NOTES DEL SEMINARI

teori
adeno
mbres
ub·uab·upc

CORBES DE GÈNERE 3

Barcelona, 2006

14

Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)

CORBES DE GÈNERE 3

Edició a cura de

E. Nart

Amb contribucions de

F. Bars
J. Guardia

G. Cardona
E. Nart

J. Fernández
R. Oyono
C. Ritzenthaler

E. Nart

Fac.de Ciències
Univ. Autònoma de Barcelona
Dep. de Matemàtiques
08193 Bellaterra
Espanya

Classificació AMS
Primària: 11G20, 14G25, 11G10, 14H45
Secundària: 11H50, 14G15

Barcelona, 2006
Amb suport parcial de MCYT, BFM-2003-06092

ISBN: 84-923250-7-0

Índex

Capítol 1

Bitangents and theta characteristics of plane quartics

Enric Nart

1.1 Curves of genus 3

Let C be a projective, smooth, geometrically irreducible curve, of genus $g > 1$, defined over an algebraically closed field k.

Let K be a canonical divisor of C, that is, $K = \operatorname{div}(\omega)$ for some regular differential $\omega \in \Omega^1(C)$. By the Riemann-Roch theorem:

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g,$$

where $\ell(D) = \dim\{f \in k(C) \mid f = 0 \text{ or } \operatorname{div}(f) + D \geq 0\}$. We have

$$\deg(K) = 2g - 2, \quad \ell(K) = g.$$

For any $P \in C$, if we subtract the Riemann-Roch formulas corresponding to the divisors $D + P$ and D, we get:

$$(\ell(D + P) - \ell(D)) + (\ell(K - D) - \ell(K - D - P)) = 1. \qquad (1.1)$$

Since both summands are non-negative integers, one of them is 0 and the other one is 1.

Weierstrass points

In this subsection we assume that $\mathrm{char}(k) = 0$.

Let us fix a point $P \in C$. An integer $1 \leq m \leq 2g-1$ is said to be a *gap* at P if it satisfies any of the following equivalent conditions:

1. $\ell((m-1)P) = \ell(mP)$
2. $\mathrm{div}_\infty(f) \neq mP$, $\forall f \in k(C)^*$
3. $\ell(K-(m-1)P) > \ell(K-mP)$
4. $\exists\, \omega \in \Omega^1(C)$ such that $\mathrm{ord}_P(\omega) = m-1$

Clearly, $1 \Leftrightarrow 2$ and $3 \Leftrightarrow 4$. By (1.1) we get $1 \Leftrightarrow 3$ too.

By the Riemann-Roch formula, we have:

$$1 = \ell(0) \leq \ell(P) \leq \ell(2P) \leq \cdots \leq \ell((2g-1)P) = g.$$

Hence, in this chain there are $g-1$ strict inequalities and g equalities, so that any point P has a succession of g gaps:

$$1 \leq m_1 < m_2 < \cdots < m_g \leq 2g-1.$$

We define the *weight* of the point P by:

$$w(P) := (m_1 - 1) + (m_2 - 1) + \cdots + (m_g - 1).$$

We say that P is *ordinary* if any of the following equivalent conditions is satisfied:

1. $w(P) = 0$
2. the succession of gaps at P is $1, 2, \ldots, g$
3. $\ell(gP) = 1$

Thus, the weight of P measures how far is P from being ordinary. A non-ordinary point is called a *Weierstrass point.* There are only a finite number of Weierstrass points:

1.1.1 Theorem. $\sum_{P\in C} w(P) = (g-1)g(g+1)$.

The non-gaps in $\mathbb{Z}_+$ form a subsemigroup:

$$\operatorname{div}_\infty(f) = m,\ \operatorname{div}_\infty(g) = n \Longrightarrow \operatorname{div}_\infty(fg) = m+n.$$

Hence,

$$2 \text{ non-gap at } P \Longleftrightarrow \text{the succession of gaps at } P \text{ is } 1, 3, \ldots, 2g-1.$$

1.1.2 Theorem. *The following conditions are equivalent:*

1. *C is hyperelliptic*
2. *2 is a non-gap at all Weierstrass points of C*
3. *2 is a non-gap at some Weierstrass points of C*

PROOF: If C is hyperelliptic, we have $\ell(2P) = 2$ for all Weierstrass points. Conversely, if $\ell(2P) = 2$ for one single P, there is some function f with $\operatorname{div}_\infty(f) = 2P$ and it determines a morphism $f\colon C \longrightarrow \mathbb{P}^1$ of degree two. □

Thus, for a genus 3 curve we have two different situations concerning the Weierstrass points. If C is hyperelliptic, it has 8 Weierstrass points of weight 3 and succession of gaps 1,3,5. If C is not hyperelliptic, it has (say) N Weierstrass points of weight 1 (and succession of gaps 1,2,4) and M Weierstrass points of weight 2 (and succession of gaps 1,2,5), with $N + 2M = 24$.

Canonical morphism

The canonical divisor has no base-points. In fact, by (1.1) applied to the divisor $D = 0$,

$$\ell(K) = \ell(K-P) \Longrightarrow \ell(P) = 2 \Longrightarrow g = 0,$$

since there would exist a non-constant function of degree 1. Hence, if we choose a basis $\omega_1, \ldots, \omega_g$ of $\Omega^1(C)$ we can define a morphism:

$$\phi\colon C \longrightarrow \mathbb{P}^{g-1}, \qquad P \mapsto (\omega_1(P), \ldots, \omega_g(P)),$$

where $\omega(P) := f(P)$ for any expression $\omega = f\, dt_P$, with $f,\ t_P \in k(C)$ and t_P local parameter at P. This morphism is called the *canonical morphism.* It is unique up to automorphisms of $\mathbb{P}^{g-1}$.

1.1.3 Theorem. *The canonical morphism is an immersion if and only if C is non-hyperelliptic.*

PROOF: The morphism ϕ is an immersion iff K is very ample and this is equivalent to $\ell(K-P-Q) = g-2$ for all $P, Q \in C$ [Har77, IV]. By the Riemann-Roch formula, this is equivalent to $\ell(P+Q) = 1$ for all P, Q and this is clearly equivalent to C non-hyperelliptic. □

Let $H = V(a_1x_1 + \cdots + a_gx_g) \subset \mathbb{P}^{g-1}$ be a hyperplane. By the very definition of ϕ we have,

$$\phi^*(\phi(C)\cdot H) = \operatorname{div}(a_1\omega_1 + \cdots + a_g\omega_g),$$

so that $\phi(C)$ is a curve of degree $2g-2$. Moreover, criterion 4 above for m to be a gap at P is translated into:

$$m \text{ is a gap at } P \iff \exists H \text{ hyperplane s.t. } (\phi(C)\cdot H)_{\phi(P)} = m-1. \tag{1.2}$$

Assume now that $g = 3$. If C is hyperelliptic, then $\phi(C)$ is a double-conic and ϕ has degree 2, but if C is non-hyperelliptic, then ϕ is an isomorphism between C and the smooth plane quartic $\phi(C)$. Conversely, any smooth plane quartic has degree $d = 4$, genus $g = \frac{1}{2}(d-1)(d-2) = 3$ and it is easy to deduce from the adjunction formula that the canonical inclusion coincides with the canonical morphism, so that C is non-hyperelliptic.

Thus, if we want to study non-hyperelliptic curves C of $g = 3$ we can assume that $C \subseteq \mathbb{P}^2$ is a smooth plane quartic, given by a homogeneous equation $F(x, y, z) = 0$. Up to scalar multiplication there is a canonical basis of $\Omega^1(C)$, given by the three regular differentials whose divisors are respectively $(C\cdot V(x))$, $(C\cdot V(y))$, $(C\cdot V(z))$. It is easy to check that in affine coordinates x, y these are the differentials

$$\frac{1}{\partial F/\partial y}dx,\ \frac{x}{\partial F/\partial y}dx,\ \frac{y}{\partial F/\partial y}dx.$$

If $\operatorname{char}(k) = 0$, by (1.2) and the remark at the end of last subsection, we have for any point $P \in C$:

$$w(P) = 1 \iff 4 \text{ is a gap at } P \iff P \text{ is a flex of } C,$$
$$w(P) = 2 \iff 5 \text{ is a gap at } P \iff P \text{ is a hyperflex of } C,$$

where the terms *flex* and *hyperflex* indicate that the tangent at P cuts C with intersection multiplicity 3 and 4 respectively.

Thus, the Weierstrass points can be effectively computed by cutting C with the Hessian curve:

$$H_C\colon \begin{vmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{vmatrix} = 0$$

The Hessian has degree 6 and it cuts C in the Weierstrass divisor:

$$(H_C \cdot C) = \sum_{P \in C} w(P)[P] = \sum_{P\,\text{flex}} [P] + \sum_{P\,\text{hyperflex}} 2[P].$$

The different possibilites for the number of flexes and hyperflexes are well studied (cf. [Ver83]). Let us mention as extreme cases that the Fermat quartic, $x^4+y^4+z^4 = 0$, has 12 hyperflexes and no flexes, whereas the Klein quartic, $x^3y + y^3z + z^3x = 0$ has 24 flexes and no hyperflex.

1.2 Symplectic geometry over $\mathbb{F}_2$

The geometric configuration of the bitangents of a plane quartic C is explained by the symplectic geometry of the space of 2-torsion points of the jacobian of C, with respect to the Weil pairing (cf. section 1.3). Let us first study this symplectic spaces in an abstract setting.

Let V be a $\mathbb{F}_2$-vector space of finite dimension $2g$, equipped with a non-degenerate symplectic form (i.e. bilinear and alternate):

$$\langle\ ,\ \rangle\colon V \times V \longrightarrow \mathbb{F}_2$$

Since the pairing is non-degenerate, it induces an isomorphism $V \simeq V^*$. We shall denote by $v^* := \langle\, v, - \,\rangle$ the linear form corresponding to each vector $v \in V$ under this isomorphism.

Such a bilinear form admits always a symplectic basis, such that the matrix of $\langle\ ,\ \rangle$ with respect to the basis is:

$$J = \left(\begin{array}{c|c} 0 & I \\ \hline I & 0 \end{array}\right).$$

We can consider the *symplectic group*:

$$\begin{aligned} \mathrm{Sp}(V) := \mathrm{Aut}\big(V, \langle\ ,\ \rangle\big) \simeq \mathrm{Sp}_{2g}(\mathbb{F}_2) = \\ = \{M \in \mathrm{GL}_{2g}(\mathbb{F}_2) \mid {}^tMJM = J\}. \end{aligned}$$

Clearly, $|\,\mathrm{Sp}(V)|$ coincides with the number of symplectic bases of V. Hence,

$$|\,\mathrm{Sp}(V)| = 2^{2g} \prod_{i=1}^{g} \left(2^{2i} - 1\right).$$

Quadratic forms

A quadratic form associated to $(V, \langle\ ,\ \rangle)$ is a map, $Q\colon V \longrightarrow \mathbb{F}_2$, such that

$$Q(u+v) = Q(u) + Q(v) + \langle\, u,\, v \,\rangle, \quad \forall u, v \in V.$$

Note that Q restricted to any isotropic subspace is a linear form.

We denote by QV the set of all quadratic forms associated to V. This set QV is a principal homogeneous space over V^*. It is clear from the definition that for any fixed $Q_0 \in$ QV, we have a bijection:

$$V^* \longrightarrow \mathrm{QV}, \qquad v^* \mapsto Q_0 + v^*,$$

whose inverse mapping is $Q \mapsto Q + Q_0$. In particular, the sum $Q + Q' + Q''$ of three quadratic forms is again a quadratic form.

Let us fix a symplectic basis $x_1, \ldots, x_g; y_1, \ldots, y_g$ of V. For any quadratic form Q we compute $Q(w)$ in terms of the coordinates,

$$w = \lambda_1 x_1 + \cdots + \lambda_g x_g + \mu_1 y_1 + \cdots + \mu_g y_g$$

of any vector $w \in V$. For simplicity, we shall write $w = (\lambda, \mu)$, with $\lambda = (\lambda_1, \dots, \lambda_g)$, $\mu = (\mu_1, \dots, \mu_g) \in \mathbb{F}_2^g$. In coordinates, the most simple quadratic form is:

$$Q_0(w) := \lambda \cdot \mu,$$

where $\cdot$ denotes the usual dot product of g-tuples. Now, for any other vector $v \in V$, with coordinates $v = (\epsilon', \epsilon)$, the linear form v^* acts:

$$v^*(w) = \langle\, v, w \,\rangle = \epsilon \cdot \lambda + \epsilon' \cdot \mu.$$

Hence, the form $Q := Q_0 + v^*$ acts by:

$$Q(w) = \epsilon \cdot \lambda + \epsilon' \cdot \mu + \lambda \cdot \mu. \tag{1.3}$$

We say that (ϵ, ϵ') are the coordinates of Q with respect to this basis and we write $Q = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$. Note that

$$\epsilon = (Q(x_1), \dots, Q(x_g)), \quad \epsilon' = (Q(y_1), \dots, Q(y_g)).$$

In coordinates we have:

$$\begin{aligned} &\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} + (\lambda, \mu)^* = \begin{bmatrix} \epsilon + \mu \\ \epsilon' + \lambda \end{bmatrix}, \\ &\begin{bmatrix} \epsilon_1 \\ \epsilon_1' \end{bmatrix} + \begin{bmatrix} \epsilon_2 \\ \epsilon_2' \end{bmatrix} + \begin{bmatrix} \epsilon_3 \\ \epsilon_3' \end{bmatrix} = \begin{bmatrix} \epsilon_1 + \epsilon_2 + \epsilon_3 \\ \epsilon_1' + \epsilon_2' + \epsilon_3' \end{bmatrix}. \end{aligned} \tag{1.4}$$

Arf invariant

1.2.1 Lemma. *The number of vectors* $(\lambda, \mu) \in \mathbb{F}_2^{2g}$ *such that* $\lambda \cdot \mu = 0, 1$ *is respectively* $2^{g-1}(2^g + 1)$, $2^{g-1}(2^g - 1)$.

PROOF: Let us fix $\lambda \in \mathbb{F}_2^g$ and think of $\lambda \cdot \mu = 0, 1$ as a system of linear equations. For $\lambda = 0$ this system has respectively $2^g, 0$ solutions, whereas for $\lambda \neq 0$ it has always 2^{g-1} solutions. □

1.2.2 Definition. Fix a symplectic basis $x_1, \dots, x_g; y_1, \dots, y_g$ of V. For any quadratic form $Q = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$, we define the Arf invariant of Q as

$$\mathrm{Arf}(Q) := \epsilon \cdot \epsilon' \in \mathbb{F}_2.$$

We say that Q is respectively *even,odd* according to $\mathrm{Arf}(Q) = 0, 1$.

By Lemma 1.2.1, there are $2^{g-1}(2^g + 1)$ even quadratic forms and $2^{g-1}(2^g - 1)$ odd ones. Moreover, we can rewrite (1.3) as:

$$Q(w) = (\epsilon' + \lambda) \cdot (\epsilon + \mu) + \mathrm{Arf}(Q).$$

Hence, again by Lemma 1.2.1, we have

$$\mathrm{Arf}(Q) = 0 \implies |Q^{-1}(0)| = 2^{g-1}(2^g + 1),$$
$$\mathrm{Arf}(Q) = 1 \implies |Q^{-1}(0)| = 2^{g-1}(2^g - 1).$$

Since the number of zeros of Q is an intrinsic invariant, we see that $\mathrm{Arf}(Q)$ is independent of the choice of the symplectic basis. We denote respectively by $\mathrm{QV}_{\mathrm{even}}$, $\mathrm{QV}_{\mathrm{odd}}$ the subsets of even and odd quadratic forms.

The following observation is an immediate consequence of (1.3), (1.4) and the definition of the Arf invariant.

1.2.3 Lemma. *For any $v \in V$ and quadratic forms Q, Q_0, Q_1, Q_2 we have,*

$$\mathrm{Arf}(Q + v^*) = \mathrm{Arf}(Q) + Q(v),$$
$$\mathrm{Arf}(Q_0 + Q_1 + Q_2) = \mathrm{Arf}(Q_0) + \mathrm{Arf}(Q_1) + \mathrm{Arf}(Q_2) + \langle v_1, v_2 \rangle,$$

where $v_1^* = Q_0 + Q_1$, $v_2^* = Q_0 + Q_2$.

The symplectic group $\mathrm{Sp}(V)$ acts on the set QV:

$$(\sigma Q)(v) := Q(\sigma^{-1} v), \quad \forall \sigma \in \mathrm{Sp}(V), \forall v \in V.$$

Since Q and σQ have the same number of zeros, this action respects the Arf invariant.

1.2.4 Proposition. *The action of* $\mathrm{Sp}(V)$ *on* QV_{even} *(resp.* QV_{odd}*) is doubly transitive.*

Syzygetic triads and tetrads

1.2.5 Definition. We say that a triad Q_0, Q_1, Q_2 of quadratic forms is even,odd according to $Q_0 + Q_1 + Q_2$ being even,odd.

An odd triad of odd quadratic forms is also called a syzygetic triad.

As an immediate consequence of Lemma 1.2.3, we have,

1.2.6 Corollary. *Let Q_0, Q_1, Q_2 be odd quadratic forms and let $v_i^* = Q_0 + Q_i$, for $i = 1, 2$. Then,*

$$Q_0 + Q_1 + Q_2 \textit{ is odd} \iff \langle v_1, v_2 \rangle = 0.$$

1.2.7 Lemma. *Assume that $g = 3$ and let Q_0, Q_1, Q_2, Q_3 be a tetrad of odd quadratic forms. Then, the following conditions are equivalent:*

1. *$Q_0 + Q_1 + Q_2 + Q_3 = 0$*
2. *All four triads Q_i, Q_j, Q_k are odd*
3. *Three of the four triads Q_i, Q_j, Q_k are odd*

Proof: If the sum of the four quadratic forms is zero, it is obvious that each triad is odd.

Denote $Q_0 + Q_i = v_i^*$, for $i = 1, 2, 3$. Since all four quadratic forms are odd, we have $Q_0(v_i) = 0$ for $i = 1, 2, 3$ by Lemma 1.2.3. Assume now that the three triads Q_i, Q_j, Q_k containing Q_0 are odd. By Corollary 1.2.6, the subspace $W = \langle v_1, v_2, v_3 \rangle_{\mathbb{F}_2}$ is isotropic.

If it were $\dim W = 3$, this subspace W would be a maximal isotropic space; but this is not possible, since Q_0 would be even! In fact, with respect to any symplectic basis starting with v_1, v_2, v_3 we would have $Q_0 = \begin{bmatrix} 0 & 0 & 0 \\ * & * & * \end{bmatrix}$. Hence, v_1, v_2, v_3 are linearly dependent, and since they are non-zero and pairwise different, we have necessarily $v_1 + v_2 + v_3 = 0$. Therefore, $Q_0 + Q_1 + Q_2 + Q_3 = 0$. □

1.2.8 Definition. If $g = 3$, any tetrad of odd quadratic forms satisfying the conditions of Lemma 1.2.7 is called a syzygetic tetrad.

Steiner sets

For any $v \in V$, $v \neq 0$, consider the *Steiner set* S_v defined as:

$$S_v := \{Q \in \mathrm{QV}_{\mathrm{odd}} \mid Q(v) = 0\} = \{Q \in \mathrm{QV}_{\mathrm{odd}} \mid Q + v^* \in \mathrm{QV}_{\mathrm{odd}}\}.$$

We say that two forms $Q, Q' \in S_v$ *are paired in* S_v if $Q + Q' = v^*$. Every $Q \in S_v$ is paired to a single $Q' = Q + v^*$, which clearly belongs to S_v too.

1.2.9 Lemma. *Each Steiner set has* $2^{g-2}(2^{g-1}-1)$ *pairs of odd quadratic forms.*

Proof: The pairs $\{Q,\, Q + v^*\} \subseteq S_v$ are in bijection with the odd quadratic forms of the symplectic space $\langle\, v \,\rangle^{\perp}/\langle\, v \,\rangle$, which has dimension $2g - 2$. □

1.2.10 Lemma. *Assume that* $g = 3$ *and let* Q_0, Q_1, Q_2 *be a triad of odd quadratic forms belonging to a Steiner set* S_v. *Then,*

$$Q_0,\ Q_1,\ Q_2 \text{ is an odd triad} \iff \text{two of them are paired in } S_v.$$

Proof: If, for instance, $Q_0 + Q_1 = v^*$, then, clearly, $Q_0 + Q_1 + Q_2 = Q_2 + v^*$ is odd.

Conversely, assume that $Q_0 + Q_1 + Q_2$ is odd and $Q_1 \neq Q_0 + v^*$, $Q_2 \neq Q_0 + v^*$. Then, $Q_0, Q_1, Q_2, Q_0 + v^*$ is a tetrad of odd forms satisfying that each triad containing Q_0 is odd. By Lemma 1.2.7, these four forms add to zero, so that $Q_1 + Q_2 = v^*$ and Q_1, Q_2 are paired in S_v. □

Let us gather some enumerative results for $g = 3$.

1.2.11 Proposition. *Assume that* $g = 3$. *Then,*

1. *There are respectively 36,28 even,odd quadratic forms.*
2. *There are 63 Steiner sets, each containing 6 pairs of quadratic forms.*

3. *There are 1260 syzygetic triads and 315 syzygetic tetrads of quadratic forms.*

PROOF: The first two assertions are contained in the previous results.

Let us prove the third assertion. Note that each syzygetic triad Q_0, Q_1, Q_2 is contained in the three different Steiner sets generated by the pairs $\{Q_0, Q_1\}$, $\{Q_0, Q_2\}$, $\{Q_1, Q_2\}$. For instance, if $Q_0 + Q_1 = v^*$, by assumption $Q_2 + v^*$ is odd, so that Q_0, Q_1, $Q_2 \in S_v$. On the other hand, in a fixed Steiner set there are 60 syzygetic triads by Lemma 1.2.10; we have 6 pairs of forms and to each pair we can add 10 forms to form a syzygetic triad. Thus, the total number of such triads is $63 \cdot 60/3 = 1260$.

By Lemma 1.2.7 each syzygetic triad is contained in a unique syzygetic tetrad and there are 4 triads in each tetrad; thus, the total number of syzygetic tetrads is $1260/4 = 315$. □

We describe now the combinatorial structure of the 63 Steiner sets:

1.2.12 Proposition. *Let* $v, w \in V - \{0\}$, $v \neq w$.

If $\langle v, w \rangle = 0$, *the three Steiner sets* S_v, S_w, S_{v+w} *have a syzygetic tetrad in common, which is also the whole intersection of each pair*

$$S_v \cap S_w = S_v \cap S_{v+w} = S_w \cap S_{v+w}.$$

Hence, $S_v \cup S_w \cup S_{v+w} = \mathrm{QV}_{odd}$.

If $\langle v, w \rangle = 1$, *the Steiner sets* S_v, S_w *have six quadratic forms in common, which contain no pair neither in* S_v *nor* S_w. *Hence,* $S_v \cup S_w \cup S_{v+w} = S_v \cup S_w$ *contains only 18 odd quadratic forms.*

PROOF: If $\langle v, w \rangle = 0$, we can extend this couple of vectors to a symplectic basis: $v, w, u; v', w', u'$. In coordinates with respect to this basis, the odd quadratic forms Q satisfying $Q(v) = 0 = Q(w)$ are given by: $Q = \begin{bmatrix} 0 & 0 & 1 \\ * & * & 1 \end{bmatrix}$. Hence, we have 4 such forms and their sum is zero.

The case $\langle v, w \rangle = 1$ can be handled in a similar way. □

Aronhold sets

We assume throughout this subsection that $g = 3$.

1.2.13 Definition. An Aronhold set of quadratic forms associated to V is a set of 7 odd quadratic forms such that each triad is even (or asyzygetic).

As an immediate consequence of Corollary 1.2.6 we get the following criterion,

1.2.14 Lemma. *Let Q_0, Q_1, Q_2, Q_3, Q_4, Q_5, Q_6 be a family of seven odd quadratic forms and let $v_i^* = Q_0 + Q_i$ for $i = 1, \dots, 6$.*

They form an Aronhold set iff $\langle v_i, v_j \rangle = 1$, for all $i \neq j$.

In particular, in this case the family $v_1, \dots, v_6$ is a basis of V. More generally:

1.2.15 Lemma. *Let $v_1, \dots, v_m$ be a family of vectors of V satisfying $\langle v_i, v_j \rangle = 1$, for all $i \neq j$. Then,*

1. *If m is even, these vectors are linearly independent.*
2. *If m is odd and $v_1 + \cdots + v_m \neq 0$, these vectors are linearly independent.*

Proof: For any non-empty set $I \subseteq \{1, 2, \dots, m\}$, let $w_I := \sum_{i \in I} v_i$. We have,

$$|I| \text{ even } \implies \langle w_I, v_i \rangle = 1, \ \forall i \in I \implies w_I \neq 0,$$

$$|I| \text{ odd, } |I| < m \implies \langle w_I, v_i \rangle = 1, \ \forall i \notin I \implies w_I \neq 0.$$

□

It is easy to construct Aronhold sets from Steiner sets. Let us fix an Steiner set S_v and let

$$Q_0, Q_1, Q_2, Q_3, Q_4, Q_5$$

be any choice of one form in each of the 6 pairs of S_v. Denote again $v_i^* = Q_0 + Q_i$ for $i = 1, \dots, 5$. Since all forms are odd and all triads Q_0, $Q_0 + v^*$, Q_i are odd, we have by Lemma 1.2.3 and Corollary 1.2.6:

$$Q_0(v_i) = 0, \quad \langle v, v_i \rangle = 0, \quad \forall i.$$

By Lemma 1.2.10, all triads we can form with these quadratic forms are even and by Corollary 1.2.6 we have $\langle v_i, v_j \rangle = 1$, for all $i \neq j$. By Lemma 1.2.15 we have

$$v_1+v_2+v_3+v_4+v_5 \neq 0 \implies v_1,\ v_2,\ v_3,\ v_4,\ v_5 \text{ lin. independent} \implies$$
$$\implies \langle v_1,\ v_2,\ v_3,\ v_4,\ v_5 \rangle^{\perp} = \{0, v\} \implies v_1 + v_2 + v_3 + v_4 + v_5 = v.$$

Hence, in any case $v_1+v_2+v_3+v_4+v_5 \in \{0, v\}$. If $v_1+v_2+v_3+v_4+v_5 = 0$ it is impossible to extend our family to an Aronhold set, but if $v_1 + v_2 + v_3 + v_4 + v_5 = v$ there is a unique odd form Q_6 such that Q_0, Q_1, Q_2, Q_3, Q_4, Q_5, Q_6 is an Aronhold set. In fact, by non-degeneracy, there are two solutions of $\langle w, v_i \rangle = 1$, for $i = 1, \dots, 5$, and if w is one solution, the other one is $w + v$. Since,

$$Q_0(w + v) = Q_0(w) + Q_0(v) + \langle v, w \rangle = Q_0(w) + 1,$$

we see that exactly one of the two quadratic forms $Q_0 + w^*$, $Q_0 + (w + v)^*$ is odd.

We can construct in this way 32 different Aronhold sets from each Steiner set. In fact, once a good choice of forms in each pair is considered, we get all other possible good choices by replacing an even number of forms Q by their pairs $Q + v^*$; thus, we get 15 choices by replacing two forms, 15 choices by replacing four forms and 1 choice by replacing all six forms.

All Aronhold sets can be constructed in this way. More precisely, each Aronhold set can be constructed from 7 different Steiner sets in this way. In fact, if Q_0, Q_1, Q_2, Q_3, Q_4, Q_5, Q_6 is an Aronhold set, just by dropping one quadratic form we get 7 different families of 6 quadratic forms, that represent one choice of forms in each one of the different pairs of forms in a concrete Steiner set. For instance, if we drop Q_6 and denote as usual $Q_0 + Q_i = v_i^*$, from the fact that all Q_i are odd and all triads are even, we get

$$Q_0(v_i) = 0, \ \forall i, \qquad \langle v_i, v_j \rangle = 1, \ \forall i \neq j.$$

Hence, if for each $I \subseteq \{1, \ldots, 5\}$ we let $w_I = \sum_{i \in I} v_i$, we can check in a recurrent way that:

$$Q_0(w_I) = \begin{cases} 0, & \text{for } |I| = 1, 4, 5, \\ 1, & \text{for } |I| = 2, 3. \end{cases}$$

In particular, for $v := v_1 + v_2 + v_3 + v_4 + v_5$ we have $Q_i(v) = Q_0(v) + v_i^*(v) = 0$ for all i, so that $Q_i \in S_v$ for all i.

Since $63 \times 32/7 = 288$, we have proved:

1.2.16 Proposition. *There are 288 Aronhold sets.*

Another way to construct Aronhold sets is to relate them to symplectic bases:

1.2.17 Proposition. *There is a bijection between the set of ordered Aronhold sets and the set of symplectic bases.*

PROOF: There is a bijection between symplectic bases

$$x_1,\ x_2,\ x_3; y_1,\ y_2,\ y_3$$

of V and bases v_1, v_2, v_3, v_4, v_5, v_6 of V satisfying $\langle\, v_i, v_j \,\rangle = 1$ for all $i \neq j$. This bijection can be established, for instance, through the relations:

$$\begin{aligned} x_1 &= v_1, & y_1 &= v_1 + v_2 + v_3 + v_4 + v_5 + v_6, \\ x_2 &= v_2 + v_3, & y_2 &= v_3 + v_4 + v_5 + v_6, \\ x_3 &= v_4 + v_5, & y_3 &= v_5 + v_6. \end{aligned} \tag{1.5}$$

Now, to any ordered Aronhold set we can associate as usual such a basis v_1, v_2, v_3, v_4, v_5, v_6. Conversely, given such a basis, we can consider the symplectic basis given by (1.5) and consider the quadratic form $Q_0 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. It is easy to check that $Q_0(v_i) = 0$ for all i, so that all quadratic forms $Q_i := Q_0 + v_i^*$ are odd and they form an ordered Aronhold set. □

Since there are $2^9 \cdot 3 \cdot 15 \cdot 63$ symplectic bases, dividing this number by 7! we see again that there are 288 Aronhold sets.

1.3 Theta characteristics and bitangents

We go back to our original setting, where C is a projective, smooth, geometrically irreducible curve, of genus $g > 1$, defined over an algebraically closed field k. We assume from now on that $\mathrm{char}(k) \neq 2$.

1.3.1 Definition. A theta characteristic is a class $[D]$ of semicanonical divisors: $2D \equiv K$. We denote by $\mathrm{TCh} \subseteq \mathrm{Pic}^{g-1}(C)$ the set of all theta characteristics.

Since $\mathrm{Pic}^0(C)$ is a divisible group, the set TCh is non-empty and, in consequence, it is a principal homogeneous space over the group $V := \mathrm{Pic}^0(C)[2]$ of 2-torsion points of $\mathrm{Pic}^0(C)$. In particular, there are 2^{2g} theta characteristics.

Consider V as a symplectic space over $\mathbb{F}_2$ with respect to the symplectic form given by the Weil pairing composed with the unique non-trivial group isomorphism between $\mu_2(k)$ and $\mathbb{F}_2$:

$$e_2(\ ,\ )\colon V \longrightarrow \{-1,1\} \simeq \mathbb{F}_2.$$

1.3.2 Theorem. (Mumford, [ACGH85, App.B]) *There is a canonical bijection between* TCh *and* QV *given by: $D \mapsto Q_D$, where,*

$$Q_D\colon\ \mathrm{Pic}^0(C)[2] \longrightarrow \mathbb{F}_2, \quad \alpha \mapsto (\ell(D+\alpha) + \ell(D)) \pmod 2.$$

The quadratic form Q_D is respectively even,odd iff $\ell(D)$ is even,odd. We say accordingly that D is even,odd.

Let us check that this bijection is compatible with the respective actions of V^* on QV and V on TCh. Moreover, we compute the theta characteristic corresponding to a sum of three quadratic forms:

1.3.3 Lemma. *For any $D, D', D'' \in$ TCh,*

1. $Q_D + Q_{D'} = e_2(D' - D, -) = e_2(D + D' - K, -)$
2. $Q_D + Q_{D'} + Q_{D''} = Q_{D+D'+D''-K} = Q_{D+D'-D''}$

PROOF: Let $\alpha := D' - D \equiv D + D' - K \in V$. For any $\beta \in V$ we have,

$$\begin{aligned} &Q_D(\beta) + e_2(\alpha,\beta) = Q_D(\alpha) + Q_D(\alpha+\beta) = \\ &\quad = (\ell(D+\alpha) + \ell(D+\alpha+\beta)) \pmod 2 = Q_{D+\alpha}(\beta) = Q_{D'}(\beta). \end{aligned}$$

This proves the first assertion. The second assertion is easily derived from the first one:

$$Q_{D+D'-D''} = Q_D + e_2(D'-D'', -) = Q_D + Q_{D'} + Q_{D''}.$$

□

Theta characteristics of hyperelliptic curves

Assume that C is hyperelliptic. There are $2g+2$ different Weierstrass points, $P_1, \dots, P_{2g+2}$, all of them with weight $\frac{1}{2}(g-1)g$. All divisors $2[P_i]$ are in the same class, $H \in \operatorname{Pic}^2(C)$, which is called the hyperelliptic divisor class. The canonical divisor is $K = (g-1)H$.

For simplicity denote $P_\infty := P_{2g+2}$. Let $B_g := \{1, 2, \dots, 2g+1\}$; for any subset $T \subseteq B_g$, the divisor:

$$\alpha_T := \left(\sum_{i\in T}[P_i]\right) - |T|[P_\infty],$$

is a 2-torsion class and $\alpha_T \equiv \alpha_{B_g - T}$.

1.3.4 Proposition. *The divisors α_T for $|T|$ even (resp. $|T|$ odd) represent faithfully all classes of* $\operatorname{Pic}^0(C)[2]$.

Morever, for $|T|$, $|T'|$ even, the Weil pairing can be identified to:

$$e_2(\alpha_T, \alpha_{T'}) = |T \cap T'| \pmod 2.$$

Clearly, $D_0 := (g-1)[P_\infty]$ is a theta characteristic; hence, if T runs on all subsets of B_g with $|T|$ even (resp. $|T|$ odd) we get all theta characteristics by:

$$D_T := D_0 + \alpha_T.$$

Note that D_0 corresponds to $T = \emptyset$.

1.3.5 Lemma. *For any $T \subseteq B_g$,*

$$D_T \text{ is even iff } |T| \equiv g+1 \text{ or } g+2 \pmod 4.$$

Proof: Let $N = g - 1 + |T|$ and let $D = N[P_\infty] - \sum_{i \in T}[P_i]$. We have, $D_T = \alpha_T + D_0 \equiv -\alpha_T + D_0 = D$. Hence,

$$L(D_T) \simeq L(D) \subseteq L(N[P_\infty]) = \langle 1, x, x^2, \ldots, x^{[N/2]} \rangle,$$

where $x \in k(C)$ satisfies $\operatorname{div}_\infty(x) = 2[P_\infty]$.

Therefore, $L(D)$ is identified to the linear subspace of all polynomials in x of degree $\leq [N/2]$ vanishing at $|T|$ points; hence,

$$\ell(D_T) = [N/2] + 1 - |T| = \begin{cases} \frac{g-1-|T|}{2} + 1, & \text{if } |T| \not\equiv g \pmod 2, \\ \frac{g-|T|}{2} + 1, & \text{if } |T| \equiv g \pmod 2, \end{cases}$$

and $\ell(D_T)$ is even iff $|T| \equiv g+1 \pmod 4$, or $|T| \equiv g+2 \pmod 4$, respectively. □

Configuration of the bitangents

We consider now the case $g = 3$ and C non-hyperelliptic. As we saw in section 1.1 we can assume that $C \subseteq \mathbb{P}^2$ is a smooth plane quartic, given by an equation $F(x, y, z) = 0$. We keep our assumption that $\operatorname{char}(k) \neq 2$.

We start with a trivial observation; for any divisor D of degree 2,

$$\ell(D) > 0 \implies D \equiv P + Q \implies \ell(D) = 1.$$

In particular,

1.3.6 Lemma. *For any theta characteristic D we have $\ell(D) = 0, 1$ according to D being even,odd.*

A bitangent of C is a line L such that $(L \cdot C) = 2[P] + 2[Q]$, for some points $P, Q \in C$. Thus, if L is a bitangent, the divisor $\frac{1}{2}(L \cdot C) = [P] + [Q]$ is always an odd theta characteristic.

Note that the tangent lines at hyperflexes of C are particular cases of bitangents.

1.3.7 Theorem. *The correspondence $L \mapsto \frac{1}{2}(L \cdot C)$ establishes a bijection between the set of bitangents and the set of odd theta characteristics of C.*

Proof: Since C is non-hyperelliptic we have,

$$[P]+[Q] \equiv [R]+[S] \implies [P]+[Q] = [R]+[S],$$

and the correspondence is injective. Moreover, any odd theta characteristic D is linearly equivalent to some effective divisor $[P]+[Q]$ and, since $2D \equiv K$, the line joining P and Q is a bitangent. □

1.3.8 Corollary. *C has 28 bitangents.*

We want to study the geometric and combinatorial properties of this set $\operatorname{Bit}(C)$ of 28 lines of $\mathbb{P}^2$. We can use identifications:

$$\begin{array}{ccccc} \operatorname{Bit}(C) & \leftrightarrow & \mathrm{TCh}_{\mathrm{odd}} & \leftrightarrow & \mathrm{QV}_{\mathrm{odd}} \\ L & & D = \frac{1}{2}(L \cdot C) & & Q_L := Q_D \end{array}$$

and use the properties of the symplectic space $V = \operatorname{Pic}^0(C)[2]$ that we studied in section 1.2. For instance, concepts like syzygetic triads or tetrads of bitangents, a Steiner set of bitangents or an Aronhold set of bitangents have an obvious meaning.

1.3.9 Theorem. *Let L_1, L_2, L_3, L_4 be a tetrad of bitangents of C. There is a conic $\mathcal{Q} \subseteq \mathbb{P}^2$ such that $(\mathcal{Q} \cdot C) = (L_1L_2L_3L_4 \cdot C)$ iff they form a syzygetic tetrad.*

Proof: Let i be the canonical inclusion of C in $\mathbb{P}^2$. Since

$$i^*(\mathcal{O}_{\mathbb{P}^2}(2)) = 2K,$$

there is a conic cutting C in a concrete effective divisor E iff $E \equiv 2K$.

For $i = 1,2,3,4$ let $D_i := \frac{1}{2}(L_i \cdot C)$ be the odd theta characteristic corresponding to L_i. We have,

$$D_1 + D_2 + D_3 + D_4 \equiv 2K \iff D_1 + D_2 + D_3 - K \equiv K - D_4 \equiv D_4.$$

By Lemma 1.3.3 this is equivalent to $Q_{D_1} + Q_{D_2} + Q_{D_3} = Q_{D_4}$. □

1.3.10 Corollary. (Steiner-Hesse)

1. *For any pair L, M of bitangents, there are 5 other pairs L', M' of bitangents such that there exists a conic cutting C in the divisor $\frac{1}{2}(LML'M' \cdot C)$*

2. *There are 315 conics cutting C in a divisor which is 1/2 the intersection divisor of C with 4 bitangents.*

PROOF: These pairs of bitangents correspond to pairs of quadratic forms in the Steiner set S_v, where $Q_L + Q_M = v^*$.

The second assertion is consequence of Proposition 1.2.11. □

The existence of such a conic has interest because it leads to a normal model of C of the form: $\mathcal{Q}^2 = LML'M'$. In fact, by the fundamental theorem of Max Noether [Ful69, 5.5], from the fact that $(\mathcal{Q}^2 \cdot C) = (LML'M' \cdot C)$ one deduces that there are constant $a, b \in k$ such that $F = a\mathcal{Q}^2 + bLML'M'$ and we can normalize the equations of the conics and the bitangents so that $a = 1$, $b = -1$. However, by the above corollary, each quartic has 315 different normal equations of this type.

One might guess from these facts that it is easy to classify smooth plane quartics up to isomorphism. However, although the moduli space $\mathcal{M}_3$ of curves of genus 3 has been extensively studied, it is still an open problem to find explicit equations for this 6-dimensional irreducible variety.

Aronhold sets of bitangents have been classically studied because they determine the whole set of bitangents and even more, they determine the quartic equation itself. A very natural question is to ask if the curve equation is uniquely determined by the 28 bitangent lines. This question has a positive answer, but, surprisingly enough, it has been obtained very recently [Leh05], [CS03].

1.4 Theta functions

Theta functions are holomorphic functions, $\theta\colon \mathbb{C}^g \longrightarrow \mathbb{C}$, which determine a global section of a line bundle of a polarized complex abelian variety of dimension g.

We are interested in the theta functions associated to the jacobian variety $\mathrm{Jac}(C)$ equipped with its canonical principal polarization. Let us briefly recall the construction of this polarized abelian variety.

Jacobian variety of C

Let C be a projective, smooth, geometrically irreducible curve, of genus $g > 1$, defined over $\mathbb{C}$.

We define the jacobian variety of C as the complex g-dimensional torus $\mathrm{Jac}(C) := \Omega^1(C)^*/H_1(C,\mathbb{Z})$, where $H_1(C,\mathbb{Z})$ is identified to a lattice of the complex vector space $\Omega^1(C)^*$ by letting any 1-cycle $x \in H_1(C,\mathbb{Z})$ act as the linear form $\omega \mapsto \int_x \omega$.

Let $x_1,\dots,x_g; y_1,\dots,y_g$ be a $\mathbb{Z}$-basis of $H_1(C,\mathbb{Z})$ such that the intersection product has matrix:

$$M := \left(\begin{array}{c|c} 0 & -I \\ \hline I & 0 \end{array}\right).$$

We work in coordinates with respect to the $\mathbb{C}$-basis $y_1,\dots,y_g$ of $\Omega^1(C)^*$. Let $\omega_1,\dots,\omega_g$ be its dual basis. The period matrix of $\mathrm{Jac}(C)$ with respect to our choices of bases of $\Omega^1(C)^*$ and $H_1(C,\mathbb{Z})$ is:

$$\left(Z \mid I \right), \qquad \text{where } Z = \left(\int_{x_i} \omega_j \right).$$

Thus, we identify $\mathrm{Jac}(C)$ with the complex torus $\mathbb{C}^g/\Lambda$, where Λ is the lattice generated by the columns of the period matrix $\left(Z \mid I \right)$, which we still denote by $x_1,\dots,x_g; y_1,\dots,y_g$. The matrix Z belongs to Siegel's upper half-space:

$$Z = {}^tZ, \qquad \mathrm{Im}(Z) > 0.$$

Notation. By identifying vectors in $\mathbb{C}^g$ and $\mathbb{R}^g$ to 1-row matrices, any $u \in \mathbb{C}^g$ can be written as $u = u_1 Z + u_2$, for uniquely determined

$u_1,\, u_2 \in \mathbb{R}^g$. In the sequel we shall write simply $u = (u_1, u_2) \in \mathbb{C}^g$. With this notation, $u \in \Lambda$ iff $u_1,\, u_2 \in \mathbb{Z}^g$.

We consider on $\mathbb{C}^g$ the real alternating form E, having matrix $-M$ with respect to the $\mathbb{R}$-basis $x_1, \ldots, x_g; y_1, \ldots, y_g$. Since $E(\Lambda \times \Lambda) \subseteq \mathbb{Z}$, the corresponding hermitian form,

$$H(u, v) = E(iu, v) + iE(u, v),$$

belongs to the Néron-Severi group of $\mathrm{Jac}(C)$. Moreover, the matrix of H with respect to the canonical basis $y_1, \ldots, y_g$ of $\mathbb{C}^g$ is $\mathrm{Im}(Z)^{-1}$; hence, H defines a (canonical) principal polarization of $\mathrm{Jac}(C)$ and $(\mathrm{Jac}(C), H)$ is a principally polarized abelian variety.

Recall that the Abel-Jacobi map determines an embedding:

$$\mathrm{aj}_{P_0} \colon C \hookrightarrow \mathrm{Jac}(C), \quad P \mapsto \left(\int_{P_0}^{P} \omega_1, \ldots, \int_{P_0}^{P} \omega_g \right),$$

where P_0 is any fixed point of C. It induces a canonical isomorphism between $\mathrm{Pic}^0(C)$ and $\mathrm{Jac}(C)$ and non-canonical bijections between $\mathrm{Pic}^d(C)$ and $\mathrm{Jac}(C)$ for all $d \in \mathbb{Z}$:

$$\mathrm{aj} : \ \mathrm{Pic}^0(C) \xrightarrow[\sim]{} \mathrm{Jac}(C), \quad \mathrm{aj}_{P_0} \colon \ \mathrm{Pic}^d(C) \leftrightarrow \mathrm{Jac}(C)$$

Line bundles on $\mathrm{Jac}(C)$ and theta functions

We use freely the notations and results of [BG03, Ch.5]. The group $\mathrm{Pic}(\mathrm{Jac}(C))$ of line bundles on $\mathrm{Jac}(C)$ can be described in terms of Appel-Humbert data:

$$\mathrm{Pic}(\mathrm{Jac}(C)) \simeq \{(H, \alpha) \mid H \in \mathrm{NS}(\mathrm{Jac}(C)),\ \alpha \text{ is a } H\text{-semicharacter}\},$$

where an H-semicharacter is a map, $\alpha \colon \Lambda \longrightarrow \mathbb{C}_1$, with values in the group of complex numbers of absolute value 1, such that:

$$\alpha(\lambda + \mu) = \alpha(\lambda)\alpha(\mu) \exp(\pi i E(\lambda, \mu)), \ \ \forall \lambda, \mu \in \Lambda.$$

The group operation of $\mathrm{Pic}(\mathrm{Jac}(C))$ translates into

$$(H, \alpha) + (H', \alpha') = (H + H', \alpha\alpha').$$

We have chosen a canonical $H \in \mathrm{NS}^+(\mathrm{Jac}(C))$ and the choice of a symplectic basis for E allows to fix a special H-semicharacter α_0, vanishing on the two maximal isotropic spaces $\langle x_1, \dots, x_g \rangle_{\mathbb{R}}$, $\langle y_1, \dots, y_g \rangle_{\mathbb{R}}$:

$$\alpha_0(\lambda) = \alpha_0(\lambda_1 Z + \lambda_2) := \exp(\pi i E(\lambda_1, \lambda_2)) = \exp(\pi i \lambda_1 \cdot \lambda_2), \ \forall \lambda \in \Lambda.$$

We get in this way a particular line bundle $L_0 = (H, \alpha_0)$ on $\mathrm{Jac}(C)$, whose global sections satisfy:

$$\begin{aligned} &H^0(\mathrm{Jac}(C), L_0) = \{\theta\colon \mathbb{C}^g \longrightarrow \mathbb{C} \mid \theta \text{ holomorphic and} \\ &\quad \theta(z+\lambda) = \alpha_0(\lambda)\exp(-\pi i(2z+\lambda)\cdot\lambda_1)\theta(z), \ \forall z \in \mathbb{C}^g, \forall \lambda \in \Lambda\}. \end{aligned}$$

General theory shows that $\dim H^0(\mathrm{Jac}(C), L_0) = 1$; thus, up to multiplicative constants, there is a unique theta function associated to this line bundle L_0. This is *Riemann's theta function*:

$$\theta(z) = \sum_{m \in \mathbb{Z}^g} \exp\left(\pi i (mZm + 2z \cdot m)\right),$$

where in mZm, m is conveniently a 1-row or 1-column matrix.

This series converges uniformly on compact sets and defines a holomorphic function which is g-periodical with periods $y_1, \dots, y_g$. The functional equation of θ shows that $\theta(z)$ and $\theta(z+\Lambda)$ differ only by a nowhere vanishing function; hence, the divisor of zeros of θ is a divisor Θ of $\mathrm{Jac}(C) = \mathbb{C}^g/\Lambda$, which is called the *theta divisor.*

The theta divisor is ample and the linear system $|3\Theta|$ determines an embedding $\mathrm{Jac}(C) \hookrightarrow \mathbb{P}^N$, for $N = 3^g - 1$.

We are interested in the relationship of Θ with divisors of C. This is given by Riemann's singularities theorem [ACGH85, Ch.VI]. Denote,

$$W_{g-1} := \{D \in \mathrm{Pic}^{g-1}(C) \mid \ell(D) > 0\}.$$

1.4.1 Theorem. *There exists a unique theta characteristic $D_0 \in \mathrm{Pic}^{g-1}(C)$ such that,*

$$\mathrm{aj}_{P_0}(W_{g-1}) \ = \ \Theta \ + \ \mathrm{aj}_{P_0}(D_0).$$

Moreover, for any $D \in W_{g-1}$, with $\mathrm{aj}_{P_0}(D) = v + \mathrm{aj}_{P_0}(D_0)$, we have

$$\ell(D) = \mathrm{mult}_v(\Theta).$$

The multiplicity $\operatorname{mult}_v(\Theta)$ is just the order of vanishing of θ at v as an analytical fuction. The vector $\operatorname{aj}_{P_0}(D_0)$ is called the *Riemann constant.* Note that $\operatorname{aj}_{P_0}(W_{g-1})$ is the image under the Abel-Jacobi map of all effective divisors of degree $g-1$.

Since aj is an isomorphism, we have a bijection between the set TCh and the set of semiperiods of C:

$$\begin{array}{ccc} \mathrm{TCh} & \longrightarrow & \mathrm{Jac}(C)[2] = \frac{1}{2}\Lambda/\Lambda \\ D & \mapsto & \operatorname{aj}(D - D_0) \end{array}$$

We say that a semiperiod v is even,odd according to D being even,odd. By Riemann's theorem, this is equivalent to $\operatorname{mult}_v(\Theta)$ being even,odd. Since θ is an even function, the theta characteristic D_0 is always even.

We introduce the following notation for the semiperiods. For any $\epsilon, \epsilon' \in \{0,1\}^g$ we denote,

$$v_{\epsilon,\epsilon'} := \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} := \frac{1}{2}\left(\epsilon Z + \epsilon'\right).$$

Theta functions with characteristics

The set $\mathrm{Pic}^H(\mathrm{Jac}(C)) := \{L = (H,\alpha) \mid \alpha \text{ H-semicharacter}\}$ of all line bundles with a fixed hermitian form H, is a principal homogeneous space over $\mathrm{Pic}^0(\mathrm{Jac}(C)) := \{(0,\alpha) \mid \alpha \in \mathrm{Hom}(\Lambda, \mathbb{C}_1)\}$. In fact,

$$(0,\alpha) \mapsto L_0 + (0,\alpha) = (H, \alpha_0\alpha)$$

is clearly bijective. This allows one to consider a bijection:

$$\begin{array}{ccccc} \mathrm{Jac}(C) & \underset{\sim}{\rightarrow} & \mathrm{Pic}^0(\mathrm{Jac}(C)) & \xrightarrow{L_0\otimes -} & \mathrm{Pic}^H(\mathrm{Jac}(C)) \\ c & \mapsto & (0, \exp(2\pi i E(c,-)) & \mapsto & (H, \alpha_0 \exp(2\pi i E(c,-)) \end{array}$$

The first isomorphism can be identified with the isomorphism between $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C)^\wedge$, determined by the principal polarization.

The composition of these bijections is precisely: $c \mapsto t_c^*(L_0)$. Since translation by c is an analytical isomorphism of complex manifolds, we have natural isomorphisms:

$$H^0(\mathrm{Jac}(C), L_0) \underset{\sim}{\rightarrow} H^0(\mathrm{Jac}(C), t_c^*(L_0)).$$

Hence, from Riemann's theta function we can derive, essentially by considering the translates $\theta(-+c)$, all other theta functions that can be obtained from all line bundles associated to our chosen polarization H. Actually, we have to translate by c the automorphy factor of Riemann's theta function. We obtain in this way that a global section of $t_c^*(L_0)$ is given by the *theta function with characteristic* $c \in \mathbb{C}^g$:

$$\theta_c(z) := \theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(z) := \exp(\pi i\,(c_1 Z c_1 + 2c_1 \cdot (z + c_2))\,\theta(z+c) =$$
$$= \sum_{m\in\mathbb{Z}^g} \exp\left(\pi i((m+c_1)Z(m+c_1) + 2(z+c_2)\cdot(m+c_1))\right).$$

Caution. For any characteristic $c \in \mathbb{C}^g$ the isomorphism class of $t_c^*(L_0)$ depends only on the class of c modulo Λ. However, we have chosen a concrete line bundle in this isomorphy class, given by a concrete automorphy factor (a choice of a 1-cocycle in a given cohomology class in $\mathrm{H}^1(\Lambda, \mathcal{O}^*(\mathbb{C}^g))$). This choice makes the theta function θ_c depend on the representative $c \in \mathbb{C}^g$ in its class modulo Λ.

The following quasi-periodicity properties are easy to check:

1.4.2 Lemma. *For all* $c = (c_1, c_2)$, $w = (w_1, w_2) \in \mathbb{C}^g$ *and all* $\lambda = (\lambda_1, \lambda_2) \in \Lambda$,

$$\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(z+\lambda) =$$
$$= \exp\left(-\pi i(\lambda_1 Z \lambda_1 + 2(z+c_2)\cdot\lambda_1 - 2c_1\cdot\lambda_2)\right)\,\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(z),$$

$$\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(z+w) =$$
$$= \exp\left(-\pi i(w_1 Z w_1 + 2(z+c_2+w_2)\cdot w_1)\right)\,\theta\begin{bmatrix} c_1 + w_1 \\ c_2 + w_2 \end{bmatrix}(z),$$

$$\theta\begin{bmatrix} c_1 + \lambda_1 \\ c_2 + \lambda_2 \end{bmatrix}(z) = \exp(2\pi i c_1 \cdot \lambda_2)\,\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(z),$$

$$\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(-z) = \theta\begin{bmatrix} -c_1 \\ -c_2 \end{bmatrix}(z).$$

The functions $\theta_c(z)$ and $\theta(z+c)$ differ multiplicatively by a nowhere vanishing function; hence, they have the same divisor of zeros:

$$\mathrm{div}(\theta_c) = \mathrm{div}(\theta(-+c)) = \Theta + c.$$

In particular, for any $D \in W_{g-1}$ such that $\mathrm{aj}_{P_0}(D) = v + \mathrm{aj}_{P_0}(D_0)$:

$$\ell(D) = \mathrm{mult}_v(\Theta) = \mathrm{mult}_0(\theta\left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right]). \tag{1.6}$$

We are interested in the values of θ at the semiperiods. Let $c = v_{\epsilon,\epsilon'}$ be a semiperiod. Modulo Λ we can express $c_1 = \frac{1}{2}\epsilon$, $c_2 = \frac{1}{2}\epsilon'$, for some ϵ, $\epsilon' \in \{0,1\}^g$. We shall commit the following tremendous:

Abuse of notation. When $\epsilon, \epsilon' \in \{0,1\}^g$ we shall write:

$$\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}(z) := \theta_{v_{\epsilon,\epsilon'}}(z) = \theta\begin{bmatrix} \epsilon/2 \\ \epsilon'/2 \end{bmatrix}(z).$$

From now on we shall only use characteristics that are semiperiods and we hope that there is no confusion with this notation.

1.4.3 Corollary. *For all ϵ, $\epsilon' \in \{0,1\}^g$ we have,*

$$\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}(-z) = (-1)^{\epsilon\cdot\epsilon'}\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}(z).$$

Hence, $\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}(z)$ is an even,odd function iff $\epsilon \cdot \epsilon' \equiv 0, 1 \pmod 2$.

Proof: By the third equation of Lemma 1.4.2 applied to $\lambda = (\epsilon, 0)$, $c_1 = -\epsilon/2$, $c_2 = \epsilon'/2$:

$$\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}(-z) = \theta\left[\begin{smallmatrix} -\epsilon \\ -\epsilon' \end{smallmatrix}\right](z) = (-1)^{\epsilon\cdot\epsilon'}\theta\left[\begin{smallmatrix} -\epsilon \\ \epsilon' \end{smallmatrix}\right](z) = (-1)^{\epsilon\cdot\epsilon'}\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}(z).$$

□

By (1.6) we obtain:

1.4.4 Corollary. *For any theta characteristic D, corresponding to the semiperiod $v_{\epsilon,\epsilon'}$, we have,*

$$D \text{ even} \iff \mathrm{mult}_{v_{\epsilon,\epsilon'}}(\Theta) = \mathrm{mult}_0(\theta\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}) \text{ even} \iff$$
$$\iff \epsilon \cdot \epsilon' \equiv 0 \pmod 2.$$

1.4.5 Corollary. *Think of $V :=$ Jac$(C)[2]$ as an $\mathbb{F}_2$-vector space with basis $\frac{1}{2}x_1,\dots,\frac{1}{2}x_g;\frac{1}{2}y_1,\dots,\frac{1}{2}y_g$. Let D be a theta characteristic and let $\epsilon,\epsilon'\in\mathbb{F}_2^g$ be the coordinates in this basis of the semiperiod $v_{\epsilon,\epsilon'}=\mathrm{aj}_{P_0}(D)-\mathrm{aj}_{P_0}(D_0)\in V$. Then, the quadratic form $Q_D\in$ QV canonically associated to D has coordinates in this basis:*

$$v_{\epsilon,\epsilon'}=\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}\iff Q_D=\begin{bmatrix}\epsilon'\\ \epsilon\end{bmatrix}.$$

Proof: For any $w=(\lambda,\mu)\in V$, by (1.6) and Corollary 1.4.3:

$$\begin{aligned}Q_D(w) &= \big(\ell(D+\mathrm{aj}^{-1}w)+\ell(D)\big)\pmod 2 =\\ &= \left(\mathrm{mult}_0\,\theta\begin{bmatrix}\epsilon+\lambda\\ \epsilon'+\mu\end{bmatrix}+\mathrm{mult}_0\,\theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}\right)\pmod 2 =\\ &\qquad = (\epsilon+\lambda)\cdot(\epsilon'+\mu)+\epsilon\cdot\epsilon' = \epsilon\cdot\mu+\epsilon'\cdot\lambda+\lambda\cdot\mu.\end{aligned}$$

Hence, $Q_D=\begin{bmatrix}\epsilon'\\ \epsilon\end{bmatrix}$ (cf. (1.3)). □

The values $\theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(0)$ are called *Thetanullwerte.* The odd Thetanullwerte vanish, but the even ones contain important information on the geometry of C. For instance, for $g=3$ we have 36 even Thetanullwerte; by (1.6), one of these even Thetanullwerte vanishes iff the corresponding even theta characteristic D has $\ell(D)=2$. Hence,

1.4.6 Proposition. *The curve C of $g=3$ is hyperelliptic iff some even Thetanullwert vanishes.*

An interesting question is how to recover the equation of C in terms of the Thetanullwerte, or more generally, in terms of the theta functions $\theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}$. For the hyperelliptic case one may consult [Gua02].

E. Nart
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
nart@mat.uab.es

Capítol 2

Automorphism groups of genus 3 curves

Francesc Bars

Introduction

This note mainly reproduces a sketch of two proofs ([KK79],[Dol06]) of the determination of the non-trivial groups G that appear as the automorphism group of a non-hyperelliptic genus 3 curve over an algebraic closed field of characteristic zero. We display the tables obtained in these different approaches and the table given by Henn [Hen76] too. These tables are refined in order to obtain in some situations the existence of curves having as exact automorphism group the one predicted in the table and not a strictly bigger group, see theorem 2.2.3, remark 2.2.4 and the last paragraph of §2.4.

Initially I believed that the result was first obtained by Komiya and Kuribayashi [KK79] (1978). Later I discovered the existence of the manuscript of Henn [Hen76] in the subject (1976) (but I did not find yet any copy of Henn's manuscript).

More generally, we can ask: which groups appear as the automorphism group of a curve of genus $g \geq 4$? The reader interested in these questions can have a look at [MSSV05], where there is a list of groups for genus $g \leq 10$, but it is incomplete. We suggest also to check Breuer's book [Bre00], which studies all possible signatures.

Notation

We fix now some notation to be used in the rest of the chapter.

Let C be a non-singular, projective curve of genus $g \geq 2$, defined over an algebraic closed field K of characteristic 0.

By $\mathrm{WP}(C)$ we mean the set of all Weierstrass points of $C(K)$ (see the definition and basic properties of Weierstrass points in [Nar06, §1]).

It is classically known that

$$2g+2 \leq \#\,\mathrm{WP}(C) \leq (g-1)g(g+1),$$

and $\#\,\mathrm{WP}(C) = 2g+2$ if and only if C is an hyperelliptic curve.

We denote by $Aut(C)$ the group of all K-automorphism of the curve C. WP denotes a single Weierstrass point of C. For $\varphi \in Aut(C)$, $v(\varphi)$ is the number of points of C fixed by φ.

Consider a separable covering of smooth non-singular curves

$$\pi : C \to C'$$

and denote by g' the genus of C'. We can write Hurwitz's formula as follows:

$$\begin{aligned} 2g-2 = deg(\pi)(2g'-2) + \sum_{P\in C}(e_P - 1) = \\ = deg(\pi)(2g'-2) + \sum_{i=1}^{r} \frac{deg(\pi)}{v_j}(v_j - 1) = \\ = deg(\pi)(2g'-2) + deg(\pi)\sum_{i=1}^{r}(1 - v_j^{-1}), \end{aligned}$$

where r is the number of ramified points $\tilde{P}_1, \ldots, \tilde{P}_r$ of C', and for each $\tilde{P}_j$ there are $\frac{deg(\pi)}{v_j}$ branch points in C: $P_j^1, \ldots, P_j^{deg(\pi)/v_j}$ each of them with ramification index $v_j = e_{P_j^l}$.

2.1 General facts on the group $Aut(C)$

2.1.1 Lemma. *Let φ be any element of $Aut(C)$ with $\varphi \neq id$. Then φ fixes at most 2g+2 points (i.e. $v(\varphi) \leq 2g+2$).*

Proof: Denote by S the finite set of points of $C(K)$ fixed by φ. Take $P \in C(K)$ a non-fixed point by φ. We know that there exists a meromorphic function f of C, with $(f)_\infty = rP$ (the divisor of poles of f) for some r with $1 \leq r \leq g+1$ (we need to take $r = g+1$ if P is not a Weierstrass point).

Let us denote by $h := f - f\varphi$, whose divisor of poles is $(h)_\infty = rP + r(\varphi^{-1}P)$, thus h has $2r(\leq 2g+2)$ zeroes. To obtain the result, we need only to mention that every fixed point of C by φ is by construction a zero of h. □

2.1.2 Lemma. *Let be $\varphi \in Aut(C)$. If P is a* WP *of C then $\varphi(P)$ is a* WP *of C.*

Proof: φ^* transforms regular differentials into regular differentials, therefore the gap sequences (with respect to differentials) are preserved by φ^*. Thus, φ maps any WP (of some fixed weight) to another WP (of the same weight). □

Let us denote by $S_{\mathrm{WP}(C)}$ the permutation group on the set of Weierstrass points. We have a group homomorphism (lemma 2.1.2):

$$\lambda : Aut(C) \to S_{\mathrm{WP}(C)}.$$

2.1.3 Lemma. *λ is injective unless C is hyperelliptic. If C is hyperelliptic, then $ker(\lambda) = \{id, w\}$ where w denotes the hyperelliptic involution of $Aut(C)$.*

Proof: Take $\phi \in ker(\lambda)$. If C is non-hyperelliptic, we have strictly more than $2g+2$ WP points fixed by ϕ, thus by lemma 2.1.1, ϕ is the *id* automorphism.
If C is hyperelliptic, we know that $w \in ker(\lambda)$. We can suppose $\phi \neq w$ with $\phi \in ker(\lambda)$. We follow now the proof of lemma 2.1.1 with

$\phi = \varphi$. In the hypereliptic case we can take $r = 2$, therefore we have at most 4 fixed points for ϕ if it is not the identity. We know that the number of WP is $2g + 2(\geq 6)$, therefore $\phi \neq id$ and $\neq w$ does not belong to $ker(\lambda)$. □

If C is non-hyperelliptic we have a canonical immersion [Nar06, §1, Thm.1.3.],

$$\phi : C \to \mathbb{P}^{g-1},$$

and then we have a canonical model of C, $\phi(C)$, inside the projective space $\mathbb{P}^{g-1}$.

2.1.4 Proposition. *If C is a non-hyperelliptic curve, then any automorphism of C is represented by a projective transformation on $\mathbb{P}^{g-1}$ leaving $\phi(C)$ invariant.*

PROOF: For any morphism between two non-singular non-hyperelliptic curves, the pullback of the regular differentials maps to regular differentials; therefore any morphism lifts to a morphism between the projective spaces where the curves are embedded by the canonical immersions (both non-singular curves). □

Proposition 2.1.4 useful to obtain the exact automorphism group associated to a fixed non-hyperelliptic curve of genus 3. Proposition 2.1.4 and lemma 2.1.2 are key results in order to obtain the automorphism groups appearing on genus 3 curves, §2.2 (see for example theorem 2.2.7 of this notes).

Let us now list some general results using Hurwitz's formula. We need the separability condition in the following results of this subsection, which is no problem since we work in characteristic 0.

2.1.5 Lemma. *Let be $\varphi \in Aut(C)$ of prime order p. Then $p \leq g$ or $p = g + 1$ or $p = 2g + 1$.*

PROOF: Consider the Galois covering

$$\pi : C \to C/ < \varphi > .$$

Denote by $\tilde{g}$ the genus of $C/ < \varphi >$, from Hurwitz's formula we obtain:

$$2g-2 = p(2\tilde{g}-2) + v(\varphi)(p-1).$$

To prove our statement it is enough to assume $p \geq g+1$ and prove under this assumption that the only possible values for p are $g+1$ or $2g+1$.

If $\tilde{g} \geq 2$ then we have $2g-2 \geq p(2\tilde{g}-2) \geq 2p \geq 2g+2$, and this cannot happen.

If $\tilde{g} = 1$ then we have $2g-2 = v(\varphi)(p-1) \geq v(\varphi)g$. Since $v(\varphi) \geq 2$ (any automorphism of prime order of $Aut(C)$ which has one fixed point, must have at least two, see [FK80, V.2.11]), this cannot happen either.

If $\tilde{g} = 0$ then if $v(\varphi) \geq 5$ we have $2g-2 = -2p+v(\varphi)(p-1) \geq 3p-5 \geq 3g-2$, and this cannot happen. If $v(\varphi) = 4$ then from Hurwitz's formula $2g-2 = -2p+4(p-1) = 2p-4$ and this can happen only with $g = p+1$. If $v(\varphi) = 3$ then $2g-2 = -2p+3(p-1) = p-3$, which happens only for $p = 2g+1$. □

Applying Hurwitz's formula one obtains:

2.1.6 Theorem. (Hurwitz, 1893) *For any non-singular curve C of genus $g \geq 2$ we have*

$$\#Aut(C) \leq 84(g-1).$$

The proof of this result deals with the Galois cover $C \to C/Aut(C)$ and Hurwitz's formula on it, see [FK80, V.1.3].

Let us recall that we follow the notation of Hurwitz's formula introduced in the beginning of this notes.

2.1.7 Proposition. (Hurwitz, 1893) *Let be H a cyclic subgroup of $Aut(C)$ and denote by $\tilde{g}$ the genus of C/H and $m = \#H$. Then:*

1. *if $\tilde{g} \geq 2$ then $m \leq g-1$.*
2. *if $\tilde{g} = 1$ then $m \leq 2(g-1)$.*
3. *if $\tilde{g} = 0$ and* $\begin{cases} r \geq 4 \Rightarrow m \leq 2(g-1). \\ r = 4 \Rightarrow m \leq 6(g-1). \\ r = 3 \Rightarrow m \leq 10(g-1). \end{cases}$

The proof deals with Hurwitz's formula in the Galois cover $\pi : C \rightarrow C/H$.

2.1.8 Remark. *Wiman in 1895 improved the bound $m \leq 10(g-1)$ to $m \leq 2(2g+1)$ and showed that this is the best possible. Homma (1980) shows that this bound is attained if and only if the curve C is birational equivalent to $y^{m-s}(y-1)^s = x^q$ for $1 \leq s < m \leq g+1$.*

Let us finally collect some other properties that follow from an application of Hurwitz's formula:

2.1.9 Proposition. (Accola) *Let be H and H_j $1 \leq j \leq k$ subgroups of $Aut(C)$ such that $H = \bigcup_{j=1}^{k} H_j$ and $H_i \cap H_l = \{id\}$ if $i \neq l$. Denote by $m_j := \# H_j$, $m := \# H$, $\tilde{g}$ the genus of C/H and $\tilde{g}_j$ the genus of C/H_j. Then,*

$$(k-1)g + m\tilde{g} = \sum_{j=1}^{k} m_j \tilde{g}_j.$$

For a proof we refer to [FK80, V.1.10].

2.1.10 Corollary. *Let C be a genus 3 curve which is non-hyperelliptic. Then any involution σ on C is a bielliptic involution (i.e. the genus of $C/ < \sigma >$ is 1)(the researchers on Riemann surfaces instead of bielliptic involution use the terminology 2-hyperelliptic involution).*

Proof: Suppose that σ is an involution which is not a bielliptic involution, so that the genus of $C/ < \sigma >$ is two (because C is not hyperelliptic). Then, the Galois covering $\pi : C \rightarrow C/ < \sigma >$ is unramified (Hurwitz). We know that any genus 2 curve is hyperelliptic, therefore there exists $\tau \in Aut(C/ < \sigma >)$ such that the curve $(C/\sigma)/ < \tau >$ has genus 0. These covers are Galois, extend τ to a morphism on $K(C)$ the field corresponding to C this gives joint with σ a subgroup of order 4 in $Aut(C)$, $\mathbb{Z}/4$ is not possible for the ramification index of the covers, therefore we have $H = \mathbb{Z}/2 \times \mathbb{Z}/2 \leq Aut(C)$ where the genus of C/H is equal to zero. We have three involutions in H, one is σ, applying the above Accola result (proposition 2.1.9, know $k = 3, m_i = 2, m = 4$ if $H_1 =< \sigma >$ $\tilde{g}_1 = 2$ and $\tilde{g} = 0$) we obtain:

$$(3-1)3 + 30 = 2(2 + g_2 + g_3).$$

We have then that $g_2 + g_3 = 1$, therefore $g_2 = 0$ or $g_3 = 0$ which implies C is hyperelliptic, a contradiction. □

Let us make explicit the following straightforward consequence of the above proof.

2.1.11 Corollary. *Suppose that C has genus 3 and exists a subgroup H of $Aut(C)$ isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ such that the genus of C/H is zero. Impose moreover that one element of H fixes no point of C, then C is an hyperelliptic curve.*

Let us write down some results on fixed points using basically Hurwitz's formula on the covering given by fixing C by φ;

2.1.12 Lemma. *Let be $\varphi \in Aut(C)$ not the identity. Then $v(\varphi) \leq 2 + \frac{2g}{ord(\varphi)-1}$ where $ord(\varphi)$ is the order of this element in the group.*

See a proof in [FK80, V.1.5].

2.1.13 Proposition. *Let be $\varphi \in Aut(C)$ not the identity. If $v(\varphi) > 4$ then every fixed point of φ is a* WP.

We refer for a proof of this result to [FK80, V.1.7].

For more particular results on automorphism groups (for example the extension of the concept of WP to q-Weiertrass points which is useful to extend proposition 2.1.13 with $v(\varphi) > 2$ instead of 4; results around the question: when the involutions are in the center of $Aut(C)$?,...) we refer the interested reader to [FK80, chapter V].

Let us make explicit some of the general facts on $Aut(C)$ when $g = 3$:

Situation $g = 3$:
$\#Aut(C) \leq 168$ Only the primes $2, 3, 7$ can divide the order of $Aut(C)$ $Aut(C)$ is a finite subgroup of $PGL_3(K)$.

2.2 Automorphism groups of genus 3 curves

In this section we let C be a non-hyperelliptic genus 3 curve. We can think C embedded in $\mathbb{P}^2$ as a non-singular plane quartic.

Who determined first the list of groups appearing as automorphism groups on genus 3 curves over K? This is not clear to me. The result is published by Komiya and Kuribayashi in 1979 in an international available book [KK79], based in a talk deal by the authors in 1978 in Copenhagen. Recently, I noticed that the result is claimed (see [Ver83, p.62]) to be published in the year 1976 by Henn, in a publication of Heidelberg University [Hen76].

We present two approaches (at §2.2. the one given by Komiya and Kuribayashi [KK79] and at §2.1 another one given by Dolgachev [Dol06]). Both approaches study first a cyclic subgroup of $Aut(C)$ in order to obtain a model for C, and latter from this equation, obtain its fuller automorphism group. We reproduce also in §2.4 the tables and the result obtained by Henn [Hen76]. By the form of the statement, it seems that Henn's result is close to the approach given in §2.1, but I do not have Henn's manuscript [Hen76] to check this.

In §2.3 we give some results in terms of signature, we will think our curves with automorphism as points in the moduli space of genus 3 curve, and we determine which genus 3 curve has a big group of automorphism relating with the theory of "dessin d'enfant".

We want to warn the reader to be careful with the results of [Dol06] (or [KK79] in some concrete situations mainly in the hyperelliptic situation) because some restrictions on the values of the parameters or other minor details are missing or misprinted in the statements of results. Here we try to fix some of them, and hopefully this is complete at least in §2.1 following Dolgachev's approach (he introduced some of my corrections in his Lecture Notes after I sent him an e-mail noticing inaccuracies in the table. In other cases he did not believe me and they remain unchanged in Dolgachev's table, February 2005). In order to fix the minor inaccuracies on [KK79] with the hyperelliptic (and non-hyperelliptic situation, see remark 2.2.11) we refer to §6 of the paper [MSSV05] (see also the work [MSSV05] for lists of groups which appear in curves of genus ≤ 10).

2.2.1 Determination of the finite subgroups of PGL_3

We want to consider finite subgroups of PGL_3 up to conjugation. We restrict our attention to groups with less than 169 elements and the only prime orders appearing are 2, 3 or 7. For each of these subgroups in PGL_3 we shall study which ones have as fixed set in $\mathbb{P}^2$ a non-singular plane quartic. These are the automorphism groups we are looking for. Moreover we shall obtain equations for the quartics.

The idea to obtain the results is to use a cyclic subgroup H of order m, $H \leq Aut(C)$, in order to obtain a model equation for C, and from this model, find the full automorphism group. Let us review here the process used by Dolgachev in [Dol06]. We remind the reader that we try to fix some of the inaccuracies in [Dol06], for this reason we reproduce the proofs. When we write "He", we mean Dolgachev.

2.2.1 Proposition. *Let φ be an automorphism of order $m > 1$ of a non-singular plane quartic $C = V(F(X, Y, Z))$. Let us choose coordinates such that the generator of the cyclic group $H =< \varphi >$ is represented by the diagonal matrix $diag[1, \xi_m^a, \xi_m^b]$, where ξ_m is a primitive $m-$th root of unity. Then $F(X, Y, Z)$ is in the following list:*

Cyclic automorphism of order m.

	Type	$F(X,Y,Z)$
(i)	$2,(0,1)$	$Z^4 + Z^2L_2(X,Y) + L_4(X,Y)$
(ii)	$3,(0,1)$	$Z^3L_1(X,Y) + L_4(X,Y)$
(iii)	$3,(1,2)$	$X^4 + \alpha X^2YZ + XY^3 + XZ^3 + \beta Y^2Z^2$
(iv)	$4,(0,1)$	$Z^4 + L_4(X,Y)$
(v)	$4,(1,2)$	$X^4 + Y^4 + Z^4 + \delta X^2Z^2 + \gamma XY^2Z$
(vi)	$6,(3,2)$	$X^4 + Y^4 + \alpha X^2Y^2 + XZ^3$
(vii)	$7,(3,1)$	$X^3Y + Y^3Z + Z^3X$
(viii)	$8,(3,7)$	$X^4 + Y^3Z + YZ^3$
(ix)	$9,(3,2)$	$X^4 + XY^3 + Z^3Y$
(x)	$12,(3,4)$	$X^4 + Y^4 + XZ^3$

where $m, (a, b)$ is the Type of $\varphi = diag[1, \xi_m^a, \xi_m^b]$ and L_i denotes a generic homogenous polynomial of degree i.

2.2.2 Remark. *Note that, in the above list, the equation $F(X, Y, Z)$*

that we attach to some concrete type can have another type for some specific values of the parameters. For example in the situation (i) the case $L_2 = 0$ *has type* $4, (0, 1)$*; another example is (vi) with* $\alpha = 0$*, the equation having also type* $12, (3, 4)$.

PROOF:(Dolgachev) Take a non-singular plane quartic (i.e. with degree ≥ 3 in each variable) and let φ act by

$$(X : Y : Z) \mapsto (X : \xi_m^a Y : \xi_m^b Z).$$

Suppose first that $ab = 0$. Assume $a = 0$, (otherwise with the change of variables $Y \leftrightarrow Z$ we should obtain the same results). Write:

$$F := \beta Z^4 + Z^3 L_1(X, Y) + Z^2 L_2(X, Y) + Z L_3(X, Y) + L_4(X, Y).$$

If $\beta \neq 0$, then $4b \equiv 0 \mod m$, thus $m = 2$ or $m = 4$. If $m = 2$ then $L_1 = L_3 = 0$ and we obtain Type $2, (0, 1)$. If $m = 4$ $(b \neq 2)$, then $L_1 = L_2 = L_3 = 0$ and we get Type $4, (0, 1)$ (because type $4, (0, 3)$ can be reduced to this situation by change of variables $X \leftrightarrow Z$ multiplying the matrix by ξ_4).

If $\beta = 0$, then $3b = 0 \mod m$; then, $m = 3$ and thus $L_2 = L_3 = 0$ and we get Type $3, (0, 1)$ (the type $3, (0, 2)$ we can obtain with a change of variables type $3, (0, 1)$).

If $ab \neq 0$, we can suppose that $a \neq b$ and $mcd(a, b) = 1$ (otherwise by scaling we could reduce to the first situation). Then necessarily $m > 2$. Let $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$ and $P_3 = (0 : 0 : 1)$ be the reference points.

1. All reference points lie in the non-singular plane quartic

The possibilities for the equation are now:

$$\begin{aligned} F = X^3 L_{1,X}(Y, Z) + Y^3 L_{1,Y}(X, Z) + Z^3 L_{1,Z}(X, Y) + \\ + X^2 L_{2,X}(Y, Z) + Y^2 L_{2,Y}(X, Z) + Z^2 L_{2,Z}(X, Y), \end{aligned}$$

where $L_{i,B}$ denotes a homogenous polynomial of degree i with variables different from the variable B. It is easy to check that B_i can not appear in both L_{1,B_j} $j \neq i$, where $B_1 = X, B_2 = Y$ and $B_3 = Z$.

By change of the variables X,Y,Z, he assumes that:

$$F = X^3Y + Y^3Z + Z^3X + \\ + X^2L_{2,X}(Y,Z) + Y^2L_{2,Y}(X,Z) + Z^2L_{2,Z}(X,Y).$$

We see from the first 3 factors that $a = 3a + b = 3b \mod m$ therefore $m = 7$ and we can take a generator of H such that $(a,b) = (3,1)$. By checking each monomial's invariance we obtain that no other monomial enters in F; thus, we obtain Type $7,(3,1)$.

2. Two reference points lie in the plane quartic

By re-scaling the matrix φ and permuting the coordinates we can assume that $(1:0:0)$ does not lie in C. The equation is then:

$$F = X^4 + X^2L_2(Y,Z) + XL_3(Y,Z) + L_4(Y,Z),$$

because L_1 is not invariant by φ $(a,b \neq 0)$. Moreover Y^4 and Z^4 are not in L_4 because by assumption only $(1:0:0)$ does not lie in C.

Assume first that Y^3Z is in L_4. We have $3a + b = 0 \mod m$. Suppose Z^3Y is also in L_4 then $a + 3b = 0$ therefore $8b = 0 \mod m$ and then $m = 8$, we can take a generator φ with $(a,b) = (3,7)$ and we obtain Type $8,(3,7)$. If Z^3Y is not in L_4 then Z^3 is in L_3 (because non-singularity) and $3b = 0 \mod m$; this condition, together with $3a + b = 0 \mod m$, provides two situations: $m = 3$ and $(a,b) = (1,2)$ or $m = 9$ and $(a,b) = (3,2)$, but the first can not happen under the condition that Y^3Z is in L_4 and the second type is equal to $9,(3,2)$ of the table.

Up to a permutation of $Y \leftrightarrow Z$ we can assume now that Y^3Z and Z^3Y are not in L_4. By non-singularity we have that Y^3 and Z^3 should be in L_3, then $3b = 0$ and $3a = 0 \mod m$, therefore $m = 3$ and $(a,b) = (1,2)$ is the Type $3,(1,2)$ in the table.

3. One reference point lies in the plane quartic

By normalizing the matrix and permuting the coordinates we assume that $P_1 = (1:0:0)$ and $P_2 = (0:1:0)$ do not lie in C. We can write

$$F = X^4 + Y^4 + X^2L_2(Y,Z) + XL_3(Y,Z) + L_4(Y,Z),$$

where Z^4 does not enter in L_4 for the hypotheses on which references points lie or not lie in the quartic, L_1 does not appear because $ab \neq 0$. We have then $4a = 0 \bmod m$. By non-singularity Z^3 is in L_3, therefore $3b = 0 \bmod m$, hence $m = 6$ or $m = 12$. Imposing the invariance by φ we obtain

$$(*)F = X^4 + Y^4 + \alpha X^2Y^2 + XZ^3,$$

if $m = 6$ then $(a, b) = (3, 2)$ (and α may be different from 0), this is Type $6, (3, 2)$. If $m = 12$ then $(a, b) = (3, 4)$ from the above equation $(*)$ and $\alpha = 0$, this is Type $12, (3, 4)$.

4. None of the reference points lie in the plane quartic

In this situation

$$F = X^4+Y^4+Z^4+X^2L_2(Y,Z)+XL_3(Y,Z)+\alpha Y^3Z+\beta YZ^3+\iota Y^2Z^2,$$

where L_1 does not appears because $ab \neq 0$. Clearly $4a = 4b = 0 \bmod m$, therefore $m = 4$ and we can take $(a, b) = (1, 2)$ or $(1, 3)$ both situation define isomorphic curves (only by a renaming which is X, Y, Z in the equations), this is type $4, (1, 2)$. □

Let us now introduce some notation. Let G be a subgroup of the general linear group $GL(V)$ of a complex vector space of dimension 3. G is named intransitive if the representation of G in $GL(V)$ is reducible. Otherwise it is named transitive. An intransitive G is called imprimitive if G contains an intransitive normal subgroup G'; in this situation V decomposes into direct sum of G'-invariant proper subspaces and the set of representatives of G of G/G' permutates them. Let C_m denote the cyclic group of order m, S_i by the symmetric group of i-elements, A_i the alternate group of i-elements, D_i the dihedral group which has order $2i$. Denote by H_8 the group of order 8 given by $< \tau, \iota | \tau^4 = \iota^2 = 1, \tau\iota = \iota\tau^3 >$ which is an element of $Ext^1(C_2, C_4)$ and also an element of $Ext^1(C_2, C_2 \times C_2)$ (observe that H_8 is isomorphic to D_4). Q_8 denotes the quaternion group. Denote by $C_4 \circledcirc A_4$ the group given by $\{(\delta, g) \in \mu_{12} \times H : \delta^4 = \chi(g)\}/\pm 1$, where μ_n is the set of n-th roots of unity, H is the group A_4 and let take S, T a generators of H of order 2 and 3 respectively and χ is the character $\chi : H \to \mu_3$ defined by $\chi(S) = 1$ and $\chi(T) = \rho$ with ρ a fixed 3-primitive root of unity. Observe that this group is an element of $Ext^1(A_4, C_4)$ by projecting in the second component, which corresponds in the GAP library of small groups to the group identified by $(48, 33)$. You can found also a representation of this group of order 48 inside $PGL_3(\mathbb{C})$ in the table in §2.4. We denote by $C_4 \circledcirc (C_2 \times C_2)$ the group $(16, 13)$ in GAP library of small groups which is a group in $Ext^1(C_2 \times C_2, C_4)$, see this group inside the group $PGL_3(\mathbb{C})$ in the table given in §2.4.

2.2.3 Theorem. *In the following table we list all groups G for which there exists a non-singular plane quartic with automorphism group G. Moreover, we list for each group a plane quartic having exactly this group as automorphism group. These equations cover up to isomorphism all plane non-singular quartics having some non-trivial automorphism.*

Full automorphism group G.

$\lvert G\rvert$	G	$F(X, Y, Z)$	$P.M.$
168	$PSL_2(\mathbb{F}_7) \cong$ $PSL_3(\mathbb{F}_2)$	$Z^3Y + Y^3X + X^3Z$	
96	$(C_4 \times C_4) \rtimes S_3$	$Z^4 + Y^4 + X^4$	
48	$C_4 \circledcirc A_4$	$X^4 + Y^4 + Z^3X$	
24	S_4	$Z^4 + Y^4 + X^4+$ $3a(Z^2Y^2 + Z^2X^2 + Y^2X^2)$	$a \neq 0$, $a \neq \frac{-1\pm\sqrt{-7}}{2}$
16	$C_4 \circledcirc (C_2 \times C_2)$	$X^4 + Y^4 + Z^4 + \delta Z^2Y^2$	$\pm\delta \neq 0, 2, 6$, $2\sqrt{-3}$
9	C_9	$Z^4 + ZY^3 + YX^3$	
8	$H_8 = D_4$	$Z^4 + Y^4 + X^4+$ $\alpha Z^2(Y^2 + X^2) + \gamma Y^2X^2$	$\alpha \neq 0$, $\alpha \neq \gamma$
6	C_6	$Z^4 + aZ^2Y^2 + Y^4 + ZX^3$	$a \neq 0$
6	S_3	$Z^4 + Z(Y^3 + X^3)+$ $\alpha Z^2YX + \beta Y^2X^2$	$\alpha \neq \beta$, $\alpha\beta \neq 0$
4	$C_2 \times C_2$	$Z^4 + Y^4 + X^4+$ $Z^2(\alpha Y^2 + \beta X^2) + \gamma Y^2X^2$	$\alpha \neq \beta, \gamma$ $\beta \neq \gamma$
3	C_3	$Z^3L_1(Y, X) + L_4(Y, X)$	*not above*
2	C_2	$Z^4 + uZ^2L_2(Y, X)+$ $+L_4(Y, X)$	$u \neq 0$, *not above*

where P.M. means parameter restriction and "not above" means not K-isomorphic to any other model above it in the table.

2.2.4 Remark. *Any non-singular plane quartic over K with automorphism group G is K-isomorphic to the curve in the line of the group G, for some concrete values ofthe parameters. Moreover, for the lines with $n \geq 9$, the written equations have automorphism group exactly G. In §2.4 we show how one can ensure that an equation has exact group of automorphism the one predicted for the tables. We do this for the group $C_2 \times C_2$ but other situations can be implemented as well. (Information on Weierstrass points simplifies calculations).*

See §2.3 (or the table in §2.4) for the dimension of the subvariety of the moduli space of genus 3 curves representing curves with a fixed automorphism group G.

2.2.5 Remark. *The above table differs from Dolgachev's in some situations. For the reader's convenience we reproduce here Dolgachev's table in [Dol06] (in December 2004):*

n	G	$F(X,Y,Z)$	$P.M.$
168	$PSL_2(\mathbb{F}_7)$ $\cong PSL_3(\mathbb{F}_2)$	$Z^3Y + Y^3X + X^3Z$	
96	$(C_4 \times C_4) \rtimes S_3$	$Z^4 + Y^4 + X^4$	
48	$C_4 \circledcirc A_4$	$Z^4 + YX^3 + YX^3$	
24	S_4	$Z^4 + Y^4 + X^4 +$ $a(Z^2Y^2 + Z^2X^2 + Y^2X^2)$	$a^2 \neq a - 2$
16	$C_4 \times C_4$	$Z^4 + \alpha(Y^4 + X^4) + \beta Z^2X^2$	$\alpha, \beta \neq 0$
9	C_9	$Z^4 + ZY^3 + YX^3$	
8	Q_8	$Z^4 + \alpha Z^2(Y^2 + X^2) +$ $Y^4 + X^4 + \beta Y^2X^2$	$\alpha \neq \beta$
7	C_7	$Z^3Y + Y^3X + X^3Z +$ $+ aZY^2X$	$a \neq 0$
6	C_6	$Z^4 + aZ^2Y^2 + Y^4 + YX^3$	$a \neq 0$
6	S_3	$Z^4 + \alpha Z^2YX +$ $Z(Y^3 + X^3) + \beta Y^2X^2$	$a \neq 0$
4	$C_2 \times C_2$	$Z^4 + Z^2(\alpha Y^2 + \beta X^2) +$ $Y^4 + X^4 + \gamma Y^2X^2$	$\alpha \neq \beta$
3	C_3	$Z^4 + \alpha Z^2YX +$ $Z(Y^3 + X^3) + \beta Y^2X^2$	$\alpha, \beta \neq 0$
2	C_2	$Z^4 + Z^2L_2(Y,X) +$ $L_4(Y,X)$	*not above*

Typing errors explain the equations of the group of order 48 and C_6. Moreover the equation corresponding to C_3 can not be the same as S_3, some parameters on PM are not appearing in the equation for example in the curves with automorphism group S_3.
The group $C_4 \times C_4$ appears in Dolgachev's table with the equation $Z^4 + \alpha(Y^4 + X^4) + \beta Z^2X^2 = 0$. Observe that the change of variable of Y and Z with a 4-th root of α can reduce to the equation $Z^4 + Y^4 + X^4 + \beta' Z^2X^2 = 0$. It is clear that the last curve has $C_4 \times C_4$ as a subgroup of automorphisms given by diagonal matrices in $SL_3(K)$: $diag[\xi_4, \xi_4^2, \xi_4]$ and $diag[\xi_4, 1, \xi_4^3]$ where ξ_4 is a fixed 4-th root of unity of 1; however, this curve has more automorphisms, for example $\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$ which is an order two automorphism different from the above ones. Therefore this curve has a bigger group of automorphism and the equation is isomorphic to one above on it in the table. In particular, the group $C_4 \times C_4$ does not appear as an exact group of automorphism for a non-hyperelliptic genus 3 curve. Nevertheless, it appears another group of 16 elements which is not initially in Dolgachev's table.
The other big difference is the following one: Dolgachev writes that the cyclic group C_7 is the automorphism group for $Z^3Y + Y^3X + X^3Z + aZY^2X = 0$ with $a \neq 0$. This comes from a missprint calculation of the equations of Type 7(3,1) in proposition 2.2.1, observe that with $a \neq 0$ does not has Type $7(3,1)$ this equation. From proposition 2.2.1 the only curve with a cyclic group of order 7 is isomorphic to $X^3Z + Y^3X + Z^3Y = 0$.
Finally, he claims that the group of 8 elements is Q_8, but I obtain the Dihedral group $H_8 = D_4$ instead. Henn's result [Hen76] corroborates my calculations.

PROOF: (sketch, following Dolgachev)
Case 1: G an intransitive group realized as a group of automorphisms.
Case 1.a.:$V = V_1 \oplus V_2 \oplus V_3$.
Choose (X, Y, Z) such that V_1 spanned by $(1, 0, 0)$ and so on.
$\varphi \in G$ of order m, after scaling $\varphi = diag(1, a, b)$, we know models of equations and restrictions for m, a, b from above proposition 2.2.1.
Suppose $h \in G$ but $h \notin < \varphi >$, (choose m maximal with the property that G has an element of order m).

Study now situation by situation the equations on cyclic subgroups (i)-(x) (table in theorem 2.2.1):
Take $m = 12$, (x); we think $h = diag(1, \xi_{m'}^c, \xi_{m'}^d)$ then $4c = 3d = 0$ mod m', then $12|m'$ and $h \in < \varphi >$.
Nevertheless situation (x) has bigger automorphisms group which we will observe in case 1.b.
Similar arguments in the cases (v)-(x) to conclude: there are no other automorphism groups appearing as an intransitive group with $V = V_1 \oplus V_2 \oplus V_3$.(We need to observe here that in case (v) the situation $\gamma = 0$ is included in situation also (iv), by a change of name of the variables, given already bigger commutative subgroup inside the automorphism group, see next situation (iv)).

Case (iv) and suppose $h \notin < \varphi >$, let

$$L_4 = aX^4 + bY^4 + cX^3Y + dXY^3 + eX^2Y^2$$

assume $ab \neq 0$, $h = diag(\xi_{m'}^p, \xi_{m'}^q, 1)$, then $m' = 2$ or 4. If $m' = 2$ the only possibility is $(p, q) = (0, 1)$ or $(1, 0)(h \notin < \varphi >)$ where $c = d = 0$, but in this possibility we obtain a bigger group of automorphism.

If $m' = 4$, the only possibilities are:

$$(p, q) = (1, 0),\ (0, 1),\ (1, 3),\ (3, 1),\ (1, 2),\ (2, 1).$$

If $(p, q) = (1, 3)$ or $(3, 1)$ we have $c = d = 0$, so that this equation has bigger group and appears in the next cases (interchanging X and Y). If (p, q)= $(1, 2)$ or $(2, 1)$ similar as the case $(1, 3)$. The situation$(1, 0)$ implies $c = d = e = 0$, this is the Fermat quartic and it has a bigger automorphism group.
Assume now $a \neq 0$ and $b = 0$. $d \neq 0$ (non-singularity). One has $4p = 3p + q = 0$ mod m', then $c = e = 0$. But then we obtain the group $\mathbb{Z}/12$, situation (x) considered before.
Assume now $a = b = 0$. $cd \neq 0$(non-singularity). $3p + q = p + 3q = 0$ mod (m'), but then $m' = 8$ (studied above).
Similar argument applied:
Case (iii) One checks that no other element arises except when 1)$\alpha = \beta = 0$ which is the situation (ix), already studied;2)$\alpha = \beta$ then C_6 is a subgroup of the group an is already studied (vi),3)$\beta = 0$,$\alpha \neq 0$ no-reduced,4)$\alpha = 0$, $\beta \neq 0$ is C_6 in the group.
Case (ii): Since $L_1 \neq 0$ no h can exist.

Case (i): Only need to study when $h = diag(1, -1, 1)$ (i.e. we have $C_2 \times C_2$). We have that L_4 does not contain Y^3X and X^3Y and L_2 does not contain XY. In this situation one could have a bigger group of automorphism when $\alpha = \beta$ (see table).

Case 1.b. $V = V_1 \oplus V_2$ with $\dim V_2$=2, where V_2 irreducible representation of G (G is then non-abelian).
Choose coordinates s.t. $(1, 0, 0) \in V_1$, V_2 spanned by $(0, 1, 0), (0, 0, 1)$. $\overline{\varphi}$ restriction of φ to $W = V(Z) = \mathbb{P}(V_2)$, choose in SL_2. Write:

$$F = \alpha Z^4 + Z^3L_1(Y, X) + Z^2L_2(Y, X) + ZL_3(Y, X) + L_4(Y, X),$$

$L_1 = 0$ (irreducibility of V_2) and $\alpha \neq 0$(non-singularity).
If $L_2 \neq 0$, G leaves $V(L_2)$ invariant, $\overline{G}$ the restriction of G in W, the

$$\overline{G} \leq D_2$$

(always need in these arguments of case 1.b. that $\overline{G}$ is a subgroup of PSL_2, but if $\overline{G}$ is commutative we have to impose that is not a subgroup of SL_2(otherwise G commutative and is case 1.a.)), then by a change of variables of V_2 that the action of $\overline{G}$ is $u_1 : (x, y) \mapsto (-y, x)$ and $u_2 : (x, y) \mapsto (ix, -iy)$, then G can be only an extension of the $C_2 \times C_2$ (this group is $C_2 \times C_2$ in PSL_2 not in SL_2) situation above.

We need now to construct of possible $G's$ which $\overline{G}$ has the above property. Because C_2 sure is in G (see the comment in last paragraph) and re-scaling we can use the equations of (i), moreover C_4 is in G if we do the good elections, because $u_i^2 = -id$ and extending by 1 the action over X of $(X : Y : Z)$ one obtains a morphism of this degree. One can check that there are no more situations to consider, then u_1 and u_2 can be extended to G by the following matrices with ξ_4, ξ_4' 4-th root of unity (not necessary primitive):

$$\tilde{u_1} = \begin{pmatrix} \xi_4 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}; \; \tilde{u_2} = \begin{pmatrix} \xi_4' & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

We need to study all the possibilities for ξ_4 and ξ_4' up to scaling, we are in $PGL_3(K)$.

Let us make explicit two situations, the others with similar techniques are studied.

Observe for our first election in PGL_3 we choose $\varphi \in PGL_3$ with determinant 1, we obtain that $\overline{G}$ is generated in $PGL_3(K)$ by

$$\tau_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} ; \ \tau_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{pmatrix}.$$

Observe that in PGL_3 we have $\tau_i^4 = id$ and one can check that this group is Q_8. As τ_2 defines an automorphism of order 4, from the equation (v) (need re-scaling and changing the variables because now the action of this cyclic group is $diag[i, -1, 1]$) we obtain that the equation is $X^4 + Y^4 + Z^4 + \delta Z^2Y^2 + \gamma X^2YZ$. Impose now that τ_1 and τ_2 are automorphism of this equation, τ_1 implies that $\gamma = 0$, and τ_2 leaves invariant the curve

$$X^4 + Y^4 + Z^4 + \delta Z^2Y^2.$$

Since X only appears raised to the 4th power, this equation has automorphism group bigger of index 2 with respect to Q_8 with the automorphism acting only on X (we notice when $\delta = 0, \pm 6$ is isomorphic to $X^4 + Y^4 + Z^4$ which it will has bigger automorphism group, when $\delta = \pm 2$ is singular, and when $\delta = \pm 2\sqrt{-3}$ is isomorphic to $X^4 + Y^4 + Z^3X$, which one obtains a bigger automorphism group).

Let us now take another election in PGL_3 for $\overline{G}$, which we choose generated by:

$$\tau_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} ; \ \tau_2 = \begin{pmatrix} i & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{pmatrix}$$

now $\tau_2^2 = 1$ and $\tau_1^4 = 1$ and moreover $\tau_1\tau_2 = \tau_2\tau_1^3$. Moreover we have that they have a subgroup isomorphic to $C_2 \times C_2 =< \tau_1^2 \times \tau_2 >$ where $\tau_1^2 = diag[1, -1, -1]$ and $\tau_2 = diag[1, 1, -1]$, therefore to construct the equation in this situation we can use the equation obtained in case 1.a, with $C_2 \times C_2$ group of automorphism (here we do not need any change variable, 1 acts on X). Let impose that the equation $Z^4 + X^4 + Y^4 + Z^2(\alpha Y^2 + \beta X^2) + \gamma Y^2X^2$ is invariant by τ_1 and τ_2.

We obtain then for τ_1 that $\alpha = \beta$. Observe that τ_1, τ_2 generates H_8, therefore the curve

$$Z^4 + X^4 + Y^4 + \alpha Z^2(Y^2 + X^2) + \gamma Y^2 X^2$$

has a subgroup of automorphism H_8, (moreover let us observe that when $\alpha = 0$ has also as subgroup Q_8, therefore has a bigger group because $C_2 \times C_2 \leq H_8$ but $C_2 \times C_2 \not\leq Q_8$).

If $L_2 = 0$ but $L_3 \neq 0$, here $\overline{G} \leq D_3$ obtains that with the invariants of this elements one obtains a singular curve.
If $L_2 = L_3 = 0$ but $L_4 \neq 0$, $\overline{G}$ leave $V(L_4)$ invariant. One knows

$$\overline{G} \leq A_4$$

of order 12. One should study all these subgroups; for $\mathbb{Z}/2 \times \mathbb{Z}/2$ we can restrict to the equation given by step 1a and one obtains the group of 16 elements and the group of 48 elements of the table.

Case 2: G has a normal transitive imprimitive subgroup H.

H is a subgroup given above and permutates cyclically coordinates, therefore the only situations possible are (here we need to check from the list of all G finite in PGL_3 with this property has normal subgroup which appears in some situation in case 1 as a possible group of automorphism, and for every one of these possible G's, take all the equations (here we have more than the 10 situations that we began in case 1.a. because we need to joint the situations with bigger group appearing in case 1) and check which has this permutation of the variables)(here we eliminate by isomorphism some equations, for example the ones coming from (v) with $\gamma \neq 0$ with a change of variables are isomorphic to the ones happening in case 1.b with a subgroup in the automorphic group equal to D_4, similarly some situations which permutations of variables give new automorphisms are already studied in case 1.b and then are not consider now in the following list):

$$Z^4 + \alpha Z^2 Y X + Z(Y^3 + X^3) + \beta Y^2 X^2$$

$$Z^3 Y + Y^3 X + X^3 Z$$

$$Z^4 + Y^3 X + X^3 Y$$

$$Z^4 + Y^4 + Z^4 + 3a(Z^2Y^2 + Z^2X^2 + Y^2X^2)$$

In the first one of these equations, we see that the automorphism group is S_3 with the restrictions appearing above in the argument (the group is C_6 in some situations already studied in case 1a).
The second curve appearing is the Klein quartic, whose automorphism group is $PSL_2(\mathbb{F}_7)$.
The third equation is isomorphic to Fermat's quartic $X^4+Y^4+Z^4$. It has as a subgroup of automorphism $C_4^2 \rtimes S_3$ (S_3 from permutation of three variables and $C_4 \times C_4$ from automorphism coming from making a scale of the variables by a 4-th root of unity) of order 96, therefore it cannot be bigger by Hurwitz's bound.
The fourth equation, if $a = 0$ is the Fermat's curve (isomorphic to the third equation), or $a = \frac{1}{2}(-1 \pm \sqrt{-7})$ is isomorphic to Klein curve. If a does not take these values, clearly a subgroup of the $Aut(C)$ which consists with change the sign of the variable with permutations of the variables. This subgroup has order 24, and is isomorphic to S_4. To obtain that this is the full group of automorphism, we need a more careful study of the action of the automorphism group on Weierstrass points.

Case 3: G is a simple group.

There are only two transitive primitive groups of $PGL_3(K)$, one is $PGL_3(\mathbb{F}_2)$ given a quartic (taking the $(X : Y : Z)$ invariants by this group) isomorphic to the Klein quartic model which we obtained in case 2 (see next talk in the seminar, [Car06]).
The other has order bigger than 168, therefore can not be $Aut(C)$ of any genus 3 curve (by Hurwitz's theorem 2.1.6). □

2.2.2 Determination of $Aut(C)$ by cyclic covers

In this subsection we follow the proof which was printed firstly in an international accessible book (as far as I know). This is the work of Komiya and Kuribayashi [KK79]. We only write down some concrete situations of the proofs of the general statements, we refer to the original paper [KK79] for the interested reader.

Suppose that C is a non-hyperelliptic non-singular projective genus 3 curve, and suppose that C has a non-trivial automorphism σ. Clearly by Hurwitz's formula $C/ < \sigma >$ has genus 0, 1, or 2. If it is 2, we have then $\sigma^2 = id$, thus by corollary 2.1.10 C is hyperelliptic, in contradiction with our hypothesis. Therefore $C/ < \sigma >$ has genus 0 or 1, i.e. C has a Galois cyclic cover to a projective line or to an elliptic curve (as K is algebraically closed, any genus 1 curve has points).

If $Aut(C)$ has an element of order > 4 then $C/ < \sigma >$ has genus 0 (use Hurwitz's formula, proposition 2.1.7), therefore the Galois cyclic cover $\pi : C \to C/ < \sigma >$ is a cyclic cover of the projective line. We study the question about which groups are $Aut(C)$ for a genus 3 non-hyperelliptic curve C in two situations:

1. C curves which are a Galois cyclic cover of a projective line.

2. C curves which are a Galois cyclic cover of an elliptic curve but not of a projective line.

1. Cyclic covers of a projective line

Suppose that C has a Galois cyclic cover of order m then the extension of fields $K(C)/K(x)$ is a cyclic Galois extension with group C_m, then $K(C) = K(x,y)$ with $y^m \in K(x)$, therefore we can obtain an equation for our curve as follows:

$$y^m = (x - a_1)^{n_1} \cdot \ldots \cdot (x - a_r)^{n_r} \tag{2.1}$$

with $1 \leq n_i < m$ and $\sum_{i=1}^{r} n_i$ is divided by m where $a_1, \ldots, a_r$ are the points of the projective line over which the ramification occurs in the cyclic cover.

Apply now Hurwitz's proposition 2.1.7 with $g = 3$ and $\tilde{g} = 0$, we obtain that $m \leq 20$. In the original work [KK79] the situations C hyperelliptic and non-hyperelliptic genus 3 curve are deal together, but here we only do the non-hyperelliptic situation, (the results for hyperelliptic situation are stated in [KK79] and we refer to the interested reader there).

2.2.6 Theorem. *[KK79, Theorem 1] The projective, non-singular, non-hyperelliptic genus* 3 *curves which are a cyclic cover of order* m

(can have also a cyclic cover of order a multiple of m) of a projective line are listed below (up to isomorphism):

m	*Equation*
3	$y^3 = x(x-1)(x-\alpha)(x-\beta)$
4	$y^4 = x(x-1)(x-\alpha)$
6	$y^3 = x(x-1)(x-\alpha)(x-(1-\alpha))$
7	$y^3 + yx^3 + x = 0$
8	$y^4 = x(x^2-1)$
9	$y^3 = x(x^3-1)$
12	$y^4 = x^3 - 1$

,

Observe that each equation above in $\mathbb{P}^2$ becomes a non-singular quartic.

Let us here only reproduce how runs the proof of the above theorem in some concrete situation, the general proof is a study case by case with similar techniques. We know that $m \leq 20$. By Hurwitz's formula the cover $C \to C/C_m$ is not possible for $m = 5, 11, 13, 17$ and 19. From the conditions of the equation (2.1), about the ramification r and the conditions on n_i, we have that $m = 15, 16, 18$ and 20 are not possible either. Let us fix a concrete remaining m, take $m = 8$. The values of v_i can be only divisors of 8, then 2,4,8, therefore all the possibilities for the index of ramification satisfying $n_i \leq m$ and the divisibility condition are the following three:

	v_1	v_2	v_3	v_4	v_5
(i)	2	2	2	2	2
(ii)	2	2	4	4	
(iii)	4	8	8		

In the situations $(i), (ii)$ the equation becomes reducible, these situations can not occur. In the situation (iii) there are three possible different equations:
(1) $y^8 = (x-a_1)^2(x-a_2)^3(x-a_3)^3$
(2) $y^8 = (x-a_1)(x-a_2)(x-a_3)^6$
(3) $y^8 = (x-a_1)^2(x-a_2)(x-a_3)^5$
by a birational transformation $x = X$ and $y = (X-a_1)^{-2}(X-a_2)^{-1}(X-a_3)^{-1}Y$, one obtains that (2) is birational equivalent to (1), and one observes that (2) is an hyperelliptic curve, situation

that we do not work here in this talk.
Let us normalize the equation (3) as $y^8 = x^2(x-1)$. One computes a basis of differentials of the first kind $w_1 = y^{-3}dx$, $w_2 = y^{-6}xdx$, $w_3 = y^{-7}xdx$, and writing $x = -X^{-1}Y^4$, $y = Y$ one obtains a canonical model equation:

$$X^3Z + XZ^3 + Y^4 = 0$$

(and one observes that this quartic is isomorphic to Fermat's quartic $X^4 + Y^4 + Z^4 = 0$).

How can we obtain from theorem 2.2.6 the full automorphism group?
We use the equations in the projective model and case by case we study the group of elements of $PGL_3(K)$ that fix the quartic, we use here the result proposition 2.1.4, this is a work that you can find in [KK79, §2,§3] with the useful knowledge of lemma 2.1.2. More precisely, they distinguish different situations depending from the model equation, up to concrete missing situations they separate this study basically into two situations:
1) one with the affine model: $y^3 = x(x-1)(x-t)(x-s)$, and
2) second with the affine model: $y^4 = x(x-1)(x-t)$.

To obtain the exact group of automorphism (for 1) and 2)), one could study which $G \subseteq PGL_3(K)$ fixes the projective model, and this is the searching G, this is basically made in Komiya-Kuribayashi.

Let $F(X,Y,Z)$ be the equation of the quartic whose automorphism group we want to study (given by theorem 2.2.6). Solve the system of 15 equations (of degree 4 in the variables) from the equality

$$F(X',Y',Z') = kF(X,Y,Z)$$

with $k \neq 0$ where $\sigma(X,Y,Z) = (X',Y',Z')$ and $\sigma \in PGL_3(K)$.
This computation is so big, therefore to make this calculation one needs to use some more information. Komiya and Kuribayashi use the fact that WP maps by σ to WP (our lemma 2.1.2) to simplify the 15 equations to some managable systems with few equations.

They observe in the case 1) (which corresponds basically to Picard curves) that any automorphism σ fixes the point $P_\infty = (0:1:0)$, except for the equation $y^3 = x^4 - 1$. This simplify enormously the calculation of the automorphism group of the equation as a subgroup of PGL_3. In the case 2), they compute the Hessian, and observes that its Hessian has a good factorization given hight restrictions on Weierstrass points that lie on a line of multiplicity two which appears in the factorization of the Hessian, simplifying the calculation of the automorphism group inside PGL_3 (remember that $(F \cdot Hessian(F)) =$ Weierstrass points (each one with its weight multiplying)), see [KK79, pp.68-74].

Then one obtains,

2.2.7 Theorem. (Komiya-Kuribayashi) *The smooth, projective, non-hyperelliptic genus* 3 *curves which are a cyclic cover of order* m *of a projective line are isomorphic to one of the following equations and has the automorphism group associated to it:*

Equation $F(X,Y,Z)$	$Aut(V(F))$	m	*P.R.*
$Y^3Z + XZ^3 + X^3Y = 0$	$PGL_2(\mathbb{F}_7)$	7	
$Y^4 - X^3Z - XZ^3 = 0$	$(C_4 \times C_4) \rtimes S_3$	8	
$Y^3Z - X^4 + XZ^3 = 0$	C_9	9	
$Y^4 - X^3Z + Z^4 = 0$	$C_4 \circledcirc A_4$	12	
$Y^4 - X^3Z - \alpha XZ^3 +$ $+(\alpha - 1)X^2Z^2 = 0$	$C_4 \circledcirc (C_2 \times C_2)$	4	$\alpha \neq 0,\ 1, \ldots$
$X^4 - 2X^3Z + \alpha X^2Z^2 -$ $-(\alpha - 1)XZ^3 - Y^3Z = 0$	C_6	6	$\alpha \neq 1,\ 2$
$X^4 - Y^3Z -$ $-\alpha X^3Z + \beta X^2Z^2 -$ $-(\beta - \alpha + 1)XZ^3 = 0$	C_3	3	$\alpha \neq 2$ $(\alpha, \beta) \neq (0,0)$

2. Cyclic cover of a torus

We remember that the automorphism group has a cyclic element σ of order $m > 4$ then the genus of $C/ < \sigma >$ is zero and therefore a

cyclic cover of a projective line, and we did it above.
Let us impose that $m = 2, 3$ or 4. Write n the size of the whole automorphism group associated to the genus 3 curve C. Let us impose that $n > 4$ firstly, and we only make here a concrete proof in this situation to see now the key ingredients (as usual, for the general treatment, see [KK79] where work with C a general genus 3 curve which can also be an hyperelliptic curve). For $n > 4$ we have that $C/Aut(C)$ has genus 0 from Hurwitz's formula and one can see that $r \geq 3$ in this formula.
In such a situation one deduces from Hurwitz's formula that the Galois cover $\pi : C \to C/Aut(C)$ verifies the following:

1. If $r \geq 5$, then $n \leq 8$ and:
   (1) $n = 8$, $v_1 = v_2 = v_3 = v_4 = v_5 = 2$;
   (2) $n = 6$, $v_1 = v_2 = v_3 = v_4 = 2$, $v_5 = 3$.

2. If $r = 4$ then $n \leq 24$ and:
   (1) $n = 24$, $v_1 = v_2 = v_3 = 2$, $v_4 = 3$
   (2) $n = 16$, $v_1 = v_2 = v_3 = 2$, $v_4 = 4$
   (3) $n = 12$, $v_1 = v_2 = 2$, $v_3 = v_4 = 3$
   (4) $n = 8$, $v_1 = v_2 = 2$, $v_3 = v_4 = 4$
   (5) $n = 6$, $v_1 = v_2 = v_3 = v_4 = 3$.

3. If $r = 3$, then $n \leq 48$ and:
   (1) $n = 48$, $v_1 = v_2 = 3$,$v_3 = 4$
   (2) $n = 24$, $v_1 = 3$, $v_2 = v_3 = 4$
   (3) $n = 16$, $v_1 = v_2 = v_3 = 4$.

We need a study case by case. To show the ideas they use let us take the situation with $r \geq 5$ and $n = 6$. (There are situations that no such curve exists, another will obtain curves already studied above as cyclic cover of a projective line therefore we discard them).
Let us take $n = 6$ with ramification 2, 2, 2, 2, 3 and C be non-hyperelliptic. Because the automorphism group has order 6, we have an involution σ such that is bielliptic (see corollary 2.1.10). Let P_1 and P_2 be branch points with multiplicity 3 and τ the automorphism of order 3 by which P_1 and P_2 are fixed. We have that $\tau\sigma = \sigma\tau^2$ (is not cyclic here, otherwise we have already studied the situation by cyclic cover of projective line) and $C/<\tau>$ is an elliptic curve (we can suppose is not a projective line because we suppose is not a

cyclic cover of the projective line, and from Hurwitz's formula C has not genus 2).

We need some lemmas on divisors to help us:

2.2.8 Lemma. *Let C be a projective non-singular curve of genus g (≥ 3) and let ι an automorphism of C such that $C/<\iota>$ is an elliptic curve. Denote by v_P the ramification multiplicity of a branch point of the covering $\pi : C \to C/<\iota>$. Then the divisor $\sum(v_P - 1)P$ is canonical.*

PROOF: Let w be a differential of first kind of the elliptic curve, think as differential of C by pull back we obtain

$$div_C(w) = \pi^{-1} div_{C/<\iota>}(w) + \sum(v_P - 1)P = \sum(v_P - 1)P.$$

□

The following lemma is not useful in our concrete situation $n = 6$ but it is useful in others. Let us write it here.

2.2.9 Lemma. *Let C be a projective, non-singular, non-hyperelliptic genus 3 curve. Assume that C has an automorphism ι of order 4 and ι has fixed points on C. Then the $v(\iota) = 4$, denote by P_1, P_2, P_3 and P_4 this four fixed points. Moreover we have that $\sum_{i=1}^{4} P_i$ and $4P_i$ $1 \leq i \leq 4$ are canonical divisors.*

Let us follow our concrete situation with $n = 6$. We obtain from lemma 2.2.8 that $2(P_1 + P_2)$ is a canonical divisor.

Let also write the group $G = \{1, \tau, \tau^2, \sigma = \sigma_1, \sigma_2 = \tau\sigma_1, \sigma_3 = \tau^2\sigma_1\}$, where σ_i are involutions (all bielliptic).
Let $\{Q_i^{(1)}\}$, $\{Q_i^{(2)}\}$, $\{Q_i^{(3)}\}$ be the set of 4 fixed points by $\sigma_1, \sigma_2, \sigma_3$ respectively. By lemma 2.2.8 we know $\sum_{i=1}^{4}\{Q_i^{(1)}\}$, $\sum_{i=1}^{4}\{Q_i^{(2)}\}$ and $\sum_{i=1}^{4}\{Q_i^{(3)}\}$ are canonical divisors.

From the relation $\sigma_1\sigma_2\sigma_1 = \sigma_3$ we have hat $\sigma_1(\sum_{i=1}^{4}\{Q_i^{(2)}\}) = \sum_{i=1}^{4}\{Q_i^{(3)}\}$ and one checks that $\sigma_1 P_1 = P_2$. Let us define the meromorphic functions

$$div(x) = \sum_{i=1}^{4}\{Q_i^{(2)}\} - 2(P_1 + P_2)$$

$$div(y) = \sum_{i=1}^{4}\{Q_i^{(3)}\} - 2(P_1 + P_2)$$

we have $\sigma_1(x) = \alpha y$ and because σ_1 is an involution $\sigma_1(y) = \beta x$ with $\alpha\beta = 1$, rewrite y instead of αy.
Now one checks that $1, x, y$ are a basis for $L(2P_1 + 2P_2)$ with $\tau(x) = -y$ and $\tau(y) = x - y$.
Apply now the following change

$$x_1 = \frac{x - 2y + 1}{x + y + 1},\ y_1 = \frac{-2x + y + 1}{x + y + 1},$$

where now the action of σ_1 and τ are given by

$$\sigma_1 : (x_1, y_1) \mapsto (y_1, x_1),\ \ \tau : (x_1, y_1) \mapsto (y_1/x_1, 1/x_1),$$

and one has $1, x_1, y_1$ are a basis for $L(K)$ where K means the canonical divisor. Because $dimL(4K) = 11$ we obtain an equation $f(x_1, y_1) = \sum a_{i,j}x_1^i y_1^j$ with $i + j \leq 4$, $i, j \geq 0$ and with homogenous coordinates the group acts by

$$\sigma_1 \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

$$\tau \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

then the equation is invariant for the group S_3 and therefore the equation is

$$A(X^4 + Y^4 + Z^4) + B(X^3Y + Y^3X + Z^3X + X^3Z + Z^3Y + Y^3Z)$$
$$+C(X^2Y^2 + Y^2Z^2 + X^2Z^2) = 0$$

for some A, B, C. If $B = C = 0$ and $A \neq 0$ is isomorphic to $y^4 = x(x^2 - 1)$ which has cyclic cover of a projective line, this is already studied. If $B = 0$ and $AC \neq 0$ has a group of order 24, except when $C/A = 3\mu$ with $\mu \in \{\frac{-1\pm\sqrt{-7}}{2}\}$ where for this concrete situation is isomorphic to the Klein quartic which automorphism group is isomorphic to a group of 168 elements and is already studied in the cyclic cover of a projective line. For $ABC \neq 0$ we obtain that the full group of automorphism is G (this result is obtained by using proposition 2.1.4).

Working situation by situation Komiya and Kuribayashi (with similar techniques and some results on genus 3 curves with fix number of Weierstrass points from the article [KK77]) obtain the following statement:

2.2.10 Theorem. (Komiya-Kuribayashi) *A smooth, projective, non-hyperelliptic genus* 3 *curve which is a cyclic cover of an elliptic curve and not of a projective line, is isomorphic to one of the following equations and has the indicated automorphism group:*

$Equation\{F(X,Y,Z)=0\}$	$Aut(V(F))$	$P.R.$
$X^4+Y^4+Z^4+$ $+3a(X^2Y^2+X^2Z^2+Z^2Y^2)=0$	S_4	$a\neq 0$ $a^2\neq a-2$
$X^4+Y^4+Z^4+$ $+aX^2Y^2+b(X^2Z^2+Y^2Z^2)=0$	$H_8=D_4$	$a\neq b$
$X^4+Y^4+Z^4+$ $+c(X^2Y^2+Y^2Z^2+X^2Z^2)+$ $+b(X^3Y+Y^3X+Z^3X+X^3Z+$ $+Z^3Y+Y^3Z)=0$	S_3	$bc\neq 0$
$X^4+Y^4+Z^4+$ $+2aX^2Y^2+2bX^2Z^2+2cY^2Z^2=0$	$C_2\times C_2$	
$a(X^4+Y^4+Z^4)+b(X^3Y-Y^3X)+$ $+cX^2Y^2+d(X^2Z^2+Y^2Z^2)=0$	$C_2\times C_2\leq$	
$a(X^4+Y^4+Z^4)+$ $+b(X^3Y+Y^3Z+XZ^3)+$ $+c(Y^3X+X^3Z+Y^3Z)+$ $+d(X^2Y^2+X^2Z^2+Y^2Z^2)=0$	$C_3\leq$	
$X^4+Y^4+Z^4+$ $+Y^2(a_0X^2+a_1XZ+bZ^2)+$ $+(a_2X^3Z+a_3X^2Z^2+a_4XZ^3)=0$	C_2	

2.2.11 Remark. *In the column of $Aut(C)$ of the above table $\leq$ means that the group written is a subgroup of the whole automorphism group (check the appendix of [KK79] and also §III.6 [MSSV05]). These situations are listed above and then we can eliminate them from the table.*

2.2.3 Final remarks

The approach of Komiya-Kuribayashi consists in listing all the group signature pairs, and for ach one obtain the exact automorphism group which occurs if such a situation is admissible, (i.e. if its possible). Let us introduce this language a little bit.
Let C be a curve of genus ≥ 2 (in this subsection). Let H be a subgroup of $Aut(C)$ then we can consider the cover $\pi : C \to C/H$ and denote by $g_0 = genus(C/H)$ and Hurwitz's formula reads:

$$2(g-1)/|H| = 2(g_0 - 1) + \sum_{i=1}^{r}(1 - \frac{1}{m_i}),$$

then we define the signature associate to this cover is $(g_0; m_1, \ldots, m_r)$ where we have exactly r ramification points.

For Riemann surfaces of genus ≥ 2 we have a Fuchsian group K such that $C = \mathbb{H}/K$ and $Aut(C) = Norm(K)/K$ where $Norm(K)$ is the normalization inside $PSL_2(\mathbb{R})$ of K, these Fuchsian groups are added with a signature, and π relates the Fuchsian group K as a normal subgroup of a concrete Fuchsian group of signature $(g_0; m_1, \ldots, m_r)$ (see [Bre00] for an extended explanation).

Basically Hurwitz's formula gives restriction to the possible signatures for a subgroup H. One needs to obtain results in the direction: Is this group the exact group of automorphism or not?. Breuer [Bre00] lists the possible signatures and subgroups H that could be subgroups of the automorphism group for curves of genus ≤ 48, but it remains to discard a lot of signatures which does not give the exact group of automorphism (as did originally Komiya-Kuribayashi in [KK79] for genus 3 curves), in this direction the work [MSSV05] reobtains Komiya-Kuribayashi's result using more the approach on Fuchsian groups. Next, we only list, for every group which is $Aut(C)$

for a genus 3 non-hyperelliptic curve, the signature that has for the covering $\pi : C \to C/Aut(C)$ from §2.2:

$Aut(C)$	signature
$PSL_2(\mathbb{F}_7)$	$(0; 2, 3, 7)$
S_3	$(0; 2, 2, 2, 2, 3)$
C_2	(1;2,2,2,2)
$C_2 \times C_2$	$(0; 2, 2, 2, 2, 2, 2)$
D_4	$(0; 2, 2, 2, 2, 2)$
S_4	(0;2,2,2,3)
$C_4^2 \rtimes S_3$	(0;2,3,8)
$C_4 \circledcirc (C_2)^2$	(0;2,2,2,4)
$C_4 \circledcirc A_4$	(0;2,3,12)
C_3	$(0; 3, 3, 3, 3, 3)$
C_6	(0;2,3,3,6)
C_9	(0;3,9,9)

Let us recall some facts presented in the seminar on "dessins d'enfants"[Xar05] (genus of C is always is bigger than or equal to 2).

Let us denote by $\mathcal{M}_g$ the moduli space of genus g curves. Let us denote by $\mathcal{M}_{g,r}$ the moduli space of genus g curves with r different marked points where we view the marked points as unordered. It is known that the dimension of these moduli spaces ($genus \geq 2$) are given by

$$dim(\mathcal{M}_{g,r}) = 3g - 3 + r.$$

2.2.12 Remark. *From the above classification of curves with automorphism and joining the classification for hyperelliptic genus 3 curves, and because $dim(M_3) = 6$, we obtain that there a lot of non-hyperelliptic genus 3 curves that has no automorphism, in particular the generic curve for $\mathcal{M}_3$ has no automorphism. (See [ST05] for an equation of the generic genus 3 curve).*

A curve C is said to have a large automorphism group if its point in $\mathcal{M}_g$ has a neighborhood (in the complex topology) such that any other curve in this neighborhood has an automorphism group a group with strictly less elements than the automorphism group that has the curve C.

2.2.13 Theorem. (P.B.Cohen, J.Wolfart) *Let C be a curve over $\mathbb{C}$ with a large automorphism group ($g \geq 2$). Then $C/Aut(C)$ is the projective line and moreover the Galois cover $\pi : C \to C/Aut(C)$ is a Belyî morphism.*

We have by the general theory of "dessins d'enfants",

2.2.14 Corollary. *Any curve C with a large automorphism group is defined over $\overline{\mathbb{Q}}$ and therefore over a number field.*

2.2.15 Corollary. *Let C be a curve defined over $\mathbb{C}$ ($g \geq 2$). Then: C has a large automorphism group if and only if exists a Belyî function defining a normal covering $\pi : C \to \mathbb{P}^1$.*

If we center now in our tables for non-hyperelliptic genus 3 curves, observe from the signatures that the curves, which ramify in exactly three points and the genus of $C/Aut(C)$ is zero, are exactly the curves having a large automorphism group:

List of all non-hyperelliptic genus 3 curves
with large automorphism group (up to isomorphism):

C, curve	$Aut(C)$
$Z^3Y + Y^3X + X^3Z$	$PSL_2(\mathbb{F}_7)$
$Z^4 + X^4 + Y^4$	$C_4^2 \rtimes S_3$
$X^4 + Y^4 + XZ^3$	$C_4 \circledcirc A_4$
$Z^4 + ZY^3 + YX^3$	C_9

In [MSSV05] it is said that C has a large automorphism group if

$$|Aut(C)| > 4(g-1).$$

According to this terminology the genus 3 curves with $|Aut(C)| > 8$ "have large automorphism group". This other terminology does not relate well with "desinn d'enfants"theory; see the situation for the curve with automorphism group S_4 and/or $C_4 \circledcirc C_2^2$ in the tables. Nevertheless is a general fact that with this second notion of "having a large automorphism group"one can prove that the curves C which satisfy this second notion have $C/Aut(C)$ of genus 0 and the cover $\pi : C \to C/Aut(C)$ ramifies at 3 or 4 points (pp. 258-260 [FK80]).

2.2.4 Henn's table

We reproduce Henn's table [Hen76], which can be found in [Ver83].

Let G be a finite group and let $\beta : G \to PGL_3(\mathbb{C})$ be a projective representation of G. Let $S(\beta) \subseteq \mathcal{M}_3 \backslash \mathcal{H}_3$ be the locus of moduli points of non-hyperelliptic curves containing $\beta(G)$ in their automorphism group. In §2.3 we compute $s_\beta := dim(S(\beta))$, which corresponds to the number of free parameters in the equation of genus 3 curves corresponding to the points of $S(\beta)$.

2.2.16 Theorem. (Henn) *The following table classifies smooth plane quartics with non-trivial automorphisms. For each G in this table, there exists a smooth quartic C with $\beta(G) = Aut(C)$ and the locus $S(\beta)$ is an irreducible subvariety of $\mathcal{M}_3 \setminus \mathcal{H}_3$.*

G	*Equation* $F(X,Y,Z)$ *up to* $K - isomorphism$	s_β	*generators* *of* $\beta(G)$
C_2	$X^4 + X^2L_2(Y,Z) + L_4(Y,Z)$	4	$diag[-1,1,1]$
$C_2 \times C_2$	$X^4 + Y^4 + Z^4+$ $+aX^2Y^2 + bY^2Z^2 + cZ^2X^2$	3	$diag[-1,1,1]$ $diag[1,-1,1]$
C_3	$Z^3Y + X(X-Y)\cdot$ $\cdot(X-aY)(X-bY)$	2	$diag[1,1,\rho]$
C_6	$Z^3Y + X^4 + aX^2Y^2 + Y^4$	1	$diag[-1,1,\rho]$
S_3	$X^3Z + Y^3Z + X^2Y^2+$ $+aXYZ^2 + bZ^4$	2	$diag[\rho,\rho^2,1]$ B
D_4	$X^4 + Y^4 + Z^4+$ $+aX^2Y^2 + bXYZ^2$	2	$diag[i,-i,1]$ B
C_9	$X^4 + XY^3 + YZ^3$	0	$diag[\rho,1,\omega]$
$C_4 \circledcirc (C_2 \times C_2)$	$X^4 + Y^4 + Z^4 + aX^2Y^2$	1	$diag[-1,1,1]$ $diag[i,-i,1]$ B'
S_4	$X^4 + Y^4 + Z^4+$ $a(X^2Y^2 + Y^2Z^2 + Z^2X^2)$	1	A, B'
$C_4 \circledcirc A_4$	$X^4 + Y^4 + Z^4+$ $(4\rho + 2)X^2Y^2$	0	V, V'
$(C_4 \times C_4) \rtimes S_3$	$X^4 + Y^4 + Z^4$	0	A, U
$PSL_2(\mathbb{F}_7)$	$X^3Y + Y^3Z + Z^3X$	0	[Car06]

where ρ is a primitive 3-rd root of unity, $\omega^3 = \rho$ and:

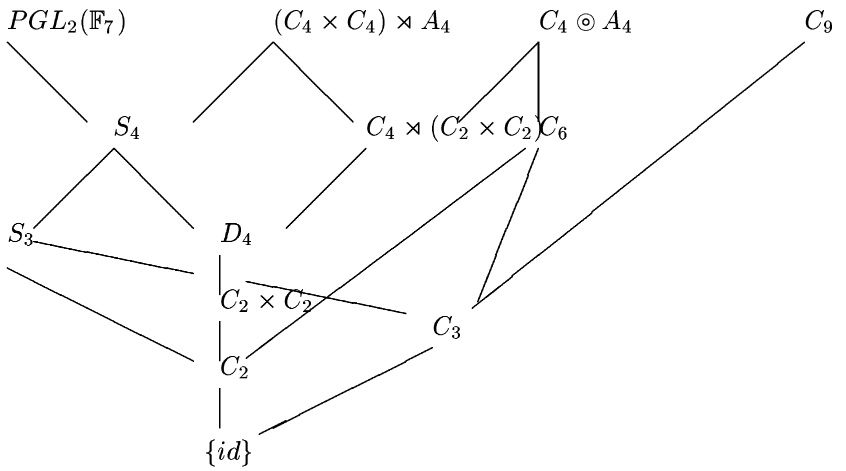
$$A := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad U := \begin{pmatrix} -i & 0 & 0 \\ 0 & 0 & 1 \\ 0 & i & 0 \end{pmatrix},$$

$$B := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B' := \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$V := \begin{pmatrix} \frac{1+i}{2} & \frac{-1+i}{2} & 0 \\ \frac{1+i}{2} & \frac{1-i}{2} & 0 \\ 0 & 0 & \rho \end{pmatrix}, \quad V' := \begin{pmatrix} \frac{1+i}{2} & \frac{-1-i}{2} & 0 \\ \frac{-1+i}{2} & \frac{-1+i}{2} & 0 \\ 0 & 0 & \rho^2 \end{pmatrix}.$$

We give here a kind of algorithm that we run only in a particular situation. We want to check when the model equation in the table has exact group of automorphism the one that is writed in the same line. For example: which models of type $X^4+Y^4+Z^4+aX^2Y^2+bY^2Z^2+cX^2Z^2$ of Henn's table have exact automorphism group $C_2 \times C_2$ and not a bigger automorphism group?

The algorithm uses the matrix presentation of the automorphism group for the models, for which we use Henn's table. The other tables help in this process too. Let us write down the scheme diagram of groups in the table ordered by inclusion (see [Ver83, p.64]):



Let us describe an algorithm to check which of the equation models of type $X^4+Y^4+Z^4+aX^2Y^2+bY^2Z^2+cX^2Z^2$ of Henn's table has exact automorphism group $C_2 \times C_2$ and not a bigger automorphism group.

From the given scheme of groups, it is enough to prove that the model equation has no D_4 as a subgroup of automorphism. Let us modify the realization of D_4 in $PGL_3(\mathbb{C})$ given in Henn's table in order that the two generators of $C_2 \times C_2$ are given by $diag[-1,1,1]$ and $diag[1,1,-1]$ (is the same group as Henn's gives, but we choose other generators for the group $C_2 \times C_2$). We write now the realization of D_4 in $PGL_3(\mathbb{C})$ in such a way that $C_2 \times C_2$ as a subgroup of D_4 is given by $diag[-1,1,1]$ and $diag[1,1,-1]$. Henn's table shows us a realization of D_4 in $PGL_3(\mathbb{C})$, we need to do a conjugation by a matrix A of this realization in order to obtain the one interested for us, in our concrete situation we need A such that:

$$A\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = diag[-1,1,1]A,$$
$$A\,diag[-1,-1,1] = diag[1,1,-1]A,$$

where $diag[-1,-1,1] = (diag[i,-i,1])^2$ (here we fix some election in choosing the variables).

Imposing this conditions we obtain that we can choose A an invertible matrix of the form

$$A = \begin{pmatrix} 1 & -1 & 0 \\ r & r & s \\ t & t & u \end{pmatrix},$$

observe $det(A) = 2(ru-ts) \neq 0$.

Let us consider the automorphism ¥ of D_4 given by

$$\frac{1}{2(ru-ts)}\begin{pmatrix} 0 & 2ui & -2si \\ ir2(ru-ts) & -2st & 2rs \\ it2(ru-ts) & -2ut & 2ru \end{pmatrix} = A\,diag[i,-i,1]A^{-1}.$$

In order that our model equation for $C_2 \times C_2$ has no bigger automorphism group is enough that ¥ is not automorphism of the model equation for $C_2 \times C_2$ in Henn's table. We compute which conditions a, b and c (in the model equation for $C_2 \times C_2$) should satisfies in order to have this ¥ as automorphism (we impose $F(\yen(X,Y,Z)) = kF(X,Y,Z)$ with F the model for $C_2 \times C_2$ and $k \neq 0$ and/or that the model F_{D_4} of D_4 by the change of A become a multiple of the model for $C_2 \times C_2$ given by Henn's table; we do this last approach for the calculations). One obtains that all the possible solutions in which the model for $C_2 \times C_2$ comes from the model of D_4 are the following: when $a = b$ or $b = c$ or $a = c$ or $a = -b$ or $a = -c$ or $b = -c$. Observe moreover that if the model of equation of $C_2 \times C_2$ of Henn's table

$$X^4 + Y^4 + Z^4 + aX^2Y^2 + bY^2Z^2 + cX^2Z^2$$

satisfies $a = b$ or $b = c$ or $a = c$ or $a = -b$ or $a = -c$ or $b = -c$, we have seen in the table of theorem 2.2.3 (for the equation with D_4 as automorphism group) that has bigger automorphism group that $C_2 \times C_2$ (straightforward for the situations $a = b$ or $b = c$ or $a = c$, and for the situations with $-$ do the change of variables $X \longleftrightarrow iX$ or $Y \longleftrightarrow iY$ or $Z \longleftrightarrow iZ$ to conclude, compare then with the result in theorem 2.2.3).

Acknowledgments

It is a big pleasure to thank Everett Howe for noticing me the existence of the work of Vermeulen [Ver83] in order to improve this manuscript, and Xavier Xarles for calling my attention on the "dessins d'enfants" seminar and the relationship of the results there with the present work.

F. Bars
Departament de Matemàtiques
Edifici C
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona
francesc@mat.uab.es

Capítol 3

La quàrtica de Klein

Gabriel Cardona i Julio Fernández

En aquest capítol estudiem la quàrtica de Klein des del punt de vista geomètric, aritmètic i modular. En primer lloc, estudiem la corba sobre els complexos, en particular el seu grup d'automorfismes, els punts distingits, el seus quocients i la seva jacobiana. Després es troben els seus punts racionals sobre $\mathbb{Q}$ i les reduccions mòdul alguns primers. Finalment, mostrem que la clàssica corba modular $X(7)$ admet la quàrtica de Klein com a model racional. També estudiem alguns quocients d'aquesta corba per subgrups d'automorfismes. Com a aplicació, donem una demostració del teorema de Stark-Heegner sobre la finitud del conjunt de cossos quadràtics imaginaris amb grup de classes trivial. La referència bàsica per a tot el capítol és [Elk99].

3.1 La quàrtica de Klein sobre $\mathbb{C}$

3.1.1 Models i automorfismes de la quàrtica de Klein

L'objecte d'estudi és la corba projectiva, llisa i irreductible de gènere 3 donada per l'equació quàrtica

$$\mathcal{X} = \{(X : Y : Z) \mid X^3Y + Y^3Z + Z^3X = 0\} \subset \mathbb{P}^2,$$

que anomenarem quàrtica de Klein. En aquesta secció estudiarem propietats de la corba sobre els nombres complexos, tot i que la majoria de resultats que donarem es poden interpretar correctament sobre una clausura algebraica de $\mathbb{Q}$ o sobre un cos de nombres que contingui les arrels setenes de la unitat. Per tal de fixar notacions, notarem per $\zeta = \zeta_7$ una arrel setena de la unitat, $K = \mathbb{Q}(\zeta)$ i $k = \mathbb{Q}(\sqrt{-7})$; els seus anells d'enters respectius són $\mathcal{O}_K = \mathbb{Z}[\zeta]$ i $\mathcal{O}_k = \mathbb{Z}[\alpha]$, amb $\alpha = \frac{-1+\sqrt{-7}}{2} = \zeta + \zeta^2 + \zeta^4$.

Els automorfismes d'aquesta quàrtica es poden representar com a elements de $\mathrm{GL}_3(\mathbb{C})$, de manera que una tal matriu M actua sobre la corba com

$$(X:Y:Z) \mapsto (X':Y':Z'), \qquad \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = M \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

De fet, el grup d'automorfismes de $\mathcal{X}$ és isomorf a $\mathrm{PSL}_2(\mathbb{F}_7)$ (o a $\mathrm{GL}_3(\mathbb{F}_2)$) i està generat per 3 automorfismes que, amb la notació matricial, es representen com:

$$g = \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix}, \qquad h = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$s = \frac{-1}{\sqrt{-7}} \begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix}.$$

Aixídoncs, tenim una representació fidel 3-dimensional del grup $G = \mathrm{PSL}_2(\mathbb{F}_7)$ de manera que la seva imatge correspon al grup d'automorfismes de $\mathcal{X}$.

De fet, podriem fer el camíinvers i, partint d'una representació de G, obtenir altres models per a $\mathcal{X}$. Considerem, doncs,

$$\rho : G = \mathrm{PSL}_2(\mathbb{F}_7) \to \mathrm{GL}_3(\mathbb{C})$$

una representació de G; via ρ, el grup G actua de manera natural sobre $\mathbb{C}[X,Y,Z]$, i la subàlgebra d'elements invariants sota aquesta acció està generada per quatre polinomis $\Phi_4, \Phi_6, \Phi_{14}, \Phi_{21}$, on el subíndex indica el grau del polinomi, entre els quals hi ha una única relació algebraica que involucra termes de grau 42. Aleshores, l'equació $\Phi_4 = 0$ dóna un model projectiu per a la corba $\mathcal{X}$, de manera que el seu grup d'automorfismes és $\rho(G)$.

Considerant la representació donada abans, els polinomis invariants que s'obtenen són:

$$\begin{aligned}
\Phi_4 &= X^3Y + Y^3Z + Z^3X, \\
\Phi_6 &= XY^5 + YZ^5 + ZX^5 - 5X^2Y^2Z^2, \\
\Phi_{14} &= X^{14} + Y^{14} + Z^{14} - 34(X^{11}Y^2Z + Y^{11}Z^2X + Z^{11}X^2Y) + \dots, \\
\Phi_{21} &= X^{21} + Y^{21} + Z^{21} - 7(X^{18}Y^2Z + Y^{18}Z^2X + Z^{18}X^2Y) + \dots,
\end{aligned}$$

mentre que la relació entre ells és

$$\Phi_{21}^2 = \Phi_{14}^3 - 1728\Phi_6^7 + \Phi_4(1008\Phi_6^4\Phi_{14} + \dots).$$

Ens referirem a aquesta representació, juntament amb el model per a $\mathcal{X}$ que se n'obté com a model de Klein.

Un altre model es pot trobar considerant la representació:

$$g \mapsto \frac{1}{2}\begin{pmatrix} -1 & 1 & \bar{\alpha} \\ \alpha & \alpha & 0 \\ -1 & 1 & \bar{\alpha} \end{pmatrix}, \quad h \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad s \mapsto -\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Calculant la corresponent subàlgebra invariant, obtenim el polinomi quàrtic invariant

$$\Phi_4' = X^4 + Y^4 + Z^4 + 3\alpha(X^2Y^2 + Y^2Z^2 + Z^2X^2),$$

que ens proporciona un altre model per a $\mathcal{X}$, que anomenarem model S_4.

Observem que, dels dos models que hem donat, en el primer la corba està definida sobre $\mathbb{Q}$ i els seus automorfismes sobre $\mathbb{Q}(\zeta_7)$, mentre que en el segon, tant la corba com els automorfismes estan definits sobre l'extensió quadràtica $\mathbb{Q}(\sqrt{-7})$.

Un es podria demanar si és possible trobar un model que sigui millor que els dos anteriors, en el sentit que tant la corba com els automorfismes estiguin definits sobre $\mathbb{Q}$. La resposta, negativa, a aquesta pregunta es pot trobar mirant la taula de caracters del grup G, de la qual es dedueix que la imatge de qualsevol representació 3-dimensional ha de contenir $\sqrt{-7}$.

c	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
$\#c$	1	21	56	42	24	24
χ_1	1	1	1	1	1	1
χ_3	3	-1	0	1	α	α
$\bar{\chi}_3$	3	-1	0	1	$\bar{\alpha}$	$\bar{\alpha}$
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

3.1.2 Punts distingits de la quàrtica de Klein

La geometria de la quàrtica de Klein, en especial els seus punts distingits, està lligada a subgrups distingits de $G = \mathrm{Aut}(\mathcal{X})$.

L'òrbita d'un punt genèric de $\mathcal{X}$ sota l'acció de G està formada per $\#G = 168$ punts diferents i, per tant, el subgrup d'isotropia d'aquest punt és trivial. Aquest fet és cert per a tots els punts de la corba llevat d'uns punts distingits, per als quals els subgrups d'isotropia corresponen a p-subgrups de G.

- 7-subgrups: Hi ha 8 subgrups; cadascun deixa fixos tres punts de $\mathbb{P}^2$, tots els quals estan sobre $\mathcal{X}$. Els 24 punts que s'obtenen d'aquesta manera són els punts de Weierstrass de la corba, i el divisor que formen coincideix amb $\Phi_4 \cdot \Phi_6$.

- 3-subgrups: Hi ha 28 subgrups; cadascun deixa fixos tres punts de $\mathbb{P}^2$, dos dels quals estan sobre $\mathcal{X}$. D'aquesta manera s'obtenen 56 punts de la corba i les 28 bitangents de $\mathcal{X}$. El divisor $\Phi_4 \cdot \Phi_{14}$ té suport en aquests 56 punts.

- 2-subgrups: Hi ha 21 subgrups; cadascun d'aquests deixa fix un punt i una recta de $\mathbb{P}^2$. El punt fix no es troba sobre $\mathcal{X}$, i la recta fixa interseca amb $\mathcal{X}$ en 4 punts. S'obtenen així84 punts que són suport del divisor $\Phi_4 \cdot \Phi_{21}$.

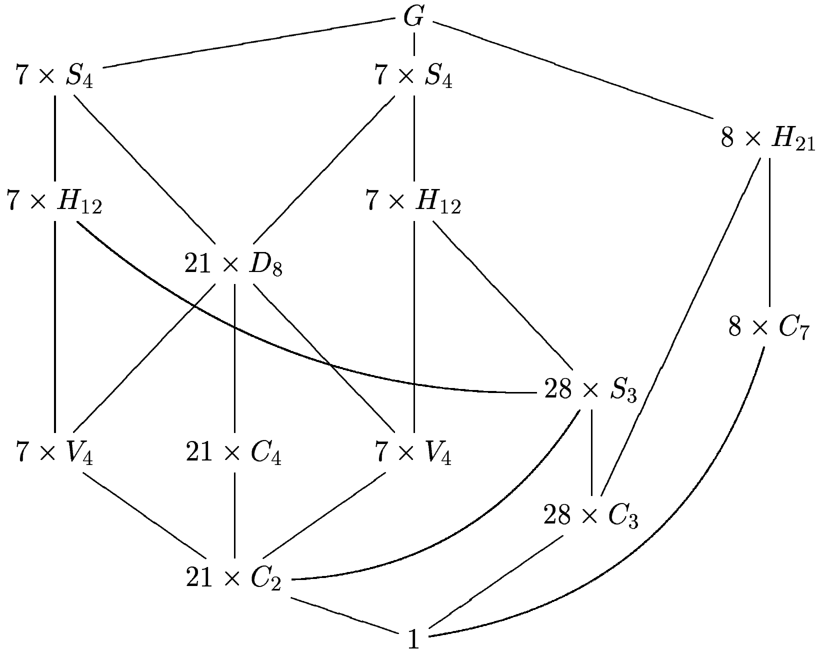


Figura 3.1: Diagrama de subgrups de G

3.1.3 Quocients de la quàrtica de Klein

Fent servir la fórmula de Hurwitz, és fàcil trobar els gèneres de les corbes quocients de $\mathcal{X}$ per subgrups d'automorfismes. El que s'obté és que aquest quocient és de gènere 3 en el cas que el subgrup sigui trivial, de gènere 1 si aquests subgrup és cíclic generat per un element d'ordre 2, 3 ó 4, i de gènere 0 altrament.

Un quocient racional Considerem el quocient, de gènere 0, pel subgrup d'ordre 7 generat per l'automorfisme g. Podem donar de manera explícita el morfisme de projecció com

$$\begin{aligned} \mathcal{X} &\to \ell = \{(a:b:c)\in\mathbb{P}^2 \mid a+b+c=0\}\\ (X:Y:Z) &\mapsto (X^3Y:Y^3Z:Z^3X). \end{aligned}$$

Amb aquest quocient obtenim també un model 7-cíclic per a $\mathcal{X}$,

$$C : y^7 = x^2(1+x),$$

i aplicacions biracionals:

$$\begin{array}{cc} \mathcal{X} \dashrightarrow C, & C \dashrightarrow \mathcal{X}, \\ (X : Y : Z) \mapsto \left(\dfrac{Y^3 Z}{Z^3 X}, \dfrac{-Y}{Z} \right), & (x, y) \mapsto (y^3 : xy : -x). \end{array}$$

Un quocient el·líptic Considerem el quocient $E_k = \mathcal{X}/\langle h \rangle$ pel subgrup d'ordre 3 generat per h. Per tal d'obtenir un model per a E_k, donat que h consisteix en la permutació cíclica $(X, Y, Z) \mapsto (Y, Z, X)$, apliquem a Φ_4 la transposició $(X, Y, Z) \mapsto (X, Z, Y)$ i, multiplicant-la amb Φ_4, obtenim un polinomi simètric en les variables X, Y, Z,

$$\begin{aligned} &(X^3Y + Y^3Z + Z^3X)(X^3Z + Z^3Y + Y^3X) = \\ &\qquad = S_2^4 + S_3(S_1^5 - 5S_1^3S_2 + S_1 s_2^2 + 7S_1^2S_3), \end{aligned}$$

on S_i són els polinomis simètrics elementals en 3 variables,

$$S_1 = X + Y + Z, \quad S_2 = XY + YZ + ZX, \quad S_3 = XYZ.$$

Així, aquesta equació proporciona un model projectiu per al quocient, a partir del qual trobem el model afíper al quocient:

$$C_k : s_2^4 + s_3(1 - 5s_2 + s_2^2 + 7s_3) = 0.$$

Fent servir un programa de càlcul simbòlic (per exemple, Maple) obtenim un model de Weierstrass per aquesta corba:

$$E_k : y^2 = x^3 - \frac{35}{16}x - \frac{49}{32},$$

aixícom també el morfisme de projecció

$$\mathcal{X} \xrightarrow{\pi} E_k : \; y^2 = x^3 - \frac{35}{16}x - \frac{49}{32}$$

que envia $(X : Y : Z)$ a:

$$\left(-\frac{4 - 20s_2 + 11s_2^2 + 28s_3}{4s_2^2}, \frac{15s_2 - 2 - 27s_2^2 + 5s_2^3 + 35s_2s_3 - 14s_3}{2s_2^3} \right)$$

amb

$$s_2 = \frac{XY + YZ + ZX}{(X+Y+Z)^2}, \quad s_3 = \frac{XYZ}{(X+Y+Z)^3}$$

i les antiimatges del punt a l'infinit, corresponents a $s_2 = s_3 = 0$, són els punts racionals de la corba $(1:0:0), (0:1:0), (0:0:1) \in \mathcal{X}$.

Un cop trobada aquesta equació de Weierstrass, es pot calcular el seu invariant $j = -3375 = -3^3 5^3$, deduir que la corba té multiplicació complexa per l'anell d'enters $\mathbb{Z}[\alpha]$, i el seu conductor és 49. De fet, E_k és isomorfa a la corba 49A1 de les taules de Cremona i, per tant, a la corba modular $X_0(49)$.

3.1.4 La quàrtica de Klein com a corba de Hurwitz

Un teorema clàssic de Hurwitz afita superiorment en $84(g-1)$ el nombre d'automorfismes d'una superfície de Riemann de gènere g; a més, un grup d'ordre $84(g-1)$ és grup d'automorfismes d'una superfície de Riemann si, i només si, es pot generar per dos elements d'ordres respectius 2 i 3 que el seu producte sigui d'ordre 7.

Les corbes que assoleixen aquesta fita en el seu nombre d'automorfismes s'anomenen corbes de Hurwitz. Donat que les corbes de gènere 2 tenen, com a màxim 48 automorfismes, no hi ha corbes de Hurwitz en gènere 2. En gènere 3, donat que l'únic grup d'ordre 168 amb les condicions anomenades anteriorment és G, i els automorfismes generadors d'ordres 2 i 3 són únics mòdul automorfismes de G, resulta que $\mathcal{X}$ és, llevat d'isomorfismes, la única corba de Hurwitz en gènere 3.

Es pot donar explícitament el recobriment per $\mathcal{X}$ de $\mathbb{P}^1$ com

$$\mathcal{X} \xrightarrow{j} \mathbb{P}^1$$
$$(X:Y:Z) \mapsto j = \frac{\Phi_{14}^3}{\Phi_6^7} = \frac{\Phi_{21}^2}{\Phi_6^7} + 1728.$$

Observem que el morfisme j té grau $4 \cdot 42 = 168$ i factoritza per G; aixídoncs, obtenim un isomorfisme entre $\mathcal{X}/G$ i $\mathbb{P}^1$. Aquest morfisme és ramificat en 3 punts, corresponents als valors de la imatge $j = 1728$, $j = 0$ i $j = \infty$, amb índexos de ramificació respectius 2, 3 i 7, i que corresponen a les condicions sobre la corba $\Phi_{21} = 0$, $\Phi_{14} = 0$ i $\Phi_6 = 0$, respectivament.

3.1.5 La jacobiana de la quàrtica de Klein

Considerem la jacobiana de $\mathcal{X}$, $\mathcal{J} = \mathrm{Jac}(C)(\mathcal{X})$ com a tor complexe, $\mathcal{J} = \mathbb{C}^3/\Lambda$. Aleshores Λ és una G-$\mathcal{O}_k$-xarxa, ja que G actua sobre $\Omega^1(\mathcal{X})$ i $\alpha = g^4+g^2+1$. Un teorema de Gross assegura que una xarxa amb aquestes propietats queda determinada llevat d'isomorfismes. Això ens permet trobar fàcilment una xarxa L que ens proporcioni un quocient isomorf a $\mathcal{J}$.

Prenem la representació de G

$$\rho(g) = \frac{1}{2}\begin{pmatrix} -1 & 1 & -\alpha-1 \\ \alpha & \alpha & 0 \\ -1 & 1 & \alpha+1 \end{pmatrix},$$

$$\rho(h) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad \rho(s) = -\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

i considerem la $\rho(G)$-$\mathcal{O}_k$-xarxa

$$\begin{aligned} L = \langle (2,0,0), (-\alpha-1, -\alpha-1, 0), (\alpha,1,1)\rangle_{\mathcal{O}_k} = \\ = \langle (2,0,0), (2\alpha,0,0), (-\alpha-1,-\alpha-1,0), (2,2,0), \\ (\alpha,1,1), (-2-\alpha,\alpha,\alpha)\rangle_{\mathbb{Z}}. \end{aligned}$$

Aleshores Λ és isomorfa a un cert múltiple de L.

Normalitzant els generadors obtinguts per a la xarxa,

$$\begin{pmatrix} 1/2 & -1/2 & (1-\alpha)/2 \\ 0 & 1/2 & -1/2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 & \alpha & 2\alpha & -1-\alpha & -2-\alpha \\ 0 & 2 & 1 & 0 & -1-\alpha & \alpha \\ 0 & 0 & 1 & 0 & 0 & \alpha \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & 0 & \alpha & 0 & 0 \\ 0 & 1 & 0 & 0 & \frac{-1-\alpha}{2} & 0 \\ 0 & 0 & 1 & 0 & 0 & \alpha \end{pmatrix},$$

obtenim que $\mathcal{J}$ és isògena al producte de tres corbes el·líptiques; a més, donat que $j(\alpha) = j((-1-\alpha)/2) = j(E_k) = -3375$, obtenim finalment que $\mathcal{J} \sim E_k^3$ i $\mathbb{Q} \otimes \mathrm{End}(\mathcal{J}) \simeq \mathbf{M}_3(\mathbb{Q}(\sqrt{-7}))$.

3.2 La quàrtica de Klein sobre $\mathbb{Q}$

3.2.1 Punts racionals i aplicacions

Els punts racionals de $\mathcal{X}$ es poden obtenir fàcilment fent servir el morfisme $\mathcal{X} \to E_k$, el qual està definit sobre $\mathbb{Q}$. Els punts racionals de E_k es poden calcular fent servir, per exemple, Magma, i s'obté que

$$E_k(\mathbb{Q}) = \{P_\infty, (7/4, 0)\}.$$

Les antiimatges del punt $(7/4, 0)$ no són racionals i, per tant, els únics punts racionals de $\mathcal{X}$ són els que tenen imatge en el punt a l'infinit de E_k; per tant,

$$\mathcal{X}(\mathbb{Q}) = \{(1:0:0), (0:1:0), (0:0:1)\}.$$

Com a aplicació, obtenim el teorema de Fermat per a l'exponent $p = 7$. En efecte, considerem

$$\mathcal{F}_7 : A^7 + B^7 + C^7 = 0$$

i el morfisme racional

$$\mathcal{F}_7 \to \mathcal{X}, \qquad (A:B:C) \mapsto (A^3C : B^3A : C^3B)$$

Donat que

$$\mathcal{X}(\mathbb{Q}) = \{(1:0:0), (0:1:0), (0:0:1)\},$$

es segueix que per tal que un punt (A, B, C) sobre $\mathcal{F}_7$ tingui coordenades racionals, almenys una d'aquestes coordenades ha de ser nul·la i obtenim el resultat.

3.2.2 Reduccions mòdul els primers 2 i 3

Reducció mòdul 2 Fent servir la caracterització de $\mathcal{X}$ que el seu grup d'automorfismes és isomorf a $\mathrm{SL}_3(\mathbb{F}_2)$, podem trobar un model per a $\mathcal{X}$ en aquesta característica simplement trobant una quàrtica invariant per aquest grup. D'aquesta manera obtenim

$$\Phi_4 = XYZ(X+Y+Z) + (X+Y+Z)^4 + (XY+YZ+ZX)^2.$$

En aquesta característica, donat que els seus automorfismes estan definits sobre $\mathbb{F}_2$, es té que la jacobiana és $\mathbb{F}_2$-isògena al cub d'una corba el·líptica amb multiplicació complexa per $\mathbb{Z}[\alpha]$.

Pel que respecta als punts racionals en cossos finits de característica 2, fent servir Magma, podem calcular el nombre d'aquests punts per a diferents extensions de $\mathbb{F}_2$, obtenint els resultats següents

m	1	2	3	4	5	6	7	8	9	10	11	12	13
$q = 2^m$	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192
$\#\mathcal{X}(\mathbb{F}_q)$	0	14	24	14	0	38	168	350	528	854	1848	4238	8736

Fem algunes remarques sobre aquest còmput del nombre de punts:

- La corba no té punts racionals sobre $\mathbb{F}_{32}$ ni, és clar, sobre $\mathbb{F}_2$.

- Sobre $\mathbb{F}_4$ i $\mathbb{F}_8$, té el nombre màxim de punts racionals entre totes les corbes definides sobre aquests cossos. A més, els punts definits sobre $\mathbb{F}_8$ són exactament els punts de Weierstrass de la corba.

- Sobre $\mathbb{F}_{16}$, la corba té els mateixos punts racionals que sobre $\mathbb{F}_4$; anàlogament, tots els punts definits sobre $\mathbb{F}_{64}$ són els punts definits sobre les subextensions $\mathbb{F}_4$ i $\mathbb{F}_8$.

Reducció mòdul 3 En el cas de característica 3, es pot prendre el model S_4, donat per l'equació

$$\Phi_4' \equiv X^4 + Y^4 + Z^4 \pmod 3,$$

i amb automorfismes definits sobre $\mathbb{F}_9$. En aquesta característica la jacobiana és $\mathbb{F}_9$-isògena al cub d'una corba el·líptica supersingular amb multiplicació complexa per $\mathbb{Z}[\alpha]$ i el polinomi característic de Frob_9 és $(T+3)^6$.

Sobre extensions de grau parell de $\mathbb{F}_3$, el nombre de punts de la corba, calculat fent servir Magma, és:

$m = 2r$	2	4	6	8	10	12
$q = 3^m = 9^r$	9	81	729	6561	59049	531441
$\#\mathcal{X}(\mathbb{F}_q)$	28	28	892	6076	60508	527068

Observem que aquest còmput del nombre de punts es pot fer de manera directa fent servir el polinomi característic obtingut abans; aquest càlcul ens dóna

$$\#\mathcal{X}(\mathbb{F}_{3^{2r}}) = 9^2 - 6(-3)^r + 1.$$

Cal observar que aquest nombre de punts racionals és, alternativament, el màxim (per a r senar) o el mínim (per a r parell), d'entre totes les corbes definides sobre aquest cossos.

Tenint en compte ara extensions de grau senar, i fent el còmput de nombre de punts com abans obtenim

m	1	3	5	7	9	11
$q = 3^m$	3	27	243	2187	19683	177147
$\#\mathcal{X}(\mathbb{F}_q)$	4	28	244	2188	19684	177148

És a dir, obtenim que $\#\mathcal{X}(\mathbb{F}_q) = q + 1$. Això és degut a que tenim una bijecció entre els punts $\mathbb{F}_q$-definits de $\mathcal{X}$ i els punts $\mathbb{F}_q$-definits d'una cònica. En efecte, de la successió exacta curta

$$1 \longrightarrow \mu_2(k) \cap k^{*2} \longrightarrow k^{*2} \overset{x \mapsto x^2}{\longrightarrow} k^{*4} \longrightarrow 1,$$

i donat que, per a extensions $k/\mathbb{F}_3$ de grau senar es té que $\mu_2(k) \cap k^{*2} = 1$, tenim que $k^{*2} = k^{*4}$ i els zeros de $X^4 + Y^4 + Z^4$ estan en bijecció amb els de $A^2 + B^2 + C^2$.

3.3 La corba modular $X(p)$ sobre $\mathbb{C}$

Sigui p un primer senar. La corba modular $X(p)$ és la compactificació cuspidal del quocient del semiplà complex superior $\mathbb{H}$ pel subgrup de matrius de $\mathrm{SL}_2(\mathbb{Z})$ que redueixen mòdul p a la matriu identitat. Es té doncs un isomorfisme de superfícies de Riemann

$$X(p)(\mathbb{C}) \;\simeq\; {}_{\Gamma(p)}\backslash\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}),$$

on $\Gamma(p)$ és el nucli de la reducció mòdul p definida a $\mathrm{PSL}_2(\mathbb{Z})$:

$$1 \longrightarrow \Gamma(p) \longrightarrow \mathrm{PSL}_2(\mathbb{Z}) \longrightarrow \mathrm{PSL}_2(\mathbb{F}_p) \longrightarrow 1.$$

En particular, el morfisme natural $X(p) \longrightarrow X(1)$ és un recobriment de Galois amb grup d'automorfismes

$$\mathrm{PSL}_2(\mathbb{Z}) \,/\, \Gamma(p) \;\simeq\; \mathrm{PSL}_2(\mathbb{F}_p).$$

A un apèndix de [Maz98], Serre demostra que aquests són, de fet, tots els automorfismes de la corba $X(p)$ quan el gènere no és zero, de forma que

$$\mathrm{Aut}\,(X(p)) \;\simeq\; \mathrm{PSL}_2(\mathbb{F}_p)$$

si $p \geq 7$.

Els únics punts ramificats del recobriment $X(p) \longrightarrow X(1)$ són els cuspidals (tots ells amb índex de ramificació p) i les antiimatges dels dos punts el·líptics de $X(1)$, cf. [Shi71]:

$$\begin{tikzcd} X(p) \arrow[d, "\mathrm{PSL}_2(\mathbb{F}_p)"'] & \overbrace{\bullet\cdots\bullet}^{(p^2-1)/2} \arrow[d, dash, dotted, "p"] & \overbrace{\bullet\cdots\bullet}^{p\,(p^2-1)/4} \arrow[d, dash, dotted, "2"] & \overbrace{\bullet\cdots\bullet}^{p\,(p^2-1)/6} \arrow[d, dash, dotted, "3"] \\ X(1) & \infty & [i] & [e^{2\pi i/3}] \end{tikzcd}$$

Aplicant la fórmula de Hurwitz, s'obté la expressió següent per al gènere de $X(p)$:

$$g\,(X(p)) \;=\; 1 + \frac{1}{24}\,(p+1)(p-1)(p-6).$$

En particular, la corba $X(7)$ té gènere 3. Com que l'ordre del seu grup d'automorfismes,

$$G \;=\; \mathrm{Aut}(X(7)) \;\simeq\; \mathrm{PSL}_2(\mathbb{Z})\,/\,\Gamma(7) \;\simeq\; \mathrm{PSL}_2(\mathbb{F}_7),$$

assoleix la cota de Hurwitz, $X(7)$ és isomorfa a la quàrtica de Klein $\mathcal{X}$. Notem que els estabilitzadors dels punts que ramifiquen sobre $X(1)$ són subgrups de G amb ordres 2, 3 i 7:

$$\begin{tikzcd} X(7) \arrow[d, "G"'] & \overbrace{\bullet\cdots\bullet}^{24} \arrow[d, dash, dotted, "7"] & \overbrace{\bullet\cdots\bullet}^{84} \arrow[d, dash, dotted, "2"] & \overbrace{\bullet\cdots\bullet}^{56} \arrow[d, dash, dotted, "3"] \\ X(1) & \infty & [i] & [e^{2\pi i/3}] \end{tikzcd}$$

3.4 La corba modular $X(p)$ sobre $\mathbb{Q}$

Per fixar un model racional per a $X(p)$, podem seguir les Seccions 6.1 i 6.2 de [Shi71]. Considerem el cos de funcions modulars per a $\Gamma(p)$ tals que el seu desenvolupament de Fourier (en termes del paràmetre local $q^{1/p} = e^{2\pi i\tau/p}$ de la punta de l'infinit) té coeficients a $\mathbb{Q}(\zeta_p)$, on ζ_p denota una arrel p-èsima no-trivial de la unitat. Aquest cos de funcions, que designem per $\mathbb{Q}(\zeta_p)(X(p))$, és una extensió de Galois de $\mathbb{Q}(j)$, on j és la funció modular clàssica per a $X(1)$. L'acció del grup de Galois d'aquesta extensió s'identifica amb una acció (a la dreta) del grup $\mathrm{GL}_2(\mathbb{F}_p)/\langle -1\rangle$ que, restringida al subgrup $\mathrm{PSL}_2(\mathbb{F}_p)$, coincideix amb l'acció natural de $\mathrm{PSL}_2(\mathbb{Z})\,/\,\Gamma(p)$ sobre $\mathbb{Q}(\zeta_p)(X(p))$, i tal que el subcòs fix pel subgrup de matrius de la forma

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \quad \text{amb} \ \ d \in \mathbb{F}_p^*,$$

és el cos de funcions modulars per a $\Gamma(p)$ amb desenvolupament de Fourier racional. Aquest cos de funcions $\mathbb{Q}(X(p))$ defineix un model racional canònic per a $X(p)$:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_p)\big(X(p)\big) \arrow[dl, dash, "\left(\begin{smallmatrix}1&0\\0&*\end{smallmatrix}\right)"'] \arrow[dd, dash, "\mathrm{GL}_2(\mathbb{F}_p)/\langle -1\rangle"] \\
\mathbb{Q}\big(X(p)\big) \arrow[dr, dash] & \\
 & \mathbb{Q}(j)
\end{tikzcd}$$

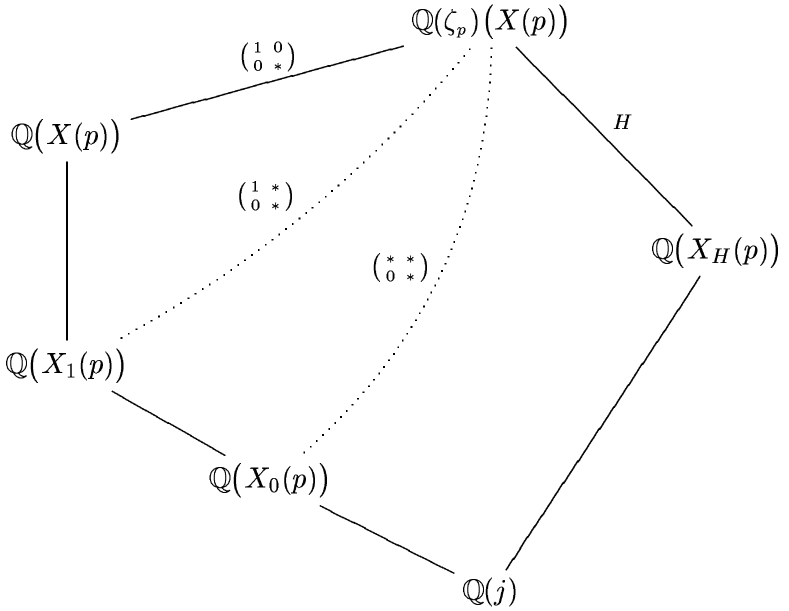
Més en general, a [Lig77], [Maz77], [Roh97] es pot trobar un procediment per definir models per a les corbes modulars associades a subgrups Γ de $\mathrm{PSL}_2(\mathbb{Z})$ que continguin $\Gamma(p)$. Concretament, per a cada subgrup H de $\mathrm{GL}_2(\mathbb{F}_p)/\langle -1\rangle$ amb determinant exhaustiu, el subcòs de $\mathbb{Q}(\zeta_p)(X(p))$ fix per H defineix un model racional $X_H(p)$ per a la corba modular associada a la superfície de Riemann compacta ${}_{\Gamma}\backslash\mathbb{H}\cup\mathbb{P}^1(\mathbb{Q})$, on Γ és el grup donat per la successió exacta

$$1 \longrightarrow \Gamma(p) \longrightarrow \Gamma \longrightarrow H \cap \mathrm{PSL}_2(\mathbb{F}_p) \longrightarrow 1.$$

Es té doncs l'isomorfisme de superfícies de Riemann

$$X_H(p)(\mathbb{C}) \ \simeq \ {}_{\Gamma}\backslash\mathbb{H}\cup\mathbb{P}^1(\mathbb{Q}).$$

Casos particulars d'això són les clàssiques corbes modulars $X_0(p)$ i $X_1(p)$, tal i com es mostra al diagrama de cossos de funcions següent:


$\mathbb{Q}(\zeta_p)(X(p))$
$\left(\begin{smallmatrix}1 & 0\\ 0 & *\end{smallmatrix}\right)$
$\mathbb{Q}(X(p))$
H
$\left(\begin{smallmatrix}1 & *\\ 0 & *\end{smallmatrix}\right)$
$\mathbb{Q}(X_H(p))$
$\left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right)$
$\mathbb{Q}(X_1(p))$
$\mathbb{Q}(X_0(p))$
$\mathbb{Q}(j)$

Els punts no-cuspidals de $X_H(p)(\overline{\mathbb{Q}})$ s'identifiquen amb les classes d'isomorfisme de parelles $(E,\ [P,Q]_H)$, on E és una corba el·líptica sobre $\overline{\mathbb{Q}}$, $[P,Q]$ és una base de la p-torsió $E[p]$, i $[P,Q]_H$ és la corresponent òrbita a $E[p] \times E[p]$ donada per l'acció del subgrup H (vist com a subgrup d'automorfismes de $E[p]$ a través de l'isomorfisme $\mathrm{GL}_2(\mathbb{F}_p) \simeq \mathrm{Aut}(E[p])$ fixat per la base $[P,Q]$). A més, aquesta identificació és compatible amb les accions de Galois respectives, de forma que un punt donat per $(E,\ [P,Q]_H)$, amb invariant j diferent de 0 i 1728, està definit sobre un cos de nombres L si, i només si, la corba el·líptica E està definida sobre L i la representació lineal

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow \mathrm{Aut}\,(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

associada a la p-torsió de E té imatge dins H.

En particular, i fent servir aquesta mateixa notació, els punts no-cuspidals de $X(p)(L)$ amb invariant j diferent de 0 i 1728 vénen donats per parelles

$$\Big(E_{/L}\,,\ [P,\ n\,Q]_{n=1,\ldots,p-1}\Big)\,,$$

on el model per a la corba el·líptica E, determinat llevat de torçaments quadràtics, es pot triar de manera que l'expressió de $\rho_{E,p}$ en la base $[P,Q]$ sigui la suma directa del caràcter trivial i del caràcter ciclotòmic χ_p . De forma equivalent, aquests punts s'identifiquen amb les classes d'isomorfisme de parelles (E,φ), on E és una corba el·líptica definida sobre L i

$$\varphi : E[p] \longrightarrow \mathbb{F}_p \times \langle\zeta_p\rangle$$

és un $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$-isomorfisme *simplèctic*, és a dir, tal que la base de $E[p]$ corresponent a la base $[\,(1,1),\ (0,\zeta_p)\,]$ de $\mathbb{F}_p \times \langle\zeta_p\rangle$ té imatge ζ_p per l'aparellament de Weil

$$\langle\ ,\ \rangle_{E,p}\ :\ E[p] \times E[p] \longrightarrow \langle\zeta_p\rangle.$$

Per als nostres objectius, ens interessarà també aplicar la construcció de la corba modular $X_H(p)$ al cas en què H correspongui al normalitzador d'un subgrup de Cartan *non-split* de $\mathrm{GL}_2(\mathbb{F}_p)$.

3.5 Subgrups de Cartan non-split

Llevat d'automorfismes, l'espai vectorial $\mathbb{F}_p \times \mathbb{F}_p$ admet $p\,(p-1)/2$ estructures diferents com a cos: una per a cada polinomi quadràtic mònic irreductible amb coeficients a $\mathbb{F}_p$. El grup d'automorfismes de cadascuna d'aquestes estructures considerada com a espai vectorial de dimensió 1 sobre $\mathbb{F}_{p^2}$ dóna lloc a un *subgrup de Cartan non-split* de $\mathrm{GL}_2(\mathbb{F}_p)$:

$$\begin{tikzcd}
C \arrow[r, dash, "\simeq"] \arrow[d, hook] & \mathrm{Aut}_{\mathbb{F}_{p^2}}(\mathbb{F}_p \times \mathbb{F}_p) \arrow[d, hook] \arrow[r, phantom, "\simeq"] & \mathbb{F}_{p^2}^* \\
\mathrm{GL}_2(\mathbb{F}_p) \arrow[r, dash, "\simeq"] & \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p \times \mathbb{F}_p) &
\end{tikzcd}$$

Els $p\,(p-1)/2$ subgrups de Cartan non-split són cíclics d'ordre p^2-1 i conjugats entre ells. Donat un d'aquests subgrups C, provinent d'una identificació de $\mathbb{F}_p \times \mathbb{F}_p$ amb $\mathbb{F}_{p^2}$, la matriu de $\mathrm{GL}_2(\mathbb{F}_p)$ corresponent a l'automorfisme no-trivial del cos $\mathbb{F}_{p^2}$ pertany al normalitzador N de C i, de fet, representa l'únic element no trivial del quocient N/C. Es té un diagrama commutatiu

$$\begin{tikzcd}
\mathbb{F}_p^* \arrow[d, hook] & & \\
\mathbb{Z}/(p^2-1)\mathbb{Z} \simeq C \arrow[r, hook, "2"] \arrow[d] & N \arrow[r, hook] \arrow[d] & \mathrm{GL}_2(\mathbb{F}_p) \arrow[d] \\
\mathbb{Z}/(p+1)\mathbb{Z} \simeq C/\mathbb{F}_p^* \arrow[r, hook, "2"] & N/\mathbb{F}_p^* \arrow[r, hook] & \mathrm{PGL}_2(\mathbb{F}_p) \\
\mathbb{Z}/\frac{p+1}{2}\mathbb{Z} \simeq \left(C/\mathbb{F}_p^*\right) \cap \mathrm{PSL}_2(\mathbb{F}_p) \arrow[r, hook] \arrow[u, hook] & \left(N/\mathbb{F}_p^*\right) \cap \mathrm{PSL}_2(\mathbb{F}_p) \arrow[r, hook] \arrow[u, hook] & \mathrm{PSL}_2(\mathbb{F}_p) \arrow[u, hook]
\end{tikzcd}$$

on $\mathbb{F}_p^*$ és el subgrup d'homotècies. El subgrup C és l'únic subgrup de Cartan non-split de $\mathrm{GL}_2(\mathbb{F}_p)$ que està contingut a N, i el grup $N/\mathbb{F}_p^*$ és isomorf al grup diedral $D_{2(p+1)}$. Si $p \equiv 3 \pmod 4$, el normalitzador N té determinant exhaustiu, la qual cosa equival a dir que el grup $\left(N/\mathbb{F}_p^*\right) \cap \mathrm{PSL}_2(\mathbb{F}_p)$ té ordre $p+1$. En el cas $p = 7$, aquest últim grup és un dels 2-subgrups de Sylow de $\mathrm{PSL}_2(\mathbb{F}_7)$, isomorfs al grup diedral D_8.

3.6 Alguns quocients de la quàrtica de Klein $X(7)_{/\mathbb{Q}}$

Recordem que el grup $G = \mathrm{Aut}(X(7))$ és isomorf a

$$\mathrm{PSL}_2(\mathbb{F}_7) \;=\; \langle g,\, h,\, s\rangle,$$

on

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad h = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}, \qquad s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Els subgrups $\langle g\rangle$, $\langle h\rangle$ i $\langle g,\, h\rangle$ tenen ordre 7, 3 i 21, respectivament, mentre que $\langle g\,s\,g^2,\, s\rangle$ és un dels 21 subgrups conjugats de $\mathrm{PSL}_2(\mathbb{F}_7)$ isomorfs al grup diedral D_8. Sigui N el normalitzador del subgrup de Cartan non-split de $\mathrm{GL}_2(\mathbb{F}_7)$ tal que

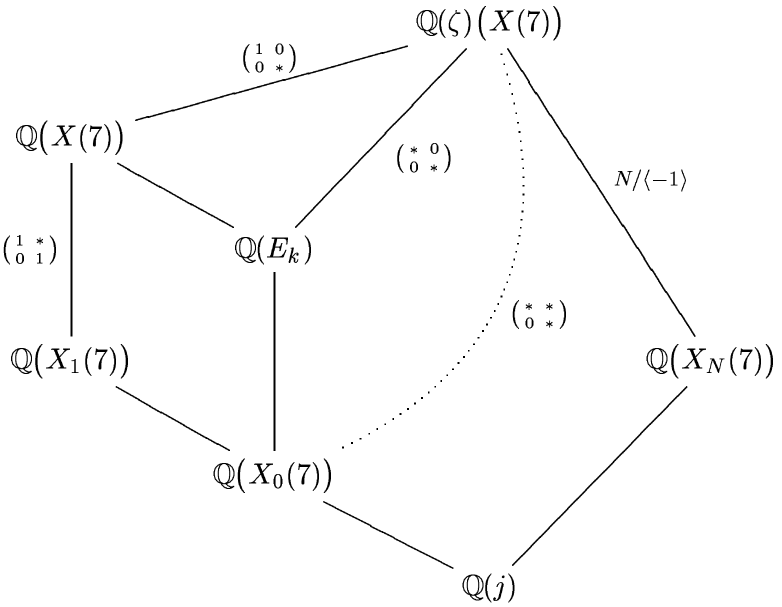
$$(N/\mathbb{F}_7^*) \cap \mathrm{PSL}_2(\mathbb{F}_7) = \langle g\,s\,g^2,\, s\rangle,$$

i sigui $X_N(7)$ la corba modular constru´da a partir de $X(7)$ i del subgrup $N/\langle -1\rangle$ de $\mathrm{GL}_2(\mathbb{F}_7)/\langle -1\rangle$ seguint el procediment de la Secció 3.4. Sobre els complexos, tenim el diagrama de quocients de $X(7)$ següent, on E_k és la corba el·líptica estudiada a la primera secció, i on identifiquem els elements de $\mathrm{PSL}_2(\mathbb{F}_7)$ que hi apareixen amb els corresponents automorfismes al grup G:

$$\begin{tikzcd}
 & & X(7) \arrow[dll, "\langle h\rangle"'] \arrow[ddl, "\langle g\rangle"'] \arrow[dddl, "\langle g,h\rangle"] \arrow[dddd, "G"] \arrow[ddr, dotted, "\langle g\,s\,g^2,s\rangle"] & \\
X_0(49)\simeq E_k \arrow[ddr] & & & \\
 & X_1(7) \arrow[d] & & X_N(7) \arrow[ddl] \\
 & X_0(7) \arrow[dr] & & \\
 & & X(1) &
\end{tikzcd}$$

Si fixem per a $X(7)$ el model canònic de Shimura (cf. Secció 3.4), tots els morfismes d'aquest diagrama es poden definir sobre $\mathbb{Q}$ llevat del corresponent al quocient $X_N(7)$. En efecte, el normalitzador d'un subgrup de Cartan non-split de $\mathrm{GL}_2(\mathbb{F}_7)$ no pot contenir el subgrup cíclic de matrius diagonals emprat per fixar el cos de funcions de $X(7)$

sobre $\mathbb{Q}$, tal i com es reflecteix al diagrama següent, on $\zeta = e^{2\pi i/7}$:


$\mathbb{Q}(\zeta)(X(7))$
$\left(\begin{smallmatrix}1 & 0\\ 0 & *\end{smallmatrix}\right)$
$\mathbb{Q}(X(7))$
$\left(\begin{smallmatrix}* & 0\\ 0 & *\end{smallmatrix}\right)$
$N/\langle -1\rangle$
$\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$
$\mathbb{Q}(E_k)$
$\left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right)$
$\mathbb{Q}(X_1(7))$
$\mathbb{Q}(X_N(7))$
$\mathbb{Q}(X_0(7))$
$\mathbb{Q}(j)$

Per estudiar amb més detall aquests cossos de funcions, vegem primer com obtenir explícitament la quàrtica de Klein $\mathcal{X}$ com a equació per al model canònic de Shimura $X(7)_{/\mathbb{Q}}$. D'ara endavant, seguirem bàsicament la Secció 4 de [Elk99].

La quàrtica de Klein $X(7)_{/\mathbb{Q}}$ i els seus punts no cuspidals

Donat que $X(7)$ és una corba no hiperel·líptica de gènere 3, l'espai de diferencials $\Omega^1_{\mathbb{Q}}(X(7))$ defineix una immersió racional

$$X(7)_{/\mathbb{Q}} \hookrightarrow \mathbb{P}^2$$

amb imatge donada per una quàrtica. L'espai vectorial $\Omega^1_{\mathbb{Q}}(X(7))$ és isomorf al de formes modulars cuspidals $S_2(\Gamma(7), \mathbb{Q})$, de forma que cada base $\{\mathsf{x}, \mathsf{y}, \mathsf{z}\}$ d'aquest darrer espai dóna lloc a una equació quàrtica per a $X(7)$ sobre $\mathbb{Q}$.

A [KL81] es construeixen *unitats modulars* per a $\Gamma(M)$, amb $M \geq 5$, a partir de *formes modulars de Klein.* En el nostre cas, es poden considerar formes cuspidals per a $\Gamma(7)$ de la forma

$$\pm\, q^{r/7} \prod_{n\geq 1} (1-q^n)^3(1-q^{7n})(1-q^{s-7+7n})(1-q^{-s+7n}),$$

amb $r,s \in \{1,\dots,6\}$ i $q = e^{2\pi i\tau}$, on $\tau \in \mathbb{H}$. Les tries $(r,s) = (4,1),(2,2),(1,4)$ corresponen respectivament a les formes modulars

$$\begin{aligned} \mathsf{x} &= q^{4/7}\,(-1+4\,q-3\,q^2-5\,q^3+5\,q^4+8\,q^6-10\,q^7+4\,q^9+\cdots), \\ \mathsf{y} &= q^{2/7}\,(1-3\,q-q^2+8\,q^3-6\,q^5-4\,q^6+2\,q^8+9\,q^{10}+8\,q^{11}+\cdots), \\ \mathsf{z} &= q^{1/7}\,(1-3\,q+4\,q^3+2\,q^4+3\,q^5-12\,q^6-5\,q^7+7\,q^9+\cdots), \end{aligned}$$

que satisfan l'equació de la quàrtica de Klein $\mathcal{X}$:

$$\mathsf{x}^3\,\mathsf{y}+\mathsf{y}^3\,\mathsf{z}+\mathsf{z}^3\,\mathsf{x} \,=\, 0.$$

Fent servir aquesta base $\{\mathsf{x},\mathsf{y},\mathsf{z}\}$, l'acció del grup d'automorfismes G sobre l'espai de diferencials $\Omega^1_{\mathbb{Q}(\zeta)}(X(7))$ ve donada pel model de Klein

$$\rho:\, G \longrightarrow \mathrm{GL}_3(\mathbb{Q}(\zeta))\,.$$

Notem que els invariants $\Phi_6,\Phi_{14},\Phi_{21}$ produeixen formes modulars cuspidals per a $\mathrm{SL}_2(\mathbb{Z})$ de pesos respectius 12, 28 i 42; concretament,

$$\Phi_6(\mathsf{x},\mathsf{y},\mathsf{z}) \,=\, \Delta, \qquad \Phi_{14}(\mathsf{x},\mathsf{y},\mathsf{z}) \,=\, \Delta^2\, G_2, \qquad \Phi_{21}(\mathsf{x},\mathsf{y},\mathsf{z}) \,=\, \Delta^3\, G_3,$$

on

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24},$$

$$G_2 = 1+240\sum_{n\geq 1}\frac{n^3\,q^n}{1-q^n}\,, \qquad G_3 = 1-504\sum_{n\geq 1}\frac{n^5\,q^n}{1-q^n}\,.$$

En particular, es té la igualtat,

$$j \,=\, \frac{\Phi_{14}(\mathsf{x},\mathsf{y},\mathsf{z})^3}{\Phi_6(\mathsf{x},\mathsf{y},\mathsf{z})^7}\,,$$

que es pot llegir com l'expressió en coordenades del morfisme *d'oblit*

$$X(7) \longrightarrow X(1).$$

Així, un punt no cuspidal $(\mathsf{x}\colon \mathsf{y}\colon \mathsf{z})$ de $X(7)$ dóna lloc a una corba el·líptica

$$E_j \;:\; y_j^2 \;=\; x_j^3 \;-\; 3\,\Phi_{14}(\mathsf{x},\mathsf{y},\mathsf{z})\,x_j \;+\; 2\,\Phi_{21}(\mathsf{x},\mathsf{y},\mathsf{z})$$

amb invariant j donat per l'expressió anterior. Torçant E_j per algun caràcter quadràtic, es pot suposar (cf. Secció 3.4) que es té un isomorfisme simplèctic

$$E_j[7] \;\simeq\; \mathbb{F}_7 \times \langle\zeta\rangle$$

compatible amb l'acció de Galois. En efecte, si P_j i Q_j són els punts de $E_j[7]$ que corresponen respectivament a $u = q^{1/7}$ i $u = \zeta$ a través de l'isomorfisme

$$\begin{array}{ccccc} E_j\,(\mathbb{C}) & \simeq & \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) & \simeq & \mathbb{C}^*/q^{\mathbb{Z}} \\ & & z & \mapsto & u = e^{2\pi i z}, \end{array}$$

i fent servir el desenvolupament

$$x_j \;=\; 12\,\Delta\left(\frac{1}{12} - 2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2} + \sum_{n\in\mathbb{Z}}\frac{q^n\,u}{(1-q^n\,u)^2}\right),$$

es pot comprovar que $x_j(P_j)$ i $x_j(Q_j)$ són polinomis en les formes modulars $\mathsf{x},\mathsf{y},\mathsf{z}$ amb coeficients a $\mathbb{Q}$ i a $\mathbb{Q}(\zeta)$, respectivament.

La corba modular $X_0(7)$

Considerem els morfismes racionals

$$\begin{tikzcd} X(7) \arrow[r, "21"] & X_0(7) \arrow[r, "8"] & X(1) \end{tikzcd}$$

corresponents a les inclusions del diagrama de cossos de funcions que hem reprodu´t abans. La corba $X_0(7)$ té gènere zero. Un generador sobre $\mathbb{Q}$ del seu cos de funcions ve donat pel quocient de funcions η de Dedekind

$$\begin{aligned} R \;=\; \frac{\eta(q)^4}{\eta(q^7)^4} \;&=\; \frac{1}{q}\prod_{n\geq 1}\frac{(1-q^n)^4}{(1-q^{7n})^4} \;= \\ &= \frac{1}{q} - 4 + 2\,q + 8\,q^2 - 5\,q^3 - 4\,q^4 - 10\,q^5 + \cdots \end{aligned}$$

De les igualtats

$$R = \frac{\Delta}{q^2}\prod_{n\geq 1}\frac{1}{(1-q^n)^{20}(1-q^{7n})^4},$$

$$\mathsf{x\,y\,z} = -q\prod_{n\geq 1}(1-q^n)^{10}(1-q^{7n})^2$$

s'obté l'expressió

$$R = \frac{\Phi_6(\mathsf{x},\mathsf{y},\mathsf{z})}{(\mathsf{x\,y\,z})^2}$$

per al morfisme $X(7) \longrightarrow X_0(7)$. Observem que aquesta funció modular és, en efecte, invariant per $\rho(g)$ i $\rho(h)$. Quant al morfisme $X_0(7) \longrightarrow X(1)$, ve donat per

$$j = \frac{(R^2+13\,R+49)\,(R^2+245\,R+7^4)^3}{R^7}.$$

La corba modular $X_1(7)$

Considerem ara els morfismes racionals

$$X(7) \xrightarrow{\quad 7 \quad} X_1(7) \xrightarrow{\quad 3 \quad} X_0(7).$$

La corba $X_1(7)$ també té gènere zero. La funció modular següent és invariant per $\rho(g)$ i, per tant, pertany a $\mathbb{Q}(X_1(7))$:

$$T = \frac{-\mathbf{y}^2\,\mathbf{z}}{\mathbf{x}^3} = \frac{1}{q}+3+4\,q+3\,q^2-5\,q^4-7\,q^5-2\,q^6+\cdots$$

La funció

$$T + T_{|h} + T_{|h^2} = \frac{-\mathbf{y}^2\,\mathbf{z}}{\mathbf{x}^3} + \frac{-\mathbf{z}^2\,\mathbf{x}}{\mathbf{y}^3} + \frac{-\mathbf{x}^2\,\mathbf{y}}{\mathbf{z}^3}$$

és llavors invariant tant per $\rho(g)$ com per $\rho(h)$, aixíque pertany a $\mathbb{Q}(X_0(7))$. Fent servir q-expansions, s'obtenen les relacions

$$T_{|h} = \frac{T-1}{T}, \qquad T_{|h^2} = \frac{1}{T-1}, \qquad T + T_{|h} + T_{|h^2} = R + 8,$$

de forma que T té grau 3 sobre el cos de funcions de $X_0(7)$; concretament,

$$R = \frac{T^3-8\,T^2+5\,T+1}{T^2-T}.$$

Així doncs, T és un generador sobre $\mathbb{Q}$ del cos de funcions de $X_1(7)$. Resulta ser el mateix *Hauptmodul* que Tate va fer servir per donar una interpretació de moduli dels punts no cuspidals de $X_1(7)$, associant-li la corba el·líptica

$$E_T:\ y^2 \,+\, (1+T-T^2)\,x\,y \,+\, (T^2-T^3)\,y \;=\; x^3 \,+\, (T^2-T^3)\,x^2,$$

de la qual l'origen és un punt de 7-torsió.

La corba modular $X_N(7)$
Considerem finalment els morfismes

$$\begin{tikzcd} X(7) \arrow[r, dotted, "8"] & X_N(7) \arrow[r, "21"] & X(1). \end{tikzcd}$$

Tot i que no se'n dóna una expressió explícita com a element de $\mathbb{Q}(\zeta)(X(7))$, a [Elk99] es prova l'existència d'un generador F sobre $\mathbb{Q}$ del cos de funcions de $X_N(7)$ tal que

$$j \;=\; 64\,\frac{\big(F\,(F^2+7)(F^2-7F+14)(5F^2-14F-7)\big)^3}{(F^3-7F^2+7F+7)^7}\,.$$

Aquesta expressió es fa servir a la demostració del teorema de Stark-Heegner.

3.7 El teorema de Stark-Heegner

La llista de cossos quadràtics imaginaris F amb grup de classes trivial comença així:

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{-11}),\ \mathbb{Q}(\sqrt{-19}),\ldots$$

Per a alguns d'ells, hi ha més d'un ordre $\mathcal{O}$ de l'anell d'enters $\mathcal{O}_F$ que sigui domini d'ideals principals:

$\mathcal{O} \subset \mathcal{O}_F$	$j(\mathcal{O})$
$\mathbb{Z}[\sqrt{-1}\,]$	$2^6\,3^3$
$\mathbb{Z}[2\sqrt{-1}\,]$	$2^3\,3^3\,11^3$
$\mathbb{Z}[\sqrt{-2}\,]$	$2^6\,5^3$
$\mathbb{Z}[\,(1+\sqrt{-3}\,)/2\,]$	0
$\mathbb{Z}[\sqrt{-3}\,]$	$2^4\,3^3\,5^3$
$\mathbb{Z}[\,(1+3\sqrt{-3}\,)/2\,]$	$-2^{15}\,3^1\,5^3$
$\mathbb{Z}[\,(1+\sqrt{-7}\,)/2\,]$	$-3^3\,5^3$
$\mathbb{Z}[\sqrt{-7}\,]$	$3^3\,5^3\,17^3$
$\mathbb{Z}[\,(1+\sqrt{-11}\,)/2\,]$	-2^{15}
$\mathbb{Z}[\,(1+\sqrt{-19}\,)/2\,]$	$-2^{15}\,3^3$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

3.7.1 Teorema *La llista anterior es completa amb només tres ordres més:*

F	$\mathcal{O} = \mathcal{O}_F$	$j(\mathcal{O})$
$\mathbb{Q}(\sqrt{-43}\,)$	$\mathbb{Z}[\,(1+\sqrt{-43}\,)/2\,]$	$-2^{18}\,3^3\,5^3$
$\mathbb{Q}(\sqrt{-67}\,)$	$\mathbb{Z}[\,(1+\sqrt{-67}\,)/2\,]$	$-2^{15}\,3^3\,5^3\,11^3$
$\mathbb{Q}(\sqrt{-163}\,)$	$\mathbb{Z}[\,(1+\sqrt{-163}\,)/2\,]$	$-2^{18}\,3^3\,5^3\,23^3\,29^3$

Prova. Sigui F un cos quadràtic imaginari amb anell d'enters $\mathcal{O}_F$ principal. Existeix llavors una corba el·líptica E definida sobre $\mathbb{Q}$ amb multiplicació complexa per $\mathcal{O}_F$, de forma que es té un isomorfisme de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-mòduls $\mathcal{O}_F \simeq \mathrm{End}(E)$. Aquest isomorfisme indueix una immersió

$$\mathcal{O}_F/(p) \hookrightarrow \mathrm{End}(E[p])$$

compatible amb les accions de Galois respectives, és a dir, tal que el diagrama

$$\begin{tikzcd}
E[p] \arrow[r, "\alpha"] \arrow[d, "\sigma"'] & E[p] \arrow[d, "\sigma"] \\
E[p] \arrow[r, "{}^{\sigma}\alpha"] & E[p]
\end{tikzcd}$$

és commutatiu per a qualssevol $\alpha \in \mathcal{O}_F$ i $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. En particular, la p-torsió de E és un $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$-mòdul de rang 1 sobre $\mathcal{O}_F/(p)$, on l'acció d'aquest darrer sobre $E[p]$ ve donada per la immersió anterior. Per tant, la restricció a $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ de la representació de Galois $\rho_{E,p}$ donada per l'acció de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre $E[p]$ té imatge dintre de

$$(\mathcal{O}_F/(p))^* \hookrightarrow \mathrm{Aut}(E[p])\,.$$

A més, la conjugació complexa ι normalitza aquest subgrup d'automorfismes:

$$\rho_{E,p}(\iota)\ (\mathcal{O}_F/(p))^*\, \rho_{E,p}(\iota) \;=\; (\mathcal{O}_F/(p))^*\,.$$

Si p és inert a F, és a dir, si $\mathcal{O}_F/(p) \simeq \mathbb{F}_{p^2}$, tenim doncs que la imatge de $\rho_{E,p}$ cau dintre del normalitzador N d'un subgrup de Cartan non-split de $\mathrm{GL}_2(\mathbb{F}_p)$ i que, per tant, la corba el·líptica E dóna lloc a un punt racional de la corba $X_N(p)$.

Prendrem ara $p = 7$. En vista de la llista encetada abans de l'enunciat del teorema, podem suposar que el discriminant de F té valor absolut més gran que 19. Es pot comprovar llavors que no pot existir cap element a $\mathcal{O}_F$ amb norma 7, de forma que $\mathcal{O}_F/(7) \simeq \mathbb{F}_{49}$. Aixídoncs, ha d'existir un valor racional F per al *Hauptmodul* de $X_N(7)$ de la Secció 3.6 tal que

$$64\,\frac{\left(F\,(F^2+7)(F^2-7F+14)(5F^2-14F-7)\right)^3}{(F^3-7F^2+7F+7)^7}$$

sigui igual a l'invariant j de E. Aquest invariant ha de ser un enter, perquè E té multiplicació complexa. Escrivint $F = m/n$ amb m, n enters primers entre si, es pot comprovar llavors que

$$m^3 - 7\,m^2\,n + 7\,m\,n^2 + 7\,n^3$$

ha de dividir 56. Els únics valors possibles per a m i n resulten ser aleshores els de la taula següent (cf. [Elk99]) :

m	n	j	$\mathcal{O} \subset \mathcal{O}_F$
0	1	0	$\mathbb{Z}[(1+\sqrt{-3})/2]$
1	0	$2^6\,5^3$	$\mathbb{Z}[\sqrt{-2}]$
1	1	-2^{15}	$\mathbb{Z}[(1+\sqrt{-11})/2]$
-1	1	$2^3\,3^3\,11^3$	$\mathbb{Z}[2\sqrt{-1}]$
2	1	$-2^{15}\,3^3\,5^3\,11^3$	$\mathbb{Z}[(1+\sqrt{-67})/2]$
3	1	$2^6\,3^3$	$\mathbb{Z}[\sqrt{-1}]$
5	1	$-2^{18}\,3^3\,5^3$	$\mathbb{Z}[(1+\sqrt{-43})/2]$
-3	5	$-2^{18}\,3^3\,5^3\,23^3\,29^3$	$\mathbb{Z}[(1+\sqrt{-163})/2]$
7	1	$2^3\,5^3\,7^5$	$----$
7	3	$2^{15}\,7^5$	$----$
11	2	$2^6\,11^3\,23^3\,149^3\,269^3$	$----$
19	9	$2^9\,17^6\,19^3\,29^3\,149^3$	$----$

Els últims quatre valors obtinguts per a la funció modular j no corresponen a corbes el·líptiques amb multiplicació complexa. □

G. Cardona
Dept. Ciències Matemàtiques i Informàtiques
Universitat de les Illes Balears
Ed. Anselm Turmeda, Campus UIB, Carretera Valldemosa, km. 7.5
07071 Palma de Mallorca, Spain
gabriel.cardona@uib.es

J. Fernàndez
Departament de Matemàtica Aplicada IV
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú
Av. Víctor Balaguer s/n
E-08800, Vilanova i la Geltrú
julio@ma4.upc.edu

Capítol 4

Mètode CM per a corbes de Picard

JORDI GUÀRDIA

L'objectiu a priori d'aquesta exposició era la presentació de l'article [KW04]. L'anàlisi detinguda del treball va revelar que una part significativa està dedicada a qüestions relacionades amb la multiplicació complexa, estudiada abastament en el STNB-2000 ([GL00]). Això ens va decidir a centrar l'exposició en les parts del treball més relacionades amb les corbes de gènere 3 (objecte d'aquest Seminari) i més específicament en les corbes de Picard. Per altra banda, el fet que l'objecte d'aquest capítol sigui un únic article fa aconsellable mirar de donar les idees i tècniques bàsiques subjacents als resultats, sense entrar en excessius detalls.

Introducció

Una corba de Picard és una corba cíclica trigonal de gènere 3:

$$Y^3 = f(X), \quad f \in \kappa[X], \quad \deg f = 4, \quad f \text{ separable.}$$

Picard s'interessà en aquestes corbes en el seu estudi de les equacions diferencials d'Euler. L'interès actual en les corbes de Picard és degut al resultat següent, que permet la seva utilització en l'àmbit de la Criptografia

Proposició. **[ERP99], [ERCH01]***Existeix un algoritme eficient per a l'addició en la jacobiana d'una corba de Picard.*

Quan hem de treballar amb una varietat abeliana en tasques criptogràfiques hem de conèixer el seu nombre de punts. El recompte de punts de varietats abelianes en cossos finits és una tasca computacionalment costosa, malgrat l'aparició en els darrers anys d'algoritmes molt potents (basats en mètodes p-àdics). És per això que sovint s'aborda la construcció de varietats abelianes amb nombre de punts conegut a priori; en aquest sentit, l'anomenat *mètode CM* és el més estès. Aquest mètode consisteix en la construcció de varietats abelianes complexes amb multiplicació complexa per l'anell d'enters O_K d'un cos de nombres K. La descomposició de l'ideal primer pO_K permet determinar el nombre de punts d'una tal varietat sobre el cos finit $\mathbb{F}_p$.

En el treball que ens ocupa, els autors mostren la manera de construir varietats abelianes de dimensió tres amb multiplicació complexa per un cos de nombres que contingui les arrels cúbiques de la unitat. Aquestes varietats abelianes resulten ser jacobianes de corbes de Picard, per la qual cosa queden determinades a partir d'una equació de la corba. Aquesta equació es calcula numèricament mitjançant funcions modulars. El càlcul numèric de totes les conjugades galoisianes d'una corba porta a l'obtenció exacta de polinomis de classes de Hilbert, dels quals se'n dedueixen models exactes de les corbes de Picard desitjades. Aquest és l'esquema bàsic del mètode CM en general.

4.1 Corbes de Picard i Multiplicació Complexa

En endavant treballarem sobre un cos κ amb $\operatorname{char}(\kappa) \neq 3$. Denotarem per $\zeta_3 \in \overline{\kappa}$ una arrel cúbica primitiva de la unitat. Una corba qualsevol $C : Y^3 = f(X)$ té un automorfisme evident d'ordre tres, donat per $\rho(x, y) = (x, \zeta_3 y)$. L'extensió d'aquest automorfisme a la jacobiana $J(C)$ de la corba ens dóna una inclusió $\mathbb{Q}(\zeta_3) \subset \operatorname{End}^0 J(C)$.

Això ja ens diu que $J(C)$ té *multiplicacions complexes*, però podria passar que no fos una varietat abeliana irreductible, per la qual cosa no podem assegurar que sigui una varietat abeliana CM [1]. Però això no serà mai culpa de l'automorfisme ρ, atès que $C/\langle\rho\rangle \simeq \mathbb{P}^1$ (de fet, el morfisme de pas al quocient determina la sèrie lineal g_3^1 que fa que C sigui una corba de Picard). Per a una corba de Picard genèrica, $J(C)$ serà simple i per tant serà una varietat abeliana amb multiplicació complexa en el sentit habitual. El resultat següent dóna un cert recíproc d'aquesta afirmació:

4.1.1 Lema *Sigui A una varietat abeliana principalment polaritzada de dimensió 3 sobre κ. Si A té multiplicació complexa per un cos CM K que conté les arrels cúbiques de la unitat i a més $\zeta_3 \in \mathrm{End}(A)$, llavors A és la jacobiana d'una corba de Picard no singular.*

Demostració: Les varietats abelianes CM són simples, ja que la seva àlgebra d'endomorfismes és un cos. Com la dimensió de l'espai de mòduli de les varietats abelianes principalment polaritzades de dimensió g és $g(g+1)/2$ i la dimensió de l'espai de mòduli de corbes de gènere g és $3g-3$, tenim que una varietat abeliana A irreductible de dimensió 3 és la jacobiana $J(C)$ d'una corba C de gènere 3. Una versió estesa del teorema de Torelli [Mil86, teorema 12.1] ens diu que no només C queda unívocament determinada per A, sinó que a més se satisfà $\mathrm{Aut}(C) = \mathrm{Aut}(A)/G$ amb $G \subseteq \{\pm 1\}$. Atès que ζ_3 és un automorfisme *autèntic* d'A i té ordre 3, ha de provenir d'un automorfisme ρ de la corba C. La corba quocient $\overline{C} := C/\langle\rho\rangle$ és racional, perquè sabem que $J(C) = A$ és simple. Per tant, el cos $\kappa(\overline{C})$ és un cos de funcions racionals $\kappa(X)$. L'extensió $\kappa(C)/\kappa(\overline{C})$ és una extensió de Kummer de grau 3, per la qual cosa ve donada per una equació $Y^3 = f(X)$, amb f un polinomi amb coeficients en κ. La fórmula de Hurwitz ens diu que el morfisme de pas al quocient $C \to \overline{C}$ és ramificat en cinc punts; si fem que l'infinit sigui un d'aquests punts, podrem garantir que el polinomi f tingui grau 4. ∎

A partir d'ara, doncs, fixarem el cos CM K que conté les arrels cúbiques de la unitat, i suposarem que $K = K_0(\zeta_3)$, on K_0 és una extensió totalment real. Fixarem també un CM-tipus Φ.

[1] Per exemple, la jacobiana de la corba $Y^3 = X^4 - 1$ és isògena a un producte de tres corbes el·líptiques.

És ben conegut que el cardinal de la reducció d'una varietat abeliana CM sobre un cos finit $\mathbb{F}_{p^n}$ està determinat per la descomposició del primer p en l'ordre de la multiplicació complexa. Ara concretarem aquesta relació en el cas de les jacobianes de les corbes de Picard, sobre un cos primitiu $\mathbb{F}_p$ amb $p \equiv 1 \pmod 3$. L'endomorfisme de Frobenius sobre $J(C)$ correspon a un element $w \in \mathcal{O} := \mathrm{End}(A) \subset K$, que satisfà $K = \mathbb{Q}(w)$. A més, el polinomi $f_w(X) := \mathrm{Irr}(w, \mathbb{Q}, X)$ coincideix amb el polinomi característic del Frobenius sobre el mòdul de Tate ℓ-àdic de $J(C)$ (amb $\ell \neq p$). Això ens diu que $\sharp J(C)(\mathbb{F}_p) = f_w(1)$.

Sigui

$$S_{\mathcal{O},p} := \{w \in \mathcal{O} : w\overline{w} = p, \mathbb{Q}(w) = K\}/\sim,$$

on $w_1 \sim w_2$ si w_1, w_2 són conjugats galoisians. Sigui

$$N_{\mathcal{O},p} := \{n \in \mathbb{N} : \exists J(C) \text{ tal que } \mathrm{End}(J(C)) = \mathcal{O}\text{i}\sharp J(C)(\mathbb{F}_p) = n\}.$$

Aquests dos conjunts tenen cardinal finit, i $|N_{\mathcal{O},p}| \leq |S_{\mathcal{O},p}|$. Els elements de $S_{\mathcal{O},p}$ poden determinar-se simplement factoritzant l'ideal (p) en $\mathcal{O}$, la qual cosa és una tasca computacionalment eficient en un grau tant baix. A partir d'aquest conjunt, és senzill determinar $\sharp J(C)(\mathbb{F}_p)$, triant elements a l'atzar del grup de classes de divisors i calculant el seu ordre.

4.2 El mètode CM

Ja hem explicat en la introducció l'esquema bàsic genèric del mètode CM. Volem concretar-lo per a corbes de Picard, però abans de ferho serà bo repassar el mètode en el cas més conegut de les corbes el·líptiques.

Recordem quins passos seguim per determinar totes les corbes el·líptiques amb multiplicació complexa per un ordre quadràtic imaginari $\mathcal{O}$:

1. Determinem $\mathrm{Cl}(\mathcal{O}) = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_h]\}$.
2. Calculem bases $\mathfrak{a}_k = \langle 1, \tau_k \rangle$.
3. Calculem numèricament $H_{\mathcal{O}}(X) = \prod_k (X - j(\tau_k))$.

4. Per a cada arrel j_k de $H_{\mathcal{O}}(X)$, determinem la corba el·líptica d'invariant j_k.

Per poder fer el mateix amb corbes de Picard ens cal:

1. **Polaritzacions:** Per poder dur a terme el pas 2, hem de polaritzar els tors complexos $\mathbb{C}^g/\Phi(\mathfrak{a}_k)$. Les polaritzacions d'aquests tors vam estudiar-les en el STNB-2000 (cf. [GL00]), on el lector trobarà tots els detalls necessaris per seguir el text de [KW04].
2. **Invariants:** Hem de definir invariants de les corbes de Picard, que juguin el mateix paper que l'invariant j de les corbes el·líptiques i permetin calcular polinomis de classes.
3. **Formes modulars**: Hem d'aprendre a calcular numèricament els invariants anteriors, i per això, essencialment ens caldrà identificar-los d'alguna manera com a formes modulars (de Siegel!).

Aquestes necessitats seran cobertes en les seccions properes.

4.3 Invariants de corbes de Picard

Una equació projectiva d'una corba de Picard genèrica té la forma:

$$C_{/\kappa} : ZY^3 = \alpha_4 X^4 + \alpha_3 X^3 Z + \alpha_2 X^2 Z^2 + \alpha_1 X Z^3 + \alpha_0 Z^4.$$

Els automorfismes lineals de $\mathbb{P}^2(\kappa)$ que mantenen aquest tipus d'equacions són anomenades *transformacions de Tshcirnhaus* i venen donades per

$$\tau \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ r & u^3 & 0 \\ 0 & 0 & u^4 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}, \quad u, r \in \kappa, u \neq 0.$$

Sota aquesta transformació, la corba C s'aplica en la corba $\overline{C}$ d'equació

$$\overline{C}_{/K} : ZY^3 = \overline{\alpha}_4 X^4 + \overline{\alpha}_3 X^3 Z + \overline{\alpha}_2 X^2 Z^2 + \overline{\alpha}_1 X Z^3 + \overline{\alpha}_0 Z^4.$$

Les dues equacions queden lligades per les relacions:

$$\begin{cases} \overline{\alpha}_4 = \alpha_4, \\ u^3\overline{\alpha}_3 = \alpha_3 + 4r\alpha_4, \\ u^6\overline{\alpha}_2 = \alpha_2 + 3r\alpha_3 + 6r^2\alpha_4, \\ u^9\overline{\alpha}_1 = \alpha_1 + 2r\alpha_2 + 3r^2\alpha_3 + 4r^3\alpha_4, \\ u^{12}\overline{\alpha}_0 = \alpha_0 + r\alpha_1 + r^2\alpha_2 + r^3\alpha_3 + r^4\alpha_4. \end{cases}$$

Per a cossos κ de característica diferent de 2 i 3, es consideren els paràmetres següents de les corbes de Picard:

$$\begin{cases} i = (12\alpha_0\alpha_4 - 3\alpha_1\alpha_3 + \alpha_2^2)/6, \\ j = (72\alpha_0\alpha_2\alpha_4 + 9\alpha_1\alpha_2\alpha_3 - 2\alpha_2^3 - 27\alpha_1^2\alpha_4 - 27\alpha_0\alpha_3^2)/72, \\ i_\alpha = i^3/j^2, \\ \Delta = (i^3 - 6j^2)/27 = j^2(i_\alpha - 6)/27. \end{cases}$$

Es pot comprovar que C és no-singular si, i només si, $\Delta \neq 0$. Les transformacions de Tschirnhaus afecten aquests paràmetres segons les relacions:

$$\begin{cases} i = u^{12}\overline{i}, \\ j = u^{18}\overline{j}, \\ i_\alpha = \overline{i}_\alpha, \\ \Delta = u^{36}\overline{\Delta}. \end{cases}$$

Si char$(\kappa) \neq 2$, sempre podem trobar una *forma normal* de qualsevol corba de Picard. Aquestes formes normals són:

$$ZY^3 = X^4 + \mathbf{g}_2X^2Z^2 + \mathbf{g}_3XZ^3 + \mathbf{g}_4Z^4,$$

Els paràmetres corresponents a una forma normal venen donats per:

$$\begin{cases} i = (12\mathbf{g}_4 + \mathbf{g}_2^2)/6 \\ j = (72\mathbf{g}_4\mathbf{g}_2 - 2\mathbf{g}_2^3 - 27\mathbf{g}_3^2)/72 \end{cases}$$

Si dues corbes $C, \overline{C}$ són isomorfes, haurà de ser $\mathbf{g}_k = u^{3k}\overline{\mathbf{g}}_k$ per a certa $u \in \kappa^*$. El recíproc també és evidentment cert. Això ens fa adonar que els quocients $\mathbf{g}_3^2/\mathbf{g}_2^3, \mathbf{g}_4/\mathbf{g}_2^2$ són invariants de la classe d'isomorfisme de C. El teorema següent ens dóna la classificació mòdul $\overline{\kappa}$-isomorfisme de les corbes de Picard (en característica diferent de 2 i 3):

4.3.1 Teorema *Siguin $C, \overline{C}$ dues corbes de Picard. Considerem els invariants $j_1 := \frac{\mathbf{g}_3^2}{\mathbf{g}_2^3}, j_2 = \frac{\mathbf{g}_4}{\mathbf{g}_2^2}$ de C i els invariants $\overline{j}_1, \overline{j}_2$ anàlegs de $\overline{C}$. Les corbes $C, \overline{C}$ són $\overline{\kappa}$-isomorfes si, i només si:*

Cas $\boxed{\mathbf{g_2 g_3 \neq 0}\textit{:}}$ $\quad j_1 = \overline{j}_1, j_2 = \overline{j}_2.$

Cas $\boxed{\mathbf{g_3 = 0, g_2 \neq 0}\textit{:}}$ $\quad j_2 = \overline{j}_2.$

Cas $\boxed{\mathbf{g_2 = 0, g_3 g_4 \neq 0}}$ $\quad \frac{j_2^3}{j_1^2} = \frac{\overline{j}_2^3}{\overline{j}_1^2}.$

Cas $\boxed{\mathbf{g_2 = g_4 = 0, g_3 \neq 0}}$ $\quad \mathbf{g}_3/\overline{\mathbf{g}}_3 \in \kappa^{*9}$

Cas $\boxed{\mathbf{g_2 = g_3 = 0, g_4 \neq 0}}$ $\quad \mathbf{g}_4/\overline{\mathbf{g}}_4 \in \kappa^{*12}.$

Cas $\boxed{\mathbf{g_2 = g_3 = g_4 = 0}}$ $\quad C \simeq_{/\kappa}: ZY^3 = X^4.$

Podem anar un pas més enllà encara, i donar representants de totes les classes d'isomorfisme:

4.3.2 Teorema *Sigui κ_0 el cos primer de κ. El cos de moduli d'una corba de Picard coincideix amb el cos de definició, i s'obté adjuntant a κ_0 els invariants de la corba.*

Demostració: El cas genèric correspon a una corba de Picard amb $g_2 g_3 \neq 0$. En aquest cas, donats $j_1, j_2 \in \overline{\kappa}$, la corba $C : Y^3 = X^4 + j_1 X^2 + j_1^2 X + j_1^2 j_2$ satisfà $j_1(C) = j_1, j_2(C) = j_2$. La resta de casos es deixen com a exercici per al lector. ■

4.4 El problema de Torelli per a corbes de Picard

En aquesta secció proposarem una solució teòrica del problema de Torelli en el cas específic de les corbes de Picard. La qüestió és: donada una matriu de períodes $Z \in \mathbb{H}_3$ de la qual sabem que el tor complex corresponent $\mathbb{C}^g/(1_g|Z)$ és isomorf a la jacobiana $J(C)$ d'una corba de Picard, hem de trobar una equació d'aquesta corba.

L'estratègia que seguirem serà determinar una equació de C de la forma

$$Y^3 = X(X-1)(X-\lambda)(X-\mu).$$

L'eina bàsica serà el resultat clàssic següent:

4.4.1 Teorema (Riemann, [Hol95]) *Sigui C corba de gènere g, i $f \in \mathbb{C}(C)$ una funció sobre C, amb divisor* $\mathrm{div}(f) = \sum_{k=1}^{m} A_k - B_k$. *Existeix una constant M tal que per a qualsevol divisor efectiu de grau g $D = P_1 + \cdots + P_g \in \mathrm{Div}^g(C)$ se satisfà la igualtat:*

$$f(D) := f(P_1)\cdots f(P_g) = M \prod_{k=1}^{m} \frac{\theta\left(\sum_{i=1}^{g} \int_{P_0}^{P_i} \overline{\omega} - \int_{P_0}^{A_k} \overline{\omega} - \Delta, Z\right)}{\theta\left(\sum_{i=1}^{g} \int_{P_0}^{P_i} \overline{\omega} - \int_{P_0}^{B_k} \overline{\omega} - \Delta, Z\right)}$$

Suposem que tenim $C : Y^3 = X(X-1)(X-\lambda)(X-\mu)$. Considerem els punts $P_0 = \infty, P_1 = (0,0), P_2 = (1,0), P_3 = (\lambda, 0), P_4 = (\mu, 0)$ fixos per l'automorfisme ρ. Apliquem el teorema de Riemann a la funció $f = x$ i el divisor $D = 2P_2 + P_3$:

$$\lambda = x(2P_2 + P_3) = M \left(\frac{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_3} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)}{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_3} \overline{\omega} - \Delta, Z\right)} \right)^3$$

Per poder calcular λ a partir de Z encara ens cal eliminar la constant M. Un truc senzill ens ho permet: només hem d'aplicar el teorema de Riemann a la funció $f = x^2$ per obtenir una expressió anàloga a l'anterior per a $\lambda^2 = x(P_2 + 2P_3)$. Dividint les dues relacions arribem a:

$$\lambda = \left(\frac{\theta\left(\int_{P_0}^{P_2} \overline{\omega} + 2\int_{P_0}^{P_3} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)}{\theta\left(\int_{P_0}^{P_2} \overline{\omega} + 2\int_{P_0}^{P_3} \overline{\omega} - \Delta, Z\right)} \frac{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_3} \overline{\omega} - \Delta, Z\right)}{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_3} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)} \right)^3$$

Anàlogament $\mu = \dfrac{x(P_2 + 2P_4)}{x(2P_2 + P_4)}$ i arribem a:

$$\mu = \left(\frac{\theta\left(\int_{P_0}^{P_2} \overline{\omega} + 2\int_{P_0}^{P_4} \overline{\omega} - \int_{P_0}^{P_k} \overline{\omega} - \Delta, Z\right)}{\theta\left(\int_{P_0}^{P_2} \overline{\omega} + 2\int_{P_0}^{P_4} \overline{\omega} - \Delta, Z\right)} \frac{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_4} \overline{\omega} - \Delta, Z\right)}{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_4} \overline{\omega} - \int_{P_0}^{P_k} \overline{\omega} - \Delta, Z\right)} \right)^3$$

Utilitzant que $(2\int_{P_0}^{P_2} + \int_{P_0}^{P_3}) + (\int_{P_0}^{P_2} + 2\int_{P_0}^{P_3}) \equiv 0$, la paritat de θ, i que $\sum_k 2\int_{P_0}^{P_k} \equiv 0$ s'obté:

4.4.2 Proposició

$$\lambda = \left(\frac{\theta\left(\int_{P_0}^{P_2} \overline{\omega} + 2\int_{P_0}^{P_3} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)}{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_3} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)} \right)^3$$

$$\mu = \left(\frac{\theta\left(\int_{P_0}^{P_2} \overline{\omega} + 2\int_{P_0}^{P_4} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)}{\theta\left(2\int_{P_0}^{P_2} \overline{\omega} + \int_{P_0}^{P_3} \overline{\omega} - \int_{P_0}^{P_1} \overline{\omega} - \Delta, Z\right)} \right)^3$$

A nivell teòric, el problema està completament resolt. Ara bé, nosaltres busquem una solució efectiva i eficient, i sota aquest prisma, el resultat anterior és totalment insatisfactori, perquè requereix el càlcul numèric d'integrals abelianes, una qüestió delicada i complexa. En la secció propera veurem com determinar el vector de Riemann Δ i les integrals abelianes $\displaystyle\int_{P_0}^{P_k} \overline{\omega}$ sense haver d'integrar.

4.5 Determinació d'integrals abelianes

Una de les parts més enginyoses del treball de Koike i Weng és la determinació a priori dels valors de les $\displaystyle\int_{P_0}^{P_k} \overline{\omega}$ sense necessitat d'integrar. La clau de la solució consisteix en usar i abusar dels automorfismes de la corba de Picard.

En endavant per simplificar emprarem la notació següent:

$$\alpha\left(\sum_{k=1}^{d} Q_k\right) := \sum_k \int_{P_0}^{Q_k} \overline{\omega}.$$

4.5.1 Proposició *El vector de Riemann Δ és l'únic element fix per ζ_3 de $J(C)[2]^{odd}$. Correspon a la recta quatritangent $Z = 0$.*

4.5.2 Proposició *Els elements $\alpha(P_1), \alpha(P_2), \alpha(P_3), \alpha(P_4) \in J(C)$ generen un subgrup $G \subset J(C)[3]$. Satisfan únicament la relació $\sum_k \alpha(P_k) = 0$.*

Demostració:

$$\begin{aligned}
&\mathrm{div}(x) = 3P_1 - 3P_0,\\
&\mathrm{div}(x-1) = 3P_2 - 3P_0,\\
&\mathrm{div}(x-\lambda) = 3P_3 - 3P_0,\\
&\mathrm{div}(x-\mu) = 3P_4 - 3P_0,\\
&\mathrm{div}(y) = P_1 + P_2 + P_3 + P_4 - 4P_0.
\end{aligned}$$

■

4.5.1 Lema *El subgrup G és $G = J(C)[1-\zeta_3]$ i té 27 elements.*

4.5.3 Proposició *El grup G té exactament 15 elements $\alpha(D)$ tals que $\theta(\alpha(D) + \Delta) = 0$. Venen donats pels divisors*

$$\{2P_1, P_1 + P_2, P_1 + P_3, P_1 + P_4, P_1 + P_0, 2P_2, P_2 + P_3,$$

$$P_2 + P_4, P_2 + P_0,\ 2P_3, P_3 + P_4, P_3 + P_0, 2P_4, P_4 + P_0, 2P_0\}.$$

Entre aquests, hi ha únicament dos conjunts de quatre elements que sumen 0:

$$\alpha(P_1), \alpha(P_2), \alpha(P_3), \alpha(P_4),$$

$$\alpha(2P_1), \alpha(2P_2), \alpha(2P_3), \alpha(2P_4).$$

4.6 L'algoritme complet

En aquesta secció detallem tots els passos que porten a la construcció d'una corba de Picard la jacobiana de la qual té CM per un cos donat.

Input: K cos CM , $\mathbb{Q}(\zeta_3) \subseteq K$, amb CM Φ tipus fixat
$\mathfrak{a} \subset O_K$,
$\xi \in O_K$ tal que $E(x,y) = \mathrm{Tr}(\zeta xy)$ és una polarització principal en $\mathbb{C}^3/(\Phi(\mathfrak{a}))$

Output: $C : Y^2 = X(X-1)(X-\lambda)(X-\mu)$ tal que $J(C) \simeq \mathbb{C}^3/(\Phi(\mathfrak{a}))$.

Algoritme:

1. Determinem una base simplèctica $(\Omega_1|\Omega_2)$ de $\Phi(\mathfrak{a})$ tal que $Z = \Omega_1^{-1}\Omega_2 \in \mathbb{H}_3$

2. Determinem la representació racional de ζ_3 en la base anterior.

3. Identifiquem $\Delta \in \frac{1}{2}\langle 1_3|Z\rangle$ fix per ζ_3 (és únic).

4. Identifiquem els 27 elements $\tau \in \frac{1}{3}\langle 1_3|Z\rangle$ fixos per ζ_3.

5. Triem entre els anteriors els 15 τ que $\theta(\tau+\Delta, Z) = 0$.

6. Determinem $\tau_1, \tau_2, \tau_3, \tau_4$ que satisfacin $\sum \tau_k = 0$.

7. Calculem λ, μ amb les fórmules de la proposició 4.4.2.

4.7 Formes modulars de Picard

Acabarem aquest capítol ressenyant un resultat teòric de Feustel i Shiga, que sembla que permetria estalviar-nos els passos 4, 5 i 6 de l'algoritme anterior.

4.7.1 Teorema (Feustel - Shiga [Hol95], pág. 60) *Considerem*

$$\theta_k(Z) := \theta\begin{bmatrix} 0 & 1/6 & 0 \\ k/3 & 1/6 & k/3 \end{bmatrix}(0, Z), \quad (k = 0, 1, 2)$$

i definim:

$$\begin{aligned} th_1(Z) &:= \theta_0(Z)^3 + \theta_1(Z)^3 + \theta_2(Z)^3, \\ th_2(Z) &:= -3\theta_0(Z)^3 + \theta_1(Z)^3 + \theta_2(Z)^3, \\ th_3(Z) &:= \theta_0(Z)^3 - 3\theta_1(Z)^3 + \theta_2(Z)^3, \\ th_4(Z) &:= \theta_0(Z)^3 + \theta_1(Z)^3 - 3\theta_2(Z)^3 \end{aligned}$$

Les funcions $th_k(Z)$ són formes modulars de Picard normalitzades *respecte un cert grup modular $S\Gamma$; satisfan les equacions funcionals:*

$$th_1(Z) + th_2(Z) + th_3(Z) + th_4(Z) = 0,$$

$$\gamma^*(th_k(Z)) = (\det\gamma)^2 sgn(\overline{\gamma}) j_\gamma th_k(\gamma Z), \; \forall\gamma \in S\Gamma, \qquad k = 1, 2, 3, 4.$$

Si $Z \in \mathbb{H}_3$ és la matriu de períodes normalitzada d'una corba de Picard C_Z, els valors $th_k(Z)$ proporcionen un model de C_Z:

$$Y^3 = (X - th_1(Z))(X - th_2(Z))(X - th_3(Z))(X - th_4(Z)).$$

J. Guàrdia
Dept. de Matemàtica Aplicada IV
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú
Av. Víctor Balaguer s/n
E-08800, Vilanova i la Geltrú
guardia@mat.upc.es

Capítol 5

Point Counting on Picard Curves in Large Characteristic

ROGER OYONO

An interesting problem in arithmetic geometry is to determine the order of $J_C(\mathbb{F}_q)$, the group of rational points on the Jacobian of a randomly chosen curve C defined over $\mathbb{F}_q$. In part, the importance of this question comes from the application of Abelian varieties to DLP-based cryptography.

5.1 Jacobian Varieties over finite fields

Let C be a non singular complete curve defined over $\mathbb{F}_q$, and let $M_r := \#C(\mathbb{F}_{q^r})$ for $r \geq 1$. The power series

$$\zeta(t, C) := \exp(\sum_{r=1}^{\infty} M_r t^r / r)$$

is called the zeta function of $C/\mathbb{F}_q$.

The zeta function gives some information about the number of $\mathbb{F}_q$-rational points on the Jacobian:

5.1.1 Theorem. (Weil)
Let C be a genus g curve defined over $\mathbb{F}_q$, and let $\zeta(t, C)$ be its zeta function. Then

1. *$\zeta(t, C)$ is a rational function of the form*
$$\zeta(t, C) = \frac{L(t, C)}{(1-t)(1-qt)},$$
where $L(t, C)$ is a polynomial (the L-polynomial of C) of degree $2g$ with integer coefficients.

2. *The polynomial $L(t, C)$ factors as*
$$L(t, C) = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \bar{\alpha_i} t),$$
where the $\bar{\alpha}_i$'s are complex conjugate of absolute values $\sqrt{q}$.

3. *The number of $\mathbb{F}_{q^r}$-rational points of the Jacobian is equal to*
$$\#J_C(\mathbb{F}_{q^r}) = \prod_{i=1}^{g} \|1 - \alpha_i^r\|^2,$$
where $\|\cdot\|$ denotes the usual absolute value. In particular
$$\#J_C(\mathbb{F}_q) = \prod_{i=1}^{g} (1 - \alpha_i)^2 = L(1, C).$$

Let π_q be the Frobenius endomorphism of C and $F_{\pi_q,C}(t)$ the characteristic polynomial of π_q on the Tate module $T_l(J_C) \otimes Q_l$. Then
$$F_{\pi_q,C}(t) = t^{2g} L(1/t, C).$$
For simplicity, we write $F(t)$ instead of $F_{\pi_q,C}(t)$ if the reference to the curve is clear. Similarly, we write $L(t)$ instead of $L(t, C)$.

If $N_r := \#C(\mathbb{F}_{q^r}) - (q^r + 1)$, and $L(t) =: \sum_{i=0}^{2g} c_i t^i$, then the coefficients c_i are determined by: $c_0 = 1,\ c_1 = N_1$,

$$c_i = \frac{1}{i} \left(N_i + \sum_{j+k=i, 1 \leq j,k \leq i-1} c_k N_j \right) , \quad i = 2, \ldots, g ,$$

$$c_{2g-i} = q^{g-i} c_i \text{ for } i = 0, \dots, g-1.$$

Thus, in order to determine the L-polynomial of a genus 3 curve, we only need to know three coefficients of this polynomial or, equivalently, the number of points $\#C(\mathbb{F}_{q^r})$ for $r = 1, 2, 3$. In terms of the N_r we have

$$c_1 = N_1 \ , \quad c_2 = \frac{1}{2}\left(N_2 + N_1^2\right), \\ c_3 = \frac{1}{3}\left(N_3 + \frac{3}{2}N_2N_1 + \frac{1}{2}N_1^3\right). \quad (5.1)$$

5.2 Picard curves

Let k be an arbitrary field and $\bar{k}$ an algebraic closure of k.

5.2.1 Definition. A Picard curve C/k is a genus 3 curve attached with a non trivial automorphism $\sigma \in \mathrm{Aut}_{\bar{k}}(C)$ such that $\sigma^3 = \mathrm{Id}$ and $(C \otimes_k \bar{k})/\langle\sigma\rangle \simeq \mathbb{P}^1_{\bar{k}}$.

If $\mathrm{char}(k) \neq 3$, a Picard curve C/k is $\bar{k}$-birationally equivalent to the non singular, absolutely irreducible curve with projective model

$$C: \ y^3 z = a_4 x^4 + a_3 x^3 z + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4 = \\ = a_4 \prod_{i=1}^{4} (x - \alpha_i z) =: p_4(x, z),$$

with $\alpha_i \in \bar{k}$, $\alpha_i \neq \alpha_j$ for $i \neq j$. In this coordinates, σ has the expression

$$\sigma(x, y, z) = (x, \zeta_3 y, z)$$

for a third primitiv root of unity ζ_3, i.e. $\zeta_3^2 + \zeta_3 + 1 = 0$.

If $\mathrm{char}(k) > 3$, there exists a normal form for Picard curves C/k :

$$C: \ y^3 z = x^4 + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4.$$

The automorphism σ fixes the points $R_i = (r_i, 0, 1)$ for $i := 1, \cdots, 4$, where the r_i are the zeros of $p_4(x, 1) \in k[x]$, and also the point $P_\infty = (0, 1, 0)$. These are also the ramification points of the covering morphism $\varphi : C \longrightarrow \mathbb{P}^1_{\overline{k}}$ induced by $k(x) \longrightarrow k(C)$. All these ramification points are inflection points with inflection tangent $x - r_i z = 0$ at R_i and $z = 0$ at P_∞ (the canonical bitangent). Observe that the inflection points R_i are collinear and belong to the line $y = 0$ and note that any line passing through two σ-conjugate points P and σP cuts the curve C on the remaining conjugate $\sigma^2 P$ and P_∞.

5.3 L-polynomials of Picard curves

In this section we investigate the L-polynomial of a Picard curve. Is the field of definition $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$, then we have:

5.3.1 Lemma. *Let C be a Picard curve over $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$. Then the L-polynomial splits over $\mathbb{Q}$. More precisely, the group order of the Jacobian is divisible by $q + 1$.*

PROOF: Since every element in $\mathbb{F}_q$ is the unique third power of an element in $\mathbb{F}_q$ we have $\#C(\mathbb{F}_q) = q + 1$. Similarly, $\#C(\mathbb{F}_{q^3}) = q^3 + 1$. Thus, $N_1 = N_3 = 0$. Now suppose $N_2 = a$. Then a is even and by (5.1), $L(t) = (qt^2 + 1)(q^2t^4 + (a/2)t^2 - qt^2 + 1)$. Substituting $t = 1$ gives the desired result. □

The most difficult case is when $q \equiv 1 \pmod 3$. In this case we will show that the characteristic polynomial $F(t)$ of Frobenius splits in $\mathbb{Z}[\zeta_3] = \mathbb{Z} \oplus \frac{-1+\sqrt{-3}}{2}\mathbb{Z}$ in two (not necessarily irreducible) factors $g(t)$ and $\overline{g}(t)$ where $\overline{g}(t)$ is obtained from $g(t)$ by applying complex conjugation to the coefficients. Moreover, for the vast majority of curves over $\mathbb{F}_q = \mathbb{F}_{p^n}$, we have

$$g(t) = t^3 - a_1 t^2 + \overline{a_1} \pi^n t - \pi^n q \ ,$$

where $\pi \in \mathbb{Z}[\zeta_3]$ such that $p = \pi\overline{\pi}$, and $v_\pi(a_1) = v_{\overline{\pi}}(a_1) = 0$.

In the case $q \equiv 1 \pmod 3$, the automorphism σ of order 3 on the Picard curve C is defined over $\mathbb{F}_q$. It extends to an automorphism of the Jacobian. Hence, $\mathbb{Z}[\zeta_3] \subseteq \mathrm{End}(J_C)$ or more precisely, $\mathbb{Z}[\zeta_3]$ is contained in the center of the endomorphism ring. Now, using [Tat66] we get three possibilities:

1. J_C is absolutely simple. Here $\mathrm{End}(J_C) \otimes \mathbb{Q}$ is a CM field of degree 6. It is a composite of a totally real field of degree 3 and $\mathbb{Q}(\zeta_3)$.

2. J_C is over $\mathbb{F}_q$ isogenous to the product of an abelian variety of dimension 2 and an elliptic curve. They are both simple over $\mathbb{F}_q$. Further, we see that the automorphism of order 3 acts on each factor. Hence, $F(t)$ splits into four factors over $\mathbb{Q}[\zeta_3]$, two factors of degree 2 and two linear factors.

3. J_C is isogenous to the product of three elliptic curves. Arguing like in (2) we see that $F(t)$ splits completely over $\mathbb{Q}[\zeta_3]$.

The first case is the most frequent one. To see this, note that there are $O(q^2)$ isomorphism classes of Picard curves over $\mathbb{F}_q$ since the moduli space has dimension 2. There are at most six isomorphism classes of elliptic curves with complex multiplication (CM) by $\mathbb{Z}[\zeta_3]$. Therefore, the number of isomorphism classes of Picard curves whose Jacobian is isogenous to the product of elliptic curves can be bounded by a constant not depending on q. Moreover, the moduli space of abelian surfaces with CM by $\mathbb{Z}[\zeta_3]$ is one-dimensional: Every abelian surface is isogenous to the Jacobian of a hyperelliptic curve C. If J_C has CM by $\mathbb{Z}[\zeta_3]$, then C can be written in the form

$$y^2 = x^6 + ax^3 + b \ ,$$

and $j = b/a^3$ determines the isomorphism class for $a \neq 0$.

From now on we restrict ourselves to the first case. For the other cases, see Remark 5.3.4.

Let K be the CM field $\mathrm{End}(J_C) \otimes \mathbb{Q}$. The points on the Jacobian form an $\mathcal{O}$-module where $\mathcal{O} \subseteq \mathcal{O}_K$ is an order in K containing the third roots of unity. Let w be an element in $\mathcal{O}_K$ corresponding to the Frobenius endomorphism π_q on the Jacobian J_C, i.e. $wP = \pi_q(P)$ for all $P \in J_C(\overline{\mathbb{F}_q})$ where the multiplication on the left hand side is the module multiplication. This property determines w uniquely.

We have $F(w) = 0$. We set $w_1 := w$ and denote by $w_2, \ldots, w_6$ the conjugates of w over $\mathbb{Q}$. We can reorder them such that $w_{i+3} = \overline{w_i}$ for $i = 1, 2, 3$. It is well-known that $w_i \overline{w_i} = q$ and $w_i + \overline{w_i}$ is a totally real element (see e.g. [Wat69]). Thus, $F(t)$ if of the very special form

$$\begin{aligned} F(t) &= (t - w_1)(t - \overline{w_1})(t - w_2)(t - \overline{w_2})(t - w_3)(t - \overline{w_3}) \\ &= t^6 - c_1 t^5 + c_2 t^4 - c_3 t^3 + q c_2 t^2 - q^2 c_1 t + q^3 \qquad (5.2) \end{aligned}$$

where

$$c_1 = \sum_{i=1}^{6} w_i \ , \quad c_2 = \sum_{i \leq j} w_i w_j \quad \text{and} \quad c_3 = \sum_{i \leq j \leq k} w_i w_j w_k \ .$$

Since $F(t)$ splits over $\mathbb{Q}(\zeta_3)$ we can write

$$F(t) = (t^3 - a_1 t^2 + a_2 t - a_3)(t^3 - \overline{a_1} t^2 + \overline{a_2} t - \overline{a_3}) \ , \qquad a_i \in \mathbb{Z}[\zeta_3] \ .$$

We put

$$g(t) = t^3 - a_1 t^2 + a_2 t - a_3 \ . \qquad (5.3)$$

Then $F(t) = g(t)\overline{g(t)}$ and

$$\#J_C(\mathbb{F}_q) = g(1)\overline{g(1)} \ . \qquad (5.4)$$

Also, $g(t)$ is the minimal polynomial of $w_i, i = 1, 2, 3$ over $\mathbb{Q}(\zeta_3)$, i.e.

$$a_1 = w_1 + w_2 + w_3, \quad a_2 = w_1 w_2 + w_1 w_3 + w_2 w_3, \quad a_3 = w_1 w_2 w_3.$$

5.3.2 Lemma. *Let C be a Picard curve over $\mathbb{F}_q$. Then $\#J_C(\mathbb{F}_q)$ is the norm of an element in $\mathbb{Z}[\zeta_3]$. In particular, if $l \equiv 2 \mod 3$ is prime and $\ell | \#J_C(\mathbb{F}_q)$, we already have $l^2 | \#J_C(\mathbb{F}_q)$.*

5.3.3 Lemma. *Let C be a Picard curve whose Frobenius has the characteristic polynomial $F(t) = g(t)\overline{g(t)}$. Then either $g(1)$ or $\overline{g(1)}$ annihilates the elements in $J_C(\mathbb{F}_q)$.*

Proof: If $F(t)$ is the characteristic polynomial of Frobenius and w is an algebraic integer such that $F(w) = 0$, then J_C is a $\mathbb{Z}[w]$-module and $w \cdot D = D$ for all $D \in J_C(\mathbb{F}_q)$. This is equivalent to $J_C(\mathbb{F}_q) \subset \ker(w - 1)$, and $(w - 1)$ divides either $g(1)$ or $\overline{g(1)}$. □

Using that $q = w_i\overline{w_i}$ for $i = 1, 2, 3$, we have

$$a_1\overline{a_3} = q\overline{a_2} \ . \tag{5.5}$$

By the triangle inequality we find

$$|a_1| = |w_1 + w_2 + w_3| \leq |w_1| + |w_2| + |w_3| = 3\sqrt{q} \ . \tag{5.6}$$

Consequently,

$$N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a_1) \leq 9q \ . \tag{5.7}$$

Let $q = p^n$ with $q \equiv 1 \pmod 3$. If $p \equiv 2 \pmod 3$, then n is even, so $n = 2n_1$ for some $n_1 \in \mathbb{N}$. Then $a_3 = \epsilon p^{3n_1}$ for some $\epsilon \in \mathbb{Z}[\zeta_3]$, $\epsilon^6 = 1$, and thus, $a_2 = \overline{a_1}\epsilon p^{n_1}$ by (5.5).

On the other hand, if $p \equiv 1 \pmod 3$ we have $p = \pi\overline{\pi}$ for some $\pi \in \mathbb{Z}[\zeta_3]$. We can write $q = p^n = \pi^n\overline{\pi}^n$. Then

$$a_3 = \epsilon\pi^{3n-2k}p^k, \quad 0 \leq k \leq \lfloor 3n/2 \rfloor, \quad \epsilon^6 = 1$$

By (5.5) we have $a_1\overline{\epsilon\pi^{3n-2k}p^k} = p^n\overline{a_2}$, and therefore

$$a_2 = \overline{a_1}\epsilon\pi^{3n-2k}p^{k-n} \ .$$

We distinguish three cases:

1. $k < n$: Here a_1 is divisible by π^{n-k}. Let a_1' be an integer in $\mathbb{Z}[\zeta_3]$ such that $a_1 = a_1'\pi^{n-k}$. We find
$$g(t) = t^3 - a_1'\pi^{n-k}t^2 + \overline{a_1'}\epsilon\pi^{2n-k}t - \epsilon\pi^{3n-2k}p^k \ .$$
Using (5.7), we see that
$$N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a_1') \leq \frac{9p^n}{p^{(n-k)}} = 9p^k \ .$$

2. $k > n$: Here $\overline{a_2}$ is divisible by p. It follows that the coefficient of t^3 in $F(t)$ is divisible by p. We find
$$g(t) = t^3 - a_1t^2 + \epsilon\overline{a_1}\pi^{3n-2k}p^{k-n}t - \epsilon\pi^{3n-2k}p^k \ .$$

3. $k = n$: Using (5.5) we see that
$$g(t) = t^3 - a_1t^2 + \epsilon\overline{a_1}\pi^n t - \epsilon\pi^n q \tag{5.8}$$
for some π with $\pi\overline{\pi} = p$.

In the first and second case the Picard curve is not ordinary, since its p-rank is smaller than 3 (for the relationship between the L-polynom and the p-Rank see e.g. [Bou00]). These cases are extremely rare, so that from now on we restrict ourselves to the third case, which is the most common one.

The main point in what follows is to determine a_1 given a_3, for which we discuss an algorithm in Section 5.4. We can bound the number of possible a_3 as follows. There are $\lfloor 3n/2 \rfloor + 1$ possibilites for k, and for each k we have 12 possibilities to choose a_3 since there are exactly 12 solutions π to the equation $\pi\overline{\pi} = p$. If π is one solution, then the other 11 solutions are given by

$$\zeta_3\pi, \zeta_3^2\pi, -\pi, -\zeta_3\pi, -\zeta_3^2\pi, \overline{\pi}, \zeta_3\overline{\pi}, \zeta_3^2\overline{\pi}, -\overline{\pi}, -\zeta_3\overline{\pi}, -\zeta_3^2\overline{\pi}.$$

5.3.4 Remark. *For the sake of completeness, let us consider the case that $F(t)$ splits over $\mathbb{Q}[\zeta_3]$.*

(2) $F(t)$ splits into two factors $f_i(t), i = 1, 2$ of degree $2i$: There are six possibilities for $f_1(t)$. Over $\mathbb{Q}(\zeta_3)$, $f_2(t)$ decomposes as $(t^2 - a_1 t + a_2)(t^2 - \overline{a_1} t + \overline{a_2})$, where $a_2\overline{a_2} = q^2$ and $a_1\overline{a_2} = q\overline{a_1}$. Thus, there is only a constant number of possibilities for the group order of $J_C(\mathbb{F}_q)$.

(3) $F(t)$ splits into three factors $f_i(t)$ of degree 2: Here for each $f_i(t)$ we have precisely six possibilities. Hence, there are at most $3^6/3!$ possibilities for $F(t)$.

5.4 A Baby-Step Giant-Step Algorithm

We now focus on the case $p = q$, and we show how to determine $\#J_C(\mathbb{F}_p) = F(1) = g(1)\overline{g(1)}$ using a time-memory trade-off. To be precise, we aim to determine the coefficients a_1, a_2, a_3 in (5.3) using Lemma 5.3.3. Since $n = k = 1$, we have exactly 12 candidates for a_3, corresponding to the 12 solutions to $p = \pi\overline{\pi}$. By applying the above method to all solutions (e.g. on 12 independent machines) we can easily determine the correct choice of a_3. Thus, here we restrict ourselves to the case that $a_3 = \pi p$. Using (5.8), we have $g(1) = 1 - a_1 + \overline{a_1}\pi - \pi p$. Since $a_1 \in \mathbb{Z} + \mathbb{Z}[\zeta_3] \subset \frac{1}{2}(\mathbb{Z} + \mathbb{Z}[\sqrt{-3}])$, we can write $a_1 = b_1 + b_2\sqrt{-3}$, where $b_i = d_i/2$ with $d_1, d_2 \in \mathbb{Z}$. Note that $d_1 \equiv d_2 \pmod 2$. Hence,

$$g(1) = 1 - \pi p - (1-\pi)b_1 - (1+\pi)\sqrt{-3}b_2 \ .$$

Now let D be a divisor in $J_C(\mathbb{F}_p)$. By Lemma 5.3.3, $g(1)D = 0$ or $\overline{g(1)}D = 0$. Without loss of generality assume that $g(1)D = 0$. Then

$$(1-\pi p)D - (1+\pi)\sqrt{-3}b_2 D = (1-\pi)b_1 D \ ,$$

or, using $\sqrt{-3} = 2\zeta_3 + 1$,

$$2(1-\pi p)D - (1+\pi)(2\zeta_3+1)d_2 D = (1-\pi)d_1 D \ . \tag{5.9}$$

Now, $d_1^2 = 4b_1^2 \le 4|a_1|^2 \le 36p$, that is, $|d_1| \le 6\sqrt{p}$, and $d_2^2 = 4b_2^2 \le 4|a_1|^2/3 \le 12p$ and therefore $|d_2| \le 2\sqrt{3p}$. To find d_1 and d_2, we mimick a baby-step giant-step approach: For all integer values d_2 with $|d_2| \le 2\sqrt{3p}$, store the left-hand side of (5.9) in a hash table (the "baby steps"), and then for all $|d_1| \le 6\sqrt{p}$ check if the right-hand side equals one of the stored elements ("giant steps"). If this is the case for a pair (d_1, d_2), then we put $a_1 = (d_1 + d_2\sqrt{-3})/2$, and we have that $2g(1)\overline{g(1)}$ is a multiple of the order of the divisor D. From this, the exact order can be easily determined, as shown in the pseudo-code below. Note that with the correct solution π, the algorithm is guaranteed to succeed, while it outputs "failure"only if the input value for π was wrong.

5.4.1 Algorithm Algorithm to compute $\operatorname{ord} D$ for $D \in J_C(\mathbb{F}_p)$.
INPUT: *Divisor $D \in J_C(\mathbb{F}_p)$, solution π to $p = \pi\overline{\pi}$*
OUTPUT: $\operatorname{ord} D$ *or "failure".*

```
1. { Precomputation: }
   $A \leftarrow 2(1-\pi p)D$, $B \leftarrow (1+\pi)(2\zeta_3+1)D$ and $C \leftarrow (1-\pi)D$.

2. $M \leftarrow \lfloor 2\sqrt{3p} \rfloor$.

3. $r_0 \leftarrow A - MB$ and $\mathcal{R} \leftarrow \{(r_0, M)\}$.

4. { Baby steps: }
   For $n \leftarrow 1, \dots, 2M$ do the following:
   $r_n \leftarrow r_{n-1} + B$.
   $\mathcal{R} \leftarrow \mathcal{R} \cup \{(r_n, M-n)\}$.
```

```
5. $s_0 \leftarrow 0$ and $t_0 \leftarrow s_0$.
   If $(s_0, j) \in \mathcal{R}$ for some $j \in \{-M, \dots, M\}$, then $a_1 \leftarrow j\sqrt{-3}/2$.
   GOTO Step (8).

6. { Giant steps: }
   For $n \leftarrow 1, \dots, \lfloor 6\sqrt{p} \rfloor$ do the following:
      $s_n \leftarrow s_{n-1} + C$.
      If $(s_n, j) \in \mathcal{R}$ for some $j \in \{-M, \dots, M\}$, then $a_1 \leftarrow (n + j\sqrt{-3})/2$. GOTO Step (8).
      $t_n \leftarrow t_{n-1} - C$.
      If $(t_n, j) \in \mathcal{R}$ for some $j \in \{-M, \dots, M\}$, then $a_1 \leftarrow (-n + j\sqrt{-3})/2$. GOTO Step (8).

7. { No match has been found, so $\pi$ was wrong. }
   Return "failure".

8. $g \leftarrow 1 - a_1 + \overline{a_1}\pi - \pi p$, $N \leftarrow 2g\overline{g}$. { $N$ is a multiple of $\operatorname{ord} D$. }

9. { Determine $\operatorname{ord} D$: }
   Factor $N$ into prime factors: $N = \prod_{i=1}^{d} p_i^{e_i}$.
   For $i \leftarrow 1, \dots, d$ find the smallest $E_i$ such that $(N/p_i^{E_i})D \neq 0$.

10. Return $T \leftarrow \prod_{i=1}^{d} p_i^{e_i - E_i + 1}$.
```

It is immediate that for each divisor D, Algorithm 5.4.1 requires at most $4(3 + \sqrt{3})\sqrt{p} \leq 19\sqrt{p}$ additions in the Jacobian to execute the baby and giant steps; the precomputation requires $O(\log p)$ operations. We need to store at most $4\sqrt{3p} + 1$ pairs $(D, j) \in J_C(\mathbb{F}_p) \times \{-M, \dots, M\}$.

Next we discuss a variant of 5.4.1 that is designed to address some of the issues that arise in implementing the arithmetic in the Jacobians of Picard curves. In particular, given two divisors D_1 and D_2, the standard addition and reduction formulas compute $D_3 \sim -D_1 - D_2$. Let this addition and reduction be denoted by $\oplus$. To compute $D_1 + D_2$, an additional inversion step is required. Correspondingly, let the standard symbol + represent addition followed by the reduction and inversion. Now, unlike the arithmetic for hyperelliptic curves, inversion is not free. We can avoid the extra inversion step by working in the wrong, inverse class half of the time. Moreover, we can exploit that $d_1 \equiv d_2 \pmod 2$ to break the search space up into two pieces that can be processed in parallel. We give the pseudo-code of the new algorithm first, with the explanation to follow. It might be helpful to note that the superscripts "+" and "-" as well as the variable toggle are due to the inversion-freeness, while the subscripts "even" and "odd" relate to the breaking up the search space.

5.4.2 Algorithm Algorithm to compute $\operatorname{ord} D$, avoiding inversions.
INPUT: *Divisor* $D \in J_C(\mathbb{F}_p)$, *solution* π *to* $p = \pi\overline{\pi}$.
OUTPUT: $\operatorname{ord} D$, *or "failure".*

```
1. { Precomputation: }
   $A_{\mathrm{even}} \leftarrow 2(1-\pi p)D$,
   $A_{\mathrm{odd}} \leftarrow 2(1-\pi p)D - (1+\pi)(2\zeta_3+1)D - (1-\pi)D$,
   $B^+ \leftarrow -2(1+\pi)(2\zeta_3+1)D$, $B^- \leftarrow 2(1+\pi)(2\zeta_3+1)D$,
   $C^+ \leftarrow 2(1-\pi)D$, $C^- \leftarrow -2(1-\pi)D$.

2. $M \leftarrow \lfloor\sqrt{3p}\rfloor + 1$, toggle $\leftarrow 1$.

3. $r^+_{even,0} \leftarrow A_{\mathrm{even}}$, $r^-_{even,0} \leftarrow A_{\mathrm{even}}$, $\mathcal{R}_{even} \leftarrow \{(r^+_{even,0}, 0)\}$.
   $r^+_{odd,0} \leftarrow A_{\mathrm{odd}}$, $r^-_{odd,0} \leftarrow A_{\mathrm{odd}}$, $\mathcal{R}_{odd} \leftarrow \{(r^+_{odd,0}, 0)\}$.

4. { Baby steps: }
   For $n \leftarrow 1, \ldots, M$ do the following:
       If (toggle $= 1$)
           $r^+_{even,n} \leftarrow r^+_{even,n-1} \oplus B^+$,
           $r^-_{even,n} \leftarrow r^-_{even,n-1} \oplus B^-$,
           $r^+_{odd,n} \leftarrow r^+_{odd,n-1} \oplus B^+$,
           $r^-_{odd,n} \leftarrow r^-_{odd,n-1} \oplus B^-$.
       Else
           $r^+_{even,n} \leftarrow r^+_{even,n-1} \oplus B^-$,
           $r^-_{even,n} \leftarrow r^-_{even,n-1} \oplus B^+$,
           $r^+_{odd,n} \leftarrow r^+_{odd,n-1} \oplus B^-$,
           $r^-_{odd,n} \leftarrow r^-_{odd,n-1} \oplus B^+$.
       $\mathcal{R}_{even} \leftarrow \mathcal{R}_{even} \cup \{(r^+_{even,n}, n), (r^-_{even,n}, -n)\}$.
       $\mathcal{R}_{odd} \leftarrow \mathcal{R}_{odd} \cup \{(r^+_{odd,n}, n), (r^-_{odd,n}, -n)\}$.
       toggle $\leftarrow -$toggle.

5. $s_0 \leftarrow 0$.
   If $(s_0, j) \in \mathcal{R}_{even}$ for some $j \in \{-M, \ldots, M\}$, then $a_1 \leftarrow j\sqrt{-3}$.
```

```
    GOTO Step (8).
    If $(s_0, j) \in \mathcal{R}_{odd}$ for some $j \in \{-M, \dots, M\}$, then $a_1 \leftarrow (1 + (2j+1)\sqrt{-3})/2$. GOTO Step (8).

6.  { Giant steps: }
    toggle $\leftarrow 1$.
    For $n \leftarrow 1, \dots, \lfloor 3\sqrt{p} \rfloor + 1$ do the following:
        If (toggle $= 1$) then $s_n \leftarrow s_{n-1} \oplus C^+$.
        Else $s_n \leftarrow s_{n-1} \oplus C^-$.
        If $(s_n, j) \in \mathcal{R}_{even}$ for some $j \in \{-M, \dots, M\}$,
            then $a_1 \leftarrow (-1)^{n+j} n + j\sqrt{-3}$. GOTO Step (8).
        If $(-s_n, j) \in \mathcal{R}_{even}$ for some $j \in \{-M, \dots, M\}$,
            then $a_1 \leftarrow (-1)^{n+1+j} n + j\sqrt{-3}$. GOTO Step (8).
        If $(s_n, j) \in \mathcal{R}_{odd}$ for some $j \in \{-M, \dots, M\}$,
            then $a_1 \leftarrow (((-1)^{n+j} 2n + 1) + (2j+1)\sqrt{-3})/2$. GOTO Step (8).
        If $(-s_n, j) \in \mathcal{R}_{odd}$ for some $j \in \{-M, \dots, M\}$,
            then $a_1 \leftarrow (((-1)^{n+1+j} 2n + 1) + (2j+1)\sqrt{-3})/2$. GOTO Step (8).
        toggle $\leftarrow -$toggle.

7.  { No match has been found, so $\pi$ was wrong. }
    Return "failure".

8.  $g \leftarrow 1 - a_1 + \overline{a_1}\pi - \pi p$ and $N \leftarrow 2g\overline{g}$. { $N$ is a multiple of $\operatorname{ord} D$. }

9.  { Determine $\operatorname{ord} D$: }
    Factor $N$ into prime factors: $N = \prod_{i=1}^{d} p_i^{e_i}$.
    For $i \leftarrow 1, \dots, d$ find the smallest $E_i$ such that $N/p_i^{E_i} D \neq 0$.

10. Return $T \leftarrow \prod_{i=1}^{d} p_i^{e_i - E_i + 1}$.
```

We now explain Algorithm 5.4.2. Let $D \in J_C(\mathbb{F}_p)$. In (5.9), if d_1, d_2 are even, there exist integers k_1, k_2 with $|k_1| \leq 3\sqrt{p}$ and $|k_2| \leq \sqrt{3p}$ and such that $d_i = 2k_i$ $(i = 1, 2)$. Substituting into (5.9) gives

$$2(1 - \pi p)D - 2(1 + \pi)(2\zeta_3 + 1)k_2 D = 2(1 - \pi)k_1 D \ .$$

In terms of A_{even}, B^+ and C^+ (Step (2) of Algorithm 5.4.2), this means

$$A_{\text{even}} + k_2 B^+ = k_1 C^+ . \tag{5.10}$$

If d_1, d_2 are odd, we instead write $d_i = 2k_i + 1$ $(i = 1, 2)$. Then

$$\begin{aligned}&[2(1-\pi p)D - 2(1+\pi)(2\zeta_3+1)D - 2(1-\pi)D] - \\ &\qquad - (1+\pi)(2\zeta_3+1)\, 2k_2\, D = (1-\pi)\, 2k_1\, D \ ,\end{aligned}$$

which in terms of A_{odd}, B^+ and C^+ reads as

$$A_{\text{odd}} + k_2 B^+ = k_1 C^+ \ .$$

Now assume for some n and j we have $(s_n, j) \in \mathcal{R}_{even}$ (which happens if d_1, d_2 even). Then

$$(-1)^j (A_{\text{even}} + jB^+) = (-1)^n n C^+ \ .$$

Comparing with (5.10), we see that $k_1 = (-1)^{j+n} n$ and $k_2 = j$. Substituting back in for a_1 yields $a_1 = (-1)^{j+n} n + j\sqrt{-3}$. The additional check if $(-s_n, j) \in \mathcal{R}_{even}$ is necessary to compensate for the lack of inversions when adding divisors. In fact, if we instead found $(-s_n, j) \in \mathcal{R}_{even}$, then we have an extra inversion to compensate for. We obtain

$$(-1)^j (A_{\text{even}} + jB^+) = (-1)^{n+1} n C^+ \ ,$$

which implies $a_1 = (-1)^{j+n+1} n + j\sqrt{-3}$. A similar argument holds for searching for k_1, k_2 in the case the d_i are odd, in which case the match is found within $\mathcal{R}_{odd}$. In any case, by construction of a_1 and with $g = 1 - a_1 + \overline{a_1}\pi - \pi p$, $2g\overline{g}$ is a multiple of $\operatorname{ord} D$.

Note that Algorithm 5.4.2 requires essentially the same number of operations in the Jacobian as Algorithm 5.4.1, but each operation is cheaper since we use "$\oplus$" instead of "$+$".

5.4.3 Remark. *Note that in the most cases, Algorithm 5.4.1 (resp. Algorithm 5.4.2) recovers not only $g(1)$ but also the coefficients of the polynomial $g(t)$. Thus gives us the whole L-polynomial of the curve C. The L-polynomial contains more information than the group order of the Jacobian alone. In particular we find $\#C(\mathbb{F}_{q^r})$ for all $r \in \mathbb{N}$.*

5.4.1 The choice of π.

In principle, we have 12 different possibility for $\pi \in \mathbb{Z}[\zeta_3]$ such that $\pi\bar{\pi} = p$. For the operation of the automorphism σ of order 3, we have to make a choice of the third root of unity modulo p. Let us call this z. The choice of π has to be consistent with the choice of the root of unity, i.e. if $\pi = a + b\zeta_3$, we must have $a + bz \equiv 0 \mod p$. We easliy see that for each set of conjugates $\{\pi, \bar{\pi}\}$ there is precisely one element which satisfies this condition. Hence, we are left with 6 instead of 12 different values of π. In fact, given a prime p, all these different values can occur. But if we restrict to special curves, we can reduce the possible set of elements further:

5.4.4 Lemma. *Let C be a Picard curve defined over $\mathbb{F}_p$ with $p \equiv 1 \mod 3$ and assume that the group order of $J_C(\mathbb{F}_p)$ is not divisible by 3. Then the element π satisfies $\pi \equiv 2 \mod (1 - \zeta_3)$.*

PROOF: $1-\zeta_3$ is prime in $\mathbb{Z}[\zeta_3]$ since $N(1-\zeta_3) = 3$ and thus $\mathbb{Z}[\zeta_3]/(1-\zeta_3) \simeq \mathbb{F}_3$. Obviously, $\pi \not\equiv 0 \mod (1-\zeta_3)$, since p is prime. Moreover, since $\#J_C(\mathbb{F}_p)$ is not divisible by 3,

$$1 - a_1 + \bar{a_1}\pi - \pi p \not\equiv 0 \mod (1 - \zeta_3).$$

Since $p \equiv 1 \mod 3$, $3 = -\zeta_3^2(1-\zeta_3)^2$ and $a_1 \equiv \bar{a_1} \mod (1-\zeta_3)$ for all $a_1 \in \mathbb{Z}[\zeta_3]$, we have

$$\begin{aligned} 1 - a_1 + \bar{a_1}\pi - \pi p &\equiv 1 - a_1 + \bar{a_1}\pi - \pi \mod (1-\zeta_3) \\ &\equiv 1 - a_1 + a_1\pi - \pi \mod (1-\zeta_3) \\ &\equiv (1-a_1)(1-\pi) \mod (1-\zeta_3). \end{aligned}$$

Hence, $\pi \not\equiv 1 \mod (1-\zeta_3)$ and the claim follows. □

To check the condition of the preceding lemma, we can use information on the 3^k-torsion part of the Jacobian immediately deduced from the defining equation of the curve. First note that the points on C with vanishing y-coordinate correspond to $(1-\zeta_3)$-torsion points of the Jacobian. Now, $J_C[1-\zeta_3] \simeq (\mathbb{Z}/3\mathbb{Z})^3$, and any three points with vanishing y-coordinate generate the entire $(1-\zeta_3)$-torsion group.

5.4.5 Lemma. *Let $q \equiv 1 \pmod 3$. Let $y^3 = f(x)$ be the defining equation of a Picard curve C and let $N = \#J_C(\mathbb{F}_q)$.*

1. *If $f(x)$ splits completely over $\mathbb{F}_q$, then $N \equiv 0 \mod 27$.*
2. *If $f(x)$ splits into three factors over $\mathbb{F}_q$, then $N \equiv 0 \mod 9$.*
3. *If $f(x)$ splits into a factor of degree 3 and a factor of degree 1, or into two factors of degree 2, then $N \equiv 0 \mod 3$.*
4. *If $f(x)$ is irreducible over $\mathbb{F}_q$, then $N \equiv 1 \mod 3$.*

PROOF:

1. Since $J_C[1-\zeta_3]$ is defined over $\mathbb{F}_q$, we have $(\mathbb{Z}/3\mathbb{Z})^3 \leq J_C(\mathbb{F}_q)$.
2. The two $(1-\zeta_3)$-torsion points arising from the roots of $f(x)$ are linearly independent. Hence, $(\mathbb{Z}/3\mathbb{Z})^2 \leq J_C(\mathbb{F}_q)$.
3. In this case, we only know that $J_C(\mathbb{F}_q)$ contains one non-trivial $(1-\zeta_3)$-torsion point.
4. Since N is a norm in $\mathbb{Z}[\zeta_3]$, it is $N \equiv 0, 1 \pmod 3$. Furthermore, if $f(x)$ is irreducible there are no $(1-\zeta_3)$-torsion points in $J_C(\mathbb{F}_q)$. Since 3 ramifies in $\mathbb{Z}[\zeta_3]$, i.e. $3 = -\zeta_3^2(1-\zeta_3)^2$, there are also no 3-torsion points in $J_C(\mathbb{F}_q)$. Since N is a norm of an element in $\mathbb{Z}[\zeta_3]$, we must have $N \equiv 1 \mod 3$.

□

5.4.2 Computing $\#J_C(\mathbb{F}_p)$.

If $\operatorname{ord} D > 12p^{5/2} + 40p^{3/2} + 12\sqrt{p}$, then $\#J_C(\mathbb{F}_p)$ is the unique multiple of $\operatorname{ord} D$ in the Hasse-Weil interval $[(\sqrt{p}-1)^6, (\sqrt{p}+1)^6]$. For cryptographically interesting curves whose Jacobian has an almost prime group order, this is the most likely case.

If, on the other hand, more than one multiple of $\operatorname{ord} D$ lies in the Hasse-Weil interval, instead of running the same algorithm with another divisor (which is not only expensive but also might not yield the desired result either), there are two ways to proceed:

Let $N = \#J_C(\mathbb{F}_p)$. First note that if a prime l with $l \equiv 2 \pmod 3$ divides N, then also $l^2 \mid N$. Hence,

$$\prod_{l \mid (\operatorname{ord} D) \;,\; l \equiv 2 \pmod 3} l^2 \mid N \,.$$

Now assume l is a prime such that $l \,||\, \operatorname{ord} D$ and $l \equiv 1 \pmod 3$. Let $D_1 = (\operatorname{ord} D/l)D$. If $l \,||\, N$, then ζ_3 must permute the l-torsion points generated by D_1 among themselves. Now let $\eta \in \mathbb{Z}/l\mathbb{Z}$ be a cube root of unity. If ζ_3 acts cyclicly on D_1, then $\eta D_1 = D_1^{\zeta_3}$ or $\eta D_1 = D_1^{\zeta_3^2}$. If neither holds, we can conclude that $l^2 \mid N$.

Thus, by checking the factors of $\operatorname{ord} D$ we may be able to determine a larger divisor of N than $\operatorname{ord} D$ itself, which may have a unique multiple in the Hasse-Weil interval and we are done.

Otherwise, note that Algorithm 5.4.2 (and 5.4.1) is designed to find *candidates* for $g(1)$. In particular, if $\operatorname{ord} D$ is very small, the value g computed in Step (8) is not necessarily equal to $g(1)$ with $g(t)$ from (5.3). Hence, if the output $\operatorname{ord} D$ does not uniquely determine N, instead of terminating we continue the computation from where the algorithm's GOTO command was executed. This produces further successful table-lookups in $\mathcal{R}$ that yield further candidates for $g(1)$. On completion of all giant steps, the set of candidates for $g(1)$ contains the correct value. Only the proper value for $g(1)$ annihilates all divisors in the Jacobian. By testing the candidates with randomly chosen divisors wrong candidates can be eliminated, and eventually $\#J_C(\mathbb{F}_p)$ can be determined from the surviving candidate.

R. Oyono
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
roger.oyono@gmx.de

Capítol 6

Genus 1 AGM methods

CHRISTOPHE RITZENTHALER

This is an overview of the Arithmetic-Geometric Mean methods in the complex and 2-adic cases. We present in this chapter the AGM algorithm for point counting invented by [Mes02]. This method is an elegant variant of Satoh's algorithm [Sat00] based on the canonical lift and belongs therefore to the set of 2-adic methods. However its true inspiration has to be sought in the complex domain where the AGM sequences have first been used to compute elliptic integrals (and actually periods of elliptic curves). Thus, we start with a review of the complex (real) case before dealing with the more arithmetic part.

This presentation is essentially basic and does not include the last improvements of the AGM algorithm, other interpretations or generalization of this method. The interested reader may find them in the two main sources of the present chapter, namely [Rit03] and [Ver03].

6.1 The complex theory

6.1.1 Computation of periods

It was historically the first case handled : Lagrange [Lag67, t.II,p.253-312] and Gauss [Gau70, t.III,p.352-353,261-403] introduced the *Arith-*

metic geometric mean to compute elliptic integrals.

6.1.1 Theorem. *Let a, b be two reals such that $0 < b < a$. We have*

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2 \cos^2 t + b^2 \sin^2 t}} = \frac{\pi}{2\mathrm{M}(a,b)},$$

where $\mathrm{M}(a,b)$ *(*arithmetic geometric mean *of a and b) is the common limit of*

$$\begin{cases} a_0 = a & a_{n+1} = \frac{a_n+b_n}{2} \\ b_0 = b & b_{n+1} = \sqrt{a_n b_n} \end{cases}$$

Since

$$|a_{n+1} - b_{n+1}| = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} = \frac{(a_n - b_n)^2}{2(\sqrt{a_n} + \sqrt{b_n})^2} \leq \frac{(a_n - b_n)^2}{8b_1} \tag{6.1}$$

these two sequences are adjacent and the convergence is quadratic. This method is then better than traditional numeric integrations.
The proof is based on a tricky change of variables which transforms the parameters a, b in the integral into a_1, b_1. Taking the limit one has then the theorem.
To understand this change of variables we are going to algebraize our problem. Put $x = e_3 + (e_2 - e_3)\sin^2 t$ with

$$\begin{cases} a_0^2 & = e_1 - e_3 \\ b_0^2 & = e_1 - e_2 \\ 0 & = e_1 + e_2 + e_3 \end{cases}$$

We can reformulate the theorem as :

6.1.2 Theorem.

$$\int_{e_3}^{e_2} \frac{dx}{\sqrt{P(x)}} = \frac{\pi}{2\mathrm{M}(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$$

with $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$, $e_3 < e_2 < e_1$.

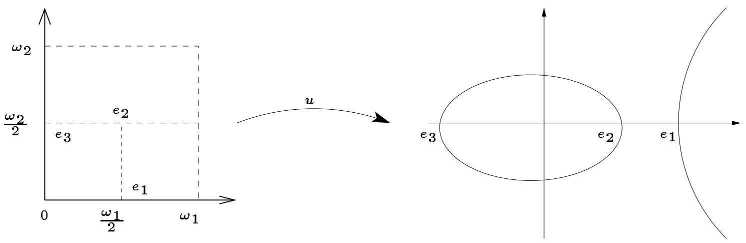
One recognizes the integral of a regular differential form on the elliptic curve $E : y^2 = P(x)$. More precisely, if one denotes by $\mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ (ω_1 real ω_2 purely imaginary) the complex torus $E(\mathbb{C})$, one has the isomorphism

$$\begin{array}{llll} u: & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) \quad z \notin \Lambda \\ & [z] & \mapsto & (0:1:0) \qquad\qquad\qquad\quad\; z \in \Lambda \end{array}$$

and (see figure 6.1)

$$\omega_1 = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} dz = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} \frac{d\mathcal{P}(z)}{\mathcal{P}'(z)} =$$
$$= 2\int_{e_3}^{e_2} \frac{dx}{y} = 2\int_{e_3}^{e_2} \frac{dt}{\sqrt{P(t)}}$$

Figura 6.1: The map u



The problem is now the computation of a perid of a differential of the 1st kind on a Riemann surface.
Let $\tau = \omega_2/\omega_1$. In the theory of abelian varieties over $\mathbb{C}$, it is classical to introduce *theta functions.* They can be seen as holomorphic sections of sheaves but we want to give here a more straightforward definition for elliptic curves (see [Ros86] for the general theory).

6.1.3 Definition. Let $\tau \in \mathbb{H}$, $\epsilon, \epsilon' \in \{0,1\}$. One defines the *theta function with characteristic* ${}^t[\epsilon, \epsilon']$ by

$$\theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](z,\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi(n+\epsilon/2)^2\tau + 2i\pi(n+\epsilon/2)(z+\epsilon'/2))$$

It is an anaytic function of the variable z. If $z = 0$, one denotes also $\theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](0,\tau) = \theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)$. When $[\epsilon,\epsilon'] \neq [1,1]$, $\theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau) \neq 0$ and is called a *theta constant.*
These values have the following properties [BM89].

6.1.4 Proposition. *1. Limit :*

$$\lim_{\operatorname{Im}\tau \to +\infty} \theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau) = \lim_{\operatorname{Im}\tau \to +\infty} \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau) = 1.$$

2. Thomae's formula :

$$\begin{cases} \omega_1\sqrt{e_1 - e_3} = & \pi \cdot \theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \\ \omega_1\sqrt{e_1 - e_2} = & \pi \cdot \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 \end{cases}$$

3. Duplication formula :

$$\begin{cases} \theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2\tau)^2 = & \frac{\theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 + \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2}{2} \\ \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2\tau)^2 = & \sqrt{\theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2} \end{cases}$$

6.1.5 Remark. *As the theta constants are positive reals (because τ is purely imaginary), the sign of the square roots is always the positive one. When it is nomore the case, the choice is a bit more subtil as we will see in 6.1.3.*

6.1.2 Proofs

We want to give two proofs of Th.6.1.2. The first one is straightforward. As the duplication formula is exactly the AGM recursion, we can write

$$\begin{cases} a_0 = \theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 & a_n = \theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2^n\tau)^2 \\ b_0 = \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 & b_n = \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2^n\tau)^2 \end{cases}$$

By the limit property, one has

$$\mathrm{M}\left(\theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2, \theta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2\right) = 1.$$

The AGM recursion being homogenous, one obtains the theorem thanks to Thomae's formula :

$$\begin{aligned} M(a_0,b_0) = M(\frac{\omega_1\sqrt{e_1-e_3}}{\pi}, \frac{\omega_1\sqrt{e_1-e_2}}{\pi}) &= \\ &= \frac{\omega_1}{\pi}M(\sqrt{e_1-e_3},\sqrt{e_1-e_2}) = 1. \end{aligned}$$

The second proof will reveal the true geometry behind the result. Consider again the elliptic curve $E : y^2 = P(x)$. This curve is isomophic to the curve $E_\tau = E_{a_0,b_0}$ defined by

$$\begin{aligned} E_\tau : y_0^2 &= x_0(x_0-(e_1-e_3))(x_0-(e_1-e_2)) && (6.2) \\ &= x_0\left(x_0 - \frac{\pi^2}{\omega_1^2}\cdot\theta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^4\right)\left(x_0 - \frac{\pi^2}{\omega_1^2}\cdot\theta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^4\right) && (6.3) \\ &= x_0(x_0-a_0^2)(x_0-b_0^2), && (6.4) \end{aligned}$$

One can then construct the following diagramm.

$$\begin{tikzcd} \mathbb{C}/\mathbb{Z}\omega_1+\mathbb{Z}2\omega_2 \arrow[r, "G:z\mapsto z"] \arrow[d, "u_{2\tau}"', "\simeq"] & \mathbb{C}/\mathbb{Z}\omega_1+\mathbb{Z}\omega_2 \arrow[d, "u_\tau", "\simeq"'] \\ E_{2\tau}(\mathbb{C}) \arrow[r, shift left, "g"] & E_\tau(\mathbb{C}) \arrow[l, shift left, "f"] \end{tikzcd}$$

where $E_{2\tau} = E_{a_1,b_1}$ and f, g are 2-isogenies given by (see for instance [BM89]):

$$\begin{aligned} g : (x_1,y_1) &\mapsto \left(x_1(1+\frac{a_1^2-b_1^2}{x_1-a_1^2}), \frac{y_1(x_1^2-2x_1a_1^2+a_1^2b_1^2)}{(x_1-a_1^2)^2}\right) && (6.5) \\ f : (x_0,y_0) &\mapsto \left(\frac{y_0^2}{4x_0^2}+(\frac{a+b}{2})^2, -\frac{y_0(a^2b^2-x_0^2)}{8x_0^2}\right) && (6.6) \end{aligned}$$

In particular the kernel of f is $< (0,0) >$.
We can now finish the proof: since $G^*(dz) = dz$ we have $g^*(dx_0/y_0) = dx_1/y_1$. Now

$$\omega_1 = 2\int_{e_1}^{\infty}\frac{dx}{y} = 2\int_0^{-\infty}\frac{-i}{2}\frac{dx_0}{y_0} = \int_0^{-\infty}-i\frac{dx_1}{y_1} = \ldots = \int_0^{-\infty}-i\frac{dx_n}{y_n}$$

(the coefficient $i/2$ comes from the isomorphism between E and E_τ). By iteration :

$$E \simeq E_\tau \to E_{2\tau} \to \ldots \to E_{2^n\tau} \to \ldots \to E_\infty : y^2 = x(x - M(a_0, b_0)^2)^2.$$

But E_∞ is a genus 0 curve which means that there exists a parametrization which gives

$$\omega_1 = \int_0^{-\infty} -i\frac{dx}{\sqrt{x(x - M(a_0, b_0)^2)^2}} =$$

$$= \left[-2\frac{\mathrm{Arctan}(\frac{\sqrt{\mathrm{x}}}{\mathrm{M(a_0,b_0)}})}{\mathrm{M(a_0, b_0)}} \right]_0^{-\infty} = \frac{\pi}{\mathrm{M}(a_0, b_0)}.$$

6.1.3 With complex values

One can wonder what happens when τ is not purely imaginary. The problem was already handled by Gauss (see [Cox84]).
Let $a, b \in \mathbb{C}$ such that $b/a \notin \{0, \pm 1\}$ with $|a| \geq |b|$.

6.1.6 Definition. $b_1 = \pm\sqrt{ab}$ is called a *good root* if $|a_1 - b_1| \leq |a_1 + b_1|$ and if $|a_1 - b_1| = |a_1 + b_1|$ one has also $\mathrm{Im}(b_1/a_1) > 0$.
The AGM sequence (a_n, b_n) is called good if b_{n+1} is a good choice of $\sqrt{a_n b_n}$ for all but a finite number of n.

6.1.7 Proposition. *(a_n, b_n) converges to a common non zero limit iff (a_n, b_n) is good.*

One defines then :

6.1.8 Definition. A number μ is called *an arithmetic-geometric mean* of (a, b) if there exists a good sequence converging to μ. We denotes by $\{M(a, b)\}$ the set of these values.
The value obtained by doing always a good choice is called *simple value* and denoted $M(a, b)$.

We have the fundamental result.

6.1.9 Theorem. (Gauss) *Let $\mu = M(a,b)$ and $\lambda = \mathrm{M}(a+b, a-b)$. Then every value $\mu' \in \{\mathrm{M}(a,b)\}$ is given by*

$$\frac{1}{\mu'} = \frac{d}{\mu} + \frac{ic}{\lambda}$$

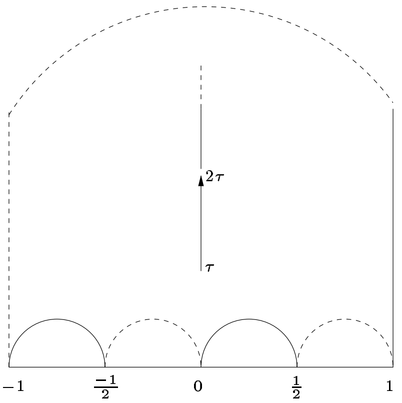
with c, d coprime such that $d \equiv 1 \pmod 4$ and $c \equiv 0 \pmod 4$.

The proof of this theorem introduces naturally the moduli space $\mathbb{H}/\Gamma^2(4)$, where

$$\Gamma^2(4) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid$$
$$a \equiv d \equiv 1 \pmod 4, c \equiv 0 \pmod 4, b \equiv 0 \pmod 2\}.$$

This moduli space parametrizes elliptic curves with a 2 and a 4 torsion points up to isomorphism. The AGM method may be interpreted as a path to the border of this moduli space (which consists of degenerated curves).

Figura 6.2: Fundamental domain for $\Gamma^2(4)$



6.1.10 Remark. *One can show that π/μ and $i\pi/\lambda$ are two independent periods of the curve $E : y^2 = x(x-a^2)(x-b^2)$.*
Recently R. Dupont [Dup04] has used the AGM algorithm in the opposite direction : knowing τ he was able to give a quadratic algorithm

to compute the theta constants. A generalization to the genus 2 case is work in progress.

6.2 2-adic method

Let $q = 2^N$, $k = \mathbb{F}_q$ and $\mathbb{Q}_q$ be the unramified extension of degree N of $\mathbb{Q}_2$, $\mathbb{Z}_q$ its ring of integers, ν its valuation and σ the Frobenius substitution (i.e the unique Galois automorphism of $\mathbb{Q}_q$ such that $\sigma x \equiv x^2 \pmod 2$). We need also a 'good' square root : when $a \in 1 + 8\mathbb{Z}_q$ then there exists a unique $b \in 1 + 4\mathbb{Z}_q$ such that $b^2 = a$. One denotes $b = \sqrt{a}$.

The aim of this section is to give an algorithm which we can present as

$$\tilde{E}/\mathbb{F}_q \text{ ordinary e.c.} \overset{\text{lift}}{\longrightarrow} E/\mathbb{Z}_q \underset{\text{cv}}{\overset{\text{AGM}}{\longrightarrow}}$$
$$\tilde{E}^{\uparrow}/\mathbb{Z}_q \text{ canonical lift} \overset{\text{AGM}}{\longrightarrow} \text{Frobenius trace of } \tilde{E}/\mathbb{F}_q.$$

Recall that the canonical lift of an ordinary elliptic curve $\tilde{E}$ defined over $\mathbb{F}_q$ is the unique (up to isomorphism) elliptic curve $\tilde{E}^{\uparrow}$ defined over $\mathbb{Z}_q$ whose special fibre is isomorphic to $\tilde{E}$ and such that

$$\mathrm{End}_{\mathbb{Q}_q}(\tilde{E}^{\uparrow}) = \mathrm{End}_{\mathbb{F}_q}(\tilde{E}).$$

It is also characterized by the existence of an isogeny

$$\mathrm{Fr}^{\uparrow} \colon \tilde{E}^{\uparrow} \to (\tilde{E}^{\uparrow})^{\sigma}$$

which lifts the relative Frobenius $\mathrm{Fr} : \tilde{E} \to \tilde{E}^{(2)}$.
Let us detail now the different parts.

6.2.1 Lift

In characteristic 0 we want to use the form $E_{a,b} : y^2 = x(x - a^2)(x - b^2)$. Of course we cannot use this model in characteristic 2 but instead a model $y^2 + xy = f(x)$. We propose two different solutions to pass from one to the other.

First solution

6.2.1 Lemma. **([Ver03])** *Let $a, b \in 1 + 4\mathbb{Z}_q$ with $b/a \in 1 + 8\mathbb{Z}_q$. Then*

$$\begin{array}{rcl} E_{a,b} & \overset{\sim}{\to} & E : y^2 + xy = x^3 + rx^2 + sx + t \\ (x, y) & \to & \left(\dfrac{x - ab}{4}, \dfrac{y - x + ab}{8}\right) \end{array}$$

for some $r, s, t \in \mathbb{Z}_q$ such that

$$\tilde{E} : y^2 + xy = x^3 + \left(\frac{a - b}{8}\right).$$

We then consider $\tilde{E}$ as $y^2 + xy = x^3 + c$, let $r \in \mathbb{Z}_q$ such that $r \equiv \sqrt{c} \pmod 2$ and take

$$\begin{cases} a_0 = 1 + 4r \\ b_0 = 1 - 4r \end{cases}$$

The advantage of this model is that there is a rational 4 torsion point $(c^{1/4}, c^{1/2})$. This point enables to find the sign of $\pm\operatorname{tr}(\pi)$ that occurs at the end of the algorithm because $\operatorname{tr}(\pi) \equiv 1 \pmod 4$. The drawback is that this model does not represent all cases. Moreover it gives no clue about a possible generalization to hyperelliptic cases.

Second solution

Starting with a general ordinary elliptic curve $\tilde{E} : y^2 + xy = x^3 + a_2x^2 + a_4x + a_6$, we can always get rid of the a_6 coefficient. We lift then $\tilde{E}$ naturally and make the transformation

$$Y^2 = (y + \frac{x}{2})^2 = x(x^2 + \frac{4a_2 + 1}{4}x + 1).$$

We can factorize the left member over $\mathbb{Q}_q$ in $x(x - \alpha)(x - \beta)$ with $\nu(\alpha) = -2$ and $\nu(\beta) = 2$. Let $X = x - \alpha$ we have then a model

$$Y^2 = X(X + \alpha)(X + \alpha - \beta).$$

As $\nu(\frac{\alpha-\beta}{\alpha}-1)=\nu(\frac{\alpha}{\beta})=4$, we can take

$$\begin{cases} a_0 = 1 \\ b_0 = \sqrt{\frac{\alpha-\beta}{\alpha}} \in 1+8\mathbb{Z}_q \end{cases}$$

and consider the curve

$$Y^2 = X(X-1)(X-b_0^2).$$

Note that this curve is not isomorphic over $\mathbb{Q}_q$ to the original one but is a quadratic twist. However, as we will obtain the trace of the Frobenius only up to a sign, this is not an issue.

6.2.2 Remark. *We have to get rid of the a_6 coefficient, otherwise we might have to factorize the left member in a ramified extension of $\mathbb{Q}_2$ (it is the case for instance with $y^2+xy=x^3+1$).*

6.2.2 Convergence

Let start with a model $E_0 = E_{a_0,b_0}$ over $\mathbb{Z}_q$ lifting $\tilde{E}$. Let denote $E_i = E_{a_i,b_i}$ the elliptic curves obtained by AGM iterations. These curves are well defined because one has at each step : $\sqrt{a_ib_i} = a_i\sqrt{b_i/a_i}$ and $b_i/a_i \in 1+8\mathbb{Z}_q$.
Let denote also $\tilde{E}^{\uparrow}$ the canonical lift of $\tilde{E}$ which is completely characterized by its j-invariant J. We want to prove that the AGM sequence converges to the Galois cycle associated to the canonical lift. We give two proofs.

First proof

We are going to use the following theorem.

6.2.3 Theorem. *[VPV01, §2] Let $x \in \mathbb{Z}_q$ such that $x \equiv J \pmod{2^n}$ for some $n \in \mathbb{N}$. Then there exists a unique $y \in \mathbb{Z}_q$ such that $y \equiv x^2 \pmod 2$ and $\Phi_2(x,y)=0$. Moreover $y \equiv j((\tilde{E}^{(2)})^{\uparrow}) = J^{\sigma} \pmod{2^{n+1}}$.*

Recall that Φ_p is the modular polynomial of order p. If E and E' are two elliptic curves that are p-isogenous then $\Phi_p(j(E),j(E'))=0$.

We have of course $\Phi_2(E_i, E_{i+1}) = 0$ by the complex computations of Section 6.1. An easy computation shows also the following congruence.

6.2.4 Lemma. $j(E_{i+1}) \equiv j(E_i)^2 \pmod 2$.

By iteration of the AGM we then obtain

$$j(E_n) \equiv j((\tilde{E}^{(2^n)})^{\uparrow}) \pmod{2^{n+1}}.$$

Second proof

The second proof uses a result of Carls. It avoids explicit invariants and is then useful for generalization.

6.2.5 Theorem. *[Car04, Th.3] Let A be an ordinary abelian variety over $\mathbb{F}_q$, $\mathcal{A}/\mathbb{Z}_q$ be an abelian scheme with special fiber A. One defines a sequence*

$$\mathcal{A} = \mathcal{A}_0 \to \mathcal{A}_1 \to \dots$$

where the kernel of the isogenies are the componants $\mathcal{A}_i[2]^{loc}$ (i.e the 2-torsion points in the kernel of the reduction). We have

$$\lim_{n \to \infty} \mathcal{A}_{Nn} = A^{\uparrow}$$

i.e. for all n, $(\mathcal{A}_{Nn})/\mathbb{Z}_q^{(Nn+1)} \simeq (A^{\uparrow}_{Nn})/\mathbb{Z}_q^{(Nn+1)}$, where

$$\mathbb{Z}_q^{(i)} = \mathbb{Z}_q/2^i\mathbb{Z}_q \simeq \mathbb{Z}/2^i\mathbb{Z}.$$

In particular the convergence is linear.

Using Section 6.1 we see that if we still denote by $f : E_i \to E_{i+1}$ the 2-isogeny induced by the AGM-iteration, then $\ker f =< (0,0) >$ and $(0,0)$ reduces on $\tilde{O}$ (because the kernel corresponds to the point $(\alpha, 0)$ in the reduction, which is of negative valuation). We can then apply Th.6.2.5.

6.2.3 Trace of the Frobenius

To compute the Frobenius polynomial we only need the trace of the Frobenius on $V_l(\tilde{E})$ for $l \neq 2$. But this trace can be already read on regular differentials. We have the classical proposition.

6.2.6 Proposition. (Satoh) *Let E be an elliptic curve over $\mathbb{Q}_q$ whose special fibre $\tilde{E}$ is smooth and let $f \in \mathrm{End}_{\mathbb{Q}_q}(E)$ be of degree d. Let ω be a regular differential on E and let $f^*(\omega) = c\omega$ be the action of f on $\Omega^1(E)$ then $\mathrm{tr}(f|_{V_l(\tilde{E})}) = c + \frac{d}{c}$.*

In particular if f lifts the Frobenius endomorphism, we have $\chi(X) = X^2 - (c + q/c)X + q$.
We need also the following elementary lemma.

6.2.7 Lemma. *Let $E_{a,b} : y^2 = x(x - a^2)(x - b^2)$ et $E_{a',b'} : y'^2 = x'(x' - a'^2)(x' - b'^2)$ with $\frac{a^2}{b^2} \equiv \frac{a'^2}{b'^2} \equiv 1 \pmod 2$. If E and E' are isomorphic then $x = u^2x'$ and $y = u^3y'$ with $u^2 = \frac{a^2+b^2}{a'^2+b'^2}$. Furthermore $\frac{a^2}{b^2} = \frac{a'^2}{b'^2}$ or $\frac{a^2}{b^2} = \frac{b'^2}{a'^2}$.*

Proof: The two curves being isomorphic, there exists $(u, r) \in (\mathbb{Z}_q^* \times \mathbb{Q}_q)$ such that $x = u^2x' + r$ and $y = u^3y'$. It is enough to show that $r = 0$. With the usual notations of [Sil92, chap.III,1.2], one has

$$\begin{aligned} -4u^2(a'^2 + b'^2) = b_2' &= b_2 + 12r = -4(a^2 + b^2) + 12r \\ 0 = u^6b_6' &= 4r(r - a^2)(r - b^2) \end{aligned}$$

The first equality shows that $r \equiv 0 \pmod 2$ and the second that $r = 0$ since neither a^2 or b^2 are congruent to 0. The first equality gives also the value of u^2. □

Let $\mathcal{E}_{a_0,b_0}$ be the canonical lift. We can then construct the following diagramm

$$\begin{tikzcd}
\mathcal{E}_{a_0^\sigma,b_0^\sigma} \arrow[d, "\phi"'] \arrow[dr, bend left, "\mathrm{Ve}^\uparrow"] & \\
\mathcal{E}_{a_1,b_1} \arrow[r, shift left, "g"] \arrow[d] & \mathcal{E}_{a_0,b_0} \arrow[l, shift left, "f"] \arrow[ul, "\mathrm{Fr}^\uparrow"'] \arrow[d] \\
\tilde{E}^{(2)} & \tilde{E} \arrow[l, "\mathrm{Fr}"]
\end{tikzcd}$$

where ϕ is an isomorphism because the maps $\mathrm{Fr}^\uparrow$ and f have the same kernel $< (0,0) >$. Let $\omega = dx/y$, we then get

$$(\mathrm{Ve}^\uparrow)^*(\omega) = (g \circ \phi)^*(\omega) = \phi^*(\omega) = \frac{\omega}{u}$$

with $u^2 = \frac{a_1^2+b_1^2}{(a_0^2)^\sigma+(b_0^2)^\sigma}$ because g acts by identity as we can see on the explicit formula (6.6) or with the complex interpretation of g as $z \mapsto z$.

We want to simplify a bit the expression of u^2. we have

$$u^2 = \left(\frac{a_1}{a_0^\sigma}\right)^2 \frac{1+\left(\frac{b_1}{a_1}\right)^2}{1+\left(\frac{b_0^\sigma}{a_0^\sigma}\right)^2}.$$

Let $\lambda_1 = b_1/a_1$ and $\lambda_0 = b_0/a_0$. By Lem.6.2.7, $\lambda_1^2 = (\lambda_0^2)^\sigma$ or $\lambda_1^2 = \frac{1}{(\lambda_0^2)^\sigma}$. Let us prove that it is the first case which occurs. We can write $\lambda_i = 1 + 8c_i$ with $c_i \in \mathbb{Z}_q$ so the first case occurs iff

$$c_1 \equiv c_0^\sigma \pmod 4.$$

By the AGM iteration, we have

$$1 + 8c_1 = \frac{1+4c_0}{\sqrt{1+8c_0}} \Rightarrow c_1 \equiv c_0^2 \pmod 4.$$

As after the first iteration c_0 is itself a square α_0^2 modulo 4, we have

$$c_0^\sigma \equiv (\alpha_0^2)^\sigma \equiv \alpha_0^4 \equiv c_0^2 \pmod 4.$$

So we get $c_1 \equiv c_0^\sigma \pmod 4$ which proves

$$u = \pm \frac{a_1}{a_0^\sigma}.$$

The trace of the Frobenius endomorphism is the same as the trace of the Verschiebung. One has

$$\operatorname{tr}(\pi|_{V_l(\tilde{E})}) = \operatorname{tr}(V|_{V_l(\tilde{E})}) = \operatorname{tr}(\mathrm{Ve}^{\sigma^{N-1}} \circ \cdots \circ \mathrm{Ve}) = \\ = \pm\left(\frac{1}{N(u)} + 2^N \cdot N(u)\right)$$

with

$$N(u) = \mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\frac{a_1}{a_0}\right).$$

6.2.4 Complexity and Conclusion

Since by the Hasse-Weil theorem $\operatorname{tr}(\pi) \leq 2\sqrt{q}$ it is enough to compute the previous norm with $\lceil N/2 \rceil + 2$ bits. In the general case, one solves the final sign problem by computing the action of the Frobenius endomorphism on 4-torsion points.
Several implementations of this method have been achieved : see [Ver03] for a nice overview and running times. The best complexity obtained is quasi-quadratic in time and quadratic in space.

One of the attractive aspect of the AGM method is the simplicity of the formulas involved. Another one is the natural generalizations one can obtain for hyperelliptic curves and non hyperelliptic curves of genus 3. However, compared to cohomological methods or Lauder deformation theory which are polynomial in the genus, it seems that the AGM methods are exponential and then unefficient for high genus.

C. Ritzenthaler
Institut de Mathématiques de Luminy, UMR 6206
163 avenue de Luminy case 907
Marseille 13288, France ritzenth@iml.univ-mrs.fr

Capítol 7

AGM method for plane quartics in characteristic 2

Enric Nart

This is a brief overview of [Rit03] and [Rit04], where the AGM method for plane quartics in characteristic 2 is developed in full detail and implemented.

7.1 Overview of the algorithm

Let $k = \mathbb{F}_q$ be a finite field of even characteristic, with $q = 2^N$. Let $C \subseteq \mathbb{P}^2$ be a smooth plane quartic, defined over k, such that:

1. $\operatorname{Jac}(C)$ is ordinary and simple,
2. $\operatorname{Jac}(C)[2] \subseteq \operatorname{Jac}(C)(k)$.

The first condition is essential for the AGM method to work. The second condition is introduced for computational reasons. Our aim is to compute the zeta function of C over k, or, equivalently, the characteristic polynomial of the endomorphism of Frobenius in $\operatorname{Jac}(C)$:

$$f_C(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + qa_2x^2 + q^2a_1x + q^3.$$

Actually the main interest lies on cryptographic applications where only $|\operatorname{Jac}(C)(k)| = f_C(1)$ is needed.

STEP 1.

Let $K := \mathbb{Q}_q$ be the unramified extension of $\mathbb{Q}_2$ of degree N. The AGM method is inspired in Satoh's idea: *consider the canonical lift of* Jac(C) *and compute the action of the lifting of Frobenius on differentials.* However, the AGM method doesn't need to look for the canonical lift. Actually *any* lift of C works.

Thus, STEP 1 consists just in lifting C/k to a smooth plane quartic $\mathcal{C}/K$ given by a Riemann model, and having all bitangents defined over K.

The assumption on the bitangents of $\mathcal{C}$ has just a computational purpose. However, in order to get a good Riemann model of $\mathcal{C}$ some work has to be done: one has to consider $\mathcal{C}$ as a quotient of a lift of an adequate 2-cover of C [Rit04, section 3]. Moreover, an Aronhold system of $\mathcal{C}$ is distinguished and normalised after a proper linear transformation.

STEP 2. Compute the $8\,(=2^g)$ "right" initial theta constants:

$$\theta_\epsilon^{(0)} \in K, \qquad \forall \epsilon \in (\mathbb{Z}/2\mathbb{Z})^3,$$

and apply AGM iteration:

$$\theta_\epsilon^{(i+1)} = \frac{1}{8} \sum_{\delta \in (\mathbb{Z}/2\mathbb{Z})^3} \sqrt{\theta_\delta^{(i)} \theta_{\delta+\epsilon}^{(i)}}, \qquad \forall \epsilon \in (\mathbb{Z}/2\mathbb{Z})^3.$$

By the Main Theorem of AGM:

$$\lim_{n \to \infty} \frac{\theta_\epsilon^{(n)}}{\theta_\epsilon^{(n+N)}} = \pm \pi_1 \pi_2 \pi_3, \tag{7.1}$$

for every $\epsilon \in (\mathbb{Z}/2\mathbb{Z})^3$, where π_1, π_2, π_3 are the roots of $f_C(x)$ that are 2-adic units.

Remarks on STEP 2.

1. There are very fast algorithms to take square roots in 2-adic fields, based on Newton iteration. However, there is an ambiguity of sign and the right sign is needed in order to get the convergence of the Main Theorem. This is achieved by a convention similar to the one taken for $\mathbb{R}$:

   $$x \in 1 + 8\mathbb{Z}_q \implies \sqrt{x} \text{ uniquely determined by } \sqrt{x} \in 1 + 4\mathbb{Z}_q.$$

   In particular,

   $$\frac{a}{b} \in 1 + 8\mathbb{Z}_q \implies \sqrt{ab} := b\sqrt{\frac{a}{b}} \text{ is uniquely determined.}$$

   All quotients of our initial theta constants satisfy this property, and this property is preserved by AGM iteration.

2. The Main Theorem is true for any ordinary C of arbitrary genus. Only the computation of the initial theta constants requires specific methods for specific families of curves. For genus 3 non-hyperelliptic curves we shall discuss the computation of the initial theta constants in the next section.

3. The convergence of the limit is linear. Every term

   $$\alpha_n := \frac{\theta_\epsilon^{(n)}}{\theta_\epsilon^{(n+N)}}$$

   is an approximation to the limit $\alpha \in \mathbb{Z}_2$ with precision $n+1$ (in 2-adic digits).

STEP 3. The 2-adic number $\beta := \alpha + \frac{q^3}{\alpha}$ is algebraic of degree 3 (rarely) or 4 (generically) over $\mathbb{Z}$.

By an algorithm of type LLL or "shortest vector", one finds the minimal polynomial $P_{sym}(x)$ of β over $\mathbb{Z}$. From this polynomial one recovers easily $f_C(\pm x)$. The algorithm is very fast, but one needs to know β with precision $10N$ bits.

The ambiguity of sign is solved by computing $|\operatorname{Jac}(C)(k)|\, D$ for a random divisor D.

The total complexity of the algorithm is $O(N^{2\mu}\log N)$ bit operations, where N^μ is the number of bit operations of the multiplication of two N-bit integers. Thus, $\mu = 2$ for standard polynomial multiplication, $\mu = \log_2 3 \sim 1.585$ with Karatsuba multiplication, and $\mu = 1+\epsilon$ with FFT. For cryptographic sizes Karatsuba multiplication provides the best performance.

7.2 Choice of the initial theta constants

Let $\sigma\colon K \longrightarrow K$ be the Frobenius substitution. Let A be an ordinary abelian variety of dimension g, principally polarized over k (think of $\operatorname{Jac}(C)$), and let $A^\uparrow$ be its canonical lift to K, canonically principally polarized over K. Recall that:

$$A \simeq A^\uparrow \pmod 2, \qquad \operatorname{End}_K(A^\uparrow) \underset{\sim}{\rightarrow} \operatorname{End}_k(A).$$

In particular, we have liftings of Frobenius and Verschiebung. By the functoriality of the canonical lift, we have also liftings of the small Frobenius Fr and the small Verschiebung Ve:

$$\begin{tikzcd} A^\uparrow \arrow[r, "\hat{f}"] \arrow[d] & (A^\uparrow)^\sigma \arrow[d] \\ A \arrow[r, "\mathrm{Fr}"] & A^{(1)} \end{tikzcd} \qquad \begin{tikzcd} (A^\uparrow)^\sigma \arrow[r, "f"] \arrow[d] & A^\uparrow \arrow[d] \\ A^{(1)} \arrow[r, "\mathrm{Ve}"] & A \end{tikzcd}$$

where the vertical arrows are reduction maps.

Let us recall some facts concerning these objects.

- $A[2] \subseteq A(k) \implies A^\uparrow[2] \subseteq A^\uparrow(K)$
- We have a decomposition as group schemes over k:

  $$A[2] = A[2]^{\mathrm{loc}} \times A[2]^{\mathrm{et}},$$

  where $A[2]^{\mathrm{loc}} = \operatorname{Ker}(\mathrm{Fr})$ and $A[2]^{\mathrm{et}} = \operatorname{Ker}(\mathrm{Ve})$.

- Although the lifts are in characteristic zero, we use the same notation:
$$A^{\uparrow}[2] = A^{\uparrow}[2]^{\mathrm{loc}} \times A^{\uparrow}[2]^{\mathrm{et}},$$
these subgroup schemes being determined by:
$$\mathrm{red}\colon A^{\uparrow}[2]^{\mathrm{et}} \xrightarrow[\sim]{} A[2]^{\mathrm{et}}, \qquad A^{\uparrow}[2]^{\mathrm{loc}} = \mathrm{Ker}(A^{\uparrow}[2] \xrightarrow{\mathrm{red}} A[2]).$$

- $A^{\uparrow}[2]^{\mathrm{loc}}$ and $A^{\uparrow}[2]^{\mathrm{et}}$ are maximal isotropic spaces with respect to the Weil pairing.

- f is an isogeny of degree 2^g with kernel $A^{\uparrow}[2]^{\mathrm{et}}$.
  $\hat{f}$ is an isogeny of degree 2^g with kernel $A^{\uparrow}[2]^{\mathrm{loc}}$.

Following Satoh, we can consider the following diagram:

$$\begin{tikzcd}
 & A^{\uparrow}_N \arrow[r, "\hat{\mathrm{can}}"] \arrow[d, "\mu"'] & \cdots\cdots & A^{\uparrow}_2 \arrow[r, "\hat{\mathrm{can}}"] \arrow[d] & A^{\uparrow}_1 \arrow[r, "\hat{\mathrm{can}}"] \arrow[d] & A^{\uparrow} \arrow[d, equal] \\
V^{\uparrow}\colon A^{\uparrow} = & (A^{\uparrow})^{\sigma^N} \arrow[r, "f"] \arrow[d] & \cdots\cdots & (A^{\uparrow})^{\sigma^2} \arrow[r, "f"] \arrow[d] & (A^{\uparrow})^{\sigma} \arrow[r, "f"] \arrow[d] & A^{\uparrow} \arrow[d] \\
V\colon A = & A^{(N)} \arrow[r, "\mathrm{Ve}"] & \cdots\cdots & A^{(2)} \arrow[r, "\mathrm{Ve}"] & A^{(1)} \arrow[r, "\mathrm{Ve}"] & A
\end{tikzcd}$$

We have denoted:
$$A^{\uparrow}_0 := A^{\uparrow}, \qquad A^{\uparrow}_{i+1} = A^{\uparrow}_i / A^{\uparrow}_i[2]^{\mathrm{loc}},$$
and $\hat{\mathrm{can}}$ is the dual of the canonical projection $A^{\uparrow}_i \xrightarrow{\mathrm{can}} A^{\uparrow}_{i+1}$.

The vertical maps in the first row are all K-isomorphisms because $\mathrm{Ker}(\hat{f}) = A^{\uparrow}[2]^{\mathrm{loc}}$. The vertical maps in the second row are reduction maps; hence, in the lower rectangle we find the Verschiebung map V and its lifting $V^{\uparrow}$ to K.

The philosophy is that the action of $V^{\uparrow}$ on differentials determines $f_C(x)$. Now, the action of $\hat{\mathrm{can}}$ on differentials is essentially trivial, so that the crutial point is to compute the action of μ on differentials.

To do this, we use the existence of a model of $A^{\uparrow}$ defined over $\overline{\mathbb{Q}}$; this allows us to consider the principally polarized abelian variety over $\mathbb{C}$:

$$A^{\uparrow}_{\mathbb{C}} := A^{\uparrow} \otimes_{\overline{\mathbb{Q}}} \mathbb{C}.$$

The symplectic space on $H^1(A^{\uparrow}_{\mathbb{C}}, \mathbb{Z})$ determined by the canonical alternating Riemann form is isomorphic to the symplectic space on $A^{\uparrow}_{\mathbb{C}}[2]$ determined by the Weil pairing. We take a symplectic basis $x_1, \dots, x_g; y_1, \dots, y_g$ such that

$$\frac{1}{2}\langle\, x_1, \dots, x_g \,\rangle = A^{\uparrow}_{\mathbb{C}}[2]^{\mathrm{loc}}.$$

Working in coordinates with respect to this basis we have $A^{\uparrow}_{\mathbb{C}} \simeq \mathbb{C}^g/(I|\Omega)$ and

$$\begin{tikzcd}
(A^{\uparrow}_1)_{\mathbb{C}} \arrow[r, "\hat{\mathrm{can}}"] \arrow[d, equal] & A^{\uparrow}_{\mathbb{C}} \arrow[d, equal] \\
\mathbb{C}^g/(I|2\Omega) \arrow[r] & \mathbb{C}^g/(I|\Omega)
\end{tikzcd}$$

where the lower map is the canonical projection $z \mapsto z$ (we see here the trivial action of $\hat{\mathrm{can}}$ on differentials). Therefore,

$$\mu_{\mathbb{C}} \colon (A^{\uparrow}_N)_{\mathbb{C}} = \mathbb{C}^g/(I|2^N\Omega) \xrightarrow[\sim]{} A^{\uparrow}_{\mathbb{C}} = \mathbb{C}^g/(I|\Omega)$$

has a special shape leading to:

$$\theta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (0,\Omega)^2 = \pm\pi_1\pi_2\cdots\pi_g\, \theta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (0, 2^N\Omega)^2,$$

for any characteristic $\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$. We can use now the duplication formula

$$\theta \begin{bmatrix} 0 \\ \epsilon \end{bmatrix} (0,2\Omega)^2 = \frac{1}{2g} \sum_{\delta\in(\mathbb{Z}/2\mathbb{Z})^g} \theta \begin{bmatrix} 0 \\ \delta \end{bmatrix} (0,\Omega)\theta \begin{bmatrix} 0 \\ \delta+\epsilon \end{bmatrix} (0,\Omega).$$

Thus, defining

$$\theta^{(i)}_{\epsilon} := \left(\frac{\theta \begin{bmatrix} 0 \\ \epsilon \end{bmatrix} (0, 2^i\Omega)}{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (0,\Omega)} \right)^2,$$

we see that AGM iteration applied to the family $(\theta_\epsilon^{(i)})_{\epsilon\in(\mathbb{Z}/2\mathbb{Z})^g}$ furnishes the family $(\theta_\epsilon^{(i+1)})_{\epsilon\in(\mathbb{Z}/2\mathbb{Z})^g}$ and

$$\frac{\theta_\epsilon^{(0)}}{\theta_\epsilon^{(N)}} = \pm\pi_1\pi_2\cdots\pi_g, \quad \forall\epsilon\in(\mathbb{Z}/2\mathbb{Z})^g. \tag{7.2}$$

All these facts are true only for the canonical lift. However, there exists a formula of Weber computing $\theta_\epsilon^{(0)}$ for any plane quartic given by a Riemann model, in terms of a suitable normalization of the bitangents [Rit04, Thm. 3]. One can apply the very same formula to the lift $\mathcal{C}/K$ of our initial plane quartic. For the values $\theta_\epsilon^{(0)}\in K$ obtained in this way, the formula (7.2) is not true anymore, since the Jacobian of $\mathcal{C}$ is not the canonical lift of the Jacobian of C. Nevertheless, (7.1) holds by Carls' theorem (cf. 6.2.5 of the previous chapter), so that we need only to perform more AGM iterations till we get the desired approximation of $\pm\pi_1\pi_2\pi_3$.

E. Nart
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
nart@mat.uab.es

Bibliografia

[ACGH85] E. Arbarello, M. Corbalba, P.A. Griffiths, J. Harris, *Geometry of Algebraic Curves, Vol. I*, Grundlehren der mathematischen Wissenschaften 267, Springer-Verlag 1985.

[BG03] P. Bàyer, J. Guàrdia, *Funcions theta*, Notes del STNB 10, Barcelona 2003.

[Bau03] M. Bauer, *The arithmetic of certain cubic function fields*, Mathematics of Computation, to appear.

[BTW04] M. Bauer, E. Teske, A. Weng, *Point counting on Picard curves in large characteristic*, preprint, Faculty of Mathematics - Waterloo, 2004.

[BM89] J.-B. Bost, J.-F. Mestre, *Moyenne Arithmético-géométrique et Périodes des courbes de genre* 1 *et* 2, Gaz. Math., S.M.F. **38** (1989), 36-64.

[BGS] A. Bostan, P. Gaudry, E. Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, preprint, 2003.

[Bou00] I. Bouw, *The p-rank of curves and covers of curves*, in *Courbes semi-stables et groupe fondamental en géometrie algèbrique (Luminy, 1998)*, number 187 in Progr. Math., pages 267–277, Basel, 2000.

[Bre00] Th. Breuer, *Characters and automorphism groups of compact Riemann surfaces*, London Mathematical Society Lecture Note Series, 280. Cambridge University Press, 2000.

[CS03] L. Caporaso, E. Sernesi, *Recovering plane curves from their bitangents*, J. Alg. Geom. 12(2003), no 2, 225-244.

[Car06] G. Cardona, *La quàrtica de Klein*, capítol 3 d'aquest volum.

[Car04] R. Carls, *A generalization of the Arithmetic-Geometric Mean*, PhD thesis, University of Groningen, 2004.

[Cox84] D. Cox, *The arithmetic-geometric mean of Gauss*, Enseign. Math. **30** (1984), 275-330.

[DH76] W. Diffie, M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, 22(1976), 644–654.

[Dol06] I. Dolgachev, *Topics in Classical Algebraic Geometry, I*, Lecture Notes, http://www.math.lsa.umich.edu/~idolga/

[Dup04] R. Dupont, *Fast evaluation of modular functions using Newton iterations and the AGM*, work in progress, 2004.

[ELW] K. Eisenträger, K. Lauter, A. Weng, *The ℓ-torsion points on the Jacobian of a Picard curve*, In preparation.

[Elk99] N.D. Elkies, *The Klein quartic in number theory*, The eightfold way, pp. 51–101, MSRI Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[Est91] J. Estrada Sarlabous, *On the Jacobian varieties of Picard curves defined over fields of characteristic $p > 0$*, Math. Nachr., 152(1991), 392–340.

[Est95] J. Estrada, *A finiteness theorem for Picard curves with good reduction*, apèndix a [Hol95].

[ERP99] J. Estrada, E. Reinaldo, J.A. Piñeiro, *On the Jacobian varieties of Picard curves: explicit addition law and algebraic structure*, Math. Nachr. 208(1999), 149-166.

[ERCH01] J. Estrada, E. Reinaldo, J.-P. Cherdieu, R.-P. Holzapfel, *The emergence of Picard Jacobian in cryptography*, Fourth Italian-Latin American Conference on Applied and Industrial Mathematics (La Habana, 2001), 266-275, Inst. Cybern. Math. Phys., La Habana, 2001.

[FK80] H.M. Farkas, I. Kra, *Riemann Surfaces*, GTM 71, Springer, (1980).

[FO] S. Flon, R. Oyono, *Fast arithmetic on Jacobians on Picard curves*, Preprint, 2003.

[FOR] S. Flon, R. Oyono, C. Ritzenthaler, *Fast addition on non-hyperelliptic genus* 3 *curves*, Preprint, 2004.

[Ful69] W. Fulton, *Algebraic Curves, an introduction to Algebraic Geometry*, Math. Lecture Note Series, W. A. Benjamin, 1969

[GG02] P. Gaudry, N. Gurel, *Counting points in medium characteristic using Kedlaya's algorithm*, Preprint, 2003.

[Gau70] C.F. Gauss, *Werke*, Vol. **12**, Göttingen, (1870-1927).

[GH78] P. Griffiths, J. Harris, *Principles of algebraic geometry*, Wiley-Interscience [John Wiley & sons], New York, 1978.

[Gua02] J. Guàrdia, *Jacobian nullwerte and algebraic equations*, J. Algebra 253(2002), no. 1, 112-132.

[GL00] J. Guàrdia, J.-C. Lario, *Varietats abelianes amb multiplicació complexa*, Notes del STNB 6, Barcelona, 2000.

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer-Verlag, Berlin-Heidelberg, 1977.

[Hen76] P. Henn, *Die Automorphismengruppen der algebraischen Funktionenkorper vom Geschlecht 3*, Inagural-Dissertation, Heidelberg, 1976.

[Hol95] R.-P. Holzapfel, *The ball and some Hilbert problems*, Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 1995.

[KW04] K. Koike, A. Weng, *Construction of CM Picard curves*, Math. of Comp. 74(2004), 499-518.

[KK77] A. Kuribayashi, K. Komiya, *On Weierstrass points of non-hyperelliptic compact Riemann surfaces of genus three*, Hiroshima Math. J. 7 (1977), 743-786.

[KK79] A. Kuribayashi, K. Komiya, *On Weierstrass points and automorphisms of curves of genus three*, Algebraic geometry (Proc. Summer Meeting, Copenhagen 1978), LNM 732, 253-299, Springer (1979).

[KL81] D.S. Kubert, S. Lang, *Modular units.* Grundlehren der Mathematischen Wissenschaften **244**, Springer-Verlag, 1981.

[Lag67] J.L. Lagrange, *Oeuvres*, Vol. **14**, Gauthiers-Villars, Paris (1867-1892).

[Leh05] D. Lehavi, *Any smooth plane quartic can be reconstructed from its bitangents*, http://www.math.ohio-state.edu/~dlehavi/

[Lig77] G. Ligozat, *Courbes modulaires de niveau* 11, in *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pp. 149–237. Lecture Notes in Math **601**, Springer, 1977.

[Man65] Ju. I. Manin, *The Hasse-Witt-matrix of an algebraic curve*, Trans. Amer. Math. Soc, 45(1965), 245.

[Maz77] B. Mazur, *Rational points on modular curves*, in *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pp. 107–148. Lecture Notes in Math **601**, Springer, 1977.

[Maz98] B. Mazur, *Open problems regarding rational points on curves and varieties*, in *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, pp. 239–265. London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, 1998.

[MSSV05] K. Magaard, T. Shaska, S. Shpectorov, H. Völklein, *The locus of curves with prescribed automorphism group*, http://www.math.uiuc.edu/Algebraic-Number-Theory/0352/.

[Mes02] J.-F. Mestre, *Algorithmes pour compter des points en petite caractéristique en genre* 1 *et* 2, available on `www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps` (2002).

[Mil86] J.-S. Milne, *Jacobian varieties*, in [CS03], pàgs. 167-212.

[Nar06] E. Nart, *Bitangents and theta characteristics of plane quartics*, capítol 1 d'aquest volum.

[PH78] S. C. Pohlig, M. E. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE-Transactions on Information Theory, 24(1978), 106–110.

[Pol78] J. M. Pollard, *Monte Carlo methods for index computation* $\pmod p$, Mathematics of Computation, 32(143)(1978), 918–924.

[Rit03] C. Ritzenthaler, *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*, PhD thesis, Université Paris 7 - Denis Diderot, June 2003 available on `http://www.math.jussieu.fr/~ritzenth`.

[Rit04] C. Ritzenthaler, *Point counting on genus 3 non hyperelliptic curves*, Algorithmic Number Theory 6th International Symposium, ANTS VI, University of Vermont 13-18 June 2004, Proceedings.

[Roh97] D. E. Rohrlich, *Modular curves, Hecke correspondence, and L-functions*, in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pp. 41–100, Springer, 1997.

[Ros86] M. Rosen, *Abelian varieties over* $\mathbb{C}$, in *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag, (1986).

[Sat00] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15**, (2000), 247-270.

[ST05] T. Shaska, J.L. Thompson, *On the generic curve of genus 3*, http://www.webpages.uidaho.edu/ tshaska/papers/genus3.pdf

[Sch01] R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, Journal de Théorie des Nombres de Bordeaux, 13(2001), 609–631.

[SS] R. Scheidler, A. Stein, *Explicit bounds for Class Numbers of Cubic Curves*, In Preparation.

[Shi71] G. Shimura, G. *Introduction to the arithmetic theory of automorphic functions*, Kano Memorial Lectures, no. 1, Publications of the Mathematical Society of Japan **11**. Iwanami Shoten, Publishers, 1971.

[Sil92] J.H Silverman, *The Arithmetic of Elliptic Curves*, **106**, Springer, 1992.

[Sti93] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math., 2(1966), 134–144.

[Thé] N. Thériault, *Index calculus attack for hyperelliptic curves of small genus*, Preprint, 2003.

[vOW99] P. C. van Oorschot, M. J. Wiener, *Parallel collision search with cryptanalytic applications*, Journal of Cryptology, 12(1999), 1–28.

[Ver03] F. Vercauteren *computing Zeta functions of curves over finite fields*, PhD thesis, Katholicke Universiteit Leuven, 2003.

[VPV01] F. Vercauteren, B. Preneel & J. Vandewalle, *A memory efficient version of Satoh's algorithm*, Adv. in Cryptology, Eurocrypt 2001 (Innsbruck, Austria, Mai 2001), Lect. Notes in Comput. Sci. **2045**, 1-13, ed. Pfitzmann, Berlin, Heidelberg: Springer-Verlag, 2001.

[Ver83] A.M. Vermeulen, *Weierstrass points of weigth two on curves of genus three*, Amsterdam University thesis, 1983.

[Wat69] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4), 2(1969), 521–560.

[Xar05] X. Xarles, *Introducció als dibuixos d'infants*, in Dibuixos d'Infants, Notes del STNB 12, pp.17-32, Barcelona 2005.