Families of Hyperelliptic Curves with Real Multiplication

Familles de courbes hyperelliptiques à multiplications réelles

Arithmetic algebraic geometry (Texel, 1989), Progr. Math. **89** (Birkhäuser Boston, 1991)

J.-F. Mestre

Translated from the French by Benjamin Smith

This version was compiled on February 9, 2012

For all integers n, we let G_n denote the polynomial

$$G_n(T) = \prod_{k=1}^{\lfloor n/2 \rfloor} \left(T - 2\cos\left(\frac{2k\pi}{n}\right)\right),$$

where $\lfloor x \rfloor$ denotes the integer part of x. We say that a curve C of genus $\lfloor n/2 \rfloor$, defined over a field k, has *real multiplication by* G_n if there exists a correspondence $\mathscr{C}$ on C such that G_n is the characteristic polynomial of the endomorphism induced by $\mathscr{C}$ on the regular differentials on C.

The endomorphism ring of the Jacobian J_C of such a curve C contains a subring isomorphic to $\mathbb{Z}[X]/(G_n(X))$ whose elements are invariant under the Rosati involution. In particular, if n is an odd prime, then J_C has real multiplication by $\mathbb{Z}[2\cos\frac{2\pi}{n}]$ in the usual terminology (see [9], for example).

In this article we construct, for all integers $n \geq 4$, a 2-dimensional family of hyperelliptic curves of genus $\lfloor n/2 \rfloor$ defined over $\mathbb{C}$ with real multiplication by G_n. More precisely, for every elliptic curve E defined over a field k of characteristic zero together with a k-rational cyclic subgroup G of order n we define a one-parameter family of hyperelliptic curves of genus $\lfloor n/2 \rfloor$ defined over k with real multiplication by G_n. If G is generated by a k-rational point, then the associated correspondence is k-rational.

In the case $n = 5$ we recover a known construction, due to Humbert (cf. for example [5, p. 374], [10, p. 20], and also [2]), which we recall here: let X be a curve of genus 2 whose Jacobian has real multiplication by $\mathbb{Z}[(1+\sqrt{5})/2]$, and let w be the hyperelliptic involution of X. Let C be a plane conic, and $f : X/\langle w \rangle \to C$ an isomorphism. If P is the image on C of a Weierstrass point of X, then there exists a numbering $P_1, \ldots, P_5$ of the images on C of the Weierstrass points of X not equal to P such that there exists a conic passing through P and inscribed in the pentagon formed by $P_1, \ldots, P_5$ (that is, tangent to the lines $P_1P_2, P_2P_3, \ldots, P_5P_1$). Comparing this statement with the elliptic curve-theoretic interpretation of Poncelet's theorem, we see that the data of X is equivalent to the data of an elliptic curve E with a point of order 5, a double covering ϕ from E to a curve of genus 0, and a point of this curve distinct from the 4 ramification points of ϕ.

We construct the family of hyperelliptic curves mentioned above in §1. More generally, for each isogeny $f : E_1 \to E_2$ of elliptic curves defined over a field k we define a hyperelliptic curve C_f over $k(T)$, where T is a free parameter; for each element R of the kernel of f there is an associated correspondence $\mathscr{C}_R$ on C_f, such that the characteristic polynomial of the endomorphism induced by $\mathscr{C}_R$ on the regular differentials on C_f is a product of polynomials G_m.

This construction allows us, for example, to obtain a 2-parameter family, defined over $\mathbb{Q}$, of hyperelliptic curves of genus 19 whose Jacobians are isogenous to a product of 19 elliptic curves.

We give some examples based on some isogenies with cyclic kernels in §2. For $n = 5, 7, 9$, the curve $X_1(n)$ classifying elliptic curves equipped with a point of order n is $\mathbb{Q}$-isomorphic to the projective line.

In these cases, we obtain a two-parameter family, defined over $\mathbb{Q}$, of curves of genus 2 (resp. 3, resp. 4) with real multiplication by G_5 (resp. G_7, resp. G_9). We give these families an explicit description, and examine also the case where $n = 13$: we derive a 2-parameter family, defined over $\mathbb{Q}$, of hyperelliptic curves of genus 6 whose Jacobians have real multiplication by G_{13}, but where the corresponding endomorphisms are not in general defined over $\mathbb{Q}$. We examine the curves C_f associated with isogenies f of even degree in §2.2. The fact that $X_1(8)$ (resp. $X_1(12)$) is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1$ implies the existence of a 2-parameter family, defined over $\mathbb{Q}$, of abelian surfaces with real multiplication by $\mathbb{Z}[\sqrt{2}]$ (resp. $\mathbb{Z}[\sqrt{3}]$).

In §3, we show that the preceding constructions permit us to obtain, for all primes $p \equiv \pm 2 \bmod 5$, a regular extension of $\mathbb{Q}(T)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_{p^2})$.

I would like to thank J.-P. Serre for the invaluable help that he kindly gave me throughout this work.

1 The curves C_f

Let E_1 and E_2 be two elliptic curves defined over a field k of characteristic zero, let x_1 (resp. x_2) be a function on E_1 (resp. E_2) with a double pole at 0_{E_1} (resp. 0_{E_2}), and let $f : E_1 \to E_2$ be an isogeny of degree n, defined over k, with kernel G.

Let u be the function of degree n such that the following diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{f} & E_2 \\ {\scriptstyle x_1}\downarrow & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1 & \xrightarrow{u} & \mathbb{P}^1 \end{array}$$

We say that u is the "abscissa function"[1] of f. We let C_f denote the hyperelliptic curve over $K = k(T)$, where T is a free parameter, defined by the affine equation

$$C_f : y^2 = u(x) - T.$$

If P_T is a point of $E_1(\overline{K})$ such that $x_2(f(P_T)) = T$, then C_f is a double covering of $\mathbb{P}^1$ ramified at the points $x_1(P_T + R)$ for each R in G, and at the points $x_1(S)$ for each point S in G satisfying $[2]S = 0$. As a result, we have the following proposition.

Proposition 1. *The genus of the hyperelliptic curve C_f is equal to $(n+m-1)/2$, where n is the cardinality of G, and m is the number of points of order 2 of G.*

1.1 The covering associated with the composition of two isogenies

Let E_1, E_2 and E_3 be three elliptic curves, and for each $i = 1,2,3$ let x_i be a function of order 2 on E_i with a double pole at 0_{E_i}. If $f_1 : E_1 \to E_2$ is an isogeny of degree n_1 and $f_2 : E_2 \to E_3$ an isogeny of degree n_2, then we let f denote the isogeny $f_2 \circ f_1 : E_1 \to E_3$, and we let u (resp. u_1, resp. u_2) denote the abscissa function of f (resp. f_1, resp. f_2). We have $u = u_2 \circ u_1$.

The mapping

$$(x, y) \mapsto (u_1(x), y)$$

defines a degree-n_1 covering from the curve $C_f : y^2 = u(x) - T$ to the curve $C_{f_2} : y^2 = u_2(x) - T$. This allows us to partially reduce the study of the curves C_f to the study of the various curves C_g, where g is an isogeny factoring f.

Example 1. Let E be an elliptic curve, and $f : E \to E$ the multiplication by 6 map on E. The genus of C_f is 19, and there exist 19 isogenies $g : F \to E$ with cyclic kernel such that there exists an isogeny $h : E \to F$ with $g \circ h = [6]$:

- Three of degree 2: the associated curves C_g have genus 1; we denote them E_1, E_2, E_3.

[1] *"équation aux abscisses"* in the original

- Four of degree 3: the associated curves C_g also have genus 1; we denote them F_1, F_2, F_3, F_4.
- Finally, the other twelve are of degree 6: the associated curves C_g have genus 3, and each covers a curve corresponding to a 2-isogeny and a curve corresponding to a 3-isogeny. The Jacobian of C_g is therefore isogenous to a product of three elliptic curves: one of type E_i, one of type F_i, and one new curve, which we denote G_i (for $i = 1, \ldots, 12$).

In this way we obtain a homomorphism

$$J_{C_f} \to \prod E_i \times \prod F_i \times \prod G_i,$$

defined over $k'(T)$, where k' is the extension of k obtained by adjoining the points of order 6. This homomorphism is an isogeny; we may prove this using the correspondences on C_f defined in §1.2 and §1.3, for example.

Theorem 1. *Let E be an elliptic curve defined over a field k of characteristic zero, and x a function of degree 2 on E with a double pole at 0_E. Let u be the rational function of degree 36 such that $x([6]P) = u(x(P))$ for all points P of E. Then the hyperelliptic curve defined by the affine model*

$$Y^2 = u(X) - T$$

(where T is a free parameter) has genus 19, and its Jacobian is isogenous to a product of 19 elliptic curves.

1.2 Involutions of C_f associated with points of order 2 of G

Suppose that the order n of G is even. Let R in G be a point of order 2 of the curve E_1. The involution of E_1 given by $P \mapsto P+R$ commutes with the involution $P \mapsto -P$, so $x_1(P+R)$ is a rational function of $x_1(P)$, and is an involution: there exist a, b, and c such that

$$x_1(P+R) = \frac{ax_1(P)+b}{cx_1(P)-a}.$$

Therefore, let $\mathscr{C}_R : C_f \to C_f$ be the involution defined by

$$\mathscr{C}_R : (x, y) \mapsto \left(\frac{ax+b}{cx-a}, y\right).$$

If we let $F = E_1/\langle R\rangle$, with $h : E_1 \to F$ the canonical morphism, then $f = g \circ h$ for some isogeny $g : F \to E_2$. The quotient $C_f/\langle\mathscr{C}_R\rangle$ is thus isomorphic to the curve C_g.

Let x_3 be a function on F of degree 2 with a double pole at 0_F, and let u be the abscissa function of g. The curve C_g then has an equation of the form

$$C_g : y^2 = u(x) - T.$$

Now, let S be a point of E_1 such that $[2]S = R$, and Q a point of order 2 on E_1 distinct from R. The curve $C_f/\langle w \circ \mathscr{C}_R\rangle$, where w is the hyperelliptic involution of C_f, has an equation of the form

$$C_f/\langle w \circ \mathscr{C}_R\rangle : y^2 = (u(x) - T)(x - x_3(h(S)))(x - x_3(h(S+Q))).$$

Let g be the genus of C_f. If g is even, then the genera of $C_f/\mathscr{C}_R$ and $C_f/(w\circ\mathscr{C}_R)$ are equal; otherwise, they are respectively equal to $(g-1)/2$ and $(g+1)/2$.

1.3 Correspondences on C_f associated with points of order > 2 of G

Let $f : E_1 \to E_2$ be an isogeny of degree n (not necessarily even) with kernel G, and let u be the abscissa function of f. For all points P of E_1 and for all points R of G, we have

$$u(x_1(P+R)) = u(x_1(P)).$$

Moreover, the functions $P \mapsto x_1(P+R)+x_1(P-R)$ and $P \mapsto x_1(P+R)x_1(P-R)$ are invariant under the involution $P \mapsto -P$, and so are rational functions in x_1 defined over $k(x_1(R))$. We denote these functions s and p. If Z is a parameter, then

$$(Z - x_1(P+R))(Z - x_1(P-R)) = Z^2 - s(x_1(P))Z + p(x_1(P)).$$

For the moment, let R be a point of G of order > 2. The equation above allows us to associate with R the symmetric $2-2$ correspondence $\mathscr{C}_R \subset C_f \times C_f$, defined over $k(x_1(R))(T)$ by the equations

$$y^2 = u(x) - T, \quad Y^2 = u(X) - T, \quad X^2 - s(x)X + p(x) = 0, \quad Y = y. \tag{1}$$

Let $P = (x, y)$ be a point on C_f; if Q is a point of E_1 such that $x = x_1(Q)$, then the image of the divisor (P) under the endomorphism of $\mathrm{Pic}(C_f)$ associated with $\mathscr{C}_R$ is $((x_1(Q+R), y)) + ((x_1(Q-R), y))$.

1.4 Action of the correspondence $\mathscr{C}_R$ on $\Omega^1(C_f)$

For all R in G, we let w_R denote the regular differential on C_f defined by

$$w_R = \frac{1}{x - x_1(R)} \frac{dx}{y}.$$

(By convention, we set $w_0 = 0$.) We have $w_S = w_R$ if and only if $R = \pm S$. The set of forms $\{w_R : R \in G \setminus \{0\}\}$ is a basis of $\Omega^1(C_f)$.

To examine the action of the correspondences $\mathscr{C}_R$ on $\Omega^1(C_f)$, we will need the following lemma:

Lemma 1. *The function F which maps the three points P, Q, R of E to*

$$F(P, Q, R) = (x_1(P) - x_1(Q-R))(x_1(P) - x_1(Q+R))(x_1(Q) - x_1(R))^2$$

is symmetric in P, Q and R.

Proof. It is clear that the permutation $Q \leftrightarrow R$ does not change the expression above. It is the same when we permute P and Q. Indeed, Q and R being fixed, the functions f and g defined respectively by

$$f(P) = (x_1(P) - x_1(Q-R))(x_1(P) - x_1(Q+R))(x_1(Q) - x_1(R))^2$$

and

$$g(P) = (x_1(Q) - x_1(P-R))(x_1(Q) - x_1(P+R))(x_1(P) - x_1(R))^2$$

have the same divisor $(Q-R)+(Q+R)+(-Q-R)+(-Q+R)$, so f and g are proportional. Letting P tend towards 0, we deduce that $f = g$. □

When E_1 is defined over $\mathbb{C}$, Lemma 1 is a consequence of the formula

$$\wp(u) - \wp(v) = \sigma(u+v)\sigma(u-v)\sigma^{-2}(u)\sigma^{-2}(v),$$

and of the fact that the function σ is odd. Indeed,

$$\begin{aligned}
&(\wp(u) - \wp(v-w))(\wp(u) - \wp(v+w))(\wp(v) - \wp(w))^2 \\
&= \sigma(u+v+w)\sigma(u+v-w)\sigma(-u+v-w)\sigma(-u+v+w)\sigma^{-4}(u)\sigma^{-4}(v)\sigma^{-4}(w) \\
&= -\sigma(u+v+w)\sigma(u+v-w)\sigma(u-v+w)\sigma(v-u+w)\sigma^{-4}(u)\sigma^{-4}(v)\sigma^{-4}(w)
\end{aligned}$$

is an expression symmetric in u, v and w. By the principle of extension of algebraic identities, we may deduce the same result for arbitrary fields k.

Recall that the endomorphism T_R of $\Omega^1(C_f)$ associated with the correspondence $\mathscr{C}_R$ is $\mathrm{Tr} \circ p_1^*$, where $p_1 : \mathscr{C}_R \to C_f$ is the first projection and $\mathrm{Tr} : \Omega^1(\mathscr{C}_R) \to \Omega^1(C_f)$ is the trace associated with the second projection.

We set $z = x_1(P)$, $z_1 = x_1(P-R)$ and $z_2 = x_1(P+R)$. For all pairs of points (P, Q) on E_1, we have

$$(z - x_1(Q-R))(z - x_1(Q+R))(x_1(Q) - x_1(R))^2 = (z_1 - x_1(Q))(z_2 - x_1(Q))(z - x_1(R))^2.$$

Taking the logarithmic derivative of this expression, we obtain

$$\frac{dz_1}{z_1 - x_1(Q)} + \frac{dz_2}{z_2 - x_1(Q)} = \frac{dz}{z - x_1(Q-R)} + \frac{dz}{z - x_1(Q+R)} - 2\frac{dz}{z - x_1(R)}.$$

Since

$$T_R(\omega_Q) = T_R(\frac{1}{z - x_1(Q)}\frac{dz}{y}) = \frac{1}{z_1 - x_1(Q)}\frac{dz_1}{y} + \frac{1}{z_2 - x_1(Q)}\frac{dz_2}{y},$$

maintaining the convention $\omega_0 = 0$ we have

$$T_R(\omega_Q) = \omega_{Q-R} + \omega_{Q+R} - 2\omega_R.$$

Proposition 2. *With the notation above, the correspondence $\mathscr{C}_R$ acts on $\Omega^1(C_f)$ by*

$$\omega_Q \mapsto \omega_{Q-R} + \omega_{Q+R} - 2\omega_R.$$

1.5 The case where G is cyclic of order n

Suppose for the moment that G is a cyclic group of order n, and let R be a generator of G.

For all W in G, we set $v_S = \omega_{S-R} - \omega_{S+R}$. Note that $v_{-S} = -v_S$, so $v_S = 0$ if and only if $[2]S = 0$. The subspace $\Omega' := \langle v_S : S \in G\rangle$ of $\Omega^1(C_f)$ is stabilized by T_R. More precisely,

$$T_R(v_S) = v_{S+R} + v_{S-R}.$$

If n is odd, then we easily verify that Ω' is equal to the whole of $\Omega^1(C_f)$. It is then clear that the endomorphism T_R of $\Omega^1(C_f)$ has characteristic polynomial

$$G_n(X) = \prod_{k=1}^{(n-1)/2} \left(X - 2\cos\frac{2k\pi}{n}\right).$$

If n is even, then the space Ω' has dimension $(n-2)/2$. We then set

$$w = \omega_{[\frac{n}{2}]R} + 2(-1)^{n/2} \sum_{i=1}^{(n-2)/2} (-1)^i \omega_{[i]R}.$$

We immediately verify that $T_R(w) = -2w$, and that $\Omega^1(C_f)$ is the direct sum of Ω' and the line generated by w. The characteristic polynomial of T_R acting on Ω' is equal to

$$\prod_{k=1}^{(n-2)/2} \left(X - 2\cos\frac{2k\pi}{n}\right),$$

so the characteristic polynomial of T_R acting on $\Omega^1(C_f)$ is equal to

$$\prod_{k=1}^{n/2} \left(X - 2\cos\frac{2k\pi}{n}\right).$$

Proposition 3. *Let $f : E_1 \to E_2$ be an n-isogeny with cyclic kernel G. The characteristic polynomial of the correspondence $\mathscr{C}_R$ acting on $\Omega^1(C_f)$ is equal to*

$$G_n(X) = \prod_{k=1}^{\lfloor n/2\rfloor} \left(X - 2\cos\frac{2k\pi}{n}\right).$$

Remark. Let Z be the normalization of the fibre product of E_1 and C_f with respect to the coverings $x_1 : E_1 \to \mathbb{P}^1$ and $x : C_f \to \mathbb{P}^1$. If E_1 is defined by the equation $z^2 = h(x)$, where h has degree 3, then a system of affine equations for Z is for example given in $\mathbb{P}^3$ by

$$z^2 = h(x), \quad y^2 = u(x).$$

For each point R in G, we may define an automorphism ϕ_R of Z of order equal to the order of R, setting $\phi(x,y,z) = (x(P+R), y, z(P+R))$, where P is the image of (x,y,z) under the projection of Z onto E_1.

Moreover, let v be the involution of Z given by $(x,y,z) \mapsto (x,y,-z)$, and let G' be the group of automorphisms of Z generated by G and v. The curve C_f is the quotient $Z/\langle v \rangle$, and

$$v \circ \phi_R \circ v = \phi_{-R}.$$

The correspondences $\mathscr{C}_R$ are none other than the images under $Z \to C_f$ of the graph correspondence of ϕ_R in $Z \times Z$. If G is cyclic of order n, then G' is the dihedral group D_n, and we find again that the characteristic polynomial of $\mathscr{C}_R$ acting on $\Omega^1(C_f)$ is G_n.

This point of view has already been developed by A. Brumer [3].

2 Examples

We find in Kubert [6, p. 217] a description of the modular curves $X_1(n)$ of genus 0, classifying the pairs (E, R) formed by an elliptic curve E together with a point R of order n, and an explicit parametrisation of these pairs. Following the preceding section, every such pair has an associated one-parameter family of hyperelliptic curves with real multiplication by G_n. Further, if E_1 is an elliptic curve defined over a field k and G is a finite subgroup of $E_1(\overline{k})$, then the formulæ allowing us to explicitly obtain the quotient curve $E_2 = E_1/G$ and an isogeny $f : E_1 \to E_2$ with kernel G have been established by Vélu [11].

2.1 Examples with n odd

The case $n = 5$

The modular curve $X_1(5)$ is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1$. If E_1 is defined by $y^2 + (1-U)xy - Uy = x^3 - Ux^2$, then the point $R = (0,0)$ of E_1 has order 5. The formulæ giving the isogeny f and the quotient curve $E_2 = E_1/\ker f$ appear in [7] (for example). We find then the family of hyperelliptic curves

$$C_5(U,T) : Y^2 = (1-Z)^3 + UZ((1-Z)^3 + UZ^2 - Z^3(1-Z)) - TZ^2(Z-1)^2.$$

The case $n = 7$

In the case of $X_1(7)$, the analogous calculations give a family of curves $C_7(U,T)$ with real multiplication by G_7, defined by

$$\begin{aligned} C_7(U,T) : Y^2 = {} & U(U-1)Z^7 - 2U(U^2-1)Z^6 + (1 - 7U + 5U^2 - 3U^3 + 2U^4 + U^5)Z^5 \\ & - U(6U^4 - 9U^3 + 12U^2 - 13U - 1)Z^4 + U(U^5 + U^4 + 4U^3 - 8U^2 - 7U - 1)Z^3 \\ & - U^2(3U^2 - 2U^2 - 8U - 3)Z^2 + U^3(U^2 - 3U - 3)Z + U^4 - TZ^2(Z-U)^2(Z-1)^2, \end{aligned}$$

where U is the parameter of $X_1(7)$ adopted in [7].

The case $n = 9$

We find in [6, p.217] a parametrisation of elliptic curves equipped with a point of order 9: the point $(0,0)$ has order 9 on the elliptic curve defined by

$$y^2 - (U^3 - U^2 - 1)xy - U^2(U-1)(U^2 - U + 1)y = x^3 - U^2(U-1)(U^2 - U + 2)x^2,$$

where U is the parameter of $X_1(9)$.

Vélu's formulæ give an equation for the associated family of hyperelliptic curves $C_9(U,T)$ of genus 4:

$$\begin{aligned} Y^2 = {} & U^4(U-1)(U^2-U+1)^3 Z^9 - 2U^3(U-1)(U^2-U+1)^2(U^3+U+1)Z^8 \\ & + U(U^2-U+1)(U^9 + U^8 - 7U^7 + 23U^6 - 39U^5 + 50U^4 - 44U^3 + 23U^2 - 10U + 1)Z^7 \\ & - (6U^{10} - 22U^9 + 67U^8 - 154U^7 + 279U^6 - 369U^5 + 353U^4 - 243U^3 + 107U^2 - 32U + 1)Z^6 \\ & + (U^{11} - 2U^{10} + 25U^9 - 91U^8 + 209U^7 - 312U^6 + 232U^5 - 237U^4 + 101U^3 - 32U^2 - 5U - 1)Z^5 \\ & - (6U^9 - 19U^8 + 51U^7 - 83U^6 + 97U^5 - 83U^4 + 29U^3 - 17U^2 - 11U + 5)Z^4 \\ & + (U^8 + U^6 + 5U^5 - 12U^4 + 2U^3 - 14U^2 - 8U - 10)Z^3 - (3U^5 - 5U^4 + 4U^3 - 11U^2 - 2U + 10)Z^2 \\ & + (U^3 - 3U^2 - 5)Z + 1 - T\left(Z(Z-1)((U^2-U+1)Z-1)(UZ-1)\right)^2. \end{aligned}$$

We have $G_9(X) = (X+1)(X^3-3X+1)$, so the Jacobian of each curve in the family $C_9(U,T)$ contains a 3-dimensional abelian variety with real multiplication by $\mathbb{Z}[2\cos\frac{2\pi}{9}]$.

The case $n = 13$

The curve $X_0(13)$ classifying elliptic curves equipped with a cyclic subgroup of order 13 is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1$. Each point of $\mathbb{P}^1(\mathbb{Q}) \cong X_0(13)(\mathbb{Q})$ that is not a cusp is associated with an elliptic curve E_1 having a $\mathbb{Q}$-rational cyclic subgroup G of order 13, and hence an isogeny $f : E_1 \to E_2 = E_1/G$ defined over $\mathbb{Q}$. If the abscissa function of f is $p(x)/q^2(x)$ and T is a parameter, then we deduce as before that the hyperelliptic curve of genus 6 defined by $z^2 = p(x) - Tq^2(x)$ has real multiplication by G_{13}. If a point R in G is defined over an extension k of $\mathbb{Q}$, then the correspondence $\mathscr{C}_R$ and its induced endomorphism on the Jacobian are defined over k. But $X_1(13)$ has no rational points over $\mathbb{Q}$ that are not cusps, so the correspondence $\mathscr{C}_R$ is never defined over $\mathbb{Q}$.

2.2 Examples with n even

Let $f : E_1 \to E_2$ be an isogeny of degree n with cyclic kernel, and let R be a generator of $\ker f$. Let $R_2 = [n/2]R$, set $E_3 = E_1/\langle R_2\rangle$, and let $g : E_3 \to E_2$ be the isogeny of degree $n/2$ derived from f as in §1.2. We have seen that if $s = \mathscr{C}_R$ is constructed as in §1.2, then the curve C_f/s is none other than C_g. More precisely, let x_3 be a function of degree 2 on E_3 with a double pole at 0, and u the abscissa function of g. The curve C_g has a defining equation

$$C_g : y^2 = u(x) - T.$$

Similarly, the curve $C' = C_f/(w \circ s)$, where w is the hyperelliptic involution of C_f, is defined by

$$C' : y^2 = (u(x) - T)(x-a)(x-b),$$

where a and b are the abscissæ of the appropriate points of order 2 of E_3 (cf. §1.2).

The case $n = 8$

In this case C_f has genus 4, and C_g and C' have genus 2. The characteristic polynomial of $\mathscr{C}_R$ is the polynomial $X(X+2)(X^2-2)$. The isogeny g factors into a product of two isogenies of degree 2, so the Jacobian of C_g is isogenous to a product of 2 elliptic curves, while the Jacobian of C' has real multiplication by $\mathbb{Z}[\sqrt{2}]$.

The curve $X_1(8)$ is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1$. It follows that *there exists a two-parameter family, defined over* $\mathbb{Q}$*, of abelian surfaces with real multiplication by* $\mathbb{Z}[\sqrt{2}]$.

To make this explicit, a family $C_4(U,T)$ in two parameters U and T of curves of genus 2 whose Jacobians have real multiplication by $\mathbb{Z}[\sqrt{2}]$ is given by

$$\begin{aligned} C_4(U,T) : Y^2 = &\left((U^2+1)^2X + U + 1\right)\left((U-1)^2(U+1)X + 1\right) \\ &\cdot\left(U^2(U-1)^2(U^2+1)X - T + \frac{(U^2+1)^2}{X} + \frac{(U+1)}{X^2} + \frac{U^2(U^2-1)^2}{(U^2+1)^2X+U+1}\right). \end{aligned}$$

Remark. In the same way, we find another result of Humbert [5, p. 379]: let X be a curve of genus 2, v its hyperelliptic involution, C a nondegenerate conic, and $\phi : X/v \to C$ an isomorphism. Let $P_1, \ldots, P_6$ be the images under ϕ of the Weierstrass points of X. The Jacobian of X has real multiplication by $\mathbb{Z}[\sqrt{2}]$ if and only if there exists a conic passing through P_1 and P_2 and inscribed in one of the quadrilaterals formed by P_3, P_4, P_5, and P_6. Through the elliptic curve-theoretic interpretation of Poncelet's theorem, such a configuration is equivalent to the data of an elliptic curve together with a point R of order 4 and a point of order 2 distinct from $2R$, and therefore to giving a curve of the same type as C'.

The case $n = 12$

Let $f : E_1 \to E_2$ be an isogeny of degree 12 with cyclic kernel, and let R be a generator of $\ker f$. The curve C_f has genus 6, and the characteristic polynomial of $\mathscr{C}_R$ acting on the regular differentials on C_f

is equal to $X(X+2)(X-1)(X+1)(X^2-3)$. If ϕ is the endomorphism of J_{C_f} induced by $\mathscr{C}_R$, then the abelian variety $A_f := \phi(\phi+2)(\phi^2-1)(J_{C_f})$ has real multiplication by $\mathbb{Z}[\sqrt{3}]$.

The curve $X_1(12)$ is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1$. It follows that *there exists a two-parameter family, defined over* $\mathbb{Q}$, *of abelian surfaces with real multiplication by* $\mathbb{Z}[\sqrt{3}]$.

Here again we may make the two-parameter family explicit, by using Kubert's parametrization of $X_1(12)$ together with Vélu's formulæ. We satisfy ourselves here with an example, since we find the general formula a little tedious to write:

Let E be the elliptic curve labelled $90G$ in the tables of [1, p. 92], for which a defining equation is

$$E : y^2 + xy + x = x^3 - x^2 - 122x + 1721.$$

Its Mordell–Weil group is cyclic of order 12, generated by the point $(-9, 49)$. Using Vélu's formulæ, we find that the equation of the corresponding hyperelliptic curve $C_3(T)$ is

$$\begin{aligned} C_3(T) : Y^2 = (X+2)\big(&432X^{12} - 2988X^{11} + 118326X^{10} - 308497X^9 - 448605X^8 - 779631X^7 + 2899412X^6 \\ &+ 5715072X^5 + 2532888X^4 - 304560X^3 + 134784X^2 + 279936X + 93312\big) \\ &- T\,(X(X+2)(X-6)(3X+2)(2X+3)(X-1))^2, \end{aligned}$$

where T is a parameter.

We let $A_3(T)$ denote the abelian subvariety of $J_{C_3(T)}$ with real multiplication by $\mathbb{Z}[\sqrt{3}]$.

Remark. Let $f : E_1 \to E_2$ be an isogeny of degree 12 with cyclic kernel. The curves C_g and C' constructed by the method given at the start of this section are of genus 3. Here the isogeny g has degree 6, so the Jacobian of C_g is isogenous to the product of two elliptic curves. The Jacobian of C' is isogenous to the product of an elliptic curve and an abelian surface with real multiplication by $\mathbb{Z}[\sqrt{3}]$. Conversely, all abelian surfaces that have real multiplication by $\mathbb{Z}[\sqrt{3}]$ may be obtained by the construction above, starting from an elliptic curve with a point R of order 6 and a point of order 2 distinct from $3R$.

3 Application: constructing regular extensions of $\mathbb{Q}(T)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_{p^2})$

Let A be an abelian surface defined over $\mathbb{Q}(T)$, non-constant (i.e. with non-constant moduli), and whose ring of $\mathbb{Q}(T)$-endomorphisms contains a subring isomorphic to the ring of integers of a quadratic real field M. Let $A[p]$ denote the p-torsion subgroup of A, and G the Galois group of the extension $L/\mathbb{Q}(T)$, where $L = \mathbb{Q}(T)(A[p])$. If p is inert in M, then $A[p]$ is a 2-dimensional $\mathbb{F}_{p^2}$-vector space, and G is isomorphic to a subgroup of the the subgroup $\mathrm{GL}'_2(\mathbb{F}_{p^2})$ of $\mathrm{GL}_2(\mathbb{F}_{p^2})$ formed by the matrices whose determinant is in $\mathbb{F}_p^*$. We easily see that the image of $\mathrm{GL}'_2(\mathbb{F}_{p^2})$ in $\mathrm{PGL}_2(\mathbb{F}_{p^2})$ is equal to $\mathrm{PSL}_2(\mathbb{F}_{p^2})$.

It follows, if $G = \mathrm{GL}'_2(\mathbb{F}_{p^2})$, that the subfield M of L fixed by the scalar matrices of G is a non-constant (and hence regular) extension of $\mathbb{Q}(T)$. However, for this to be true it is enough that for one specialisation t in $\mathbb{Q}$ of T the p-torsion points of the specialisation corresponding to A generate an extension of $\mathbb{Q}$ with Galois group $\mathrm{GL}'_2(\mathbb{F}_{p^2})$.

Some of the families of hyperelliptic curves with real multiplication described in the preceding sections allow us to construct such extensions. Consider, for example, the family $C_5(U, T)$ above. We have shown in [8] that for all odd $p \equiv \pm 2 \bmod 5$, the Galois group of the p-torsion points of the Jacobian of $C_5(-17/4, 1)$ is equal to $\mathrm{GL}'_2(\mathbb{F}_{p^2})$, whence the following theorem:

Theorem 2. *For all primes* $p \equiv \pm 2 \bmod 5$, *there exists a regular extension of* $\mathbb{Q}(T)$ *with Galois group* $\mathrm{PSL}_2(\mathbb{F}_{p^2})$.

Remark (1). W. Feit [4] has already given a proof of this theorem, except that it remained to prove that a certain curve of genus 0 has a rational point; J.-P. Serre has recently proven this. Feit's method is different to the one presented here.

Remark (2). By an analogous method, we can prove that, *for all sufficiently large primes* $p \not\equiv \pm 1 \bmod 24$, *there exists a regular etension of* $\mathbb{Q}(T)$ *with Galois group* $\mathrm{PSL}_2(\mathbb{F}_{p^2})$. By a theorem of Ribet [9, p. 801, Theorem 5.5.2], it suffices to give one curve in each of the two families $C_4(U, T)$ and $C_3(T)$ of the previous section that does not have everywhere potentially good reduction. For example, take the curve $C_4(2,12)$ from the family $C_4(U,T)$ above, defined by

$$C_4(2,12): Y^2 = 12X^5 + 20X^4 + 75X^3 + 215X^2 + 177X + 45.$$

The discriminant of its hyperelliptic polynomial is $2^{12} \cdot 3^4 \cdot 1201^3$, and its reduction mod 1201 is the curve defined by

$$Y^2 = 12(X - 1125)(X - 239)^2(X - 799)^2.$$

Thus the curve $C_4(2,12)$ does not have potentially good reduction at 1201, and we may apply Ribet's theorem (cited above): for all p sufficiently large, $p \equiv \pm 3 \bmod 8$, the Galois group of the extension of $\mathbb{Q}$ obtained by adjoining the p-torsion points of the Jacobian of $C_4(2,12)$ is equal to $\mathrm{GL}_2'(\mathbb{F}_{p^2})$.

We proceed in the same way with $C_3(T)$: for all rational numbers t, and all primes $l > 5$ strictly dividing the denominator of t, the reduction of the curve $C_3(t)$ is stable at l and also completely toric. Take, for example, $C_3(1/7)$. Applying Ribet's theorem, we see that for all sufficiently large $p \equiv \pm 5 \bmod 12$ the Galois group of the extension of $\mathbb{Q}$ obtained by adjoining the p-torsion points of the abelian variety $A_3(1/7)$ is equal to $\mathrm{GL}_2(\mathbb{F}_{p^2})$.

In fact, it is probable that, for *all* $p \equiv \pm 3 \bmod 8$ (resp. $p \equiv \pm 5 \bmod 12$), the Galois group of the points of order p of $J_{C_4(2,12)}$ (resp. of $A_3(1/7)$) is equal to $\mathrm{GL}_2'(\mathbb{F}_{p^2})$. To show this would require a detailed study of the curves $C_4(2,12)$ and $C_3(1/7)$, analogous to those of [8, Section 2].

References

[1] Numerical tables on elliptic curves, in: Modular Functions of One Variable IV, *Lecture Notes in Math.* **476** (1975), 74–144.

[2] W. Barth and R. Moore, Geometry in the space of Horrocks–Mumford surfaces, *Topology.* **28** (1989), 231–245.

[3] A. Brumer, Courbes à automorphismes et courbes à multiplications réelles, *unpublished.*

[4] W. Feit, Rigidity of Aut(PSL$_2(p^2)$), $p \equiv \pm 2 \pmod 5$, $p \neq 2$, In: *Proceedings of the Rutgers group theory year, 1983–1984,* Cambridge Univ. Press (1984), 351–356.

[5] G. Humbert, *Oeuvres.* Volume II, Gauthier–Villars (1936).

[6] D. S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (3).* **33** (1976), 193–237.

[7] J.-F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, *J. Reine Angew. Math.* **343** (1983), 23–35.

[8] J.-F. Mestre, Courbes hyperelliptiques à multiplications réelles, *C. R. Ac. Sc. Paris.* **307** (1988), 721–724.

[9] K. Ribet, Galois action on division points of abelian varieties with real multiplications, *Amer. J. of Math.* **98** (1976), 751–804.

[10] G. van der Geer, *Hilbert Modular Surfaces.* Springer–Verlag (1988).

[11] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris.* **273** (1971), 238–241.