

Abelians and their application to an elementary construction of Jacobians

Greg W. Anderson

School of Mathematics, Univ. of Minnesota, Minneapolis, MN 55455, USA

Abstract

The *abeliant* is a polynomial rule which to each n by n by $n + 2$ array with entries in a commutative ring with unit associates an n by n matrix with entries in the same ring. The theory of abelians, first introduced in an earlier paper of the author, is simplified and extended here. Now let J be the Jacobian of a nonsingular projective algebraic curve defined over an algebraically closed field. With the aid of the theory of abelians we obtain explicit defining equations for J and its group law.

1 Introduction

Let C be a nonsingular projective algebraic curve defined over an algebraically closed field k and let J be the Jacobian of C . The point of the paper is to give an elementary construction of J , i. e., to obtain by purely algebraic and relatively simple means explicit defining equations for J and its group law. For historical perspective see (Milne 1986). Our construction is similar in spirit to that of (Mumford Tata Lectures II), but differs from the latter in (at least) two important respects. Firstly, we need not assume that C is hyperelliptic. Secondly, we obtain a description of J not as a glued-together collection of affine varieties, but rather as a projective variety.

Our construction of J is based in large part on the notion of *abeliant* introduced in the author's earlier paper (Anderson 1997). The abeliant is just a polynomial rule which to each n by n by $n + 2$ array with entries in a commutative ring with unit associates an n by n matrix with entries in the same ring. We simplify and extend the theory of abelians in this paper (§2). One of the new results obtained here is an expansion of each entry of the abeliant as a sum indexed by four permutations of n letters (§2.8).

Email address: gwanders@math.umn.edu (Greg W. Anderson).

Our construction of J proceeds in three main stages. The first stage is to derive from the theory of abeliants a theory of *abstract Abel maps* (§3). The first stage is more or less pure multilinear algebra and has *a priori* nothing to do with algebraic curves. The abstract Abel map is roughly analogous to the Plücker embedding, but with this important difference: it collapses not GL_n -orbits but rather $\mathrm{GL}_n \times \mathrm{GL}_n$ -orbits to lines. In the second stage of the construction of J we set up a representation of divisor classes of C of sufficiently high degree by square rank one matrices with entries in the function field of C (§4.2) and then set up corresponding matrix representations of addition and subtraction of divisor classes (§4.3). Since the matrix representing a divisor class is well-defined only up to $\mathrm{GL}_n \times \mathrm{GL}_n$ -equivalence, we have to solve a problem in the invariant theory of $\mathrm{GL}_n \times \mathrm{GL}_n$ to complete the construction of J . Of course it is precisely this sort of problem that the theory of abstract Abel maps is designed to solve. Thus the third and final stage of the construction of J comes down to interpreting the abstract Abel map in certain special cases associated to C as *the* Abel map (Theorem 4.4.6).

The explicit elementary point of view on hyperelliptic Jacobians developed by Mumford and many others has been quite useful in number theory and computer science. To give just two examples of applications, we cite the papers (Flynn Poonen Schaefer 1997) and (Adleman DeMarrais Huang 1999). The first is a study of the rational points on a certain curve of genus 2 connected with iteration of quadratic polynomials; the second is a cryptologically motivated study of the discrete logarithm problem in Jacobians of hyperelliptic curves defined over finite fields. We expect the explicit elementary point of view on not-necessarily-hyperelliptic Jacobians developed here to be analogously useful. A particularly interesting problem that might be approachable from our point of view is that of implementing the algorithm of (Pila 1990, Theorem D) for finding ℓ^{th} roots of unity modulo p ; heretofore the sticking point has been the lack of a sufficiently explicit model for the Jacobian of the Fermat curve of degree ℓ .

2 Abeliants

We review, simplify and refine the theory of *abeliants* introduced in the author's previous paper (Anderson 1997). *Rings* are commutative with unit.

2.1 Definition

Given an n by n matrix X with entries in some ring, let X^* denote the transpose of the matrix of cofactors of X , i. e., the n by n matrix with entry

in position ji equal to $(-1)^{i+j}$ times the determinant of the matrix obtained by striking row i and column j from X ; we then have

$$X^*X = XX^* = \text{diag} \left(\underbrace{\det X, \dots, \det X}_n \right).$$

Here and elsewhere $\text{diag}(x_1, \dots, x_n)$ denotes the n by n diagonal matrix with diagonal entries x_1, \dots, x_n . Now let

$$\{X^{(\ell)}\}_{\ell=0}^{n+1}$$

be a family of n by n matrices with entries in a ring R and let

$$\{s_i\}_{i=1}^n \cup \{t_j\}_{j=1}^n$$

be a family of independent variables. Following (Anderson 1997, p. 496), we define the *abeliant*

$$\text{abel} \left(X^{(0)}, \dots, X^{(n+1)} \right) \quad \left(\text{abbreviated notation: } \text{abel}_{\ell=0}^{n+1} X^{(\ell)} \right)$$

of the given family of matrices to be the n by n matrix the entry of which in position ij is the coefficient with which the monomial

$$s_i^{-1} t_j^{-1} \cdot \prod_{a=1}^n s_a \cdot \prod_{b=1}^n t_b = s_1 \cdots \widehat{s}_i \cdots s_n t_1 \cdots \widehat{t}_j \cdots t_n \quad (1)$$

appears in the expansion of the expression

$$\text{trace} \left(X^{(0)} \left(\sum_{b=1}^n t_b X^{(b)} \right)^* X^{(n+1)} \left(\sum_{a=1}^n s_a X^{(a)} \right)^* \right) \quad (2)$$

as an R -linear combination of monomials in the s 's and t 's.

2.2 Basic properties

Let $\{X^{(\ell)}\}_{\ell=0}^{n+1}$ be a family of n by n matrices with entries in a ring R . For any square matrices X and Y with entries in a ring we have

$$\text{trace}(XY) = \text{trace}(YX), \quad (XY)^* = Y^*X^*.$$

It follows after a short calculation that

$$\text{abel}_{\ell=0}^{n+1} \left(UX^{(\ell)}V \right) = (\det U)^2 (\det V)^2 \text{abel}_{\ell=0}^{n+1} X^{(\ell)} \quad (3)$$

for all n by n matrices U and V with entries in R . For any square matrix X with entries in a ring we have

$$\text{trace}(X^T) = \text{trace}(X), \quad (X^*)^T = (X^T)^*$$

where X^T denotes the transpose of X . It follows after a short calculation that

$$\text{abel}_{\ell=0}^{n+1} X^{\langle(0|n+1)\ell\rangle} = \left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)}\right)^T = \text{abel}_{\ell=0}^{n+1} \left(X^{(\ell)}\right)^T \quad (4)$$

where $\langle 0 | n + 1 \rangle$ denotes the permutation of $\{0, \dots, n + 1\}$ exchanging 0 and $n + 1$ and fixing all other elements. We claim that

$$\left(\text{abel}_{\ell=0}^{n+1} X^{(\pi\ell)}\right)_{ij} = \left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)}\right)_{\pi i, \pi j} \quad (5)$$

where π is any permutation of $\{0, \dots, n + 1\}$ fixing 0 and $n + 1$. We claim further that for $n \geq 2$ we have

$$\left(\text{abel}_{\ell=0}^{n+1} X^{\langle[1 \mapsto 2]\ell\rangle}\right)_{12} = \left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)}\right)_{11} \quad (6)$$

where $[1 \mapsto 2]$ denotes the mapping of $\{0, \dots, n + 1\}$ to itself sending 1 to 2 and fixing all other elements. Since the proofs of (5) and (6) are similar, we supply a proof only for (6). To abbreviate notation let monomial (1) be denoted by m_{ij} , let expression (2) be denoted by F , and let

$$s^\mu t^\nu = \prod_{a=1}^n s_a^{\mu_a} \cdot \prod_{b=1}^n t_b^{\nu_b}$$

be a monomial in the s 's and t 's. Further, let $[1 \mapsto 2]^*$ be the unique R -algebra endomorphism of the polynomial ring $R[s_1, \dots, s_n, t_1, \dots, t_n]$ such that

$$[1 \mapsto 2]^* s_a = \begin{cases} 0 & \text{if } a = 1, \\ s_1 + s_2 & \text{if } a = 2, \\ s_a & \text{if } a \geq 3, \end{cases} \quad [1 \mapsto 2]^* t_b = \begin{cases} 0 & \text{if } b = 1, \\ t_1 + t_2 & \text{if } b = 2, \\ t_b & \text{if } b \geq 3, \end{cases}$$

for $a, b = 1, \dots, n$. Now the coefficient with which the monomial m_{12} (resp. m_{11}) appears in the expansion of $[1 \mapsto 2]^* F$ (resp. F) as an R -linear combination of monomials in the s 's and t 's admits interpretation as the left (resp. right) side of (6). But the coefficients in question are equal because

$$[1 \mapsto 2]^* s^\mu t^\nu = \begin{cases} m_{11} + m_{12} + m_{21} + m_{22} & \text{if } s^\mu t^\nu = m_{11}, \\ \text{a polynomial in which } m_{12} \text{ does not appear} & \text{if } s^\mu t^\nu \neq m_{11}. \end{cases}$$

Thus claim (6) is proved.

2.3 Evaluation in a special case

Let X , L , M , and Q be n by n matrices with entries in a ring R , where L , M and Q are diagonal. We write $Q = \text{diag}(q_1, \dots, q_n)$. Let $e^{(\ell)}$ (resp. $f^{(\ell)}$) be the ℓ^{th} column (resp. row) of the n by n identity matrix and put

$$E = \left(e^{(1)} + \dots + e^{(n)} \right) \left(f^{(1)} + \dots + f^{(n)} \right) = \begin{bmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{bmatrix}.$$

We claim that

$$\text{abel}(X, q_1 e^{(1)} f^{(1)}, \dots, q_n e^{(n)} f^{(n)}, LEM) = MQ^* X Q^* L. \quad (7)$$

For the proof we write

$$S = \sum_{i=1}^n s_i e^{(i)} f^{(i)} = \text{diag}(s_1, \dots, s_n), \quad T = \sum_{j=1}^n t_j e^{(j)} f^{(j)} = \text{diag}(t_1, \dots, t_n)$$

where, as above, $s_1, \dots, s_n, t_1, \dots, t_n$ are independent variables. The identity

$$\begin{aligned} & \text{trace} \left(X \left(\sum_{b=1}^n q_b t_b e^{(b)} f^{(b)} \right)^* LEM \left(\sum_{a=1}^n q_a s_a e^{(a)} f^{(a)} \right)^* \right) \\ &= \text{trace}(S^* M Q^* X Q^* L T^* E) \end{aligned}$$

is easily verified and suffices to prove the claim.

2.4 Discriminants

Let $\{X^{(\ell)}\}_{\ell=1}^{n+1}$ be a family of n by n matrices with entries in a ring R . We define the *discriminant*

$$\Delta \left(X^{(1)}, \dots, X^{(n+1)} \right) \quad (\text{abbreviated notation: } \Delta_{\ell=1}^{n+1} X^{(\ell)})$$

of the given family of matrices to be the product

$$\left(\det \left(\sum_{\ell=1}^n X^{(\ell)} \right) \right)^{2n-2} \cdot \prod_{i=1}^n \left(\det \left(\sum_{\ell \in \{1, \dots, n+1\} \setminus \{i\}} X^{(\ell)} \right) \right)^2.$$

As becomes clear presently, this nonstandard notion of discriminant is closely allied with the notion of abelian. We have

$$\Delta_{\ell=1}^{n+1} U X^{(\ell)} V = (\det U)^{4n-2} (\det V)^{4n-2} \Delta_{\ell=1}^{n+1} X^{(\ell)} \quad (8)$$

for all n by n matrices U and V with entries in R . We have

$$\Delta_{\ell=1}^{n+1} X^{(\ell)} = \Delta_{\ell=1}^{n+1} (X^{(\ell)})^T. \quad (9)$$

If there exist factorizations

$$X^{(\ell)} = u^{(\ell)} v^{(\ell)} \quad \text{for } \ell = 1, \dots, n+1$$

where $u^{(\ell)}$ (resp. $v^{(\ell)}$) is a column (resp. row) vector with entries in R , then we have

$$\det \left(\sum_{\ell \in \{1, \dots, n+1\} \setminus \{i\}} X^{(\ell)} \right) = \left| u^{(1)} \dots \widehat{u^{(i)}} \dots u^{(n+1)} \right| \cdot \begin{vmatrix} v^{(1)} \\ \vdots \\ \widehat{v^{(i)}} \\ \vdots \\ v^{(n+1)} \end{vmatrix}$$

for $i = 1, \dots, n+1$ and hence, given matrices

$$L, M, Q = \text{diag}(q_1, \dots, q_n), e^{(\ell)}, f^{(\ell)}, E$$

with entries in R as in (7) above, we have

$$\Delta \left(q_1 e^{(1)} f^{(1)}, \dots, q_n e^{(n)} f^{(n)}, LEM \right) = (\det Q)^{4n-4} (\det L)^2 (\det M)^2 \quad (10)$$

after a straightforward calculation we can safely omit.

2.5 The key relations

Let $\{X^{(\ell)}\}_{\ell=0}^{n+1}$ be a family of n by n matrices with entries in a ring R . Assume that we have factorizations

$$X^{(\ell)} = u^{(\ell)} v^{(\ell)} \quad \text{for } \ell = 1, \dots, n+1$$

where $u^{(\ell)}$ (resp. $v^{(\ell)}$) is a column (resp. row) vector with entries in R . For the moment we do not assume that $X^{(0)}$ has such a factorization. We claim that

$$\text{abel}_{\ell=0}^{n+1} X^{(\ell)} = MU^* X^{(0)} V^* L, \quad \Delta_{\ell=1}^{n+1} X^{(\ell)} = \det(MU^*)^2 \det(V^* L)^2 \quad (11)$$

where

$$M = \text{diag} \left((v^{(n+1)}V^*)_{\mathbf{1}}, \dots, (v^{(n+1)}V^*)_{\mathbf{n}} \right), \quad U = \begin{bmatrix} u^{(1)} & \dots & u^{(n)} \end{bmatrix},$$

$$V = \begin{bmatrix} v^{(1)} \\ \vdots \\ v^{(n)} \end{bmatrix}, \quad L = \text{diag} \left((U^*u^{(n+1)})_{\mathbf{1}}, \dots, (U^*u^{(n+1)})_{\mathbf{n}} \right).$$

The relations (11) are key to all applications of the abelian. Let u (resp. v) be any column (resp. row) vector of length n with entries in R . We have

$$(U^*u)_i = (-1)^{i+1} \left| u \ u^{(1)} \ \dots \ \widehat{u^{(i)}} \ \dots \ u^{(n)} \right|, \quad (vV^*)_j = (-1)^{1+j} \left| \begin{array}{c} v \\ v^{(1)} \\ \vdots \\ \widehat{v^{(j)}} \\ \vdots \\ v^{(n)} \end{array} \right| \quad (12)$$

by Cramer's Rule and hence

$$(U^*u)_i (vV^*)_i = \det \left(uv + \sum_{\ell \in \{1, \dots, n\} \setminus \{i\}} X^{(\ell)} \right). \quad (13)$$

In particular, we have

$$\det U \cdot \det V = \det \left(\sum_{\ell=1}^n X^{(\ell)} \right), \quad (LM)_{ii} = \det \left(\sum_{\ell \in \{1, \dots, n+1\} \setminus \{i\}} X^{(\ell)} \right).$$

Repeated application of (13) proves the second part of (11). Now let $e^{(\ell)}$, $f^{(\ell)}$ and E be as in (7) above and put

$$D = \det U \cdot \det V.$$

We have

$$\begin{aligned}
& D^{2n-2} \text{abel}(X^{(0)}, u^{(1)}v^{(1)}, \dots, u^{(n)}v^{(n)}, u^{(n+1)}v^{(n+1)}) \\
&= (\det U^*)^2 (\det V^*)^2 \text{abel}(X^{(0)}, u^{(1)}v^{(1)}, \dots, u^{(n)}v^{(n)}, u^{(n+1)}v^{(n+1)}) \\
&= \text{abel}(U^*X^{(0)}V^*, De^{(1)}f^{(1)}, \dots, De^{(n)}f^{(n)}, LEM) \\
&= D^{2n-2} MU^*X^{(0)}V^*L
\end{aligned}$$

by transformation law (3) and special case (7). The preceding calculation proves the first part of (11) provided that cancellation of the factor D^{2n-2} can be justified. But there is no loss of generality in assuming that the entries of the matrix $X^{(0)}$ and of the vectors $u^{(\ell)}$ and $v^{(\ell)}$ together constitute a family of independent variables, and that R is the ring generated by these variables over the integers; then R is an integral domain, $D \neq 0$, cancellation of the factor D^{2n-2} is permitted, and the first part of (11) is proved. The proof of (11) is complete.

An amplifying remark is now in order. If there exist factorizations

$$X^{(\ell)} = u^{(\ell)}v^{(\ell)} \quad \text{for } \ell = 0, \dots, n+1$$

with $u^{(\ell)}$ (resp. $v^{(\ell)}$) a column (resp. row) vector with entries in R (notice that $\ell = 0$ is now included) then the first part of key relation (11) takes the form

$$\begin{aligned}
& \left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)} \right)_{ij} \\
&= \begin{vmatrix} \widehat{v^{(0)}} \\ \vdots \\ \widehat{v^{(i)}} \\ \vdots \end{vmatrix} \cdot \left| \dots \widehat{u^{(i)}} \dots \widehat{u^{(n+1)}} \right| \cdot \begin{vmatrix} \vdots \\ \widehat{v^{(j)}} \\ \vdots \\ \widehat{v^{(n+1)}} \end{vmatrix} \cdot \left| \widehat{u^{(0)}} \dots \widehat{u^{(j)}} \dots \right| \end{vmatrix} \quad (14)
\end{aligned}$$

by (12). Identity (14) is the method we almost always use for evaluating abelians of algebro-geometric interest.

2.6 Abelians of matrices of rank ≤ 1

We say that a matrix X with entries in some ring is *of rank ≤ 1* if every two by two submatrix has vanishing determinant. Now let $\{X^{(\ell)}\}_{\ell=0}^{n+1}$ be a family

of n by n matrices with entries in a ring R . Assume that $n \geq 2$ and that

$$X^{(\ell)} \text{ is of rank } \leq 1 \text{ for } \ell = 0, \dots, n+1.$$

For distinct $i, j \in \{0, \dots, n+1\}$ put

$$D_{ij} = \left(\sum_{\ell \in \{0, \dots, n+1\} \setminus \{i, j\}} X^{(\ell)} \right).$$

For $a \in \{0, \dots, n+1\}$, let $[0 \mapsto a]$ denote the mapping of $\{0, \dots, n+1\}$ to itself sending 0 to a and fixing all other elements. For distinct $a, b \in \{0, \dots, n+1\}$ let $\langle a \mid b \rangle$ denote the permutation of $\{0, \dots, n+1\}$ exchanging a and b and fixing all other elements. We make the following claims:

$$\text{abel}_{\ell=0}^{n+1} X^{(\ell)} \text{ is a matrix of rank } \leq 1. \quad (15)$$

$$\left(\text{abel}_{\ell=0}^{n+1} X^{([0 \mapsto a] \ell)} \right)_{ij} = 0 \quad \text{unless } a \in \{0, n+1\} \text{ or } i = j = a. \quad (16)$$

$$\left(\text{abel}_{\ell=0}^{n+1} X^{([0 \mapsto n+1] \ell)} \right)_{ij} = D_{0i} D_{0j} \quad (17)$$

$$\left(\text{abel}_{\ell=0}^{n+1} X^{([0 \mapsto a] \ell)} \right)_{aa} = D_{0a} D_{0, n+1} \quad (18)$$

$$\left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)} \right)_{aa} = D_{0a} D_{a, n+1} \quad (19)$$

$$\begin{aligned} \Delta_{\ell=1}^{n+1} X^{(\ell)} &= \left(\text{abel}_{\ell=0}^{n+1} X^{(\langle 2|n+1 \rangle \langle 0|1 \rangle \ell)} \right)_{11} \\ &\cdot \left(\text{abel}_{\ell=0}^{n+1} X^{(\langle 0|1 \rangle \ell)} \right)_{11} \cdot \left(\text{abel}_{\ell=0}^{n+1} X^{(\langle 0|2 \rangle \ell)} \right)_{22} \\ &\cdot \prod_{a=3}^n \left(\text{abel}_{\ell=0}^{n+1} X^{(\langle 0|a \rangle \ell)} \right)_{aa}^2 \end{aligned} \quad (20)$$

Let $\{\tilde{X}^{(\ell)}\}_{\ell=0}^{n+1}$ be a family of matrices the entries of which constitute a family of $(n+2) \cdot n \cdot n$ independent variables. Without loss of generality we may assume that R is the quotient of the ring generated by the entries of the $\tilde{X}^{(\ell)}$ over the integers by the ideal I generated by the determinants of all two by two submatrices of the $\tilde{X}^{(\ell)}$, and we may assume that $X^{(\ell)} \equiv \tilde{X}^{(\ell)} \pmod{I}$ for all indices ℓ . As is well known the ideal I is prime and hence the ring R is an integral domain. Over the fraction field of R we have factorizations $X^{(\ell)} = u^{(\ell)} v^{(\ell)}$ with $u^{(\ell)}$ (resp. $v^{(\ell)}$) a column (resp. row) vector. The first five claims now follow immediately from relation (14). The last claim follows from the penultimate one after a straightforward calculation we can safely omit. Thus all claims are proved.

2.7 Iterated abelians

Let $\{X^{(\ell)}\}_{\ell=-n-1}^{n+1}$ be a family of n by n matrices with entries in a ring R . Assume that all the matrices $X^{(\ell)}$ are of rank ≤ 1 . We claim that

$$\text{abel}_{\ell=0}^{n+1} \text{abel} \left(X^{(-\ell)}, X^{(1)}, \dots, X^{(n+1)} \right) = \Delta_{\ell=1}^{n+1} X^{(\ell)} \cdot \text{abel}_{\ell=0}^{n+1} X^{(-\ell)}. \quad (21)$$

Arguing in much the same fashion as in the proof of fact (15) and its companions, we may assume without loss of generality that there exist factorizations $X^{(\ell)} = u^{(\ell)} v^{(\ell)}$ over R with $u^{(\ell)}$ (resp. $v^{(\ell)}$) a column (resp. row) vector. Then the claim follows by transformation law (3) and key relation (11).

2.8 Expansion of the abeliant

Let $\{X^{(\ell)}\}_{\ell=0}^{n+1}$ be a family of n by n matrices with entries in a ring R . By definition we have

$$\left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)} \right)_{ij} = \sum_{e,f,g,h=1}^n X_{fg}^{(0)} Y_{gh}^{(j)} X_{he}^{(n+1)} Y_{ef}^{(i)} \quad (22)$$

where $Y_{ef}^{(i)}$ denotes the coefficient with which the monomial $s_1 \cdots \widehat{s}_i \cdots s_n$ appears in the expansion of the matrix entry

$$\left(\sum_{a=1}^n s_a X^{(a)} \right)_{ef}^*$$

as an R -linear combination of monomials in the s 's. Now for any n by n matrix X with entries in a ring we have

$$X_{ef}^* = \sum_{\pi e=f} (-1)^\pi \prod_{c \neq e} X_{\pi c, c}$$

where the sum is extended over permutations π of $\{1, \dots, n\}$ such that $\pi e = f$, the product is extended over $c \in \{1, \dots, n\} \setminus \{e\}$ and $(-1)^\pi$ is the sign of π . It follows that

$$Y_{ef}^{(i)} = \sum_{\substack{\pi e=f \\ \theta e=i}} (-1)^\pi \prod_{c \neq e} X_{\pi c, c}^{(\theta c)}$$

where the sum is extended over permutations π and θ of $\{1, \dots, n\}$ such that $\pi e = f$ and $\theta e = i$ and the product is extended over $c \in \{1, \dots, n\} \setminus \{e\}$.

Substituting $\theta = \psi^{-1}$, $\pi = \tau\psi^{-1}$, $c = \psi a$ and making the simplification $(-1)^{\tau\psi^{-1}} = (-1)^{\tau\psi}$, we obtain the expansion

$$Y_{ef}^{(i)} = \sum_{\substack{\psi i=e \\ \tau i=f}} (-1)^{\tau\psi} \prod_{a \neq 0, i, n+1} X_{\tau a, \psi a}^{(a)}$$

where the sum is extended over permutations τ, ψ of $\{1, \dots, n\}$ such that $\psi i = e$ and $\tau i = f$ and the product is extended over $a \in \{1, \dots, n\} \setminus \{i\}$. Finally, after substituting into (22), we obtain the expansion

$$\begin{aligned} & \left(\text{abel}_{\ell=0}^{n+1} X^{(\ell)} \right)_{ij} \\ &= \sum_{\sigma, \phi, \tau, \psi} (-1)^{\sigma\phi\tau\psi} X_{\tau i, \phi j}^{(0)} \cdot \prod_{b \neq 0, j, n+1} X_{\sigma b, \phi b}^{(b)} \cdot X_{\sigma j, \psi i}^{(n+1)} \cdot \prod_{a \neq 0, i, n+1} X_{\tau a, \psi a}^{(a)} \end{aligned} \quad (23)$$

where the sum is extended over permutations σ, ϕ, τ, ψ of $\{1, \dots, n\}$ and the products are extended over $a \in \{1, \dots, n\} \setminus \{i\}$ and $b \in \{1, \dots, n\} \setminus \{j\}$.

3 The abstract Abel map

We abstract and refine the part of the theory of (Anderson 1997) having to do with invariants of $\text{GL}_n \times \text{GL}_n$.

3.1 Segre matrices

3.1.1 Basic data

Throughout §3 we work with data

$$k, n, A, L$$

consisting of

- an algebraically closed field k ,
- an integer $n \geq 2$,
- a finitely generated k -algebra A without zero divisors, and
- a finite-dimensional k -subspace $L \subset A$.

Here and below k -algebras are commutative with unit. We often refer to elements of k as *constants* or *scalars*.

3.1.2 Matrix terminology

Let X and Y be matrices with entries in a k -algebra R . We say that X is k -general if there exists both a row of X with k -linearly independent entries and a column of X with k -linearly independent entries. As in §2, we say that X is of $\text{rank} \leq 1$ if every two by two submatrix has vanishing determinant. We say that X and Y are k -equivalent if there exist square matrices Φ and Ψ with entries in k such that $\det \Phi \neq 0$, $\det \Psi \neq 0$, the product $\Phi X \Psi$ is defined, and $Y = \Phi X \Psi$. Also, given vectors x and y in a common vector space over k , we say that x is k -proportional to y if $x = cy$ for some nonzero scalar c .

3.1.3 Definition

A Segre matrix X is an object with the following properties:

- X is an n by n matrix with entries in L .
- X is of $\text{rank} \leq 1$.
- X is k -general.

If we need to draw attention to the basic data we say that X is of *type* (k, n, A, L) .

3.1.4 Key properties

Let X be a Segre matrix. The following hold:

- Any matrix with entries in A to which X is k -equivalent is a Segre matrix.
- The transpose X^T is a Segre matrix.
- There exists a factorization $X = uv$ where u (resp. v) is a column (resp. row) vector with entries in the fraction field of A .
- Given any such factorization $X = uv$, the entries of u (resp. v) are k -linearly independent.
- Given any two such factorizations $X = uv = u'v'$, there exists unique nonzero f in the fraction field of A such that $u' = fu$ and $v' = f^{-1}v$.

The proofs of these facts are very easy and therefore omitted. We take these facts for granted in all subsequent work with Segre matrices.

3.1.5 Goal

We aim to put the k -equivalence classes of Segre matrices into explicit bijective correspondence with the points of an explicitly defined projective algebraic variety over k . Our results are summarized by Theorem 3.7.6 below.

3.2 Examples of Segre matrices involving elliptic functions

3.2.1 The spaces Σ_N

For background on elliptic functions, see (Whittaker Watson, Chap. XX). Let $\sigma(z)$ be the Weierstrass σ -function attached to a lattice $\Lambda \subset \mathbb{C}$. By construction $\sigma(z)$ has simple zeroes on the lattice Λ and no other zeroes. For each nonnegative integer N , let Σ_N be the space of entire functions $f(z)$ such that the meromorphic function $f(z)/\sigma(z)^N$ is Λ -periodic. We have $\Sigma_0 = \mathbb{C}$ and for $N > 0$ we have $\dim_{\mathbb{C}} \Sigma_N = N$.

3.2.2 Specification of a type

Fix an integer $n \geq 2$. Clearly the \mathbb{C} -algebra $\bigoplus_{\ell=0}^{\infty} \Sigma_{2n\ell}$ is without zero-divisors. It can be shown that the \mathbb{C} -algebra $\bigoplus_{\ell=0}^{\infty} \Sigma_{2n\ell}$ is generated over \mathbb{C} by Σ_{2n} . It follows that the quadruple

$$\left(\mathbb{C}, n, \bigoplus_{\ell=0}^{\infty} \Sigma_{2n\ell}, \Sigma_{2n} \right) \quad (24)$$

is a type. We are going to classify Segre matrices of this type.

3.2.3 An analytic construction of Segre matrices

Let $\vec{\sigma}(z)$ be a row vector of length n with entries forming a \mathbb{C} -basis of Σ_n , e. g.

$$\vec{\sigma}(z) = \left[\sigma(z)^n \quad \sigma(z)^n \wp(z) \quad \sigma(z)^n \wp'(z) \quad \cdots \quad \sigma(z)^n \wp^{(n-2)}(z) \right],$$

where

$$\wp(z) = -\frac{d^2}{dz^2} \log \sigma(z)$$

is the Weierstrass \wp -function attached to the lattice Λ . It is not difficult to prove that for each $t \in \mathbb{C}$ the n by n matrix

$$\vec{\sigma}(z - t/n)^T \vec{\sigma}(z + t/n) \quad (25)$$

of entire functions of z is a Segre matrix of type (24) the \mathbb{C} -equivalence class of which depends only on $t \bmod \Lambda$, not on the choice of $\vec{\sigma}(z)$.

Proposition 3.2.4 *The map sending $t \in \mathbb{C}$ to the corresponding Segre matrix of the form (25) puts the complex torus \mathbb{C}/Λ in bijective correspondence with the family of \mathbb{C} -equivalence classes of Segre matrices of type (24).*

Proof. In any given fundamental domain for Λ a not-identically-vanishing function belonging to the space Σ_n has exactly n zeroes and moreover these zeroes sum to an element of Λ . Further, the family of functions Σ_n has no zero in common. Now let $X(z)$ be a matrix \mathbb{C} -equivalent to a matrix of the form (25). Then the functions in any given row of $X(z)$ have in any given fundamental domain for Λ exactly n common zeroes, and these must sum to t modulo Λ . Therefore the correspondence in question is one-to-one.

Now fix a Segre matrix $X(z)$ of type (24) arbitrarily. Choose in $X(z)$ a column $u(z)$ and a row $v(z)$, each with \mathbb{C} -linearly independent entries. Let $f(z)$ be the entry of $X(z)$ common to $u(z)$ and $v(z)$; then $f(z)$ does not vanish identically. Let p (resp. q) be the number of common zeroes of the entries of $u(z)$ (resp. $v(z)$) in any given fundamental domain for Λ . Any subspace of Σ_{2n} defined by prescribing $n+1$ zeroes in a given fundamental domain for Λ is $(n-1)$ -dimensional over \mathbb{C} ; this is a consequence of Riemann-Roch in genus one. Since the entries of $u(z)$ (resp. $v(z)$) are \mathbb{C} -linearly independent, it follows that $p \leq n$ (resp. $q \leq n$). Since every two by two submatrix of $X(z)$ has vanishing determinant, we have

$$X(z) = u(z)v(z)/f(z),$$

hence $f(z)$ divides every entry of the product $u(z)v(z)$, hence $p+q \geq 2n$, hence $p=q=n$, and hence the common zeroes of the entries of the matrix $u(z)v(z)$ coincide with the zeroes of $f(z)$.

For some complex numbers P_1, \dots, P_{2n} summing to 0 and some nonzero complex number C we have a factorization

$$f(z) = C\sigma(z - P_1) \cdots \sigma(z - P_{2n}).$$

Moreover, by re-indexing the points P_1, \dots, P_{2n} if necessary, we can arrange for the vectors

$$u^*(z) = \frac{u(z)}{C\sigma(z - P_1) \cdots \sigma(z - P_n)}, \quad v^*(z) = \frac{v(z)}{\sigma(z - P_{n+1}) \cdots \sigma(z - P_{2n})}$$

to have entries that are entire functions of z . Now put

$$t = -(P_1 + \cdots + P_n) = P_{n+1} + \cdots + P_{2n}.$$

Then the entries of the vector $u^*(z+t/n)$ (resp. $v^*(z-t/n)$) belong to Σ_n and hence, since \mathbb{C} -linearly independent, form a \mathbb{C} -basis for Σ_n . It follows that for some n by n matrices Φ and Ψ with entries in \mathbb{C} we have

$$u^*(z+t/n) = \Phi \vec{\sigma}(z)^T, \quad v^*(z-t/n) = \vec{\sigma}(z) \Psi, \quad \det \Phi \neq 0, \quad \det \Psi \neq 0.$$

Finally, we have

$$X(z) = \Phi \vec{\sigma}(z-t/n)^T \vec{\sigma}(z+t/n) \Psi,$$

i. e., $X(z)$ is \mathbb{C} -equivalent to a Segre matrix of the form (25). Therefore the correspondence in question is onto. \square

3.3 An ad hoc tensor formalism

3.3.1 Definition of $A^{\otimes \mathbb{Z}}$

Let $A^{\otimes \mathbb{Z}}$ be the tensor product over k of copies of A indexed by \mathbb{Z} , formed according to the definition (Jacquet-Langlands 1970, pp. 301-303). By that definition the k -algebra $A^{\otimes \mathbb{Z}}$ is generated by symbols of the form

$$\bigotimes_{i \in \mathbb{Z}} a_i \quad (a_i \in A, \quad a_i = 1 \text{ for } |i| \gg 0)$$

subject to obvious relations. Put

$$a^{(\ell)} := \bigotimes_{i \in \mathbb{Z}} \begin{cases} a & \text{if } i = \ell \\ 1 & \text{if } i \neq \ell \end{cases}$$

for all $a \in A$ and $\ell \in \mathbb{Z}$. More generally, given a matrix X with entries in A and $\ell \in \mathbb{Z}$ we define a matrix $X^{(\ell)}$ with entries in $A^{\otimes \mathbb{Z}}$ by the rule

$$\left(X^{(\ell)} \right)_{ij} = (X_{ij})^{(\ell)}.$$

For any subset $I \subseteq \mathbb{Z}$, let $A^{\otimes I}$ denote the k -subalgebra of $A^{\otimes \mathbb{Z}}$ generated by all elements of the form $a^{(\ell)}$ where $a \in A$ and $\ell \in I$. If I is a finite subset of \mathbb{Z} , then the k -algebra $A^{\otimes I}$ can naturally be identified with the usual tensor product over k of copies of A indexed by I . For any subset $I \subseteq \mathbb{Z}$, the k -algebra $A^{\otimes I}$ is characterized in the category of commutative k -algebras with unit by a universal property we need not belabor. We make the identifications

$$a^{(0)} = a$$

for all $a \in A$, thus equipping $A^{\otimes \mathbb{Z}}$ with the structure of A -algebra. Finally, note that the k -algebra $A^{\otimes \mathbb{Z}}$ is without zero divisors; this fact plays an extremely important role in the sequel.

3.3.2 Partial specializations of $A^{\otimes \mathbb{Z}}$

Let S be the set of k -algebra homomorphisms $A \rightarrow k$. For all $a \in A$ and $s \in S$ we denote the value in k of a at s by $a|_s$. More generally, given a matrix X with entries in A , we define a matrix $X|_s$ with entries in k by the rule

$$(X_{ij})|_s = (X|_s)_{ij}.$$

Now let I be a set of integers and let

$$\mathbf{s} = \{s_\ell\}_{\ell \in I} \in S^I$$

be any family of points of S indexed by I . We define the *partial specialization*

$$(a \mapsto a||_{\mathbf{s}}) : A^{\otimes \mathbb{Z}} \rightarrow A^{\otimes (\mathbb{Z} \setminus I)}$$

associated to the family \mathbf{s} to be the unique k -algebra homomorphism such that

$$a^{(\ell)}||_{\mathbf{s}} = \begin{cases} a|_{s_\ell} & \text{if } \ell \in I \\ a^{(\ell)} & \text{if } \ell \notin I \end{cases}$$

for all $a \in A$ and $\ell \in \mathbb{Z}$. More generally, given a matrix X with entries in $A^{\otimes \mathbb{Z}}$, we define a matrix $X||_{\mathbf{s}}$ with entries in $A^{\otimes (\mathbb{Z} \setminus I)}$ by the rule

$$(X||_{\mathbf{s}})_{ij} = (X_{ij})||_{\mathbf{s}}.$$

3.3.3 Derangements and their action on $A^{\otimes \mathbb{Z}}$

A *derangement* is by definition a map of the set \mathbb{Z} of integers to itself. The *support* of a derangement σ is by definition the set

$$\{\ell \in \mathbb{Z} \mid \sigma \ell \neq \ell\},$$

i. e., the set of integers actually moved by σ . For each derangement σ we define

$$\sigma_* : A^{\otimes \mathbb{Z}} \rightarrow A^{\otimes \mathbb{Z}}$$

to be the unique k -algebra homomorphism such that

$$\sigma_*(a^{(\ell)}) = a^{(\sigma \ell)}$$

for all $a \in A$ and $\ell \in \mathbb{Z}$ and more generally, given any matrix Z with entries in $A^{\otimes \mathbb{Z}}$, we define a matrix $\sigma_* Z$ with entries in $A^{\otimes \mathbb{Z}}$ by the rule

$$(\sigma_* Z)_{ij} = \sigma_*(Z_{ij}).$$

For any derangements σ and τ we have

$$\sigma_*\tau_* = (\sigma\tau)_*.$$

3.3.4 The bar operation

We define the *bar operation*

$$(a \mapsto \bar{a}) : A^{\otimes \mathbb{Z}} \xrightarrow{\sim} A^{\otimes \mathbb{Z}}$$

to be the unique k -algebra automorphism such that

$$\overline{a^{(\ell)}} = a^{(-\ell)}$$

for all $a \in A$ and $\ell \in \mathbb{Z}$. More generally, given a matrix Z with entries in $A^{\otimes \mathbb{Z}}$ we define \overline{Z} by the rule

$$(\overline{Z})_{ij} = \overline{Z}_{ij}.$$

The bar operation is none other than the automorphism of $A^{\otimes \mathbb{Z}}$ associated to the sign-reversing derangement $\ell \mapsto -\ell$. Since

$$\bar{a} = \overline{a^{(0)}} = a^{(0)} = a$$

for all $a \in A$, the bar operation is an A -algebra automorphism.

3.3.5 Special derangements

Given distinct integers i and j , let $\langle i \mid j \rangle$ be the unique derangement with support $\{i, j\}$; in other words, $\langle i \mid j \rangle$ exchanges i and j and fixes all other integers. Given integers i and j (possibly not distinct), let $[i \mapsto j]$ be the unique derangement with support contained in the set $\{i\}$ sending i to j ; in other words, $[i \mapsto j]$ maps i to j and fixes all other integers.

3.4 Criteria for k -generality

Lemma 3.4.1 *Let integers $\ell_1 < \dots < \ell_N$ be given. Let u be a column vector of length N with entries in A and put*

$$U = \begin{bmatrix} u^{(\ell_1)} & \dots & u^{(\ell_N)} \end{bmatrix}$$

thereby defining an N by N matrix with entries in $A^{\otimes \{\ell_1, \dots, \ell_N\}}$. The entries of the vector u are k -linearly dependent if and only if the determinant of the matrix U vanishes identically.

Proof.

(\Rightarrow) By row operations leaving the determinant unchanged we can transform U to a matrix with an identically vanishing row.

(\Leftarrow) We proceed by induction on N . The case $N = 1$ is trivial; assume now that $N > 1$. Without loss of generality we may assume that the determinant of every $N - 1$ by $N - 1$ submatrix of U is nonvanishing, for otherwise we are done by induction on N . Also without loss of generality we may assume that $(\ell_1, \dots, \ell_N) = (0, \dots, N - 1)$. Expanding U by minors of the first column we obtain a relation

$$a_1 u_1 + \dots + a_N u_N = 0 \quad (a_1, \dots, a_N \in A^{\otimes\{1, \dots, N-1\}}, \quad a_1 \cdots a_N \neq 0)$$

among the entries of u . By the Nullstellensatz there exists

$$\mathbf{s} = (s_1, \dots, s_{N-1}) \in S^{\{1, \dots, N-1\}}$$

such that

$$(a_1 \cdots a_N) \|\mathbf{s} = (a_1 \|\mathbf{s}) \cdots (a_n \|\mathbf{s}) \neq 0$$

and for any such \mathbf{s} we obtain by partial specialization a nontrivial k -linear relation

$$(a_1 u_1 + \dots + a_N u_N) \|\mathbf{s} = (a_1 \|\mathbf{s}) \cdot u_1 + \dots + (a_N \|\mathbf{s}) \cdot u_N = 0$$

among the entries of u . \square

Lemma 3.4.2 *Let integers $\ell_1 < \dots < \ell_n$ be given. Let X be an n by n matrix with entries in A of rank ≤ 1 . The matrix X is k -general if and only if $\det \left(\sum_{\nu=1}^n X^{(\ell_\nu)} \right) \neq 0$.*

Proof. We may assume without loss of generality that $(\ell_1, \dots, \ell_n) = (1, \dots, n)$. Let u be the j^{th} column of X and let v be the i^{th} row of X , where i and j are presently to be chosen in a useful way. Put

$$U = \begin{bmatrix} u^{(1)} & \dots & u^{(n)} \end{bmatrix}, \quad V = \begin{bmatrix} v^{(1)} \\ \vdots \\ v^{(n)} \end{bmatrix}.$$

We claim that

$$\det U \cdot \det V = \det \left(X^{(1)} + \dots + X^{(n)} \right) \cdot X_{ij}^{(1)} \cdots X_{ij}^{(n)}. \quad (26)$$

In any case we have

$$X_{ij} X = uv$$

since X is of rank ≤ 1 . If $X_{ij} = 0$, then both sides of (26) vanish. Suppose now that $X_{ij} \neq 0$. After localizing A suitably, we may assume that X_{ij} is a unit of A . Then we have

$$X^{(1)} + \cdots + X^{(n)} = u \operatorname{diag} \left(X_{ij}^{(1)}, \dots, X_{ij}^{(n)} \right)^{-1} v,$$

whence (26) after taking determinants on both sides and rearranging the resulting identity. The claim is proved.

To prove the implication (\Rightarrow) , we choose i and j so that the entries of u are k -linearly independent and the entries of v are k -linearly independent. Then the entry X_{ij} common to u and v is nonzero and the left side of (26) is nonvanishing by Lemma 3.4.1. It follows that the determinant in question does not vanish.

To prove the implication (\Leftarrow) , we choose i and j so that $X_{ij} \neq 0$. Then the right side of (26) is nonvanishing and hence neither $\det U$ or $\det V$ vanish. By Lemma 3.4.1 the entries of u are k -linearly independent and the entries of v are k -linearly independent. It follows that the matrix X is k -general. \square

Proposition 3.4.3 *Let X be an n by n matrix with entries in A of rank ≤ 1 . The following conditions are equivalent:*

$$X \text{ is } k\text{-general.} \tag{27}$$

$$\Delta_{\ell=1}^{n+1} X^{(\ell)} \neq 0. \tag{28}$$

$$\operatorname{abel}_{\ell=0}^{n+1} X^{(\ell)} \neq 0. \tag{29}$$

Proof. For distinct $i, j \in \{0, \dots, n+1\}$ put

$$D_{ij} = \det \left(\sum_{\ell \in \{0, \dots, n+1\} \setminus \{i, j\}} X^{(\ell)} \right).$$

Consider two more conditions:

$$D_{ij} \neq 0 \text{ for some distinct } i, j \in \{0, \dots, n+1\}. \tag{30}$$

$$D_{ij} \neq 0 \text{ for all distinct } i, j \in \{0, \dots, n+1\}. \tag{31}$$

We have implications

$$(31) \Rightarrow (28) \Rightarrow (30) \Rightarrow (27) \Rightarrow (31) \Rightarrow (29),$$

the first two by definition of the discriminant, the next two by Lemma 3.4.2, and the last by identity (19). To complete the proof it suffices to prove the

implication (29) \Rightarrow (30). Put $Z = \text{abel}_{\ell=0}^{n+1} X^{(\ell)}$ to abbreviate notation. By hypothesis there exist indices i and j such that $Z_{ij} \neq 0$. We then have

$$0 \neq Z_{ij} \cdot \langle 0 \mid n+1 \rangle_* Z_{ij} = Z_{ij} Z_{ji} = Z_{ii} Z_{jj} = D_{0i} D_{i,n+1} D_{0j} D_{j,n+1},$$

the first equality by identity (4), the second by fact (15) and the third by identity (19). Therefore condition (29) does indeed imply condition (30). \square

3.5 Normalization and self-similarity

3.5.1 Definitions

Let an n by n matrix X with entries in A of rank ≤ 1 be given. Let

$$\mathbf{s} = (s_1, \dots, s_{n+1}) \in S^{\{1, \dots, n+1\}}$$

be given. We say that X is \mathbf{s} -normalized under the following conditions:

$$\text{For } i, j, \ell = 1, \dots, n \text{ we have } X_{ij}|_{s_\ell} \neq 0 \text{ if and only if } i = j = \ell. \quad (32)$$

$$\text{For } i, j = 1, \dots, n \text{ we have } X_{ij}|_{s_{n+1}} = 1. \quad (33)$$

We say that X is \mathbf{s} -self-similar under the following conditions:

$$\Delta \left(X|_{s_1}, \dots, X|_{s_{n+1}} \right) \neq 0. \quad (34)$$

$$\text{abel} \left(X, X|_{s_1}, \dots, X|_{s_{n+1}} \right) \text{ is } k\text{-proportional to } X. \quad (35)$$

Proposition 3.5.2 *Fix an n by n matrix X with entries in A of rank ≤ 1 . Fix $\mathbf{s} = (s_1, \dots, s_{n+1}) \in S^{\{1, \dots, n+1\}}$. (i) If X is \mathbf{s} -normalized then condition (34) holds. (ii) If condition (34) holds then X is k -general.*

Proof. (i) This follows from identity (10). (ii) Put $\Delta = \Delta_{\ell=1}^{n+1} X^{(\ell)}$. By hypothesis $\Delta|_{\mathbf{s}} \neq 0$, hence $\Delta \neq 0$, whence the result by Proposition 3.4.3. \square

Proposition 3.5.3 *Fix a Segre matrix X and $\mathbf{s} = (s_1, \dots, s_{n+1}) \in S^{\{1, \dots, n+1\}}$. There exist n by n matrices Φ and Ψ with entries in k such that*

$$\Phi X \Psi = \text{abel} \left(X, X|_{s_1}, \dots, X|_{s_{n+1}} \right), \quad (\det \Phi)^2 (\det \Psi)^2 = \Delta \left(X|_{s_1}, \dots, X|_{s_{n+1}} \right).$$

Moreover if X is \mathbf{s} -normalized then Φ and Ψ may be taken diagonal.

Proof. This follows directly from key relation (11). \square

Lemma 3.5.4 Fix a Segre matrix X and $\mathbf{s} = (s_1, \dots, s_{n+1}) \in S^{\{1, \dots, n+1\}}$. If X is \mathbf{s} -self-similar then there exist diagonal matrices Φ and Ψ with entries in k such that $\det \Phi \cdot \det \Psi \neq 0$ and $\Phi^{-1}X\Psi^{-1}$ is \mathbf{s} -normalized.

Proof. By hypothesis (35) there exists a nonzero scalar c such that

$$X = c \cdot \text{abel} \left(X, X|_{s_1}, \dots, X|_{s_{n+1}} \right).$$

It follows by identity (16) that for $\ell = 1, \dots, n$ every entry of the matrix

$$X|_{s_\ell} = c \cdot \text{abel} \left(X|_{s_\ell}, X|_{s_1}, \dots, X|_{s_{n+1}} \right)$$

vanishes save possibly the ℓ^{th} diagonal entry. Let E be the n by n matrix with all entries equal to 1. Since $X|_{s_{n+1}}$ is of rank ≤ 1 we can write

$$X|_{s_{n+1}} = \Phi E \Psi$$

where Φ and Ψ are diagonal matrices with entries in k . By hypothesis (34) and identity (10) neither is it possible for $\det \Phi \cdot \det \Psi$ to vanish, nor for there to exist some index $\ell = 1, \dots, n$ such that the ℓ^{th} diagonal entry of $X|_{s_\ell}$ vanishes. Therefore the pair (Φ, Ψ) has all the desired properties. \square

Proposition 3.5.5 Fix a Segre matrix X and $\mathbf{s} \in S^{\{1, \dots, n+1\}}$. Put

$$Z = \text{abel}_{\ell=0}^{n+1} X^{(\ell)}, \quad \Delta = \Delta_{\ell=1}^{n+1} X^{(\ell)}.$$

Assume that $\Delta|_{\mathbf{s}} \neq 0$. (i) Up to k -proportionality $Z|_{\mathbf{s}}$ is the unique \mathbf{s} -self-similar Segre matrix k -equivalent to X . (ii) There exists a unique \mathbf{s} -normalized Segre matrix k -equivalent to X .

Proof. (i) By Proposition 3.5.3 the matrix

$$Z|_{\mathbf{s}} = \text{abel} \left(X, X|_{s_1}, \dots, X|_{s_{n+1}} \right)$$

is a Segre matrix k -equivalent to X . Further, $Z|_{\mathbf{s}}$ is \mathbf{s} -self-similar by the iterated abelian identity (21). Finally, any two k -equivalent \mathbf{s} -self-similar Segre matrices are k -proportional by the abelian transformation law (3).

(ii) We may assume without loss of generality that X is \mathbf{s} -self-similar. By Lemma 3.5.4 there exists at least one \mathbf{s} -normalized Segre matrix k -equivalent to X . Now suppose that Y and Y' are \mathbf{s} -normalized Segre matrices both k -equivalent to X . By Proposition 3.5.3 and our additional assumption that X is \mathbf{s} -self-similar, we have $X = \Phi Y \Psi = \Phi' Y' \Psi'$ where Φ, Ψ, Φ', Ψ' are non-singular diagonal matrices with entries in k , hence we have $\Phi E \Psi = \Phi' E \Psi'$ where E is the n by n matrix with all entries equal to 1, hence there exists a nonzero scalar c such that $\Phi' = c\Phi$ and $\Psi' = c^{-1}\Psi$, and hence $Y = Y'$. \square

3.6 The abstract Abel map: definition and key properties

3.6.1 Definition

The *abstract Abel map* by definition sends each Segre matrix X to the n by n matrix $\text{abel}_{\ell=0}^{n+1} X^{(\ell)}$ with entries in $A^{\otimes\{0,\dots,n+1\}}$. The abstract Abel map generalizes and abstracts the explicit algebraic representation of the Abel map studied in (Anderson 1997).

3.6.2 Catalog of key properties

Fix a Segre matrix X . Let

$$Z = \text{abel}_{\ell=0}^{n+1} X^{(\ell)}, \quad \Delta = \Delta_{\ell=1}^{n+1} X^{(\ell)}$$

be the image of X under the abstract Abel map and the naturally associated discriminant, respectively. The following hold:

- $Z \neq 0$ and $\Delta \neq 0$, by Proposition 3.4.3.
- If X is replaced by a k -equivalent matrix, then Z and Δ are replaced by nonzero scalar multiples, by (3) and (8).
- If X is replaced by X^T , then Z is replaced by Z^T and Δ remains unchanged, by (4) and (9).
- $\langle 0 | n + 1 \rangle_* Z = Z^T$, by (4).
- $\pi_* Z_{ij} = Z_{\pi i, \pi j}$ for any bijective derangement π supported in $\{1, \dots, n\}$, by (5).
- $[1 \mapsto 2]_* Z_{12} = Z_{11}$, by (6).
- Z is of rank ≤ 1 , by (15).
- $\Delta = \langle 2 | n + 1 \rangle_* \langle 0 | 1 \rangle_* Z_{11} \cdot \langle 0 | 1 \rangle_* Z_{11} \cdot \langle 0 | 2 \rangle_* Z_{22} \cdot \prod_{\ell=3}^n (\langle 0 | \ell \rangle_* Z_{\ell\ell})^2$, by (20).
- $\text{abel}_{\ell=0}^{n+1} [0 \mapsto -\ell]_* Z = \Delta \cdot \bar{Z}$, by (21).
- $Z_{ij} \in k\text{-span of } L \cdot \prod_{b \in \{1, \dots, n\} \setminus \{j\}} L^{(b)} \cdot L^{(n+1)} \cdot \prod_{a \in \{1, \dots, n\} \setminus \{i\}} L^{(a)}$, by (23).

Proposition 3.6.3 (“The abstract Abel theorem”) *Let X and X' be Segre matrices with corresponding images Z and Z' under the abstract Abel map, respectively. Then X' is k -equivalent to X if and only if Z' is k -proportional to Z .*

Proof.

(\Rightarrow) This follows directly from identity (3).

(\Leftarrow) Put

$$\Delta = \Delta_{\ell=1}^{n+1} X^{(\ell)}, \quad \Delta' = \Delta_{\ell=1}^{n+1} (X')^{(\ell)}.$$

By Proposition 3.4.3 neither Δ nor Δ' vanish identically. By the Nullstellensatz there exists

$$\mathbf{s} = (s_1, \dots, s_{n+1}) \in S^{\{1, \dots, n+1\}}$$

such that

$$\Delta \|_{\mathbf{s}} \neq 0, \quad \Delta' \|_{\mathbf{s}} \neq 0.$$

By Proposition 3.5.3 and hypothesis we have

$$X \sim Z \|_{\mathbf{s}} \sim Z' \|_{\mathbf{s}} \sim X',$$

where \sim denotes k -equivalence. \square

3.7 Characterization of the image of the abstract Abel map

3.7.1 J -matrices

A J -matrix Z is by definition an object with the following properties:

$$Z \text{ is an } n \text{ by } n \text{ matrix with entries in the } k\text{-span of } L \cdot A^{\otimes\{1, \dots, n+1\}}. \quad (36)$$

$$Z \neq 0. \quad (37)$$

$$Z \text{ is of rank } \leq 1. \quad (38)$$

$$\text{abel}_{\ell=0}^{n+1}[0 \mapsto -\ell]_* Z = \Delta \cdot \bar{Z} \text{ for some } 0 \neq \Delta \in A^{\otimes\{1, \dots, n+1\}}. \quad (39)$$

Since $A^{\otimes \mathbb{Z}}$ is a k -algebra without zero-divisors, Z uniquely determines Δ . We call Δ the *discriminant* of the J -matrix Z . If we need to call attention to the basic data we say that Z is a J -matrix of *type* (k, n, A, L) . In view of the properties catalogued in §3.6.2, it is clear that every matrix in the image of the abstract Abel map is automatically a J -matrix.

Proposition 3.7.2 (“The abstract Jacobi inversion theorem”) *Fix a J -matrix Z with associated discriminant Δ . (i) For all $\mathbf{s} \in S^{\{1, \dots, n+1\}}$ the*

partial specialization $\Delta|_{\mathbf{s}}$ is a scalar and for some \mathbf{s} that scalar does not vanish. (ii) For any $\mathbf{s} \in S^{\{1, \dots, n+1\}}$ such that the scalar $\Delta|_{\mathbf{s}}$ does not vanish, the corresponding partial specialization $Z|_{\mathbf{s}}$ is a Segre matrix with image under the abstract Abel map k -proportional to Z .

Proof.

(i) This follows from the Nullstellensatz.

(ii) Put

$$X = Z|_{\mathbf{s}}.$$

The matrix X is an n by n matrix with entries in L by condition (36) and of rank ≤ 1 by condition (38). By applying firstly the partial specialization operation $|_{\mathbf{s}}$ and secondly the bar operation to both sides of the identity figuring in condition (39), we obtain the relation

$$\text{abel}_{\ell=0}^{n+1} X^{(\ell)} = \Delta|_{\mathbf{s}} \cdot Z.$$

The right side does not vanish by condition (37) combined with our hypothesis that $\Delta|_{\mathbf{s}} \neq 0$. It follows by Proposition 3.4.3 that X is k -general and hence a Segre matrix. It follows as well that the image of X under the abstract Abel map is k -proportional to Z . \square

3.7.3 Jacobi matrices

A *Jacobi matrix* Z is by definition an object with the following properties:

$$Z \text{ is an } n \text{ by } n \text{ matrix with entries in } A^{\otimes\{0, \dots, n+1\}}. \quad (40)$$

$$Z \neq 0. \quad (41)$$

$$Z_{12} \in k\text{-span of } L \cdot L^{(1)} \cdot L^{(2)} \cdot (L^{(3)})^2 \cdots (L^{(n)})^2 \cdot L^{(n+1)}. \quad (42)$$

$$Z_{11} = [1 \mapsto 2]_* Z_{12}. \quad (43)$$

$$\pi_* Z_{ij} = Z_{\pi i, \pi j} \text{ for any bijective derangement } \pi \text{ supported} \\ \text{in } \{1, \dots, n\}. \quad (44)$$

$$\begin{vmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{vmatrix} = 0. \quad (45)$$

$$\text{abel}_{\ell=0}^{n+1} [0 \mapsto -\ell]_* Z = \Delta \cdot \bar{Z}, \quad (46)$$

where

$$\Delta = \langle 2|n+1 \rangle_* \langle 0|1 \rangle_* Z_{11} \cdot \langle 0|1 \rangle_* Z_{11} \cdot \langle 0|2 \rangle_* Z_{22} \cdot \prod_{\ell=3}^n (\langle 0|\ell \rangle_* Z_{\ell\ell})^2. \quad (47)$$

We call Δ the *discriminant* of the Jacobi matrix Z . If we need to draw attention to the basic data we say that Z is of *type* (k, n, A, L) . It is clear that the set of k -proportionality classes of Jacobi matrices forms a projective algebraic variety. Moreover, in view of the properties cataloged in §3.6.2, it is clear that the abstract Abel map takes its values in the set of Jacobi matrices. Note that a Jacobi matrix Z is uniquely determined by its entry Z_{12} .

Lemma 3.7.4 *The discriminant of a Jacobi matrix does not vanish identically and belongs to $A^{\otimes\{1, \dots, n+1\}}$.*

Proof. Fix a Jacobi matrix Z with associated discriminant Δ . By conditions (41) and (44) either every diagonal entry of Z is nonvanishing or every off-diagonal entry of Z is nonvanishing; but then by condition (45) every entry Z is nonvanishing. By definition (47) it follows that Δ does not vanish identically. By conditions (42) and (43) we have

$$Z_{11} \in A^{\otimes\{0, 2, \dots, n+1\}}.$$

By condition (44) we have

$$Z_{\ell\ell} = \langle 1|\ell \rangle_* Z_{11} \in A^{\otimes\{0, \dots, n+1\} \setminus \{\ell\}}$$

and further

$$\langle \ell|0 \rangle_* Z_{\ell\ell} \in A^{\otimes\{1, \dots, n+1\}}, \quad \langle 2|n+1 \rangle_* \langle 1|0 \rangle_* Z_{11} \in A^{\otimes\{1, \dots, n+1\}}.$$

By definition (47) it follows that Δ belongs to $A^{\otimes\{1, \dots, n+1\}}$. \square

Proposition 3.7.5 *Every Jacobi matrix is a J -matrix and vice versa.*

Proof. By Proposition 3.7.2 every J -matrix is in the image of the abstract Abel map and hence a Jacobi matrix in view of the properties cataloged in §3.6.2. Thus the “vice versa” part of the proposition is proved. Now fix a Jacobi matrix Z with associated discriminant Δ . We verify that Z has the properties required of a J -matrix as follows. To abbreviate notation temporarily let V denote the k -span of $L \cdot A^{\otimes\{1, \dots, n+1\}}$. We have $Z_{12} \in V$ by condition (42). We have $[1 \mapsto 2]_* V \subseteq V$ and hence $Z_{11} \in V$ by condition (43). We have $\pi_* V \subseteq V$ for any bijective derangement π supported in $\{1, \dots, n\}$ and hence $Z_{ij} \in V$ for all $i, j \in \{1, \dots, n\}$ by condition (44). Therefore Z satisfies condition (36). Conditions (37) and (41) are exactly the same. Clearly Z satisfies condition (38) by conditions (44) and (45). Finally, Z satisfies condition (39) by condition (46) combined with Lemma 3.7.4. \square

Theorem 3.7.6 (i) *The set of k -proportionality classes of Jacobi matrices forms a projective algebraic variety.* (ii) *The abstract Abel map takes values in the set of Jacobi matrices.* (iii) *The abstract Abel map puts the k -equivalence classes of Segre matrices into bijective correspondence with the k -proportionality classes of Jacobi matrices.*

Proof.

(i,ii) These facts have already been noted above.

(iii) The correspondence in question is well-defined and one-to-one by Proposition 3.6.3. The correspondence is onto by Propositions 3.7.2 and 3.7.5. \square

3.7.7 Remark

We briefly describe the big picture in more geometrical language. We temporarily introduce the following notation:

- Let V be the quasi-affine variety of Segre matrices.
- Let G denote the product of two copies of the n by n general linear group over k and let G act in the obvious way on V .
- Let J be the projective variety of k -proportionality classes of Jacobi matrices.

For each $\mathbf{s} \in S^{\{1, \dots, n+1\}}$:

- Let $V_{\mathbf{s}}$ be the open subvariety of V consisting of Segre matrices X satisfying the inequality $\Delta_{\ell=1}^{n+1}(X|_{s_{\ell}}) \neq 0$.
- Let $U_{\mathbf{s}}$ be the affine variety consisting of n by n matrices X with entries in L that are of rank ≤ 1 and \mathbf{s} -normalized.
- Let $U'_{\mathbf{s}}$ be the quasi-projective variety consisting of \mathbf{s} -self-similar Segre matrices modulo k -proportionality.
- Let $J_{\mathbf{s}}$ be the open subvariety of J consisting of points represented by Jacobi matrices with discriminant Δ such that $\Delta|_{\mathbf{s}} \neq 0$.

By Proposition 3.4.3 and the Nullstellensatz the open subvarieties $V_{\mathbf{s}}$ cover V . By identity (8) the variety $V_{\mathbf{s}}$ is G -stable. By Proposition 3.5.2 the variety $U_{\mathbf{s}}$ is contained in $V_{\mathbf{s}}$. By Proposition 3.5.5 the quotient $V_{\mathbf{s}}/G$ can naturally be identified with $U'_{\mathbf{s}}$ and also with $U_{\mathbf{s}}$. By Lemma 3.7.4 and the Nullstellensatz the open sets $J_{\mathbf{s}}$ cover J . By Propositions 3.5.5, 3.6.3, 3.7.2 and 3.7.5, the set $J_{\mathbf{s}}$ can naturally be identified with $U'_{\mathbf{s}}$ and hence also with $U_{\mathbf{s}}$. The upshot is that the family $\{U_{\mathbf{s}}\}$ can be viewed as an affine open covering of J .

3.8 Examples of Jacobi matrices involving elliptic functions

3.8.1 The set up

We continue in the set up of §3.2.1. By Proposition 3.2.4 combined with Theorem 3.7.6 every Jacobi matrix of type (24) is \mathbb{C} -proportional to the image of some matrix of the form (25) under the abstract Abel map for a value of the parameter $t \in \mathbb{C}$ uniquely determined modulo the period lattice Λ . To figure out what these Jacobi matrices actually look like, we are going to apply the abstract Abel map to the matrix (25). But before we proceed we have a notational collision to deal with: $f^{(\ell)}$ denotes the ℓ^{th} derivative of f in the present context. To fix the problem we think of and write out the “superscript ℓ ” operation defined in §3.3.1 as the high school algebra operation of “substitution of the variable z_ℓ for the variable z .”

3.8.2 A classical determinant identity and related abelian identity

By combining the classical identity

$$\begin{vmatrix} 1 & \frac{\wp(z_1)}{1!} & -\frac{\wp'(z_1)}{2!} & \dots & \frac{(-1)^{n-2}\wp^{(n-2)}(z_1)}{(n-1)!} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \frac{\wp(z_n)}{1!} & -\frac{\wp'(z_n)}{2!} & \dots & \frac{(-1)^{n-2}\wp^{(n-2)}(z_n)}{(n-1)!} \end{vmatrix} = \frac{\sigma\left(\sum_{i=1}^n z_i\right) \cdot \prod_{1 \leq i < j \leq n} \sigma(z_i - z_j)}{\prod_{i=1}^n \sigma(z_i)^n} \quad (48)$$

(see (Frobenius Stickelberger 1877, p. 179) or (Whittaker Watson, Chap. XX, Misc. Ex. 21)) with abelian identity (14), we find after a straightforward calculation that

$$\begin{aligned}
& \left(\text{abel}_{\ell=0}^{n+1} \vec{\sigma}(z_\ell - t/n)^T \vec{\sigma}(z_\ell + t/n) \right)_{ij} / \left(\det \begin{bmatrix} \frac{\vec{\sigma}^{(n)}(0)}{n!} \\ \frac{\vec{\sigma}^{(n-2)}(0)}{(n-2)!} \\ \vdots \\ \frac{\vec{\sigma}(0)}{0!} \end{bmatrix} \right)^4 \\
&= \sigma \left(t + \sum_{\ell \in \{0, \dots, n+1\} \setminus \{0, i\}} z_\ell \right) \times \sigma \left(t - \sum_{\ell \in \{0, \dots, n+1\} \setminus \{i, n+1\}} z_\ell \right) \\
&\times \sigma \left(t + \sum_{\ell \in \{0, \dots, n+1\} \setminus \{j, n+1\}} z_\ell \right) \times \sigma \left(t - \sum_{\ell \in \{0, \dots, n+1\} \setminus \{0, j\}} z_\ell \right) \quad (49) \\
&\times \prod_{\substack{\alpha, \beta \in \{0, \dots, n+1\} \setminus \{0, i\} \\ \alpha < \beta}} \sigma(z_\alpha - z_\beta) \times \prod_{\substack{\alpha, \beta \in \{0, \dots, n+1\} \setminus \{i, n+1\} \\ \alpha < \beta}} \sigma(z_\alpha - z_\beta) \\
&\times \prod_{\substack{\alpha, \beta \in \{0, \dots, n+1\} \setminus \{j, n+1\} \\ \alpha < \beta}} \sigma(z_\alpha - z_\beta) \times \prod_{\substack{\alpha, \beta \in \{0, \dots, n+1\} \setminus \{0, j\} \\ \alpha < \beta}} \sigma(z_\alpha - z_\beta).
\end{aligned}$$

Identity (49) granted, it is not difficult to verify that the variety of \mathbb{C} -proportionality classes of Jacobi matrices is a complex manifold isomorphic to the complex torus \mathbb{C}/Λ . We omit further details.

4 Elementary construction of Jacobians

4.1 Basic notation and terminology

As above, let k be an algebraically closed field. We work in the category of quasi-projective varieties over k . As above, let C be a nonsingular projective algebraic curve of genus g . We assume that $g > 0$. *Divisors* are divisors of C . Given a divisor D , we write $L(D) = H^0(C, \mathcal{O}_C(D))$ and $\ell(D) = \dim_k L(D)$.

4.2 Matrix representation of divisor classes

Lemma 4.2.1 *Let D be a divisor such that $\deg D \geq 2g$. Then we have*

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

Moreover, we have

$$\ell(D') \geq \ell(D) \Rightarrow \deg D' \geq \deg D$$

for all divisors D' .

Proof. Riemann-Roch. \square

4.2.2 G -forms

Let G be a divisor such that

$$\deg G \equiv 0 \pmod{2}, \quad \frac{1}{2} \deg G \geq 2g$$

and put

$$n = \frac{1}{2} \deg G - g + 1.$$

By definition a G -form X is an object with the following properties:

- X is an n by n matrix with entries in $L(G)$.
- Every two by two submatrix of X has vanishing determinant.
- There exists in X some row and also some column with k -linearly independent entries.

A G -form is the same thing as a Segre matrix of type

$$\left(k, n, \bigoplus_{m=0}^{\infty} L(mG), L(G) \right).$$

If $G > 0$, then a G -form can also be viewed as a Segre matrix of type

$$\left(k, n, H^0(C \setminus \text{supp } G, \mathcal{O}_C), L(G) \right).$$

Here and below $\text{supp } D$ denotes the support of a divisor D . Our immediate goal is to put the k -equivalence classes of G -forms in canonical bijective correspondence with the divisor classes of degree $\frac{1}{2} \deg G$. The “dictionary” we ultimately obtain is summarized by Proposition 4.2.6 below.

4.2.3 Representation of divisors of degree $\frac{1}{2} \deg G$ by G -forms

Let G and n be as above. Let D be a divisor of degree $\frac{1}{2} \deg G$. Let u (resp. v) be a column (resp. row) vector with entries forming a k -basis for $L(D)$ (resp. $L(G - D)$). Put $X = uv$. It is clear that X is a G -form the k -equivalence class of which depends only on D , not on the choice of vectors u and v . In this situation we say that the G -form X represents the divisor D of degree $\frac{1}{2} \deg G$. We claim that for every divisor D' in the divisor class of D and every G -form X' representing D' , the G -form X is k -equivalent to X' . To prove the claim, write $D = D' + (f)$ where f is a nonzero meromorphic function on C . Then

$$L(D') = f \cdot L(D), \quad L(G - D') = f^{-1} \cdot L(G - D),$$

hence the G -form $X = uv = (fu)(f^{-1}v)$ represents not only D but also D' , and hence X is k -equivalent to X' . The claim is proved.

4.2.4 Unique determination of the class of a divisor by a representing G -form

Let G and n be as above. Suppose that divisors D and D' of degree $\frac{1}{2} \deg G$ are represented by k -equivalent G -forms X and X' , respectively. We claim that D and D' belong to the same divisor class. To prove the claim we may assume without loss of generality that $X = X'$. Write $X = uv = u'v'$ where u and u' are column vectors, v and v' are row vectors, and the entries of u (resp. v , u' , v') form a k -basis for $L(D)$ (resp. $L(G - D)$, $L(D')$, $L(G - D')$). There exists a unique nonzero meromorphic function f on C such that $u' = fu$ and $v' = f^{-1}v$, hence

$$L(D) = f^{-1} \cdot L(D') = L(D' + (f)) \subset L(\min(D, D' + (f))),$$

and hence $D = D' + (f)$ by Lemma 4.2.1. The claim is proved.

4.2.5 Construction of a divisor represented by a given G -form

Let G and n be as above. Let X be a G -form. Choose a column u and a row v of X each with k -linearly independent entries. Let f be the entry common to u and v ; then f does not vanish identically. Consider now the effective divisors

$$D = G + \min_j(v_j), \quad E = G + \min_i(u_i), \quad F = G + (f).$$

We claim that X represents the divisor D . In any case, since X is of rank ≤ 1 we have $X = uv/f$ and hence

$$D + E \geq F, \quad \deg D + \deg E \geq \deg F = \deg G.$$

Since the entries of v are k -linearly independent and belong to $L(G - D)$, we have $\ell(G - D) \geq n$ and hence $\frac{1}{2} \deg G \geq \deg D$ by Lemma 4.2.1. Similarly we have $\frac{1}{2} \deg G \geq \deg E$. It follows that

$$\deg D = \deg E = \frac{1}{2} \deg G = \frac{1}{2} \deg F, \quad D + E = F.$$

In turn it follows that the entries of v form a k -basis for $L(G - D)$ and that the entries of u/f form a k -basis for $L(G - E + (f)) = L(D)$. Therefore $X = uv/f$ does indeed represent the divisor D . The claim is proved.

Proposition 4.2.6 *Let G be a divisor of even degree such that $\frac{1}{2} \deg G \geq 2g$. There exists a unique bijective correspondence*

$$\left\{ \begin{array}{l} k\text{-equivalence} \\ \text{classes of } G\text{-forms} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{divisor classes} \\ \text{of degree } \frac{1}{2} \deg G \end{array} \right\}$$

with respect to which, for any G -form X and any divisor D of degree $\frac{1}{2} \deg G$, the k -equivalence class of X corresponds to the divisor class of D if and only if X represents D .

Proof. All the hard work is done; we just have to sum up. For each divisor D of degree $\frac{1}{2} \deg G$ arbitrarily fix a column (resp. row) vector u_D (resp. v_D) with entries forming a k -basis of $L(D)$ (resp. $L(G - D)$). The product $u_D v_D$ is a G -form the k -equivalence class of which depends only on D , not on the choice of u_D and v_D (§4.2.3). The map $D \mapsto u_D v_D$ sends divisor classes into k -equivalence classes (§4.2.3). The map $D \mapsto u_D v_D$ sends distinct divisor classes into distinct k -equivalence classes (§4.2.4). The image of the map $D \mapsto u_D v_D$ meets every k -equivalence class of G -forms (§4.2.5). \square

4.2.7 Remark

The dictionary provided by Proposition 4.2.6 is essentially just a chapter of algebro-geometrical folklore, cf. (Eisenbud Koh Stillman 1988, Prop. 1.1). The Eisenbud-Koh-Stillman paper greatly inspired us. Our presentation of the dictionary is a much simplified version of the presentation in (Anderson 1997).

4.3 Matrix representation of divisor class addition and subtraction

4.3.1 A theorem of Mumford

By (Mumford 1970, Thm. 6, p. 52) we have

$$\left. \begin{array}{l} \deg D \geq 2g + 1 \\ \deg E \geq 2g \end{array} \right\} \Rightarrow L(D + E) = k\text{-span of } L(D) \cdot L(E) \quad (50)$$

for all divisors D and E .

4.3.2 Kronecker products

Given a p by q matrix A and an r by s matrix B both with entries in some ring R , the *Kronecker product* $A \circ B$ is defined to be the pr by qs matrix with entries in R admitting a decomposition into r by s blocks of the form

$$A \circ B = \begin{bmatrix} & & & \vdots & & \\ & & & & & \\ \dots & & A_{ij}B & & \dots & \\ & & & \vdots & & \\ & & & & & \end{bmatrix}.$$

The Kronecker product of matrices is compatible with ordinary matrix multiplication in the sense that

$$(A \circ B)(X \circ Y) = (AX) \circ (BY)$$

whenever AX and BY are defined.

Proposition 4.3.3 *Let divisors G , G' , D and D' be given subject to the following conditions:*

$$\deg G = 2 \cdot \deg D, \quad \deg G' = 2 \cdot \deg D',$$

$$\min\left(\frac{1}{2} \deg G, \frac{1}{2} \deg G'\right) \geq 2g, \quad \max\left(\frac{1}{2} \deg G, \frac{1}{2} \deg G'\right) \geq 2g + 1.$$

Put

$$n = \frac{1}{2} \deg G - g + 1, \quad n' = \frac{1}{2} \deg G' - g + 1,$$

and

$$n'' = \frac{1}{2} (\deg G + \deg G') - g + 1 = n + n' + g - 1.$$

Fix a G -form X representing D and a G' -form X' representing D' . Let P and Q be any nn' by nn' permutation matrices and consider the block decomposition

$$P(X \circ X')Q = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where the block d is n'' by n'' and the other blocks are of the appropriate sizes. (i) For some P and Q the corresponding block d is k -general. (ii) For any P and Q such that d is k -general, d is a $(G + G')$ -form representing $D + D'$.

Proof. Write $X = uv$ and $X' = u'v'$ where u (resp. v, u', v') is a column (resp. row, column, row) vector with entries forming a k -basis of $L(D)$ (resp. $L(G - D), L(D'), L(G' - D')$).

(i) By Mumford's theorem (50) the entries of $u \circ u'$ span $L(D + D')$ over k and hence for some permutation matrix P the last n'' entries of the vector $P(u \circ u')$ form a k -basis of $L(D + D')$. Similarly, the entries of $v \circ v'$ span $L(G + G' - D - D')$ over k and for some permutation matrix Q the last n'' entries of $(v \circ v')Q$ form a k -basis of $L(G + G' - D - D')$. With P and Q thus chosen the block d is a $(G + G')$ -form representing $D + D'$ and a *fortiori* k -general.

(ii) Now suppose we are given P and Q such that d is k -general. Then the last n'' entries of $P(u \circ u')$ are forced to be k -linearly independent and hence to form a k -basis of $L(D + D')$. Similarly the last n'' entries $(v \circ v')Q$ are forced to form a k -basis of $L(G + G' - D - D')$. Then the block d is indeed a $(G + G')$ -form representing $D + D'$. \square

Lemma 4.3.4 *Let E be a nonzero effective divisor. Let \mathcal{R}_E be the ring consisting of the meromorphic functions on C regular in a neighborhood of the support of E and let $\mathcal{I}_E \subset \mathcal{R}_E$ be the ideal consisting of functions vanishing to order at least E . Then there exists a k -linear functional*

$$\sigma : \mathcal{R}_E \rightarrow k$$

factoring through the quotient $\mathcal{R}_E/\mathcal{I}_E$ such that the induced k -bilinear map

$$((a \bmod \mathcal{I}_E, b \bmod \mathcal{I}_E) \mapsto \sigma(ab)) : \mathcal{R}_E/\mathcal{I}_E \times \mathcal{R}_E/\mathcal{I}_E \rightarrow k \quad (51)$$

is a perfect pairing of $(\deg E)$ -dimensional vector spaces over k .

Proof. Choose any meromorphic differential ω on C such that

$$\text{ord}_x \omega + \text{ord}_x E = 0$$

for all points $x \in \text{supp } E$, where ord_x abbreviates “order of vanishing at x ”. Then, so we claim, the k -linear functional

$$\left(a \mapsto \sum_{x \in \text{supp } E} \text{Res}_x(a\omega) \right) : \mathcal{R}_E \rightarrow k$$

has all the desired properties. The proof of the claim is an exercise in residue calculus we can safely omit. \square

Lemma 4.3.5 *Let G and E be divisors such that*

$$\deg G \equiv 0 \pmod{2}, \quad E > 0, \quad \frac{1}{2} \deg G - \deg E > 2g - 2.$$

There exists a k -linear functional

$$\rho : L(G) \rightarrow k$$

factoring through the quotient $\frac{L(G)}{L(G-E)}$ such that for all divisors D of degree $\frac{1}{2} \deg G$ the induced k -bilinear map

$$((a + L(D - E), b + L(G - D - E)) \mapsto \rho(ab)) : \frac{L(D)}{L(D-E)} \times \frac{L(G-D)}{L(G-D-E)} \rightarrow k$$

is a perfect pairing of $(\deg E)$ -dimensional vector spaces over k .

Proof. For each divisor D choose a meromorphic function f_D on C such that

$$\text{ord}_x f = \text{ord}_x D$$

for all points $x \in \text{supp } E$; then we have

$$L(D) \subseteq f_D^{-1} \mathcal{R}_E, \quad L(D) \cap f_D^{-1} \mathcal{I}_E = L(D - E),$$

where \mathcal{R}_E and \mathcal{I}_E are as defined in Lemma 4.3.4. Now choose a k -linear functional $\sigma : \mathcal{R}_E \rightarrow k$ such that the pairing (51) is perfect and put

$$\rho = (x \mapsto \sigma(f_G x)) : L(G) \rightarrow k,$$

thereby defining a k -linear functional factoring through the quotient $\frac{L(G)}{L(G-E)}$. Suppose now that $\deg D = \frac{1}{2} \deg G$ and consider the commutative diagram

$$\begin{array}{ccccccc} \frac{L(D)}{L(D-E)} & \times & \frac{L(G-D)}{L(G-D-E)} & \xrightarrow{\times} & \frac{L(G)}{L(G-E)} & \xrightarrow{\rho} & k \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{R}_E/\mathcal{I}_E & \times & \mathcal{R}_E/\mathcal{I}_E & \xrightarrow{\times} & \mathcal{R}_E/\mathcal{I}_E & \xrightarrow{\sigma} & k \end{array}$$

where the vertical arrows are induced by multiplication by

$$f_D, \quad f_G f_D^{-1}, \quad f_G, \quad 1,$$

respectively. By construction all the vertical arrows are injective and of course the last is bijective. Further, the source of each vertical arrow other than the last is of dimension over k equal to $\deg E$ by Riemann-Roch. Therefore all the vertical arrows are bijective and hence ρ has the desired nondegeneracy property. \square

4.3.6 Compression functionals

In the situation of Lemma 4.3.5 we call $\rho : L(G) \rightarrow k$ an E -compression functional. To make the calculations below run smoothly it is convenient to introduce in this context the following notation. Given any matrix Y with entries in $L(G)$, let ρY be the result of applying ρ entrywise to Y , i. e., the matrix with entries in k defined by the rule $(\rho Y)_{ij} = \rho Y_{ij}$.

Proposition 4.3.7 *Let G and E be divisors such that*

$$\deg G \equiv 0 \pmod{2}, \quad E > 0, \quad \frac{1}{2} \deg G - \deg E \geq 2g$$

and put

$$n = \frac{1}{2} \deg G - \deg E - g + 1, \quad n' = \frac{1}{2} \deg G - g + 1 = n + \deg E.$$

Let $\rho : L(G) \rightarrow k$ be an E -compression functional. Let D be a divisor of degree $\frac{1}{2} \deg G$ and let X be a G -form representing D . Let P and Q be any n' by n' permutation matrices and consider the block decomposition

$$PXQ = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where the block a is $\deg E$ by $\deg E$, the block d is n by n and the other blocks are of the appropriate sizes. (i) For some P and Q we have $\det pa \neq 0$. (ii) For any P and Q such that $\det pa \neq 0$ the matrix z defined by the rule

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -(\rho c)(\rho a)^{-1} & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & -(\rho a)^{-1}(\rho b) \\ 0 & 1 \end{bmatrix}$$

is a $(G - 2E)$ -form representing $D - E$.

Proof. Write $X = uv$ where u (resp. v) is a column (resp. row) vector with entries forming a k -basis of $L(D)$ (resp. $L(G - D)$).

(i) For suitably chosen permutation matrices P and Q the first $\deg E$ entries of the column vector Pu (resp. row vector vQ) project to a k -basis of the

quotient $\frac{L(D)}{L(D-E)}$ (resp. $\frac{L(G-D)}{L(G-D-E)}$). For such P and Q we have $\det \rho a \neq 0$ by definition of E -compression functional.

(ii) After replacing X by PXQ we may assume that $P = Q = 1$. After replacing X by the k -equivalent matrix $\begin{bmatrix} w & x \\ y & z \end{bmatrix}$ we may assume that

$$\det \rho a \neq 0, \quad \rho b = 0, \quad \rho c = 0,$$

in which case our task is simply to show that the block d is a $(G - 2E)$ -form. By definition of E -compression functional the first $\deg E$ entries of u (resp. v) project to a k -basis of the quotient $\frac{L(D)}{L(D-E)}$ (resp. $\frac{L(G-D)}{L(G-D-E)}$). Also by definition of E -compression functional the last n entries of u must belong to $L(D - E)$ and since k -linearly independent must form a k -basis of $L(D - E)$. Similarly the last n entries of v must form a k -basis of $L(G - D - E)$. Therefore d is indeed a $(G - 2E)$ -form representing $D - E$. \square

4.4 Completion of the construction

4.4.1 Candidate for the Jacobian

Fix an effective divisor E of degree $\geq 2g + 1$ and put

$$S = C \setminus \text{supp } E, \quad A = H^0(S, \mathcal{O}_C), \quad n = \ell(E) = \deg E - g + 1, \quad L = L(2E).$$

The projective algebraic variety J of k -proportionality classes of Jacobi matrices of type (k, n, A, L) is our candidate for the Jacobian of C .

4.4.2 Candidate for the Abel map

For each divisor D of degree zero arbitrarily fix a $2E$ -form X_D representing $D + E$. Now a $2E$ -form is the same thing as a Segre matrix of type (k, n, A, L) . By Proposition 4.2.6 it follows that the map $D \mapsto X_D$ puts the divisor classes of degree zero in bijective correspondence with the k -equivalence classes of Segre matrices of type (k, n, A, L) . For each divisor D of degree zero let Z_D be the image of X_D under the abstract Abel map. By Theorem 3.7.6 it follows that the map $D \mapsto Z_D$ puts the classes of divisors of degree zero into bijective correspondence with the points of J . The bijective map from classes of divisors of degree zero to J induced by the map $D \mapsto Z_D$ is our candidate for the Abel map.

Lemma 4.4.3 *For all divisors D of degree zero, X_{-D} is k -equivalent to X_D^T , and (hence) Z_{-D} is k -proportional to Z_D^T .*

Proof. This boils down to the transpose symmetry (4) of the abelian. \square

Lemma 4.4.4 *Fix an E -compression functional $\rho : L(4E) \rightarrow k$. Fix Segre matrices X and X' of type (k, n, A, L) . Fix a divisor D (resp. D') such that X (resp. X') is k -equivalent to X_D (resp. $X_{D'}$). Let P and Q be any n^2 by n^2 permutation matrices and consider the block decomposition*

$$P(X \circ X')Q = \begin{bmatrix} \bullet & \bullet & \bullet \\ \bullet & a & b \\ \bullet & c & d \end{bmatrix}$$

where the block a is $\deg E$ by $\deg E$, the block d is n by n , the other blocks are of the appropriate sizes, and the bullets hold places for blocks the contents of which do not concern us. Further, consider the block-decomposed matrix

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \det \rho a \cdot \begin{bmatrix} \det \rho a & 0 \\ -(\rho c)(\rho a)^* & \det \rho a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \det \rho a & -(\rho a)^*(\rho b) \\ 0 & \det \rho a \end{bmatrix}.$$

(i) For some P and Q the corresponding block z is k -general. (ii) For any P and Q such that the corresponding block z is k -general, z is a Segre matrix of type (k, n, A, L) and moreover z is k -equivalent to $X_{D+D'}$.

Proof. (i) By Propositions 4.3.3 and 4.3.7 there exist P and Q such that the following hold:

- $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a $4E$ -form representing $D + D' + 2E$.
- $\det \rho a \neq 0$.
- z is a $2E$ -form representing $D + D' + E$.

A fortiori z is k -general.

(ii) By hypothesis we have

$$\det \rho w \neq 0, \quad \rho x = 0, \quad \rho y = 0,$$

and there exists a factorization

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix} \begin{bmatrix} r & s \end{bmatrix}$$

where the entries of the column vector (resp. row vector) on the right belong to $L(D + D' + 2E)$ (resp. $L(-D - D' + 2E)$), the blocks p and r are vectors of length $\deg E$, and the blocks q and s are vectors of length n . By definition of E -compression functional (Lemma 4.3.5) it follows that the entries of p (resp. r) project to a k -basis of the quotient $\frac{L(D+D'+2E)}{L(D+D'+E)}$ (resp. $\frac{L(-D-D'+2E)}{L(-D-D'+E)}$). Also by definition of $2E$ -compression functional it follows that the entries of q (resp. s) belong to $L(D + D' + E)$ (resp. $L(-D - D' + E)$). Finally, since $z = qs$ is k -general, the entries of q (resp. s) must be k -linearly independent, and hence the entries of q (resp. s) must form a k -basis of $L(D + D' + E)$ (resp. $L(-D - D' + E)$). Therefore the block z is indeed a $2E$ -form representing $D + D' + E$ and hence k -equivalent to $X_{D+D'}$. \square

Lemma 4.4.5 *Fix an E -compression functional $\rho : L(4E) \rightarrow k$. Fix Jacobi matrices Z and Z' of type (k, n, A, L) with discriminants Δ and Δ' , respectively. Fix a divisor D (resp. D') of degree zero such that Z (resp. Z') is k -proportional to Z_D (resp. $Z_{D'}$). For any $\mathbf{s}, \mathbf{s}' \in S^{\{1, \dots, n+1\}}$ and any n^2 by n^2 permutation matrices P and Q consider the block decomposition*

$$P((Z||_{\mathbf{s}}) \circ (Z'||_{\mathbf{s}'}))Q = \begin{bmatrix} \bullet & \bullet & \bullet \\ \bullet & a & b \\ \bullet & c & d \end{bmatrix},$$

where the block a is $\deg E$ by $\deg E$, the block d is n by n , the other blocks are of the appropriate sizes, and the bullets hold places for blocks the contents of which do not concern us. Consider the block decomposed matrix

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \Delta||_{\mathbf{s}} \cdot \Delta'||_{\mathbf{s}'} \cdot \det \rho a \cdot \begin{bmatrix} \det \rho a & 0 \\ -(\rho c)(\rho a)^* & \det \rho a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \det \rho a & -(\rho a)^*(\rho b) \\ 0 & \det \rho a \end{bmatrix}$$

and finally put

$$Z'' = \text{abel}_{\ell=0}^{n+1} z^{(\ell)}.$$

(i) There exist \mathbf{s}, \mathbf{s}' , P and Q such that Z'' does not vanish identically. (ii) For any \mathbf{s}, \mathbf{s}' , P and Q such that Z'' does not vanish identically, Z'' is a Jacobi matrix of type (k, n, A, L) and moreover Z'' is k -proportional to $Z_{D+D'}$.

Proof. (i) By Proposition 3.7.2 there exists $\mathbf{s} \in S^{\{1, \dots, n+1\}}$ (resp. $\mathbf{s}' \in S^{\{1, \dots, n+1\}}$) such that $\Delta||_{\mathbf{s}}$ (resp. $\Delta'||_{\mathbf{s}'}$) is a nonzero scalar and hence the corresponding partially specialized matrix $Z||_{\mathbf{s}}$ (resp. $Z'||_{\mathbf{s}'}$) is k -equivalent to X_D (resp. $X_{D'}$).

By Lemma 4.4.4 there exist P and Q such that the block z is k -general. Finally, Z'' does not vanish by Proposition 3.4.3.

(ii) By Proposition 3.7.2 and hypothesis the partial specialization $\Delta|_s$ (resp. $\Delta'|_{s'}$) is a nonzero scalar and hence the corresponding partial specialization $Z|_s$ (resp. $Z'|_{s'}$) is a Segre matrices of type (k, n, A, L) that is k -equivalent to X_D (resp. $X_{D'}$). By hypothesis $\det \rho a$ is a nonzero scalar and hence z is by Lemma 4.4.4 a Segre matrix of type (k, n, A, L) that is k -equivalent to $X_{D+D'}$. Finally, since Z'' is the image of z under the abstract Abel map, Z'' is k -proportional to $Z_{D+D'}$. \square

Theorem 4.4.6 *There is exactly one way to equip our candidate for the Jacobian (§4.4.1) with the structure of algebraic group so that our candidate for the Abel map (§4.4.2) becomes a group homomorphism. (Thus our candidates become the Jacobian and the Abel map.)*

Proof. Since our candidate for the Abel map is bijective, the set underlying J comes canonically equipped with a group law. The only issue remaining to be resolved is whether or not that group law is algebraic, i. e., expressible Zariski-locally by regular functions. Well, by Lemma 4.4.3 the inversion operation in J is algebraic, and by Lemma 4.4.5 the addition operation in J is algebraic. We're done. \square

4.5 Remark

To give some indication of how the complexity of our construction of J grows as a function of the genus of C , we make the following observation. Suppose that C is a nonsingular plane algebraic curve of degree $d \geq 3$ and hence genus $\frac{(d-1)(d-2)}{2} > 0$ with defining equation $F = F(x, y, z) \in k[x, y, z]$. By the method of proof of Theorem 4.4.6 the divisor classes of C of degree zero can be put in natural bijective correspondence with the k -equivalence classes of Segre matrices of type

$$\left(k, \frac{d(d-1)}{2}, k[x, y, z]/(F), \{\text{forms of degree } 2d-4\}/(F) \right) \quad (52)$$

and in turn the Jacobian of C can be identified with the projective variety of k -proportionality classes of Jacobi matrices of type (52).

5 Acknowledgements

I thank Dinesh Thakur for comments on preliminary drafts of this paper. I thank Joel Roberts for discussions concerning ideals generated by two by two minors. I thank Hendryk Lenstra for comments on a preliminary draft of this paper, and in particular for pointing out Pila's paper to me. I thank Jeremy Teitelbaum for a conversation helpful for devising the example of §4.5. I thank the referee for constructive criticism.

References

- [Adleman DeMarrais Huang 1999] L. M. Adleman, J. DeMarrais, M.-D. Huang, A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over $\text{GF}(q)$, *Theoret. Comp. Sci.* **226** (1999), 7–18.
- [Anderson 1997] G. W. Anderson, An explicit algebraic representation of the Abel map, *Internat. Math. Res. Notices* **11** (1997), 495-521.
- [Eisenbud Koh Stillman 1988] D. Eisenbud, J. Koh, M. Stillman, Determinantal equations for curves of high degree, *Amer. J. Math.* **110** (1988), 513-539.
- [Flynn Poonen Schaefer 1997] E. V. Flynn, B. Poonen, E. F. Schaefer, Cycles of quadratic polynomials and rational points on a genus-2 curve, *Duke Math. J.* **90** (1997), 435-463.
- [Frobenius Stickelberger 1877] F. Frobenius, J. Stickelberger, Zur Theorie der elliptischen Functionen, *J. reine u. angew. Math.* **83** (1877), 175-179.
- [Jacquet-Langlands 1970] H. Jacquet, R. P. Langlands, Automorphic Forms on $\text{GL}(2)$, *Lec. Notes in Math.* **114**, Springer, New York, 1970.
- [Milne 1986] J. S. Milne, Jacobian varieties, in *Arithmetic Geometry* (G. Cornell and J. Silverman, Eds.), pp. 167–212, Springer, New York, 1986.
- [Mumford 1970] D. Mumford, Varieties defined by quadratic equations, in *Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969)*, pp. 29–100, Edizioni Cremonese, Rome, 1970.
- [Mumford Tata Lectures II] D. Mumford, Tata Lectures on Theta II: Jacobian Theta Functions and Differential Equations, with the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, *Progr. Math.* **43**, Birkhäuser Boston, Inc., Boston, MA, 1984.
- [Pila 1990] J. Pila, Frobenius maps of abelian varieties and finding roots of unity in finite fields, *Math. Comp.* **55** (1990), Issue 192, 745-763.
- [Whittaker Watson] E. T. Whittaker, G. N. Watson, *A course of modern analysis*, 4th ed., Cambridge University Press, Cambridge, 1927