Palestine Journal of Mathematics

Vol. 12(4)(2023) , 440–451

EXTENDED GENUS FIELD OF CYCLIC KUMMER EXTENSIONS OF RATIONAL FUNCTION FIELDS

Edgar Omar Curiel–Anaya, Myriam Rosalía Maldonado–Ramírez and Martha Rzedowski–Calderón

Communicated by Zafar Ahsan

MSC 2010 Classifications: Primary 11R58; Secondary 11R29.

Keywords and phrases: Global function fields, extended genus fields, cyclic Kummer extensions.

Abstract For a cyclic Kummer extension K of a rational function field k is considered, via class field theory, the extended Hilbert class field K_H^+ of K and the corresponding extended genus field K_g^+ of K over k, along the lines of the definitions of R. Clement for such extensions of prime degree. We obtain K_g^+ explicitly. Also, we use cohomology to determine the number of ambiguous classes and obtain a reciprocity law for K/k. Finally, we present a necessary and sufficient condition for a prime of K to decompose fully in K_g^+.

1 Introduction

For a number field K, one of the most important arithmetic objects attached to K is its class group. This group is isomorphic to the Galois group of the extension K_H/K, where K_H denotes the maximal unramified abelian extension of K. The field K_H is the *Hilbert class field of* K (HCF). We have that K_H/K is a finite extension and also that K_H is the abelian extension of K such that the primes of K that are fully ramified in K_H are precisely the non-zero principal ideals of K. One variant of the HCF is the *extended* or *narrow Hilbert class field of* K, denoted by K_H^+. The field K_H^+ is the maximal abelian extension of K unramified at the finite primes. We have that K_H^+/K is a finite extension, that $K_H \subseteq K_H^+$ and also that K_H^+ is the abelian extension of K where a prime of K is fully decomposed precisely when it is a principal ideal generated by a totally positive element, that is, an element such that all its real conjugates are positive.

In order to study the class group of K, but also interesting by itself, it is considered an intermediate field $K \subseteq K_g \subseteq K_H$, called the *genus field of* K (relative to $\mathbb{Q}$). The field K_g is, by definition, the composite of K and the maximal abelian extension of $\mathbb{Q}$ contained in K_H. That is, $K_g = Kk^*$, where k^* is the maximal abelian extension of $\mathbb{Q}$ contained in K_H. Similarly, it is considered the *extended* or *narrow genus field of* K (relative to $\mathbb{Q}$) K_g^+, as the composite of K and the maximal abelian extension of $\mathbb{Q}$ contained in K_H^+. These definitions are due to A. Fröhlich ([3, 4]). For a number field K, the fields K_H, K_H^+, K_g and K_g^+ are defined without any ambiguity and all of them are finite extensions of K. In particular, when K/k is an abelian extension, K_g (resp. K_g^+) is the maximal abelian extension of k contained in K_H (resp. K_H^+).

When we study global function fields and we want to consider genus fields and/or extended genus fields, the situation is different from the number field case since the extensions of constants of any global function field K are unramified so that the maximal unramified abelian extension of K is of infinite degree over K. That is, if we consider the straight analog of the Hilbert class field as the maximal unramified abelian extension of K we have to deal with infinite extensions.

There have been a good number of alternatives to define a Hilbert class field that is a *finite* extension of a global function field K. One of them is to define the Hilbert class field of K as the maximal *geometric* abelian extension of K, that is, the maximal unramified abelian extension of K with the same field of constants as K. It turns out that there are h_K such extensions, where h_K denotes the class number of K, that is, the cardinality of the zero degree divisor class group of K which is a finite group. This definition has the issue that K_H is not unique but there are h_K different choices.

To avoid infinite extensions and the lack of uniqueness of K_H, we have to deal with extensions of constants. Since every prime in K is eventually inert in an extension of constants, the most accepted way to define K_H is first to fix a non-empty finite set S of primes of K and then consider the maximal unramified abelian extension of K where the primes of S decompose fully. Such field is denoted by $K_{H,S}$ and it is a finite extension of K. The Galois group of $K_{H,S}/K$ is isomorphic to the ideal class group of the Dedekind ring $\mathcal{O}_S := \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}$. This ideal class group is a finite group. B. Anglès and J.-F. Jaulent [1] have given class field theory definitions of Hilbert class field and extended Hilbert class field that work for any global field.

R. Clement [2] offered another definition of extended Hilbert class field for a cyclic Kummer extension K of $k := \mathbb{F}_q(T)$, the rational function field, of prime degree l (necessarily $l|q-1$) and consequently another definition of extended genus field K_g^+ of K (relative to k). As far as we know, she was the first one to consider the concept of extended genus field for global function fields.

Since the introduction of the concept of *genus* by C. F. Gauss, in the study of quadratic forms and its translation to number fields by D. Hilbert, the concept has been studied by several authors. H. Hasse [5] was the first to give a definition of genus field by means of class field theory. Hasse gave his definition for quadratic number fields. The concept was generalized by H. Leopoldt in [6] to finite abelian extensions of the field of rational numbers $\mathbb{Q}$. As a consequence of the work of Hasse, the Galois group of K_H^+/K, where K is a quadratic extension of $\mathbb{Q}$, is isomorphic to I_K/P_{K^+}, where I_K is the group of fractional ideals of K and P_{K^+} is the subgroup of principal ideals generated by a totally positive element of K. Since K is a quadratic extension of $\mathbb{Q}$, to be a totally positive element of K is equivalent to have that its norm in $\mathbb{Q}$ is a square of a real number. This concept was brought to the case of a cyclic extension K/k of prime degree l with $l|q-1$ by Clement. She defined K_H^+ as the class field of K corresponding to the subgroup $\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$ of the idèle group J_K of K, where $\Delta := \big\{(x_{\mathfrak{p}})_{\mathfrak{p}|\infty} \in \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \mid \prod \mathrm{N}_{K_{\mathfrak{p}}/k_\infty} x_{\mathfrak{p}} \in k_\infty^{*l}\big\}$ and where ∞ denotes the infinite prime of k, that is the pole of T in k . This definition only works for cyclic Kummer extensions of k of prime degree.

The aim of this paper is to confirm that the definition of K_H^+ given by Clement can be extended to general cyclic Kummer extensions K of k and to obtain the extended genus field of a general cyclic Kummer extension of k explicitly. We use cohomology theory to determine the number of ambiguous classes. Finally, we obtain a reciprocity law for K/k and present a necessary and sufficient condition for a prime of K to decompose fully in K_g^+. We use techniques similar to the ones used by Clement.

2 Cyclic Kummer extensions of *k*

For any global field E, J_E denotes the idèle group of E. For a place $\mathfrak{p}$ of E, $E_{\mathfrak{p}}$ denotes the completion of E at $\mathfrak{p}$ and $U_{\mathfrak{p}}$ the group of local units of $E_{\mathfrak{p}}$. Let $k := \mathbb{F}_q(T)$ be the rational function field over the finite field $\mathbb{F}_q$, $R_T := \mathbb{F}_q[T]$ and $R_T^+ := \{P \in R_T \mid P \text{ is monic and irreducible}\}$. The infinite prime $\infty = \mathcal{P}_\infty$ of k is the pole of T in k. Finally, for any $m \in \mathbb{N}$, C_m denotes the cyclic group of order m.

Let $n \in \mathbb{N}$ be a natural number dividing $q-1$: $n|q-1$. Let K/k be a cyclic Kummer extension of degree n. Therefore, $K = k\big(\sqrt[n]{D}\big)$ with $D = \gamma P_1^{\alpha_1} \cdots P_r^{\alpha_r} \in R_T$, $\gamma \in \mathbb{F}_q^*$, $P_1, \ldots, P_r \in R_T^+$ and $1 \leq \alpha_i \leq n-1$ for $1 \leq i \leq r$. The ramified finite primes are $P_1, \ldots, P_r$. Let e_i denote the ramification index of P_i in K/k, $1 \leq i \leq r$. Denote by e_∞ and f_∞ the ramification index and the inertia degree of any prime $\mathfrak{p}$ in K above $\mathcal{P}_\infty$.

Define

$$\Delta := \big\{(x_{\mathfrak{p}})_{\mathfrak{p}|\infty} \mid \prod_{\mathfrak{p}|\infty} \mathrm{N}_{K_{\mathfrak{p}}^*/k_\infty^*}(x_{\mathfrak{p}}) \in k_\infty^{*n}\big\} \subseteq J_K,$$

$$J_K^+ := \{\vec{\alpha} \in J_K \mid (\alpha_{\mathfrak{p}})_{\mathfrak{p}|\infty} \in \Delta\}$$

and

$$K^+ := K^* \cap J_K^+ = \{(x, \dots, x \dots) \mid x \in K^*, (x)_{\mathfrak{p}|\infty} \in \Delta\}$$
$$= \{x \in K^* \mid \mathrm{N}_{K/k}(x) \in k_\infty^{*n}\}.$$

Lemma 2.1. *Let $n \in \mathbb{N}$ be a divisor of $q-1$. Then $\frac{k_\infty^*}{k_\infty^{*n}} \cong C_n \times C_n$.*

Proof. It follows from the group structure of k_∞^*, the fact that $n|q-1 = |\mathbb{F}_q^*|$ and, since n is relatively prime to the characteristic of k, that $\big(U_\infty^{(1)}\big)^n = U_\infty^{(1)}$, where $U_\infty^{(1)}$ are the one units of k_∞^*. □

Lemma 2.2. *We have*

(1) $J_k = k^*\big(k_\infty^* \times \prod_{P\in R_T^+} U_P\big)$.

(2) $K^* J_K^+ = J_K$.

Proof. (1) Let $\vec{\beta} = (\beta_\infty, \beta_P)_{P\in R_T^+} \in J_k$. Let $Q_1, \dots, Q_t \in R_T^+$ be the finite primes such that $v_{Q_i}(\beta_{Q_i}) = c_i \neq 0$. We have that $v_P(\beta_P) = 0$ for all $P \in R_T^+ \setminus \{Q_1, \dots, Q_t\}$. Define $f \in k^*$ as $f = \prod_{i=1}^t Q_i^{c_i}$. Then $f^{-1}\vec{\beta} \in \big(k_\infty^* \times \prod_{P\in R_T^+} U_P\big)$ and the result follows.

(2) Let $\vec{\alpha} \in J_K$. By the approximation theorem, there exists $x \in K^*$ such that $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}} - x) > v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})$ for all $\mathfrak{p}|\infty$. Then $x^{-1}\alpha_{\mathfrak{p}} \in U_K^{(1)} = \big(U_K^{(1)}\big)^n$ and $\mathrm{N}_{K_{\mathfrak{p}}/k_\infty}(x^{-1}\alpha_{\mathfrak{p}}) \in k_\infty^{*n}$. Hence $x^{-1}\vec{\alpha} \in J_K^+$. □

Lemma 2.3. *The map* $\mathrm{N}\colon \frac{\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*}{\Delta} \longrightarrow \frac{k_\infty^*}{k_\infty^{*n}}$ *induced by the norm, is injective. Furthermore, the sequence*

$$1 \longrightarrow \frac{\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*}{\Delta} \xrightarrow{\ \mathrm{N}\ } \frac{k_\infty^*}{k_\infty^{*n}} \xrightarrow{\ \pi\ } \frac{k_\infty^*}{\mathrm{N}\big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*\big)} \longrightarrow 1,$$

is exact, where $\mathrm{N}\big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*\big) = \{\prod_{\mathfrak{p}|\infty} \mathrm{N}_{K_{\mathfrak{p}}^*/k_\infty^*}(x_{\mathfrak{p}}) \in k_\infty^* \mid x_{\mathfrak{p}} \in K_{\mathfrak{p}}^*\}$.

Proof. Follows from the definition of Δ. □

Remark 2.4. For any finite Galois extension E/F of global function fields, we have that if $\mathcal{P}$ is prime in F and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two primes in E above $\mathcal{P}$, then $\mathrm{N}_{E_{\mathfrak{p}_1}/F_{\mathcal{P}}}(E_{\mathfrak{p}_1}^*) = \mathrm{N}_{E_{\mathfrak{p}_2}/F_{\mathcal{P}}}(E_{\mathfrak{p}_2}^*)$.

Corollary 2.5. *We have* $\big[\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* : \Delta\big] = \frac{n^2}{e_\infty f_\infty}$.

Proof. From Lemma 2.3 we obtain that

$$\Big[\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* : \Delta\Big] = \frac{\big[k_\infty^* : k_\infty^{*n}\big]}{\big[k_\infty^* : \mathrm{N}\big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*\big)\big]},$$

and from Remark 2.4 we have that $\mathrm{N}\big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*\big) = \mathrm{N}_{K_{\mathfrak{p}}^*/k_\infty^*}(K_{\mathfrak{p}}^*)$ for any $\mathfrak{p}|\mathcal{P}_\infty$. From the fundamental result of local field theory, we have that $\big[k_\infty^* : \mathrm{N}_{K_{\mathfrak{p}}^*/k_\infty^*}(K_{\mathfrak{p}}^*)\big] = e_\infty f_\infty$. The result now follows from Lemma 2.1. □

Remark 2.6. We have

$$\frac{\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*}{\Delta} \cong \frac{\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{P\in R_T^+} U_P}{\Delta \times \prod_{P\in R_T^+} U_P}.$$

Lemma 2.7. *We have the following equalities*

$$\begin{aligned}
&\frac{\left[\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* : \Delta\right]}{\left[K^* \cap \left(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right) : K^* \cap \left(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right)\right]} \\
&\qquad = \frac{\left[\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}} : \Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right]}{\left[K^* \cap \left(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right) : K^* \cap \left(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right)\right]} \\
&\qquad = \left[K^*\Big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)/K^* : K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)/K^*\right] \\
&\qquad = \left[K^*\Big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big) : K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)\right].
\end{aligned}$$

Proof. The first equality follows from Remark 2.6. The second equality is a consequence of the fact that for any finite subgroups A, B, C of an abelian group X with $A \subseteq B$, we have $\frac{B\cap C}{A\cap C} \cong \frac{CA\cap B}{A}$. The last equality is a consequence of the third isomorphism theorem. □

Let $\mathcal{O}_K$ be the integral closure of R_T in K. Let U_K be the group of units of $\mathcal{O}_K$: $U_K = \mathcal{O}_K^*$. Set $U_K^+ := \{\alpha \in U_K \mid \mathrm{N}_{K/k}(\alpha) \in k_\infty^{*n}\} = \{\alpha \in U_K \mid \mathrm{N}_{K/k}(\alpha) \in \mathbb{F}_q^{*n}\} = U_K \cap K^+$.

Lemma 2.8. *We have*

$$\frac{U_K}{U_K^+} \cong \frac{K^* \cap \left(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right)}{K^* \cap \left(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right)}.$$

Proof. The natural map

$$\begin{aligned}
\varphi\colon U_K &\longrightarrow \frac{K^* \cap \left(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right)}{K^* \cap \left(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\right)} \\
\alpha &\mapsto (\alpha, \ldots, \alpha, \ldots) \bmod \Big(K^* \cap \Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)\Big),
\end{aligned}$$

is a group epimorphism with $\ker\varphi = U_K^+$. □

Lemma 2.9. *We have* $[U_K : U_K^+] \mid n$.

Proof. Let $\rho\colon U_K\colon \longrightarrow \mathrm{N}_{K/k}(U_K)/\mathbb{F}_q^{*n}$ be given by $\rho(\alpha) = \mathrm{N}_{K/k}(\alpha) \bmod \mathbb{F}_q^{*n}$. Then $\ker\rho = U_K^+$. It follows that U_K/U_K^+ is a subgroup of $\mathbb{F}_q^*/\mathbb{F}_q^{*n} \cong C_n$. □

Remark 2.10. In Lemma 2.9 we may have $[U_K : U_K^+] < n$. For instance, if $\mathcal{P}_\infty$ is totally inert in K/k, then $U_K = \mathbb{F}_q^*$ and $U_K = U_K^+$.

3 Extended Hilbert class field and extended genus field

Let K/k be a cyclic Kummer extension of degree n. We will define the extended Hilbert class field of K by means of an open subgroup of finite index in J_K. To do this, first, we prove the following proposition which is the generalization of the corresponding one in Clement's paper. We present the proof for the sake of completeness.

Proposition 3.1. *The index of* $K^*\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)$ *in the idèle group* J_K *is finite.*

Proof. We have that $K^*\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big) \subseteq K^*\big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)$. On the one hand, we have that $J_K/\Big(K^*\big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\Big) \cong Cl(\mathcal{O}_K)$, the ideal class group of $\mathcal{O}_K$, which is a finite group.

On the other hand, we have

$$\Big[K^*\Big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big) : K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)\Big]$$

$$= \frac{\Big[\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* : \Delta\Big]}{\Big[K^* \cap \big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big) : K^* \cap \big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\Big]} = \frac{\Big[\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* : \Delta\Big]}{\big[U_K : U_K^+\big]}.$$

The result follows from Corollary 2.5 and Lemma 2.9. □

Remark 3.2. The group Δ is the inverse image of k_∞^{*n} under the norm map, which is a continuous function. Hence the subgroup $K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)$ is an open subgroup of J_K of finite index.

Definition 3.3. We define the *extended Hilbert class field* K_H^+ of K as the class field associated with the idèle subgroup $K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)$ of J_K.

Remark 3.4. We have that K_H^+/K is a finite Galois extension,

$$\mathrm{Gal}(K_H^+/K) \cong \frac{J_K}{K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)}$$

and also that K_H^+/K is unramified at every finite place $\mathfrak{p}$ of K.

Proposition 3.5. *We have*

$$\frac{J_K}{K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)} \cong \frac{J_K^+}{K^+\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)} \cong \frac{I_K}{P_K^+},$$

where I_K is the group of non-zero fractional ideals of $\mathcal{O}_K$, P_K the subgroup of principal ideals of I_K, and P_K^+ the subgroup of P_K of fractional ideals (β) such that $\beta \in K^+$.

Proof. From Lemma 2.2 we obtain that the natural map $\varphi\colon J_K^+ \mapsto J_K/K^*$ is surjective and $\ker\varphi = K^* \cap J_K^+ = K^+$. Let $\rho = \hat{\varphi}^{-1}\colon J_K/K^* \longrightarrow J_K^+/K^+$ be the induced isomorphism. Then $\rho\big(K^*(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}})/K^*\big) = \big(J_K^+ \cap K^*(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}})\big)/K^+$. It follows that

$$\frac{J_K^+/K^+}{\big(J_K^+ \cap K^*(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}})\big)/K^+} \cong \frac{J_K/K^*}{K^*(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}})/K^*}.$$

The first isomorphism follows since $J_K^+ \cap K^*\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big) = K^+\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)$. For the second isomorphism it is considered the map $\theta\colon J_K^+ \longrightarrow I_K/P_K^+$ given by $\big((\alpha_{\mathfrak{p}})_{\mathfrak{p}|\infty}, (\alpha_{\mathfrak{p}})_{\mathfrak{p}\nmid\infty}\big) \mapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \bmod P_K^+$. Then θ is a group epimorphism and $\ker\theta = K^+\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)$. □

Definition 3.6. The *extended ideal class group of K* is defined by

$$Cl^+(\mathcal{O}_K) := \frac{I_K}{P_K^+} \cong \mathrm{Gal}(K_H^+/K).$$

Proposition 3.7. *The extension K_H^+/k is a Galois extension.*

Proof. It follows from the facts that $\rho(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}) = \Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$ for all k–embeddings ρ of K_H^+ into a fixed algebraic closure of K_H^+ and that K/k is a Galois extension. □

Proposition 3.8. *The finite primes in K that decompose fully in K_H^+ are precisely the principal ideals generated by an element $\beta \in K^*$ satisfying $\mathrm{N}_{K/k}(\beta) \in k_\infty^{*n}$.*

Proof. From class field theory, see for instance [7, Corolario 17.6.47], we have that $\mathfrak{p}$ decomposes fully in K_H^+/K if and only if $K_{\mathfrak{p}}^* \subseteq K^*\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)$. Let π be such that $v_{\mathfrak{p}}(\pi) = 1$. We have

$$K_{\mathfrak{p}}^* \subseteq K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big) \iff (1,1,\ldots,x,1,\ldots) \in K^*\Big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\Big)$$

for each $x \in K_{\mathfrak{p}}^*$, in particular for $x = \pi$. Therefore there exist $\beta \in K^*$ and $\vec{\alpha} \in \Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$ such that $(1,1,\ldots,\pi,1,\ldots) = \beta\vec{\alpha}$. It follows that $v_{\mathfrak{q}}(\beta) = 0$ for every finite prime $\mathfrak{q} \neq \mathfrak{p}$ and $v_{\mathfrak{p}}(\beta^{-1}\pi) = 0$. Therefore the only prime dividing $\langle\beta\rangle$ is $\mathfrak{p}$ and it does so to the power 1. Hence $\mathfrak{p} = \langle\beta\rangle$.

On the other hand, $(\beta^{-1})_{\mathfrak{q}|\infty} \in \Delta$ so that $\mathrm{N}_{K/k}(\beta) = \prod_{\mathfrak{q}|\infty} \mathrm{N}_{K_{\mathfrak{q}}^*/k_\infty^*}(\beta) \in k_\infty^{*n}$. □

Corollary 3.9. *If $Q \in R_T^+$ is inert in K, then $\mathfrak{q}$ decomposes fully in K_H^+ where $\mathfrak{q} = Q\mathcal{O}_K$ is the prime in K above Q.*

Proof. We have $\mathrm{N}_{K/k}(\mathfrak{q}) = Q^n$. The result follows. □

Definition 3.10. We define the *extended genus field K_g^+ of K (relative to k)* as the maximal abelian extension of k contained in K_H^+.

Remark 3.11. From class field theory, see for instance [7, Proposición 17.6.48], the field K_g^+ is the class field associated with $k^*\,\mathrm{N}_{K/k}\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)$.

Proposition 3.12. *The degree of K_g^+ over k and the degree of K_g^+ over K are given by*

$$\big[K_g^+ : k\big] = n\prod_{i=1}^r e_i \quad \textit{and} \quad \big[K_g^+ : K\big] = \prod_{i=1}^r e_i.$$

Proof. Let $P \in R_T^+$. Then from Remark 2.4 we obtain that $\prod_{\mathfrak{p}|P} \mathrm{N}_{K_{\mathfrak{p}}/k_P}(U_{\mathfrak{p}}) = \mathrm{N}_{K_{\mathfrak{p}}/k_P}(U_{\mathfrak{p}})$ for any fixed prime $\mathfrak{p}|P$. From the theory of local fields, we have $[U_P : \mathrm{N}_{K_{\mathfrak{p}}/k_P}(U_{\mathfrak{p}})] = e_P$, the ramification index of P in K/k. Recall that $e_P = 1$ if P is unramified and $e_{P_i} = e_i$, $1 \le i \le r$.

Therefore, from Lemmas 2.1 and 2.2 and since $k^* \cap \big(k_\infty^* \times \prod_{P\in R_T^+} U_P\big) = \mathbb{F}_q^*$, we obtain

$$\begin{aligned}
\big[K_g^+ : k\big] &= \big[J_k/k^* : \big(k^*\,\mathrm{N}_{K/k}\,\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\big)/k^*\big] \\
&= \Big[k^*\big(k_\infty^* \times \prod_{P\in R_T^+} U_P\big) : k^*\,\mathrm{N}_{K/k}\,\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\Big] \\
&= \frac{\big[k_\infty^* \times \prod_{P\in R_T^+} U_P : \mathrm{N}_{K/k}\,\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\big]}{\big[k^* \cap \big(k_\infty^* \times \prod_{P\in R_T^+} U_P\big) : k^* \cap \big(\mathrm{N}_{K/k}\,\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\big)\big]} \\
&= \frac{\big[k_\infty^* \times \prod_{P\in R_T^+} U_P : \mathrm{N}_{K/k}\,\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big)\big]}{\big[\mathbb{F}_q^* : \mathbb{F}_q^{*n}\big]} \\
&= \frac{[k_\infty^* : k_\infty^{*n}] \cdot \prod_{P\in R_T^+} [U_P : \mathrm{N}_{K_{\mathfrak{p}}/k_P}(U_{\mathfrak{p}})]}{n} = \frac{n^2\prod_{i=1}^r e_i}{n} = n\prod_{i=1}^r e_i.
\end{aligned}$$

Finally, since $[K : k] = n$, it follows that $\big[K_g^+ : K\big] = \prod_{i=1}^r e_i$. □

Define $\Gamma := \mathbb{F}_{q^n}\big(T, \sqrt[e_1]{P_1}, \ldots, \sqrt[e_r]{P_r}\big)$. Then $[\Gamma : k] = n\prod_{i=1}^r e_i = [K_g^+ : k]$ and Γ/k is an abelian extension. On the other hand, by Abhyankar's Lemma, the ramification index of P_i in $K\Gamma$ is e_i, $1 \le i \le r$ and Γ/k is unramified at every $P \in R_T^+ \setminus \{P_1, \ldots, P_r\}$. It follows that Γ/K is unramified at every finite prime $P \in R_T^+$.

We are ready to prove our main result, which gives an explicit and nice expression for K_g^+.

Theorem 3.13. *Let $n \in \mathbb{N}$ be a natural number dividing $q-1$: $n|q-1$. Let K/k be a cyclic Kummer extension of degree n, $K = k\big(\sqrt[n]{D}\big)$ with $D = \gamma P_1^{\alpha_1}\cdots P_r^{\alpha_r} \in R_T$, $\gamma \in \mathbb{F}_q^*$,*

$P_1, \ldots, P_r \in R_T^+$ and $1 \leq \alpha_i \leq n-1$ for $1 \leq i \leq r$. The ramified finite primes are $P_1, \ldots, P_r$. Let e_i be the ramification index of P_i in K/k, $1 \leq i \leq r$.

Then

$$K_g^+ = \Gamma = \mathbb{F}_{q^n}\big(T, \sqrt[e_1]{P_1}, \ldots, \sqrt[e_r]{P_r}\big).$$

Proof. It suffices to prove that $\Gamma \subseteq K_H^+$ since K_g^+ is the maximal abelian extension of k contained in K_H^+ and Γ/k is an abelian extension. Now, let $H := \mathrm{Gal}(\Gamma/k) \cong C_n \times C_{e_1} \times \cdots \times C_{e_r}$. Since $e_i | n$ for all $1 \leq i \leq r$, H is of exponent n. Therefore, it is enough to show that any abelian extension of k, containing K, of exponent n and such that it is unramified at the finite primes of K, is contained in K_H^+.

Let L be such an extension. By class field theory, it is enough to prove that $K^*\big(\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}\big) \subseteq K^* \,\mathrm{N}_{L/K}(J_L)$. We have the following commutative diagram

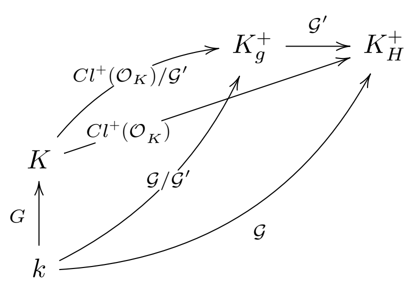
$$\begin{array}{ccc} J_K & \xrightarrow{\ \rho_K\ } & \mathrm{Gal}(L/K) \\ {\scriptstyle \mathrm{N}_{K/k}}\downarrow & & \downarrow{\scriptstyle \iota} \\ J_k & \xrightarrow[\ \rho_k\ ]{} & \mathrm{Gal}(L/k) \cong C_{m_1} \times \cdots \times C_{m_t}, \end{array}$$

where ρ_K and ρ_k denote Artin's reciprocity maps, ι is the natural embedding and $m_j | n$, $1 \leq j \leq t$. The norm of an element $\vec{\alpha} \in \Delta$ is of the form $(\beta, 1, \ldots, 1, \ldots) \in J_k^n$. Therefore $(\beta, 1, \ldots, 1, \ldots) \in \ker \rho_k$. Hence $\rho_K(\Delta) \in \ker \rho_K = K^* \,\mathrm{N}_{L/K}(J_L)$. Since L/K is unramified at every finite prime, it follows that $U_{\mathfrak{p}} \subseteq K^* \,\mathrm{N}_{L/K}(J_L)$ for every finite prime $\mathfrak{p}$. Therefore $\Delta \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}} \subseteq K^* \,\mathrm{N}_{L/K}(J_L)$. The result follows. □

4 Ambiguous classes

We understand by *ambiguous classes* the elements of $Cl^+(\mathcal{O}_K)$ fixed under the action of $G := \mathrm{Gal}(K/k)$: $Cl^+(\mathcal{O}_K)^G$. We are interested in the number of such classes.

Let $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$. Let $\rho\colon Cl^+(\mathcal{O}_K) \longrightarrow Cl^+(\mathcal{O}_K)^{1-\sigma}$ be the map $[\mathfrak{a}] \mapsto [\mathfrak{a}][\mathfrak{a}]^{-\sigma}$ for $\mathfrak{a} \in I_K$ and $[\mathfrak{a}] = \mathfrak{a} \bmod P_K^+$. Then ρ is an epimorphism and $\ker \rho = Cl^+(\mathcal{O}_K)^G$. In particular, $\frac{Cl^+(\mathcal{O}_K)}{Cl^+(\mathcal{O}_K)^{1-\sigma}} \cong Cl^+(\mathcal{O}_K)^G$. Let $\mathcal{G} := \mathrm{Gal}(K_H^+/k)$. Since K_g^+ is the maximal abelian extension of k contained in K_H^+, we have that the commutator subgroup $\mathcal{G}'$ is isomorphic to $\mathrm{Gal}(K_H^+/K_g^+)$.



Now, we have that $\mathcal{G}' \cong Cl^+(\mathcal{O}_K)^{1-\sigma}$. To find $|Cl^+(\mathcal{O}_K)^G|$ we need several results on cohomology theory, most of them well known.

First, we have the exact sequence

$$1 \longrightarrow K^+ \longrightarrow K^* \longrightarrow K^*/K^+ \longrightarrow 1,$$

From Hilbert's theorem 90, we have $H^1(G, K^*) = \{1\}$, therefore we obtain the cohomology exact sequence

$$1 \longrightarrow k^* \longrightarrow k^* \longrightarrow (K^*/K^+)^G \longrightarrow H^1(G, K^+) \longrightarrow 1,$$

so that $H^1(G, K^+) \cong (K^*/K^+)^G$. We have, for any $a \in K^*$, $\sigma(a)/a \in K^+$, which implies that $(K^*/K^+)^G = K^*/K^+$. Using the approximation theorem, we obtain that

$$K^*/K^+ \cong \big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^*\big)/\Delta.$$

From Corollary 2.5 it follows that

$$|H^1(G, K^+)| = \frac{n^2}{e_\infty f_\infty}.$$

Lemma 4.1. *The Herbrand quotient of U_K is $h(G, U_K) = \frac{e_\infty f_\infty}{n}$.*

Proof. From Dirichlet's unit theorem, we have that $U_K \cong \mathbb{Z}^{m-1} \times \mathbb{F}_q^*$ where m is the number of primes of K above the infinite prime $\mathcal{P}_\infty$ of k. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the primes of K that lie above $\mathcal{P}_\infty$, ordered such that $\sigma(\mathfrak{p}_j) = \mathfrak{p}_{j+1}$ for $1 \le j \le m-1$ and $\sigma(\mathfrak{p}_m) = \mathfrak{p}_1$. Choose $a \in \mathbb{N}$ such that $\big(\frac{\mathfrak{p}_j}{\mathfrak{p}_{j+1}}\big)^a = \langle \mu_j \rangle$ is a principal ideal and $\mu_j \in U_K$, for all $1 \le j \le m-1$. We have $\sigma(\mu_j) = \mu_{j+1}$ for $1 \le j \le m-2$ and $\sigma(\mu_{m-1}) = (\mu_1 \cdots \mu_{m-1})^{-1} =: \mu_m$. Thus $\sigma(\mu_m) = \mu_1$.

It follows that $V := \langle \mu_1, \ldots, \mu_{m-1} \rangle$ is a G–submodule of U_K of finite index. Furthermore, $V \cong \big(\mathbb{Z}[G/D]\big)/\mathbb{Z}$ as G–modules, where D is the decomposition group of any of the primes of K above $\mathcal{P}_\infty$.

We have an exact sequence of G–modules

$$1 \longrightarrow V \longrightarrow U_K \longrightarrow F \longrightarrow 1,$$

where F is finite. Then we have $h(G, U_K) = h(G, V)$. Now, from the exact sequence of G–modules

$$1 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G/D] \longrightarrow V \longrightarrow 1,$$

we obtain that

$$h(G, V) = \frac{h(G, \mathbb{Z}[G/D])}{h(G, \mathbb{Z})} = \frac{n/m}{n} = \frac{1}{m} = \frac{e_\infty f_\infty}{n}.$$

□

Lemma 4.2. *We have $|H^1(G, U_K^+)| = n^2/e_\infty f_\infty$.*

Proof. Since U_K/U_K^+ is finite, it follows that $h(G, U_K) = h(G, U_K^+) = e_\infty f_\infty/n$. Now, we have the Tate cohomology group

$$\hat{H}^0(G, U_K^+) = \frac{(U_K^+)^G}{\mathrm{N}_{K/k}(U_K^+)} = \frac{\mathbb{F}_q^*}{\mathbb{F}_q^{*n}} \cong C_n.$$

The result follows. □

Lemma 4.3. *We have $|I_K/I_k| = e_1 \cdots e_r$.*

Proof. For any $P \in R_T^+$, let $\mathfrak{a}_P = \big(\prod_{\mathfrak{p}|P} \mathfrak{p}\big)^{e_P}$ be the conorm of P, where e_P denotes the ramification index of P in K/k. Then I_K^G is the free abelian group with free generators $\{\mathfrak{a}_P\}_{P \in R_T^+}$. Since I_k is the free abelian group with generators $\{P\}_{P \in R_T^+} = \{\mathfrak{a}_P^{e_P}\}_{P \in R_T^+}$ and the ramified finite primes are $P_1, \ldots, P_r$ with ramification indices $e_1, \ldots, e_r$, we get the result. □

Theorem 4.4. *The number of ambiguous classes $\big|Cl^+(\mathcal{O}_K)^G\big|$ is equal to $e_1 \cdots e_r$.*

Proof. From the exact sequence $1 \longrightarrow P_K^+ \longrightarrow I_K \longrightarrow Cl^+(\mathcal{O}_K) \longrightarrow 1$, and since $H^1(G, I_K) = \{1\}$, we obtain the cohomology sequence

$$1 \longrightarrow (P_K^+)^G \longrightarrow I_K^G \longrightarrow Cl^+(\mathcal{O}_K)^G \longrightarrow H^1(G, P_K^+) \longrightarrow 1.$$

Dividing the first two terms by $I_k = P_k \subseteq P_K^G$, we obtain

$$\left|Cl^+(\mathcal{O}_K)^G\right| = \frac{\left|I_K^G/I_k\right|}{\left|(P_K^+)^G/I_k\right|} \cdot \left|H^1(G, P_K^+)\right|.$$

Next, we consider the exact sequence of G–modules

$$1 \longrightarrow U_K^+ \longrightarrow K^+ \longrightarrow P_K^+ \longrightarrow 1.$$

Since $\left(U_K^+\right) = \mathbb{F}_q^*$ and $(K^+)^G = k^*$, we obtain the exact cohomology sequence

$$\begin{aligned} 1 \longrightarrow \mathbb{F}_q^* \longrightarrow k^* \longrightarrow \left(P_K^+\right)^G \longrightarrow H^1(G, U_K^+) \longrightarrow H^1(G, K^+) \\ \longrightarrow H^1(G, P_K^+) \xrightarrow{\nu} H^2(G, U_K^+) \xrightarrow{\rho} H^2(G, K^+) \longrightarrow \cdots \end{aligned}$$

Now, we have that $I_k \cong k^*/\mathbb{F}_q^*$, that

$$\begin{aligned} H^2(G, U_K^+) \cong H^0(G, U_K^+) &= \frac{\left(U_K^+\right)^G}{\mathrm{N}_{K/k}\left(U_K^+\right)} = \frac{\mathbb{F}_q^*}{\mathbb{F}_q^{*n}}, \\ H^2(G, K^+) \cong H^0(G, K^+) &= \frac{\left(K^+\right)^G}{\mathrm{N}_{K/k}\left(K^+\right)} = \frac{k^*}{\mathrm{N}_{K/k}(K^+)} \end{aligned}$$

and that ρ is an injective map. Therefore, we obtain the exact sequence

$$1 \longrightarrow \frac{\left(P_K^+\right)^G}{I_k} \longrightarrow H^1(G, U_K^+) \longrightarrow H^1(G, K^+) \longrightarrow H^1(G, P_K^+) \longrightarrow 1.$$

Therefore

$$\frac{\left|H^1(G, P_K^+)\right|}{\left|\left(P_K^+\right)^G/I_k\right|} = \frac{\left|H^1(G, K^+)\right|}{\left|H^1(G, U_K^+)\right|}.$$

The result now follows from Lemma 4.3. □

Theorem 4.5. *We have*

$$\mathrm{Gal}(K_g^+/K) \cong \frac{Cl^+(\mathcal{O}_K)}{Cl^+(\mathcal{O}_K)^{1-\sigma}} \cong Cl^+(\mathcal{O}_K)^G.$$

Proof. From the isomorphism $\frac{Cl^+(\mathcal{O}_K)}{Cl^+(\mathcal{O}_K)^{1-\sigma}} \cong Cl^+(\mathcal{O}_K)^G$ and Theorem 4.4, we obtain that $\left|Cl^+(\mathcal{O}_K)^{1-\sigma}\right| = \left|\mathcal{G}'\right| = \left[K_H^+ : K_g^+\right]$, where $\mathcal{G} = \mathrm{Gal}(K_H^+/k)$.

Let $\rho\colon Cl^+(\mathcal{O}_K) \longrightarrow \mathrm{Gal}(K_H^+/K) \subseteq \mathcal{G}$ be the Artin reciprocity map. For any $\mathfrak{b} \in Cl^+(\mathcal{O}_K)$ we have

$$\begin{aligned} \rho\left(\mathfrak{b}^{1-\sigma}\right) = \rho(\mathfrak{b})\rho\left(\mathfrak{b}^{-\sigma}\right) = \rho(\mathfrak{b})\rho\left(\mathfrak{b}^{\sigma}\right)^{-1} = \rho(\mathfrak{b})\left(\sigma^{-1}\rho(\mathfrak{b})\sigma\right)^{-1} \\ = \rho(\mathfrak{b})\sigma^{-1}\rho(\mathfrak{b})^{-1}\sigma \in \mathcal{G}'. \end{aligned}$$

Hence $\rho\left(Cl^+(\mathcal{O}_K)^{1-\sigma}\right) = \mathcal{G}'$ and we get the result. □

5 A reciprocity law for K/k

Here we present a reciprocity law that is analogous to the quadratic reciprocity law. Let $K = k\big(\sqrt[n]{D}\big)$ be as in Section 2. Let $Q \in R_T^+$ be such that $Q \nmid D$. Let $\mathfrak{q}$ be a prime in K above Q. The extension $K_{\mathfrak{q}}/k_Q$ of local fields is unramified of degree f, the inertia degree of $\mathfrak{q}/Q$. We denote the residue fields by $\hat{K}$ and $\hat{k}$ respectively. If Q is of degree d, then $|\hat{k}| = q^d$ and $|\hat{K}| = q^{df}$. We denote by φ_Q the element of $\mathrm{Gal}(K/k)$ that corresponds to the Frobenius generator of $\mathrm{Gal}(\hat{K}/\hat{k})$. Then φ_Q is given by

$$\varphi_Q\big(\sqrt[n]{D}\big) \equiv \big(\sqrt[n]{D}\big)^{q^d} \bmod \mathfrak{q},$$

that is,

$$\frac{\varphi_Q\big(\sqrt[n]{D}\big)}{\sqrt[n]{D}} \equiv D^{\frac{q^d-1}{n}} \bmod \mathfrak{q}.$$

Since $n|q^d - 1$, both sides of the congruence belong to k. Furthermore there exists $j \in \mathbb{N}$ such that $\varphi_Q\big(\sqrt[n]{D}\big)/\sqrt[n]{D} = \zeta_n^j$, where ζ_n is a primitive n–th root of unity.

Definition 5.1. We define the *residue symbol*

$$\left(\frac{D}{Q}\right)_n \in \mathbb{F}_q^*$$

as the unique n–th root of unity satisfying

$$\left(\frac{D}{Q}\right)_n \equiv D^{\frac{q^d-1}{n}} \bmod Q.$$

More generally, if $R = \prod_{j=1}^t Q_j^{\alpha_j} \in R_T$ is relatively prime to D,

$$\left(\frac{D}{R}\right)_n := \prod_{j=1}^t \left(\frac{D}{Q_j}\right)_n^{\alpha_j}.$$

Equivalently, if $\mathfrak{a}$ is a non-zero ideal of R_T relatively prime to D,

$$\left(\frac{D}{\mathfrak{a}}\right)_n := \prod_{P \in R_T^+} \left(\frac{D}{P}\right)_n^{v_P(\mathfrak{a})}.$$

Note that Q decomposes fully in K if and only if $\left(\frac{D}{Q}\right)_n = 1$.

The main properties of the symbol $\left(\frac{D}{Q}\right)_n$ are given in the following proposition, we omit the straightforward proof.

Proposition 5.2. *We have*

(1) *Let $C, D \in R_T$ and $Q \in R_T^+$ be such that $Q \nmid CD$. Then*

$$\left(\frac{C}{Q}\right)_n \left(\frac{D}{Q}\right)_n = \left(\frac{CD}{Q}\right)_n.$$

(2) *For $Q \nmid D$, we have $\left(\frac{D}{Q}\right)_n = 1$ if and only if $D \bmod Q \in \big((R_T/\langle Q\rangle)^*\big)^n$.*

(3) *For* $a \in \mathbb{F}_q^*$,

$$\left(\frac{a}{Q}\right)_n = a^{\frac{q^d-1}{n}}.$$

□

Definition 5.3. Let $\mathfrak{p}$ be a prime in k and let $R, S \in R_T$ be two relatively prime non-zero polynomials: $\gcd(R,S) = 1$. We define the *Hilbert norm residue symbol* by

$$\big(R,S\big)_{\mathfrak{p}} := \frac{\big(S, k_{\mathfrak{p}}\big(\sqrt[n]{R}\big)/k_{\mathfrak{p}}\big)\big(\sqrt[n]{R}\big)}{\sqrt[n]{R}},$$

where $\big(S, k_{\mathfrak{p}}\big(\sqrt[n]{R}\big)/k_{\mathfrak{p}}\big)$ denotes the local norm residue symbol.

We have the following *symbol product formula*.

$$\prod_{\mathfrak{p}} \big(R,S\big)_{\mathfrak{p}} = 1,$$

where $\mathfrak{p}$ runs through all the prime divisors of k, from which it is obtained the following *reciprocity law*.

Theorem 5.4. *Let* $Q, R \in R_T^+$ *be of degrees* $\delta(Q)$ *and* $\delta(R)$ *respectively. Then*

$$\left(\frac{Q}{\langle R\rangle}\right)_n \cdot \left(\frac{R}{\langle Q\rangle}\right)_n^{-1} = \left[\frac{(-1)^{\delta(Q)\delta(R)} b_0^{\delta(Q)}}{a_0^{\delta(R)}}\right]^{\frac{q-1}{n}} = 1.$$

Proof. Similar to [2, Proposition 4.1]. □

Finally, we give our generalization to Theorem 4.2 [2].

Theorem 5.5. *We have that a prime* $\mathfrak{p}$ *of* $\mathcal{O}_K$ *decomposes fully in* K_g^+ *if and only if each finite prime of* k *ramified in* K*, that is, each* P_j*,* $1 \le j \le r$*, decomposes fully in* $k\big(\sqrt[n]{B}\big)/k$*, where* B *is a monic generator of* $\mathrm{N}_{K/k}\,\mathfrak{p}$ *and* n *divides* $\deg B$.

Proof. Let $d_j := \deg P_j$ and $P_j^* := (-1)^{d_j} P_j$, $1 \le j \le r$. We have that $\mathfrak{p}$ decomposes fully in K_g^+/K if and only if the Artin symbol $(\mathfrak{p}, K_g^+/K) = 1$. Since $K_g^+ = \mathbb{F}_{q^n}\big(\sqrt[e_1]{P_1}, \ldots, \sqrt[e_r]{P_r}\big) = \mathbb{F}_{q^n}\big(\sqrt[e_1]{P_1^*}, \ldots, \sqrt[e_r]{P_r^*}\big)$, we have $(\mathfrak{p}, K_g^+/K) = 1$ if and only if $(\mathfrak{p}, K_g^+/K)|_{k\left(\sqrt[e_j]{P_j^*}\right)} = 1$ for all $1 \le j \le r$, and $(\mathfrak{p}, K_g^+/K)|_{\mathbb{F}_{q^n}(T)} = 1$. This is equivalent to

$$(\mathrm{N}_{K/k}\,\mathfrak{p}, k\big(\sqrt[e_j]{P_j^*}\big)/k) = 1 \iff \left(\frac{P_j^*}{\mathrm{N}_{K/k}\,\mathfrak{p}}\right)_{e_j} = 1 \quad \text{for all} \quad 1 \le j \le r,$$

and

$$(\mathrm{N}_{K/k}\,\mathfrak{p}, \mathbb{F}_{q^n}(T)/k) = 1 \iff \left(\frac{\xi}{\mathrm{N}_{K/k}\,\mathfrak{p}}\right)_n = 1,$$

where ξ is a generator of $\mathbb{F}_q^*$.

Let $h = \deg B$. Then, by the reciprocity law,

$$\begin{aligned}\left(\frac{P_j^*}{\mathrm{N}_{K/k}\,\mathfrak{p}}\right)_{e_j} &= \left(\frac{-1}{\mathrm{N}_{K/k}\,\mathfrak{p}}\right)_{e_j}^{d_j} \left(\frac{P_j}{\mathrm{N}_{K/k}\,\mathfrak{p}}\right)_{e_j} \\ &= (-1)^{((q^h-1)/e_j)d_j} (-1)^{hd_j(q-1)/e_j} \left(\frac{B}{\langle P_j\rangle}\right)_{e_j} = \left(\frac{B}{\langle P_j\rangle}\right)_{e_j},\end{aligned}$$

for $1 \le j \le r$.

Therefore, $\mathfrak{p}$ decomposes fully in K_g^+/K if and only if $\big(P_j(T), k\big(\sqrt[n]{B}\big)/k\big) = 1$ for $1 \le j \le r$ and $\xi^{(q^h-1)/n} = 1$. The last equality is equivalent to $n|h$ since the order of ξ in $\mathbb{F}_q^*$ is $q-1$ and $q \equiv 1 \bmod n$. □

References

[1] B. Anglès and J.–F. Jaulent, Théorie des genres des corps globaux, *Manuscripta Math.* **101**, no. 4, 513–532 (2000).

[2] R. Clement, The genus field of an algebraic function field, *J. Number Theory* **40**, no. 3, 359–375, (1992).

[3] A. Fröhlich, The genus field and genus group in finite number fields, *Mathematika* **6**, 40–46. (1959).

[4] A. Fröhlich, The genus field and genus group in finite number fields II, *Mathematika* **6**, 142–146. (1959).

[5] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörpern, *J. Math. Soc. Japan* **3**, 45–51, (1951).

[6] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, *Math. Nachr.* **9**, 351–362 (1953).

[7] M. Rzedowski–Calderón and G. Villa–Salvador, *Campos ciclotómicos numéricos y de funciones*, segunda versión, 2017, https://arxiv.org/abs/1407.3238.

Author information

Edgar Omar Curiel–Anaya, Departamento de Control Automático
Centro de Investigación y de Estudios Avanzados del I.P.N., México.
E-mail: edgaro78@hotmail.com

Myriam Rosalía Maldonado–Ramírez, Departamento de Matemáticas
Escuela Superior de Física y Matemáticas del Instituto Politécnico Nacional, México.
E-mail: mrmaldonador@ipn.mx

Martha Rzedowski–Calderón, Departamento de Control Automático
Centro de Investigación y de Estudios Avanzados del I.P.N., México.
E-mail: mrzedowski@ctrl.cinvestav.mx

Received: October 10, 2022.
Accepted: December 29, 2022.