Group law on the neutral component of the Jacobian of a real hyperelliptic curve having many real components

Goulwen FICHOU[1]

ABSTRACT. Let C be a real algebraic curve of genus g with at least g real components $B_1, \dots, B_g$. We give an embedding of C into a blow up in one point of the projective plane. It allows us to describe geometrically the neutral real component $Pic^o(C)^o$ of the Jacobian of C thanks to an isomorphism with the product $B_1 \times \cdots \times B_g$. This induces an explicit geometric description of $Pic^o(C)^o$ in the projective plane, where the group law is given by intersection with curves of genus g.

INTRODUCTION

Let C be a real algebraic curve, that is a smooth, proper and geometrically irreducible scheme over $\mathbb{R}$ of dimension 1. Let g be its genus. Denote by $C(\mathbb{R})$ the set of real points of C. As a topological space, $C(\mathbb{R})$ is a disjoint union of circles $\bigcup_s \mathbb{S}^1$, with s the number of connected components of $C(\mathbb{R})$. Harnack Inequality [7] implies that s can not be greater than $g+1$. In the case where $s \geq g$, one says that the curve C has many real components.

In the study of the Jacobian of a curve, these curves are of particular interest because they admit a geometric description of the group law on the real points of the neutral component $Pic^o(C)^o$ of their Jacobian. Actually one knows that topologically $Pic^o(C)^o$ is the product of g circles $(\mathbb{S}^1)^g$ [2], [6], but a result of J. Huisman gave more: a group isomorphism between $Pic^o(C)^o$ and the product of g real components of C [9]. The aim of the present paper is to deduice from this result a geometric description in the real projective plane of the group law on the real points of $Pic^o(C)^o$ for a real hyperelliptic curve C having many real components. Moreover we can give equations to calculate explicitly on this part of the Jacobian.

The particular case of a real curve of genus 2 having many real components, that is two or three, has already been studied in [4]. Remark that such a curve is necessarily hyperelliptic [3]. We gave a group isomorphism between $Pic^o(C)^o$ and the product $B = B_1 \times B_2$ of two real branches of C, when C is defined in $\mathbb{P}^2$ by an equation of the type $xy^2 = P(x)$, $P \in \mathbb{R}[X]$, $\deg(P) = 4$. Then the group law on B is given by taking the intersection of C with certain conics, generalizing the geometric description of the group structure on the neutral real branch of a real elliptic curve which is described by intersections with lines [10].

Let C be a real hyperelliptic curve of genus $g \geq 2$ having many real components. Our starting point is the isomorphism, given in [9], between $Pic^o(C)^o$ and the product $B = B_1 \times \cdots \times B_g$ of g distinct real connected components $B_1, \dots, B_g$ of C, where C is embedded in $\mathbb{P}^{2g}$. We will show that it is possible to consider C as a curve in $\mathbb{P}^2$ with an equation of the type $Q(x)y^2 = P(x)$ where $P, Q \in \mathbb{R}[X]$, $\deg P = \deg Q - 3 = g+2$.

[1]Département de Mathématiques, Université d'Angers, 2 bd Lavoisier, 49045 Angers, France
E-mail: fichou@tonton.univ-angers.fr

Then we will give the description of the group law on B by intersecting C with certain curves on $\mathbb{P}^2$ of degree g and equation $ys(x) = r(x)$ (see figure 1 for an example with $g = 4$, and theorem 3.3 for a precise wording).

One may note that there exist already results dealing with computations on the Jacobian of an hyperelliptic curve, for example D.G. Cantor gave in [1] an algorithm which calculates the sum of two elements on the Jacobian of a hyperelliptic curve defined over a field with characteristic different from 2. His method, which enables one to calculate on the whole Jacobian, requires the choice of a good representative in each equivalence class of divisors of degree 0, and to associate to this representative a pair of polynomials. Then the sum is deduced from Euclidean divisions and computations of GCD. The advantage of our method, which makes sense only in the restricted case of real hyperelliptic curves having many real components, and which computes only on the real points of the neutral component of the Jacobian, lies in the fact that it enables us to find a natural description of this subgroup of the Jacobian, that is without choosing representatives. Moreover, with an algorithmic point of view, the computation of the sum of two elements on the Jacobian only requires us to solve a linear system of order $2g$, and to find the intersection of two curves in the real projective plane.

Let us add that there exists a generalization to this geometric description of the group law on $Pic^o(C)^o$ for real plane curves having many pseudo-lines [5]. But without the hyperelliptic hypothesis, proofs are less elementary in [5]. And, overall, one has no more equations to perform effective computations.

In the first part one studies curves in $\mathbb{P}^2$ with equation $Q(x)y^2 = P(x)$ where $P, Q \in \mathbb{R}[X]$, $\deg P = \deg Q - 3 = g + 2$. Note that such a curve is hyperelliptic. Actually we will show that a real hyperelliptic curve C with many real components is birationally isomorphic to such a curve. In the second part, we will give an embedding of C in the blowing-up of $\mathbb{P}^2$ in one point. This blowing-up can also be embedded in $\mathbb{P}^{2g}$ where we know a geometric desciption of the group law on $Pic^o(C)^o$ as it has been explained above. Then it remains to go back to the projective plane via the blowing-up of $\mathbb{P}^2$, and to describe explicitly the group law on B, in the last part.

Let us note finally that in the particular case of curves of genus 2, some equations allowed us to justify the embedding of the blowing-up of $\mathbb{P}^2$ in $\mathbb{P}^4$. But this basic method used in [4] does not seem to generalize easily to the case of real hyperelliptic curves of genus greater than 2. To embed this blowing-up of $\mathbb{P}^2$ in $\mathbb{P}^{2g}$, we refer in this paper to the complex structure of the curve C (see proposition 2.1).

1. CURVES DEFINED BY $Q(x)y^2 = P(x)$

Let us choose a projective coordinate system $[z : x : y]$ on the real projective plane $\mathbb{P}^2$. The purpose of the first proposition is to give conditions to enable the curve defined by the equation $Q(x)y^2 = P(x)$ in the affine part $\{z = 1\}$ of $\mathbb{P}^2$ to be irreducible and sufficiently smooth.

Proposition 1.1. *Let $g \geq 2$ be an integer and $P, Q \in \mathbb{R}[X]$ be polynomials such that $\deg(P) = \deg(Q) + 3 = g + 2$, P and Q are separable and relatively prime. Suppose that P has at least g real roots, Q splits over $\mathbb{R}$, the real roots of Q are separated by those of P and there exists at least one root of P stricly greater than the roots of Q. Then the curve in $\mathbb{P}^2$ defined in the affine part of $\mathbb{P}^2$ by the equation*

$$Q(x)y^2 = P(x)$$

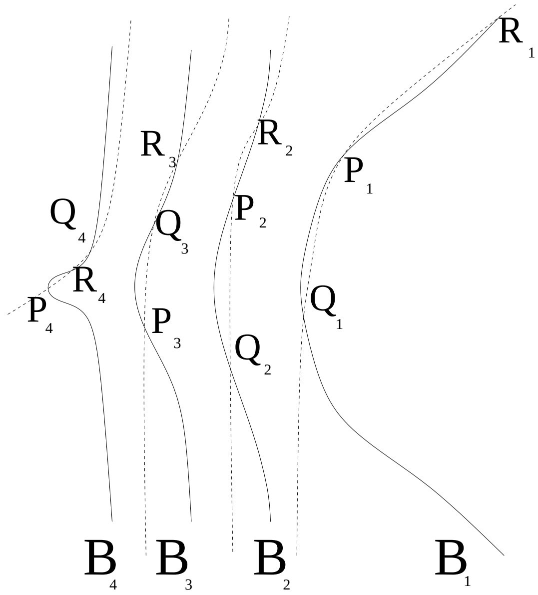

FIGURE 1. The sum of $P = (P_1, P_2, P_3, P_4)$ and $Q = (Q_1, Q_2, Q_3, Q_4)$ in B is $P + Q = -R$, where the curve giving the sum is represented in dotted line and C in full line.

is geometrically irreducible, smooth out of the point $(0:1:0)$ *which is a real ordinary singular point of order* g*, hyperelliptic of genus* g*, and exactly* g *real branches pass through* $(0:1:0)$*. In particular the normalization of the curve has many real branches.*

Proof. This statement is a direct generalization of proposition 1.1 of [4]. The fact that the projection $(x, y) \longrightarrow x$ is a morphism of degree 2 over $\mathbb{P}^1$ implies that the curve is hyperelliptic. $\square$

Remark. C has exactly $g+1$ real branches if and only if P splits over $\mathbb{R}$.

One can state a converse to the proposition, which is actually the starting point of the present paper. Although again it is a direct generalization of a proposition of [4], we recall its proof in order to fix notations that will be useful in the sequel.

Proposition 1.2. *Let* C *be a real hyperelliptic curve of genus* g*, geometrically irreducible, smooth, proper, with many real branches. There exist polynomials* $P, Q \in \mathbb{R}[X]$ *which satisfy* $\deg(P) = g+2$*,* $\deg(Q) = g-1$*,* P *is separable with at least* g *real roots,* Q *splits over* $\mathbb{R}$*, the real roots of* P *separate those of* Q *and there exists at least one root of* P *stricly greater than the roots of* Q *such that* C *is birationally isomorphic to the curve in* $\mathbb{P}^2$ *defined in the affine part of* $\mathbb{P}^2$ *by the equation*

$$Q(x)y^2 = P(x).$$

Proof. It is well known that C is birationally isomorphic to a curve in $\mathbb{P}^2$ given in the affine part $\{z = 1\}$ by an equation of the type $y^2 = R(x)$ with $R \in \mathbb{R}[X]$, $\deg(R) = 2g+1$, R separable with at least $2g-1$ real roots. Denote $x_1 > x_2 > \cdots > x_{2g-1}$ the sequence of the $2g-1$ higher real roots of R, and S the polynomial

$$S(X) = \frac{R(X)}{\prod_{i=1}^{2g-1}(X - x_i)} \in \mathbb{R}[X].$$

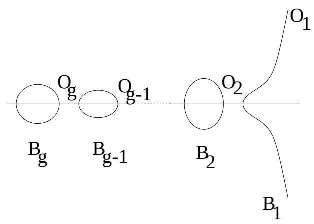

FIGURE 2. Curve C given by an equation of the type $y^2 = R(x)$ with $R \in \mathbb{R}[X]$, $\deg(R) = 2g+1$, separable with at least $2g-1$ real roots.

Define $P(X) = S(X)\prod_{i=1}^{g}(X - x_{2i-1})$ and $Q(X) = \prod_{i=1}^{g-1}(X - x_{2i})$. Then $R = PQ$. The application $(x, y) \longrightarrow (x, \frac{y}{Q(x)})$ is a birational isomorphism of $\mathbb{P}^2$, with inverse $(x, y) \longrightarrow (x, yQ(x))$, which exchanges the curves of equation $y^2 = R(x)$ and $y^2 = \frac{P(x)}{Q(x)}$. $\square$

Let us fix once for all a curve C of genus g geometrically irreducible, smooth, proper, with many real branches. Then C is birationally isomorphic to a curve of $\mathbb{P}^2$ given by an equation of the type $y^2 = R(x)$, with $R \in \mathbb{R}[X]$ separable of degree $2g+1$ with at least $2g-1$ real roots, as in the latter proof. Denote O_i the point of C with coordinates $(x_{2i-2} : 0 : 1)$ for $i \in \{2, \dots, g\}$ and O_1 the point $(0 : 1 : 0)$. The points O_i, for $i \in \{1, \dots, g\}$, are Weierstrass points of C. Let B_i be the connected component of $C(\mathbb{R})$ containing O_i, for $i \in \{1, \dots, g\}$ (see figure 2).

Corollary 1.3. *The birational embedding $\varphi : C \longrightarrow \mathbb{P}^2$ of the latter proposition is the morphism associated to the linear system $|3O_1 + O_2 + \cdots + O_g|$.*

Proof. One can show that $\varphi^*(\{Z = 0\}) = 3O_1 + O_2 + \cdots + O_g$ in a similar way that in [4], corollary 1.3.

It remains to note that the divisor $3O_1 + O_2 + \cdots + O_g$ is non special by [9], theorem 2.3. It follows from Riemann-Roch theorem that the dimension of the linear system $|3O_1 + O_2 + \cdots + O_g|$ is $g + 2 - g = 2$.

$\square$

2. THE CURVE IN $\mathbb{P}^{2g}$

The divisor $3O$ on the curve C is non special and very ample because its degree equals $3g$ [8] and so the linear system $|3O|$ induces an embedding of C into $\mathbb{P}^{2g}$. We know how to describe geometrically the group law on $Pic^o(C)^o$ as it has been recalled in the introduction (cf [9]). The way to do it is to consider the group isomorphism between $B = B_1 \times \cdots \times B_g$ and $Pic^o(C)^o$ which associates to $(P_1, \dots, P_g) \in B$ the linear equivalence class of the divisor $\sum_{i=1}^{g} P_i - O_i \in Pic^o(C)^o$. Let us describe the group law on B. The neutral element is $(O_1, \dots, O_g)$. For $(P, Q) \in B^2$, there exists a unique hyperplane in $\mathbb{P}^{2g}$ which passes through the points P_i, Q_i, O_i, $i \in \{1, \dots, g\}$. This hyperplane crosses C in g other points $R_i \in B_i$ for $i \in \{1, \dots, g\}$. Then the sum $P + Q$ is defined by $P + Q = -R$ where $R = (R_1, \dots, R_g)$. One finds the inverse of P by choosing $Q = (O_1, \dots, O_g)$ in this description.

In order to give a geometric description of the group structure on B in the projective plane, let us split the embedding of C into $\mathbb{P}^{2g}$. We will pass through the blowing-up of $\mathbb{P}^2$ at the unique singular point of $\varphi(C)$ in $\mathbb{P}^2$. Let us denote by K this blowing-up, the real points of K consisting topologically of a Klein bottle.

The image of $\varphi(C)$ in K is its normalization $\widetilde{C}$ because of proposition 1.2, therefore we obtain the first step: an embedding $C \longrightarrow K$. Now we will embed K into $\mathbb{P}^{2g}$ in the following way: let E be the exceptional divisor on K and $\widetilde{H} = \pi^*(H)$ where π is the morphism of the blowing-up and H the hyperplane divisor of $\mathbb{P}^2$.

Proposition 2.1. *The linear system $|g\widetilde{H} - (g-1)E|$ induces an embedding ψ of K into $\mathbb{P}^{2g}$.*

Proof. What we have to do is to check that $g\widetilde{H} - (g-1)E$ is a very ample divisor on K, and that the dimension of $|g\widetilde{H} - (g-1)E|$ is $2g$.

Let us show that $g\widetilde{H} - (g-1)E$ is very ample as a complex divisor. The elements of $|g\widetilde{H} - (g-1)E|$ can be identified with the curves of $\mathbb{P}^2$ of degree g passing through $(0:1:0)$ with multiplicity at least $g-1$. The equation of such a curve in the affine part $\{y=1\}$ of $\mathbb{P}^2$ is of the type $\sum_{g-1 \leq i+j \leq g} a_{i,j} x^i z^j$ with $a_{i,j} \in \mathbb{C}$, hence $\dim |g\widetilde{H} - (g-1)E| = 2g$.

Now, in order to show that $g\widetilde{H} - (g-1)E$ is very ample, it suffices to check that for all $p, q \in \mathbb{P}^2$, p and q possibly infinitely near, $\dim |D - p - q| = \dim |D| - 2$ where $D = gH - (g-1)(0:1:0)$ (cf [8], 4.0.2. p 396). For $p \in \mathbb{P}^2$ one has $\dim |D - p| = \dim |D| - 1$ because there exist a curve in $|D|$ which does not pass through p (or which does not have a given tangent line in $(0:1:0)$ in the case where p and q are infinitely near). It remains to check that for any q in $\mathbb{P}^2$ there exists a curve of $|D|$ passing through p but not through q. If p and q are not infinitely near it is easy. If they are, one needs a curve passing through $(0:1:0)$ with a given tangent line, and with an order of contact equals exactly 2. One can choose the curve with equation in the affine part $\{y=1\}$: $(aZ + bX + (aZ - bX)^2)x^{g-2}$ in the case where the tangent line is given by $\{aZ + bX = 0\}$, and the one given by $(aZ + bX + (aZ - bX)^2)Z^{g-2}$ otherwise.

Therefore as a complex divisor $g\widetilde{H} - (g-1)E$ is very ample. Moreover it is equivariant with respect to the action of the Galois group of $\mathbb{C}$ over $\mathbb{R}$ because its support is real. Hence as a real divisor $g\widetilde{H} - (g-1)E$ is also very ample. $\square$

Corollary 2.2. *The embedding of C into $\mathbb{P}^{2g}$ induced by the ones of C into K and of K into $\mathbb{P}^{2g}$ is the morphism associated to the linear system $|3O|$.*

Proof. We must show that the divisors $(\psi \circ \varphi)^*(\{Z = 0\})$ and $3O$ are linearly equivalent.

But $(\psi \circ \varphi)^*(\{Z = 0\}) = \varphi^*(g\widetilde{H} - (g-1)E)$, and this divisor corresponds to the intersection product $\widetilde{C} \cdot (g\widetilde{H} - (g-1)E)$ on $\widetilde{C}$. So $\widetilde{C} \cdot (g\widetilde{H} - (g-1)E) = g\widetilde{C} \cdot \widetilde{H} - (g-1)\widetilde{C} \cdot E = g(3O_1 + O_2 + \cdots + O_g) - (g-1)O = 2gO_1 + O$.

What remains to check is that $2gO_1 + O$ is linearly equivalent to $3O$ or, in other words, that $2gO_1$ is linearly equivalent to $2O$. Let $\widetilde{O}_i$ be the other Weierstrass point of C on B_i for $i \in \{1, \ldots, g\}$ and A be the divisor of degree 2 corresponding to the remaining two Weierstrass points, which are either both real or complex conjugate points (there are $2g+2$ Weierstrass points on a hyperelliptic curve, cf [3]).

The projection onto the line $\{x = 0\}$ of C, where C is regarded as in proposition 1.1, implies that $2O_1 + O \sim \widetilde{O}_1 + \cdots + \widetilde{O}_g + A$. Moreover the projection of C onto the line $\{x = 0\}$ considering C given by an equation of the type $y^2 = R(X)$ induces that $\widetilde{O}_1 + \cdots + \widetilde{O}_g + A + O_2 + \cdots + O_g \sim (2g+1)O_1$. Joining both results gives the equivalence we were looking for: $2gO_1 \sim 2O$.

The conclusion comes from the fact that the dimension of $|3O|$ is $2g$ by Riemann-Roch theorem.

□

3. GROUP LAW ON B

Let us begin with a classical result. The hyperelliptic involution of the curve induces the multiplication by -1 on the Jacobian.

Proposition 3.1. *The inverse of* $(P_1, \ldots, P_g)$ *is* $(J(P_1), \ldots, J(P_g))$.

Proof. The isomorphism between $B = B_1 \times \cdots \times B_g$ and $Pic^o(C)^o$ is given by $(P_1, \ldots, P_g) \longrightarrow [(P_1 - O_1) + \cdots + (P_g - O_g)]$ where $[D]$ denotes the class of the divisor D (cf [9]). □

In order to describe the additive law, let us first give the result in terms of linear system in K.

Proposition 3.2. *For all* $(P, Q) \in B^2$ *there exists a unique divisor* $D \in |g\widetilde{H} - (g-1)E|$ *such that* $D \cdot \widetilde{C} \geq \sum_{i=1}^{g} P_i + Q_i$. *Moreover there exist exactly* g *points* $R_1, \ldots, R_g$ *on* $B_1, \ldots, B_g$ *respectively such that* $D \cdot \widetilde{C} = \sum_{i=1}^{g} P_i + Q_i + R_i$. *Then the sum* $P + Q$ *is given by* $P + Q = -R$.

Proof. This result follows directly from the group law description on B in $\mathbb{P}^{2g}$, which has been explained at the beginning of the previous section. Actually the embedding of K into $\mathbb{P}^{2g}$ of proposition 2.1. induces a bijection between the linear system of hyperplanes of $\mathbb{P}^{2g}$ and $|g\widetilde{H} - (g-1)E|$. □

Now we can give the geometric description of the additive law in $\mathbb{P}^2$ on the product $\varphi(B_1) \times \cdots \times \varphi(B_g)$ of the images of the branches B_i of C in $\mathbb{P}^2$.

Theorem 3.3. *Let* $P, Q \in \varphi(B_1) \times \cdots \times \varphi(B_g)$. *There exists a unique curve* D *in* $\mathbb{P}^2$ *of degree* g *which passes through points* $P_1, \ldots, P_g, Q_1, \ldots, Q_g$ *and* $(0:1:0)$ *of* $\varphi(C(\mathbb{R}))$ *(with multiplicity).*

Moreover there exist $R_1 \in \varphi(B_1), \ldots, R_g \in \varphi(B_g)$ *determined only by* D *such that*

$$D \cdot \varphi(C) = P_1 + \cdots + P_g + Q_1 + \cdots + Q_g + R_1 + \cdots + R_g + g(g-1)(0:1:0).$$

Then the sum of P *and* Q *is* $P + Q = -(R_1, \ldots, R_g)$.

Proof. The intersection points of $\varphi(C)$ and D are real because they are real in K. Moreover $(0:1:0)$, which is the unique point of $\varphi(C)$ at infinity, concentrates the remainder of the intersection multiplicity; by Bezout Theorem this multiplicity is $g(g+2) - 3g = g(g-1)$.

□

Remark. The subsets of $\varphi(B_1) \times \cdots \times \varphi(B_g)$ of the type $\{O_1\} \times \cdots \times \{O_{i-1}\} \times \varphi(B_i) \times \{O_{i+1}\} \times \cdots \times \{O_g\}$ are never subgroups of $\varphi(B_1) \times \cdots \times \varphi(B_g)$; they are not even stable with respect to the group law (see figure 3).

The 2-torsion elements of B form a subgroup of order 2^g. It is an easy game to read it out of B. Denote by $\widetilde{O_i}$ the other Weierstrass point of $\varphi(C)$ on $\varphi(B_i)$, that is the point of $\varphi(B_i)$ crossing the line $\{y = 0\}$ in $\mathbb{P}^2$, for $i \in \{1, \ldots, g\}$.

Proposition 3.4. *The* 2*-torsion elements of* $\varphi(B_1) \times \cdots \times \varphi(B_g)$ *are the elements of the type* $(P_1, \ldots, P_g)$ *with* $P_i \in \{O_i, \widetilde{O_i}\}$ *for* $i \in \{1, \ldots, g\}$.

Remark. In the particular case of an elliptic curve, the 3-torsion points of the real points of the neutral component of the Jacobian are the real inflection points of the curve. In the present case of a real hyperelliptic curve C with many real branches, one might have believed in the fact that points of the type $(P_1, \ldots, P_g)$ with P_i a

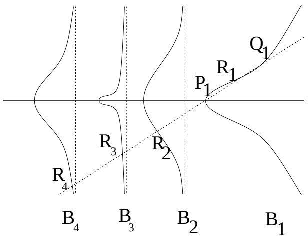

FIGURE 3. $(P_1, O_2, \ldots, O_g) + (Q_1, O_2, \ldots, O_g) = (J(R_1), \ldots, J(R_g))$ and $J(R_i) = O_i$ for $i \geq 2$ if and only if $Q_1 = J(P_1)$.

inflection point of $\varphi(C)$ form the 3-torsion subgroup, all the more so since they form sets with the same cardinal number 3^g! Unfortunately this is not true (cf [4]).

Acknowledgements. The author wish to thank Johan Huisman for his help during this work, and also Pawel Goldstein for his careful rereading of the english version.

References

[1] Cantor, D.G.: Computing in the Jacobian of a Hyperelliptique Curve, Math. Comp. 48 (1987), 95-101

[2] Ciliberto, C., Pedrini, C.: Real abelian varieties and real algebraic curves, Lectures in real geometry, F. Broglia (ed.), de Gruyter Exp. Math. 23, 1996, 167-256

[3] Farkas, H.M., Kra, I.: Riemann Surfaces, Grad. Texts in Math. 71, Springer Verlag, 1980

[4] Fichou, G.: Loi de groupe sur la composante neutre de la jacobienne d'une courbe réelle de genre 2 ayant beaucoup de composantes réelles, Manuscripta Math. 104, (2001) 459-466

[5] Fichou, G., Huisman, J.: A geometric description of the neutral component of the Jacobian of a real plane curve having many pseudo-lines, to appear in Math. Nach.

[6] Gross, B.H, Harris, J.: Real algebraic curves, Ann. scient. Ec. Norm. Sup. t. 14 (1981), 157-182

[7] Harnack, A.: Über die Vieltheiligkeit der ebenen algebraischen Curven, Math. Ann. 10 (1876), 189-198

[8] Hartshorne, R.: Algebraic Geometry, Grad. Texts in Math. 52, Springer Verlag, 1977

[9] Huisman, J.: On the neutral component of the Jacobian of a real algebraic curve having many components, Indag. Math. 12(1) (2001) 73-81

[10] Silverman, J.H.: The arithmetic of elliptic curves, Grad. Texts in Math. 106, Springer Verlag, 1986