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 $v$, $v \geq 1$.

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

\[(a_{hi})_{1 \leq i \leq \beta_h, 0 \leq h \leq 2n}\]

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

\[N_v = \sum_{1 \leq i \leq \beta_h, 0 \leq h \leq 2n} (-1)^h a_{hi}^v.\]

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

\[(q^n / a_{hi,1}, \ldots, q^n / a_{hi,\beta_h})\] and \[(a_{hi+1,1}, \ldots, a_{hi+1,\beta_h})\]

are permutations of each other.

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

In addition it was later conjectured that

4. If $P_h = \prod_{i=1}^{\beta_h} (1 - a_{hi} T), 0 \leq h \leq 2n$, 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 $0 \leq h \leq 2n$ then the sequences $(q^h / a_{hi,1}, \ldots, q^h / a_{hi,\beta_h})$ and $(a_{hi,1}, \ldots, a_{hi,\beta_h})$ coincide up to permutation.

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

To see that 3 and 4 would imply 5 note that 3 is equivalent to the assertion $\bar{a}_{hi} = q^h / a_{hi}$. 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.

297
Hence complex conjugation: $\alpha_{hi} \rightarrow \bar{\alpha}_{hi}$ defines a permutation of the sequence $(\alpha_{ih})_{1 \leq i \leq d}$. 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 $0 \leq h \leq 2n$ then the sequences

$$(q^{-h}\alpha_{h,1}, \ldots, q^{-h}\alpha_{h,d}) \text{ and } (\alpha_{2n-h,1}, \ldots, \alpha_{2n-h,d_{2n-h}})$$

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

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

5'. $P_{2n-h}(T) = P_h(q^{-h}T)$, \hspace{1cm} $0 \leq h \leq 2n$.

Another way of stating 5 is:

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

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, $0 \leq h \leq 2n$, 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 $\alpha_{hi}$ such that $|\alpha_{hi}| \neq q^{h/2}$ occur in pairs $\alpha_{hi}, \bar{\alpha}_{hi}$, where $\alpha_{hi}, \bar{\alpha}_{hi} = q^{h/2}$.

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: $1 + u_jT + q^hT^2$ 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 $f: V \rightarrow W$ 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 \(P(X) = a_nX^n + \cdots + a_1X + a_0, a_n \neq 0\), be a polynomial of degree \(n\) over a field. Then the reverse of \(P\) is the polynomial \(a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n\). 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 \(f: V \rightarrow V\) be a linear transformation that preserves the inner product. Then the characteristic polynomial of \(f\) is either symmetric or antisymmetric.

**Proof.** Let \(f^t: V \rightarrow V\) 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 \((e^j)\) is the dual basis of \((e_i)\) with respect to the given inner product then the matrix of \(f^t\) with respect to \((e^j)\) 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 \(\det(\text{identity} - X \cdot f)\) 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 \(f: V \rightarrow V\) 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: \(\alpha \rightarrow \alpha^{-1}\) 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 \(\overline{X}\) over \(\mathcal{O}\). Fix a complex imbedding: \(\mathcal{O} \subset \mathbb{C}\) and let \(X_C\) be the projective nonsingular complex algebraic variety

\[X_C = \overline{X} \times_{\text{Spec}(\mathcal{O})} \text{Spec}(\mathbb{C}).\]
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 \( G \). Let \( H^*(X, K) \) be either the \( q' \)-adic [1] or the \( K \)-adic [2] cohomology of \( X \) respectively. If \( K=\mathbb{Z}_{q'} \) then let \( K\subset C \) be a complex imbedding of the ring \( K \). In either case let \( H^*(X, C)=H^*(X, K) \otimes_{K} C \). Then the ring \( H^*(X, C) \) is canonically isomorphic to the classical complex cohomology algebra \( H^*(XC, C) \) of the complex algebraic variety \( XC \). Identify these two rings.

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

\[
(f^2)^*(u)=q \cdot u.
\]

\( f^*: H^*(X, C) \to H^*(X, C) \) preserves cup products. Hence if we define

\[
g^h=q^{-h/2}f^h, \quad 0 \leq h \leq 2n,
\]

then \( g^*: H^*(X, C) \to H^*(X, C) \) preserves cup products and \( g^2(u)=u \).

By the functional equation 1.2, to prove 1.5 it suffices to consider the case \( 0 \leq h \leq n \).

If \( 0 \leq h \leq n \) and \( v, w \in H^h(XC, C) \) 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 \( H^h(XC, C) \). 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 \( (a_{h,i})_{1 \leq i \leq 2n_h} \) are the eigenvalues of \( g^h \) with the appropriate multiplicities then

(3) The sequences \( (a_{h,i})_{1 \leq i \leq 2n_h} \) and \( (a_{h,i})_{1 \leq i \leq 2n_h} \) are permutations of each other.

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

(4) The sequences \( (a_{h,i})_{1 \leq i \leq 2n_h} \) and \( (g^{h/2}a_{h,i})_{1 \leq i \leq 2n_h} \) coincide up to permutation.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use