Addition in the Jacobian of non-hyperelliptic genus 3 curves and rationality of the intersection points of a line with a plane quartic

Stéphane Flon, Roger Oyono, Christophe Ritzenthaler

C. Ritzenthaler, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail : ritzenth@iml.univ-mrs.fr
web : http ://iml.univ-mrs.fr/∼ritzenth/

General setting

Non-hyperelliptic genus 3 curves = smooth plane quartics.

Choice of a good divisor at infinity $\rightsquigarrow$ condition $(*)$: There is a rational line l^∞ which crosses the quartic C in four k-points $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$. Let $D^\infty = P_1^\infty + P_2^\infty + P_3^\infty$.

Because $\mathrm{Sym}^3 C \to \mathrm{Jac}(C)$, $D^+ \mapsto D^+ - D^\infty$ is surjective, a element $D \in \mathrm{Jac}(C)$ is a sum of three points called D^+.

Question : how do we compute (efficiently) $D_1 + D_2$ in terms of D_1^+, D_2^+ ?

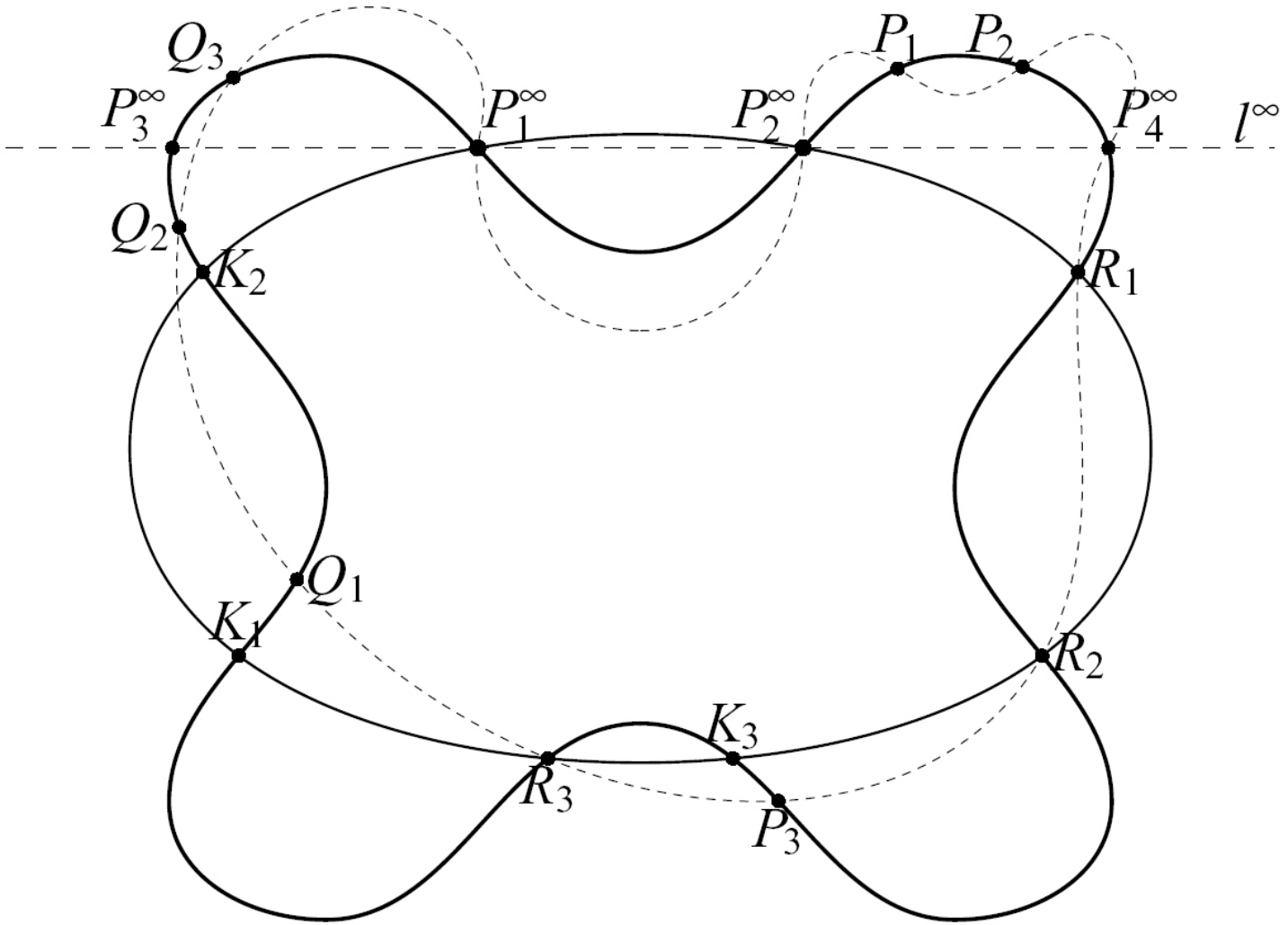
A geometric addition algorithm

Let $D_1, D_2 \in \mathrm{Jac}(C)(k)$. Then $D_1 + D_2$ is equivalent to a divisor $D = D^+ - D^\infty$, where the points in the support of D^+ are given by the following algorithm :

1. Take a cubic E which goes (with multiplicity) through the support of D_1^+, D_2^+ and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.
2. Take a conic Q which goes through the support of D_3 and P_1^∞, P_2^∞. This conic also crosses C in the residual effective divisor D^+.

Why ? Because $(I^\infty \cdot C) \sim \kappa$, $(Q \cdot C) \sim 2\kappa$ and $(E \cdot C) \sim 3\kappa$.

A chord construction



Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x)$$

with $\deg(f_4) \leq 4$ and

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x)$$

with $\deg(f_4) \leq 4$ and

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case) ;

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x)$$

with $\deg(f_4) \leq 4$ and

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case) ;
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case). If $\mathrm{char}(k) \neq 3$ we can write $C : y^3 + h_2(x)y = f_4(x)$.

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x)$$

with $\deg(f_4) \leq 4$ and

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case) ;
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case). If $\mathrm{char}(k) \neq 3$ we can write $C : y^3 + h_2(x)y = f_4(x)$.
3. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 2$ if $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (hyperflex case). These curves are the $C_{3,4}$-curves.

Special forms of the curve

C admits an equation of the form

$$C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x)$$

with $\deg(f_4) \leq 4$ and

1. $\deg(h_1) \leq 2$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty$ (tangent case) ;
2. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 3$ if $P_1^\infty = P_2^\infty = P_4^\infty$ (flex case). If $\mathrm{char}(k) \neq 3$ we can write $C : y^3 + h_2(x)y = f_4(x)$.
3. $\deg(h_1) \leq 1$ and $\deg(h_2) \leq 2$ if $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (hyperflex case). These curves are the $C_{3,4}$-curves.
4. If $\mathrm{char}(k) \neq 3$, $C : y^3 = f_4(x)$ (Picard curves) iif P_1^∞ is a rational Galois point.

$\rightsquigarrow$: the more special, the better.

Some complexities

In the case $\mathrm{char}(k) > 5$ and C has a model $y^3 + h_2(x)y = f_4(x)$ with $\deg(h_2) \leq 3$.

Operation		hyperelliptic of genus 3	$C_{3,4}$ Picard	$C_{3,4}$ $\deg(h_2) = 1$	$C_{3,4}$ $\deg(h_2) = 2$	'generic' quartic $\deg(h_2) = 3$
Our	Add		2I+130M	2I+138M	2I+145M	2I+163M
Methods	Dbl		2I+152M	2I+160M	2I+167M	2I+185M
Previous	Add	I+70M [GMACT]	2I+140M [BEFG]	2I+147M [BEFG]	2I+117M [SM], 2I+150M [BEFG]	
Work	Dbl	I+71M [GMACT]	2I+164M [BEFG]	2I+171M [BEFG]	2I+129 M [SM], 2I+174M [BEFG]	

Remarks :

- Salem and Makdisi work with a good choice of Riemann-Roch spaces.
- Basiri, Enge, Faugère and Gürel work with ideals in function fields.
- Others (Blache, Cherdieu, Sarlabous,...) work on the more general problem of reduction and give only asymptotics.

Study of the condition $(*)$ over $\mathbb{F}_q$

1. A rational hyperflex. Quartics with a hyperflex form a sub-variety of codimension 1. But generically, if there is a hyperflex, it is rational.

Study of the condition $(*)$ over $\mathbb{F}_q$

1. A rational hyperflex. Quartics with a hyperflex form a sub-variety of codimension 1. But generically, if there is a hyperflex, it is rational.
2. A rational flex. When $\mathrm{char}(k) > 3$, smooth plane quartics have 24 flexes counted with multiplicities. Heuristics and computations seem to show that the probability that C has at least one rational flex is asymptotically ($q \mapsto \infty$) about 0.63 (probability that a degree 24 polynomial has at least one root).
   This seems true even in characteristic 2 and 3.

Study of the condition $(*)$ over $\mathbb{F}_q$

1. A rational hyperflex. Quartics with a hyperflex form a sub-variety of codimension 1. But generically, if there is a hyperflex, it is rational.
2. A rational flex. When $\mathrm{char}(k) > 3$, smooth plane quartics have 24 flexes counted with multiplicities. Heuristics and computations seem to show that the probability that C has at least one rational flex is asymptotically ($q \mapsto \infty$) about 0.63 (probability that a degree 24 polynomial has at least one root).
   This seems true even in characteristic 2 and 3.

Caution : in char. $2, 3$ the computations of the flexes cannot be done with the ordinary Hessian (which is zero) $\rightsquigarrow$ find a good substitute.

The generic case

Follow an idea of Diem-Thomé.

1. Let $P \in C(k)$. Consider the separable geometric cover $\phi : C \to |\kappa - P| = \mathbb{P}^1$ of degree 3 induced by the linear system $|\kappa - P|$.

The generic case

Follow an idea of Diem-Thomé.

1. Let $P \in C(k)$. Consider the separable geometric cover $\phi : C \longrightarrow |\kappa - P| = \mathbb{P}^1$ of degree 3 induced by the linear system $|\kappa - P|$.
2. Using effective Chebotarev's density theorem for function fields, one gets estimation on the number of completely split divisors in $|\kappa - P|$.

The generic case

Follow an idea of Diem-Thomé.

1. Let $P \in C(k)$. Consider the separable geometric cover $\phi : C \to |\kappa - P| = \mathbb{P}^1$ of degree 3 induced by the linear system $|\kappa - P|$.
2. Using effective Chebotarev's density theorem for function fields, one gets estimation on the number of completely split divisors in $|\kappa - P|$.

Theorem

If $q \geq 127$, there is always a line satisfying $(*)$.

Remark : The number of Galois points (i.e. P such that ϕ is Galois) is at most 4 if $\mathrm{char}(k) \neq 3$ and 28 if $\mathrm{char}(k) = 3$.

The tangent case

Let $T : C \to \mathrm{Sym}^2(C)$, $p \mapsto T_p(C) \cdot C - 2p$ be the tangential correspondence. We associate to it its correspondence curve

$$X = \{(p, q) \in C \times C : q \in T(p)\}$$

which is defined over k. Let $\phi : X \to C$ be the first projection.

We want to prove that there is a rational point on X when q is big enough.

The tangent case

Let $T : C \to \mathrm{Sym}^2(C)$, $p \mapsto T_p(C) \cdot C - 2p$ be the tangential correspondence. We associate to it its correspondence curve

$$X = \{(p, q) \in C \times C : q \in T(p)\}$$

which is defined over k. Let $\phi : X \to C$ be the first projection.

We want to prove that there is a rational point on X when q is big enough.

Proposition (Aubry, Perret)

Let X defined over $\mathbb{F}_q$ be a geometrically irreducible curve of arithmetic genus π_X. Then

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2\pi_X\sqrt{q}.$$

In particular if $q \geq (2\pi_X)^2$ then X has a rational point.

Question : How to show that X is absolutely irreducible (+ estimate π_X) ?

The tangent case (continued)

Lemma

Let $\phi : X \to Y$ be a separable morphism of degree 2 between two projective curves over k such that

- *Y is smooth and abs. irreducible;*
- *There exists a point $P_0 \in Y$ such that ϕ is ramified at P_0 and $\phi^{-1}(P_0)$ is not singular.*

Then X is abs. irreducible.

The tangent case (continued)

Lemma

Let $\phi : X \to Y$ be a separable morphism of degree 2 between two projective curves over k such that

- *Y is smooth and abs. irreducible ;*
- *There exists a point $P_0 \in Y$ such that ϕ is ramified at P_0 and $\phi^{-1}(P_0)$ is not singular.*

Then X is abs. irreducible.

Proposition

we have the following properties :

1. *the ramification points of ϕ are the bitangence points.*
2. *If $char(k) \neq 2$, the only possible singular points of X are the points (P, P) where P is a hyperflex of C.*

The tangent case (end)

Lemma

Suppose $char(k) \neq 2$. There is always a bitangence point which is not a hyperflex except if $char(k) = 3$ and C is geometrically isomorphic to the Fermat quartic $x^4 + y^4 + z^4 = 0$.

The tangent case (end)

Lemma

Suppose $char(k) \neq 2$. There is always a bitangence point which is not a hyperflex except if $char(k) = 3$ and C is geometrically isomorphic to the Fermat quartic $x^4 + y^4 + z^4 = 0$.

Theorem

Suppose $char(k) \neq 2$. If $q \geq 66^2 + 1$ there exists a tangent to C which cuts C at rational points only.

Remark : estimation of $\pi_X = 33$ by Hurwitz formula or thanks to the general theory of correspondences.

Question : The characteristic 2 case ? (P, Q) with P a bitangence point is a singular point on X. There seem to exist cases where X is not abs. irreducible (for instance the Klein quartic $x^3y + y^3z + z^3x = 0$).