A NOTE ON WEIERSTRASS POINTS

DONALD L. McQUILLAN

1. In **(4)** G. Lewittes proved some theorems connecting automorphisms of a compact Riemann surface with the Weierstrass points of the surface, and in **(5)** he applied these results to elliptic modular functions. We refer the reader to these papers for definitions and details. It is our purpose in this note to point out that these results are of a purely algebraic nature, valid in arbitrary algebraic function fields of one variable over algebraically closed ground fields (with an obvious restriction on the characteristic). We shall also make use of the calculation carried out in **(5)** to obtain a rather easy extension of a theorem proved in **(6**, p. 312**)**.

The methods and ideas used here have two sources, namely, (i) two papers of Hecke **(2, 3)** where he analyses completely the representation of $\mathrm{LF}(2, p)$ obtained from the action of this group on the differentials of the first kind in the field of elliptic modular functions of level p, and (ii) a paper of Chevalley and Weil **(1)** extending these ideas to an arbitrary compact Riemann surface.

Let K be an algebraic function field of one variable with field of constants k; it is assumed that k is algebraically closed and of arbitrary characteristic p. Let σ be an automorphism of K of the order N, where $(p, N) = 1$. We denote by G the cyclic group generated by σ and by L the subfield of K left fixed by G. Let $A(K)$ denote the differentials of the first kind of K; $A(K)$ is a vector-space over k of dimension g where g is the genus of K. Now $A(K)$ is a $k - G$ module and so it yields a representation R of G in the general linear group of $g \times g$ matrices over k. By the theory of group representations **(7)** R is equivalent to a representation by diagonal matrices since G is Abelian, k is algebraically closed, and $(p, N) = 1$. The N irreducible representations of G in k are defined by $\psi_b(\sigma) = \epsilon^b$, where ϵ is a primitive Nth root of unity and $0 \leqslant b \leqslant N - 1$, and so we can assume that

$$R(\sigma) = \mathrm{diag}\{\ldots, \psi_b(\sigma), \ldots\}.$$

We call $M(b)$ the multiplicity of ψ_b in R and proceed to sketch a method for computing this multiplicity; cf. **(6)**, for example.

Since K is a Kummer extension of L there exists θ in K such that $K = L(\theta)$, $\sigma(\theta) = \epsilon\theta$, and $\theta^N = f$, where $f \in L$. If $\mathfrak{P}$ is a typical place of L and P a place of K lying over $\mathfrak{P}$, then we denote by $e(\mathfrak{P})$ the ramification index of P over $\mathfrak{P}$ and by $m(\mathfrak{P})$ the valuation of θ at P (it is clear that these integers depend only on $\mathfrak{P}$ and that $m(\mathfrak{P})$ and $e(\mathfrak{P})$ are relatively prime). Now $M(b)$ is just the

Received July 6, 1965. This work was supported by a National Science Foundation grant.

dimension (over k) of that subspace of $A(K)$ consisting of differentials ω with the property that $\sigma(\omega) = \psi_b(\sigma)\omega$. But these are precisely the differentials ω which satisfy $\sigma(\theta^{-b}\omega) = \theta^{-b}\omega$, so that $\theta^{-b}\omega \in A(L)$, i.e. $\omega = \theta^b\phi\omega^*$, where ω^* is a fixed non-zero differential of L and $\phi \in L$. It follows that $M(b)$ is the dimension (over k) of the space of functions ϕ in L with the property that $\theta^b\phi\omega^* \in A(K)$. One applies the Riemann–Roch theorem in a standard way to obtain

THEOREM 1. *The multiplicity $M(b)$ of ψ_b in R is given by*

$$M(b) = g^* - 1 + \sum_{\mathfrak{P}} \langle -bm(\mathfrak{P})/e(\mathfrak{P}) \rangle + s(b).$$

Here $\langle x \rangle$ denotes the fractional part of the real number x, g^* is the genus of L, $s(b) = 1$ if $b = 0$ and $s(b) = 0$ otherwise, and the summation extends over all places $\mathfrak{P}$ of L.

The theorems of Lewittes referred to above are easy consequences of this result. Thus we have

THEOREM 2. (i) $M(0) = g^*$.

(ii) *If $r(b)$ denotes the number of places $\mathfrak{P}$ with the property that $e(\mathfrak{P})$ does not divide b, then*

$$g^* - 1 + r(b)(N-1)/N \geqslant M(b) \geqslant g^* - 1 + r(b)/N.$$

In particular if $r(b) = 0$ $(b \not\equiv 0)$, then

$$M(b) = g^* - 1.$$

(iii) *If $(b, N) = 1$, then*

$$r - g^* + 1 - (2g-2)/N \leqslant M(b) \leqslant 3g^* - 3 + (2g-2)/N,$$

where r is the total number of places of L which ramify in K.

Proof. (i) is obvious; now, if $e(\mathfrak{P})$ does not divide b, then

$$\frac{1}{N} \leqslant \frac{1}{e(\mathfrak{P})} \leqslant \left\langle \frac{-bm(\mathfrak{P})}{e(\mathfrak{P})} \right\rangle \leqslant \frac{e(\mathfrak{P}) - 1}{e(\mathfrak{P})} \leqslant \frac{N-1}{N}.$$

Part (ii) follows at once and part (iii) follows from the fact that

$$2g - 2 = (2g^* - 2)N + N \sum_{\mathfrak{P}} (e(\mathfrak{P}) - 1)/e(\mathfrak{P}),$$

i.e., from the relative genus formula applied to the tamely ramified extension K/L.

This is in fact a slightly stronger statement than that of **(4)**.

We have already remarked that the representation R of $A(K)$ can be brought to diagonal form and so there is a basis $\omega_1, \omega_2, \ldots, \omega_g$ of $A(K)$ such that for each subscript i there exists a b with the property $\sigma(\omega_1) = \epsilon^b \omega_i$. Suppose now that $\sigma(P) = P$ for some place P of K and that ω_i has a zero of order $\gamma_i - 1$ at P, with say $\gamma_1 < \gamma_2 < \ldots < \gamma_g$. Then $\gamma_i \equiv b \pmod{N}$ by the preceding

https://doi.org/10.4153/CJM-1967-018-8 Published online by Cambridge University Press

choice of the basis $\omega_1, \omega_2, \ldots, \omega_g$. On the other hand, by the Weierstrass gap theorem, $\{\gamma_1, \gamma_2, \ldots, \gamma_g\}$ is the so-called gap-sequence at P. Thus $M(b)$ is just the number of gaps at P which are congruent to b modulo N. It follows that if P is not a Weierstrass point, i.e., if $\gamma_i = i$ for $i = 1, 2, \ldots, g$, then $g^* = M(0) = [g/N]$. From the relative genus formula applied to K/L we then get the following theorem.

THEOREM 3. *If $\sigma(P) = P$ for some place P and P is not a Weierstrass point, then*

$$\sum_{\mathfrak{P}} \left(1 - \frac{1}{e(\mathfrak{P})}\right) = 2\left\langle \frac{g}{N} \right\rangle + 2\frac{N-1}{N}.$$

Now if σ fixes more than four places of K the above equality is violated and so we can state

COROLLARY 1. *If σ fixes more than four places of K, then each fixed place is a Weierstrass point.*

Similarly one has

COROLLARY 2. *If $g \equiv 0 \pmod{N}$ and σ fixes more than two places of K, then each fixed place is a Weierstrass point.*

As was noted in **(5)**, the results of Schoeneberg **(8)** on Weierstrass points in the fields of elliptic modular functions with level can be deduced from Corollary 1. Our proof shows that these results are still valid in these fields when the characteristic is positive but does not divide the level and is different from 2 and 3.

2. Now let K be the field of elliptic modular functions of level N. For simplicity we shall assume that N is odd, say $N = p_1^{n_1} p_2^{n_2} \ldots p_t^{n_t}$, where the p_i are distinct odd primes and put $n = p_1 p_2 \ldots p_t$. K is a finite Galois extension of $C(j)$, where j is the Weierstrass invariant, and the Galois group is $\mathrm{LF}(2, N)$. The element

$$S = \pm\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

has the order N and generates the inertia group of a place of K lying over $j = \infty$. From Theorem 1 of §1 (cf. **(6)**) or from **(5)** one gets, by taking $\sigma = T$,

$$M(b) = g^* - 1 + \sum_{d \mid N} \phi(N/d) 2^{Q(d)-1} \sum_{\substack{(r,\, d)=1 \\ r > o(d)}} \left\langle \frac{-br}{d} \right\rangle,$$

where $r > o(d)$ means that r is a quadratic residue modulo d and $Q(d)$ is the number of distinct prime divisors of d.

If $R(N)$ is the multiplicative group of residues modulo N which are relatively prime to N, then we can define a homomorphism,

$$f_N: R(N) \to Z_2 \times Z_2 \times \ldots Z_2 \quad (t \text{ factors}),$$

https://doi.org/10.4153/CJM-1967-018-8 Published online by Cambridge University Press

by $f_N(a) = [(a/p_1), (a/p_2), \ldots, (a/p_t)]$, where (a/p) is the Legendre symbol. This homomorphism is surjective by the Chinese remainder theorem and $a \in \ker(f_N)$ if and only if a is a quadratic residue modulo N. If, for instance, $f_N(a) = f_N(b) = (e_1, e_2, \ldots, e_t) = e$, then we shall say that a and b are of the same type e relative to N and write

$$a \overset{N}{\sim} b (\overset{N}{\sim} e).$$

THEOREM. *If a and b are of the same type e relative to N, then*

$$M(a) = M(b) (= M(e) \text{ say}).$$

If $n \equiv 3 \pmod 4$ and $n > 3$, then

$$\sum_e \operatorname{sgn}(e) M(e) = (2^{t-1}N/n) h(-n),$$

where $h(-n)$ is the class-number of the imaginary quadratic field $Q(\sqrt{-n})$, and

$$\operatorname{sgn}(e) = \prod_{i=1}^{t} e_i.$$

Proof. Let d be a divisor of N. Since $a \overset{N}{\sim} b$, it follows that $a \overset{d}{\sim} b$, and so the cosets $a.\ker(f_d)$ and $b.\ker(f_d)$ are the same. Therefore,

$$\sum_{\substack{(r,\,d)=1 \\ r>o(d)}} \left\langle \frac{-ar}{d} \right\rangle = \sum_{\substack{(r,\,d)=1 \\ r>o(d)}} \left\langle \frac{-br}{d} \right\rangle$$

and so $M(a) = M(b)$, which proves the first part of the theorem. Now if $a \overset{N}{\sim} e$ we set

$$c(d) = \sum_e \operatorname{sgn}(e) \sum_{\substack{(r,\,d)=1 \\ r>o(d)}} \left\langle \frac{-ar}{d} \right\rangle.$$

By rearranging subscripts we may assume that $d = p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s}$, where $1 \leqslant s \leqslant t$ and $d_i > 0$ for $i = 1, 2, \ldots, s$. By what we have just proved, it follows that

$$c(d) = \sum_e \sum_x \operatorname{sgn}(e) \langle -x/d \rangle,$$

where the second summation is over a complete set of integers x such that $(x, d) = 1$ and x is of type $(e_1, e_2, \ldots, e_s)$ relative to d. If $s < t$, it is clear that $c(d) = 0$. Thus the only divisors d of N which contribute to $\sum_e \operatorname{sgn}(e) M(e)$ are those which are divisible by *all* the distinct prime divisors of N. We now show that $c(d) = c(n)$ for such a divisor d. If $d = n$, there is nothing to prove and so we may assume that $d = p\delta$, where δ is again such a divisor and $p = p_i$ for some i. Let $\{a_i\}$ be a complete set of integers of type $(e_1, \ldots, e_t) = e$ relative to δ and less than δ, where $i = 1, 2, \ldots, \phi(\delta)/2^t$. Then $\{a_i + mp\}$, where $i = 1, 2, \ldots, \phi(\delta)/2^t$ and $m = 0, 1, 2, \ldots, p - 1$, gives a complete set

of type $(e_1, \ldots, e_t)$ relative to d and less than d. Therefore

$$\sum_{\substack{d \\ a \sim e}} \left\langle \frac{-a}{d} \right\rangle = \sum_{i,m} \left\langle -\frac{a_i + mp}{d} \right\rangle$$

$$= \sum_{i,m} \frac{(p-m)\delta - a_i}{p\delta}$$

$$= \sum_{i} \left\{ \left\langle \frac{-a_i}{\delta} \right\rangle + \frac{1}{2}(p-1) \right\}.$$

Consequently $c(d) = c(\delta)$ and by repeating the argument we get $c(d) = c(n)$. It follows now that

$$\sum_e \operatorname{sgn}(e) M(e) = 2^{t-1} \sum_d \phi(N/d) \sum_{(a,n)=1} \operatorname{sgn}(a) \langle -a/n \rangle,$$

where d runs through all divisors d of N such that $p_i | d$ for $i = 1, 2, \ldots, t$, and

$$\operatorname{sgn}(a) = \prod_{i=1}^{t} (a/p_i).$$

For such d one easily sees that $\sum_d \phi(N/d) = N/n$. Finally, since

$$\operatorname{sgn}(a) = \prod_{i=1}^{t} (a/p_i) = (-n/a),$$

where $(-n/a)$ is the Kronecker symbol, we have

$$\sum \operatorname{sgn}(a) \langle -a/n \rangle = h(-n).$$

The statement of the theorem follows at once.

References

1. C. Chevalley and A. Weil, *Ueber das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers*, Abh. Math. Sem. Univ. Hamburg, *10* (1934), 358–361.
2. E. Hecke, *Ueber ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg, *6* (1928), 235–257.
3. ——— *Ueber das Verhalten der Integrale 1. Gattung bei Abbildungen . . .*, Abh. Math. Sem. Univ. Hamburg, *8* (1930), 271–281.
4. G. Lewittes, *Automorphisms of compact Riemann surfaces*, Amer. J. Math., *85* (1963), 734–752.
5. ——— *Gaps at Weierstrass points for the modular group*, Bull. Amer. Math. Soc., *69* (1963), 578–582.
6. D. L. McQuillan, *A generalization of a theorem of Hecke*, Amer. J. Math., *84* (1962), 306–316.
7. I. Reiner and C. Curtis, *Representation theory of finite groups and associative algebras* (New York, 1962).
8. B. Schoeneberg, *Ueber die Weierstrass Punkte in den Körpern der Elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg, *17* (1951), 104–111.

University of Wisconsin,
Madison