A RESULT ON THE WEIL ZETA FUNCTION

BY
SAUL LUBKIN

1. **Results.** We recall Weil's conjectures [4] about the zeta function of a complete, nonsingular algebraic variety X over the field of q elements, q a prime power. We assume that X is projective and that X admits a projective lifting back to characteristic zero. Let N_v be the number of points of X rational over the field k_v, where k_v is the extension of k of degree v, $v \geqq 1$.

1 (Lefschetz theorem). *There exists a doubly indexed sequence*

$$(\alpha_{hi})_{1 \leqq i \leqq \beta_h;\ 0 \leqq h \leqq 2n}$$

of algebraic integers, where n is the dimension of X and $(\beta_h)_{0 \leqq h \leqq 2n}$ are the Betti numbers of any lifting of X to characteristic zero such that

$$N_v = \sum_{1 \leqq i \leqq \beta_h;\ 0 \leqq h \leqq 2n} (-1)^h \alpha_{hi}^v.$$

2 (Functional equation). $0 \leqq h \leqq 2n$ *implies that the sequences*

$$(q^n/\alpha_{h,1}, \ldots, q^n/\alpha_{h,\beta_h}) \quad \textit{and} \quad (\alpha_{2n-h,1}, \ldots, \alpha_{2n-h,\beta_{2n-h}})$$

are permutations of each other.

3 (Riemann hypothesis). $|\alpha_{hi}| = q^{h/2}$, $1 \leqq i \leqq \beta_h$, $0 \leqq h \leqq 2n$.

In addition it was later conjectured that

4. *If $P_h = \prod_{i=1}^{\beta_h} (1 - \alpha_{hi} T)$, $0 \leqq h \leqq 2n$, then the coefficients of the polynomials P_h are rational integers.*

Conjectures 1 and 2 are now known. (See [1] and [2] for two different proofs.) Conjectures 3 and 4 are still unknown. (Under the assumption of conjecture 3 for the usual absolute value on the algebraic numbers, conjecture 4 is equivalent to the assertion that, for every absolute value on the algebraic numbers extending the usual absolute value on the rational numbers, conjecture 3 holds.) In this paper I prove a previously unknown result that would follow if both 3 and 4 were known, but that is not a consequence of either 3 or 4 alone. The result is:

5. *If $0 \leqq h \leqq 2n$ then the sequences $(q^h/\alpha_{h,1}, \ldots, q^h/\alpha_{h,\beta_h})$ and $(\alpha_{h,1}, \ldots, \alpha_{h,\beta_h})$ coincide up to permutation.*

Another way of stating 5 is: If the algebraic integer α occurs m times in the sequence $(\alpha_{h,1}, \ldots, \alpha_{h,\beta_h})$ then the algebraic integer q^h/α likewise occurs m times.

(To see that 3 and 4 would imply 5 note that 3 is equivalent to the assertion $\bar{\alpha}_{hi} = q^h/\alpha_{hi}$. 4 asserts that the coefficients of P_h are rational and in particular real.

Presented to the Society, January 24, 1967; received by the editors November 7, 1966 and, in revised form, October 24, 1967.

Hence complex conjugation: $\alpha_{hi} \to \bar{\alpha}_{hi}$ defines a permutation of the sequence $(\alpha_{hi})_{1 \leqq i \leqq \beta_h}$. But by 3 $\bar{\alpha}_{hi} = q^h/\alpha_{hi}$. This proves 5.)

Note that for $h=n$ 5 is a special case of the functional equation 2. 2 and 5 imply

5′. *If* $0 \leqq h \leqq 2n$ *then the sequences*

$$(q^{n-h}\alpha_{h,1}, \ldots, q^{n-h}\alpha_{h,\beta_h}) \quad \textit{and} \quad (\alpha_{2n-h,1}, \ldots, \alpha_{2n-h,\beta_{2n-h}})$$

are permutations of each other.

2, 5 and 5′ are such that any two imply the third. Since 2 is known ([1], [2]) and we prove 5 in this paper all three statements hold.

2, 5 and 5′ can be written in terms of the Weil polynomials P_h:

2. $P_{2n-h}(T) = \pm q^{\beta_h(n-(h/2))} T^{\beta_h} P_h(1/q^n T)$,

5. $P_h(T) = \pm q^{h\beta_h/2} T^{\beta_h} P_h(1/q^h T)$, and

5′. $P_{2n-h}(T) = P_h(q^{n-h}T)$, $\quad 0 \leqq h \leqq 2n$.

Another way of stating 5 is:

5. *The polynomial* $P_h(q^{-h/2}T)$ *is either symmetric or antisymmetric*, $0 \leqq h \leqq 2n$.

5′ written in terms of the Weil polynomials is particularly simple. Since 2 is well known ([1], [2]) the new result 5 proved in this paper is equivalent to 5′.

I also note (and leave it as an exercise to the reader) that if the "Riemann hypothesis" were known then the new result 5 would be equivalent to the assertion that the coefficients of the Weil polynomials P_h are real, $0 \leqq h \leqq 2n$, thus implying a portion of 4. Also the new result 5 does give some information about the Riemann hypothesis 3. Namely it implies that those α_{hi} such that $|\alpha_{hi}| \neq q^{h/2}$ occur in pairs α_{hi}, $\alpha_{hi'}$ where $\alpha_{hi} \cdot \alpha_{hi'} = q^{h/2}$.

5 is also equivalent to the assertion that each of the Weil polynomials P_h factors, uniquely up to order, into a product of linear factors: $(1 - q^{h/2}T)$, $(1 + q^{h/2}T)$ and quadratic factors: $1 + u_j T + q^h T^2$ where the u_j are algebraic integers $\neq \pm 2q^{h/2}$. The Riemann hypothesis is equivalent to the assertion that the u_j are all real.

Our proof of 5 is elementary. Cohomology is used; either of our well-known cohomology theories ([1], [2]) suffices. The main new idea is to apply a very simple and, probably, previously unobserved result about the characteristic polynomial of a linear transformation of a finite dimensional vector space that preserves some nondegenerate inner product (2.1).

2. **Nondegenerate inner products on a finite dimensional vector space.** Let V be a finite dimensional vector space over a field k. An *inner product* on V is a linear transformation from $V \otimes_k V$ into k, the image of the element $v \otimes w$ being written as $v \cdot w$, $v, w \in V$. A linear transformation $f\colon V \to W$ of finite dimensional vector spaces with inner products over k *preserves inner products* if $v, w \in V$ implies $f(v) \cdot f(w) = v \cdot w$.

An inner product on the finite dimensional vector space V is *nondegenerate* if $0 \neq v \in V$ implies there exists $w \in V$ such that $v \cdot w \neq 0$. (Notice that we do *not* require that $v \neq 0$ implies $v \cdot v \neq 0$—such an inner product is *definite*—, that $v, w \in V$

implies $v \cdot w = w \cdot v$—such an inner product is *symmetric*—or that $v, w \in V$ implies $v \cdot w = -w \cdot v$—such an inner product is *antisymmetric*.)

Let $P(X) = a_n X^n + \cdots + a_1 X + a_0$, $a_n \neq 0$, be a polynomial of degree n over a field. Then the *reverse* of P is the polynomial $a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n$. The polynomial is *symmetric* (respectively: *antisymmetric*) if it coincides with its reverse (respectively: with the negative of its reverse).

THEOREM 1. *Let V be a finite dimensional vector space over a field together with a nondegenerate inner product. Let $f\colon V \to V$ be a linear transformation that preserves the inner product. Then the characteristic polynomial of f is either symmetric or antisymmetric.*

Proof. Let $f^t\colon V \to V$ be the transpose of f with respect to the given inner product. Then f^t is the unique linear transformation such that

(1) $f^t(v) \cdot w = v \cdot f(w)$, $v, w \in V$.

If (e_i) is a basis of V and if (e_i') is the dual basis of (e_i) with respect to the given inner product then the matrix of f^t with respect to (e_i') is the transpose of the matrix of f with respect to (e_i). Hence f and f^t have the same characteristic polynomial.

Since f preserves the inner product we have $f^t(f(v)) \cdot w = f(v) \cdot f(w) = v \cdot w$, $v, w \in V$. Hence $f^t(f(v)) = v$, $v \in V$,

(2) $f^t \circ f = \text{identity}$.

Hence f is an automorphism of V. Since f^t and f have the same characteristic polynomial they have the same determinant. Taking the determinant of (2) gives

(3) $\det f = \pm 1$.

Considering the definition of the characteristic polynomial as $\det(\text{identity} \cdot X - f)$ and using the fact that $\det(f) = \pm 1$ we see that the characteristic polynomial of f^{-1} is $\pm$ the reverse of the characteristic polynomial of f. By (2) $f^{-1} = f^t$ which has the same characteristic polynomial as f. Hence the characteristic polynomial of f is either symmetric or antisymmetric.

COROLLARY 1.1. *Let V be a finite dimensional vector space over a field and let $f\colon V \to V$ be a linear transformation that preserves some nondegenerate inner product. Let $(\alpha_1, \ldots, \alpha_n)$ be the sequence of eigenvalues with multiplicities of f. Then the sequences $(\alpha_1, \ldots, \alpha_n)$ and $(\alpha_1^{-1}, \ldots, \alpha_n^{-1})$ coincide up to permutation.*

Proof. A polynomial is either symmetric or antisymmetric if and only if the mapping: $\alpha \to \alpha^{-1}$ is a bijection of the roots preserving multiplicities. Hence the corollary is equivalent to the theorem.

3. **Proof of 1.5.** The notations being as in §1 let $\mathcal{O}$ be a complete discrete valuation ring with quotient field of characteristic zero such that X admits a projective lifting $\mathfrak{X}$ over $\mathcal{O}$. Fix a complex imbedding: $\mathcal{O} \subset \mathbf{C}$ and let $X_{\mathbf{C}}$ be the projective nonsingular complex algebraic variety

$$X_{\mathbf{C}} = \mathfrak{X} \times_{\operatorname{Spec}(\mathcal{O})} \operatorname{Spec}(\mathbf{C}).$$

Let K be either the ring of q'-adic integers, q' a rational prime unequal to the characteristic of k, or the quotient field of $\mathcal{O}$. Let $H^*(X, K)$ be either the q'-adic [1] or the K-adic [2] cohomology of X respectively. If $K=\hat{\boldsymbol{Z}}_{q'}$ then let $K\subset \boldsymbol{C}$ be a complex imbedding of the ring K. In either case let $H^*(X, \boldsymbol{C})=H^*(X, K) \otimes_K \boldsymbol{C}$. Then the ring $H^*(X, \boldsymbol{C})$ is canonically isomorphic to the classical complex cohomology algebra $H^*(X_{\boldsymbol{C}}, \boldsymbol{C})$ of the complex algebraic variety $X_{\boldsymbol{C}}$. Identify these two rings.

Let $u \in H^2(X_{\boldsymbol{C}}, \boldsymbol{C})$ denote the "Kähler class" ([5], see also [3])—the class of a generic hyperplane section of $X_{\boldsymbol{C}}$. Then $u \in H^2(X, \boldsymbol{C})=H^2(X, K) \otimes_K \boldsymbol{C}$ is the canonical class of a generic hyperplane section H of X ([1], [2]). Hence if $f^* = (f^h)_{0 \leqq h \leqq 2n}$ denotes the maps induced by the Frobenius ([1], [2]) on the cohomology groups $H^*(X, \boldsymbol{C})=(H^h(X, \boldsymbol{C}))_{0 \leqq h \leqq 2n}$ then

(1) $f^2(u)=q\cdot u$.

$f^*\colon H^*(X, \boldsymbol{C}) \to H^*(X, \boldsymbol{C})$ preserves cup products. Hence if we define

(2) $g^h=q^{-h/2}\cdot f^h, \quad 0\leqq h\leqq 2n,$

then $g^*\colon H^*(X, \boldsymbol{C}) \to H^*(X, \boldsymbol{C})$ preserves cup products and $g^2(u)=u$.

By the functional equation 1.2, to prove 1.5 it suffices to consider the case $0\leqq h\leqq n$.

If $0\leqq h\leqq n$ and $v, w \in H^h(X_{\boldsymbol{C}}, \boldsymbol{C})$ then define $v\cdot w=u^{n-h} \cup v \cup w$. Then [5] the assignment $(v, w) \to v\cdot w$ is a nondegenerate inner product on the finite dimensional vector space $H^h(X_{\boldsymbol{C}}, \boldsymbol{C})$. Since g^* preserves cup products and $g^2(u)=u$ it follows that g^h preserves this nondegenerate inner product. Hence by 2.1.1 if $(a_{h,i})_{1\leqq i\leqq b_h}$ are the eigenvalues of g^h with the appropriate multiplicities then

(3) The sequences $(a_{h,i}^{-1})_{1\leqq i\leqq b_h}$ and $(a_{h,i})_{1\leqq i\leqq b_h}$ are permutations of each other.

The sequence $(\alpha_{h,i})_{1\leqq i\leqq \beta_h}$ of §1 is the sequence of eigenvalues with multiplicities of the linear transformation $f^h\colon H^h(X, \boldsymbol{C}) \to H^h(X, \boldsymbol{C})$, modified in a manner similar to the Remark, p. 253 of [2] to make all the $\alpha_{h,i}$ algebraic integers. Hence by (2)

(4) The sequences $(\alpha_{h,i})_{1\leqq i\leqq \beta_h}$ and $(q^{h/2}a_{h,i})_{1\leqq i\leqq b_h}$ coincide up to permutation.

(3) and (4) imply 1.5.

Bibliography

1. S. Lubkin, *On a conjecture of André Weil*, Amer. J. Math. **89** (1967), 443–548.

2. ———, *A p-adic proof of Weil's conjectures*, Ann. of Math. (2) **87** (1968), 105–255.

3. J.-P. Serre, *Analogues kählériens de certaines conjectures de Weil*, Ann. of Math. (2) **71** (1960), 392–394.

4. A. Weil, *Number of solutions of equations over finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

5. ———, *Introduction à l'étude des variétés kählériennes*, Actualités Sci. Indust., No. 1267, Hermann, Paris, 1958; Russian transl., IL, Moscow, 1961.

University of California,
Berkeley, California