GAPS AT WEIERSTRASS POINTS FOR THE MODULAR GROUP

BY JOSEPH LEWITTES[1]

Communicated by Felix Browder, April 15, 1963

Let S be a compact Riemann surface of genus $g \geqq 2$, $h: S \to S$ an automorphism of order N, and H the cyclic group of order N generated by h. One has a representation of H by letting it act on the g complex-dimensional space A_1 of abelian differentials of the first kind on S by $h: \varphi \to \varphi h$ for all $\varphi \in A_1$. At each point $P \in S$ there is a gap sequence $\gamma(P) = \gamma_1(P), \cdots, \gamma_g(P)$ where the $\gamma_j(P)$ are integers satisfying $1 = \gamma_1(P) < \gamma_2(P) < \cdots < \gamma_g(P) < 2g$ such that there is no function on S having a pole of order $\gamma_j(P)$ at P and everywhere else finite. The complementary integers to $\gamma(P)$ in the sequence of integers from 1 to $2g$ are the nongaps at P. A point is a Weierstrass point if $\gamma_g(P) > g$.

In [3] the following was proved:

(I) Suppose $P = h(P)$ is a fixed point for h with gap sequence $\gamma_1, \cdots, \gamma_g$ and that h rotates at P by ϵ, i.e., if z is a local parameter at P, $z(P) = 0$, then $h(z) = \epsilon z + \cdots$, $\epsilon^N = 1$. Then, with respect to a suitable basis for A_1, h is represented by the diagonal matrix $(h) = \text{diag}\,(\epsilon^{\gamma_1}, \epsilon^{\gamma_2}, \cdots, \epsilon^{\gamma_g})$.

A corollary of this is

(II) If $P = h(P)$ is not a Weierstrass point then h has at most four fixed points. Thus if h has more than four fixed points all its fixed points are Weierstrass points.

Let Γ be the inhomogeneous modular group, $\Gamma(N)$ the principal congruence subgroup of level $N > 2$, $S(N)$ the compactified fundamental domain for $\Gamma(N)$ which is a Riemann surface of genus $g(N) = 1 + N^2(N-6)/24 \prod_{p|N} (1 - 1/p^2)$ where the product is over primes dividing N. For details see Chapter 1 of [2]. $\Gamma/\Gamma(N)$ is a group of automorphisms of $S(N)$ whose fixed points are at three kinds of points. Firstly, parabolic points (cusps), equivalent under $\Gamma/\Gamma(N)$ to ∞ which is fixed under the cyclic group of order N generated by (the coset of) $T: \tau \to \tau + 1$. Secondly, elliptic points of order 2, equivalent to $i = \sqrt{-1}$ which is fixed under the cyclic group of order 2 generated by $S: \tau \to -1/\tau$. Thirdly, elliptic points of order 3, equivalent to $\rho = e^{2\pi i/3}$ which is fixed under the cyclic group of order 3 gener-

[1] Supported by NSF G-18929. The author wishes to acknowledge his gratitude to Professor H. E. Rauch for suggesting this area of research and helping to see it through and also to Professor D. J. Newman for several enlightening discussions.

ated by $ST: \tau \to -1/(\tau+1)$. Equivalent points have the same gap sequence. Observe that the rotation at ∞ by T is $e^{2\pi i/N}$, at i by S is -1, at ρ by ST is ρ^2.

Schoeneberg [4] has shown that for $N \geqq 7$ the cusps are Weierstrass points and that except for some doubtful cases but certainly for $N \geqq 13$ all elliptic points are Weierstrass points. For the elliptic points he computes the number of fixed points for S and ST and one sees that for $N > 13$ this number is greater than four so that the result follows from (II) above. The doubtful cases are precisely when the number of fixed points is not greater than four.

Let $N > 2$, $d \mid N$, $d \neq N$, denote by $F(d)$ the number of points on $S(N)$ fixed under T^d and by $f(d)$ the number of points fixed under T^d but not under any T^e for $e \mid d$, $e \neq d$. Clearly $F(d) = \sum_{e \mid d} f(e)$. Any cusp $P \in S(N)$ may be written as $P = U(\infty)$ for some $U \in \Gamma$ and is fixed under T^d if and only if $U^{-1}T^dU(\infty) = \infty$. But any element of $\Gamma/\Gamma(N)$ of order N/d leaving ∞ fixed is necessarily of the form T^{dr}. Thus $U^{-1}T^dU = T^{dr}$ and we see that T^d rotates at P by $e^{2\pi i dr/N}$. Thus $F(d)$ is $1/2N$ times the number of incongruent mod N matrices of integers

$$V = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

satisfying

$$\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 1 & dr \\ 0 & 1 \end{pmatrix} \pmod{N} \tag{1}$$

subject to

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{N}. \tag{2}$$

The factor $1/2N$ arises because $\pm V$ are incongruent solutions which determine the same transformation U and for every $P = U(\infty)$ we have $P = UT^k(\infty)$ for $1 \leqq k \leqq N$.

(1), (2) reduce to $\gamma \equiv 0 \pmod{N/d}$ and $\alpha\delta \equiv \alpha^2 r \equiv 1 \pmod{N/d}$ showing that α, δ are inverse units and r a quadratic residue mod N/d. γ mod N has d possible values, $\gamma_k = k(N/d)$, $1 \leqq k \leqq d$. (2) implies $(\alpha, \gamma_k, N) = 1$ and since $(\gamma_k, N) = (k, d)N/d$ we have $(\alpha, (k, d)N/d) = 1$ so α mod $(k, d)N/d$ has $\phi((k, d)N/d)$ values (ϕ being the Euler ϕ function) or α mod N has $d/(k, d)\phi((k, d)N/d)$ values. For each permissible value mod N of α and γ there are N incongruent pairs β, δ satisfying (2), (see [2, p. 9]). Thus the number of incongruent solutions of (1) and (2) is $N\sum_{k=1}^{d} d/(k, d)\phi((k, d)N/d)$, which, upon collecting together for $e \mid d$ the $\phi(d/e)$ terms for which $(k, d) = e$ and then replacing e by d/e, gives $F(d) = \frac{1}{2}\sum_{e \mid d} e\phi(e)\phi(N/e)$. Of the above solu-

tions, $P = U(\infty)$ is one of the $f(d)$ points if and only if it has $\gamma \equiv 0 \pmod{N/d}$ but $\gamma \not\equiv 0 \pmod{N/e}$ for every $e \mid d$, $e < d$. But of the d values of γ mod N exactly $\phi(d)$ satisfy this condition, so $f(d) = \frac{1}{2}d\phi(d)\phi(N/d)$. It may now be observed that for $N \geqq 8$ there is a d for which $F(d) \geqq 5$ which by (II) implies all cusps are Weierstrass points. For $N = 7$, T has only 3 fixed points but the result follows from the gaps at ∞ computed below.

If $\hat{S}(N)$ is the orbit space of $S(N)$ under the cyclic group of order N generated by T, then $\hat{S}(N)$ has, by the Riemann-Hurwitz relation, genus $\hat{g}(N) = 1 + (2g(N) - 2 - B(N))/2N$ where $B(N)$ is the total branch order of $S(N)$ over $\hat{S}(N)$ which is $B(N) = \sum_{d \mid N} f(d)(N/d - 1)$ $= \frac{1}{2}\sum_{d \mid N} \phi(d)\phi(N/d)(N - d)$. The $f(d)$ points for T^d determine $f(d)/d$ points $\hat{P}$ on $\hat{S}$, and at each of the d points lying over a given $\hat{P}$, T^d rotates by the same amount determined by $\alpha^2 r \equiv 1 \pmod{N/d}$. As we have seen, the $f(d)$ points arise from $\phi(d)$ values of γ mod N and for each of these γ, α mod N/d has $\phi(N/d)$ values so that r mod N/d has $\phi(N/d)/2^{Q(N/d)}$ values, since this is the number of incongruent, relatively prime, quadratic residues mod N/d, where, for any integer n, $Q(n)$ is the number of odd prime divisors of n plus 0, 1, or 2 according as $4 \nmid n$, $4 \mid n$ but $8 \nmid n$, or $8 \mid n$. Thus at the $f(d)/d$ points $\hat{P}$ on $\hat{S}$ each quadratic residue r mod N/d occurs as the rotation by T^d over $\hat{P}$ exactly $2^{Q(N/d)-2}\phi(d)$ times.

Knowing the rotations we may apply the formula of Chevalley and Weil [1] to determine $M(k)$, the multiplicity of $e^{2\pi ik/N}$, $0 \leqq k \leqq N - 1$ in the diagonal form for (T) representing T on A_1. In our case, i.e., a cyclic group, this formula can be deduced from the Riemann-Roch theorem and reads: $M(0) = \hat{g}(N)$, while for $1 \leqq k \leqq N - 1$,

$$M(k) = \hat{g}(N) - 1 + \sum_{\substack{d \mid N \\ k \not\equiv 0 \pmod{d}}} \phi\left(\frac{N}{d}\right) 2^{Q(d)-1} \sum_{\substack{(r,d)=1 \\ r \equiv x^2 \pmod{d}}} \left(1 - \frac{[kr]_d}{d}\right)$$

where for any integer n, $[n]_d$ is defined by $n \equiv [n]_d \pmod{d}$ and $0 \leqq [n]_d \leqq d - 1$ and $r \equiv x^2 \pmod{d}$ means r is a quadratic residue.

In the case of $N = p$, a prime, this reduces to $M(0) = \hat{g}(p) = (p - 5)(p - 7)/24$, for $(k/p) = 1$,

$$M(k) = \hat{g}(p) - 1 + \frac{p - 1}{2} - \frac{1}{2p}\sum_{n=1}^{p}\left(1 + \left(\frac{n}{p}\right)\right)n$$

for $(k/p) = -1$,

$$M(k) = \hat{g}(p) - 1 + \frac{1}{2p}\sum_{n=1}^{p}\left(1 + \left(\frac{n}{p}\right)\right)n,$$

where (n/p) is the Legendre symbol. Finally, if $p \equiv 1 \pmod 4$, since $((p-n)/p) = (n/p)$ the above reduces to $M(k) = \hat{g}(p) - 1 + (p-1)/4$ for all k, $1 \leqq k \leqq N-1$.

By (I) above, $M(k)$ is the number of gaps at ∞ which are congruent to k mod N. Now we recall the following (proved in [3], essentially due to Hurwitz): In the notation of (I), if $F(h)$ is the number of fixed points of h then $F(h) \leqq 2\sigma_1$, where σ_1 is the least first nongap among all points which are not left fixed by h. We use this as $\sigma_1 \geqq F(d)/2$ which says that the first nongap at ∞ is $\geqq$ half the number of fixed points of T^d where T^d does not leave all parabolic points fixed. Using these facts, and remembering that the nongaps are closed under addition, the gaps have been determined for $N = 7, 8, 9, 10, 12$. For $N = 11$ complete results were not obtained. In general it seems that these methods will give all the gaps when N is not a prime for then $g(N)$ is smaller with respect to N (e.g. $N = 11$, $g = 26$; $N = 12$, $g = 25$); also there is then a $d \mid N$ with $d > 1$ so that the inequality $\sigma_1 \geqq F(d)/2$ gives a better estimate for σ_1 (e.g. $N = 11$, $\sigma_1 \geqq F(1)/2 = 5/2$; $N = 12$, $\sigma_1 \geqq F(6)/2 = 8$).

Let $[a, b]$ be the integers n such that $a \leqq n \leqq b$. Our results for $\gamma(\infty)$ the gap sequence at ∞ are:

$N = 7$, $g = 3$, $\gamma(\infty) = 1, 2, 4$

$N = 8$, $g = 5$, $\gamma(\infty) = 1, 2, 3, 5, 9$

$N = 9$, $g = 10$, $\gamma(\infty) = [1, 5], 7, 8, 10, 13, 16$

$N = 10$, $g = 13$, $\gamma(\infty) = [1, 9], 11, 13, 17, 19$

$N = 12$, $g = 25$, $\gamma(\infty) = [1, 11], [13, 17], 19, 21, 22, 25, 26, 29, 31, 37, 49.$

When $N = 11$, $g = 26$, I only know that $[1, 12]$ 14, 15, 16, 20, are gaps while 22, 33, 35, 39, 40, 41, $[43, 52]$ are not gaps. Thus ten gaps are still missing.

Finally we point out something which may be of interest. In the notation of (I), we have that $\det(h) = \epsilon^{G(P)}$ where $G(P) = \sum_{j=1}^{g} \gamma_j(P)$ is the sum of the gaps at P. Since $\det(ST) = \det(S) \det(T)$ and the determinant is invariant under a change of basis, we have that

$$(\rho^2)^{G(\rho)} = (-1)^{G(i)}(e^{2\pi i/N})^{G(\infty)}, \qquad \text{for } N \geqq 7.$$

In particular when $(N, 2) = (N, 3) = 1$ this implies $G(\rho) \equiv 0 \pmod 3$, $G(i) \equiv 0 \pmod 2$, $G(\infty) \equiv 0 \pmod N$.

BIBLIOGRAPHY

1. C. Chevalley and A. Weil, *Über das Verhalten der Integrale. 1. Gattung bei Automorphismen des Funktionenkörpers*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 358–361.

2. R. C. Gunning, *Lectures on modular forms*, Princeton Univ. Press, Princeton, N. J., 1962.

3. J. Lewittes, *Automorphisms of compact Riemann surfaces*, Thesis, Yeshiva University, New York, 1962.

4. B. Schoeneberg, *Über die Weierstrass Punkte in den Körpern der Elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg **17** (1951), 104–111.

YESHIVA UNIVERSITY

SOME RESULTS ON THE EXTENSION OF OPERATORS[1]

BY JORAM LINDENSTRAUSS

Communicated by Felix Browder, April 15, 1963

1. **Introduction.** The subject of the present note is closely related to questions treated in [6] and [7] (cf. also [8]). In §2 we state some results showing that certain extension properties for operators with a two-dimensional range imply extension properties for a much larger class of operators. Extension properties for operators with a two-dimensional range are, in a sense, the weakest possible, since by the Hahn Banach theorem operators with a one-dimensional range can always be extended in a norm preserving manner.

The results stated in §3 demonstrate the rôle of finite dimensional spaces whose unit cell is a polyhedron in some problems concerning norm preserving extension of operators. Proofs of the results stated here will be published elsewhere.

I wish to express my thanks to Professor S. Kakutani for many valuable discussions concerning the subject of this note.

NOTATIONS. All Banach spaces are assumed to be over the reals. S_X denotes the unit cell $\{x; \|x\| \leqq 1\}$ of the Banach space X. By "cell" we mean a translate of rS_X, $r>0$. All operators are assumed to be linear and bounded.

2. Our first theorem complements the main result of [7] (cf. also [8, Theorem 1]).

THEOREM 1. *Let X be a Banach space such that S_X has at least one extreme point. The following statements are equivalent.*

[1] Research supported by NSF Grant No. 25222.