数理解析研究所講究録
998巻 1997年 198-202

ON THE CYCLOTOMIC UNITS IN FUNCTION FIELDS

LINSHENG YIN

Department of Mathematics, Zhongshan University, Guangzhou 510275, P. R. China

1. Background.

In classical number theory, there are two famous cases in which unit index is equal to class number up to an elementary factor for algebraic number fields. We first recall them briefly.

(1). Cyclotomic units. Let $\mathbb{Q}$ be the rational number field and let $\zeta_m = \exp(\frac{2\pi i}{m})$, where m is a positive integer and $m \not\equiv 2(\mathrm{mod}4)$. Let C be the group of cyclotomic units of $K = \mathbb{Q}(\zeta_m)$. Let h^+ be the class number of the maximal real subfield of K. Let O_K^* is the unit group of K. It is proved by Kummer that $[O_K^* : C] = h^+$ when $m = p$ is a prime. It is easy to show that Kummer's result is also right when $m = p^r$. What is the index of C for general m? This was answered by Sinnott in 1978.

Theorem [S]. *We have*

$$[O_K^* : C] = 2^a h^+$$

where $a = 2^{s-2} - s + 1$ *and* s *is the number of the distinct prime divisors of* m.

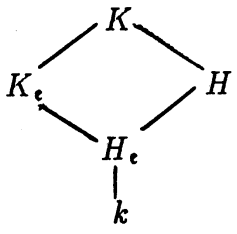
(2). Elliptic units. Let $k = \mathbb{Q}(\sqrt{-d})$ $(d > 0)$ be an imaginary quadratic field. Let $H_{\mathfrak{e}}$ and $H_{\mathfrak{m}}$ be the Hilbert class field and the ray class field with conductor $\mathfrak{m}$ of k, where $\mathfrak{m}$ is an ideal of the integral ring of k. G. Robert constructed the elliptic unit groups of $H_{\mathfrak{e}}$ and of $H_{\mathfrak{m}}$ and calculated their indices.

Theorem [R]. *Assume* $\mathfrak{m} = \mathfrak{e}$ *or* $\mathfrak{p}^n$. *Let* $E_{\mathfrak{m}}$ *be the elliptic unit group of* $H_{\mathfrak{m}}$. *Then*

$$[O_{H_{\mathfrak{m}}}^* : E_{\mathfrak{m}}] = (12^{[H_{\mathfrak{m}}:k]-1}/t)h$$

where h *is the class number of* $H_{\mathfrak{m}}$ *and* t *is a positive integer such that* $t \mid 12$.

Now we consider the case of characteristic $p > 0$. Let k be the function field of a projective smooth curve over the finite field $\mathbb{F}_q$, where $q = p^n$ is a prime power. Let ∞ be a closed point of the curve with degree d_∞. Let $\mathbb{A}$ be the Dedekind subring of k consisting of those functions having no pole other than ∞. Let $\mathbb{F}_\infty (\simeq \mathbb{F}_{q^{d_\infty}})$ be the residue field at ∞. Let $\mathfrak{m}$ be an ideal of $\mathbb{A}$. Let $H_{\mathfrak{e}}$ be the Hilbert class field of (k, ∞) and let $H = H_{\mathfrak{m}}$ be the ray class field of (k, ∞) modulo $\mathfrak{m}$. How to describe $H_{\mathfrak{e}}$ and $H_{\mathfrak{m}}$ clearly? Using Drinfeld modules, we can obviously construct the simple extensions $K_{\mathfrak{e}}$ and $K = K_{\mathfrak{m}}$ of $H_{\mathfrak{e}}$ and $H_{\mathfrak{m}}$ respectively, i.e., we have the following diagram of abelian extensions of k



and $H_\mathfrak{e}$ (resp. $H_\mathfrak{m}$) is the maximal "real" subfield of $K_\mathfrak{e}$ (resp. $K_\mathfrak{m}$) in which ∞ splits completely. Moreover we have $J = \mathrm{Gal}(K/H) \simeq \mathbb{F}_\infty^*$ and $J_\mathfrak{e} = \mathrm{Gal}(K_\mathfrak{e}/H_\mathfrak{e}) \simeq \mathbb{F}_\infty^*/\mathbb{F}_q^*$.

2. Drinfeld modules and cyclotomic extensions.

In this section we introduce chiefly the cyclotomic extensions arising in the theory of Drinfeld modules. The reader can refer to [H] for details.

Let Ω be the completion of an algebraic closure of k_∞. Let F the Frobenus of Ω raising each element to its q-power. Let $\Omega\{F\}$ be the noncommutative $\mathbb{F}_q$–algebra generated by F over Ω. A Drinfeld $\mathbb{A}$-module(of generic characteristic) ρ is a $\mathbb{F}_q$–algebra homomorphism: $\rho : \mathbb{A} \longrightarrow \Omega\{F\}$. For $x \in \mathbb{A}$, we define $\deg x$ by $\#(\mathbb{A}/x\mathbb{A}) = q^{\deg x}$. It is well-known that there exists a positive integer r such that for any $x \in \mathbb{A}$ we have

$$\rho_x = aF^{r\deg x} + \sum_{i<r\deg x} a_i F^i$$

where $a,\ a_i \in \Omega$ and $a \neq 0$. We call r to be the rank of ρ.

A sign-function is a homomorphism $\mathrm{sgn} : k_\infty^* \longrightarrow \mathbb{F}_\infty^*$ satisfying

(1) $\mathrm{sgn}(a) = a$ for $a \in \mathbb{F}_\infty^*$.

(2) $\mathrm{sgn}(U^{(1)}) = 1$, where $U^{(1)}$ is the 1-unit group of k_∞.

There are $W_\infty = q^{d_\infty} - 1$ sign functions. We fix one such function sgn. A rank 1 Drinfeld $\mathbb{A}$-module ρ is called sgn-normalized, if for all $x \in \mathbb{A}$ the coefficient $\mu_\rho(x)$ of the highest order term of ρ_x is a twisting of the sign function sgn, i.e., there exists $\sigma \in \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_q)$ such that $\mu_\rho = \sigma \circ \mathrm{sgn}$. In each isomorphism class of rank 1 Drinfeld $\mathbb{A}$-modules there exist $\kappa = (q^{d_\infty} - 1)/(q-1)$ sgn-normalized modules. Totally there exist κh sgn-normalized modules, where $h = h(\mathbb{A})$ is the class number of $\mathbb{A}$. Let X denote the set of these normalized modules. The normalizing field $K_\mathfrak{e}$ of $(k, \infty, \mathrm{sgn})$ is generated over k by the coefficients of ρ_x for any $\rho \in X$ and any $x \in \mathbb{A} - \mathbb{F}_q$. It is independent of ρ or x. For $\rho \in X$, let $\Lambda_\mathfrak{m}^\rho = \{\alpha \in \Omega \mid \rho_x(\alpha) = 0 \text{ for } x \in \mathfrak{m}\}$ be the $\mathfrak{m}$-torsion points associated to ρ, which is an $\mathbb{A}$-module via ρ isomorphic to $\mathbb{A}/\mathfrak{m}$. Let $\Lambda_\mathfrak{m} = \cup_{\rho\in X}\Lambda_\mathfrak{m}^\rho$. Then $K = K_\mathfrak{e}(\Lambda_\mathfrak{m}^\rho) = K_\mathfrak{e}(\Lambda_\mathfrak{m})$ is abelian over k and is called the cyclotomic extention of k with conductor $\mathfrak{m}$. Analogy to the case of cyclotomic number fields, we give the following definition.

Definition. *Let $P = P_\mathfrak{m}$ be the subgroup of K^* generated by $\Lambda_\mathfrak{m} - \{0\}$ and by $\mathbb{F}_\infty^*$. Let $C = P \cap O_K^*$. Call C (resp. P) the group of cyclotomic units (resp. cyclotomic numbers) of K.*

3. Conclusions.

For a finite extension F/k, we denote O_F the integral closure of $\mathbb{A}$ in F, O_F^* the unit group of F, $h(O_F)$ the ideal class number of O_F, $h(F)$ the divisor class number of F. We have $h = h(\mathbb{A}) = d_\infty h(k)$. Let $G_1 = \mathrm{Gal}(H_\mathfrak{e}/k) \simeq \mathrm{Pic}(\mathbb{A})$ and let $N = N_\mathfrak{m}$ be the subgroup of G_1 generated by the Artin symbols $\tau_\mathfrak{p} = (\mathfrak{p}, H_\mathfrak{e}/k)$ for all primes $\mathfrak{p} \mid \mathfrak{m}$. Let $e = [G_1 : N_\mathfrak{m}]$ be the index. We first calculate the rank of C [Sect. 2, Y1].

(1). $\mathrm{rank}\, C = [H : k] - e$.

Thus the rank of C is less than that of O_K^* unless $N_\mathfrak{m} = G_1$. The reason is that C does not contain enough unramified units if $N_\mathfrak{m} \neq G_1$. This means that the rank of $C \cap K_\mathfrak{e}$ is less than that of $O_{K_\mathfrak{e}}^*$ in this case. We then construct the group $\bar{E}$ of unramified elliptic units of $K_\mathfrak{e}$ with maximal rank in $K_\mathfrak{e}$ and naterally extend C by $\bar{C} = C \cdot \bar{E}$. We chiefly explain the construction of $\bar{E}$ here. Using the ξ-invariant of Drinfeld modules, we first constructed a

$\mathrm{Gal}(K_\mathfrak{e}/k)$–submodule Q of $K_\mathfrak{e}$ and let $E = Q \cap O_{K_\mathfrak{e}}^*$. We proved that $\bar{E} = E^{1/(q-1)} \subset K_\mathfrak{e}$. Let s be the number of distinct prime divisors of $\mathfrak{m}$. We regard $K_\mathfrak{e}$ as the cyclotomic extension with conductor $\mathfrak{e}$ and understand that $s = 0$ means $\mathfrak{m} = \mathfrak{e}$. Let $\bar{C}_\mathfrak{e} = \bar{E}$. Our next conclusion gives the indices of $\bar{E}$ and $\bar{C}$ respectively.

(2). *Assume* $(h, q-1) = 1$ *when* $s \geq 3$. *Then*

$$[O_K^* : \bar{C}] = (q-1)^a h(O_H)$$

where $a = 0$ *if* $s = 0$ *or* 1, *and* $a = e(2^{s-2} - 1) - (s-2)$ *if* $s \geq 2$.

We conjecture that the restrictive hypothesis above is unnecessary. Our last conclusion is an application of the index formula in the case when the conductor is a prime ideal. In the classical theory of numbers, the Kummer criterion is a very important result on the p-divisibility of the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where p is a prime and ζ_p is a primitive p-th root of 1. The last conclusion gives the analogue and generalization of this criterion to function fields. We first defined Bernoulli ideals of $\mathbb{A}$ (cf. [Sect 5, Y2]). Let B_i be the i-th Bernoulli ideal of $\mathbb{A}$. By using the index formula in (2), we got (cf. [Sect 6, Y2])

(3). *Let* $\mathfrak{m} = \mathfrak{p}$ *be a prime and let* $d = \deg \mathfrak{p} > 1$. *If* p *divides* $h(O_{H_\mathfrak{p}})$, *then there is an ideal* B_i, $i \equiv 0 (\mathrm{mod}(q-1))$ *and* $1 \leq i \leq q^d - 2$, *such that* $\mathfrak{p} \mid B_i$.

We also proved these Bernoulli ideals above are non-zero [Sect. 7, Y2].

4. Outline of the calculation of the indices.

In this section, we only give an outline of the calculation of the indices. For the details and the proofs of the other conclusions, we refer to [Y1], [Y2]. We first explain three definitions used in the calculation.

(1). lattice index. Let $G = \mathrm{Gal}(K/k)$. For a subset T of G, write $s(T) = \sum_{\sigma \in T} \sigma$. Let $e^+ = (1/W_\infty)s(J)$ and let $e_1 = (1/|G|)s(G)$. Let $Y = (1 - e_1)e^+\mathbb{Q}[G]$. It is a $\mathbb{Q}$-subspace of $\mathbb{Q}[G]$ with dimension $r = [H : k] - 1$. A lattice in Y is a finitely generated subgroup of Y with the maximal rank. Let L and L' be two lattices in Y. Then there exists a nonsingular linear transformation $A : Y \to Y$ such that $A(L) = L'$. Sinnott [S] defined the index $(L : L')$ to be $(L : L') = |\det A|$. Clearly $(L : L')$ does not depend on the choice of A. When $L' \subseteq L$ one sees the index is equal to $[L : L']$. Let L'' be another lattice of Y. It is easy to see $(L : L'') = (L : L')(L' : L'')$.

(2). Logarithm map. The logarithm map is defined to be the map $l : K^* \longrightarrow \mathbb{Q}[G]$ such that

$$l(x) = \sum_{\sigma \in G} v_\infty(x^\sigma)\sigma^{-1}$$

for $x \in K^*$, where v_∞ is the extension to Ω of the normalized valuation of k_∞ at ∞. We also write $l^* = (1 - e_1)l$.

(3). Some G–modules. For a prime ideal $\mathfrak{p}$ of $\mathbb{A}$, let $T_\mathfrak{p}$ be the inertia group of $\mathfrak{p}$ in G and let $F_\mathfrak{p}$ be any Frobenius automorphism for $\mathfrak{p}$, which is well defined modulo $T_\mathfrak{p}$. We set $\bar{\sigma}_\mathfrak{p} = F_\mathfrak{p}^{-1} s(T_\mathfrak{p})/|T_\mathfrak{p}|$. Notice that $\bar{\sigma}_\mathfrak{p}$ is the unique element in $\mathbb{C}[G]$ satisfying $\chi(\bar{\sigma}_\mathfrak{p}) = \chi(\mathfrak{p})$ for any $\chi \in \hat{G}$, the character group of G with complex values.

Let $I_\mathfrak{f} = \mathrm{Gal}(K/K_\mathfrak{f})$ for $\mathfrak{f} \mid \mathfrak{m}$. Note that $I_\mathfrak{e} = \mathrm{Gal}(K/K_\mathfrak{e}) \simeq (\mathbb{A}/\mathfrak{m})^*$. We define V to be the $R = \mathbb{Z}[G]$-submodule of $\mathbb{Q}[G]$ generated by

$$\alpha_\mathfrak{f} = s(I_\mathfrak{f}) \prod_{\mathfrak{p} \mid \mathfrak{f}} (1 - \bar{\sigma}_\mathfrak{p})$$

with $\mathfrak{f} \mid \mathfrak{m}$, $\mathfrak{f} \neq \mathfrak{e}$. We also set $U = V + s(I_\mathfrak{e})R$ and $U' = (q-1)V + s(I_\mathfrak{e})R$.

For any R-module M, we denote by M_0 the submodule of elements killed by $s(G)$. Obviously $V_0 = V$, $U_0 = V + s(I_\mathfrak{e})R_0$ and $U'_0 = (q-1)V + s(I_\mathfrak{e})R_0$.

Now we can explain the outline of the calculation of the indices. In the following we permit $\mathfrak{m} = \mathfrak{e}$ (i.e. $s = 0$) and assume $P_\mathfrak{e} = C_\mathfrak{e} = \mathbb{F}_\infty^*$. We also assume $V = 0$ and $e = h$ in this case. Let $P' = \mathbb{F}_\infty^* P_\mathfrak{m}^{s(J_1)} Q_{\mathfrak{m}'}$ and let $C' = P' \cap O_K^*$. We have $C' = \mathbb{F}_\infty^* \bar{C}^{q-1}$. Thus

$$[O_K^* : \bar{C}] = (q-1)^{-r}[O_K^* : C'] = (q-1)^{-r}[l(O_K^*) : l(C')]$$

(*)

$$= (q-1)^{-r}(l(O_K^*) : e^+R_0)(e^+R_0 : e^+U_0)(e^+U_0 : e^+U'_0)(e^+U'_0 : l^*(P'))(l^*(P') : l(C')).$$

To calculate the index, we need compute the five indices in the right hand side of (*). Here we only explain their calculations briefly and write the values. For details we refer to [Y1] and [Y2].

(4.1). It is easy to see that $(e^+R_0 : l(O_K^*))$ is equal to the regulator $R(K)$ of K. Using a property of the extension $K_\mathfrak{e}/H_\mathfrak{e}$, we get the relation of $R(K)$ with $R(H)$ [Cor.1.6, Y2]. We have

$$\text{(a)} \qquad (l(O_K^*) : e^+R_0) = 1/R(K) = \begin{cases} 1/(\kappa^{r-1}R(H)) & \text{if } s = 0 \\ \kappa Q_0/(W_\infty^r R(H)) & \text{if } s \geq 1 \end{cases}$$

where $\kappa = (q^{d_\infty} - 1)/(q-1)$ and $Q_0 = [O_K^* : O_{\bar{H}}^*]$, which is equal to 1 if $s = 1$ and $q-1$ if $s > 1$. Here $\bar{H} = K_\mathfrak{e}H$.

(4.2). First we proved that e^+V is a free subgroup of $\mathbb{Q}[G]$ with rank $r - e + 1$ [Lem.3.1, Y1]. We also showed that [Lem.3.1, Y2] $e^+V \cap e^+s(I_\mathfrak{e})R = (q-1)e^+V \cap e^+s(I_\mathfrak{e})R$. Thus $e^+U_0/e^+U'_0 \simeq e^+V/(q-1)e^+V$ and we have

$$\text{(b)} \qquad [e^+U_0 : e^+U'_0] = (q-1)^{[H:k]-e} = (q-1)^{r-e+1}.$$

Obviously the equality is also valid when $\mathfrak{m} = \mathfrak{e}$.

(4.3). We define

$$\omega = W_\infty \sum_{\chi \neq 1,\ \text{real}} L_k(0, \bar{\chi}) e_\chi$$

where $e_\chi \in \mathbb{C}[G]$ is the idempotent associated to χ, and $L_k(s, \bar{\chi})$ is the Artin L-function associated to the character $\bar{\chi}$. Here $\bar{\chi}$ is the inverse of χ. By [Prop.4.1 and Lem.4.2, Y1], we have $l^*(P') = \omega U'_0 = \omega e^+U'_0$. Using the analytic class number formula, we get

$$\text{(c)} \qquad (e^+U'_0 : l^*(P')) = \det \omega = \prod_{1 \neq \chi \in \widehat{G/J}} W_\infty L_k(0, \bar{\chi}) = W_\infty^r \frac{R(H)h(O_H)}{\kappa h}.$$

(4.4). To compute $[l^*(P') : l^*(C')]$ we write $\tilde{P} = (P')^\kappa = \mathbb{F}_q^* P_\mathfrak{m}^{s(J)} Q^{s(J_\mathfrak{e})}$ and $\tilde{C} = \tilde{P} \cap O_K^* = \mathbb{F}_q^* \bar{C}^{W_\infty}$. Regard $\tilde{P} \cap \ker l^*/\mathbb{F}_q^*$ as a subgroup of $\tilde{P}/\tilde{C}$. We have

$$[l^*(P') : l(C')] = [l^*(\tilde{P}) : l(\tilde{C})] = [\tilde{P}/\tilde{C} : \tilde{P} \cap \ker l^*/\mathbb{F}_q^*] = [\tilde{P}/\tilde{C} : \tilde{Q} \cap k].$$

Using the property [Prop.2.4, Y2] $\tilde{Q}/(\tilde{Q}\cap k)\tilde{E}\simeq G_1$, where $\tilde{Q}=Q^{s(J_\epsilon)}$ and $\tilde{E}=E^{s(J_\epsilon)}$, we can compute the last index. We have

$$\text{(d)}\qquad [l^*(P'):l(C')]=(q-1)^{-s}\Phi(\mathfrak{m})h$$

where s be the number of distinct prime divisors of $\mathfrak{m}$ and $\Phi(\mathfrak{m})=\#(\mathbb{A}/\mathfrak{m})$ is the Euler Φ-function. Notice that the result is also valid when $\mathfrak{m}=\mathfrak{e}$.

(4.5). At the last, we need calculate the lattice index $(e^+R_0:e^+U_0)$. To do this we need to decide some J–cohomologies. In Sinnott's case they are trivial $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$-modules. But in our case they are non-trivial $\mathrm{Pic}(\mathbb{A})$-modules. We can not decide them compleyely. This produces the condition in our conclulation.

Assume $(h,q-1)=1$ when $s\geq 3$. Then

$$\text{(e)}\qquad (e^+R_0:e^+U_0)=\begin{cases}(q-1)^e/\Phi(\mathfrak{m}), & \text{if } s=1\\ (q-1)^{e2^{s-2}}/\Phi(\mathfrak{m}), & \text{if } s\geq 2.\end{cases}$$

Clearly $(e^+R_0:e^+U_0)=1$ when $\mathfrak{m}=\mathfrak{e}$. By substituting (a)-(e) into (*), we get the indices at once.

References

[H] D.Hayes, *A brief introduction to Drinfeld modules, in* "The Arithmetic of Function Fields" (D.Goss, D.Hayes, M.Rosen, Ed.) (1992), W.de Gruyter, Berlin, 1–32.

[R] G.Robert, *Unites Elliptiques,*, Bull. Soc. Math. France **36** (1973), 5-77.

[S] W.Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. **108** (1978), 107–134.

[Y1] L.Yin, *Index-class number formulas over global function fields*, Compositio Math., in press.

[Y2] L.Yin, *On the index of cyclotomic units in characteristic p and its applications*, J. Number Theory, in press.