ANDRÉ WEIL. *Remarques sur un mémoire d'Hermite.* Arch. Math., Vol. V, 1954, pp. 197–202. (Also in *Collected Works*, Vol. II, Springer-Verlag, pp. 111–116.)

Translated in April 1998 by Alexander R. Perlis at The University of Arizona. In making this translation, I tried to keep the phrasing close to the original. To this end, I thank Robert V. Perlis at Louisiana State University and William G. McCallum at The University of Arizona for identifying the intended meaning (and for suggesting accurate translations) of a few sentences that presented particular difficulties. I am responsible for all remaining flaws and errors, and welcome suggestions and/or corrections. Please contact me at the email address `aprl@math.arizona.edu`. This is the 6 December 1998 version of this document—the latest version may be obtained anonymously from the website `www.math.arizona.edu/~aprl`. Regarding the mathematical content of André Weil's paper, the reader is referred to his more recent article: *Euler and the jacobians of elliptic curves*, in *Arithmetic and geometry, Vol. I*, edited by Michael Artin and John Tate, Birkhäuser Boston, 1983, pp. 353–359.

[1954a] Remarks on a paper of Hermite

TO ALEXANDER OSTROWSKI

At the beginning of his beautiful paper on binary biquadratic forms, HERMITE stated the relation

$$4g^3 - if^2g - jf^3 = h^2 \tag{A}$$

between the biquadratic form f, its invariants i, j and its covariants g, h, a relation that he says was discovered independently by CAYLEY and by himself and for which he then gives a proof. We will give here an interpretation of it that will make its interest visible from the point of view of the theory of algebraic curves of genus 1.

With the notation of HERMITE, we write

$$f(X,Y) = aX^4 + 4bX^3Y + 6cX^2Y^2 + 4b'XY^3 + a'Y^4,$$

where a, b, c, b', a' are elements of a base field k for which it is only necessary to assume that its characteristic is neither 2 nor 3. The invariants i, j are polynomials in a, b, c, b', a':

$$i = aa' - 4bb' + 3c^2, \qquad j = aca' + 2bcb' - ab'^2 - a'b^2 - c^3. \tag{I}$$

The covariants g, h are polynomials in a, b, c, b', a', X, Y, homogeneous in X and Y of degrees 4 and 6, respectively. The functions $\varphi = f^{-1}g$, $\psi = f^{-3/2}h$ are also homogeneous in X and Y of degree 0, and the relation of CAYLEY–HERMITE can be written:

$$\psi^2 = 4\varphi^3 - i\varphi - j.$$

Said another way, the formulas

$$\xi = \varphi(x,1) = z^{-2}g(x,1), \qquad \zeta = \psi(x,1) = z^{-3}h(x,1)$$

define a correspondence between the curves

$$z^2 = f(x,1) = ax^4 + 4bx^3 + 6cx^2 + 4b'x + a' \tag{II}$$

and

$$\zeta^2 = 4\xi^3 - i\xi - j. \tag{III}$$

We will suppose henceforth, once and for all, that f is a product of distinct linear factors; (II) is then a curve of genus 1. We will polish off the result of CAYLEY–HERMITE by showing that (III) is the jacobian of (II), that is to say that there is a birational correspondence, over the base field k, between the points of (III) and the divisor classes of degree 0 on (II); one will see at the same time that (II) and (III) are birationally equivalent over the algebraic closure of k, which, by the way, is already contained in the results of HERMITE. As (II) contains rational divisors of degree 2 over k (for example the divisor of poles of x), one can, in virtue of the theorem of RIEMANN–ROCH, consider, in place of divisor classes of degree 0, the effective divisor classes of degree 2; if such a divisor has the points (x_1, z_1), (x_2, z_2) for components, distinct or not, it will be denoted $(x_1, z_1) + (x_2, z_2)$.

Let us associate to the biquadratic form f the symmetric multilinear form f^* in four pairs of variables $(X_\nu, Y_\nu)_{1\le\nu\le4}$ such that one has

$$f(X,Y) = f^*(X,Y;X,Y;X,Y;X,Y).$$

This form is unique, and is written explicitly:

$$\begin{aligned} f^* = {} & aX_1X_2X_3X_4 + b(Y_1X_2X_3X_4+X_1Y_2X_3X_4+X_1X_2Y_3X_4+X_1X_2X_3Y_4) \\ & + c(Y_1Y_2X_3X_4+Y_1X_2Y_3X_4+Y_1X_2X_3Y_4+X_1Y_2Y_3X_4+X_1Y_2X_3Y_4+ \\ & \quad +X_1X_2Y_3Y_4) \\ & + b'(X_1Y_2Y_3Y_4+Y_1X_2Y_3Y_4+Y_1Y_2X_3Y_4+Y_1Y_2Y_3X_4) + a'Y_1Y_2Y_3Y_4. \end{aligned}$$

It is evidently covariant with respect to f in the sense that, if F is the transformation of f by the substitution $(X,Y) \to (\alpha X + \beta Y, \gamma X + \delta Y)$, then the symmetric multilinear form F^* associated to F, as f^* is to f, is the transformation of f^* by the substitution

$$(X_\nu, Y_\nu) \to (\alpha X_\nu + \beta Y_\nu, \gamma X_\nu + \delta Y_\nu) \quad (\nu = 1,2,3,4)$$

on the four pairs of variables (X_ν, Y_ν). For brevity of notation, let us put, for any indices λ, μ, ν, ϱ,

$$f_{\lambda\mu\nu\varrho} = f^*(X_\lambda, Y_\lambda; X_\mu, Y_\mu; X_\nu, Y_\nu; X_\varrho, Y_\varrho),$$

and let us agree moreover to write f_λ in place of $f_{\lambda\lambda\lambda\lambda}$; thus $f_\lambda = f(X_\lambda, Y_\lambda)$.

Let us now consider the functions

$$\varphi(X_1, Y_1; X_2, Y_2) = \frac{f_{1122} - {f_1}^{1/2} {f_2}^{1/2}}{2(X_1Y_2 - X_2Y_1)^2}$$
$$\psi(X_1, Y_1; X_2, Y_2) = \frac{{f_2}^{1/2} f_{1112} - {f_1}^{1/2} f_{2221}}{(X_1Y_2 - X_2Y_1)^3}.$$

They are homogeneous of degree 0 separately in (X_1, Y_1) and in (X_2, Y_2). If one applies on these two pairs of variables the substitution

$$(X_1, Y_1; X_2, Y_2) \to (\alpha X_1 + \beta Y_1, \gamma X_1 + \delta Y_1; \alpha X_2 + \beta Y_2, \gamma X_2 + \delta Y_2),$$

and recalls that F denotes the transformation of f by the substitution $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$, then φ and ψ behave as the covariants of f, that is to say that the expressions Φ, Ψ formed in the same manner as F will satisfy the relations

$$\Phi(X_1,Y_1; X_2,Y_2) = (\alpha\delta - \beta\gamma)^2 \varphi(\alpha X_1 + \beta Y_1, \gamma X_1 + \delta Y_1; \alpha X_2 + \beta Y_2, \gamma X_2 + \delta Y_2)$$
$$\Psi(X_1,Y_1; X_2,Y_2) = (\alpha\delta - \beta\gamma)^3 \psi(\alpha X_1 + \beta Y_1, \gamma X_1 + \delta Y_1; \alpha X_2 + \beta Y_2, \gamma X_2 + \delta Y_2).$$

Let us take α, β, γ, δ in an algebraic extension of k such that $\alpha\delta - \beta\gamma = 1$ and such that F reduces to the canonical form

$$f(\alpha X + \beta Y, \gamma X + \delta Y) = F(X, Y) = 4X^3Y - g_2XY^3 - g_3Y^4.$$

The invariants i, j of Cayley defined by the formulas (I) have then the same value for f and for F, which gives $i = g_2$, $j = g_3$; these invariants are none other than the coefficients of the normal form (said to be of Weierstrass), a form already indicated as such by Hermite in the cited note [1, p. 360]. Let us now write the covariants Φ, Ψ with X_1, Y_1, X_2, Y_2 replaced by $\xi_1, 1, \xi_2, 1$:

$$\Phi(\xi_1, 1; \xi_2, 1) = \frac{1}{4(\xi_1 - \xi_2)^2}[(\xi_1 + \xi_2)(4\xi_1\xi_2 - i) - 2j - 2{F_1}^{1/2}{F_2}^{1/2}]$$

$$\Psi(\xi_1, 1; \xi_2, 1) = \frac{1}{4(\xi_1 - \xi_2)^3}[{F_2}^{1/2}(4{\xi_1}^3 + 12{\xi_1}^2\xi_2 - 3i\xi_1 - i\xi_2 - 4j)$$
$$- {F_1}^{1/2}(4{\xi_2}^3 + 12\xi_1{\xi_2}^2 - i\xi_1 - 3i\xi_2 - 4j)],$$

with

$$F_1 = 4{\xi_1}^3 - i\xi_1 - j, \qquad F_2 = 4{\xi_2}^3 - i\xi_2 - j.$$

In the above formulas, let us write ζ_1, ζ_2 in place of ${F_1}^{1/2}$, ${F_2}^{1/2}$; (ξ_1, ζ_1) and (ξ_2, ζ_2) will then be two points on the curve (III). One also verifies, by a calculation that does not present difficulties, that the point $(\Phi, -\Psi)$ is the third point of intersection of this curve with the line that passes by the two points in question; said another way, the formulas written above for Φ, Ψ are the addition formulas for the curve (III), its point at infinity being taken, as usual, as the neutral element of the group. If one supposes, for example, that the base field k is a subfield of the field of complex numbers, (III) will be uniformized by means of the elliptic functions of Weierstrass by the formulas $\xi = \wp u$, $\zeta = \wp' u$; and, if u_1, u_2 are the elliptic arguments of the points (ξ_1, ζ_1), (ξ_2, ζ_2), one will have

$$\Phi = \wp(u_1 + u_2), \qquad \Psi = \wp'(u_1 + u_2),$$

as one can likewise verify by comparison with the addition formulas of the elliptic functions.

Let us continue making use of the language of elliptic functions; the reader familiar with the theory of abstract abelian varieties, or simply with fields of algebraic functions of genus 1, will have no trouble making the translation in abstract terms, valid for all ground fields of characteristic other than 2 or 3. Let us consider the curve (II); in virtue of the manner in which one has defined F, (II) and (III) are birationally equivalent over the field $k(\alpha, \beta, \gamma, \delta)$, a birational correspondence between the one and the other being given by the formulas

$$x = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}, \qquad z = \frac{\zeta}{(\gamma\xi + \delta)^2}.$$

Said another way, the coordinates x, z of a point of (II) express themselves by means of the elliptic argument u by the formulas

$$x = \frac{\alpha\wp u + \beta}{\gamma\wp u + \delta}, \qquad z = \frac{\wp' u}{(\gamma\wp u + \delta)^2}.$$

Reciprocally, moreover, u is defined as the integral of the differential of the first kind $du = dx/z = d\xi/\zeta$. Letting the points (x_1, z_1), (x_2, z_2) correspond to the elliptic arguments u_1, u_2, then, by virtue of the covariance of φ, ψ, one has:

$$\wp(u_1 + u_2) = \varphi(x_1, 1; x_2, 1), \qquad \wp'(u_1 + u_2) = \psi(x_1, 1; x_2, 1),$$

it being understood that, in the right-hand side, ${f_1}^{1/2}$ and ${f_2}^{1/2}$ are to be replaced by z_1 and z_2, respectively; one can say, from the point of view of the projective theory of biquadratic forms, that one has given a covariant formulation of the addition formulas for elliptic functions.

In order for the two divisors $(x_1, z_1) + (x_2, z_1)$ and $(x_1', z_1') + (x_2', z_2')$ of degree 2 on the curve (II), whose components belong respectively to the elliptic arguments u_1, u_2, u_1', u_2', to be linearly equivalent, it is necessary and sufficient that $u_1 + u_2$ and $u_1' + u_2'$ differ only by a period, that is to say that $\wp$ and $\wp'$ have the same values for these arguments. It follows that there is a birational correspondence between the class of the divisor $(x_1, z_1) + (x_2, z_2)$ on the curve (II) and the point (φ, ψ) on the curve (III), a correspondence expressed by the above formulas. These being rational over k, this result can be interpreted as saying that (III) is the jacobian of (II) over the ground field k.

To retrieve the relation of Cayley–Hermite, one writes φ, ψ in the form

$$\varphi(X_1, Y_1; X_2, Y_2) = \frac{1}{f_{1122} + {f_1}^{1/2}{f_2}^{1/2}} \cdot \frac{{f_{1122}}^2 - f_1 f_2}{2(X_1Y_2 - X_2Y_1)^2}$$
$$\psi(X_1, Y_1; X_2, Y_2) = \frac{1}{{f_2}^{1/2} f_{1112} + {f_1}^{1/2} f_{2221}} \cdot \frac{f_2{f_{1112}}^2 - f_1{f_{2221}}^2}{(X_1Y_2 - X_2Y_1)^3}.$$

A calculation shows that the fractions that figure as second factors of the second equation are in reality polynomials in a, b, c, b', a', X_1, Y_1, X_2, Y_2, and that, if one substitutes (X, Y) both for (X_1, Y_1) and for (X_2, Y_2) in these polynomials, they reduce respectively to $2g(X, Y)$ and to $2h(X, Y)$, where g, h are the covariants considered by Hermite. Said another way, one has:

$$\varphi(X, Y; X, Y) = \frac{g(X,Y)}{f(X,Y)}, \qquad \psi(X, Y; X, Y) = \frac{h(X,Y)}{f(X,Y)^{3/2}},$$

and the relation of Cayley–Hermite expresses that they are the coordinates of a point of the curve (III).

Taking another point of view, one can also say that the curves (II) and (III) form the two components of an algebraic group. For two points of (III), the law of the group is the usual law given by the addition formulas of $\wp u$, $\wp' u$, the neutral element being the point at infinity on (III). For two points of (II), the law of the group is given by the formulas written above, the sum of two such points (x_1, z_1), (x_2, z_2) being then the point (φ, ψ) of (III) that one has made to correspond with the class of the divisor $(x_1, z_1) + (x_2, z_2)$. Finally, to a point (x, z) of (II) and a point (ξ, ζ) of (III), the group law associates the point (x', z') of (II) such that one has the linear equivalence

$$(x, z) + (\xi, \zeta) \sim (x', z') + \infty$$

where (ξ, ζ) is identified with the class of the divisor of degree 2 to which it corresponds on (II), and where ∞ designates the class of the divisor of the poles of x on (II), or, what amounts to the same by the identification in question, the point at infinity on (III). It amounts to the same as saying that (x', z') is determined by the condition that (ξ, ζ) be a point of (III) corresponding to the class of the divisor $(x, -z) + (x', z')$ on (II).

Under this form, our results are susceptible of being generalized as follows. Let C be a curve of genus 1 over a ground field k. For all integers n, there is a curve C_n in birational correspondence over k with the divisor classes of degree n on C. In virtue of the theorem of Riemann–Roch, one can define C_n for $n > 0$ by means of the classes of effective divisors of degree n: C_0 is the jacobian of C, and C_1 can be identified with C; the curves C_n are also birationally equivalent to each other over the algebraic closure of k. Let d be the smallest integer > 0 among the degrees of the divisors on C that are rational with respect to k; then C_m and C_n will be birationally equivalent over k if $m \equiv n \pmod{d}$ and in this case only. Under these conditions, one can define an abelian algebraic group whose components are the curves C_0, C_1, …, C_{d-1}; it admits C_0 as a subgroup, the C_i being the cosets of this subgroup, and the quotient group being cyclic of order d. The case $d = 2$ is essentially the one that has been studied above. As is well known, if k is a field of finitely many elements, one necessarily has $d = 1$; it will be interesting to examine whether d is capable of taking all integer values when k is the field of rationals. Perhaps the above notions might serve to classify the set of curves of genus 1, over a given ground field k, whose jacobian is a given curve; the latter necessarily has a rational point, namely the neutral element of the algebraic group of which it forms the support, and one can then therefore suppose the jacobian to be given in the "Weierstrass" normal form if the characteristic is neither 2 nor 3. For the case $d = 2$, it is possible that the study of this problem could lead to the recovery and the deepening of the results of Hermite on the arithmetic theory of biquadratic forms and in particular on the reduction of these forms, results exposed in the second part of the note that served as our point of departure.

Bibliography

[1] Ch. Hermite, Sur la théorie des fonctions homogènes à deux indeterminées. Premier Mémoire, Oeuvres t. I, p. 350 = J. reine angew. Math. **52**, 1 (1856).

Received 19 October 1953