{b} \subset K_\mathfrak{b}$$

for the ring of $\mathfrak{b}$-adic integers in the field $K_\mathfrak{b}$. We consider the subring $\mathcal{O}\left[\frac{1}{2}\right] \subset K$ generated by $\frac{1}{2}$ over $\mathcal{O}$. We have

$$\mathcal{O} \subset \mathcal{O}\left[\frac{1}{2}\right] \subset K.$$

If $\mathfrak{b} \subset \mathcal{O}$ is a maximal ideal in $\mathcal{O}$ with odd residual characteristic then

$$\mathcal{O} \subset \mathcal{O}\left[\frac{1}{2}\right] \subset \mathcal{O}_\mathfrak{b},$$

the ideal $\mathfrak{b}\mathcal{O}\left[\frac{1}{2}\right]$ is a maximal ideal in $\mathcal{O}\left[\frac{1}{2}\right]$ and

$$k(\mathfrak{b}) = \mathcal{O}/\mathfrak{b} = \mathcal{O}\left[\frac{1}{2}\right]/\mathfrak{b}\mathcal{O}\left[\frac{1}{2}\right] = \mathcal{O}_\mathfrak{b}/\mathfrak{b}\mathcal{O}_\mathfrak{b}.$$

Lemma 3.1(ii) and its proof admit the following straightforward generalization.

Lemma 6.1. *Let*

$$u(x) = u_{n,B,C}(x) := x^n + Bx + C \in \mathcal{O}[x]$$

be a monic polynomial of degree $n > 1$ such that $B \neq 0$ and $C \neq 0$. Let $\mathfrak{b}$ be a maximal ideal in $\mathcal{O}$ that enjoys the following properties.

(i) $B\mathcal{O} + C\mathcal{O} + \mathfrak{b} = \mathcal{O}$.
(ii) $n\mathcal{O} + B\mathcal{O} + \mathfrak{b} = \mathcal{O}$.
(iii) $(n-1)\mathcal{O} + C\mathcal{O} + \mathfrak{b} = \mathcal{O}$.

Suppose that $u(x)$ has no multiple roots. Let us consider the polynomial

$$\bar{u}(x) := u(x) \bmod \mathfrak{b} \in k(\mathfrak{b})[x].$$

Then:

(a) *$\bar{u}(x)$ has, at most, one multiple root in an algebraic closure of $k(\mathfrak{b})$.*
(b) *If such a multiple root say, γ, does exist, then*

$$n(n-1)BC \notin \mathfrak{b}$$

and γ is a double root of $\bar{u}(x)$. In addition, γ is a nonzero element of $k(\mathfrak{b})$.

(c) *If such a multiple root does exist then either the field extension $K(\mathfrak{R}_u)/K$ is unramified at $\mathfrak{b}$ or a corresponding inertia subgroup at $\mathfrak{b}$ in*

$$\mathrm{Gal}(K(\mathfrak{R}_u)/K) = \mathrm{Gal}(u/\mathrm{K}) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

is generated by a transposition. In both cases the Galois extension $K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})$ is unramified at all prime divisors of $\mathfrak{b}$.

Remark 6.2. In the notation of Lemma 6.1, suppose that $\bar{u}(x)$ has *no* multiple roots, i.e., $\Delta(u) \notin \mathfrak{b}$. Then clearly the Galois extension $K(\mathfrak{R}_u)/K$ is unramified at $\mathfrak{b}$.

Proof. We have

$$\bar{u}(x) := x^n + \bar{B}x + \bar{C} \in k(\mathfrak{b})[x]$$

where

$$\bar{B} = B \bmod \mathfrak{b} \in k(\mathfrak{b}),\ \bar{C} = C \bmod \mathfrak{b} \in k(\mathfrak{b}).$$

The condition (i) implies that either $\bar{B} \neq 0$ or $\bar{C} \neq 0$. The condition (ii) implies that if $\bar{B} = 0$ then $n \neq 0$ in $k(\mathfrak{b})$. It follows that if $\bar{B} = 0$ then $n\bar{C} \neq 0$.

The condition (iii) implies that if $(n-1) = 0$ in $k(\mathfrak{b})$ then $\bar{C} \neq 0$ (and, of course, $n \neq 0$ in $k(\mathfrak{b})$). On the other hand, if $\bar{C} = 0$ then $(n-1) \neq 0$ in $k(\mathfrak{b})$.

Suppose $\bar{u}(x)$ has a multiple root γ in an algebraic closure of $k(\mathfrak{b})$. Then as in the proof of Lemma 3.1(2),

$$0 = \Delta(\bar{u}) = (-1)^{n(n-1)/2} n^n \bar{C}^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} \bar{B}^n = 0.$$

This implies that

$$n^n \bar{C}^{n-1} = \pm (n-1)^{n-1} \bar{B}^n. \tag{5}$$

This implies that if $(n-1) = 0$ in $k(\mathfrak{b})$ then $\bar{C} = 0$, which is not the case. This proves that $(n-1) \neq 0$ in $k(\mathfrak{b})$. On the other hand, if $\bar{B} = 0$ then $\bar{C} \neq 0$ and $n \neq 0$ in $k(\mathfrak{b})$. Then formula (5) implies that $\bar{C} = 0$ and we get a contradiction that proves that $\bar{B} \neq 0$. If $n = 0$ in $k(\mathfrak{b})$ then $n - 1 \neq 0$ in $k(\mathfrak{b})$ and formula (5) implies that $\bar{B} = 0$, which is not the case. The obtained contradiction proves that $n \neq 0$ in $k(\mathfrak{b})$. If $\bar{C} = 0$ then formula (5) implies that $\bar{B} = 0$, which is not the case. This proves that the maximal ideal $\mathfrak{b}$ does *not* contain $n(n-1)BC$.

On the other hand, we have as in the proof of Lemma 3.1(2) that

$$x \cdot \bar{u}'(x) - n \cdot \bar{u}(x) = -(n-1)\bar{B}x - n\bar{C}$$

and therefore

$$-(n-1)\bar{B}\gamma - n\bar{C} = 0.$$

It follows that

$$\gamma = -\frac{n\bar{C}}{(n-1)\bar{B}}$$

is a *nonzero* element of $k(\mathfrak{b})$. The second derivative $\bar{u}''(x) = n(n-1)x^{n-2}$ and

$$\bar{u}''(\gamma) = n(n-1)\gamma^{n-2} \neq 0.$$

It follows that γ is a *double* root of $\bar{u}(x)$. This proves (a) and (b).

In order to prove (c), notice that as in the proof of Lemma 3.1(ii)(c), there exists a monic degree $(n-2)$ polynomial $\bar{h}(x) \in k(\mathfrak{b})[x]$ such that

$$\bar{u}(x) = (x-\gamma)^2 \cdot \bar{h}(x)$$

and $\bar{h}(x)$ and $(x-\gamma)^2$ are relatively prime. By Hensel's Lemma, there exist monic polynomials

$$h(x), v(x) \in \mathcal{O}_{\mathfrak{b}}[x],\ \deg(h) = n-2, \deg(v) = 2$$

such that

$$u(x) = v(x)h(x)$$

and

$$\bar{h}(x) = h(x) \bmod \mathfrak{b},\ (x-\gamma)^2 = v(x) \bmod \mathfrak{b}.$$

This implies that the splitting field $K_{\mathfrak{b}}(\mathfrak{R}_h)$ of $h(x)$ (over $K_{\mathfrak{b}}$) is an unramified extension of $\mathrm{K}_{\mathfrak{b}}$ while the splitting field $\mathrm{K}_{\mathfrak{b}}(\mathfrak{R}_u)$ of $u(x)$ (over $\mathrm{K}_{\mathfrak{b}}$) is obtained from $\mathrm{K}_{\mathfrak{b}}(\mathfrak{R}_h)$ by adjoining to it two (distinct) roots say, α_1 and α_2 of quadratic $v(x)$. The field $K_{\mathfrak{b}}(\mathfrak{R}_u)$ coincides either with $K_{\mathfrak{b}}(\mathfrak{R}_h)$ or with a certain quadratic extension of $\mathrm{K}_{\mathfrak{b}}(\mathfrak{R}_h)$, ramified or unramified. It follows that the inertia subgroup I of

$$\mathrm{Gal}(K_{\mathfrak{b}}(\mathfrak{R}_u)/K_{\mathfrak{b}}) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

is either trivial or is generated by the *transposition* that permutes α_1 and α_2 (and leaves invariant every root of $h(x)$). In the former case $K(\mathfrak{R}_u)/K$ is unramified at $\mathfrak{b}$ while in the latter one an inertia subgroup in

$$\mathrm{Gal}(K(\mathfrak{R}_u)/K) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

that corresponds to $\mathfrak{b}$ is generated by a transposition. In both cases the Galois (sub)group $\mathrm{Gal}(K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)}))$ does not contain transpositions (see Sect. 1.1). This implies that $K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})$ is *unramified* at all prime divisors of $\mathfrak{b}$. $\square$

Corollary 3.5 admits the following partial generalization.

Lemma 6.3. *Let K be a number field and $\mathcal{O}$ be its ring of integers Let*

$$u(x) = u_{n,B,C}(x) := x^n + Bx + C \in \mathcal{O}[x]$$

be a monic polynomial without multiple roots of degree $n > 1$ such that both B and C are not zeros. Suppose that there is a nonnegative integer N such that

$$2^N\mathcal{O} \subset B\mathcal{O} + C\mathcal{O},\ 2^N\mathcal{O} \subset n\mathcal{O} + B\mathcal{O},\ 2^N\mathcal{O} \subset (n-1)\mathcal{O} + C\mathcal{O}.$$

Suppose that there is a nonnegative integer M such that the discriminant $D := \Delta(u) = 2^{2M} \cdot D_0$ with $D_0 \in \mathcal{O}$.

Assume also that D, D_0 and K enjoy the following properties.

(i) *D is not a square in K and*

$$D_0 - 1 \in 4\mathcal{O}.$$

(ii) *The class number of K is odd (e.g., $\mathcal{O}$ is a principal ideal domain).*

(iii) *Either K is totally imaginary, i.e., it does not admit an embedding into the field of real numbers or K is totally real and D_0 is totally positive.*

Then:

(a) *The quadratic extension $K(\sqrt{\Delta(u)})/K$ is unramified at every prime divisor of 2. The Galois extension $K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})$ is unramified at every prime ideal $\mathfrak{b}$ of odd residual characteristic.*

(b) *There exists a maximal ideal $\mathfrak{b} \subset \mathcal{O}$ with residue field $k(\mathfrak{b})$ of odd characteristic that enjoys the following properties.*

  (i) *$D_0 \in \mathfrak{b}$, the polynomial*

$$u(x) \bmod \mathfrak{b} \in k(\mathfrak{b})[x]$$

  has exactly one multiple root and its multiplicity is 2. In addition, this root lies in $k(\mathfrak{b})$.

  (ii) *The field extension $K(\mathfrak{R}_u)/K$ is ramified at $\mathfrak{b}$ and the Galois group*

$$\mathrm{Gal}(K(\mathfrak{R}_u)/K) = \mathrm{Gal}(u/\mathrm{K}) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

  contains a transposition. In particular, if $\mathrm{Gal}(u/\mathrm{K})$ is doubly transitive then

$$\mathrm{Gal}(u/\mathrm{K}) = \mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$$

  and

$$\mathrm{Gal}(K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})) = \mathbf{A}_n.$$

Proof. Let us prove (a). Clearly,

$$E := K\left(\sqrt{D_0}\right) = K\left(\sqrt{D}\right) = K\left(\sqrt{\Delta(u)}\right) \subset K(\mathfrak{R}_u)$$

is a quadratic extension of K. Notice that

$$\theta = \frac{1+\sqrt{D_0}}{2} \in E$$

is a root of the quadratic equation

$$v_2(x) := x^2 - x + \frac{1-D_0}{4} \in \mathcal{O}[x]$$

and therefore is an algebraic integer. In addition,

$$E = K(\theta).$$

If a maximal ideal $\mathfrak{b}_2$ in $\mathcal{O}$ has residual characteristic 2 then the quadratic polynomial

$$v_2(x) \bmod \mathfrak{b}_2 = x^2 - x + \left(\frac{1-D_0}{4}\right) \bmod \mathfrak{b}_2 \in k(\mathfrak{b}_2)[x]$$

has no multiple roots, because its derivative is a nonzero constant -1. This implies that E/K is unramified at all prime divisors of 2. On the other hand, the conditions of Lemma 6.1 hold for all maximal ideals $\mathfrak{b}$ of $\mathcal{O}$ with *odd* residual characteristic. Now Remark 6.2 and Lemma 6.1(c) imply that the Galois extension $K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})$ is unramified at every $\mathfrak{b}$ of odd residual characteristic. This proves (a).

In order to prove (b), notice that the condition (iii) implies that either all archimedean places of both E and K are complex or all archimedean places of both E and K are real. This implies that E/K is unramified at all infinite primes. Since the class number of K is odd, the classical results about Hilbert class fields [6, Ch. 2, Sect. 1.2] imply that there is a maximal ideal $\mathfrak{b} \subset \mathcal{O}$ such that $E/K = K(\sqrt{D})/K$ is *ramified* at $\mathfrak{b}$. Since E/K is unramified at all prime divisors of 2, the residual characteristic of $\mathfrak{b}$ is *odd*, i.e., $2 \notin \mathfrak{b}$. This implies that

$$\Delta(u) = D \in \mathfrak{b}.$$

Since $D = 2^{2M} \cdot D_0$ and $\mathfrak{b}$ is a prime (actually, maximal) ideal in $\mathcal{O}$, we have $D_0 \in \mathfrak{b}$. It also follows that

$$u(x) \bmod \mathfrak{b} \in k(\mathfrak{b})[x]$$

has a multiple root. Now we are in a position to apply Lemma 6.1. Since $K(\mathfrak{R}_u) \supset E$, the field extension $K(\mathfrak{R}_u)/K$ is *ramified* at $\mathfrak{b}$. Applying Lemma 6.1, we conclude that $u(x) \bmod \mathfrak{b}$ has exactly one multiple root, this root is double and lies in $k(\mathfrak{b})$. In addition,

$$\mathrm{Gal}(K(\mathfrak{R}_u)/K) \subset \mathrm{Perm}(\mathfrak{R}_u)$$

contains a transposition. This implies that if $\mathrm{Gal}(K(\mathfrak{R}_u)/K)$ is doubly transitive then $\mathrm{Gal}(K(\mathfrak{R}_u)/K)$ coincides with $\mathrm{Perm}(\mathfrak{R}_u) \cong \mathbf{S}_n$. Of course, this implies that $\mathrm{Gal}(K(\mathfrak{R}_u)/K(\sqrt{\Delta(u)})) = \mathbf{A}_n$. □

6.4 (Generalized Mori quadruples). Let us consider a quadruple $(g, \mathfrak{p}, \mathbf{b}, \mathbf{c})$ where g is a positive integer, $\mathfrak{p}$ is a maximal ideal in $\mathcal{O}$ while $\mathbf{b}$ and $\mathbf{c}$ are elements of $\mathcal{O}$ that enjoy the following properties.

(i) The residue field $k(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$ is a finite field of *odd* characteristic. If q is the cardinality of $k(\mathfrak{p})$ then every prime divisor of g is also a divisor of $\frac{q-1}{2}$. In particular, if g is even then $(q-1)$ is divisible by 4.

(ii) The residue $\mathbf{b} \bmod \mathfrak{p}$ is a primitive element of $k(\mathfrak{p})$, i.e., it has multiplicative order $q-1$. In particular,

$$\mathbf{b}\mathcal{O} + \mathfrak{p} = \mathcal{O}.$$

The conditions (i) and (ii) imply that for each prime divisor d of g the residue $\mathbf{b} \bmod \mathfrak{p}$ is *not* a dth power in $k(\mathfrak{p})$. Since $(q-1)$ is even, $\mathbf{b} \bmod \mathfrak{p}$ is *not* a square in $k(\mathfrak{p})$. So, if d is a prime divisor of $2g$ then $\mathbf{b} \bmod \mathfrak{p}$ is *not* a dth power in $k(\mathfrak{p})$. If $2g$ is divisible by 4 then g is even and $(q-1)$ is divisible by 4, i.e., -1 is a square in $k(\mathfrak{p})$. It follows that $-4\mathbf{b} \bmod \mathfrak{p}$ is *not* a square in $k(\mathfrak{p})$. Thanks to Theorem 9.1 of [7, Ch. VI, Sect. 9], the last two assertions imply that the polynomial

$$x^{2g} - \mathbf{b} \bmod \mathfrak{p} \in k(\mathfrak{p})[x]$$

is irreducible over $k(\mathfrak{p})$. This implies that its Galois group over (the finite field) $k(\mathfrak{p})$ is an order $2g$ cyclic group.

(iii) $\mathbf{c} \in \mathfrak{p}$, $\mathbf{c} - 1 \in 2\mathcal{O}$ and

$$\mathcal{O} = \mathbf{b}\mathcal{O} + \mathbf{c}\mathcal{O} = \mathbf{b}\mathcal{O} + (2g+1)\mathcal{O} = 2g\mathcal{O} + \mathbf{c}\mathcal{O}.$$

We call such a quadruple a *generalized Mori quadruple* (in K).

Example 6.5. Suppose that K and g are given. By Dirichlet's Theorem about primes in arithmetic progressions, there is a prime p that does *not* divide $(2g+1)$ and is congruent to 1 modulo $2g$. (In fact, there are infinitely many such primes.) Clearly, p is *odd*. Let us choose a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ that contains p and denote by q the cardinality of the finite residue field $k(\mathfrak{p})$. Then $\mathrm{char}(k(\mathfrak{p}))=p$ and q is a power of p. This implies that $q-1$ is divisible by $p-1$ and therefore is divisible by $2g$. Let us choose a generator $\tilde{\mathbf{b}}\in k(\mathfrak{p})$ of the multiplicative cyclic group $k(\mathfrak{p})^*$. Let r be a nonzero integer that is *relatively prime* to $(2g+1)$. (E.g., $r=\pm 1, \pm 2$.) Using Chinese Remainder Theorem, one may find $\mathbf{b}\in\mathcal{O}$ such that

$$\mathbf{b} \bmod \mathfrak{p}=\tilde{\mathbf{b}},\ \ \mathbf{b}-r\in(2g+1)\mathcal{O}.$$

(Clearly, $\mathbf{b}\not\in\mathfrak{p}$.) Now the same Theorem allows us to find $\mathbf{c}\in\mathfrak{p}\subset\mathcal{O}$ such that $\mathbf{c}-1\in 2g\mathbf{b}\mathcal{O}$. Then $(g,\mathfrak{p},\mathbf{b},\mathbf{c})$ is a generalized Mori quadruple in K.

Let us consider the polynomials

$$F(x)=F_{g,\mathfrak{p},\mathbf{b},\mathbf{c}}(x)=x^{2g+1}-\mathbf{b}x-\frac{\mathbf{c}}{4}\in\mathcal{O}\left[\frac{1}{2}\right][x]\subset K[x]$$

and

$$U(x)=2^{2g+1}F(x/2)=x^{2g+1}-2^{2g}\mathbf{b}x-2^{2g-1}\mathbf{c}\in\mathcal{O}[x]\subset K[x].$$

Theorem 6.6. *Let $(g,\mathfrak{p},\mathbf{b},\mathbf{c})$ be a generalized Mori quadruple in K. Assume also that there exists a maximal ideal $\mathfrak{b}_2\subset\mathcal{O}$ of residual characteristic 2 such that the ramification index $e(\mathfrak{b}_2)$ of $\mathfrak{b}_2$ (over 2) in $K/\mathbb{Q}$ is relatively prime to $(2g+1)$. Then:*

(i) *The polynomial*

$$F(x)=F_{g,\mathfrak{p},\mathbf{b},\mathbf{c}}(x)\in K[x]$$

is irreducible over $K_{\mathfrak{b}_2}$ and therefore over K. In addition, the Galois extension $K(\mathfrak{R}_F)/K$ is ramified at $\mathfrak{b}_2$.

(ii) *The transitive Galois group*

$$\mathrm{Gal}(F/\mathrm{K})=\mathrm{Gal}(K(\mathfrak{R}_F)/K)\subset\mathrm{Perm}(\mathfrak{R}_F)=\mathbf{S}_{2g+1}$$

contains a cycle of length $2g$. In particular, $\mathrm{Gal}(F/\mathrm{K})$ is doubly transitive and is not contained in $\mathbf{A}_{2g+1}$, and $\Delta(F)$ is not a square in K.

(iii) *Assume that K is a totally imaginary number field with odd class number. Then $\mathrm{Gal}(F/K)=\mathrm{Perm}(\mathfrak{R}_F)$. If, in addition, $g>1$ then $\mathrm{End}(J(C_F))=\mathbb{Z}$.*

(iv) *Assume that K is a totally imaginary number field with odd class number and $g>1$. Then:*

  (1) *for all primes ℓ the image $\rho_{\ell,F}(\mathrm{Gal}(K))$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(J(C_F)),e_\ell)$.*

  (2) *Let L be a number field that contains K and $\mathrm{Gal}(L)$ be the absolute Galois group of L, which we view as an open subgroup of finite index in $\mathrm{Gal}(L)$. Then for all but finitely many primes ℓ the image $\rho_{\ell,F}(\mathrm{Gal}(L))$ coincides with $\mathrm{Gp}(T_\ell(J(C_F)),e_\ell)$.*

Remark 6.7. If K is a quadratic field then for every maximal ideal $\mathfrak{b}_2\subset\mathcal{O}$ (with residual characteristic 2) the ramification index $e(\mathfrak{b}_2)$ of $\mathfrak{b}_2$ in $K/\mathbb{Q}$ is either 1 or 2: in both cases it is relatively prime to odd $(2g+1)$. This implies that if K is an *imaginary quadratic field* with *odd class number* then all the conclusions of Theorem 6.6 hold for every generalized Mori quadruple $(g,\mathfrak{p},\mathbf{b},\mathbf{c})$. In particular, the Galois extension $K(\mathfrak{R}_F)/K$ is *ramified* at *every* $\mathfrak{b}_2$.

One may find the list of imaginary quadratic fields with *small* (≤ 23) odd class number in [1, pp. 322–324]; see also [16, Table 4 on p. 936].

Proof of Theorem 6.6. The $\mathfrak{b}_2$-adic Newton polygon of $F(x)$ consists of one *segment* that connects the points $(0, -2e(\mathfrak{b}_2))$ and $(2g+1, 0)$, which are its only integer points, because $e(\mathfrak{b}_2)$ and $(2g+1)$ are relatively prime and therefore $2e(\mathfrak{b}_2)$ and $(2g+1)$ are relatively prime. Now the irreducibility of $F(x)$ over $K_{\mathfrak{b}_2}$ follows from Eisenstein–Dumas Criterion [9, Cor. 3.6 on p. 316], [4, p. 502]. This proves (i). It also proves that the Galois extension $K(\mathfrak{R}_F)/K$ is *ramified* at $\mathfrak{b}_2$.

In order to prove (ii), let us consider the reduction

$$\tilde{F}(x) = F(x) \bmod \mathfrak{p}\mathcal{O}\left[\frac{1}{2}\right] = x^{2g+1} - \tilde{\mathbf{b}}x \in k(\mathfrak{p})[x]$$

where

$$\tilde{\mathbf{b}} = \mathbf{b} \bmod \mathfrak{p} \in k(\mathfrak{p}).$$

So,

$$\tilde{F}(x) = x(x^{2g} - \tilde{\mathbf{b}}) \in k(\mathfrak{p})[x].$$

We have already seen (Sect. 6.4) that $x^{2g} - \tilde{\mathbf{b}}$ is irreducible over $k(\mathfrak{p})$ and its Galois group is an order $2g$ cyclic group. We also know that $\tilde{\mathbf{b}} \ne 0$ and therefore the polynomials x and $x^{2g} - \tilde{\mathbf{b}}$ are relatively prime. This implies that $K(\mathfrak{R}_F)/K$ is unramified at $\mathfrak{p}$ and a corresponding *Frobenius element* in $\mathrm{Gal}(K(\mathfrak{R}_F)/K) \subset \mathrm{Perm}(\mathfrak{R}_F)$ is a cycle of length $2g$. This proves (ii). (Compare with arguments on p. 107 of [8].)

The map $\alpha \mapsto 2\alpha$ is a $\mathrm{Gal}(K)$-equivariant bijection between the sets of roots $\mathfrak{R}_F$ and $\mathfrak{R}_U$, which induces a group isomorphism between permutation groups $\mathrm{Gal}(\mathfrak{R}_F) \subset \mathrm{Perm}(\mathfrak{R}_F)$ and $\mathrm{Gal}(\mathfrak{R}_U) \subset \mathrm{Perm}(\mathfrak{R}_U)$. In particular, the double transitivity of $\mathrm{Gal}(\mathfrak{R}_F)$ implies the double transitivity of $\mathrm{Gal}(\mathfrak{R}_U)$. On the other hand,

$$\Delta(U) = 2^{(2g+1)2g}\Delta(F) = \left[2^{(2g+1)g}\right]^2 \Delta(F).$$

This implies that $\Delta(U)$ is *not* a square in K as well. The discriminant $\Delta(U)$ is given by the formula (Remark 3.2)

$$\begin{aligned} D := \Delta(U) &= (-1)^{(2g+1)2g/2}(2g+1)^{2g+1}[-2^{2g-1}\mathbf{c}]^{2g} + (-1)^{2g(2g-1)/2}(2g)^{2g}[-2^{2g}\mathfrak{b}]^{2g+1} \\ &= (-1)^g 2^{2g(2g-1)}\left[(2g+1)^{2g+1}\mathbf{c}^{2g} - 2^{6g}g^{2g}\mathfrak{b}^{2g+1}\right] = \\ &\quad 2^{2[g(2g-1)]}\left\{(-1)^g\left[(2g+1)^{2g+1}\mathbf{c}^{2g} - 2^{6g}g^{2g}\mathfrak{b}^{2g+1}\right]\right\}. \end{aligned}$$

We have

$$D = 2^{2M}D_0$$

where $M = g(2g-1)$ is a positive integer and

$$D_0 = (-1)^g\left[(2g+1)^{2g+1}\mathbf{c}^{2g} - 2^{6g}g^{2g}\mathfrak{b}^{2g+1}\right] \in \mathcal{O}.$$

Since $\mathbf{c} - 1 \in 2\mathcal{O}$, we have $\mathbf{c}^2 - 1 \in 4\mathcal{O}$ and

$$D_0 \equiv (-1)^g(2g+1)^{2g+1} \bmod 4\mathcal{O}.$$

Since $(2g+1)^{2g} = \left[(2g+1)^2\right]^g \equiv 1 \bmod 4$, we conclude that

$$D_0 \equiv (-1)^g(2g+1) \bmod 4\mathcal{O}.$$

This implies that

$$D_0 - 1 \in 4\mathcal{O}.$$

Applying Lemma 6.3 to

$$n = 2g+1, B = -2^{2g}\mathbf{b}, C = -2^{2g-1}\mathbf{c}, u(x) = U(x), M = g(2g-1), N = 2g,$$

we conclude that doubly transitive $\mathrm{Gal}(U/K)$ coincides with $\mathrm{Perm}(\mathfrak{R}_U)$ and therefore $\mathrm{Gal}(F/K)$ coincides with $\mathrm{Perm}(\mathfrak{R}_F) \cong \mathbf{S}_{2g+1}$. If $g > 1$ then Theorem 1.2 tells us that $\mathrm{End}(J(C_F)) = \mathbb{Z}$. This proves (iii). We also obtain that there exists a maximal ideal $\mathfrak{b} \subset \mathcal{O}$ with odd residual characteristic such that

$$U(x) \bmod \mathfrak{b} \in k(\mathfrak{b})[x]$$

has exactly one multiple root, this root is double and lies in $k(\mathfrak{b})$. Since

$$F(x) = \frac{U(2x)}{2^{2g+1}},$$

we obtain that

$$F(x) \bmod \mathfrak{b}\mathcal{O}\left[\frac{1}{2}\right] = \frac{U(2x)}{2^{2g+1}} \bmod \mathfrak{b} \in k(\mathfrak{b})[x].$$

This implies that the polynomial $F(x) \bmod \mathfrak{b}\mathcal{O}\left[\frac{1}{2}\right] \in k(\mathfrak{b})[x]$ has exactly one multiple root, this root is double and lies in $k(\mathfrak{b})$. The properties of $F(x) \bmod \mathfrak{b}\mathcal{O}\left[\frac{1}{2}\right]$ imply that $J(C_F)$ has a *semistable reduction* at $\mathfrak{b}$ with *toric dimension* 1. Now it follows from [21, Th. 4.3] that for for all primes ℓ the image $\rho_{\ell,F}(\mathrm{Gal}(K))$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(J(C_F)), e_\ell)$. It follows from [5, Th. 1] that if L is a number field containing K then for all but finitely many primes ℓ the image $\rho_{\ell,F}(\mathrm{Gal}(L))$ coincides with $\mathrm{Gp}(T_\ell(J(C_F)), e_\ell)$. This proves (iv). □

Corollary 6.8. *We keep the notation of Theorem 6.6. Let K be an imaginary quadratic field with odd class number. Let $(g, \mathfrak{p}, \mathbf{b}, \mathbf{c})$ be a generalized Mori quadruple in K and*

$$F(x) = F_{g,\mathfrak{p},\mathbf{b},\mathbf{c}}(x) \in K[x].$$

Then

$$\mathrm{Gal}(K(\mathfrak{R}_F)/K(\sqrt{\Delta(F)})) = \mathbf{A}_{2g+1}$$

and the Galois extension $K(\mathfrak{R}_F)/K(\sqrt{\Delta(F)})$ is unramified everywhere outside 2 and ramified at all prime divisors of 2.

Proof. As above, let us consider the polynomial

$$U(x) = 2^{2g+1}F(x/2) = x^{2g+1} - 2^{2g}\mathbf{b}x - 2^{2g-1}\mathbf{c} \in \mathcal{O}[x] \subset K[x].$$

We have

$$K(\mathfrak{R}_F) = K(\mathfrak{R}_U),\ K(\sqrt{\Delta(F)}) = K(\sqrt{\Delta(U)}).$$

Since

$$\mathbf{S}_{2g+1} = \mathrm{Perm}(\mathfrak{R}_U) = \mathrm{Gal}(U/K) = \mathrm{Gal}(K(\mathfrak{R}_U)/K),$$

we have

$$\mathrm{Gal}(K(\mathfrak{R}_U)/K(\sqrt{\Delta(U)})) = \mathbf{A}_{2g+1}.$$

It follows from Remark 6.7 that the Galois extension $K(\mathfrak{R}_U)/K$ is *ramified* at every prime divisor of 2 (in K). On the other hand, Lemma 6.3(a) (applied to $u(x) = U(x)$) tells us that the quadratic extension $K(\sqrt{\Delta(U)})/K$ is *unramified* at every prime divisor of 2 (in K). Since all the field extensions involved are Galois, $K(\mathfrak{R}_U)/K(\sqrt{\Delta(U)})$ is *ramified* at every prime divisor of 2 (in $K(\sqrt{\Delta(U)})$).

Since K is purely imaginary, $K(\sqrt{\Delta(U)})$ is also purely imaginary and therefore (its every field extension, including) $K(\mathfrak{R}_U)$ is unramified at all infinite places (in $K(\sqrt{\Delta(U)})$).

Remark 6.2 and Lemma 6.3(a) (applied to $u(x) = U(x)$) imply that the field extension $K(\mathfrak{R}_U)/K(\sqrt{\Delta(U)})$ is *unramified* at all maximal ideals $\mathfrak{b}$ in $\mathcal{O}$ with odd residual characteristic. $\square$

7. Corrigendum to [20]

- Page 660, the 6th displayed formula: insert $\subset$ between $\mathrm{End}_{\mathrm{Gal}(K)}V_\ell(X)$ and $\mathrm{End}_{\mathbb{Q}_\ell}V_\ell(X)$.
- Page 662, Theorem 2.6, line 3: r_1 should be r_2.
- Page 664, Remark 2.16: The reference to [23, Theorem 1.5] should be replaced by [23, Theorem 1].
- Page 664, Theorem 2.20. The following additional condition on ℓ was inadvertently omitted.
  "(iii) *If* C *is the center of* $\mathrm{End}(X)$ *then* $C/\ell C$ *is the center of* $\mathrm{End}(X)/\ell\mathrm{End}(X)$."
  In addition, "be" on the last line should be "is".
- Page 666, Theorem. 3.3. Line 2: ℓ should be assumed to be in P, i.e. one should read "*Then for all but finitely many* $\ell \in P$ . . .". In addition, X_n should be X_ℓ throughout lines 3–6.
- Page 668, Lemma 3.9, line 1: Isog_P should be Is_P.
- Page 668, Theorem 3.10, line 1: replace $\mathrm{Isog}_P((X\times X^t)^8, K, 1)$ by $\mathrm{Is}_P((X\times X^t)^4, K, 1)$.
- Page 670, Sect. 5.1, the first displayed formula: t should be g.
- Page 672, line 9: X'_ℓ should be X_ℓ.

(I am grateful to Kestutis Cesnavicius, who has sent me this list of typos.)

References

[1] S. Arno, M.L. Robinson, F.S. Wheeler, *Imaginary quadratic fields with small odd class number*. Acta Arithmetica **LXXXIII** (1998), 295–330.

[2] S.D. Cohen, A. Movahhedi, A. Salinier, *Double transitivity of Galois groups of trinomials*. Acta Arithmetica **LXXXII** (1997), 1–15.

[3] D.K. Faddeev, I.S. Sominsky, Problems in Higher Algebra (in Russian), 5th edition. Nauka, Moscow, 1954; English translation of 9th edition: Mir, Moscow, 1972.

[4] Sh. Gao, *Absolute irreducibility of polynomials via Newton polytopes*. J. Algebra **237** (2001), 501–520.

[5] Ch. Hall, *An open image theorem for a general class of abelian varieties*. Bull. London Math. Soc. **43** (2011), 703–711.

[6] H. Koch, Algebraic Number Theory (Number Theory II). Encyclopaedia of Mathematical Sciences **62**, Springer-Verlag, Berlin Heidelberg, 1992.

[7] S. Lang, Algebra, 3rd edition. Addison-Wesley, 1993.

[8] Sh. Mori, *The endomorphism rings of some abelian varieties II*. Japan. J. Math. **3** (1977), 105–109.

[9] J.L. Mott, *Eisenstein type irreducibility criteria*. In "Zero-Dimensional Commutative Rings (Knoxville, TN, 1994)" (D.F. Anderson and D.E. Dobbs, eds), Lecture Notes in Pure and Appl. Math., Vol. **171**, pp. 307–329, Marcel Dekker Inc., New York, 1995.

[10] D. Mumford, Abelian varieties, 2nd edition. Oxford University Press, 1974.

[11] H. Osada, *The Galois groups of the polynomials* $X^n + aX^l + b$. J. Number Theory **25** (1987), no. 2, 230–238.

[12] K.A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*. Ann. of Math. **101** (1975), 555–562.

[13] E.S. Selmer, *On the irreducibility of certain trinomials*. Math. Scand. **4** (1956), 287–302.

[14] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, 2nd edition. Addison–Wesley, 1989.

[15] J.-P. Serre, Topics in Galois Theory. Boston and London, Jones and Bartlett Publ. 1992.

[16] M. Watkins, *Class numbers of imaginary quadratic fields*. Mathematics of Computation **73** (2003), 907–938.

[17] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.

[18] Yu. G. Zarhin, *Very simple* 2*-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), 403–431.

[19] Yu. G. Zarhin, *Families of absolutely simple hyperelliptic jacobians*. Proc. London Math. Soc. (3) **100** (2010), 24–54.

[20] Yu. G. Zarhin, *Abelian varieties over fields of finite characteristic*. Central European J. Math. **12** (2014), 659–674.

[21] Yu. G. Zarhin, *Two-dimensional families of hyperelliptic jacobians with big monodromy*. Trans. Amer. Math. Soc., to appear; arXiv:1310.6532 [math.AG] .

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu