Can. J. Math.Vol. **43** (5), 1991 pp. 1055–1064

EXPLICIT HYPERELLIPTIC CURVES WITH REAL MULTIPLICATION AND PERMUTATION POLYNOMIALS

WALTER TAUTZ, JAAP TOP AND ALAIN VERBERKMOES

ABSTRACT. The aim of this paper is to present a very explicit construction of one parameter families of hyperelliptic curves C of genus $(p-1)/2$, for any odd prime number p, with the property that the endomorphism algebra of the jacobian of C contains the real subfield $Q\big(2\cos(2\pi/p)\big)$ of the cyclotomic field $Q(e^{2\pi i/p})$.

Two proofs of the fact that the constructed curves have this property will be given. One is by providing a double cover with the pth roots of unity in its automorphism group. The other is by explicitly writing down equations of a correspondence in $C \times C$ which defines multiplication by $2\cos(2\pi/p)$ on the jacobian of C. As a byproduct we obtain polynomials which define bijective maps $\mathbf{F}_\ell \longrightarrow \mathbf{F}_\ell$ for all prime numbers in certain congruence classes.

1. **Introduction.** In a beautiful Comptes Rendus note [3], J. F. Mestre presented a construction of hyperelliptic curves whose jacobians have real multiplication. As an application he found that the groups $\mathrm{PSL}_2(\mathbf{F}_{p^2})$, for $p \equiv \pm 2 \bmod 5$, can be realized as Galois groups over the rationals. An important tool in Mestre's construction is provided by torsion points on elliptic curves. One idea which led to the results presented in our paper was to try to mimic Mestre's approach with 'elliptic curve' replaced by the multiplicative group $\mathbf{G}_m$.

Another important motivation was given by recent work of Van Geemen and Werner [1]. They compute Betti- and Hodge numbers of several three-folds. A particular example they study is associated with the equation

$$f(x,y) = f(w,z),$$

where $f(x,y) = 0$ defines a skew pentagon in the x,y-plane. It turns out that 'level surfaces' $f(x,y) = c$ define double covers of hyperelliptic curves of genus 2, whose jacobian has real multiplication by $\frac{1+\sqrt{5}}{2}$. It may well be that this can be 'explained' in terms of classical work of Humbert, who described abelian surfaces with real multiplication in terms of the configuration of the ramification locus of the associated Kummer surface seen in a natural way as double cover of the plane.

Still another motivation to provide examples of jacobians with many endomorphisms can be found in recent work of De Jong and Noot [2]. They showed that the jacobian of the curve $y^n = x(x-1)(x-\lambda)$ has for $n = 5, 7$ a CM-field of degree 8,12 resp. in its

Received by the editors March 21, 1990.

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

endomorphism algebra for infinitely many values of λ. One can ask the same question for families related to the ones presented here; e.g. for the family

$$y^3 = x^5 - 5x^3 + 5x + t$$

of curves of genus 4. Analogous to what will be shown below, one checks that these curves already have the field $\mathbf{Q}(\sqrt{-3}, \sqrt{5})$ in the endomorphism algebra of their jacobian. However, investigating the action of the endomorphisms on homomorphic 1-forms leads one to believe that the situation here is in an essential way different from the one in their paper. We will not go into the case of non-hyperelliptic curves here.

The main result of this paper is the following.

THEOREM 1. *Let $p \geq 3$ be a prime number. Denote by ζ_p a primitive pth root of unity (in $\bar{\mathbf{Q}}$). Let $g \in \mathbf{Z}[X]$ be the minimal polynomial of $-\zeta_p - \zeta_p^{-1}$. Put $f_t(X) := Xg(X^2 - 2) + t$. The equation*

$$y^2 = f_t(x)$$

defines a family of curves of genus $(p-1)/2$ whose jacobians contain the field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ in their endomorphism algebra.

While investigating the families of curves mentioned in the theorem above we found a rather amusing additional result: *

THEOREM 2. *Let g be as defined above and let ℓ be a prime number. The map*

$$x \longmapsto xg(x^2 - 2) \colon \mathbf{F}_\ell \longrightarrow \mathbf{F}_\ell$$

is bijective for all prime numbers ℓ such that $\ell^4 \not\equiv 1 \bmod p$.

For $p = 5$ it is even bijective whenever $\ell \equiv \pm 2 \bmod 5$.

A simple consequence of this theorem is that a smooth complete model of the curve over $\mathbf{F}_\ell$ defined by $y^m = xg(x^2 - 2)$ (for $\ell \not| m$ and $\ell^4 \not\equiv 1 \bmod p$) has exactly $\ell + 1$ $\mathbf{F}_\ell$-rational points. Although it is possible to 'explain' this fact using the real multiplications, it is certainly nice to have such an elementary proof as well. The special case $p = 5$ yields the polynomial $X^5 - 5X^3 + 5X$. The fact that this defines a bijection $\mathbf{F}_\ell \longrightarrow \mathbf{F}_\ell$ was submitted as an exercise in the problem session of Nieuw Archief voor Wiskunde.

It is a pleasure for us to thank Bas Edixhoven, Noam Elkies, Bert van Geemen, Johan de Jong, Ernst Kani, Jean-François Mestre, Rutger Noot, Frans Oort, Chad Schoen and Noriko Yui for showing interest and/or giving some useful remarks. Most of this work was done at the Mathematisch Instituut der Rijksuniversiteit te Utrecht. The initial typesetting of the manuscript was done at the Department of Mathematics and Statistics of Queen's University, Kingston. We thank both institutions for their hospitality.

* Recently we found out that an even stronger result than Theorem 2 is well known and in fact very classical. See Ken Williams's paper in Duke Math. J. **38**(1971) 659–665 for a good reference.

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

2. **The construction.** Let $n \geq 2$ be an integer. Suppose k is a field of characteristic not dividing $2n$. Over k, we define a family of curves $\mathcal{D}_t$ as the smooth, projective model corresponding to the equation

$$y^2 = x(x^{2n} + tx^n + 1).$$

The curves $\mathcal{D}_t$ have many automorphisms. On the model given by the equation above one easily discovers a $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, given by the hyperelliptic involution and the map $(x, y) \longmapsto (\zeta x, \zeta^{(n+1)/2} y)$ for an nth root of unity ζ. Furthermore, we have the involution σ given by

$$\sigma\colon (x, y) \longmapsto \left(\frac{1}{x}, \frac{y}{x^{n+1}}\right).$$

Note that σ does not commute with the $\mathbf{Z}/n\mathbf{Z}$ while it does commute with the hyperelliptic involution. Hence the quotient

$$C_t := \mathcal{D}_t / \langle \sigma \rangle$$

is again hyperelliptic, but the $\mathbf{Z}/n\mathbf{Z}$ does not descend to automorphisms of C_t. However, it does of course define correspondences on C_t. This observation is the basis for the present paper.

We start by providing a model for the quotient $\mathcal{D}_t / \langle \sigma \rangle$.

PROPOSITION 3. *The quotient C_t of the curve $\mathcal{D}_t$ given by the equation*

$$y^2 = x(x^{2n} + tx^n + 1)$$

modulo the involution $\sigma\colon (x, y) \longmapsto \left(\frac{1}{x}, \frac{y}{x^{n+1}}\right)$ is given by

$$y^2 = x \cdot g(x^2 - 2) + t$$

if n is odd, and

$$y^2 = (x + 2)\big(g(x^2 - 2) + t\big)$$

in case n is even.

Here $g(X) \in k[X]$ is the monic polynomial whose zeroes are all the numbers $\zeta + \zeta^{-1}$, for $\zeta \in \bar{k} \setminus \{-1\}$ satisfying $\zeta^n = -1$. The model given is in fact birationally isomorphic to C_t over the base field k.

PROOF. Since σ and the hyperelliptic involution commute, we obtain a commutative diagram

$$\begin{tikzcd} \mathcal{D}_t \arrow[r] \arrow[d] & C_t \arrow[d] \\ \mathbf{P}^1 \arrow[r] & \mathbf{P}^1 \end{tikzcd}$$

in which all morphisms have degree 2. The map $\mathbf{P}^1 \longrightarrow \mathbf{P}^1$ here can be given as $x \longmapsto x + 1/x$. From this description it is clear that a model of C_t is given by the equation

$$y^2 = h_t(x),$$

in which h_t is a polynomial with simple zeroes at all numbers of the form $\alpha+\alpha^{-1}$, where α is a root of $x^{2n}+tx^n+1=0$, and in case n is even, another simple zero at -2.

Now in $k[X,X^{-1}]$ the relations

$$X^{2n}+1=X^n(X+X^{-1})\cdot g(X^2+X^{-2}),$$

for n odd, and

$$X^{2n}+1=X^n g(X^2+X^{-2})$$

for even n hold. This can be checked by noting that both sides define monic polynomials of the same degree with the same set of zeroes. It follows easily that the expressions given in the statement of the proposition define such polynomials $h_t(X)$.

Moreover, taking the model $y^2 = x(x^{2n}+tx^n+1)$ for $\mathcal{D}_t$, the field of σ-invariant functions on $\mathcal{D}_t$ over k is generated by $\eta = yx^{-(n+1)/2}$ and $\xi = x+x^{-1}$ in case n is odd, and $\xi = x+x^{-1}$, $\eta = y(1+x^{-1})x^{-n/2}$ in case n is even. Again using the relations above one finds

$$\eta^2=\xi\cdot g(\xi^2-2)+t$$

and

$$\eta^2=(\xi+2)\big(g(\xi^2-2)+t\big),$$

respectively. This proves the proposition. ∎

REMARK. Starting similarly from $y^2=x^{2n}+tx^n+1$ one can take the quotient under the involution given by $(x,y)\longmapsto\big(1/x,y/x^n\big)$. Using the same notations as above, the quotient is for odd n described by the equation $y^2=(x+2)\big(xg(x^2-2)+t\big)$ and for even n by $y^2=g(x^2-2)+t$. In fact, the two examples are closely related: both are covered by the curve given by $y^2=x^{4n}+tx^{2n}+1$.

3. **Proofs.**

3.1 *The main result.* We use the setup and notations from the previous section, but from now on we restrict ourselves to the case $n=p$ is an odd prime number. Fix the model $y^2=x(x^{2p}+tx^p+1)$ for $\mathcal{D}_t$ and take $\zeta\in\mathrm{Aut}(\mathcal{D}_t)$ given by

$$\zeta:(x,y)\longmapsto(\zeta_p x,\zeta_p^{(p+1)/2}y),$$

where $\zeta_p\in\bar{k}$ is a primitive pth root of unity. Let $[\zeta]$ be the automorphism of the jacobian $\mathrm{Jac}(\mathcal{D}_t)$ corresponding to ζ.

To prove our main result, it suffices to show that the endomorphism $[\zeta]+[\zeta]^{-1}$ 'restricts' to the jacobian of $\mathcal{C}_t$. This will follow if one shows that its action on the tangent space at the origin of $\mathrm{Jac}(\mathcal{D}_t)$ stabilizes the subspace on which the involution σ acts trivially. Equivalently, one has to check that the action of $\zeta+\zeta^{-1}$, seen as element of the group ring $k[\mathrm{Aut}(\mathcal{D}_t)]$, stabilizes the space $\omega(\mathcal{D}_t)^\sigma$ of σ-invariant differentials in $H^0(\mathcal{D}_t,\Omega^1_{\mathcal{D}_t/k})$.

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

A basis for $\omega(\mathcal{D}_t)^\sigma$ is given by the differentials

$$\omega_j = (x^j - x^{p-1-j})\frac{dx}{y}; \qquad 0 \leq j \leq (p-3)/2.$$

One computes

$$\big(\zeta^* + (\zeta^{-1})^*\big)\omega_j = \big(\zeta_p^{(p+1)/2-j-1} + (\zeta_p^{-1})^{(p+1)/2-j-1}\big)\omega_j.$$

From this, Theorem 1 follows.

3.2 *Remarks on simpleness.* We will now take a closer look at the special case $t = 0$. Assume that the ground field is $k = \mathbf{Q}$. The curves $\mathcal{C}_0$ and $\mathcal{D}_0$ have an additional automorphism:

$$\iota\colon (x,y) \longmapsto (-x, iy).$$

Here i is a square root of -1. Obviously, ι and ζ commute, and ι^2 acts as -1 on both jacobians. As above, $[\zeta]$+$[\zeta^{-1}]$ acts on the tangent space at the origin of Jac$(\mathcal{C}_0)$. Together with the action of $[\iota]$ this provides a representation of the field $K = \mathbf{Q}(\zeta_p, i)$. Fixing an embedding of K into $\mathbf{C}$, this representation determines a CM-type of the CM-field K([4], pp. 42–44). This is described in the following

PROPOSITION 4. *The* CM-*type of the field* $K = \mathbf{Q}(\zeta_p + \zeta_p^{-1}, i) \subset \mathbf{C}$ *corresponding to the curve* $y^2 = xg(x^2 - 2)$ *can be described as follows.*

Write Gal$(K/\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{F}_p^*/\langle \pm 1 \rangle$, *where the* $\mathbf{Z}/2\mathbf{Z}$ *corresponds to* Gal$\big(\mathbf{Q}(i)/\mathbf{Q}\big)$ *and* $\mathbf{F}_p^*$ *to the Galois group of* $\mathbf{Q}(\zeta_p)/\mathbf{Q}$.

Then the CM-*type is given by the partition*

$$\mathrm{Gal}(K/\mathbf{Q}) = V_1 \cup V_2,$$

where V_1 *and* V_2 *are subsets of* $(p-1)/2$ *elements defined by*

$$V_1 = \{(0,\pm 1), (1, \pm 2), (0, \pm 3), (1, \pm 4), \ldots\}$$

and

$$V_2 = \{(1,\pm 1), (0, \pm 2), (1, \pm 3), (0, \pm 4), \ldots\}.$$

PROOF. Similar to the discussion in (3.1) above, it suffices to compute the action of $\zeta^* + (\zeta^{-1})^*$ and ι^* on global differentials of $\mathcal{D}_0$ invariant under $(x,y) \longmapsto \big(1/x, y/x^{n+1}\big)$. A basis of these differentials and the action of $\zeta^* + (\zeta^{-1})^*$ on it was already computed. Since

$$\iota^*\omega_j = (-1)^j i\omega_j,$$

this implies the proposition. ∎

Using a criterion provided by Shimura and Taniyama, the above description allows us to prove the following.

PROPOSITION 5. *In characteristic zero, the jacobian of the hyperelliptic curve given by*

$$C_0 : j^2 = xg(x^2 - 2)$$

where $g \in \mathbf{Z}[X]$ is the minimal polynomial of $-2\cos(2\pi/p)$, is absolutely simple for all prime numbers p except for $p = 5$.

A direct consequence of this is

COROLLARY 6. *In characteristic zero, the jacobian of $y^2 = xg(x^2-2)+t$ is absolutely simple for general t if $p \neq 5$.* ■

REMARK. We do not know whether the corollary is also true for $p = 5$. Of course, the fact that the jacobian of C_0 is *not* simple in that case doesn't give any information on the situation for general t. In fact, by computing characteristic polynomials of Frobenius over various finite fields for some values of t, we are tempted to believe that also for $p = 5$ we obtain in general absolutely simple jacobians.

PROOF OF PROPOSITION 5. By [4], p. 69 it suffices to show that the CM-type described above is primitive if and only if $p \neq 5$. In our case this means that multiplication by a non-trivial element of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{F}_p^*/\langle \pm 1 \rangle$ does not fix the sets V_1 and V_2, unless $p = 5$.

For $p = 5$ multiplication by $(1, \pm 2)$ provides such an element, hence the CM-type is not primitive. The cases $p < 5$ are trivial (the corresponding curve has genus 1). Hence we may and will assume $p > 5$. Of course, an element fixing V_1 will also fix V_2. Hence we restrict our attention to one of these, say

$$\{(0, \pm 1), (1, \pm 2), (0, \pm 3), \ldots\}.$$

This set is the union of two subsets: write V' for the ones with first coordinate 0 and V'' for the others. We distinguish three cases.

CASE 1. Assume $p \equiv 3 \bmod 4$. Since V' and V'' have different cardinality, an element in $\mathbf{Z}/2\mathbf{Z} \times \mathbf{F}_p^*/\langle \pm 1 \rangle$ fixing their union must be of the form $\alpha = (0, *)$. This element acts without fixed points on V', hence order $(\alpha) | \# V' = (p-3)/4$. The order of α divides the order of the group $\mathbf{F}_p^*/\langle \pm 1 \rangle$ as well, which is $(p-1)/2$. It follows that order $(\alpha) = 1$, i.e. α is the unit element of the group.

CASE 2. Assume $p \equiv 1 \bmod 4$ and the element α interchanges the sets V' and V''. Then α interchanges the sets $(0, \pm 2)V'$ and $(0, \pm 2)V''$ as well. Define for $0 \leq j \leq 3$ the sets

$$W_j := \{\beta \in \mathbf{F}_p^*/\langle \pm 1 \rangle ; \beta \text{ is represented by } b \in \mathbf{Z}$$
$$\text{with } 0 < b < p \text{ and } b \equiv j \bmod 4\}.$$

Then $W_0 = W_1$ and $W_2 = W_3$. Furthermore

$$(0, \pm 2)V'' = \{(1, \beta); \quad \beta \in W_0\}$$

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

and

$$(0, \pm 2)V' = \{(0, \beta); \quad \beta \in W_2\}.$$

Write $\alpha = (1, \beta)$ and represent β by $b \in \mathbf{Z}$ with $0 < b < p$ and b odd. By assumption, multiplication by β interchanges the sets W_0 and W_2. We will show that β cannot exist by examining what it does to the elements $\pm 1, \pm 2, \pm 3$ and ± 5.

Because $b \cdot 1$ represents an element of $W_2 = W_3$, it follows $b \equiv 3 \bmod 4$. Next, $p/2 < b < p$, since otherwise $0 < b \cdot 2 < p$ which would imply that $b \cdot 2$ represented an element in W_2. Similarly one finds $b < 2p/3$, because if this were not the case then $0 < b \cdot 3 - 2p < p$ and $b \cdot 3 - 2p \equiv 3 \bmod 4$, hence both ± 3 and $\beta \cdot \pm 3$ would be elements of $W_3 = W_2$.

Hence we either have $2p/5 < b < 3p/5$ or $3p/5 < b < 4p/5$. By looking at $b \cdot 5 - 2p$ and $b \cdot 5 - 3p$ in these respective cases, one checks that neither can occur.

CASE 3. Assume $p \equiv 1 \bmod 4$ and the element α fixes the sets V' and V''. Using the same idea and notations as in Case 2, one now has to look for elements $b \in \mathbf{Z}$ such that $0 < b < p$ and $b \equiv 1 \bmod 4$.

By studying $b \cdot 2$ one finds $0 < b < p/2$. Proceeding by induction, it follows by looking at $b \cdot 2^k$ that $0 < b < 2^k$ for all k such that $2^k < p$. By taking the maximal such k one finds $0 < b < p/2^k < 2$, hence $b = 1$.

This finishes the proof. ■

3.3 *Correspondences.* From now on the only constraint on the characteristic is that it does not divide $2p$. Instead of using the curves $\mathcal{D}_t$ to obtain endomorphisms of the jacobians of C_t one can construct these endomorphisms directly in terms of correspondences on C_t. As before, C_t is assumed to be given by the model $y^2 = xg(x^2 - 2) + t$. Consider the morphism φ given as

$$\varphi \colon C_t \times C_t \longrightarrow \mathbf{P}^1 \times \mathbf{P}^1$$

which sends a pair of points (P_1, P_2) to their y-coordinates $\big(y(P_1), y(P_2)\big)$.

The inverse image $\varphi^{-1}(\Delta)$ of the diagonal $\Delta \subset \mathbf{P}^1 \times \mathbf{P}^1$ consists of the diagonal in $C_t \times C_t$, and another component. This other part is locally described by the set of equations

$$y_1^2 = x_1 g(x_1^2 - 2) + t$$
$$y_2^2 = x^2 g(x_2^2 - 2) + t$$
$$y_1 = y_2$$
$$\frac{x_1 g(x_1^2 - 2) - x_2 g(x_2^2 - 2)}{x_1 - x_2} = 0.$$

It turns out that the curve in $C_t \times C_t$ described by these equations is reducible. To see this, one can use

LEMMA 7. *Let p be a prime number. Consider the monic minimal polynomial $f \in \mathbf{Z}[X]$ of $\zeta_p + \zeta_p^{-1}$, where ζ_p is a primitive pth root of unity (in $\mathbf{C}$). Define $F(T) := Tf(T^2+2)$. Then*

$$F(X) - F(Y) = (X - Y) \cdot \prod_{k=1}^{(p-1)/2} (X^2 - \vartheta_k XY + Y^2 + 4 - \vartheta_k^2).$$

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

Here $\vartheta_k = \zeta_p^k + \zeta_p^{-k}$.

PROOF. Let Δ be the difference between the lefthand and righthand side of the formula above. For $i \in \mathbf{Z}$ define $\xi_i := \zeta_p^i - \zeta_p^{-1}$. Let $0 < i, j < p$ and $i \neq j$. One computes

$$\xi_i^2 - (\zeta_p^{i-j} + \zeta_p^{j-i})\xi_i\xi_j + \xi_j^2 + 4 - (\zeta_p^{i-j} + \zeta_p^{j-i})^2 = 0.$$

It follows that $\Delta(\xi_i, \xi_j) = 0$. Since the total degree of Δ is less than p, and $(\xi_i, \xi_j) \neq (\xi_k, \xi_l)$ whenever either $i \not\equiv k \bmod p$ or $j \not\equiv l \bmod p$ one concludes that $\Delta = 0$. ∎

Over the field k under consideration, choose i to be a square root of -1. The polynomial f from the lemma will be considered as a polynomial in $k[X]$. One has $f(X) = g(-X)$, hence (with $\vartheta_j = \zeta^j + \zeta^{-j}$)

$$\begin{aligned} &x_1 g(x_1^2 - 2) - x_2 g(x_2^2 - 2) \\ &\quad = x_1 f\big((ix_1)^2 + 2\big) - x_2 f\big((ix_2)^2 + 2\big) \\ &\quad = (-i)(ix_1 - ix_2) \cdot \prod_{j=1}^{(p-1)/2} \{(ix_1)^2 - \vartheta_j(ix_1)(ix_2) + (ix_2)^2 + 4 - \vartheta_j^2\} \\ &\quad = \pm(x_2 - x_1) \cdot \prod_{j=1}^{(p-1)/2} \{x_1^2 - \vartheta_j x_1 x_2 + x_2^2 - 4 + \vartheta_j^2\}. \end{aligned}$$

In terms of the description of $\varphi^{-1}(\Delta)$ given at the beginning of this section, it should be clear that each factor in the product given above corresponds to an irreducible component. One can use these to obtain endomorphisms of $\mathrm{Jac}(\mathcal{C}_t)$. The example $p = 5$ will be worked out below.

3.4 *Permutation polynomials.* We are now ready to prove Theorem 2. Given p prime and $g \in \mathbf{Z}[X]$ as before, consider for prime numbers ℓ the map

$$a \bmod \ell \longmapsto ag(a^2 - 2) \bmod \ell.$$

The theorem is easy for $p = 2$, hence suppose p is odd. Let $\zeta \in \bar{\mathbf{F}}_\ell$ be a primitive pth root of unity.

If $\alpha \neq \beta$ have the same image under the map we consider, this precisely means that for some j between 0 and $(p+1)/2$ one has

$$\alpha^2 - (\zeta^j + \zeta^{-j})\alpha\beta + \beta^2 = 4 - (\zeta^j + \zeta^{-j})^2.$$

By if necessary changing the choice of the primitive pth root of unity we may assume $j = 1$. In case $\ell \not\equiv \pm 1 \bmod p$ this means that $\zeta, \zeta^{-1}, \zeta^\ell$ and $\zeta^{-\ell}$ are the zeroes of an irreducible polynomial over $\mathbf{F}_\ell$. In particular this implies $\ell^4 \equiv 1 \bmod p$.

In case $p = 5$, the polynomial is $xg(x^2 - 2) = x^5 - 5x^3 + 5x$. The case $\ell = 2$ is easily checked. Assume $\ell > 2$ and write $x_1 = \xi_1 + \xi_2, x_2 = \xi_1 - \xi_2$. Then

$$\begin{aligned} &\frac{x_1^5 - 5x_1^3 + 5x_1 - x_2^5 + 5x_2^3 - 5x_2}{x_1 - x_2} \\ &\quad = \Big(\sqrt{5}\xi_1^2 + (\sqrt{5} - 2)\xi_2^2 + \frac{5 - 3\sqrt{5}}{2}\Big) \cdot \Big(\sqrt{5}\xi_1^2 + (\sqrt{5} + 2)\xi_2^2 - \frac{5 + 3\sqrt{5}}{2}\Big). \end{aligned}$$

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

A pair $\alpha \neq \beta \in \mathbf{F}_\ell$ such that $\alpha g(\alpha^2-2) = \beta g(\beta^2-2)$ yields a pair $(\xi_1, \xi_2) \in \mathbf{F}_\ell \times \mathbf{F}_\ell$ corresponding to a point on one of the two conics described above. Since 1 and $\sqrt{5} \in \mathbf{F}_{\ell^2}$ are linearly independent over $\mathbf{F}_\ell$, this would lead to $2\xi^2 = 5/2$ which is impossible since $\sqrt{5} \notin \mathbf{F}_\ell$ for $\ell \not\equiv \pm 1 \bmod 5$. ■

3.5 EXAMPLE: $p = 5$. In the special case $p = 5$ we now take a closer look at the correspondences on C_t mentioned above. As used in the previous section, write

$$g_1(\xi_1, \xi_2) = \sqrt{5}\xi_1^2 + (\sqrt{5}-2)\xi_2^2 + \frac{5-3\sqrt{5}}{2}.$$

Consider the correspondence Γ described locally by

$$\begin{aligned} y_1^2 &= x_1^5 - 5x_1^3 + 5x_1 + t \\ y_2^2 &= x_2^5 - 5x_2^3 + 5x_2 + t \\ y_1 &= y_2 \\ g_1\Big(\frac{x_1+x_2}{2}, \frac{x_1-x_2}{2}\Big) &= 0 \end{aligned}$$

For $i = 1, 2$ one has projections $\pi_i \colon \Gamma \longrightarrow C_t$ described by $(x_1, y_1, x_2, y_2) \longmapsto (x_i, y_i)$.

The fiber of π_2 over a point (x_2, y_2) consists of two points; their x_1-coordinate satisfies

$$\sqrt{5}(x_1+x_2)^2 + (\sqrt{5}-2)(x_1-x_2)^2 + 2(5-3\sqrt{5}) = 0.$$

It follows that the involution τ on Γ which interchanges the points in the fibers of π_2 is given by

$$\tau \colon (x_1, y_1, x_2, y_2) \longmapsto \Big(-x_1 - \Big(\frac{1}{2} + \frac{1}{2}\sqrt{5}\Big)x_2, y_1, x_2, y_2\Big).$$

The correspondence Γ yields an endomorphism of the jacobian of C_t whose tangent mapping on the tangent space at the origin can be computed as before on $H^0(C_t, \Omega^1_{C_t})$. It is given by

$$\omega \longmapsto \pi_1^*\omega + \tau^*\pi_1^*\omega.$$

A straightforward computation (using that

$$\{(\sqrt{5}-1)x_1 + x_2\}\, dx_1 = -\{x_1 + (\sqrt{5}-1)x_2\}\, dx_2$$

on Γ) reveals that on the basis $\{dx/y, x dx/y\}$ of $H^0(C_t, \Omega^1_{C_t})$ this tangent mapping is given by the matrix

$$\begin{pmatrix} -\frac{1}{2} - \frac{1}{2}\sqrt{5} & 0 \\ 0 & -\frac{1}{2} + \frac{1}{2}\sqrt{5} \end{pmatrix}$$

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press

REFERENCES

1. B. van Geemen and J. Werner, *Nodal Quintics in* $\mathbf{P}^4$, Math. Inst. R. U. Utrecht, 1989, preprint.

2. J. de Jong and R. Noot, *Jacobians with complex multiplication*, Math. Inst. R. U. Utrecht, 1989, preprint.

3. J. F. Mestre, *Courbes hyperelliptiques à multiplications reélles*, C. R. Acad. Sci. Paris, **307** Série I(1988), 721–724.

4. G. Shimura and Y. Taniyama, *Complex multiplication abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan **6**(1961).

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
K7L 3N6

Erasmus Univ. Rotterdam
Vakgroep Wiskunde
Postbus 1738
3000 DR Rotterdam
The Netherlands

Mathematisch Instituut
Rijksuniversiteit Utrecht
P.O. Box 80.010
3508 TA Utrecht
The Netherlands

https://doi.org/10.4153/CJM-1991-061-x Published online by Cambridge University Press