TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 341, Number 1, January 1994

CIRCULAR UNITS OF FUNCTION FIELDS

FREDERICK F. HARROP

ABSTRACT. A unit index-class number formula is proved for subfields of cyclotomic function fields in analogy with similar results for subfields of cyclotomic number fields.

Let m be a positive integer and let $\zeta_m = \exp(2\pi i/m)$. Let $K_m = \mathbb{Q}(\zeta_m)$ denote the mth cyclotomic field, and K_m^+ its maximal real subfield. The ring of integers in K_m (resp. K_m^+) is $\mathbb{Z}[\zeta_m]$ (resp. $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$). In [2] Sinnott showed that the index of circular units in the full group of units of $\mathbb{Q}(\zeta_m)$ equals the class number of $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ multiplied by a power of 2 which depends exclusively on the number of prime factors of m. Sinnott [3] subsequently generalized this result to an arbitrary abelian field.

There is a parallel setup for function fields of characteristic p. Let $\mathbb{F}_q$ be the finite field with q elements, let $R_T = \mathbb{F}_q[T]$ be the ring of polynomials over $\mathbb{F}_q$ (with T transcendental over $\mathbb{F}_q$), and let $\mathbb{F}_q(T)$ be the field of rational functions over $\mathbb{F}_q$. To each polynomial $M \in R_T$ one can associate an extension K_M, called the Mth *cyclotomic function field*, which enjoys properties analogous to those of the cyclotomic number field K_m. In particular, Galovich and Rosen [1] proved the analogue of Sinnott's theorem in this setting. The purpose of this paper is to extend this unit index-class number formula to an arbitrary subfield of K_M.

Let k be any subfield of the Mth cyclotomic function field (M monic), G the Galois group of k over $\mathbb{F}_q(T)$, k^+ the maximal subfield of k in which ∞ splits, $O_k(O_{k^+})$ the integral closure of $\mathbb{F}_q[T]$ in $k(k^+)$, and O_k^* the unit group of O_k. In §3, we define a subgroup C of O_k^*, which we call the circular units of k. Our main result is that C has finite index in O_k^*, and that this index may be written in the form

$$[O_k^* : C] = h(O_{k^+}) \cdot c_k^+,$$

where $h(O_{k^+})$ is the class number of O_{k^+}, and c_k^+ is a rational number whose definition does not involve $h(O_{k^+})$.

We now briefly describe the contents of the rest of this paper. In §1, we present the relevant definitions and facts in the function field setting. We also state the analytic class number formula. In §2, we review ordinary distributions on $\mathbb{F}_q(T)/R_T$, discuss an index notation, and obtain a preliminary result on the structure of a certain module. The circular units are introduced in §3 and

Received by the editors February 1, 1990 and, in revised form, November 27, 1991.
1991 *Mathematics Subject Classification.* Primary 11R58.

0002-9947/94 $1.00 + $.25 per page

the main result of this paper is proved. The last section is devoted to the determination of a factor of the index formula in special cases.

Since the arguments in the function field case closely follow those of the number field case, we will frequently refer the reader to Sinnott's paper [3] for the details.

We would like to thank the referee for several helpful suggestions.

1. Subfields of cyclotomic function fields

For the convenience of the reader, we begin this section with a rapid review of the theory of cyclotomic function fields. We also describe some basic notation used throughout this paper.

For any commutative ring R, let R^* denote the unit group of R. If R is a Dedekind domain, then $C(R)$ represents the ideal class group of R.

For any set X, $|X|$ will denote the cardinality of X.

For any two fields E and F such that $F \subseteq E$, the Galois group of E over F will be denoted $\mathrm{Gal}(E/F)$.

Let ∞ stand for the prime divisor of $\mathbb{F}_q(T)$ corresponding to $1/T$, and ord_∞ the associated normalized valuation.

We now describe the R_T-action on the algebraic closure $\mathbb{F}_q(T)^{\mathrm{ac}}$ of $\mathbb{F}_q(T)$. Let $u \in \mathbb{F}_q(T)^{\mathrm{ac}}$ and $M \in R_T$. Then set

$$u^M = M(\varphi + \mu)(u)$$

where the operators φ and μ on $\mathbb{F}_q(T)^{\mathrm{ac}}$ are defined by $\varphi(u) = u^q$ and $\mu(u) = Tu$. The action $u \mapsto u^M$ gives the additive group of $\mathbb{F}_q(T)^{\mathrm{ac}}$ the structure of an R_T-module. The following properties hold:

(1) If the degree of M is d, then $\Lambda_M = \{\lambda \mid \lambda^M = 0\}$ contains q^d elements. Moreover, Λ_M is a cyclic R_T-module, isomorphic to $R_T/(M)$, for every $M \neq 0$ in R_T.

(2) The field $K_M = \mathbb{F}_q(T)(\Lambda_M)$, the extension of $\mathbb{F}_q(T)$ in $\mathbb{F}_q(T)^{\mathrm{ac}}$ obtained by adding the points of Λ_M to $\mathbb{F}_q(T)$, is an abelian extension of $\mathbb{F}_q(T)$. The Galois group G_M of K_M over $\mathbb{F}_q(T)$ can be canonically identified with the multiplicative group $(R_T/(M))^*$ by the correspondence $A \mapsto \sigma_A$, where $\sigma_A(\lambda) = \lambda^A$ for each $\lambda \in \Lambda_M$. Let $\Phi(M)$ denote the order of $(R_T/(M))^*$.

(3) Let $J = \{\sigma_a \in G_M \mid a \in \mathbb{F}_q^*\}$, and let K_M^+ denote the fixed field of J. Then $[K_M : K_M^+] = q - 1$. K_M^+ is the maximal subfield of K_M in which P_∞ splits completely, and consequently is called the *maximal real subfield* of K_M.

(4) Let $M = P^r$, where P is a monic irreducible polynomial and r is a positive integer. In the extension K_M every prime divisor except (P) and ∞ is unramified. (P) is totally ramified in K_M.

(5) ∞ is tamely ramified in K_M. More precisely, ∞ splits into $\Phi(M)/(q-1)$ prime divisors in K_M, each of which has ramification index $q - 1$ and inertia degree 1.

(6) J is both the inertia group and decomposition group of each infinite prime of K_M, and so every infinite prime of K_M^+ ramifies fully in K_M and K_M^+ is the decomposition field of the infinite prime ∞ of $\mathbb{F}_q(T)$.

In the remainder of this paper we assume that M is a fixed monic polynomial. Let k be any subfield of K_M; without loss of generality, we may suppose that M is the monic polynomial of smallest possible degree satisfying this property. The Galois group $\mathrm{Gal}(K_M/k)$ is a subgroup of $\mathrm{Gal}(K_M/\mathbb{F}_q(T))$,

which can be considered as $(R_T/(M))^*$. So $\mathrm{Gal}(K_M/k)$ can be considered as a subgroup I of $(R_T/(M))^*$ and the Galois group $G = \mathrm{Gal}(k/\mathbb{F}_q(T))$ as the quotient group $(R_T/(M))^*/I$.

In analogy with the maximal real subfield of an abelian field, we call $k^+ = k \cap K_M^+$ the *maximal real subfield* of k; k^+ is the maximal subfield of k in which ∞ splits. It is easy to see that $G^+ = \mathrm{Gal}(k/k^+) \cong IJ/I \cong J/J \cap I$. Moreover, every infinite prime of k^+ totally ramifies in k. Finally, $J/J \cap I$ is the inertia group of any infinite prime of k.

The field $\mathbb{F}_q(T)_\infty$, the completion of $\mathbb{F}_q(T)$ at the infinite prime, plays the role that the field of real numbers plays classically.

Definition. Let $x \in \mathbb{F}_q(T)_\infty = \mathbb{F}_q((1/T))$. We call x *monic in* $\mathbb{F}_q(T)_\infty$ if $x/(1/T)^{\mathrm{ord}_\infty x} \equiv 1 \pmod{(1/T)}$.

The notion of "monic in $\mathbb{F}_q(T)_\infty$" is exactly analogous to that of "positive in $\mathbb{R}$".

Let O_k (resp. O_{k^+}) denote the integral closure of R_T in k (resp. k^+).

Proposition 1.1. *Let* $Q_0 = [O_k^* : O_{k^+}^*]$. *Then* Q_0 *is a positive divisor of* $q - 1$.

Proof. Let $\varepsilon \in O_k^*$. For each $\sigma_a \in J/J \cap I$, consider $u_a = \sigma_a(\varepsilon)/\varepsilon$. Obviously $u_a \in O_k^*$, and for any infinite prime $\mathfrak{P}$ of k, $\mathrm{ord}_{\mathfrak{P}}(\varepsilon) = \mathrm{ord}_{\mathfrak{P}}(\sigma_a(\varepsilon))$. This implies that u_a is a unit at every prime divisor of k, and so $u_a \in \mathbb{F}_q^*$. Therefore, if j is a generator of $J/J \cap I$, then $\varepsilon \mapsto \varepsilon^{1-j} = \varepsilon/j(\varepsilon)$ induces an inclusion $O_k^*/O_{k^+}^* \hookrightarrow \mathbb{F}_q^*$, so that Q_0 is a positive divisor of $q - 1$. This concludes the proof of the proposition.

Let $\mathscr{S}$ and S denote the set of infinite primes of k and k^+, respectively. Let $\mathscr{D}^0(\mathscr{S})$ (resp. $\mathscr{D}^0(S)$) be the group of k-divisors (resp. k^+-divisors) of degree zero generated by $\mathscr{S}$ (resp. S). Both of these groups are free abelian of rank $r = [k^+ : \mathbb{F}_q(T)] - 1$. Let $\mathscr{P}(\mathscr{S})$ (resp. $\mathscr{P}(S)$) denote the group of principal k-divisors (resp. k^+-divisors) divisible only by the primes in $\mathscr{S}$ (resp. S). We set $R(k) = [\mathscr{D}^0(\mathscr{S}) : \mathscr{P}(\mathscr{S})]$ and $R(k^+) = [\mathscr{D}^0(S) : \mathscr{P}(S)]$. The indices, which are both finite, are called the *regulators* of k and k^+. The following lemma exhibits the relation between the two regulators:

Lemma 1.2. $R(k) = R(k^+)|J/J \cap I|^r/Q_0$.

Proof. We split up the index $[\mathscr{D}^0(\mathscr{S}) : \mathscr{P}(S)]$ in two ways. First,

$$[\mathscr{D}^0(\mathscr{S}) : \mathscr{P}(S)] = [\mathscr{D}^0(\mathscr{S}) : \mathscr{P}(\mathscr{S})][\mathscr{P}(\mathscr{S}) : \mathscr{P}(S)] = R(k)Q_0.$$

Second,

$$[\mathscr{D}^0 : (\mathscr{S}) : \mathscr{P}(S)] = [\mathscr{D}^0(\mathscr{S}) : \mathscr{D}^0(S)][\mathscr{D}^0(S) : \mathscr{P}(S)] = |J/J \cap I|^r R(k^+)$$

as each infinite prime of k^+ totally ramifies in k. This completes the proof.

We close this section by stating the analytic class number formula. (See [1] for details.)

Let $C_{k^+}^0$ denote the group of k^+-divisor classes of degree zero and $h(k^+)$ its associated order. Then $h(k^+) = h(O_{k^+})R(k^+)$, where $h(O_{k^+})$ is the order of the ideal class group of O_{k^+}.

Let χ be a primitive Dirichlet character whose conductor, F_χ (a monic polynomial), divides M. Call χ a *real character* if $\chi(a) = 1$ for all $a \in \mathbb{F}_q^*$.

If A is a monic polynomial of degree less than $d_\chi = \deg(F_\chi)$, set $m(A) = (d_\chi - 1 - e)(q-1) - 1$ if A has degree e. Denoting the trivial character by χ_0 and recalling that $r = [k^+ : \mathbb{F}_q(T)] - 1$, we find that

$$h(k^+) = (q-1)^{-r} \prod_{\chi \neq \chi_0} \left(\sum_A m(A)\chi(A) \right),$$

where the product is taken over all real nontrivial characters of G and the sum is taken over the monics A of degree less than d_χ which are prime to F_χ.

2. Distributions

A function $u: \mathbb{F}_q(T)/R_T - \{0\} \to \mathbb{C}$ is called an *ordinary distribution on* $\mathbb{F}_q(T)/R_T$ if

$$\sum_{A \bmod N} u\left(\frac{r+A}{N}\right) = u(r)$$

for any polynomial $N \neq 0$ and any $r \in \mathbb{F}_q(T)/R_T$. The sum here is taken over a complete residue system modulo N.

The ordinary distribution that we will concentrate on was constructed by Galovich-Rosen [1]. Let $x = A/N \in k/R_T$, where $A, N \in R_T$ and $\deg(A) = e < d = \deg(N)$. Define $\varphi(x) = (q-1)(d-e-1) - 1$. Then φ is an ordinary distribution on $\mathbb{F}_q(T)/R_T$.

Let χ be a primitive Dirichlet character with conductor F_χ, a monic polynomial, such that $\chi \neq \chi_0$ and $\chi(a) = 1$ for all $a \in \mathbb{F}_q^*$. If F is a monic polynomial divisible by F_χ, let

$$\varphi_F(\chi) = \sum_{\substack{A \bmod F \\ (A,F)=1}} \chi(A)\varphi(A/F).$$

One can verify that

$$\varphi_F(\chi) = \varphi_{F_\chi}(\chi) \prod_{Q|F} (1 - \chi(Q))$$

where the product is taken over the monic prime polynomials which divide F.

Any ordinary distribution u on $\mathbb{F}_q(T)/R_T$ induces by restriction a distribution on $R_T(N) = (1/N)R_T/R_T$ for any polynomial $N \neq 0$. We abuse the notation and also label the restriction u. Recalling that the conductor of k is the monic polynomial M, we reformulate the analytic class number formula of the previous section as follows:

$$h(k^+) = (q-1)^{-r} \prod_{\substack{\chi \neq \chi_0 \\ \chi(IJ)=1}} \left(\sum_{A \in (R_T/M)^*} \varphi(A/M)\chi(A) \right).$$

Next we discuss an index notation used in this paper.

Let V be a finite-dimensional vector space over $\mathbb{Q}$, and let L be a $\mathbb{Z}$-submodule of V. Let V' be a $\mathbb{Q}$-subspace of V containing L. We call L a *lattice* in V' if L is free as a $\mathbb{Z}$-module, L spans V', and $\operatorname{rank}_{\mathbb{Z}} L = \dim_{\mathbb{Q}} V'$.

If L and L' are lattices in a $\mathbb{Q}$-vector space V', then the *index* $(L : L')$ is defined to be

$$(L : L') = |\det(A_1)|,$$

where A_1 is an automorphism of V' such that $A_1(L) = L'$. The index $(L : L')$ does not depend on the choice of A_1. Moreover, if $L' \subseteq L$, then $(L : L') = [L : L']$, the group index of L' in L (if $[L : L']$ is finite).

For any monic prime polynomial Q, T_Q will denote the inertia group of Q, and e_Q the idempotent in $\mathbb{Q}[G]$ associated with T_Q:

$$e_Q = S(T_Q)/|T_Q|;$$

here, for any subset X of G, $S(X)$ denotes the sum in $R = \mathbb{Z}[G]$ of the elements of X.

To any polynomial W prime to M, the Artin map associates an element of $G_M = G(K_M/\mathbb{F}_q(T))$ whose restriction to $G = G(k/\mathbb{F}_q(T))$ will be denoted (W, k). If χ is a multiplicative character from G to $\mathbb{C}^*$, we denote also by χ the corresponding primitive Dirichlet character; for W prime to M we have the formula $\chi(W) = \chi((W, k))$.

Let $\mathbb{C}[G]$ denote the group algebra of G over the field of complex numbers $\mathbb{C}$. Let $\chi: G \to \mathbb{C}^*$ be a character of G. Let $\rho_k^\chi: \mathbb{C}[G] \to \mathbb{C}$ denote the ring homomorphism

$$\rho_k^\chi\left(\sum_{\sigma\in G} c_\sigma \sigma\right) = \sum_{\sigma\in G} c_\sigma \chi(\sigma).$$

For any polynomial W, let $(W, k)^*$ be the unique element of $\mathbb{C}[G]$ such that

$$\rho_k^\chi((W, k)^*) = \overline{\chi}(W),$$

for all χ. Here $\overline{\chi}$ denotes the inverse of χ as a primitive Dirichlet character. Explicitly, we have

$$(W, k)^* = \sum_\chi \overline{\chi}(W) e_\chi,$$

where e_χ is the idempotent associated to χ in $\mathbb{C}[G]$:

$$e_\chi = \frac{1}{|G|} \sum_{\sigma\in G} \chi(\sigma)\sigma^{-1};$$

here $|G|$ denotes the order of G. The uniqueness of $(W, k)^*$ follows from the fact that the characters of G are linearly independent over $\mathbb{C}$. Since the set of primitive Dirichlet characters whose conductors are prime to W forms a subgroup of the group of all primitive Dirichlet characters, $(W, k)^*$ lies in $\mathbb{Q}[G]$, and $(W, k)^* = (W, k)^{-1}$ whenever W is prime to the conductor, M, of k. In particular, if $W = Q$ is a monic prime polynomial, then $(Q, k)^* = \delta_Q^{-1} e_Q$, where δ_Q is a Frobenius automorphism for Q in G; δ_Q is well-defined modulo T_Q.

For any monic polynomial N, let λ_N be a generator of Λ_N, K_N the cyclotomic function field $\mathbb{F}_q(T)(\Lambda_N)$, G_N the Galois group of K_N over $\mathbb{F}_q(T)$, and R_N the integral group ring of G_N. We identify $(R_T/(N))^*$ with G_N by the Artin map $W \to (W, K_N)$. Finally, define the subfield k_N of k by $k_N = k \cap K_N$.

The next result is the function field analogue of Sinnott's [3, Proposition 2.3]. But first we introduce some notation.

For each monic polynomial N, and each monic polynomial divisor f of N, let

$$\alpha_{f,N} = [K_N : k_N K_f] S(\mathrm{Gal}(k/k_f)) \prod_{Q|f} (1 - (Q, k)^*),$$

where the product is taken over monic prime polynomials Q that divide f. Let U be the R-module generated in $\mathbb{Q}[G]$ by these elements $\alpha_{f,N}$ (for all monic polynomials N, and all monic polynomial divisors f of N).

Let $\overline{M}$ denote the product of the monic prime polynomials dividing the monic polynomial M, the conductor of k. For any monic polynomial N which divides $\overline{M}$, we denote by T_N the compositum in $G = \mathrm{Gal}(k/\mathbb{F}_q(T))$ of the inertia groups T_Q of k, for each monic prime Q dividing N. Thus $T_1 = \{1\}$, $T_{\overline{M}} = G$.

The proof of Proposition 2.1 is so directly analogous to Sinnott's proof in the number field case that the reader should refer to [3, Proposition 2.3].

Proposition 2.1. *U is generated as an R-module by the elements*

$$S(T_N) \prod_{Q|\overline{M}/N} (1 - (Q, k)^*),$$

where N varies over the monic polynomials which divide $\overline{M}$.

As a $\mathbb{Z}$-module, U is free of rank $[k : \mathbb{F}_q(T)]$, and so is a lattice in $\mathbb{Q}[G]$.

3. Circular units

Let N be any monic polynomial in R_T of degree greater than zero, and let A be any polynomial not divisible by N. Let λ_N be a generator of Λ_N. Define the *circular numbers* D of k to be the subgroup of k^* generated by $\mathbb{F}_q^*$ and all elements $N_{K_N/k_N}(\lambda_N^A)$. Call $C = D \cap O_k^*$, the set of *circular units* of the cyclotomic function field k. Clearly C is a subgroup of O_k^*. We shall show that C is a subgroup of finite index in O_k^*.

Observe that $\alpha^{1-\sigma} = \alpha/\sigma(\alpha) \in C$, for any $\alpha \in D$ and any $\sigma \in G$; this is a consequence of the fact that $\lambda/\lambda^A \in C$ for any torsion point $\lambda \neq 0$, and any polynomial A prime to the order of λ.

Our first lemma gives two basic properties of D.

Lemma 3.1. *The group $\mathbb{F}_q^*$ is a subgroup of C, and the group $\mathbb{F}_q(T)^*$ of nonzero rational functions lies in D. Furthermore, if $\alpha \in D$, then:*

(a) *$\alpha \in \mathbb{F}_q^*$ if and only if $\alpha^{S(J)} = 1$.*

(b) *$\alpha \in C$ if and only if $N_{k/\mathbb{F}_q(T)}(\alpha) = a$ for some $a \in \mathbb{F}_q^*$.*

Proof. Since $\mathbb{F}_q^*$ is contained in D and O_k^*, it is a subgroup of C.

Because

$$Q = N_{k_Q/\mathbb{F}_q(T)}(N_{K_Q/k_Q}(\lambda_Q))$$

for any monic prime polynomial Q, it follows that $\mathbb{F}_q(T)^*$ is a subgroup of D.

To prove (a), let $\alpha \in \mathbb{F}_q^*$. Then $\alpha^{S(J)} = \alpha^{q-1} = 1$.

Suppose $\alpha^{S(J)} = 1$. For any $\lambda \in \Lambda_N^*$ and for any $\sigma_a \in J$, $(N_{K_N/k_N}(\lambda))^{\sigma_a} = N_{K_N/k_N}(\lambda^{\sigma_a}) = N_{K_N/k_N}(a\lambda)$, which implies that

$$N_{K_N/k_N}(\lambda)^{S(J)} = \left(\prod_{a\in\mathbb{F}_q^*} a\right)^{[K_N : k_N]} (N_{K_N/k_N}(\lambda))^{q-1} = (-1)^{[K_N : k_N]}(N_{K_N/k_N}(\lambda))^{q-1}.$$

Thus, for $\alpha \in D$, $\alpha^{S(J)} = \pm\alpha^{q-1}$. If $\alpha^{S(J)} = 1$, then $\alpha^{q-1} = \pm 1$. As $\mathbb{F}_q^*$ is the set of roots of unity of k^*, it follows that $\alpha \in \mathbb{F}_q^*$.

To prove (b), let $\alpha \in C$. Then $N_{k/\mathbb{F}_q(T)}(\alpha) \in R_T^* = \mathbb{F}_q^*$.

If $\alpha \in D$ and $N_{k/\mathbb{F}_q(T)}(\alpha) = a$ for some $a \in \mathbb{F}_q^*$, then since $\alpha^{1-\sigma} \in C$ for any $\sigma \in G$,

$$N_{k/\mathbb{F}_q(T)}(\alpha) = \alpha^{S(G)} \equiv \alpha^{|G|} \pmod{C}.$$

Hence if $N_{k/\mathbb{F}_q(T)}(\alpha)$ is a unit, so is $\alpha^{|G|}$, and thus so is α.

We next determine $D^{S(G)}$. The statement and proof in [3, §4] carry over verbatim.

Lemma 3.2. *$D^{S(G)}$ is generated by $Q^{[k : k_{Q^e}]}$ with Q varying over the monic primes in R_T. Here Q^e denotes the highest power of Q dividing M; of course, e depends on Q.*

From this time on we fix an infinite prime $\mathfrak{P}$ of k. Define $l: k^* \to \mathbb{Q}[G]$ by

$$l(\alpha) = \sum_{\sigma\in G} \operatorname{ord}_{\sigma^{-1}(\mathfrak{P})}(\alpha)\sigma^{-1}.$$

The map l is clearly a group homomorphism.

For any monic prime polynomial Q, let $d_Q = \deg(Q)$. We now scrutinize the kernel of l.

Proposition 3.3.

(a) $\ker(l) \cap C = \mathbb{F}_q^* = \ker(l) \cap O_k^*$

(b) $\ker(l) \cap D = \mathscr{N}$, *where*

$$\mathscr{N} = \mathbb{F}_q^* \times \left\{ \prod_{\substack{Q \text{ monic} \\ \text{prime}}} Q^{n_Q} \mid n_Q \in \mathbb{Z},\ n_Q = 0 \text{ for all but finitely many } Q, \right.$$
$$\left. \text{and } \operatorname{ord}_\infty\left(\prod_Q Q^{n_Q}\right) = -\sum_Q d_Q n_Q = 0 \right\}^{1/(q-1)}.$$

Proof. (a) Let $\alpha \in \ker(l) \cap C$. Since $l(\alpha) = 0$, α has no zeros or poles in $\mathscr{S}$, the set of infinite primes of k. Since $\alpha \in C \subseteq O_k^*$, α has no zeros or poles in O_k. Thus $\alpha \in \mathbb{F}_q^*$. The converse is obvious. Likewise $\ker(l) \cap O_k^* = \mathbb{F}_q^*$.

(b) It is easy to see that $\mathscr{N} \subseteq D \cap \ker(l)$. For the reverse inclusion, let $\alpha \in D \cap \ker(l)$. Then for all $\sigma \in G$, $\alpha^{1-\sigma} \in C$ and $l(\alpha^{1-\sigma}) = 0$. Hence $\alpha^{1-\sigma} \in \mathbb{F}_q^*$ for all $\sigma \in G$. Consequently $\alpha^{q-1} = g(T) \in \mathbb{F}_q(T)^*$. Since $l(\alpha) = 0$,

$$\operatorname{ord}_\infty(g(T)) = \frac{1}{|J/J\cap I|} \operatorname{ord}_{\sigma^{-1}(\mathfrak{P})}(g(T)) = 0.$$

This completes the proof.

Proposition 3.3(a) implies that

$$O_k^*/C \cong l(O_k^*)/l(C).$$

We will prove that $(l(O^*)_k : l(C)) = h(O_{k+}^*)\cdot c_k^+$, where c_k^+ is a rational number whose definition does not involve $h(O_{k+}^*)$.

Let $T_1 = l(D)$ and $T_0 = \{x \in T_1 \mid S(G)x = 0\}$. Clearly $T_0 \supseteq l(C)$ (Lemma 3.1(b)). In the number field case, Sinnott [3, Lemma 4.2] shows that $T_0 = l(C)$. In the function field case, however, the inclusion is proper. It will follow from Proposition 3.6 that the index $[T_0 : l(C)]$ is finite.

For any $\mathbb{Z}[G]$-module A, we denote by A_0 the set of elements of A annihilated by $S(G)$, and by A^G the set of elements fixed by G. Also for any set $X = \{\dots, x, \dots\}$, $\langle \dots, x, \dots \rangle$ will denote the abelian group generated by the elements of X.

For any character χ of G let

$$e_\chi = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1}$$

be the idempotent in $\mathbb{C}[G]$ associated to χ. In particular, the idempotent corresponding to the trivial character is $e_1 = S(G)/|G|$.

Call k *imaginary* if $J \cap I = \{1\}$, *real* if $J \cap I = J$.

Lemma 3.4. *$T_0 = T_1 \cap (1-e_1)T_1$. T_0 has finite index in T_1; in fact, $[(1-e_1)T_1 : T_0] = [I_1 : I_2][T_1^G : l(\mathbb{F}_q(T)^*)]^{-1}$, where I_1 and I_2 are the subgroups of $\mathbb{Q}$ given by*

$$I_1 = \langle \dots, d_P/[k_{P^e} : \mathbb{F}_q(T)], \dots \rangle I_2 = \mathbb{Z}.$$

Here P ranges over all monic prime polynomials, and, for each P, P^e denotes the largest power of P dividing the conductor M of k. Finally, $[T_1^G : l(\mathbb{F}_q(T)^*)] = |(D/\mathbb{F}_q(T)^*)_{q-1}|$, where $(D/\mathbb{F}_q(T)^*)_{q-1}$ denotes the group of elements of $D/\mathbb{F}_q(T)^*$ whose order divides $q-1$. In particular, if k is real, then $[T_1^G : l(\mathbb{F}_q(T)^*)] = 1$.

Proof. The first assertion follows immediately from the definitions.

Next we show that the index $[(1-e_1)T_1 : T_0]$ is defined. Since $T_0 = T_1 \cap (1-e_1)T_1$, we have

$$(1-e_1)T_1/T_0 \cong ((1-e_1)T_1 + T_1)/T_1 \cong (e_1T_1 + T_1)/T_1 \cong e_1T_1/T_1^G$$

since $(1-e_1)T_1 + T_1 = e_1T_1 + T_1$ and $e_1T_1 \cap T_1 = T_1^G$.

By Lemma 3.2 we have

$$\begin{aligned} e_1T_1 &= \frac{S(G)}{|G|}l(D) = \frac{1}{|G|}l(D^{S(G)}) = \sum_P \frac{1}{[k_{P^e} : \mathbb{F}_q(T)]}l(P)\mathbb{Z} \\ &= \left|\frac{J}{J\cap I}\right|\sum_P\left(\frac{d_P}{[k_{P^e} : \mathbb{F}_q(T)]}\right)\mathbb{Z}S(G) = \left|\frac{J}{J\cap I}\right| I_1S(G), \end{aligned}$$

where the summation is taken over all monic prime polynomials P, and for each such polynomial, d_P denotes its degree.

Next we examine the group T_1^G. First we remark that $l(\mathbb{F}_q(T)^*) \subseteq T_1^G$, since $\mathbb{F}_q(T)^* \subseteq D$ by Lemma 3.1. We have

$$l(\mathbb{F}_q(T)^*) = \sum_P l(P)\mathbb{Z} = \left|\frac{J}{J \cap I}\right| \left(\sum_P d_P \mathbb{Z}\right) S(G) = \left|\frac{J}{J \cap I}\right| (\mathbb{Z}S(G))$$

since there are monic irreducibles of every degree. Hence $e_1 T_1 / l(\mathbb{F}_q(T)^*) \cong I_1/I_2$ and so $[(1-e_1)T_1 : T_0] = [I_1 : I_2][T_1^G : l(\mathbb{F}_q(T)^*)]^{-1}$.

As $I_1/I_2 = I_1/\mathbb{Z} \subseteq \frac{1}{[k:\mathbb{F}_q(T)]}\mathbb{Z}/\mathbb{Z}$, $[I_1 : I_2]$ is finite. Consequently, since $T_1^G/l(\mathbb{F}_q(T)^*)$ is a subgroup of $e_1 T_1/l(\mathbb{F}_q(T)^*) \cong I_1/I_2$, $[T_1^G : l(\mathbb{F}_q(T)^*)]$ is finite. Therefore, $[(1-e_1)T_1 : T_0]$ is finite.

We next prove that $[T_1^G : l(\mathbb{F}_q(T)^*)] = |(D/\mathbb{F}_q(T)^*)_{q-1}|$. Let α be an element of D such that $l(\alpha)$ lies in T_1^G. Then $(\sigma-1)l(\alpha) = l(\alpha^{\sigma-1}) = 0$ for all $\sigma \in G$. By Proposition 3.3(a), $\alpha^{\sigma-1}$ is in $\mathbb{F}_q^*$ for all σ in G. Now $\alpha^{\sigma-1}$ is in $\mathbb{F}_q^*$ for all σ in G if and only if $(\alpha^{\sigma-1})^{S(J)} = 1$ for all σ in G by Lemma 3.1(a); this is equivalent to the assertion that $\alpha^{S(J)}$ lies in $\mathbb{F}_q(T)^*$; this, in turn, is equivalent to the assertion that α^{q-1} lies in $\mathbb{F}_q(T)^*$. Conversely, if α is an element of D such that α^{q-1} lies in $\mathbb{F}_q(T)^*$, it is clear that $l(\alpha)$ lies in T_1^G.

Finally, suppose that k is real and let $\alpha \in D$ be such that $\alpha^{q-1} \in \mathbb{F}_q(T)^*$. Let $E = \mathbb{F}_q(T)$. Then $E(\alpha)/E$ is a Kummer extension of E and its Galois group is clearly given by elements in J. Since $E(\alpha) \subseteq k$, and k is real, it follows that the Galois group of $E(\alpha)/E$ is trivial, and so $\alpha \in E^*$ as asserted. This concludes the proof of Lemma 3.4.

In order to investigate $[T_0 : l(C)]$ we need necessary and sufficient conditions for when a given $x \in D$ has the property that (a) $l(x) \in T_0$; (b) $l(x) \in l(C)$. These conditions are provided by the next lemma. But first we need to simplify $l(x) \pmod{l(C)}$ for any $x \in D$.

Write the conductor, M, of k as $M = \prod_{i=1}^g Q_i^{e_i}$, where $Q_1, \ldots, Q_g$ are distinct monic primes and $e_i \geq 1$. Write $d_i = \deg(Q_i)$. Let λ_i be a generator of $\Lambda_{Q^{e_i}}$, $1 \leq i \leq g$.

Let

$$x = \prod_{\substack{N \text{ monic} \\ N \neq 1}} \prod_{A \nmid N} (N_{K_N/k_N}(\lambda_N^A))^{a(\lambda_N^A)}$$

be any element of D. If λ_N^A is a generator of Λ_L as an R_T-module where L is not a prime power, then λ_N^A is a unit of O_L (see [1, Corollary 1.9]), so λ_N^A is a unit of O_N, hence $N_{K_N/k_N}(\lambda_N^A)$ is a unit of k_N, hence a unit of k, and, consequently, $N_{K_N/k_N}(\lambda_N^A) \in C$. If λ_N^A is a generator of $\Lambda_{Q^{e_Q}}$ as an R_T-module where Q is a monic prime polynomial which does not divide M, then $K_{Q^{e_Q}} = \mathbb{F}_q(T)(\lambda_N^A)$, $k \cap K_{Q^{e_Q}} = \mathbb{F}_q(T)$, and

$$\begin{aligned} N_{K_N/k_N}(\lambda_N^A) &= N_{k_N K_{Q^{e_Q}}/k_N}(N_{K_N/k_N K_{Q^{e_Q}}}(\lambda_N^A)) = N_{k_N K_{Q^{e_Q}}/k_N}(\lambda_N^A)^{[K_N : k_N K_{Q^{e_Q}}]} \\ &= N_{K_{Q^{e_Q}}/\mathbb{F}_q(T)}(\lambda_N^A)^{[K_N : k_N K_{Q^{e_Q}}]} = (\pm Q)^{[K_N : k_N K_{Q^{e_Q}}]}. \end{aligned}$$

If λ_N^A is a generator of $\Lambda_{Q_i^{b_i}}$, where $b_i \geq e_i$, then $k_{Q_i^{b_i}} = k_{Q_i^{e_i}}$ and so

$$N_{K_N/k_N}(\lambda_N^A) = N_{kK_{Q_i^{b_i}}/k_N}(N_{K_N/kK_{Q_i^{b_i}}}(\lambda_N^A)) = N_{K_{Q_i^{b_i}}/k_{Q_i^{e_i}}}(\lambda_N^A)^{[K_N : k_N K_{Q_i^{b_i}}]}$$
$$= N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(N_{K_{Q_i^{b_i}}/k_{Q_i^{e_i}}}(\lambda_N^A)^{[K_N : k_N K_{Q_i^{b_i}}]}) = N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i^\tau)^{[K_N : k_N K_{Q_i^{b_i}}]}$$

where τ is an element of $\mathrm{Gal}(K_{Q_i^{e_i}}/\mathbb{F}_q(T))$. Hence

$$N_{K_N/k_N}(\lambda_N^A) = ((N_{Q_i^{e_i}}/k_{Q_i^{e_i}}(\lambda_i))^\sigma)^{[K_N : k_N K_{Q_i^{b_i}}]}$$

where σ is an element of $G = \mathrm{Gal}(k/\mathbb{F}_q(T))$. Finally, if λ_N^A is a generator of $\Lambda_{Q_i^{c_i}}$, where $1 \leq c_i < e_i$, then $k_{Q_i^{c_i}} \subseteq k_{Q_i^{e_i}}$ and so

$$N_{K_N/k_N}(\lambda_N^A) = N_{k_N K_{Q_i^{c_i}}/k_N}(N_{K_N/k_N K_{Q_i^{c_i}}}(\lambda_N^A)) = N_{k_N K_{Q_i^{c_i}}/k_N}(\lambda_N^A)^{[K_N : k_N K_{Q_i^{c_i}}]}$$
$$= N_{K_{Q_i^{c_i}}/k_{Q_i^{c_i}}}(\lambda_N^A)^{[K_N : k_N K_{Q_i^{c_i}}]} = N_{K_{Q_i^{c_i}}/k_{Q_i^{c_i}}}(N_{K_{Q_i^{e_i}}/K_{Q_i^{c_i}}}(\lambda_i^\gamma))^{[K_N : k_N K_{Q_i^{c_i}}]}$$

for some $\gamma \in \mathrm{Gal}(K_{Q_i^{e_i}}/\mathbb{F}_q(T))$. Hence

$$N_{K_N/k_N}(\lambda_N^A) = N_{K_{Q_i^{e_i}}/k_{Q_i^{c_i}}}(\lambda_i^\gamma)^{[K_N : k_N K_{Q_i^{c_i}}]} = N_{k_{Q_i^{e_i}}/k_{Q_i^{c_i}}}(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i^\gamma))^{[K_N : k_N K_{Q_i^{c_i}}]}$$
$$= N_{k_{Q_i^{e_i}}/k_{Q_i^{c_i}}}(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i)^\tau)^{[K_N : k_N K_{Q_i^{c_i}}]}$$

for some $\tau \in G = \mathrm{Gal}(k/\mathbb{F}_q(T))$. Thus

$$N_{K_N/k_N}(\lambda_N^A) = (N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i))^{\left(\sum_{\sigma\in G} b(\sigma)\sigma\right)[K_N : k_N K_{Q_i^{e_i}}]}$$

with $b(\sigma) \in \mathbb{Z}$. Therefore, recalling that $\sigma\alpha \equiv \alpha(C)$ for $\alpha \in D$,

$$l(x) \equiv \sum_{i=1}^{g} n_i l(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i)) + \sum_{\substack{Q \nmid M \\ Q \text{ monic prime}}} n_Q l(Q) \pmod{l(C)}$$

for some integers n_i, $1 \leq i \leq g$, and n_Q, $Q \nmid M$, Q a monic prime polynomial. Of course, almost all of the n_Q are zero.

Recall that $d_i = \deg(Q_i)$ if Q_i is a monic prime polynomial which divides M, the conductor of k. Likewise, let $d_Q = \deg(Q)$ if Q is a monic prime polynomial which does not divide M.

Lemma 3.5. *Suppose*

$$l(x) \equiv \sum_{i=1}^{g} n_i l(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i)) + \sum_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} n_Q l(Q) \pmod{l(C)},$$

where each n_i, n_Q is in $\mathbb{Z}$.

(a) $l(x) \in T_0$ *if and only if*

$$\sum_{i=1}^{g} \frac{n_i d_i}{[k_{Q_i^{e_i}} : \mathbb{F}_q(T)]} + \sum_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} n_Q d_Q = 0$$

(b) $l(x) \in l(C)$ *if and only if*

$$[k_{Q_i^{e_i}} : \mathbb{F}_q(T)] \mid (q-1)n_i$$

for $i = 1, \ldots, g$ *and the* n_i, n_Q *satisfy the linear equation in* (a).

Proof. (a) Since $l(C) \subseteq T_0$,

$$S(G)l(x) = \sum_{i=1}^{g} n_i S(G) l(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i)) + \sum_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} n_Q S(G) l(Q).$$

But $(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i))^{S(G)} = (\pm Q_i)^{[k : k_{Q_i^{e_i}}]}$ for $i = 1, \ldots, g$, and $Q^{S(G)} = Q^{[k : \mathbb{F}_q(T)]}$ for $Q \nmid M$, Q a monic prime. Hence $S(G)l(x) = 0$ if and only if $l(f) = 0$, where

$$f = \prod_{i=1}^{g} Q_i^{n_i[k : k_{Q_i^{e_i}}]} \prod_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} Q^{n_Q[k : \mathbb{F}_q(T)]}.$$

However, $(1/|J/J \cap I|)l(f) = (-\deg(f))S(G)$. Consequently $S(G)l(x) = 0$ if and only if $\deg(f) = 0$. This establishes (a).

(b) There exists $c \in C$ such that

$$l(x) = l\left(\prod_{i=1}^{g} \left(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i) \right)^{n_i} \cdot \prod_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} Q^{n_Q} \right) = l(c)$$

if and only if

$$\prod_{i=1}^{g} (N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i))^{n_i} \cdot \prod_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} Q^{n_Q} = cy$$

for some $y \in \mathcal{N}$. From the definition of $\mathcal{N}$,

$$y = a \left(\prod_{i=1}^{g} Q_i^{a_i} \cdot \prod_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} Q^{a_Q} \right)^{1/(q-1)}$$

where $a \in \mathbb{F}_q^*$ and $a_i, a_Q \in \mathbb{Z}$.

Let P be any monic prime polynomial and $\mathfrak{P}$ any prime of k lying over P. We have

$$\operatorname{ord}_{\mathfrak{P}}\left(\prod_{i=1}^{g}\left(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i)\right)^{n_i}\cdot\prod_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}Q^{n_Q}\right)=\operatorname{ord}_{\mathfrak{P}}(cy)=\operatorname{ord}_{\mathfrak{P}}(y).$$

It is easily verified that

$$n_P=a_P[k_{P^e}:\mathbb{F}_q(T)]/(q-1)$$

where, of course, P^e is the largest power of P dividing M. In particular, if $P=Q_i$ for some i, $1\le i\le g$, then

$$n_i=a_i[k_{Q_i^{e_i}}:\mathbb{F}_q(T)]/(q-1),$$

and so $[k_{Q_i^{e_i}}:\mathbb{F}_q(T)]\mid(q-1)n_i$.

Conversely, suppose that $[k_{Q_i^{e_i}}:\mathbb{F}_q(T)]a_i=(q-1)n_i$, where $a_i\in\mathbb{Z}$ for $i=1,\dots,g$, and suppose the n_i and n_Q satisfy the linear equation in (a). If Q is a prime polynomial such that $Q\nmid M$, let $a_Q=(q-1)n_Q$. Then

$$\begin{aligned}l(x)&\equiv\sum_{i=1}^{g}n_i l(N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i))+\sum_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}n_Q l(Q)\\&\equiv\sum_{i=1}^{g}\left(\frac{a_i}{q-1}\right)l((N_{K_{Q_i^{e_i}}/k_{Q_i^{e_i}}}(\lambda_i))^{[k_{Q_i^{e_i}}:\mathbb{F}_q(T)]})+\sum_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}\left(\frac{a_Q}{q-1}\right)l(Q)\\&\equiv\sum_{i=1}^{g}l(Q_i^{a_i/(q-1)})+\sum_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}l(Q^{a_Q/(q-1)})\\&\equiv l\left(\prod_{i=1}^{g}Q_i^{a_i/(q-1)}\cdot\prod_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}Q^{q_Q/(q-1)}\right)\pmod{l(C)}.\end{aligned}$$

Also,

$$\begin{aligned}\operatorname{ord}_\infty\left(\prod_{i=1}^{g}Q_i^{a_i}\cdot\prod_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}Q^{a_Q}\right)&=-\sum_{i=1}^{g}a_i d_i-\sum_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}a_Q d_Q\\&=-\sum_{i=1}^{g}\frac{(q-1)n_i d_i}{[k_{Q_i^{e_i}}:\mathbb{F}_q(T)]}-\sum_{\substack{Q\nmid M\\ Q \text{ monic}\\ \text{prime}}}(q-1)n_Q d_Q=0.\end{aligned}$$

Therefore

$$\prod_{i=1}^{g} Q_i^{a_i/(q-1)} \cdot \prod_{\substack{Q \nmid M \\ Q \text{ monic} \\ \text{prime}}} Q^{a_Q(q-1)} \in \mathcal{N}$$

which implies that $l(x) \in l(C)$. This completes the proof of the lemma.

Let $\mathbb{R}^\infty$ denote the set of all sequences $\beta = (b_0, b_1, b_2, \dots, b_n, \dots)$, where the b_i's are elements of the set of real numbers $\mathbb{R}$ and all but finitely many of them are zero. Equipped with the obvious operations of addition and scalar multiplication, $\mathbb{R}^\infty$ becomes a vector space over $\mathbb{R}$.

Let L_1, L_2, and L_3 be lattices in $\mathbb{R}^\infty$ which are defined as follows:

$$L_1 = \left\{ (\dots, y_P, \dots) \mid y_P = \frac{d_P}{[k_{Q_P^{e_P}} : \mathbb{F}_q(T)]} x_P \quad \text{where } x_P \in \mathbb{Z} \right\},$$

$$L_2 = \{ (\dots, y_P, \dots) \mid y_P = d_P x_P \quad \text{where } x_P \in \mathbb{Z} \},$$

$$L_3 = \left\{ (\dots, y_P, \dots) \mid y_P = \frac{(q-1)d_P}{[k_{Q_P^{e_P}} : \mathbb{F}_q(T)]} x_P \quad \text{where } x_P \in \mathbb{Z} \right\}.$$

Here P runs through the monic prime polynomials of $R_T = \mathbb{F}_q[T]$. Obviously, $L_2 \subseteq L_1$ and $L_3 \subseteq L_1$. Define $\psi: L_1 \to \mathbb{R}$ by $\psi(\dots, y_P, \dots) = \sum y_P$.

Recall that the conductor $M = \prod_{i=1}^{g} Q_i^{e_i}$.

Proposition 3.6.

$$[(1-e_1)T_1 : l(C)] = \prod_{i=1}^{g} [k_{Q_i^{e_i}} : \mathbb{F}_q(T)] \cdot \left| \left(\frac{D}{\mathbb{F}_q(T)^*} \right)_{q-1} \right|^{-1} \cdot [L_1 : L_2 + L_3]^{-1} \cdot [\psi(L_2) : \psi(L_2 \cap L_3)]^{-1} \cdot [\psi(L_1) : \psi(L_3)].$$

In particular, the index $[T_0 : l(C)]$ *is defined.*

Proof. Notice that $\psi(L_1)/\psi(L_2) = I_1/I_2 \cong e_1 T_1 / l(\mathbb{F}_q(T)^*)$, where I_1 and I_2 are the subgroups of $\mathbb{R}$ defined in Lemma 3.4. Let K_3 and $K_{2,3}$ be the kernel of ψ on L_3 and $L_2 \cap L_3$, respectively. It follows from Lemma 3.5 that $K_3 \cong T_0$ and $K_{2,3} \cong l(C)$. Hence

$$\begin{aligned} [L_3 : L_2 \cap L_3] &= [\psi(L_3) : \psi(L_2 \cap L_3)] \cdot [K_3 : K_{2,3}] \\ &= [\psi(L_3) : \psi(L_2 \cap L_3)] \cdot [T_0 : l(C)]. \end{aligned}$$

Since $L_3/L_2 \cap L_3 \cong L_2 + L_3/L_2$, we have

$$[L_2 + L_3 : L_2] = [\psi(L_3) : \psi(L_2 \cap L_3)] \cdot [T_0 : l(C)].$$

Multiplying both sides by $[L_1 : L_2 + L_3]$, we obtain

$$[L_1 : L_2] = [L_1 : L_2 + L_3] \cdot [\psi(L_3) : \psi(L_2 \cap L_3)] \cdot [T_0 : L(C)],$$

hence

$$\begin{aligned}\prod_{i=1}^{g}[k_{Q_i^{e_i}} : \mathbb{F}_q(T)] &= [L_1 : L_2 + L_3] \cdot [\psi(L_3) : \psi(L_2 \cap L_3)] \cdot [T_0 : l(C)] \\ &= [L_1 : L_2 + L_3] \cdot [\psi(L_1) : \psi(L_3)] \cdot [\psi(L_3) : \psi(L_2 \cap L_3)] \\ &\quad \cdot [T_0 : l(C)] \cdot [\psi(L_1) : \psi(L_3)]^{-1} \\ &= [L_1 : L_2 + L_3][\psi(L_1) : \psi(L_2)] \cdot [\psi(L_2) : \psi(L_2 \cap L_3)] \\ &\quad \cdot [T_0 : l(C)] \cdot [\psi(L_1) : \psi(L_3)]^{-1} \\ &= [L_1 : L_2 + L_3] \cdot [I_1 : I_2] \cdot [\psi(L_2) : \psi(L_2 \cap L_3)] \\ &\quad \cdot [T_0 : l(C)] \cdot [\psi(L_1) : \psi(L_3)]^{-1} \\ &= [L_1 : L_2 + L_3] \cdot [(1 - e_1)T_1 : T_0] \cdot [T_1^G : l(\mathbb{F}_q(T)^*)] \\ &\quad \cdot [T_0 : l(C)] \cdot [\psi(L_2) : \psi(L_2 \cap L_3)] \cdot [\psi(L_1) : \psi(L_3)]^{-1} \\ &= [L_1 : L_2 + L_3] \cdot [(1 - e_1)T_1 : l(C)] \cdot \left| \left(\frac{D}{\mathbb{F}_q(T)^*} \right)_{q-1} \right| \\ &\quad \cdot [\psi(L_2) : \psi(L_2 \cap L_3)] \cdot [\psi(L_1) : \psi(L_3)]^{-1}.\end{aligned}$$

Solving for $[(1 - e_1)T_1 : l(C)]$, we obtain the statement of the proposition.

Our Proposition 3.7 and Corollary 3.8 are the function field analogues of Sinnott's [3, Proposition 4.2 and Corollary]. The proofs carry over verbatim. First, however, we need the following remark.

For any monic polynomial $N \neq 1$, and any infinite prime $\mathfrak{P}_N$ of $K_N = \mathbb{F}_q(T)(\Lambda_N)$, we may choose $\lambda_N \in \Lambda_N$ such that $\mathrm{ord}_{\mathfrak{P}_N}(\lambda_N) = (\deg(N) - 1) \cdot (q - 1) - 1$. (The existence of such a λ_N is guaranteed by [1, Proposition 1.10].) The restriction of the distribution φ introduced in §2 to $(1/N)R_T/R_T$ is such that $\varphi(A/N) = m(A) = \mathrm{ord}_{\mathfrak{P}_N}(\lambda_N^A)$ whenever N does not divide A. (See [1, Lemma 1.6].)

Proposition 3.7. *Let $N \neq 1$ be any monic polynomial, and let D be a monic divisor of N with $D \neq N$. Let λ_N be chosen as in the preceding paragraph. Let $f = N/D$. Then*

$$(1 - e_1)l(N_{K_N/k_N}(\lambda_N^D)) = \omega'[K_N : k_N K_f]S(\mathrm{Gal}(k/k_f)) \cdot \prod_{Q|f}(1 - (Q, k)^*)$$

where the product is taken over all monic prime polynomials Q which divide f. Here

$$\omega' = \sum_{\chi \neq \chi_0} \varphi_{F_\chi}(\overline{\chi}) e_\chi,$$

where the sum is over the nontrivial real characters χ of G.

Corollary 3.8. $(1 - e_1)T_1 = \omega' U$.

We now state our main result. Recall that $R = \mathbb{Z}[G]$.

Theorem 3.9. *The index* $[O_k^* : C]$ *is defined. In fact,*

$$[O_k^* : C] = h(O_{k^+}) \cdot Q_0 \cdot |J \cap I|^{2r} \cdot \left| \left(\frac{D}{\mathbb{F}_q(T)^*} \right)_{q-1} \right|^{-1}$$
$$\cdot \frac{\prod_{i=1}^{g} [k_{Q_i^{e_i}} : \mathbb{F}_q(T)]}{[k : \mathbb{F}_q(T)]} \cdot (e^+R : e^+U)$$
$$\cdot [L_1 : L_2 + L_3]^{-1} \cdot [\psi(L_2) : \psi(L_2 \cap L_3)]^{-1} \cdot [\psi(L_1) : \psi(L_3)].$$

Proof. The mapping l sends O_k^* and C to subgroups of the $\mathbb{Q}$-vector space $X = (1 - e_1)e^+\mathbb{Q}[G]$. X has dimension $r = [k^+ : \mathbb{F}_q(T)] - 1$. By Proposition 3.3(a), we have

$$O_k^*/C \cong l(O_k^*)/l(C).$$

Now

$$\omega' U = \omega' e^+ U_0,$$

since $\omega' e^+ = \omega'$ and $U = U_0 + U^G$ [3, proof of Proposition 2.2]. We write formally

$$(l(O_k^*) : l(C)) = (l(O_k^*) : e^+R_0)(e^+R_0 : e^+U_0)(e^+U_0 : (1-e_1)T_1)((1-e_1)T_1 : l(C)).$$

We will show that each of the groups appearing on the right is a lattice in X. This will establish the finiteness of the index $[O_k^* : C]$.

(1) $(l(O_k^*) : e^+R_0)$. Dirichlet's unit theorem implies that $l(O_k^*)$ is a lattice in X, and e^+R_0 is also a lattice in X. In fact, the r elements $e^+(\sigma - 1)$, where $\sigma \in G^+ = \mathrm{Gal}(k^+/\mathbb{F}_q(T))$ and $\sigma \neq 1$, form a $\mathbb{Z}$-basis for e^+R_0. Let $\eta_1, \ldots, \eta_r$ be a set of fundamental units of O_k^*. For any $\varepsilon \in O_k^*$, $\sum_{\sigma \in G} \mathrm{ord}_{\sigma^{-1}(\mathfrak{P})}(\varepsilon) = 0$, where $\mathfrak{P}$ is a fixed infinite prime of k. Therefore,

$$l(\eta_i) = \sum_{\substack{\sigma \in G \\ \sigma \neq 1}} \mathrm{ord}_{\sigma^{-1}(\mathfrak{P})}(\eta_i)(\sigma^{-1} - 1).$$

Since $IJ/I \cong J/J \cap I$ is the intertia group of any infinite prime of k,

$$\mathrm{ord}_{\sigma^{-1}(\mathfrak{P})}(\eta_i) = \mathrm{ord}_{\tau^{-1}(\mathfrak{P})}(\eta_i) \quad \text{if } \tau = \gamma\sigma$$

for some $\gamma \in J/J \cap I$. Thus we have

$$l(\eta_i) = \left| \frac{J}{J \cap I} \right| \sum_{\substack{\sigma \in G^+ \\ \sigma \neq 1}} \mathrm{ord}_{\sigma^{-1}(\mathfrak{P})}(\eta_i) e^+(\sigma^{-1} - 1).$$

An easy calculation shows that

$$\left| \det_{\substack{1 \neq \sigma \in G^+ \\ i = 1, \ldots, r}} (\mathrm{ord}_{\sigma^{-1}(\mathfrak{P})}(\eta_i)) \right| = R(k) = |R(k^+)| J/J \cap I|^r / Q_0$$

where Q_0 is the "unit index" $[O_k^* : O_{k^+}^*]$. The last equality follows from Lemma 1.2. Hence

$$(e^+R_0 : l(O_k^*)) = |J/J \cap I|^r R(k) = |J/J \cap I|^{2r} R(k^+)/Q_0.$$

Thus

$$(l(O_k^*) : e^+R_0) = Q_0/|J/J \cap I|^{2r} R(k^+).$$

(2) $(e^+R_0 : e^+U_0)$. By Proposition 3.4, U is free abelian of rank $[k : \mathbb{F}_q(T)]$. Thus e^+U is free abelian of rank $[k : \mathbb{F}_q(T)]/|J/J \cap I| = r + 1$ and e^+U_0 is free abelian of rank r. Thus $(e^+R_0 : e^+U_0)$ is defined. Appealing to Sinnott's [3] proof of Lemma 1.2(a), we have

$$(e^+R : e^+U) = (S(G)e^+R : S(G)e^+U)(e^+R_0 : e^+U_0);$$

we have used the fact that $(e^+A)_0 = e^+A_0$ for any $\mathbb{Z}[G]$-module A in $\mathbb{Q}[G]$. Referring again to Sinnott's [3] proof of Proposition 2.2, we find that $U = U_0 + U^G = U_0 + S(G)\mathbb{Z}$. Therefore

$$(S(G)e^+R : S(G)e^+U) = |G| = [k : \mathbb{F}_q(T)],$$

from which one concludes that

$$(e^+R_0 : e^+U_0) = (e^+R : e^+U)/[k : \mathbb{F}_q(T)].$$

(3) $(e^+U_0 : (1 - e_1)T_1)$. By Corollary 3.8 and the fact that $\omega'U = \omega'e^+U_0$, we have $(1 - e_1)T_1 = \omega'e^+U_0$.

Let $F : X \to X$ be the linear transformation defined by $F(x) = \omega'x$. Then $F(e^+U_0) = (1 - e_1)T_1$. The computation of $\det(F)$ from the expression for ω', together with the analytic class number formula, yields

$$\det(F) = \prod_{\chi \neq \chi_0} \varphi_{F_\chi}(\chi) = (q-1)^r \prod_{\chi \neq \chi_0} \left(\sum_A m(A)\chi(A) \right) = (q-1)^{2r} h(k^+),$$

where in each case the product is taken over the nontrivial real characters of G and the sum is taken over monic A of degree less than $d_\chi = \deg(F_\chi)$ which are prime to F_χ. It follows that $(1 - e_1)T_1$ is a lattice in X and that

$$(e^+U_0 : (1 - e_1)T_1) = (q-1)^{2r} h(k^+).$$

(4) $((1 - e_1)T_1 : l(C))$. In Proposition 3.6 we showed that

$$\begin{aligned}((1 - e_1)T_1 : l(C)) = \prod_{i=1}^{g} [k_{Q_i^{e_i}} : \mathbb{F}_q(T)] \cdot \left| \left(\frac{D}{\mathbb{F}_q(T)^*} \right)_{q-1} \right|^{-1} \cdot [L_1 : L_2 + L_3]^{-1} \\ \cdot [\psi(L_2) : \psi(L_2 \cap L_3)]^{-1} \cdot [\psi(L_1) : \psi(L_3)]\end{aligned}$$

and so $l(C)$ is a lattice in X.

Combining (1)–(4), and the relation $h(k^+) = h(O_{k^+})R(k^+)$, we see that

$$\begin{aligned}[O_k^* : C] &= \frac{Q_0}{|J/J \cap I|^{2r} R(k^+)} \cdot \frac{(e^+R : e^+U)}{[k : \mathbb{F}_q(T)]} \cdot (q-1)^{2r} h(k^+) \\ &\quad \cdot \prod_{i=1}^{g} [k_{Q_i^{e_i}} : \mathbb{F}_q(T)] \cdot \left| \left(\frac{D}{\mathbb{F}_q(T)^*} \right)_{q-1} \right|^{-1} \cdot [L_1 : L_2 + L_3]^{-1} \\ &\quad \cdot [\psi(L_2) : \psi(L_2 \cap L_3)]^{-1} \cdot [\psi(L_1) : \psi(L_3)] \\ [O_k^* : C] &= h(O_{k^+}) \cdot Q_0 \cdot |J \cap I|^{2r} \cdot \left| \left(\frac{D}{\mathbb{F}_q(T)^*} \right)_{q-1} \right|^{-1} \\ &\quad \cdot \frac{\prod_{i=1}^{g} [k_{Q_i^{e_i}} : \mathbb{F}_q(T)]}{[k : \mathbb{F}_q(T)]} \cdot (e^+R : e^+U) \cdot [L_1 : L_2 + L_3]^{-1} \\ &\quad \cdot [\psi(L_2) : \psi(L_2 \cap L_3)]^{-1} \cdot [\psi(L_1) : \psi(L_3)].\end{aligned}$$

4. $(e^+R : e^+U)$

In this section, we state two results about the R-module U. They are direct analogues of results in the number field setting (see [3, §5]), and their proofs carry over almost verbatim to the function field setting.

Recall that T_N, where N is a monic polynomial which divides $\overline{M}$, is the compositum of the inertia groups T_Q as Q varies through the monic primes dividing N. Let U_N be the R-module generated in $\mathbb{Q}[G]$ by the elements

$$S(T_A) \prod_{Q|N/A} (1 - (Q, k)^*)$$

where the product is taken over the monic primes Q dividing N/A, and A varies over the monic polynomials which divide N. Then, in particular,

$$U_1 = R, \qquad U_{\overline{M}} = U.$$

If Q is a monic prime that divides $\overline{M}$, but not N, we have

$$U_{NQ} = U_N(T_Q) + (1 - (Q, k)^*)U_N,$$

where $U_N(T_Q)$ is defined to be the R-module generated in $\mathbb{Q}[G]$ by the elements

$$S(T_{AQ}) \prod_{Q|N/A} (1 - (Q, k)^*),$$

as A varies over the monic polynomials which divide N.

Proposition 4.2. *For any monic polynomial N which divides $\overline{M}$, and any α in $\mathbb{Q}[G]$, the index $(\alpha R : \alpha U_N)$ is an integer divisible only by the primes dividing $|T_N|$. In particular, the index $(e^+R : e^+U)$ is an integer divisible only by the primes dividing $|G|$.*

References

1. S. Galovich and M. Rosen, *Units and class groups in cyclotomic function fields*, J. Number Theory **14** (1982), 156–184.
2. W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. (2) **108** (1978), 107–134.
3. ——, *On the Stickelberger ideal and the circular units of an abelian field*, Invent Math. **62** (1980), 181–234.

Department of Mathematics and Computer Science, Rhode Island College, Providence, Rhode Island 02908