Hyperelliptic Jacobians in differential Galois theory (preliminary report)

Jerald J. Kovacic
Department of Mathematics
The City College of The City University of New York
New York, NY 10031

jkovacic@member.ams.org
http://mysite.verizon.net/jkovacic

December 13, 2003

Introduction

Picard-Vessiot theory has had a renaissance, however differential Galois theory has not. One of the reasons is that there are few examples. Theoretically, any connected algebraic group, linear or not, is the Galois group of a strongly normal extension, but explicit examples are in short supply. In fact there is only one, the Weierstrass $\wp$-function. If the theory is to be useful, we need some "meaty" examples. This a preliminary report on work to find some.

Throughout, $\mathcal{F}$ is a Δ-field of characteristic 0 with algebraically closed field of constants $\mathcal{F}^\Delta = \mathcal{C}$. For ease of exposition we assume that $\mathcal{F}$ is ordinary. However everything we say goes through for partial differential fields as well. We use $\mathcal{G}$ to denote a Δ-extension field of $\mathcal{F}$.

Logarithmic derivative of matrices

Let $\eta \in \mathrm{GL}(n)$, then

$$\ell\delta\eta = \eta'\eta^{-1}$$

is the *logarithmic derivative* of η.

Proposition. *If $G \subset \mathrm{GL}(n)$ is an algebraic group defined over $\mathcal{C}$ and $\ell(G) \subset \mathrm{Mat}(n)$ is its Lie algebra of matrices, then*

$$\eta \in G \quad \Longrightarrow \quad \ell\delta\eta \in \ell(G).$$

Using this, we can construct Picard-Vessiot extensions:

Proposition. *Suppose that $\mathcal{G} = \mathcal{F}(\eta)$, where*

1. $\eta \in G_{\mathcal{G}}$.
2. $\ell\delta\eta \in \ell_{\mathcal{F}}(G)$.
3. $\mathcal{G}^{\Delta} = \mathcal{C}$.

Then $\mathcal{G}$ is a Picard-Vessiot extension of $\mathcal{F}$ whose Galois group is a subgroup of $G_{\mathcal{C}}$.

In the Weil set-up you have a universal differential field $\mathcal{U}$, and we get a mapping

$$\ell\delta\colon G_{\mathcal{U}} \to \ell_{\mathcal{U}}(G)$$

It turns out to be surjective. It is not rational since it involves derivatives. However, it is differential rational when you think of G and $\ell(G)$ as differential algebraic groups.

In general it is only a crossed homomorphism, but if G is commutative then it is a group homomorphism. This is important for the classification of differential algebraic groups. For example, Cassidy [5, Proposition 31, p. 937] classifies Zariski dense subgroups of $\mathbf{G}_{\mathbf{m}}^n$ using the logarithmic derivative.

Invariant derivations

Now let G be any connected algebraic group defined over $\mathcal{C}$, which is not necessarily linear. We denote right translation by

$$\rho_h \colon G \to G \qquad \rho_h(g) = gh,$$

If $\mathcal{C}(G)$ is the field of rational functions we have

$$\rho_h^{\#} \colon \mathcal{C}(G) \to \mathcal{C}(G), \qquad (\rho_h^{\#}(\phi))(g) = \phi(gh).$$

A derivation D of $\mathcal{C}(G)$ over $\mathcal{C}$ is *invariant* if

$$D \circ \rho_h^{\#} = \rho_h^{\#} \circ D$$

for every $h \in G$.

Definition. The *Lie algebra* of G is the set of all invariant derivations of $\mathcal{C}(G)$. It is denoted by $\mathfrak{L}(G)$.

Let $g \in G$, and denote the local ring at g by $\mathcal{O}_g$. A derivation T of $\mathcal{O}_g$ into $\mathcal{C}$ is called a *local derivation at* g if

$$T(\phi\psi) = \phi(g)T(\psi) + \psi(g)T(\phi).$$

Definition. The Lie algebra of all local derivations at g is the *tangent space* at g. It is denoted by $\mathfrak{T}_g(G)$.

Definition. Let $D \in \mathfrak{L}(G)$. Define a local derivation D_g by the formula

$$D_g(\phi) = (D(\phi))(g).$$

Proposition. *Fix $g \in G$. The mapping*

$$\mathfrak{L}(G) \to \mathfrak{T}_g(G), \qquad D \mapsto D_g,$$

is an isomorphism of Lie algebras.

Logarithmic derivative

For matrix groups $G \subset \mathrm{GL}(n)$ we have a isomorphisms

$$\begin{array}{ccccc} \ell(G) & \longrightarrow & \mathfrak{L}(G) & \longrightarrow & \mathfrak{T}_\eta(G) \\ \ell\delta\eta & \longrightarrow & D(\ell\delta\eta) & \longrightarrow & (D(\ell\delta\eta))_\eta. \end{array}$$

If $X = (X_{ij})$ are the coordinate functions then

$$D(\ell\delta\eta)X = \ell\delta\eta X = \eta'\eta^{-1}X,$$

and

$$D(\ell\delta\eta)_\eta(X) = (\eta'\eta^{-1}X)(\eta) = \eta'.$$

We generalize this.

Definition. Let G be a connected algebraic group defined over $\mathcal{C}$ (not necessarily linear). Let $\eta \in G$. Then

$$\ell\delta\eta \in \mathfrak{L}(G)$$

is the unique element whose tangent vector $(\ell\delta\eta)_\eta \in \mathfrak{T}_\eta$ satisfies

$$(\ell\delta\eta)_\eta(\phi) = (\phi(\eta))'$$

whenever $\phi \in \mathcal{C}(G)$.

See Kolchin [7, p. 349] or Kovacic [9, Section 1, p. 270].

Proposition. *Let G be a connected algebraic group defined over $\mathcal{C}$ and $\eta \in G_\mathcal{G}$. Suppose that*

1. $\mathcal{G} = \mathcal{F}(\eta)$.
2. $\ell\delta\eta \in \mathfrak{L}_\mathcal{F}(G)$.
3. $\mathcal{G}^\Delta = \mathcal{C}$.

Then $\mathcal{G}$ is a strongly normal extension of $\mathcal{F}$ whose Galois group is a subgroup of $G_\mathcal{C}$.

See Kolchin [7, Theorem 7, p. 419] or Kovacic [8, p. 586].

Hyperelliptic curve

Consider the curve C_1:

$$y^2 = f(x) = 4 \prod_{k=1}^{2g+1} (x - e_k),$$

where $e_1, \ldots, e_{2g+1} \in \mathcal{C}$ are distinct. We add one point, called ∞, which is $\overline{x} = \overline{y} = 0$ in the second chart C_2:

$$\overline{y}^2 = \overline{f}(x) = 4\overline{x} \prod_{k=1}^{2g+1} (1 - e_k\overline{x}).$$

These are patched by

$$\overline{x} = \frac{1}{x}, \qquad \text{and} \qquad \overline{y} = \frac{y}{x^{g+1}}.$$

The union of these, C, is smooth (even at ∞) and complete. It is the hyperelliptic curve of genus g.

The "classic" algebraic treatment is Mumford [10]. The appendix of Koblitz [6] is a nice introduction, although the emphasis is on cryptography.

For every $a \in \mathcal{C}$ there are two points (a, b) and $(a, -b)$ in C except at the "branch points" $a = e_k$, $b = 0$. ∞ is also a branch point. Analytically, C is a two-sheeted covering of the Riemann sphere with $2g + 2$ branch points: $E_k = (e_k, 0)$ and ∞.

The function that switches the sheets

$$I : C \to C, \qquad I(a, b) = (a, -b), \quad I(\infty) = \infty,$$

is called the hyperelliptic involution.

Valuations

Because C is smooth, the local ring $\mathcal{O}_P$ at every point P is a regular local ring. Thus the maximal ideal $\mathfrak{m}_P$ is principal and $\mathcal{O}_P$ is a discrete valuation ring, with valuation ν_P.

If $P = (a, b)$ is not a branch point,

$$\nu_P(x - a) = 1 \qquad \text{and} \qquad \nu_P(y - b) = 1.$$

If $P = E_k = (e_k, 0)$ is a finite branch point,

$$\nu_{E_k}(x - e_k) = 2 \qquad \text{and} \qquad \nu_{E_k}(y) = 1.$$

Finally,

$$\nu_\infty(\overline{x}) = 2 \qquad \text{and} \qquad \nu_\infty(\overline{y}) = 1,$$

and

$$\begin{aligned} \nu_\infty(x) &= -\nu_\infty(\overline{x}) = -2 \\ \nu_\infty(y) &= \nu_\infty(\overline{y}) - (g+1)\nu_\infty(\overline{x}) = -(2g+1). \end{aligned}$$

Using these valuations Bertrand [2] has implemented efficient algorithms for computing hyperelliptic integrals.

The Singer algorithm for solving linear homogeneous differential equations should also be implementable. However, as far as I am aware, no one has done any work on this.

Divisors

A divisor is a formal sum of points of C

$$D = \sum_{i=1}^{r} n_i P_i$$

where $n_i \in \mathbb{Z}$ and $P_i \in C$ (including ∞). The degree of D is

$$\deg D = \sum_{i=1}^{r} n_i.$$

The group of all divisors is $\mathcal{D}$ and the subgroup of divisors of degree 0 is $\mathcal{D}_0$

Proposition. *$\phi \in \mathbb{C}(x, y)$ has a finite number of poles and zeros.*

For hyperelliptic curves, this is easy since ϕ can be written in the form

$$\phi = \frac{A(x) + B(x)y}{C(x)}$$

where $A(x), B(x), C(x) \in \mathbb{C}[x]$.

Definition. If $\phi \in \mathbb{C}(x, y)$ then the divisor of ϕ is

$$(\phi) = \sum_{P \in C} \nu_P(\phi)\, P.$$

The divisor of a function is called a *principal divisor*.

Definition. Two divisors D and E are linearly equivalent, written $D \sim E$, if there is a function $\phi \in \mathbb{C}(x, y)$ such that

$$D = E + (\phi).$$

Proposition. *ϕ has the same number of poles as zeros (counted with multiplicity), i.e.* $\deg(\phi) = 0$.

For hyperelliptic curves this is also easy since

$$\phi \cdot I(\phi) = \frac{A(x) + B(x)y}{C(x)} \cdot \frac{A(x) - B(x)y}{C(x)} = \frac{A(x)^2 - f(x)B(x)^2}{C(x)^2}$$

is a rational function of x alone.

Since equivalent divisors have the same degree we also have an equivalence relation on $\mathcal{D}_0$.

Definition. $\mathrm{Jac}(C) = \mathcal{D}_0/\sim$, i.e. the group of divisors of degree 0 modulo principal divisors.

Proposition. $\mathrm{Jac}(C)$ *is an Abelian variety.*

Mumford [10, p. 3.38].

Semi-reduced divisors

From now on we deal only with divisors of degree 0, which we write as

$$D = \sum_{i=1}^{r} n_i P_i - n\infty,$$

where $P_i \neq \infty$, $P_i \neq P_j$, $n_i \neq 0$, and $\sum_{i=1}^{r} n_i = n$.

Definition. We say that D is *semi-reduced* if

1. $n_i > 0$,
2. if $i \neq j$ then $P_i \neq I(P_j)$,
3. if P_i is a branch point then $n_i = 1$.

Proposition. *Every divisor is equivalent to a semi-reduced divisor.*

Suppose that $P = (a, b)$ is not a branch point. Consider the rational function $x - a \in \mathcal{C}(x)$. Its divisor is

$$(x - a) = P + I(P) - 2\infty$$

hence

$$-P \sim I(P) - 2\infty.$$

Thus the first condition ($n_i > 0$) is easy to obtain. If P is not a branch and both P and $I(P)$ appear in D then we use the formula

$$P + I(P) \sim 2\infty$$

to get the second condition. Finally, for a branch point,

$$2E_k = (x - e_k) + 2\infty \quad \text{i.e.} \quad 2E_k \sim 2\infty,$$

which gives the third condition.

Reduced divisors

Definition. A semi-reduced divisor

$$D = \sum_{i=1}^{r} n_i P_i - n\infty$$

is *reduced* if $n \leq g$.

Since D has degree 0, $n = \sum_{i=1}^{r} n_i$. In the next section we sketch the proof of the following.

Proposition. *Any divisor of degree* 0 *is equivalent to a* unique *reduced divisor.*

Corollary. $\mathrm{Jac}(C)$ *may be identified with the set of reduced divisors.*

Corollary. $\mathrm{Jac}(C)$ *may be identified with* $\bigoplus_{n=0}^{g} C_1^{(n)}$ *where* $C_1^{(n)}$ *is the* n*-fold symmetric product.*

The addition law on $\mathrm{Jac}(C)$ is:

If D and E are reduced divisors then $D + E$ is the unique reduced divisor equivalent to $D + E$.

Reduction step

We look at the special case where

$$D = \sum_{i=1}^{g+1} P_i - (g+1)\infty,$$

with $P_i = (a_i, b_i)$ distinct (i.e. $n_i = 1$ and $n = g+1$). In addition we assume that P_i is not a branch point. Let

$$U(x) = \prod_{i=1}^{g+1}(x - a_i)$$

$$V(x) = \sum_{i=1}^{g+1} \prod_{\substack{j=1 \\ j\neq i}}^{g+1} \frac{x - a_j}{a_i - a_j}\, b_i.$$

$V(x)$ is the Lagrange interpolation polynomial so

1. $\deg V(x) = g$,
2. $V(a_i) = b_i$ for $i = 1, \ldots, g+1$.

In the general case, where the P_i are not distinct, we need Hermite interpolation rather than Lagrange, and the formulas are more complicated.

Define a rational function

$$\phi = \frac{y + V(x)}{U(x)} \in \mathcal{C}(x, y).$$

The finite poles of ϕ are zeros of $U(x)$, i.e. P_i and $I(P_i)$. Since

$$(y + V(x))(P_i) = b_i + V(a_i) = 2b_i \neq 0,$$

P_i are poles of ϕ. But

$$(y + V(x))(I(P_i)) = -b_i + V(a_i) = 0,$$

so $I(P_i)$ are not poles of ϕ. At ∞:

$$\begin{array}{rlll} \nu_\infty(\phi) = \nu_\infty(y + V(x)) & & - & \nu_\infty(U(x)) \\ = \min(-(2g+1), -2g) & & + & 2(g+1) \\ = 1. & & & \end{array}$$

Therefore ϕ has $g + 1$ poles $(P_1, \ldots, P_{g+1})$, and a single zero at ∞. It must have g more zeroes, i.e.

$$(\phi) = -P_1 - \cdots - P_{g+1} + \infty + Q_1 + \cdots + Q_g.$$

Hence

$$\begin{aligned} D &= P_1 + \cdots + P_{g+1} - (g+1)\infty \\ &\sim Q_1 + \cdots + Q_g - g\infty. \end{aligned}$$

The right hand side need not be semi-reduced, but we can replace it by a semi-reduced divisor, which will then be reduced.

Suppose that $Q_j = (c_j, d_j)$ and let

$$W(x) = \prod_{j=1}^{g} (x - c_j).$$

Now $y - V(x)$ vanishes at each P_i and $y + V(x)$ vanishes at each Q_j, therefore

$$(y - V(x))(y + V(x)) = f(x) - V^2(x)$$

vanishes at $P_1, \ldots, P_{g+1}, Q_1, \ldots, Q_g$. Therefore

$$f(x) - V^2(x) = 4U(x)W(x).$$

Therefore we can compute $W(x)$ by division of polynomials, The c_j are roots of $W(x) = 0$ and

$$d_j = -V(c_j).$$

Iterating this reduction we can start with any divisor of degree 0 and find a reduced divisor equivalent to it. This can be easily made into an algorithm, see, for example, Murty [11]. A much more efficient algorithm, avoiding iteration, is due to Cantor [4]. Because it is usually applied to the sum of two divisors it is called the addition algorithm.

Elliptic curve

Suppose that $g = 1$, and $y^2 = 4x^3 - g_2 x - g_3$. Then

$$U(x) = (x - a_1)(x - a_2)$$

$$V(x) = \frac{x - a_1}{a_1 - a_2}\, b_1 + \frac{x - a_2}{a_2 - a_1}\, b_2,$$

$$W(x) = x - c_1,$$

$$f(x) - V^2(x) = 4U(x)W(x),$$

therefore

$$4x^3 - g_2 x - g_3 - V^2(x) = 4U(x)W(x) = 4(x - a_1)(x - a_2)(x - c_1)$$

Look at the coefficient of x^2:

$$0 - \left(\frac{b_1}{a_1 - a_2} + \frac{b_2}{a_2 - a_1} \right)^2 = 4(-a_1 - a_2 - c_1)$$

which gives

$$c_1 = -a_1 - a_2 + \frac{1}{4} \left(\frac{b_1 - b_2}{a_1 - a_2} \right)^2 .$$

This is the "well-known" addition formula.

Lie algebra

Let $x_1, \ldots, x_g$ be indeterminates over $\mathcal{C}$ and define y_i by $y_i^2 = f(x_i)$. The field $\mathcal{C}(x_1, y_1, \ldots, x_g, y_g)$ is denoted by $C(\mathbf{x}, \mathbf{y})$, it is the field of rational functions of C^g, the g-th power of C.

Proposition. $\mathcal{C}(\mathrm{Jac}(C))$ *is the field* $\mathcal{C}(\mathbf{x}, \mathbf{y})_{\mathrm{sym}}$ *consisting of all functions that are symmetric in the indices.*

$\mathcal{C}(\mathrm{Jac}(C))$ can be explicitly described using the elementary symmetric functions and coefficients of the Lagrange interpolation polynomial.

Recall, $\mathcal{L}(\mathrm{Jac}(C))$ is the Lie algebra of all invariant derivations of $\mathcal{C}(\mathrm{Jac}(C))$. Since $\mathcal{C}(\mathbf{x}, \mathbf{y})$ is algebraic over $\mathcal{C}(\mathrm{Jac}(C))$, every derivation of $\mathcal{C}(\mathrm{Jac}(C))$ extends to a derivation of $\mathcal{C}(\mathbf{x}, \mathbf{y})$. Because $\mathcal{C}(\mathbf{x}, \mathbf{y})$ is algebraic over $\mathcal{C}(\mathbf{x})$ the derivation is determined by its action on $x_1, \ldots, x_g$.

We denote by

$$\sigma_k(x_1, \ldots, \widehat{x_i}, \ldots, x_g) = \sum_{\substack{1 \le j_1 < \cdots < j_k \le g \\ j_1 \ne i, \ldots, j_k \ne i}} x_{j_1} \cdots x_{j_k}$$

the the elementary symmetric functions of $g-1$ variables where x_i is omitted.

Definition. Define derivations D_k of $\mathcal{C}(\mathbf{x}, \mathbf{y})$, for $k = 0, \ldots, g-1$, by

$$D_k(x_i) = \sigma_k(x_1, \ldots, \widehat{x_i}, \ldots, x_g) \frac{y_i}{\prod_{j \ne i}(x_i - x_j)}.$$

Proposition. D_k *are invariant and form a basis of* $\mathcal{L}(\mathrm{Jac}(C))$.

This is proved by differentiating the formula

$$f(x) - V^2(x) = 4U(x)W(x)$$

and then applying some "well-known" identities.

Logarithmic derivative

Let $\mathcal{G}$ be an extension of $\mathcal{F}$ and fix a reduced divisor

$$\eta = (\eta_1, \xi_1) + \cdots + (\eta_g, \xi_g) - g\infty \in \mathrm{Jac}(C)_{\mathcal{G}}.$$

We wish to compute

$$\ell\delta\eta \in \mathcal{L}(\mathrm{Jac}(C)),$$

i.e. find $A_0, \ldots, A_{g-1} \in \mathcal{G}$ with

$$\ell\delta\eta = \sum_{k=0}^{g-1} (-1)^k A_k D_{g-1-k}$$

We can then identify $\ell\delta\eta$ with the g-tuple

$$\ell\delta\eta = (A_0, \ldots, A_{g-1}).$$

By definition

$$(\ell\delta(\eta)(x_i))(\eta) = (x_i(\eta))' = \eta_i',$$

so

$$\begin{aligned}\eta_i' &= \sum_{k=0}^{g-1} (-1)^k A_k \left(D_{g-1-k}(x_i)\right)(\eta) \\ &= \frac{\xi_i}{\prod_{j\neq i}(\eta_i - \eta_j)} \sum_{k=0}^{g-1} (-1)^k \sigma_{g-1-k}(\eta_1, \ldots, \widehat{\eta_i}, \ldots, \eta_g) A_k.\end{aligned}$$

If A_k is replaced by η_ℓ^k, the sum on the right is

$$\begin{aligned}&\textstyle\sum_k (-1)^k \sigma_{g-1-k}(\eta_1, \ldots, \widehat{\eta_i}, \ldots, \eta_g)\eta_\ell^k \\ &= \textstyle\prod_{j\neq i}(\eta_\ell - \eta_j) = \begin{cases} \prod_{j\neq i}(\eta_i - \eta_j) & \text{if } \ell = i \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Therefore

$$A_k = \sum_{i=1}^{g} \frac{\eta_i'}{\xi_i}\, \eta_i^k$$

Strongly normal extensions

Proposition. *Suppose that η_i, ξ_i satisfy*

1. $\xi_i^2 = f(\eta_i)$, *for* $i = 1, \ldots, g$, *and*
2. $A_k = \sum_{i=1}^{g} \frac{\eta_i'}{\xi_i}\, \eta_i^k \in \mathcal{F}$ *for* $k = 0, \ldots, g-1$.

Then $\mathcal{F}(\eta_1, \xi_1, \ldots, \eta_g, \xi_g)_{\mathrm{sym}}$ is a strongly normal extension of $\mathcal{F}$ whose Galois group is a subgroup of $\mathrm{Jac}(C)$.

For $g = 1$ we get

$$A_0 = \frac{\eta'}{\xi}$$

which is "well-known" and can be rewritten

$$\eta'^2 = A_0^2\, \xi^2 = A_0^2\, f(\eta).$$

For $g = 2$ we get

$$A_0 = \frac{\eta_1'}{\xi_1} + \frac{\eta_2'}{\xi_2}$$

$$A_1 = \frac{\eta_1'}{\xi_1}\, \eta_1 + \frac{\eta_2'}{\xi_2}\, \eta_2.$$

I have no idea how to simplify this.

Kleinian $\wp$-functions

Baker [1] is the standard reference for this material. Buchstaber et al. [3] is more readible, but less complete.

Here $\mathbf{u} = (u_1, \ldots, u_g)$ are complex variables.

Definition. The hyperelliptic Kleinian σ-function is defined by the formula

$$\sigma(\mathbf{u}) = C[e^{\mathbf{u}^{\mathrm{T}}\chi\mathbf{u}}\theta((2\omega)^{-1}\mathbf{u} - \mathbf{K}_a \mid \tau)]e^{2i\pi\mathbf{q}'^{\mathrm{T}}\{-(2\omega)^{-1}\mathbf{u}+\frac{1}{2}\tau\mathbf{q}'-\mathbf{q}\}}.$$

Buchstaber et. al. [3, pp. 8 and 9] or Baker [1, p. 24 ff.].

Definition. For $1 \leq i, j \leq g$ define

$$\wp_{ij}(\mathbf{u}) = -\frac{\partial^2 \ln \sigma(\mathbf{u})}{\partial u_i \partial u_j}.$$

Buchstaber et. al [3, p. 9] or Baker [1, p. 36].

Let $x_1(\mathbf{u}), \ldots, x_g(\mathbf{u})$ be solutions of the equation

$$P(X; \mathbf{u}) = X^g - \wp_{g,g}(\mathbf{u})X^{g-1} - \wp_{g,g-1}(\mathbf{u})X^{g-2} - \cdots - \wp_{g,1}(\mathbf{u}) = 0,$$

and define

$$y_i(\mathbf{u}) = -\frac{\partial P(X; \mathbf{u})}{\partial u_g}(x_i).$$

Proposition. *$(x_i, y_i) \in C_1$ and, for $k = 0, \ldots, g-1$,*

$$\sum_{i=1}^{g} \frac{x_i^k(\mathbf{u})}{y_i(\mathbf{u})} \frac{\partial x_i(\mathbf{u})}{\partial u_j} = \begin{cases} 1 & \text{if } j = k+1, \\ 0 & \text{otherwise.} \end{cases}$$

Buchstaber et al. [3, p. 11].

Fix a differential field $\mathcal{F}$ consisting of functions of a single complex variable x, for example $\mathcal{F} = \mathbb{C}(x)$.

Suppose that $\mathbf{a} = (a_0, \ldots, a_{g-1})$ where a_i is a function of x (not necessarily in $\mathcal{F}$). Let $\eta_i = x_i(\mathbf{a})$ and $\xi_i = y_i(\mathbf{a})$. If

$$\ell\delta\eta = (A_0, \ldots, A_{g-1}),$$

then, for $k = 0, \ldots, g-1$,

$$A_k = \sum_{i=1}^{g} \frac{\eta_i'}{\xi_i}\,\eta_i^k = \sum_{i=1}^{g} \frac{\eta_i^k}{\xi_i}\left(\sum_{j=1}^{g} \frac{\partial x_i(\mathbf{u})}{\partial u_j}\right)(\mathbf{a})\,a_{j-1}'$$

$$= \sum_{j=1}^{g}\left(\sum_{i=1}^{g} \frac{x_i^k(\mathbf{u})}{y_i(\mathbf{u})}\frac{\partial x_i(\mathbf{u})}{\partial u_j}\right)(\mathbf{a})\,a_{j-1}'$$

$$= a_k'$$

Proposition. *Suppose that $a_i' \in \mathcal{F}$. Then $\mathcal{G} = \mathcal{F}(\eta)_{\mathrm{sym}}$ is a strongly normal extension of $\mathcal{F}$ whose Galois group is a subgroup of* $\mathrm{Jac}(C)$.

References

[1] H. F. Baker, *An introduction to the theory of multiply periodic functions*, Cambridge University Press, Cambridge, England, 1907.

[2] Laurent Bertrand, *Computing a hyperelliptic integral using arithmetic in the Jacobian of the curve*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), 275–298. MR 96m:14074

[3] V. M. Buchstaber, V. Z. Enolskiĭ, and D. V. Leĭ kin, *Hyperelliptic Kleinian functions and applications*, Solitons, Geometry, and Topology: on the Crossroad, Amer. Math. Soc. Transl. Ser. 2, vol. 179, Amer. Math. Soc., Providence, RI, 1997, pp. 1–33. MR 98b:14029

[4] David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101. MR 88f:11118

[5] P. J. Cassidy, *Differential algebraic groups*, Amer. J. Math. **94** (1972), 891–954. MR 50 #13058

[6] Neal Koblitz, *Algebraic aspects of cryptography, with an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato*, Algorithms and Computation in Mathematics, vol. 3, Springer-Verlag, Berlin, 1998, ISBN 3-540-63446-0. MR 2000a:94012

[7] E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1973. MR 58 #27929

[8] J. Kovacic, *The inverse problem in the Galois theory of differential fields*, Ann. of Math. (2) **89** (1969), 583–608. MR 39 #5535

[9] ———, *On the inverse problem in the Galois theory of differential fields. II.*, Ann. of Math. (2) **93** (1971), 269–284. MR 44 #2732

[10] David Mumford, *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston Inc., Boston, MA, 1984, ISBN 0-8176-3110-0. MR 86b:14017

[11] V. Kumar Murty, *The addition law on hyperelliptic Jacobians*, Currents Trends in Number Theory (Allahabad, 2000), Hindustan Book Agency, New Delhi, 2002, pp. 101–110. MR 2003h:14037