TOKYO J. MATH.
VOL. 17, NO. 2, 1994

Elementary Functions Based on Elliptic Curves

Keiji NISHIOKA

Keio University

1. w-elementary functions.

Let K be an ordinary differential field of characteristic 0 with a single differentiation D. We assume K has the field of constants C which is algebraically closed. We fix a universal extension U of K.

Let R be a differential field extension of K with finite transcendence degree over K. By $\Omega_{R/K}$ denote the R-module of all differentials of R over K and by $d_{R/K}$ the canonical derivation of R to $\Omega_{R/K}$. With D there associates an additive endomorphism D^1 of $\Omega_{R/K}$, satisfying

$$D^1(ad_{R/K}b)=D(a)d_{R/K}b+ad_{R/K}(Db), \qquad a, b\in R .$$

If a and b are algebraically dependent over C then $D^1(ad_{R/K}b)=d_{R/K}(aDb)$ holds (cf. Rosenlicht [3]).

Consider an elliptic curve E defined over C which is given in the Weierstrass form

$$y^2=4x^3-g_2x-g_3 , \qquad g_2, g_3\in C , \quad g_2^3-27g_3^2\neq 0 .$$

By $E(R)$ we denote the set of all R-rational points on E and by $E(R)^*$ the set $E(R)\setminus\{O_E\}$, where O_E denotes the zero element of E. Let $P=(1, x, y)$ be an R-rational point on E. We consider the following three types of peculiar differentials in $\Omega_{R/C}$

$$\omega_I(P)=\frac{d_{R/C}x}{y} \quad \text{and} \quad \omega_{II}(P)=x\frac{d_{R/C}x}{y} .$$

For a point $Q=(1, x(Q), y(Q))\in E(C)^*$ by $\omega_{III}(P; Q)$ we denote the differential in $\Omega_{R/C}$

$$\frac{1}{2}\,\frac{y+y(Q)}{x-x(Q)}\,\frac{d_{R/C}x}{y} .$$

In case $P\in E(C)$ we think that these differentials take the zero differential. In the case where $R=C(x, y)$ with $x\notin C$ any differential ω in $\Omega_{R/C}$ has the unique expression

Received April 20, 1993

$$\omega = df + \alpha\omega_I(P) + \beta\omega_{II}(P) + \sum_{Q\in E(C)^*} \gamma_Q\omega_{III}(P; Q),$$

where $f \in R$, α, β, $\gamma_Q \in C$ (cf. Robert [2, p. 138]).

By φ denote the R-linear mapping of $\Omega_{R/C}$ to R with the property that $\varphi d_{R/C} = D$ and by ϕ_K the R-linear mapping of $\Omega_{R/C}$ to $\Omega_{R/K}$ with the property that $\phi_K d_{R/C} = d_{R/K}$. The existence of these mappings is guaranteed by the universality of the differential module $\Omega_{R/C}$. We also note the fact that the equality $D^1\phi_K = \phi_K D^1$ holds on $\Omega_{R/C}$.

Let R be a differential field extension of K. We assume the field of constants of R is the same as C. Let x, y, u be three elements of R and $P=(1, x, y)$ be a point on some elliptic curve E defined over C. We say that x is a w_I-element of u if

$$Dx/y = Du$$

holds. This means $\varphi(\omega_I(P) - d_{R/C}u) = 0$. For simplicity we omit describing y explicitly. Namely x is regarded as a solution of an algebraic differential equation of the second order. We say that x is a w_{II}-element of u if

$$xDx/y = Du$$

holds. We say also that x is a w_{III}-element of u if for a certain point $Q \in E(C)^*$

$$\frac{1}{2}\,\frac{y+y(Q)}{x-x(Q)}\,\frac{Dx}{y} = Du$$

holds. We conversely say that u is a w_i-integral of x if x is a w_i-element of u, where $i = I, II, III$. We shall furthermore say that x is a w_i-element over K if it is a w_i-element of some element of K. For a w_i-integral we also adopt like wording.

DEFINITION. A w-elementary extension of K is the terminal differential extension W_n of a finite chain of differential field extensions of K:

$$K = W_0 \subset W_1 \subset W_2 \subset \cdots \subset W_n,$$

such that the field of constants of W_n is the same as C and for each i $W_i = W_{i-1}\langle x_i\rangle$, where x_i is over W_{i-1} i) algebraic, or ii) a w_j-element for some j, or iii) a w_j-integral for some j, or iv) an exponential, or v) a logarithm.

Here recall that x is said to be an exponential over K if there is an element $u \in K$ with $Dx/x = Du$ and x is said to be a logarithm over K if there is a nonzero element $u \in K$ with $Dx = Du/u$.

We shall prove the following.

THEOREM. *Let a be an element of K and suppose that there exists a w-elementary extension of K in which an integral of a is contained. Then a can be written in the form*

$$a=Db+\sum_j \alpha_j \frac{Db_j}{b_j}+\sum_i \beta_i \frac{Du_i}{v_i}+\sum_i \gamma_i u_i \frac{Du_i}{v_i}+\sum_i \sum_{Q\in E_i(C)^*} \delta_i(Q)\frac{v_i+v_i(Q)}{u_i-u_i(Q)}\frac{Du_i}{v_i}, \quad (1)$$

where the sums denote finite sums, b, $b_j \in K$, i runs through an index set of a family of elliptic curves E_i defined over C, $(1, u_i, v_i)\in E_i(K)$, and α_i, β_i, $\gamma_i(Q)$, $\delta_i(Q)\in C$.

For the sake of convenience, we call the right member of the above equality the w-expression over K.

A particular case of this theorem is seen in Abel [1], where he deals only with algebraic extensions. His result will be explained in the next section.

2. Abel's theorem.

Let R be a differential field extension of K. For simplicity we here assume that R is algebraically closed. Let E be an elliptic curve defined over C and $P_i=(1, x_i, y_i)\in E(R)$ $(i=1, 2, 3)$ with $P_1\oplus P_2\oplus P_3=O_E$. The additive theorem for differentials of the first kind says

$$\sum_{i=1}^{3} \omega_I(P_i)=0\,, \quad (2)$$

for differentials of the second kind

$$\sum_{i=1}^{3} \omega_{II}(P_i)=\frac{1}{2}d_{R/C}\frac{y_1-y_2}{x_1-x_2}\,, \quad (3)$$

and for differentials of the third kind

$$\sum_{i=1}^{3} \omega_{III}(P_i\,;\,Q)=\frac{d_{R/C}(s(x(Q))-y(Q))}{s(x(Q))-y(Q)}\,, \quad (4)$$

where $Q=(1, x(Q), y(Q))\in E(C)^*$, $s(x)=y_1+((y_1-y_2)/(x_1-x_2))(x-x_1)$.

These formulas are valid even when some of the P_i are equal, though a suitable limit process must be needed. For instance the quotient $(y_1-y_2)/(x_1-x_2)$ is used in the form

$$\frac{y_1^2-y_2^2}{(x_1-x_2)(y_1+y_2)}=\frac{4(x_1^2+x_1x_2+x_2^2)-g_2}{y_1+y_2}$$

when $P_1=P_2$.

The proof can be obtained through the theory of elliptic functions, by the use of Lefschetz' principle. Let z_1, z_2 be new variables, $z_1+z_2+z_3=0$ and $x_i=\wp(z_i)$, $y_i=\wp'(z_i)$. Formulas (2), (3) are obtained respectively by taking the differentials of

$$\sum_i z_i=0\,, \qquad \sum_i \zeta(z_i)=\frac{1}{2}\,\frac{\zeta''(z_1)-\zeta''(z_2)}{\zeta'(z_1)-\zeta'(z_2)}\,.$$

Formula (4) is obtained by taking the logarithmic differential of

$$-\frac{\sigma(z_1-z_0)\sigma(z_2-z_0)\sigma(z_3-z_0)}{\sigma(z_0)^3\sigma(z_1)\sigma(z_2)\sigma(z_3)}=\wp'(z_1)-\wp'(z_0)+\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}(\wp(z_0)-\wp(z_1)),$$

where $Q=(1, \wp(z_0), \wp'(z_0))$. (cf. Whittaker and Watson [4].) Of course, for verification straightforward but somewhat tedious calculation will do, or for more details we must refer to Abel's original paper.

Abel's theorem is this: *Suppose $a\in K$ have a w-expression over a certain algebraic extension of K. Then a has a w-expression over K.*

PROOF. Suppose a has a w-expression over a normal algebraic extension N of K. Let η denote the differential in $\Omega_{N/C}$

$$d_{N/C}b+\sum_j \alpha_j\frac{d_{N/C}b_j}{b_j}+\sum_i \beta_i\frac{d_{N/C}u_i}{v_i}+\sum_i \gamma_i u_i\frac{d_{N/C}u_i}{v_i}+\sum_i \sum_{Q\in E_i(C)^*}\delta_i(Q)\frac{v_i+v_i(Q)}{u_i-u_i(Q)}\frac{d_{N/C}u_i}{v_i},$$

whose image $\varphi\eta$ is the w-expression over N. For each automorphism $\sigma\in Gal(N/K)$ we define a K-vector automorphism σ^* of $\Omega_{N/C}$ by

$$\sigma^*(ud_{N/C}v)=\sigma(u)d_{N/C}\sigma(v), \qquad u, v\in N.$$

Then clearly $\sigma\varphi=\varphi\sigma^*$ holds on $\Omega_{N/C}$. Since σ is a differential one, $\sigma\varphi\eta$ is a w-expression of a over N. According to formulas (2), (3), (4), the differential $\xi=\sum_{\sigma\in Gal(N/K)}\sigma^*\eta$ consists of differentials in $\Omega_{K/C}$ which are of the same types as in η. The expression $\varphi\xi$ is a w-expression of $a|Gal(N/K)|$ over K. This completes the proof.

3. Two lemmas.

We here assume that K is algebraically closed.

LEMMA 1. *Let $P_i=(1, x_i, y_i)$, $i=1, 2$, be respectively non C-rational points on elliptic curves E_i defined over C. Suppose that $R=K(x_1, y_1)$ is a differential field extension of K with the field of constants C, $x_2, y_2\in R$ and x_2 has a pole at O_{E_1}. Then $x_2, y_2\in C(x_1, y_1)$ and $d_{R/C}x_2/y_2=cd_{R/C}x_1/y_1$, $c\in C$.*

PROOF. Since $d_{R/K}x_2/y_2$ is a differential of the first kind, there is a $c\in K$ with $d_{R/K}x_2/y_2=cd_{R/K}x_1/y_1$. Applying D^1, we have

$$d_{R/K}\left(\frac{Dx_2}{y_2}\right)=D(c)\frac{d_{R/K}x_1}{y_1}+cd_{R/K}\left(\frac{Dx_1}{y_1}\right),$$

and hence $Dc=0$, namely $c\in C$. Let t denote a uniformizing parameter at O_{E_1} and $\wp_i\in K((t))$ denote the solution of the equation with a pole at $t=0$

$$\left(\frac{dy}{dt}\right)^2 = 4y^3 - g_{i2}y - g_{i3} ,$$

where g_{i2}, g_{i3} are the constants appearing in the defining equation for E_i. As a matter of fact $\wp_i \in C((t))$. Then we have a representation $x_1 = \wp_1(t)$, $y_1 = \wp'_1(t)$ and x_2, y_2 as elements of $K((t))$ satisfy the equation $dx_2/dt = cy_2$. Hence $x_2 = \wp_2(ct)$, $y_2 = \wp'_2(ct)$ are contained in $C((t))$.

Recall the following well-known fact: Let R be a rational function field over K. Suppose a differential

$$\xi = d_{R/C}e + \sum_j \kappa_j \frac{d_{R/C}e_j}{e_j} \in \Omega_{R/C} ,$$

the κ_j being linearly independent over the rational number field, satisfies $\phi_K \xi = 0$. Then $e, e_j \in K$.

This turns out to be a special case of the following, by thinking of rational function fields as subfields of certain elliptic function fields.

LEMMA 2. *Let E be an elliptic curve defined over C and $P = (1, x, y)$ a non K-rational point on E and $R = K(x, y)$. Given a differential in $\Omega_{R/C}$*

$$\xi = d_{R/C}e + \sum_j \kappa_j \frac{d_{R/C}e_j}{e_j} + \lambda\omega_I(P) + \mu\omega_{II}(P) + \sum_{Q \in E(C)^*} \nu(Q)\omega_{III}(P; Q) ,$$

with κ_j, λ, μ, $\nu(Q) \in C$, κ_j being linearly independent over the field of rational numbers. Suppose that $\phi_K \xi = 0$. Then $e \in K$, $\mu = 0$ and there exist the $f_j \in K$ with

$$\sum_j \kappa_j \frac{d_{R/C}f_j}{f_j} = \sum_j \kappa_j \frac{d_{R/C}(e_j)}{e_j} + \lambda\omega_I(P) + \sum_{Q \in E(C)^*} \nu(Q)\omega_{III}(P, Q) .$$

PROOF. Usual argument on poles readily draws the first assertion. Hence

$$\sum_j \kappa_j \frac{d_{R/K}e_j}{e_j} + \lambda\phi_K\omega_I(P) + \sum_{Q \in E(C)^*} \nu(Q)\phi_K\omega_{III}(P; Q) = 0 .$$

Let $Q \in E(K)$ and $m_j(Q)$ denote the residue of $d_{R/K}e_j/e_j$ at Q. If Q neither effectively appears in the above sum nor equals O_E, then $\sum_j \kappa m_j(Q) = 0$, which implies $m_j(Q) = 0$. For Q with $\nu(Q) \neq 0$, $\sum_j \kappa_j m_j(Q) + \nu(Q) = 0$. Hence there exists a $\lambda_j \in K$ such that

$$\frac{d_{R/K}e_j}{e_j} = \lambda_j\phi_K\omega_I(P) + \sum_Q m_j(Q)\phi_K\omega_{III}(P; Q) ,$$

with $\lambda + \sum_j \kappa_j\lambda_j = 0$. Applying D^1 to this,

$$d_{R/K}\left(\frac{De_j}{e_j} - \lambda_j \frac{Dx}{y} - \sum_Q m_j(Q) \frac{y + y(Q)}{x - x(Q)} \frac{Dx}{y}\right) = D(\lambda_j)\phi_K\omega_I(P) ,$$

and hence $\lambda_j \in C$. Let $P=(1, \wp(t), \wp'(t))$, with t a uniformizing parameter at O_E. Then $Y=e_j$ satisfies

$$\frac{1}{Y}\frac{dY}{dt}=\lambda_j+\sum_Q m_j(Q)\frac{y+y(Q)}{(x-x(Q))}\,.$$

If we denote by f_j the coefficient of the first term in $e_j \in K((t))$, $z_j=e_j/f_j \in C((t)) \cap R = C(x, y)$ also satisfies the above. The element $z_j \in R$ satisfies

$$\frac{d_{R/C}z_j}{z_j}=\lambda_j\omega_I(P)+\sum_Q m_j(Q)\omega_{III}(P; Q)\,.$$

Consequently

$$\sum_j \kappa_j \frac{d_{R/C}f_j}{f_j}=\sum_j \frac{d_{R/C}(e_j)}{e_j}-\sum_j \kappa_j \frac{d_{R/C}z_j}{z_j}$$
$$=\sum_j \frac{d_{R/C}(e_j)}{e_j}+\lambda\omega_I(P)+\sum_Q \nu(Q)\omega_{III}(P, Q)\,.$$

4. Proof of Theorem.

By induction on the length of chain we prove the theorem. As easily seen in the induction argument, thanks for the theorem of Abel, it is sufficient to show that a has a w-expression over K provided K is algebraically closed and a has a w-expression over a certain w-elementary extension of K generated by a single element x which satisfies one of the conditions (ii)$\sim$(v) over K. Let R denote the differential field extension $K\langle x\rangle$ of K. Assume $a \in K$ has the w-expression over R:

$$a=Db+\sum_j \alpha_j \frac{Db_j}{b_j}+\sum_i \beta_i \frac{Du_i}{v_i}+\sum_i \gamma_i u_i \frac{Du_i}{v_i}+\sum_i \sum_{Q\in E_i(C)^*} \delta_i(Q)\frac{v_i+v_i(Q)}{u_i-u_i(Q)}\frac{Du_i}{v_i}\,.$$

Let η be the differential in $\Omega_{R/C}$ defined by

$$\eta=d_{R/C}b+\sum_j \alpha_j \frac{d_{R/C}b_j}{b_j}+\sum_i \beta_i \frac{d_{R/C}u_i}{v_i}+\sum_i \gamma_i u_i \frac{d_{R/C}u_i}{v_i}$$
$$+\sum_i \sum_{Q\in E_i(C)^*} \delta_i(Q)\frac{v_i+v_i(Q)}{u_i-u_i(Q)}\frac{d_{R/C}u_i}{v_i}\,. \tag{5}$$

We then have $a=\varphi\eta$ and $D^1\phi_K\eta=0$ because the left member is $\phi_K D^1\eta=\phi_K d_{R/C}a=d_{R/K}a=0$.

The argument is divided into several cases, according as (ii)$\sim$(v).

1) $Dx \in K$. Since the field $R=K(x)$ has genus 0, differentials of types ω_k appearing in (5) are all elements of $\Omega_{K/C}$. Hence $\phi_K\eta$ contains only exact and logarithmic differentials. Since $D^1 d_{R/K}x=d_{R/K}Dx=0$, if we let $\phi_K\eta=c d_{R/K}x$, $c \in R$, we see $c \in C$.

Therefore

$$d_{R/K}(b-cx)+\sum_j \alpha_j \frac{d_{R/L}b_j}{b_j}=0\,.$$

By Lemma 2, $e=b-cx\in K$ and part of logarithmic differentials in (5) is represented by a C-linear combination of those in $\Omega_{K/C}$, say ξ. Replacing $d_{R/C}b$ by $d_{R/C}e+cd_{R/C}x$ and using ξ, we rewrite η. Since Dx has a w-expression over K, so has $a=\varphi\eta$.

2) $Dx/x\in K$. As in the preceding it is seen that differentials of types ω_k in (5) are those in $\Omega_{K/C}$. Since $d_{R/K}x/x$ vanishes when applying D^1 there is a constant c with $\phi_K\eta=cd_{R/K}x/x$. Hence

$$db+\sum_j \alpha_j \frac{d_{R/K}b_j}{b_j}-c\frac{d_{R/K}x}{x}=0\,.$$

By Lemma 2, $b\in K$ and part of logarithmic differentials in η are represented by a C-linear combination of those in $\Omega_{K/C}$ and $d_{R/C}x/x$. Using these and the fact that Dx/x has a w-expression over K, making a suitable modification in the expression of η, we see a has a w-expression over K.

From now on we treat the case where x is a w_k-element over K for some k in relation to an elliptic curve E defined over C. Before going ahead, we modify expression (5) of η in a more convenient form. According to formulas (2), (3), (4), we may assume that either the elements u_i has a pole at the zero element O_E of E or $u_i\in K$. Using Lemma 1, this time, $C(u_i, v_i)\subset C(x, y)$. In the first case differentials of types ω_k in (5) are thus described as a C-linear combination of $\omega_I(P)$, $\omega_{II}(P)$, $\omega_{III}(P;Q)$ and exact differentials in $\Omega_{C(x,y)/C}$. Here we set $P=(1, x, y)$. Consequently η has the expression

$$\begin{aligned}\eta=d_{R/C}b&+\sum_j \alpha_j\frac{d_{R/C}b_j}{b_j}+\sum_i \beta_i\frac{d_{R/C}u_i}{v_i}+\sum_i \gamma_i u_i\frac{d_{R/C}u_i}{v_i}\\&+\sum_i\sum_{Q\in E_i(C)^*}\delta_i(Q)\frac{v_i+v_i(Q)}{u_i-u_i(Q)}\,\frac{d_{R/C}u_i}{v_i}+\lambda\omega_I(P)+\mu\omega_{II}(P)\\&+\sum_{Q\in E(C)^*}\nu(Q)\omega_{III}(P;Q)\,,\end{aligned}\tag{6}$$

where $b, b_j\in R$, $u_i, v_i\in K$, α_j, β_i, γ_i, $\delta_i(Q)$, λ, μ, $\nu(Q)\in C$. We may assume that the α_j are linearly independent over rational number field. Applying ϕ_K to this,

$$\phi_K\eta=d_{R/K}b+\sum_j \alpha_j\frac{d_{R/K}b_j}{b_j}+\lambda\phi_K\omega_I(P)+\mu\phi_K\omega_{II}(P)+\sum_{Q\in E(C)^*}\nu(Q)\phi_K\omega_{III}(P;Q)\,.$$

3) $\varphi\omega_I(P)\in K$. Then we first find $\phi_K\eta=c\phi_K\omega_I(P)$, $c\in C$, since $D^1\phi_K\omega_I(P)=0$. By Lemma 2, b, $b_j\in K$, $\mu=0$, and there exist the f_j with

$$\sum_j \alpha_j \frac{d_{R/C} f_j}{f_j} = \sum_j \alpha_j \frac{d_{R/C} b_j}{b_j} + (\lambda - c)\omega_I(P) + \sum_{Q \in E(C)^*} \nu(Q)\omega_{III}(P\,;Q)\,.$$

Since Dx/y has a w-expression over K by assumption, this together with (6) shows a has a w-expression over K.

4) $\varphi\omega_{II}(P) \in K$. By the same argument as above, $\phi_K \eta = c\phi_K \omega_{II}(P)$, $c \in C$. By Lemma 2, b, $b_j \in K$, $\mu = c$ and there exist the f_j with

$$\sum_j \alpha_j \frac{d_{R/C} f_j}{f_j} = \sum_j \alpha_j \frac{d_{R/C} b_j}{b_j} + \lambda\omega_I(P) + \sum_{Q \in E(C)^*} \nu(Q)\omega_{III}(P\,;Q)\,.$$

Using the assumption $\varphi\omega_{II}(P)$ has a w-expression over K, we see a has a w-expression over K.

5) $\varphi\omega_{III}(P\,;Q_0) \in K$. Readily $\phi_K \eta = c\phi_K \omega_{III}(P\,;Q_0)$, $c \in C$. Owing to this, b, $b_j \in K$, $\mu = 0$ and there exist the f_j with

$$\sum_j \alpha_j \frac{d_{R/C} f_j}{f_j} = \sum_j \alpha_j \frac{d_{R/C} b_j}{b_j} + \lambda\omega_I(P) + \sum_{Q \in E(C)^*} \nu(Q)\omega_{III}(P\,;Q) - c\omega_{III}(P, Q_0)\,.$$

Therefore a has a w-expression over K.

We thus complete the proof.

References

[1] N. H. Abel, Précis d'une théorie des fonctions elliptiques, J. Math. **1** (1826), 185–221.
[2] A. Robert, *Elliptic Curves*, Lecture Notes in Math. **326** (1973), Springer.
[3] M. Rosenlicht, The nonminimality of the differential closure, Pacific J. Math. **52** (1974), 529–537.
[4] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge Univ. Press (1958).

Present Address:
Faculty of Environmental Information, Keio University at SFC,
5322 Endoh, Fujisawa, 252 Japan.