ACTA ARITHMETICA
139.1 (2009)

A note on global units and local units of function fields

by

SU HU and YAN LI (Beijing)

1. Introduction. Let K be any Galois extension of $\mathbb{Q}$, and U_K be the unit group of K. For any place v of K, let U_v be the group of local units of K_v. Recently, the second author and Xianke Zhang [6] considered the problem of whether there exists an odd prime p such that the map

$$U_K/U_K^2 \to \prod_{v\mid p} U_v/U_v^2$$

is injective. In fact, they proved that the existence of such primes is equivalent to $\mathrm{Hom}(U_K/U_K^2, \{\pm 1\})$ is a cyclic $\mathbb{F}_2[\mathrm{Gal}(K/\mathbb{Q})]$-module. Moreover, they also proved that if the class number $h_{\mathbb{Q}(\zeta_{p^r})^+}$ is odd, then such primes exist for $\mathbb{Q}(\zeta_{p^r})^+$ and $\mathbb{Q}(\zeta_{p^r})$, where p is an odd prime and $\mathbb{Q}(\zeta_{p^r})^+$ is the maximal real subfield of $\mathbb{Q}(\zeta_{p^r})$.

Let K be a geometric Galois extension of the rational function field $k = \mathbb{F}_q(t)$. Let O_K be the integral closure of $\mathbb{F}_q[t]$ in K. Let U_K be the group of units of O_K and U_v be the group of local units of K_v. In this note, we will generalize the second author and Zhang's methods to consider the question whether there exists a finite place P of $\mathbb{F}_q(t)$ such that the map

$$U_K/U_K^d \to \prod_{v\mid P} U_v/U_v^d$$

is injective, where $d > 1$ is a factor of $q-1$. Let μ_d be the group of dth roots of unity. We will prove there exist such places P if and only if $\mathrm{Hom}(U_K/U_K^d, \mu_d)$ is a cyclic $\mathbb{Z}/d\mathbb{Z}[\mathrm{Gal}(K/k)]$-module. When K is a quadratic function field, we will prove in Section 4 that there exist such places if and only if either K is imaginary, or K is real and d is odd, or K is real, d is even and there exists a fundamental unit ϵ_0 of O_K such that $N(\epsilon_0)$ is a generator of $\mathbb{F}_q^*$. Let A be a monic irreducible polynomial. Suppose that $K = k(\Lambda_A)$ is the Ath cyclotomic function field and K^+ is the maximal real subfield of K. In

2000 *Mathematics Subject Classification*: Primary 11R58; Secondary 11R60.
Key words and phrases: global unit, local unit, cyclotomic function field, cyclotomic unit.

DOI: 10.4064/aa139-1-1

Section 5, we will prove that such places exist for K and K^+ if the class number of O_{K^+} is relatively prime to d. It should be noted that the proof heavily relies on Galovich and Rosen's work on Sinnott's circular units in cyclotomic function fields [3].

2. Preliminaries. For each $d \mid q-1$, define $L = K(\sqrt[d]{U_K})$. Since $\mathbb{F}_q$ contains dth roots of unity, L is an abelian extension of K of exponent d. Set $\mathrm{Gal}(L/K) = H$ and $\mathrm{Gal}(K/\mathbb{F}_q(t)) = G$. Define an action of G on H by $gh = \tilde{g}h\tilde{g}^{-1}$, where $g \in G$, $h \in H$ and $\tilde{g}$ is a lift of g in $\mathrm{Gal}(L/\mathbb{F}_q(t))$. By Kummer theory (e.g. Theorem 8.1 of [5]), there is a non-degenerate G-equivariant bilinear pairing

$$H \times U_K/U_K^d \to \mu_d, \qquad (h, \bar{u}) = \frac{h(\sqrt[d]{u})}{\sqrt[d]{u}}.$$

Therefore we have $H \cong \mathrm{Hom}(U_K/U_K^d, \mu_d)$ as G-modules. The action of G on $\mathrm{Hom}(U_K/U_K^d, \mu_d)$ is defined by

$$gf(\bar{u}) = f(g^{-1}\bar{u})$$

for $g \in \mathrm{Gal}(K/\mathbb{F}_q(t))$, $f \in \mathrm{Hom}(U_K/U_K^d, \mu_d)$, $\bar{u} \in U_K/U_K^d$.

Assume the infinite place $(1/t)$ of $\mathbb{F}_q(t)$ splits into r places of K. By Dirichlet's unit theorem, the rank of U_K/U_K^d as $\mathbb{Z}/d\mathbb{Z}$-module is equal to r. Let $\{u_1, \ldots, u_r\} \subset U_K$ be representatives such that $\overline{u}_1, \ldots, \overline{u}_r$ form a $\mathbb{Z}/d\mathbb{Z}$-basis of U_K/U_K^d. Then it is easy to show that

$$H \simeq \mathrm{Gal}(K(\sqrt[d]{u_1})/K) \times \cdots \times \mathrm{Gal}(K(\sqrt[d]{u_r})/K).$$

The isomorphism is given by restriction to the subfields.

The following is Chebotarev's density theorem for global function fields (Theorem 9.13A of [7]).

Theorem 2.1 (Chebotarev). *Let L/K be a Galois extension of global function fields and* $\mathrm{Gal}(L/K) = H$. *Let $C \subset H$ be a conjugacy class and S'_K be the set of primes of K which are unramified in L. Then*

$$\delta(\{\mathfrak{p} \in S'_K \mid (\mathfrak{p}, L/K) = C\}) = \#C/\#H,$$

where δ means Dirichlet density. In particular, every conjugacy class C is of the form $(\mathfrak{p}, L/K)$ for infinitely many places $\mathfrak{p}$ of K.

Lemma 2.2. *Let $u \in U_K$ and $\mathfrak{p}$ be a place of K which is unramified in L. Then $u \in U_{\mathfrak{p}}^d$ if and only if $(\mathfrak{p}, L/K)$ fixes $K(\sqrt[d]{u})$, where $L = K(\sqrt[d]{U_K})$ (see the beginning of this section).*

Proof. $u \in U_{\mathfrak{p}}^d$ is equivalent to $\mathfrak{p}$ splitting completely in $K(\sqrt[d]{u})$. Since $\mathfrak{p}$ is unramified in $K(\sqrt[d]{u})$, this is equivalent to $(\mathfrak{p}, K(\sqrt[d]{u})/K) = \mathrm{Id}$. As the Artin symbol satisfies $(\mathfrak{p}, L/K)|_{K(\sqrt[d]{u})} = (\mathfrak{p}, K(\sqrt[d]{u})/K)$, the result follows. ∎

3. Proof of the main result

PROPOSITION 3.1. *The natural map $U_K/U_K^d \to \prod_v U_v/U_v^d$ is injective, where v runs over all finite places of K.*

Proof. Let u belong to the kernel of the map. Then $u \in U_v^d$ for all v. By Lemma 2.2, $(v, K(\sqrt[d]{u})/K) = \mathrm{Id}$ for all finite places v. Consequently, $\delta(\{\mathfrak{p} \in S'_K \mid (\mathfrak{p}, L/K) = \mathrm{Id}\}) = 1$. By Chebotarev's density theorem, the extension $K(\sqrt[d]{u})/K$ is trivial. Thus $u \in U_K^d$. ∎

PROPOSITION 3.2. *There exist places $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of K such that the natural map*

$$U_K/U_K^d \to \prod_{1\le i\le r} U_{\mathfrak{p}_i}/U_{\mathfrak{p}_i}^d$$

is injective.

Proof. Let $\sigma_1, \dots, \sigma_r \in H$ be such that the restriction of σ_i to $K(\sqrt[d]{u_j})$ is trivial when $j \neq i$ and is a generator of $\mathrm{Gal}(K(\sqrt[d]{u_j})/K)$ for $j = i$. By Chebotarev's density theorem, there exist finite places $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of K such that $(\mathfrak{p}_i, L/K) = \sigma_i$. If u belongs to the kernel, then $u \in U_{K_{\mathfrak{p}_i}}^d$. By Lemma 2.2, σ_i fixes $K(\sqrt[d]{u})$. By construction, $\sigma_1, \dots, \sigma_r$ generate H, so $K(\sqrt[d]{u}) = K$ by Galois theory. Thus $u \in U_K^d$. ∎

PROPOSITION 3.3. *Let P be a finite place of $\mathbb{F}_q(t)$. Then the natural map*

$$U_K/U_K^d \to \prod_{v\mid P} U_v/U_v^d$$

is injective if and only if for some place $v \mid P$ (hence for all $v \mid P$), $(v, L/K)$ is a $\mathbb{Z}/d\mathbb{Z}[G]$ generator of H.

Proof. Let u be any unit of K. By Lemma 2.2,

$$u \in U_v^d,\ \forall v \mid P \ \Leftrightarrow\ (v, L/K) \text{ fixes } K(\sqrt[d]{u}),\ \forall v \mid P.$$

It is obvious that

$$u \in U_K^d \ \Leftrightarrow\ K(\sqrt[d]{u}) = K.$$

Thus, $U_K/U_K^d \to \prod_{v\mid P} U_v/U_v^d$ being injective is equivalent to

$$\forall u \in U_K,\ (v, L/K) \text{ fixes } K(\sqrt[d]{u}),\ \forall v \mid P \ \Rightarrow\ K(\sqrt[d]{u}) = K.$$

By Galois theory, this is equivalent to the subgroup generated by $(v, L/K)$ for all $v \mid P$ being equal to H. Recall the definition of the action of G on H in Section 2: $(gv, L/K) = \tilde{g}(v, L/K)\tilde{g}^{-1} = g(v, L/K)$. This is also equivalent to $(v, L/K)$ being a $\mathbb{Z}/d\mathbb{Z}[G]$ generator of H for any $v \mid P$. ∎

THEOREM 3.4. *There exists a finite place P of $\mathbb{F}_q(t)$ such that the map*

$$U_K/U_K^d \to \prod_{v\mid P} U_v/U_v^d$$

is injective if and only if $\mathrm{Hom}(U_K/U_K^d, \mu_d)$ is a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module.

Proof. Since H is isomorphic to $\mathrm{Hom}(U_K/U_K^d, \mu_d)$ as $\mathbb{Z}/d\mathbb{Z}[G]$-modules, the "only if" part follows easily from Proposition 3.3. Conversely, if H is a cyclic module, let $\sigma \in H$ be a $\mathbb{Z}/d\mathbb{Z}[G]$ generator of H. By Chebotarev's density theorem, there exists a finite place $\mathfrak{p}$ such that $(\mathfrak{p}, L/K) = \sigma$. Also by Proposition 3.3, we conclude that $U_K/U_K^d \to \prod_{g\in G} U_{g\mathfrak{p}}/U_{g\mathfrak{p}}^d$ is injective. ∎

The following definition can be found on page 371 of [8].

Definition 3.5. An extension K of $k = \mathbb{F}_q(t)$ is called *totally real* if the prime at infinity of k (which corresponds to $1/t$) splits completely in K.

Lemma 3.6. *Let G be a finite group and V be a free $\mathbb{Z}/d\mathbb{Z}$-module of rank $r = \#G$. Assume G acts on V linearly. Then V is a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module if and only if $V^* = \mathrm{Hom}(V, \mathbb{Z}/d\mathbb{Z})$ is a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module.*

Theorem 3.7. *If K is a totally real geometric Galois extension of $\mathbb{F}_q(t)$, there exists a finite place P of $\mathbb{F}_q(t)$ such that the natural map*

$$U_K/U_K^d \to \prod_{v|P} U_v/U_v^d$$

is injective if and only if U_K/U_K^d is a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module.

Proof. Suppose that $[K : \mathbb{F}_q(t)] = n$. By Definition 3.5, K has n infinite places. By Dirichlet's unit theorem, U_K/U_K^d is a free $\mathbb{Z}/d\mathbb{Z}$-module of rank n. By Theorem 3.4, the injectivity in question is equivalent to $\mathrm{Hom}(U_K/U_K^d, \mu_d)$ being a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module. Applying Lemma 3.6 to $V = U_K/U_K^d$, we get the desired result. ∎

A unit u is called a *Minkowski unit* if its Galois conjugates generate a subgroup of finite index in the whole unit group. We know that such units always exist (see [9, Lemma 5.27], the proof is the same for global function fields).

Corollary 3.8. *Let $K/\mathbb{F}_q(t)$ be a totally real geometric Galois extension. There exists a finite place P of $\mathbb{F}_q(t)$ such that the natural map*

$$U_K/U_K^d \to \prod_{v|P} U_v/U_v^d$$

is injective if and only if there exists a Minkowski unit ϵ such that the index of $\mathbb{Z}[G]\epsilon$ in U_K is relatively prime to d.

Proof. By Theorem 3.4, the existence of such P is equivalent to U_K/U_K^d being a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module. This means that there exists a unit ϵ such that $U_K = U_K^d(\mathbb{Z}[G]\epsilon)$. Let $E = \mathbb{Z}[G]\epsilon$. We get

$$U_K = EU_K^d \;\Leftrightarrow\; U_K/E = (U_K/E)^d \;\Leftrightarrow\; (\#U_K/E, d) = 1.$$

This completes the proof of the corollary. ∎

4. The case of quadratic function fields. In this section, we assume K is a quadratic extension of $k=\mathbb{F}_q(t)$ and $2\nmid q$. We will use the theory developed in Section 3 to investigate the situation of quadratic function fields. Such fields can be written as $k(\sqrt{D})$, where D is a square free polynomial of $\mathbb{F}_q[t]$. They were systematically studied by E. Artin [1].

Fix a generator g of $\mathbb{F}_q^*$. Then we can assume that the leading coefficient of D is 1 or g. The infinite place $(1/t)$ is splitting, inertial, or ramified in K when, respectively: the degree of D is even and $\operatorname{sgn}(D)=1$; the degree of D is even and $\operatorname{sgn}(D)=g$; or the degree of D is odd. Then the field K is called real, inertial imaginary, or ramified imaginary respectively, according to E. Artin [1]. When K is real, we let ϵ_0 be the fundamental unit of K. Any fundamental unit is determined only up to multiplication by a constant, thus its norm is either a square or g times a square. So multiplying ϵ_0 by an appropriate constant we can assume $N(\epsilon_0)$ is 1 or g.

Now we state the main theorem of this section.

THEOREM 4.1. *Let the notations be as above. There exists a finite place P of $\mathbb{F}_q(t)$ such that*

$$U_K/U_K^d\to\prod_{v|P}U_v/U_v^d$$

is injective if and only if either K is imaginary, or K is real and d is odd, or K is real, d is even and $N(\epsilon_0)=g$.

Proof. If K is imaginary, then $U_K=\mathbb{F}_q^*$ and $U_K/U_K^d=\mathbb{F}_q^*/\mathbb{F}_q^{*d}$ is a cyclic group. Thus $\operatorname{Hom}(U_K/U_K^d,\mathbb{Z}/d\mathbb{Z})$ is a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module. By Theorem 3.4, there exists a finite place P of $\mathbb{F}_q(t)$ such that

$$U_K/U_K^d\to\prod_{v|P}U_v/U_v^d$$

is injective.

If K is real, then $U_K=\langle\epsilon_0\rangle\times\mathbb{F}_q^*$. By Corollary 3.8, the existence of such places is equivalent to the existence of a Minkowski unit ϵ such that $(\#U_K/\mathbb{Z}[G]\epsilon,d)=1$. If $N(\epsilon_0)=g$, we can take $\epsilon=\epsilon_0$, and then $U_K=\mathbb{Z}[G]\epsilon$. If $N(\epsilon_0)=1$ and d is odd, we can take $\epsilon=g\epsilon_0$, and then

$$\mathbb{Z}[G]\epsilon=\mathbb{Z}\epsilon\oplus\langle N(\epsilon)\rangle=\mathbb{Z}\epsilon\oplus\langle g^2\rangle.$$

Thus $\#U_K/\mathbb{Z}[G]\epsilon=2$ is prime to d. If $N(\epsilon_0)=1$ and d is even, for any Minkowski unit ϵ, write $\epsilon=\epsilon_0^kg^l$, $k,l\in\mathbb{Z},k\neq0$. As above,

$$\mathbb{Z}[G]\epsilon=\mathbb{Z}\epsilon\oplus\langle N(\epsilon)\rangle=\mathbb{Z}\epsilon\oplus\langle g^{2l}\rangle\subset\mathbb{Z}\epsilon\oplus\langle g^2\rangle.$$

Thus $2\,|\,\#U_K/\mathbb{Z}[G]\epsilon$, so $2\,|\,(\#U_K/\mathbb{Z}[G]\epsilon,d)$. The proof is complete. ∎

5. The case of cyclotomic function fields. Before stating the main theorem of this section, we must introduce some notation. Write $k = \mathbb{F}_q(t)$ and $R = \mathbb{F}_q[t]$. Let k^{ac} be the algebraic closure of k. In order to construct the explicit class field theory for k, Carlitz [2] introduced an R-module structure on k^{ac}, called the *Carlitz module* (see also [4]). Let $\mathrm{End}(k^{\mathrm{ac}})$ be the ring of $\mathbb{F}_q$-algebra endomorphisms of k^{ac}. Let

$$\rho : R \to \mathrm{End}(k^{\mathrm{ac}}), \qquad M \mapsto \rho_M,$$

be a ring homomorphism defined by

$$\rho_a(\alpha) = a\alpha, \qquad \rho_t(\alpha) = t\alpha + \alpha^q,$$

where $a \in \mathbb{F}_q$ and $\alpha \in k^{\mathrm{ac}}$. Let

$$\Lambda_M = \{\alpha \in k^{\mathrm{ac}} \mid \rho_M(\alpha) = 0\},$$

which is called the *M-torsion module* of k^{ac}. If M is monic, $k(\Lambda_M)$ is called the Mth *cyclotomic function field*. Chapter 12 of [7] gives a nice exposition of the theory of cyclotomic function fields. Let $S_\infty(k(\Lambda_M))$ be the set of infinite places of $k(\Lambda_M)$ and U_M be the group of $S_\infty(k(\Lambda_M))$-units of $k(\Lambda_M)$. For simplicity, let P(3) denote the following property: there exists a finite place P in $\mathbb{F}_q(t)$ such that $U_K/U_K^d \to \prod_{v\mid P} U_v/U_v^d$ is injective, where K is a geometric Galois extension of $\mathbb{F}_q(t)$. Now we can state the main theorem of this section.

Theorem 5.1. *Let A be a monic irreducible polynomial in $\mathbb{F}_q[t]$, $K = k(\Lambda_A)$ and K^+ be the maximal real subfield of K (for the definitions, see Theorem 12.14 of [7]). Let h_A be the class number of O_K and h_A^+ be the class number of O_K^+. If $d \mid q-1$ and $(h_A^+, d) = 1$, then P(3) holds for K and K^+.*

Before proving the above theorem, we briefly recall Galovich and Rosen's work on Sinnott's cyclotomic units in cyclotomic function fields [3].

Definition 5.2. Let M be a monic polynomial in $\mathbb{F}_q[t]$, and λ be a primitive M-torsion element. Define

$$S = \{\rho_B(\lambda)/\lambda \mid B \text{ is a monic polynomial, } 0 < \deg B < \deg M, (B, M) = 1\}$$

(obviously, $S \subset U_{k(\Lambda_M)^+}$). The elements in the subgroup generated by S are called the *Kummer–Hilbert circular units*, denoted by $C_y(k(\Lambda_M)^+)$. Let G be the multiplicative subgroup of $k(\Lambda_M)^*$ generated by $\mathbb{F}_q^*$ and $\Lambda_M^* = \Lambda_M - \{0\}$. The elements of $C = G \cap U_{k(\Lambda_M)}$ and $C^+ = C \cap U_{k(\Lambda_M)^+}$ are called the *Sinnott circular units* of $k(\Lambda_M)$ and $k(\Lambda_M)^+$, respectively.

Remark 5.3. Since A is irreducible, from [3] we know that

$$U_K = U_{K^+}, \qquad C = C^+ \quad \text{and} \quad C^+ = \mathbb{F}_q^* C_y(K^+).$$

In this case, Galovich and Rosen proved (see [3])

THEOREM 5.4 (Galovich–Rosen). $[U_K : C] = [U_{K^+} : C^+] = h_A^+$.

Now we can start the proof of Theorem 5.1.

Proof of Theorem 5.1. Let

$$G = \mathrm{Gal}(K/k) \quad \text{and} \quad G^+ = \mathrm{Gal}(K^+/k).$$

From Remark 5.3, we have $U_K/U_K^d = U_{K^+}/U_{K^+}^d$. Thus $\mathrm{Hom}(U_K/U_K^d, \mu_d)$ is a cyclic $\mathbb{Z}/d\mathbb{Z}[G]$-module if and only if $\mathrm{Hom}(U_{K^+}/U_{K^+}^d, \mu_d)$ is a cyclic $\mathbb{Z}/d\mathbb{Z}[G^+]$-module. By Theorem 3.4, P(3) holds for K if and only if P(3) holds for K^+. From Theorem 5.4, $h_A^+ = [U_{K^+} : C^+]$, so $([U_{K^+} : C^+], d) = 1$ by assumption. If we can show that C^+ is a cyclic $\mathbb{Z}/d\mathbb{Z}[G^+]$-module, then by Corollary 3.8, we will complete the proof. Suppose M is a generator of $(\mathbb{F}_q[t]/A\mathbb{F}_q[t])^*$. Since by Remark 5.3, $C^+ = \mathbb{F}_q^* C_y(K^+)$, C^+ is generated by the set

$$\tilde{S} = \{\rho_{M^i}(\lambda)/\lambda \mid 1 \le i \le q^{\deg A} - 1\}.$$

For each polynomial W relatively prime to A there is a unique element $\sigma_W \in G$ such that $\sigma_W(\lambda) = \rho_W(\lambda)$ where λ is a primitive A-torsion element (see Theorem 12.8 of [7]). Using the definition of the group ring action, the multiplicity of σ_N, and cancellation in a telescoping product, we have

$$\begin{aligned} \frac{\rho_{M^{i+1}}(\lambda)}{\lambda} &= \frac{\sigma_{M^{i+1}}(\lambda)}{\lambda} \\ &= (1 + \sigma_M + \sigma_{M^2} + \cdots + \sigma_{M^i})\, \frac{\sigma_M(\lambda)}{\lambda}. \end{aligned}$$

Thus

$$C^+ = \mathbb{Z}[G]\, \frac{\sigma_M(\lambda)}{\lambda} = \mathbb{Z}[G^+]\, \frac{\sigma_M(\lambda)}{\lambda}$$

is a cyclic module, and the proof is finished. ■

Acknowledgements. The authors are enormously grateful to the anonymous referee for his/her helpful comments.

References

[1] E. Artin, *Quadratische Körper im Gebiete der höherer Kongruenzen I*, Math. Z. 19 (1924), 153–206.

[2] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. 43 (1938), 167–182.

[3] S. Galovich and M. Rosen, *Units and class groups in cyclotomic function field*, J. Number Theory 14 (1982), 156–184.

[4] D. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77–91.

[5] S. Lang, *Algebra*, 3rd rev. ed., Springer, New York, 1986.

[6] Y. Li and X. Zhang, *Global unit squares and local unit squares*, J. Number Theory 128 (2008), 2687–2694.

[7] M. Rosen, *Number Theory in Function Fields*, Springer, New York, 2002.
[8] —, *The Hilbert class field in function fields*, Exp. Math. 5 (1987), 365–378.
[9] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

Department of Mathematical Sciences
Tsinghua University
Beijing 100084, China
E-mail: hus04@mails.tsinghua.edu.cn
liyan_00@mails.tsinghua.edu.cn

Received on 10.3.2008
and in revised form on 12.2.2009 (5659)