Michigan Math. J. 49 (2001)

An Explicit Theorem of the Square for Hyperelliptic Jacobians

Jane Arledge & David Grant

Introduction

Let A be an abelian variety over a field k, D a symmetric divisor on A, s and d the sum and difference maps from $A \times A$ into A, and p_1 and p_2 the projections onto the first and second factors. The theorem of the square and the seesaw principle [M1, Secs. 5, 6] guarantee that there exists a function $f(u, v)$ on $A \times A$ (determined up to constant multiples) with divisor $s^*D + d^*D - 2p_1^*D - 2p_2^*D$. Since this function encodes all the information about the group morphism on A, it is useful to know $f(u, v)$ explicitly. Indeed, if $a, b, c \in A$ and if D_c is the image of D under the translation-by-c map, then the divisor of $f\big(u - \frac{a+b}{2}, -\frac{a+b}{2}\big)/f\big(u - \frac{a+b}{2}, \frac{-a+b}{2}\big)$ is $D_{a+b} + D - D_a - D_b$, which is the theorem of the square for D. If k is the complex numbers, then the construction of f is classical. One merely takes a theta function θ with divisor D (see e.g. [La]); then

$$f(u, v) = \theta(u + v)\theta(u - v)/\theta(u)^2\theta(v)^2,$$

for u, v in the universal cover of A, has the desired property.

When A is the Jacobian J of a curve C, it is useful to determine f in terms of symmetric functions on C. If k is the complex numbers and D is a theta divisor of J, then Riemann's theta identities (see [Mu, p. 212]) express $\theta(u + v)\theta(u - v)$ in terms of sums of products of theta functions with characteristics evaluated at u and v. When C is hyperelliptic, Baker [Ba2] described how the resulting functions of u and v can be expressed as explicit symmetric functions in the coordinates of the points in the support of the divisors corresponding to u and v; he found a way to express $f(u, v)$ as a polynomial in the second logarithmic derivatives of a theta function evaluated at u and v. In genus 1, Baker's formula was well known and is a cornerstone of the analytic theory of elliptic curves. In genus 2, this formula was recently used to understand the group law on J [G1], the derivatives of theta functions [G3], and the arithmetic of certain points on intersections of divisors [G2]. In genus 3, some of these same applications were carried out in [O]; in [A], a version of this formula was needed that worked over any field k in order to understand the arithmetic of certain torsion points.

In this paper we prove a version of Baker's formula for hyperelliptic curves of any genus g over any field k, generalizing the argument in [A]. Our formula takes a different shape than Baker's, but it must agree with his when k is the complex

Received October 4, 2000. Revision received April 9, 2001.