BOL. SOC. BRAS. MAT. VOL. 9, N.º 1 (1978), 89 – 95

Adele rings of global field of positive characteristc

Stuart Turner

1. The zeta function, the adele ring, and the Jacobian variety.

Let k be a global field of characteristic $p>0$ with field of constants $\mathbb{F}_q$. Let Ω denote the set of places of k. For $v\in\Omega$ let k_v be the completion of k at v and q_v be the cardinality of the residue field of k_v. For $s\in C$, Re $(s)>1$ the zeta function ζ_k of k is given by the absolutely convergent product $\zeta_k(s)=\prod_{v\in\Omega}(1-q_v^{-s})^{-1}$.

There exists a complete non-singular curve C defined over $\mathbb{F}_q$ such that $K(C)$, the field of rational functions on C, is isomorphic to k. C is unique up to $\mathbb{F}_q$-isomorphism. Let $N(C)_n$ denote card $C(\mathbb{F}_{q^n})$, the number of $\mathbb{F}_{q^n}$-rational points on C. Let ζ_C be the zeta function of C and set $T=q^{-s}$, then $\zeta_k(s)=\zeta_C(T)$ and $\dfrac{d(ln\zeta_C(T))}{dT}=\sum_{n\geq 1}N(C)_n T^{n-1}$. This power series has radius of convergence q^{-1}.

Finally, ζ_C can be written

$$\zeta_C(T)=\frac{P_k(T)}{(1-T)(1-qT)} \tag{1}$$

with $P_k(T)\in\mathbb{Z}[T]$, deg $P_k(T)=2g$ where g is the genus of C. P_k satisfies the functional equation $P_k(T)=q^g\,T^{2g}\,P_k\left(\dfrac{1}{qT}\right)$ and $P_k(0)=1$.

Let k_A denote the adele ring of k.

Theorem 1. *Let k', k'' be global fields of positive characteristic such that $P_{k'}=P_{k''}$. Then k'_A and k''_A are isomorphic topological rings.*

Proof. Let $P(T)$ be a polynomial which occurs as the numerator of the zeta function of some global field k of positive characteristic. It suffices to show that one can use P to construct a topological ring isomorphic to k_A. First, (deg P)/2 is the genus g of k. Write $P(T)=a_{2g}T^{2g}+\ldots+1$. From the functional equation for P one sees that the cardinality of the constant field of k is the positive integer q such that $q^g=a_{2g}$. Hence P determines g and q.

Recebido em novembro de 1977.

Let C be any complete non-singular curve defined over $\mathbb{F}_q$ such that $\zeta_C(T) = \dfrac{P(T)}{(1-T)(1-qT)}$. (The examples in §3 show that for some choices of P, there can exist non-isomorphic C with this property.) Since $\dfrac{d(\ln \zeta_C(T))}{dT} = \sum_{n \geq 1} N(C)_n T^{n-1}$ and since this power series defines an analytic function in the disc $|T| < q^{-1}$, the $N(C)_n$ are determined by P. For n a positive integer define $M(C)_n = \text{card } \{x \in C(\mathbb{F}_{q^n}) \mid x \notin C(\mathbb{F}_{q^{n'}}),\ n'\ n,\ n' \neq n\}$. The subfields of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$ are of the form $\mathbb{F}_{q^{n'}}$ with $n'\ n$, so it is easy to see that the set $\{N(C)_{n'}\}_{n' \leq n}$ determines $M(C)_n$. As we have seen, the $N(C)_{n'}$ can be determined from P.

For each positive integer n let r_n be a complete eguicharacteristic discrete valuation ring with residue field $\mathbb{F}_{q^n}$. By the Cohen structure theorem ([17], Chapter VIII, §12) r_n is isomorphic to $\mathbb{F}_{qn}[[X]]$. Let k_n be the quotient field of r_n. Let $r_{n,1}, r_{n,2}, \ldots, r_{n,M_n}$ be complete discrete valuation rings isomorphic to r_n and $k_{n,1}, \ldots, k_{n,M_n}$ be their quotient fields. Consider the sets

$$\{k_{n,i}\}_{n \varepsilon N} \qquad \text{and} \qquad \{r_{n,i}\}_{n \varepsilon N}\,.$$
$$1 \leq i \leq M_n \qquad 1 \leq i \leq M_n$$

Form the restricted direct product D of the $k_{n,i}$ with respect to the $r_{n,i}$. D is clearly isomorphic to k_A.

Corollary. *Let k', k'' be global fields with field of constants $\mathbb{F}_q$ such that $\zeta_{k'} = \zeta_{k''}$. Then k'_A and k''_A are isomorphic topological rings.*

Proof. The corollary follows immediately from the theorem and from (1).

Remark. It can be shown that there exist algebraic number fields k' and k'' with the same ς-function, but with non-isomorphic adele rings ([3], Theorem 1).

Theorem 2. *Let k, k' be global fields of positive characteristic such that k_A and k'_A are isomorphic topological rings. Then $\zeta_k = \zeta_{k'}$ and $P_k = P_{k'}$.*

Proof. To prove the first assertion it suffices to show that one can determine ζ_k from k_A. Let M be a closed maximal ideal of k_A, then there exists a $v_M \in \Omega$ such that k_A/M and k_{v_M} are isomorphic topological fields. Conversely, given $v \varepsilon \Omega$, there exists a closed maximal ideal $M_v \subseteq k_A$ such that k/M_v is isomorphic to k_v. This correspondence between the closed maximal ideals of k_A and Ω is one-to-one ([2], proof of lemma 7). Let r_v be the maximal

compact subring of k_v, m_v be the maximal ideal of r_v, and $q_v = \text{card } (r_v/m_v)$. Since $\zeta_k(s) = \prod_{v \in \Omega} (1 - q_v^{-s})^{-1}$, k_A determines ζ_k.

Let q be the cardinality of the field of constants of k. Since $P_k(q^{-s}) = (1-q^{-s})(1-q^{1-s})\zeta_k(s)$, to prove the second assertion of the theorem it suffices to show that one can determine q from k_A. The topology of $k_A{}^x$, the adele group of k, can be defined directly from the topology of k_A, without referring to k or its completions ([13], Chapter IV, §3, definition 2). Let $\| : k_A{}^x \to \mathbb{R}_+{}^x$ be the continuous homomorphism defined by the Haar module. Then q generates the image of $\|$ in $\mathbb{R}_+{}^x$. ([13], Chapter IV, §3, proposition 3; Chapter VII, §5, corollary 6.).

Remark. The same proof shows that two algebraic number fields with isomorphic adele rings have the same zeta funtion.

Let k, k' be global fields with field of constants $\mathbb{F}_q$ and C, C' be complete, non-singular curves defined over $\mathbb{F}_q$ with their function fields isomorphic to k and k' respectively. Let $A = J(C)$ and $B = J(C')$ be their Jacobian varieties. A and B are defined over $\mathbb{F}_q$. Let $\pi_A \in \text{End } A$ (resp. $\pi_B \in \text{End } B$) be the Frobenius endomorphism of A (resp. B) and f_A (resp. f_B) be the characteristic polynomial of π_A. Then $P_k(T) = q^g f_A(T)$. Furthermore, A is F_q-isogenous to B if and only if $f_A = f_B$ ([10), theorem 1). Combining this result with the corollary to theorem 1 and theorem 2 gives.

Proposition. *Let k, k' be global fields with field of constants $\mathbb{F}_q$. Then the following are equivalent:*

i) $\zeta_k = \zeta_{k'}$.
ii) *$J(C)$ and $J(C')$ are $\mathbb{F}_q$-isogenous.*
iii) *k_A and k'_A are isomorphic topological rings.*

In [11] it is shown that there exist infinitely many non-isomorphic singular curves of genus two defined and irreducible over $\mathbb{F}_p n$, n odd, which have the same zeta function.

2. The adelic theta function

It is not possible in general to reconstruct C from $J(C)$. However, if $\mathscr{C}(\theta)$ denotes the polarization of $J(C)$ defined by a canonical divisor θ (or equivalently by a translation θ_a of θ) on $J(C)$, C can be reconstructed from the principally polarized abelian variety $(J(C), \mathscr{C}(\theta))$ ([7], [16]). In the classical case where C is replaced by a compact Riemann surface M and

$J(C)$ by an algebrizable complex torus $J(M)$ it is possible to choose the canonical divisor θ on $J(M)$ so that θ is "cut out" by the zeros of Riemann's theta function ([5], [6], [8]). We now show that it is possible to recover k from k_A in an analogous way.

Recall that k can be canonically identified with a discrete subfield of k_A which we also denote by k. Let $\hat{k}_A$ be the Pontryagin dual of k_A. Let T be the group of complex numbers of modulus one and $< . , . > : k_A x \hat{k}_A \to T$ denote the canonical pairing. Let R be the maximal compact subring of k_A and ϕ be the characteristic function of R. Define

$$\theta_k : k_A x \hat{k}_A \to \mathbb{C}$$

by

$$\theta_k(x, x^*) = \int_k \phi(x + \xi) < \xi, \ x^* > d\alpha(\xi),$$

where α is the Haar measure on k which gives each point measure one. θ_k is the adelic analogue of Riemann's theta function ([15], §§ 16, 40). θ_k is continuous and since k is discrete

$$\theta_k(x, x^*) = \sum_{\xi \in k} \phi(x + \xi) < \xi, \ x^* > .$$

Proposition. *Let* $= \mathbb{F}_q{}^* = \{x^* \in \hat{k}_A \mid x^*(a) = 1$ *for* $a \in \mathbb{F}_q\}$. *Let* $x \in k_A$. *If there exists* $\xi \in k$ *such that* $x + \xi \in R$, *then* $\theta_k(x, x^*) = q < \xi, \ x^* >$, *for* $x^* \in \mathbb{F}_{q*}$ *and* $\theta_k(x, x^*) = 0$ *for* $x^* \notin \mathbb{F}_q{}^*$. *If there exists no* $\xi \in k$ *such that* $x + \xi \in R$, *then* $\theta_k(x, x^*) = 0$ *for all* $x^* \in \hat{k}_A$.

Proof. Let $\xi \in k$ be such that $x + \xi \in R$. Then $x + \xi + a \in R$ for all $a \in \mathbb{F}_q$ and $\xi' \in k$ has the property $x + \xi' \in R$ if and only if $\xi' = \xi + a$ for some $a \in \mathbb{F}_q$. Hence

$$\theta_k(x, x^*) = \sum_{a \in \mathbb{F}_q} \langle \xi + a, x^* \rangle = \langle \xi, x^* \rangle \sum_{a \in \mathbb{F}_q} \langle a, x^* \rangle$$

for any $x^* \in \hat{k}_A$. If $x^* \in \mathbb{F}_{q*}$, this sum has the value $q\langle \xi, x^* \rangle$. If $x \notin \mathbb{F}_{q*}$, this sum is zero. The last assertion of the proposition is obvious.

Theorem. *Let* A *be a topological ring and* k, k' *be global fields such that* k_A *and* k'_A *are isomorphic to* A. *Let* $\phi : A \to k_A$ *and* $\psi : A \to k'_A$ *be isomorphisms of topological rings and* $\hat{\phi} : \hat{k}_A \to \hat{A}$, $\hat{\psi} : \hat{k}'_A \to \hat{A}$ *be the dual isomorphisms. Let* $\theta_{A,k} : A \times \hat{A} \to \mathbb{C}$ (*resp.* $\theta_{A,k'} : A \times \hat{A} \to \mathbb{C}$) *be the function*

$\theta_k^o(\phi, \hat{\phi}^{-1})$ (*resp.* $\theta_{k'}^o(\psi, \hat{\psi}^{-1})$). *Let* F *and* F' *be the fields of constants of* k *and* k' *respectively. If* $\phi^{-1}(F) = \psi^{-1}(F')$ *and* $\theta_{A,k}(x, x^*) = \theta_{A,k'}(x, x^*)$ *for all* $x \in \phi^{-1}(k) \cup \psi^{-1}(k')$ *and all* $x^* \in \phi^{-1}(F)_*$, *then* $\phi^{-1}(k) = \psi^{-1}(k')$.

Proof. Let $\mathbb{F}_q = \phi^{-1}(F) = \psi^{-1}(F')$. By the propositon $\theta_{A,k}(x, x^*) = q\langle -x, x^* \rangle$ for each $x^* \in \mathbb{F}_{q*}$, so by the hypothesis $\theta_{A,k'}(x, x^*) = q\langle -x, x^* \rangle$. Using the proposition one sees that there exists $\xi' \in k'$ such that $\theta_{A,k'}(x, x^*) = q\langle \psi^{-1}(\xi'), x^* \rangle$ for each $x^* \in \mathbb{F}_{q*}$. So $\langle -x, x^* \rangle = \langle \psi^{-1}(\xi'), x^* \rangle$ for each $x^* \in \mathbb{F}_{q*}$. However, the set of x^* in $\hat{A}$ which induce the trivial character on $\mathbb{F}_q$ separate the cosets of $\mathbb{F}_q$ in A. So $\psi^{-1}(\xi') = -x + a$ for some $a \in \mathbb{F}_q$. Hence $\phi^{-1}(K) \subset \psi^{-1}(k')$, symmetrically $\psi^{-1}(k') \subset \psi^{-1}(k)$.

3. Examples.

We now give two ways of constructing sets of isogenous, non-isomorphic cuves of genus one. By the proposition of 1. Such curves have the same zeta function and the adele rings of their function fields are isomorphic.

Let $j \in \mathbb{F}_q n$, n 1, $j \notin \mathbb{F}_q$. There exists an elliptic curve E defined over $\mathbb{F}_q n$ and unique up to $\mathbb{F}_q n$-isomorphism with invariant j([4]). Let k be the function field of E and k^q be the image of k under the endomorphism $x \to x^q$. There is an elliptic curve $E^{(q)}$ defined over $\mathbb{F}_q n$ with function field k^q. $E^{(q)}$ has invariant j^q. Since $j \neq j^q$, E and $E^{(q)}$ are not isomorphic over $\overline{\mathbb{F}}_q$ or over any other field containing $\mathbb{F}_q$. Let $i : E \to E^{(q)}$ be the morphism determined by the inclusion $k^q \subset k$. i is a purely inseparable isogeny of degree q.

The existence of non-isomorphic elliptic curves which are separably isogenous can be shown using the general theory of abelian varieties over finite fields. We begin by recalling the principal theorems.

Let A be an abelian variety defined over $\mathbb{F}_q$, π_A be the Frobenius endomorphism of A and f_A be the characteristic polynomial of π_A. f_A is a monic polynomial degree 2 dim A with integer coeffients. The roots of f_A have complex absolute value $q^{1/2}$ ([15]). Since $f_A(\pi_A) = 0$, π_A may be regarded as an algebraic integer determined up to conjugacy. For every embedding $\rho : \mathbb{Q}(\pi_A) \to \mathbb{C}$, $\rho(\pi_A)$ has absolute value $q^{1/2}$. Generally, an algebraic integer π is called a Weil number for q if for every embedding $\rho : \mathbb{Q}(\pi) \to \mathbb{C}$, $\rho(\pi)$ has absolute value $q^{1/2}$ ([9], [12]). There is a one-to-one correspondence between the set of conjugacy classes of Weil numbers for q and the set of isogeny classes of elementary abelian varieties defined over $\mathbb{F}_q$ ([1], [9], [12]).

From now on we assume that A is elementary and $q = p^n$. Let End A denote the ring of $\mathbb{F}_q$-endomorphisms of A and let $E = (\text{End } A)\,\mathbb{Q}$. E is a

division algebra with center $F = \mathbb{Q}(\pi_A)$. E has invariant $1/2$ at each real place of F, invariant zero at each finite place of F prime to p, and invariant $\frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)}[F_v : \mathbb{Q}_p]$ at a place v of F lying over p. Finally, $2 \dim A = [E : F]^{1/2}[F : \mathbb{Q}]$ ([9]).

Let I be an ideal in End A and $H(I) = \bigcap_{a \in I} \mathrm{Ker}\ a$. I is called a kernel ideal if $I = \{a \mid aH(I) = 0\}$ ([12], 3.2). Let I, J be kernel ideals. Then $A/_{H(I)}$ is $\mathbb{F}_q$-isomorphic to $A/_{H(J)}$ if and only if $I = \lambda J$ for some invertible $\lambda \in E$ ([12], theorem 3.11). Let M be a maximal order in E. Then there is an abelian variety B, $\mathbb{F}_q$-isogeneous to A, with End $B \simeq M$ ([12]) theorem 3.13). Every ideal $I \subset$ End B is a kernel ideal and the rank of $H(I)$ equals the reduced norm of I ([12], theorem 3.15); End $B/_{H(I)}$ is also a maximal order ([12], theorem 3.14).

Consider $\pi = \frac{-1+\sqrt{-31}}{2}$, $\bar{\pi} = \frac{-1-\sqrt{-31}}{2}$. π and $\bar{\pi}$ are Weil numbers for 8. Let A be an elementary abelian variety in the isogeny class determined by π and $\bar{\pi} \cdot Z[\pi]$ is the maximal order in $\mathbb{Q}(\sqrt{-31})$ and $(2) = p_1 p_2$, where

$$p_1 = \left(-1-\sqrt{-31}, \frac{3+\sqrt{-31}}{2}\right), \quad p_2 = \left(1+\sqrt{-31}, \frac{3-\sqrt{-31}}{2}\right)$$

$(\pi) = p_1^3$ and $(\bar{\pi}) = p_2^3$. Tate's theorem shows that dim $A = 1$ and End $A \times \mathbb{Q} \simeq \mathbb{Q}(\pi)$. By Waterhouse's theorems there exists an elliptic curve E defined over $\mathbb{F}_8$ and isogeneous to A such that End $E = Z[\pi]$. Since the norm of p_i, $i = 1, 2$, is two, the isogenies $i_1 : E \to E/_{H(p_1)}$ and $i_2 : E \to E/_{H(p_2)}$ are of degree two. As (1), p_1, and p_2 are representatives of the three ideal classes of $\mathbb{Q}(\sqrt{-31})$, no two of these curves are isomorphic over $\mathbb{F}_8$. The isogenies i_1 and i_2 may be inseparable, however theorem 5.3 of [12] implies that thare exist separable isogenies from any one of these curves to any other.

References

[1] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan 20, 1968, 83-95.

[2] K. Iwasawa, *On the rings of valuation vectors*, Ann. Math 57, 1953, 331-356.

[3] K. Komatsu. *On the adele rings of algebraic number fields*, preprint.

[4] S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, Mass, 1973, Appendix 1 by J. Tate.

[5] J. Lewittes, *Riemann Surfaces and the theta functions*, Acta Math. 111, 1964, 37-61.

[6] H. Martens, *Three lectures on the classical theory of Jacobian varieties*, Algebraic geometry, Oslo, 1970: Wolters-Noodhoff, Groningen, 1972.

[7] T. Matsusaka, *On a theorem of Torelli*, AJM 80 (1958), 784-800.

[8] A Mayer, *Generating curves on abelian varieties and Riemann's theta-function*, Ann. Scuola Norm. Sup. Pisa, Ser. III, 19, 1965, 107-111.

[9] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini*, Sem. Bourbaki 21, 1968/69, no. 352.

[10] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2, 1966, 134-144.

[11] S. Turner, *Principal polarizations of abelian surfaces over finite fields*, to appear.

[12] W. Waterhouse, *Abelian varieties over finite fields*, Ann. Scient. Éc. Norm. Sup, 4, t. 2, 1969, 521-560.

[13] A. Weil, *Basic Number Theory*, Die Grundlehren der math. Wissenschaften, Band 144, Springer-Verlag, Berlin and New York, 1967.

[14] A. Weil, *Courbes algébriques et varietés abéliennes*, Hermann, Paris, 1971.

[15] A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math., 111, 1964, 143-211.

[16] A. Weil, *Zum Beweis des Torellischen Satzes*, Nachrichten der Akademie der Wissenschaften in Göttingen 2 (1957), 33-53.

[17] O. Zariski and P. Samuel, *Commutative Algebra*, Van Nostrand Princeton, 1960.

Departamento de Matemática
Pontifícia Universidade Católica do Rio de Janeiro
Rua Marquês de São Vicente 209/263
Rio de Janeiro, Brasil