Canad. Math. Bull. Vol. 33 (3), 1990

A NOTE ON RELATIONS BETWEEN THE ZETA-FUNCTIONS OF GALOIS COVERINGS OF CURVES OVER FINITE FIELDS

BY
AMILCAR PACHECO

ABSTRACT. Let C be a complete irreducible nonsingular algebraic curve defined over a finite field k. Let G be a finite subgroup of the group of automorphisms $\mathrm{Aut}(C)$ of C. We prove that certain idempotent relations in the rational group ring $\mathbb{Q}[G]$ imply other relations between the zeta-functions of the quotient curves C/H, where H is a subgroup of G. In particular we generalize some results of Kani in the special case of curves over finite fields.

Introduction. Let C be a complete irreducible nonsingular algebraic curve defined over a finite field $k = \mathbb{F}_q$. Let G be a finite subgroup of the group of automorphisms $\mathrm{Aut}(C)$ of C. For any subgroup H of G let C/H be the quotient curve. Let g_H, respectively σ_H, be the genus, respectively the Hasse-Witt invariant of C/H.

If C is defined over an arbitrary field K then Kani proves that certain idempotent relations in the rational group ring $\mathbb{Q}[G]$ imply relations between the genera, respectively the Hasse-Witt invariants, of the curves C/H (see [4, Theorems 1, 2]). In the case where C is defined over a finite field $\mathbb{F}_q$, we show that these idempotent relations imply relations between the zeta-functions $\zeta_{C/H|\mathbb{F}_q}$, which yield the desired relations.

The Result. Let H be a subgroup of G and

$$\epsilon_H \stackrel{\text{def}}{=} \frac{1}{|H|} \cdot \sum_{h \in H} h \in \mathbb{Q}[G]$$

the "norm idempotent" associated to H.

Let $\zeta_{C/H|\mathbb{F}_q}$ be the zeta-function of C/H. Recall that

$$\zeta_{C/H|\mathbb{F}_q}(t) = \exp\left(\sum_{\nu>0} \#C/H(k_\nu) \cdot \frac{t^\nu}{\nu}\right), \tag{1}$$

where $\#C/H(k_\nu)$ is the number of k_ν – rational points of C/H and $k_\nu = \mathbb{F}_{q^\nu}$.

Received by the editors February 15, 1989 and, in revised form, June 5, 1989.
AMS (1980) Mathematics Subject Classification Number: 14G10.

THEOREM. *Any relation* $\sum_H r_H \cdot \epsilon_H = 0$, *with* $r_H \in \mathbb{Z}$, *between the norm idempotents yields a relation*

$$\prod_H \zeta_{C/H|\mathbb{F}_q}(t)^{r_H} = 1.$$

To prove this theorem we need the following well-known result (cf. [2]).

TWISTING LEMMA. *Let* $\pi : Y \longrightarrow X$ *be a finite Galois covering of complete irreducible nonsingular algebraic curves defined over a finite field* $k = \mathbb{F}_q$ *with Galois group* G *of order* m. *Then for each* $\sigma \in G$ *there exists a curve* $Y^{(\sigma)}$ *defined over* k *with* $Y^{(id)} = Y$ *and* $Y^{(\sigma)}$ *isomorphic to* Y *over* $\bar{k}$ *such that*

$$\frac{1}{m} \cdot \sum_{\sigma \in G} \#Y^{(\sigma)}(k) = \#X(k),$$

where $\#Y^{(\sigma)}(k)$, *respectively* $\#X(k)$ *denotes the number of* k – *rational points of* $Y^{(\sigma)}$, *respectively* X.

REMARK. The twisted curves are defined as follows. Let $k_m \stackrel{\text{def}}{=} \mathbb{F}_{q^m}$ and f be the generator of $\text{Gal}(k_m/k)$. Let $k_m(Y)$ be the constant field extension of $k(Y)$ by k_m. The Galois group $\text{Gal}(k_m(Y)/k(X))$ is isomorphic to $\text{Gal}(k(Y)/k(X) \times \text{Gal}(k_m/k)$. For each $\sigma \in \text{Gal}(k(Y)/k(X))$ let

$$k(Y^{(\sigma)}) \stackrel{\text{def}}{=} k_m(Y)^{(\sigma, f)}$$

be the subfield of $k_m(Y)$ fixed by (σ, f). This is the function field of $Y^{(\sigma)}$ over k (*cf.* [7, Chapter **X** , Theorem 2.2]). The relation between the k-rational points of X and those of the curves $Y^{(\sigma)}$'s is not difficult to obtain (*cf.* [3, Lemma 3.18]).

PROOF OF THEOREM. By the Twisting lemma for each $\nu > 0$ we have

$$\#C/H(k_\nu) = \frac{1}{|H|} \cdot \sum_{h \in H} \#C^{(h)}(k_\nu). \tag{2}$$

Let J_C be the Jacobian variety of C. Each $\sigma \in \text{Aut}(C)$ induces an automorphism in the divisor group $\text{Div}(C)$ of C:

$$\sigma^* \left(\sum_P n_P \cdot P \right) = \sum_P n_P \cdot \sigma P.$$

Moreover for each function x of C we have $\sigma^*((x)) = (\sigma x)$. Thus σ induces an automorphism α_σ in J_C. Similarly, if F is the Frobenius morphism of C over k then F induces an endomorphism α_F in J_C.

By [8, p. 81]

$$\#C^{(h)}(k_\nu) = 1 + q^\nu - \text{Tr}\left(\alpha_{h^{-1}} \circ \alpha_{F^\nu} | J_C\right). \tag{3}$$

Let ℓ be a prime number with $\ell \neq p$. Let $T_\ell(J_C)$ be the ℓ-adic Tate module of J_C. By [8, p. 218, Theorem 36] or [5, p. 186, Theorem 3] there exists an anti-representation

$$\begin{aligned} \mathrm{End}(J_C) &\longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(J_C)) \\ \alpha &\longmapsto \alpha^*, \end{aligned}$$

where $\mathbb{Z}_\ell$ denotes the ℓ-adic integers, such that the characteristic polynomials of α and α^* are equal (see [8, p. 213]). In particular

$$\mathrm{Tr}(\alpha \mid J_C) = \mathrm{Tr}(\alpha^* \mid T_\ell(J_C)). \tag{4}$$

By (1), (2), (3) and (4) we have

$$\log \zeta_{C/H|\mathbb{F}_q}(t) = \sum_{\nu>0} \left(1 + q^\nu - \frac{1}{|H|} \cdot \sum_{h\in H} \mathrm{Tr}(\alpha_h^* \circ \alpha_{F^\nu}^* | T_\ell(J_C)) \right) \cdot \frac{t^\nu}{\nu}. \tag{5}$$

Note that

$$\sum_H r_H = 1_G \left(\sum_H r_H \cdot \epsilon_H \right) = 0,$$

where 1_G is the trivial character of G. Whence by (5)

$$\sum_H r_H \cdot \log \zeta_{C/H|\mathbb{F}_q}(t) = -\sum_{\nu>0} \left(\sum_H \frac{r_H}{|H|} \sum_{h\in H} \mathrm{Tr}(a_h^* \circ \alpha_{F^\nu}^* | T_\ell(J_C)) \right) \cdot \frac{t^\nu}{\nu}. \tag{6}$$

Extend $\rho : G \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(J_C))$ given by $\sigma \longmapsto \alpha_\sigma^*$ to a map of the same name $\rho : \mathbb{Q}_\ell[G] \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(J_C)) \otimes \mathbb{Q}_\ell$, where $\mathbb{Q}_\ell$ denotes the ℓ – adic numbers. Then $\rho(\epsilon_H) = \frac{1}{|H|} \sum_{h\in H} \alpha_h^*$. Consider

$$\mu_\nu \stackrel{\mathrm{def}}{=} \rho \left(\sum_H r_H \cdot \epsilon_H \right) \circ \alpha_{F^\nu}^* = \sum_H \frac{r_H}{|H|} \cdot \sum_{h\in H} \alpha_h^* \circ \alpha_{F^\nu}^*.$$

Since $\sum_H r_H \cdot \epsilon_H = 0$ we have $\mu_\nu = 0$, $\nu > 0$. Hence

$$\sum_H r_H \cdot \log \zeta_{C/H|\mathbb{F}_q}(t) = 0,$$

i.e.,

$$\prod_H \zeta_{C/H|\mathbb{F}_q}(t)^{r_H} = 1 \qquad \square$$

Corollary. *Any relation* $\sum_H r_H \cdot \epsilon_H = 0$, *with* $r_H \in \mathbb{Z}$, *between the norm idempotents yields relations* $\sum_H r_H \cdot g_H = 0$ *and* $\sum_H r_H \cdot \sigma_H = 0$.

PROOF. By [8, p. 71, 83]

$$\zeta_{C/H|\mathbb{F}_q}(t) = \frac{P_{C/H}(t)}{(1-t)\cdot(1-qt)},$$

where $P_{C/H}(t) \in \mathbb{Z}[t]$ of degree $2g_H$. Thus

$$\prod_H \zeta_{C/H|\mathbb{F}_q}(t)^{r_H} = \frac{\prod_H P_{C/H}(t)^{r_H}}{\prod_H (1-t)\cdot(1-qt))^{r_H}}. \tag{7}$$

We take degrees of both sides of (7) and conclude from the theorem that $\sum_H r_H \cdot g_H = 0$.

Since $\deg(P_{C/H}(t) \bmod p)$ is the Hasse-Witt invariant σ_H [6, Theorem 1], we conclude as above, by taking degrees of both sides of (7) reduced modulo p, that $\sum_H r_H \cdot \sigma_H = 0$. □

REFERENCES

1. R. D. Accola, *Two theorems on Riemann surfaces with noncyclic automorphisms groups*, Proc. **AMS 25** (1970), 598–602.
2. E. Bombieri, *Hilbert's 8th problem: an analogue, in Mathematical Developments arising from Hilbert's problems*, Proc. Symp. Pure Math. American Mathematical Society, **28**, 269–274.
3. M. D. Fried, M. Jarden, *Field Arithmetic*, Berlin, Heidelberg, Springer-Verlag, 1986.
4. E. Kani, *Relations between the genera and the Hasse-Witt invariants of Galois coverings of curves*, Can. Math. Bull. **28** (3), 321–327 (1985).
5. S. Lang, *Abelian Varieties*, New York, Springer-Verlag, 1983.
6. J. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, Trans. Amer. Math. Soc. **45**, 245–264 (1965).
7. J. Silverman, *The Arithmetic of Elliptic Curves*, New York, Springer-Verlag, 1986.
8. A. Weil, *Courbes Algébriques et Variétés Abélienes*, Hermann, Paris, 1971.

Instituto de Matemática Pura e Aplicada
Estrada Dona Castorina 110
22460 Rio de Janeiro, RJ
Brasil.