An analogue of the Weierstrass ζ-function in characteristic p

José Felipe Voloch

To J.W.S. Cassels on the occasion of his 75th birthday.

0. Introduction

Cassels, in [C], has noticed a remarkable analogy between an algebraic function introduced by Deuring [D] in positive characteristic and the Weierstrass ζ-function in the classical theory of elliptic functions. The purpose of this note is to take this analogy further. One of our main goals is to use this function to give a very explicit description of the universal vectorial extension of elliptic curves, which will give a characteristic p analogue of results of Lang and Katz. Also, Mazur and Tate [MT] have defined, for an elliptic curve defined over a local field of residue characteristic p with ordinary reduction, an analogue of the Weierstrass σ-function which is defined on the formal group of the curve. In characteristic p their construction can be performed for an ordinary curve over any field and it turns out, as in the classical theory, that the logarithmic derivative of the Mazur-Tate σ-function is the characteristic p ζ-function.

Acknowledgements: I would like to thank A. Broumas, A. Buium and J. Tate for many helpful conversations and the NSF (grant DMS-9301157) and the Alfred P. Sloan Foundation for financial support.

1. Quick review of the classical case

Let E be an elliptic curve over $\mathbf{C}$ and ω a non-zero holomorphic differential on E. By integrating ω along closed paths on $E(\mathbf{C})$ we get the period lattice Λ and $E(\mathbf{C})$ is isomorphic to $\mathbf{C}/\Lambda$. If E has a Weierstrass equation $y^2 = x^3 + a_4x + a_6$, and $\omega = dx/2y$ then this isomorphism is given by $z \bmod \Lambda \mapsto (\wp(z), (1/2)\wp'(z))$, and $\omega = dz$, where $\wp(z)$ is the Weierstrass $\wp$-function attached to the lattice Λ. It is a periodic meromorphic function with periods Λ, holomorphic in $\mathbf{C} \setminus \Lambda$ and having expansion $\wp(z) = z^{-2} + O(1)$ near

$z = 0$. The Weierstrass ζ-function is, by definition, the unique odd meromorphic function satisfying $d\zeta/dz = -\wp$. It is quasi-periodic, i.e., it satisfies $\zeta(z+\lambda) = \zeta(z) + \eta(\lambda), \lambda \in \Lambda$, where η is linear in λ. The values $\eta(\lambda), \lambda \in \Lambda$ are called the quasi-periods. Finally, it satisfies

$$\zeta(z+w) = \zeta(z) + \zeta(w) + \frac{\wp'(z) - \wp'(w)}{2(\wp(z) - \wp(w))}.$$

(See [A], Ch. 7 and [L], Ch. 18).

The universal extension of E by a vector group is a commutative algebraic group $E^\dagger$ which sits in a non-split exact sequence $0 \to \mathbf{G}_a \to E^\dagger \to E \to 0$. It can be constructed as the group of isomorphism classes of invertible sheaves on E with an integrable connection. Lang ([L], 18.1) and Katz ([K], appendix C) describe $E^\dagger$ in terms of ζ as follows: $E^\dagger(\mathbf{C})$ is isomorphic to $\mathbf{C}^2/\Lambda'$ where $\Lambda' = \{(\lambda, \eta(\lambda)) | \lambda \in \Lambda\}$ and given $(a, v) \in \mathbf{C}^2$ it corresponds to the integrable connection on $\mathcal{O}_E((P) - (0))$, where $P = (\wp(a), 1/2\wp'(a))$, given by the differential $(\zeta(z-a) - \zeta(z) + v)dz$.

2. The characteristic p ζ-function

Let K be a field of characteristic p and E/K an elliptic curve. Let $E^{(p)}$ be the target of Frobenius $F : E \to E^{(p)}$. Let $V : E^{(p)} \to E$ be the dual isogeny, i.e., the Verschiebung. Fix a holomorphic differential ω on E. Choose a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

such that $\omega = dx/(2y + a_1x + a_3)$. If $p \neq 2$, assume further that $a_1 = a_3 = 0$, put $f(x) = x^3 + a_2x^2 + a_4x + a_6$, and define polynomials $U, T \in K[x]$, with $\deg U \leq p-2$, and an element $A \in K$ by:

$$y^{p-1} = f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^pT(x).$$

If $p = 2$ let $A = a_1$. Then A is the Hasse invariant of E. Let B be the coefficient of x^{p-2} of $U(x)$ if p is odd and $B = 1$ for $p = 2$.

Lemma. *For p odd we have $f'(x)T(x) + 2f(x)T'(x) = -Ax + B$.*

Proof. Since $f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^p T(x)$, it follows that

$$((p-1)/2)f(x)^{(p-3)/2} f'(x) = U'(x) - Ax^{p-2} + x^p T'(x),$$

hence

$$x^p(f'(x)T(x) + 2f(x)T'(x)) = -f'(x)(U(x) + Ax^{p-1}) - 2f(x)(U'(x) - Ax^{p-2}).$$

But the last polynomial has degree at most $p+1$, so comparing coefficients, the result follows.

We will consider the function field of E as a subfield of the function field of $E^{(p)}$ via V.

Definition. *The characteristic p Weierstrass ζ-function is the rational function z on $E^{(p)}$ satisfying $z^p - Az = -yT(x), p \neq 2$ and $z^2 - Az = x + a_2, p = 2$ and, if E is ordinary, such that $z + (y/x)$ vanishes at 0.*

It is easy to check that, in the ordinary case, the equation defining z describes a cyclic, étale cover of E of degree p, which has to be $E^{(p)}$ (see [D], pg.254 or [V], lemma 1.1).

Let $\omega^{(p)}$ the differential on $E^{(p)}$ obtained from ω on E by transport of structure.

Proposition 1 (Cassels [C] §5,6). *If E is ordinary, the function z satisfies $z(P+P_0) = z(P) + \eta(P_0)$ for all $P_0 \in \ker V$, where η is linear in P_0 and satisfies $\eta(P_0)^p - A\eta(P_0) = 0$. Furthermore, if $p \neq 2$, z is odd and $dz/\omega = -x + B/A$.*

Proof. (Sketch) Since $z^p - Az$ is invariant under translation by points of $\ker V$, the first part follows, except for the linearity, which is straightforward. From the definition of z, $Adz = d(yT(x)) = (-Ax + B)\omega$, by the lemma.

The values $\eta(P_0), P_0 \in \ker V$ are the analogues of the quasi-periods. The derivation d/ω corresponds to d/dz in the complex case, so z satisfies a similar differential equation as ζ. We will discuss the discrepancy coming from the constant B/A in the next section. The analogue of Proposition 1 in the supersingular case is the equation $dz = -B^p\omega^{(p)}$ which is easily verified. Superficially, this result is analogous to the differential equation satisfied by z in the ordinary case, but is also an analogue of the quasi-periodicity of z. Namely, over a ring with nilpotents, the map $P \mapsto z(Q+P) - z(Q)$ induces an isomorphism η between $\ker V$ and α_p such that the differential dv on α_p (if v is a coordinate on α_p) corresponds to $dz = -B^p\omega^{(p)}$.

The following result gives an addition theorem for z.

Proposition 2. $z(P+Q) = z(P) + z(Q) + \frac{y(Q)-y(P)}{x(Q)-x(P)}$.

Proof. Assume first that E is ordinary. Let Q be a fixed arbitrary point of $E^{(p)}$ and consider $z(P+Q)-z(P)-z(Q)$ as a function of P. It is clearly invariant under translations by points of $\ker V$ and is therefore a function on E. As z has simple poles on the points of $\ker V$ and no others, it follows that $z(P+Q) - z(P) - z(Q)$, as a function on E, has simple poles at 0 and $-V(Q)$ and no others, thus

$$z(P+Q) - z(P) - z(Q) = c(Q)\frac{y(Q) - y(P)}{(x(Q) - x(P))} + d(Q)$$

where $c(Q)$ and $d(Q)$ are some constants depending on Q. But interchanging the roles of P and Q, it follows that $c(Q) = c, d(Q) = d$ are absolute constants. (I learned this trick from A. Broumas in a analogous context). One can then easily check that $c = 1, d = 0$ by making $P, Q \to 0$ and looking at the formal group or by taking d/ω and using the addition formula for x. An alternate proof can be given using the addition formula for the ζ function and proposition 3 of the next section. The supersingular case follows from the generic case by specialization.

3. The Mazur-Tate σ-function

Let K be an algebraically closed field of characteristic p and E/K an ordinary elliptic curve. Let $E^{(p^n)}$ be the image of the n-th iterate of Frobenius $F^n : E \to E^{(p^n)}$. Let $V_n : E^{(p^n)} \to E$ be the dual isogeny, so that V_n are separable, by hypothesis. We will consider the function field of E as a subfield of the function field of $E^{(p^n)}$ via V_n. We will also identify the formal groups of E and $E^{(p^n)}$ via V_n. Assume $p \neq 2$ and choose a function s_n on $E^{(p^n)}$ with divisor $\sum_{P\in\ker V_n}(P) - p^n(0)$. Choose a local parameter t at 0 so that $\omega = (1+O(t))dt$ near 0. Mazur and Tate define the σ-function to be the power series in t given by $\sigma = \lim_{n\to\infty} t^{p^n} s_n$ after normalizing $s_n = t^{p^n-1} + O(t^{p^n})$. We refer to [MT] for the many interesting properties of this function. Let, just as in the classical theory, $\zeta = \sigma^{-1}d\sigma/\omega$.

Proposition 3. *With the above definitions $\zeta = z$.*

Proof. Let $\zeta_n = s_n^{-1}ds_n/\omega$, then $\zeta = \lim \zeta_n$. Note that ζ_n is odd and has simple poles at the points of $\ker V_n$ and no others and that the residues of $\zeta_n\omega$ at the poles is 1. Clearly, these properties uniquely determine ζ_n as a function on $E^{(p^n)}$. But ζ_1, as a function on $E^{(p^n)}$ has these properties also, so $\zeta_1 = \zeta_n, \forall n$. Finally, z was shown to have these same properties (for $n = 1$) in [V], lemma 1.1. However, in [V], there is an inaccuracy, in that the differential dx/y was used when it should have been $dx/2y$ and leads to a factor of -2 being missing throughout the paper. This was pointed out to me by A. Broumas. Also, what is denoted by z in [V] is what is denoted here by $-z$. Anyhow, this completes the proof.

This result leads to an alternative definition of the quasi-periods, as follows. Given $P \in \ker V$, let f be the function on $E^{(p)}$ with divisor $p((P)-(0))$. Then $\eta(P) = -df/f\omega$. To see this, let τ be the operator $\tau h(Q) = h(Q+P)$ on functions h on $E^{(p)}$. Then:

$$\eta(P)\omega = (\tau z - z)\omega = \tau z\omega - z\omega = \tau(ds_1/s_1) - ds_1/s_1 = d(\tau s_1/s_1)/(\tau s_1/s_1).$$

Now, it is clear that $(\tau s_1/s_1)$ has divisor $p(0-(-P))$ and, therefore $f(\tau s_1/s_1) = h^p$ for some function h on $E^{(p)}$ and the result follows.

Note that the function x in the Weierstrass equation for E is determined by ω up to the addition of a constant. Mazur and Tate then noted that a choice for x can be made by letting $x = -d\zeta/\omega$ and called this a canonical eks-function (sic). It now follows from propositions 1 and 3 that this canonical eks-function is characterized, in characteristic $p > 2$, by $B = 0$.

If K is a local field and E has split multiplicative reduction then E is a Tate curve, so it admits a parametrization $E = \mathbf{G}_m/q^{\mathbf{Z}}$, where q is in the maximal ideal of the valuation ring of K and, if u is the parameter on $\mathbf{G}_m$ and we choose $\omega = du/u$, then σ has the following product expansion (See [MT] or [L], Ch. 18):

$$\sigma(u) = (u^{1/2} - u^{-1/2}) \prod_{n=1}^{\infty} \frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2}.$$

By direct substitution one gets the functional equation $\sigma(qu) = -(q^{1/2}u)^{-1}\sigma(u)$. Logarithmic differentiation of these formulas lead to a series expansion for ζ, namely,

$$\zeta(u) = \frac{(u+u^{-1}+2)}{2(u-u^{-1})} + \sum_{n=1}^{\infty} \left(\frac{q^n}{(u-q^n)} - \frac{q^n u}{(1-q^n u)} \right),$$

and to the equation $\zeta(qu) = \zeta(u) - 1$. Now, $E^{(p)}$ is the Tate curve with multiplicative period q^p, and the Verschiebung is induced by the identity on $\mathbf{G}_m$. Therefore q represents a point in $E^{(p)}$ which generates $\ker V$ and the last formula then reads $\eta(q) = -1$, giving the quasi-periods of the Tate curve in characteristic p.

4. The universal vectorial extension

The universal extension of E by a vector group is a commutative algebraic group $E^\dagger$ which sits in a non-split exact sequence $0 \to \mathbf{G}_a \to E^\dagger \to E \to 0$. It can be constructed as the group of isomorphism classes of invertible sheaves of degree zero on E with an integrable connection. In characteristic $p > 0$ it is known (Rosenlicht [R], pg. 704) that $E^\dagger$ splits up to isogeny and that the maximal abelian subvariety of $E^\dagger$ is $E^{(p)}$. The next result makes these facts explicit.

Theorem. *$E^\dagger$ is isomorphic to the quotient of $E^{(p)} \times \mathbf{G}_a$ by the subgroup-scheme given by the graph of the homomorphism $\eta : \ker V \to \mathbf{G}_a$. The isomorphism is obtained by associating to each point $(P, v) \in E^{(p)} \times \mathbf{G}_a$ the connection on $\mathcal{O}_E((V(P)) - (0))$ given by the differential $(f_P + v)\omega$ where $f_P(Q) = z(Q-P) - z(Q)$ is a function on E that has simple poles at $V(P)$ and 0 and the residues of $f_P\omega$ at these points are $1, -1$ respectively.*

Proof. Clearly f_P is invariant by the action of $\ker V$ so defines a function on E and the statement about the poles and residues follow from the corresponding properties of z. Thus we have a map from $E^{(p)} \times \mathbf{G}_a$ to $E^\dagger$, which is clearly surjective. Since $f_{P+P'}(Q) = f_{P'}(Q+P) + f_P(Q)$ it follows that this map is a homomorphism. Finally its kernel corresponds to $P \in \ker V$, so that $f_P = -\eta(P)$, and $v = -f_P = \eta(P)$, as desired.

References

[A] L.V. Ahlfors, *Complex Analysis*, McGraw-Hill, New York, 1966.

[C] J.W.S. Cassels, *Some elliptic function identities*, Acta Arithmetica **XVIII** (1971) 37-52.

[D] M. Deuring, *Die Typen der Multiplicatorenringe elliptischer Functionenkörper*, Hamburger Abhandlungen **14** (1941) 197-272.

[K] N. M. Katz, *The Eisenstein measure and p-adic interpolation*, Amer. J. of Math. **99** (1977) 238-311.

[L] S. Lang, *Elliptic Functions* Addison Wesley, Reading, Mass, 1973.

[MT] B. Mazur and J. Tate, *The p-adic sigma function*, Duke J. of Math. **62** (1991) 663-688.

[R] M.Rosenlicht, *Extensions of vector groups by abelian varieties*, Am. J. of Math., **80** (1958), 685-714.

[V] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990) 247-258.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu