Palestine Journal of Mathematics

Vol. 9(2)(2020) , 999–1019

GENUS FIELDS OF GLOBAL FIELDS

Elizabeth Ramírez–Ramírez, Martha Rzedowski–Calderón and Gabriel Villa–Salvador

Communicated by Jose Luis Lopez-Bonilla

MSC 2010 Classifications: Primary 11R58; Secondary 11R60, 11R29.

Keywords and phrases: Global fields, genus fields, extended genus fields.

Abstract In this paper we obtain the extended genus field of a global field. First we define the extended genus field of a global function field and we obtain, via class field theory, the description of the extended genus field of an arbitrary global function field. In the last part of the paper we use the techniques for function fields to describe the extended genus field of an arbitrary number field.

1 Introduction

The study of *narrow* or *extended genus fields* goes back to C.F. Gauss [8] who introduced the genus concept in the context of quadratic forms. During the first half of the last century, the concept was imported to quadratic number fields. H. Hasse [9] studied genus theory of quadratic number fields by means of class field theory. H.W. Leopoldt [11] generalized the work of Hasse by introducing the concept of genus field for a finite abelian extension of the rational field. Leopoldt studied extended genus fields using the arithmetic of abelian fields by means of *Dirichlet characters*. The first to introduce the concept of genus field and of extended genus field of a nonabelian finite extension of the rational field was A. Frölich who defined the concept of genus field of an arbitrary finite extension of $\mathbb{Q}$ [6, 7]. For a number field K, Frölich defined the genus field K (with respecto to the rational field $\mathbb{Q}$) as $K_{\mathfrak{ge}} := KF$ where $F/\mathbb{Q}$ is the maximum abelian extension such that KF/K is unramified everywhere. Similarly, the extended genus field is $K_{\mathfrak{gex}} = KL$ where $L/\mathbb{Q}$ is the maximum abelian extension such that KL/K is unramified at the finite primes. Numerous authors have studied genus fields and extended genus fields for finite field extensions $K/\mathbb{Q}$ over $\mathbb{Q}$.

In the case of number fields, the concepts of *Hilbert class field* and of *extended Hilbert class field* are defined without any ambiguity. The Hilbert class field K_H and the extended Hilbert class field K_{H^+} of a number field $K/\mathbb{Q}$ are defined as the maximum abelian unramified extension and the maximum abelian extension unramified at the finite primes of K, respectively. In this way, the concepts of genus field and of extended genus field are defined depending on the concept of the Hilbert class field, and of the extended Hilbert class field respectively. Namely, we have $K \subseteq K_{\mathfrak{ge}} \subseteq K_H$ and the Galois group $\mathrm{Gal}(K_H/K)$ is isomorphic to the class group Cl_K of K. The genus field $K_{\mathfrak{ge}}$ corresponds to a subgroup G_K of Cl_K and we have $\mathrm{Gal}(K_{\mathfrak{ge}}/K) \cong Cl_K/G_K$. The degree $[K_{\mathfrak{ge}} : K]$ is called the *genus number* of K and $\mathrm{Gal}(K_{\mathfrak{ge}}/K)$ is called the *genus group* of K. Similarly, $K \subseteq K_{\mathfrak{gex}} \subseteq K_{H^+}$ and $K_{\mathfrak{gex}}$ corresponds to a subgroup G_{K^+} of $\mathrm{Gal}(K_{\mathfrak{gex}}/K) \cong Cl_{K^+}$.

For global function fields the picture is different due to the fact that there are several concepts of Hilbert class field and of extended Hilbert class field, depending on which aspect you are interested in. The direct definition of the Hilbert class field K_H of a global function field K over $\mathbb{F}_q$ as the maximum unramified abelian extension of K has the disadvantage of being of infinite degree over K due to the extensions of constants. In the extensions of constants, every prime is eventually inert, so, if we are interested in a definition of a Hilbert class field of finite degree over the base field, we must impose some condition on the extension of constants. It seems that the first one to consider extended genus fields in the case of function fields was R. Clement in [5], where she considered the case of a cyclic tame extension $K/\mathbb{F}_q(T)$ of prime degree l different from the characteristic p of $\mathbb{F}_q$. She developed the theory along the lines of the case studied by

Hasse in [9]. Later on, S. Bae and J.K. Koo [3] generalized the results of Clement following the development given by Frölich. They defined the extended genus field for extensions of an arbitrary global function field K defining an analogue to the cyclotomic function field extensions of $\mathbb{F}_q(T)$ given by the Carlitz module.

M. Rosen defined in [15] the Hilbert class field of a global function field K as the maximum abelian unramified extension of K such that a fixed nonempty finite set of prime divisors of K decompose fully. Using this definition of Hilbert class field, G. Peng [14] found the genus field of a cyclic tame extension of prime degree over the rational function field $k = \mathbb{F}_q(T)$. His method used the analogue for function fields of the Conner–Hurrelbrink exact hexagon in number fields. The wild prime case was presented by S. Hu and Y. Li in [10] where they described explicitly the genus field of an Artin–Schreier extension of the rational function field. In [2, 12, 13] we developed a theory of genus fields using the same concept of Hilbert class field. In those papers, the ideas of Leopoldt using Dirichlet characters were strongly used.

In this paper we are interested in describing, using class field theory, the extended genus field of a finite separable extension of k. B. Anglès and J.-F. Jaulent in [1] established the general theory of extended genus fields of global fields, either function or numeric. We use a concept of extended genus field for function fields different from the one defined by Anglès and Jaulent. With this concept, when we describe the finite abelian extension L where $K_{\mathfrak{gex}} = KL$, we may write L as the composition of a sort of P–components, where P runs through the finite primes of k. We consider these P–components L_P as the composition of E_P, the P–component of the projection E of L in a cyclotomic function field given by the Carlitz module, and a field S which codifies the behavior of the infinite prime. More precisely, S codifies the wild ramification and the inertia of the infinite prime of k. To this end, we need to consider the idèle group corresponding to an arbitrary cyclotomic function field. Finally, we describe the field S.

It turns out, that the same approach works for number fields. Indeed, in the number field case, the problem is simpler because, by the Kronecker–Weber theorem, any abelian extension of $\mathbb{Q}$ is cyclotomic, that is, it is contained in a cyclotomic number field. In the function field case, the maximum abelian extension of k consists of three components: one cyclotomic, one of constants and one, also cyclotomic, where the infinite prime is totally and wildly ramified and it is the only ramified prime. In the number field case, the "p–components" can be found explicitly for $p \geq 3$ depending only on their degree over $\mathbb{Q}$. The case $p = 2$ does not depend only on its degree over $\mathbb{Q}$ since, for $n \geq 3$, the cyclotomic field $\mathbb{Q}(\zeta_{2^n})$ is not cyclic. We give a criterion to describe the 2–component of $K_{\mathfrak{gex}}$. Finally, we present some results on the behavior of the genus field of a composition. For number fields, a similar result was obtained by M. Bhaskaran in [4] and by X. Zhang [18].

2 Preliminaries and notations

We denote by $k = \mathbb{F}_q(T)$ the global rational function filed with field of constants the finite field of q elements $\mathbb{F}_q$. Let $R_T = \mathbb{F}_q[T]$ be the ring of polynomials, that is, the ring of integers of k with respect to the pole of T, the infinite prime $\mathfrak{p}_\infty$. Let $R_T^+ := \{P \in R_T \mid P \text{ is monic and irreducible}\}$. The elements of R_T^+ are the *finite primes* of k and $\mathfrak{p}_\infty$ is the *infinite prime* of k. For $N \in R_T$, Λ_N denotes the N–th torsion of the Carlitz module. A finite extension F/k will be called *cyclotomic* if there exists $N \in R_T$ such that $k \subseteq F \subseteq k(\Lambda_N)$.

Given a cyclotomic function field E, the group of Dirichlet characters X corresponding to E is the group X such that $X \subseteq \widehat{(R_T/\langle N\rangle)^*} \cong \widehat{\mathrm{Gal}(k(\Lambda_N)/k)} = \mathrm{Hom}\big((R_T/\langle N\rangle)^*, \mathbb{C}^*\big)$ and $E = k(\Lambda_N)^H$ where $H = \cap_{\chi\in X} \ker \chi$. For the basic results on Dirichlet characters, we refer to [17, §12.6].

For a group of Dirichlet characters X, let $Y = \prod_{P\in R_T} X_P$ where $X_P = \{\chi_P \mid \chi \in X\}$ and χ_P is the P–th component of χ: $\chi = \prod_{P\in R_T^+} \chi_P$. If E is the field corresponding to X, we define $E_{\mathfrak{gex}}$ as the field corresponding to Y. We have that $E_{\mathfrak{gex}}$ is the maximum unramified extension at the finite primes of E contained in a cyclotomic function field. The infinite prime $\mathfrak{p}_\infty$ might be ramified in $E_{\mathfrak{gex}}/k$ (see [12]).

Let $L_n = k(\Lambda_{1/T^{n+1}})^{\mathbb{F}_q^*}$, $n \in \mathbb{N} \cup \{0\}$ where $\mathbb{F}_q^* \subseteq \Big(R_{1/T}/\langle 1/T^{n+1}\rangle\Big)^*$, is isomorphic to the inertia group of the prime corresponding to T in $k\big(\Lambda_{1/T^{n+1}}\big)/k$. The prime $\mathfrak{p}_\infty$ is the only ramified prime in L_n/k and it is totally and wildly ramified. For $m \in \mathbb{N}$, and for any finite extension F/k, F_m denotes the extension of constants: $F_m = F\mathbb{F}_{q^m}$. In particular $k_m = \mathbb{F}_{q^m}(T)$.

Given a finite abelian extension K/k, there exist $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N}$ and $N \in R_T$ such that $K \subseteq L_n k(\Lambda_N) k_m =: {}_n k(\Lambda_N)_m$ (see [17, Theorem 12.8.31]). We define $M := L_n k_m$. In M/k no finite prime of k is ramified.

For any extension E/F of global fields and for any place $\mathfrak{P}$ of E and $\mathfrak{p} = \mathfrak{P} \cap F$, the ramification index is denoted by $e_{E/F}(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p})$ and the inertia degree is denoted by $f_{E/F}(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p})$. When the extension is Galois we denote $e_{\mathfrak{p}}(E|F) = e_{E/F}(\mathfrak{P}|\mathfrak{p})$ and $f_{\mathfrak{p}}(E|F) = f_{E/F}(\mathfrak{P}|\mathfrak{p})$. In particular for any abelian extension E/k, $e_P(E|k)$ and $f_P(E|k)$ denote the ramification index and the inertia degree of $P \in R_T^+$ in E/k respectively, and we denote by $e_\infty(E|k)$ and $f_\infty(E|k)$ the ramification index and the inertia degree of $\mathfrak{p}_\infty$ in E/k. The symbol $e_\infty^{\text{wild}}(E|F)$ denotes the wild ramification part of the infinite primes in E/F. Similarly, $I_{E/F}(\mathfrak{P}|\mathfrak{p})$ denotes the inertia group and $D_{E/F}(\mathfrak{P}|\mathfrak{p})$ the decomposition group.

For any finite separable extension K/k the *finite primes* of K are the primes over the primes P in R_T^+ and the *infinite primes* of K are the primes over $\mathfrak{p}_\infty$. The *Hilbert class field* K_H of K is the maximum abelian extension of K unramified at every finite prime of K and where all the infinite primes of K are fully decomposed. The *genus field* $K_{\mathfrak{ge}}$ of K/k is the maximum extension of K contained in K_H and such that it is the composite $K_{\mathfrak{ge}} = KF$ where F/k is abelian. We choose F the maximum possible. In other words, F is the maximum abelian extension of k contained in K_H.

Let K/k be a finite abelian extension. We know that $K_{\mathfrak{ge}} = KE_{\mathfrak{ge}}^H$ is the genus field of K where H is the decomposition group of the infinite primes in KE/K and $E := KM \cap k(\Lambda_N)$ (see [2]). We also know that $KE_{\mathfrak{ge}}/K_{\mathfrak{ge}}$ and KE/K are extensions of constants.

For a local field F with prime $\mathfrak{p}$, we denote by $F(\mathfrak{p}) \cong \mathbb{F}_q$ the residue field of F, $U_{\mathfrak{p}}^{(n)} = 1+\mathfrak{p}^n$ the n–th units of F, $n \in \mathbb{N} \cup \{0\}$.

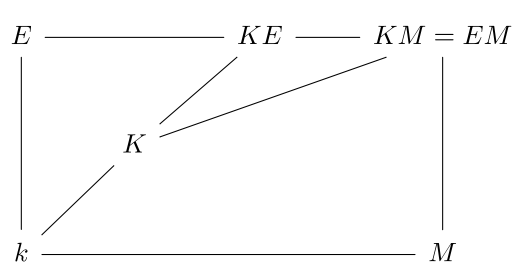
Let $\pi = \pi_F = \pi_{\mathfrak{p}}$ be a uniformizing element for $\mathfrak{p}$, that is, $v_{\mathfrak{p}}(\pi) = 1$. Then the multiplicative group of F satisfies $F^* \cong \langle \pi \rangle \times U_{\mathfrak{p}} \cong \langle \pi \rangle \times \mathbb{F}_q^* \times U_{\mathfrak{p}}^{(1)}$ as groups.

3 Extended genus field of a global function field

Let K/k be a finite abelian extension. Let $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N}$ and $N \in R_T$ be such that $K \subseteq {}_n k(\Lambda_N)_m$. Let $E = KM \cap k(\Lambda_N)$. Define *the extended genus field of* K as

$$K_{\mathfrak{gex}} := KE_{\mathfrak{gex}}.$$

Note that $K_{\mathfrak{gex}}/K$ is unramified at the finite primes since $E_{\mathfrak{gex}}/E$ is unramified at the finite primes, so that $KE_{\mathfrak{gex}}/KE$ is unramified at the finite primes and we also know that KE/K is unramified at the finite primes ([2]).



Now $KM = EM/E$ is ramified at most at the infinite prime $\mathfrak{p}_\infty$ and the inertia of $\mathfrak{p}_\infty$ in the extension $EM = KM/E$ is contained in M. Hence EM/E is unramified at the finite primes. The same holds for KM/K and we have $K \subseteq KE \subseteq KM = EM$. In short, $K_{\mathfrak{gex}}/K$ is unramified at the finite primes. We also have that $K_{\mathfrak{gex}}/K$ is tamely ramified at $\mathfrak{p}_\infty$ since $E_{\mathfrak{gex}}/k$ is tamely ramified at $\mathfrak{p}_\infty$ so that $KE_{\mathfrak{gex}}/K$ is tamely ramified at $\mathfrak{p}_\infty$ and $K_{\mathfrak{gex}} = KE_{\mathfrak{gex}}$.

We also have $[E_{\mathfrak{gex}} : E_{\mathfrak{ge}}^H] | q-1$ since $e_\infty(E_{\mathfrak{gex}}|E) | q-1$ where in general, for a finite abelian extension L/F, $e_\infty(L|F)$ denotes the ramification index of the infinite primes of F in L, and $H \subseteq I_\infty(E_{\mathfrak{gex}}|k)$, where in general $I_\infty(L|F)$ denotes the inertia group of the infinite primes in the Galois extension L/F. In other words, the infinite primes of $E_{\mathfrak{ge}}^H$ are fully ramified in the extension $E_{\mathfrak{ger}}/E_{\mathfrak{ge}}^H$. Thus we have

$$[E_{\mathfrak{ger}} : E_{\mathfrak{ge}}^H] = e_\infty(E_{\mathfrak{ger}}|E_{\mathfrak{ge}}^H)|e_\infty(k(\Lambda_N)|k) = q-1.$$

Therefore we have that $K_{\mathfrak{ger}} = KE_{\mathfrak{ger}}/KE_{\mathfrak{ge}}^H = K_{\mathfrak{ge}}$ is unramified at the finite primes, the infinite primes are tamely ramified, and $[K_{\mathfrak{ger}} : K_{\mathfrak{ge}}]|q-1$.

Now let K/k be a finite and separable extension. We define $K_{\mathfrak{ger}}$ as $KF_{\mathfrak{ger}}$ where $K_{\mathfrak{ge}} = KF$, that is, F is the maximum abelian extension of k contained in the Hilbert class field K_H of K (see [2]). Observe that $F_{\mathfrak{ge}} = F$.

Note that $[K_{\mathfrak{ger}} : K_{\mathfrak{ge}}]|[F_{\mathfrak{ger}} : F_{\mathfrak{ge}}]|q-1$ and the only possible ramified primes in $K_{\mathfrak{ger}}/K_{\mathfrak{ge}}$ are the infinite primes and they are tamely ramified.

Definition 3.1. For a finite separable extension K/k, we define the *extended genus field of* K as $K_{\mathfrak{ger}} = KF_{\mathfrak{ger}} = KL$ where $L = F_{\mathfrak{ger}}$. We stress that we choose F to be the maximum abelian extension of k such that $K_{\mathfrak{ge}} = KF$.

Remark 3.2. For a finite prime $P \in R_T^+$, the tame part of the ramification of P in $K_{\mathfrak{ger}}/k$ can be obtained in the following way. Let $d_P = \deg P$ and let $e_P(L|k) = e_P^{(0)} e_P^{(w)} = e^{\text{tame}}(P) e_P^{(w)}$ where $\gcd(p, e_P^{(0)}) = 1$ and $e_P^{(w)} = p^{\alpha_P}$ for some integer $\alpha_P \geq 0$. Since L/k is abelian, we have $e^{(0)}|q^{d_P} - 1$ (see [16, Proposición 10.4.8]).

Consider the extension $k_P^{(0)}/k$ where P is the only finite prime ramified, $k_P^{(0)} \subseteq L$ and $e_P^{(0)}|[k_P^{(0)} : k]$. Note that $[k(\Lambda_P) : k] = q^{d_P} - 1$. Then $Kk_P^{(0)} \subseteq K_{\mathfrak{ger}}$ and $Kk_P^{(0)}/K$ is unramfied at the finite primes. Thus, by Abhyankar Lemma,

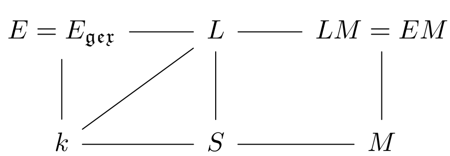
$$e_P(K|k) = e_P(Kk_P^{(0)}|k) = \text{lcm}[e_P(K|k), e_P(k_P^{(0)}|k)] = \text{lcm}[e_P(K|k), e_P^{(0)}]$$

Therefore $e_P^{(0)}|e_P(K|k)$. Since $e_P^{(0)}$ is the maximum with this property, it follows that

$$e^{\text{tame}}(P) = e_P^{(0)} = \gcd(q^{d_P} - 1, e_P(K|k)).$$

We now obtain $K_{\mathfrak{ger}} = KL$ where L satisfies $L_{\mathfrak{ger}} = L$, L/k abelian and L is the maximum with respect to this property. Let $L \subseteq {}_n k(\Lambda_N)_m$. If necessary, we may assume n, m, N are minimum, where $m \in \mathbb{N}$ is the conductor of constants (see [2]), $N \in R_T$ and $n \in \mathbb{N} \cup \{0\}$. In this situation we define *the conductor of* L as (m, N, n).

Let $E := LM \cap k(\Lambda_N)$. Then $EM = LM$ and $L_{\mathfrak{ger}} = L = E_{\mathfrak{ger}} L$ so that $E_{\mathfrak{ger}} \subseteq L$ and $E = E_{\mathfrak{ger}}$. In fact, $E_{\mathfrak{ger}} \subseteq L \subseteq LM = EM$, hence $E_{\mathfrak{ger}} M \subseteq EM$ and from the Galois correspondence, $E_{\mathfrak{ger}} \subseteq E$. Thus $E_{\mathfrak{ger}} = E$.



Let $S := L \cap M$. We have $S \subseteq M = L_n k_m$.

Let $X = Y = \prod_{P \in R_T^+} X_P$ be the group of Dirichlet characters associated to $E_{\mathfrak{ger}} = E$. Then if E_P is the field associated to X_P, with $P \in R_T^+$, $E = \prod_{P \in R_T^+} E_P$ where $E_P = k$ for almost all P and if $P_1, \ldots, P_r$ are the finite primes ramified in E/k, $X_{P_i} \neq \{1\}$, $E_{P_i} \neq k$, $E_{P_i} \cap \prod_{j \neq i} E_{P_j} = k$, $1 \leq i \leq r$ and $E = E_{P_1} \cdots E_{P_r}$, $\widehat{\text{Gal}(E/k)} \cong X = Y = \prod_{P \in R_T^+} X_P = \prod_{P \in R_T^+} \widehat{\text{Gal}(E_P/k)} \cong \prod_{i=1}^r \widehat{\text{Gal}(E_{P_i}/k)}$. Thus

$$\text{Gal}(E/k) \cong \prod_{i=1}^r \text{Gal}(E_{P_i}/k).$$

For any nonempty finite subset $\mathcal{A} \subseteq R_T^+$, we define $E_{\mathcal{A}} := \prod_{P\in\mathcal{A}} E_P$. We may consider E_P as the "P–th primary component" of E.

$$\begin{array}{ccccc}
E = \prod_{P\in R_T^+} E_P = E_{\mathfrak{ger}} & \text{———} & L = ES & \text{———} & LM = EM \\
| & & | & & | \\
E_P & \text{———} & L_P = E_P S & \text{———} & L_P M = E_P M \\
| & & | & & | \\
k & \text{———} & S = L\cap M & \text{———} & M
\end{array}$$

We define $L_P := E_P M \cap L$. We have that $E_P \subseteq E \subseteq L$ and $E_P \subseteq E_P M$. Therefore $E_P \subseteq L_P$. From the Galois correspondence, we have

$$L_P = E_P S.$$

For any nonempty finite subset $\mathcal{A} \subseteq R_T^+$, we let $L_{\mathcal{A}} := E_{\mathcal{A}} M \cap k(\Lambda_N)$. From the Galois correspondence we obtain $L_{\mathcal{A}} = E_{\mathcal{A}} S$ and in particular

$$L_{\mathcal{A}} = \Big(\prod_{P\in\mathcal{A}} E_P\Big) S = \prod_{P\in\mathcal{A}} (E_P S) = \prod_{P\in\mathcal{A}} L_P.$$

We have

Proposition 3.3. *For any $A, B \in R_T \setminus \{0\}$, let $L_A := E_A M \cap L$, where $E_A := \prod_{\substack{P|A\\ P\in R_T^+}} E_P$, that is, $E_A = E_{\mathcal{A}}$ and $L_A = L_{\mathcal{A}}$, where $\mathcal{A} = \{P \in R_T^+ \mid P|A\}$. Then we have*

$$L_{AB} = L_A L_B.$$

Furthermore, if $\gcd(A,B) = 1$ *we have $L_A \cap L_B = S = L \cap M$.*

Proof. It remains to consider the case $\gcd(A,B) = 1$. We have $E_A = \prod_{P|A} E_P$, $E_B = \prod_{P|B} E_P$ and $\{P \in R_T^+ \mid P|A\} \cap \{P \in R_T^+ \mid P|B\} = \emptyset$. Therefore $E_A \cap E_B = k$ and $kL \cap M = L \cap M = S$. The result follows from the Galois correspondence. □

Now, for $P \in R_T^+$, $L_P = E_P M \cap L \supseteq M \cap L = S$ and $L_P \neq S \iff P \in \{P_1, \ldots, P_r\}$. In fact, $L_P = E_P M \cap L \neq S \iff E_P M \neq M \iff E_P \neq k \iff P \in \{P_1, \ldots, P_r\}$.

Finally, $E = \prod_{P\in R_T^+} E_P = \prod_{i=1}^r E_{P_i}$. Therefore, since $EM = LM$, in particular $L \subseteq EM$. We have

$$\begin{aligned} L = EM \cap L = \Big(\prod_{i=1}^r E_{P_i}\Big) M \cap L = \prod_{i=1}^r (E_{P_i} M \cap L) = \prod_{i=1}^r L_{P_i} \\ = \prod_{i=1}^r L_{P_i} \cdot \prod_{P\notin\{P_1,\ldots,P_r\}} S = \prod_{P\in R_T^+} L_P. \end{aligned}$$

Thus

$$L = \prod_{i=1}^r L_{P_i} = \prod_{P\in R_T^+} L_P.$$

We have proved

Theorem 3.4. *For $A \in R_T$, we define $L_A = E_A M \cap L$. Let $S = L \cap M$. We have*

(1) *For all $A, B \in R_T$, $L_{AB} = L_A L_B$.*

(2) $L_A \supseteq S$ *for all* $A \in R_T$ *and* $L_A = S \iff P_i \nmid A$ *for all* $1 \le i \le r$.

(3) $L_A \cap L_B = S$ *for all* $A, B \in R_T$ *such that* $\gcd(A, B) = 1$.

(4) $L = \prod_{P \in R_T^+} L_P = \prod_{i=1}^{r} L_{P_i}$. □

In order to compute L we need to know S, that is, the behavior of $\mathfrak{p}_\infty$, and also each E_P for $P \in R_T^+$. First, we have that if $P \in R_T^+$ is unramified in K/k, then P is unramified in E/k and therefore in L/k. Indeed, if P were ramified in L/k, then we would have

$$e_P(KL|K) = e_P(KL|K)e_P(K|k) = e_P(KL|k) = e_P(KL|L)e_P(L|k) > 1$$

so that $e_P(KL|K) > 1$ contrary to the definition of L.

$$\begin{array}{ccc} K & \text{——} & KL \\ | & & | \\ k & \text{——} & L \end{array}$$

Thus, it suffices to know E_{P_i}, $1 \le i \le r$ where $P_1, \ldots, P_r$ are the finite primes ramified in K/k and therefore these are the only possible finite primes ramified in E/k and in L/k. Now, in E_P/k the only finite prime ramified is P and $\mathfrak{p}_\infty$ is tamely ramified. Note that the tame ramification index of $\mathfrak{p}_\infty$ in E/k and in L/k is the same. This is a consequence of $L = ES$.

In general we consider an arbitrary global function field F. Let J_F be the idèle group of F and let $C_F = J_F/F^*$ be the idèle class group of F. To find E_P for $P \in \{P_1, \ldots, P_r\}$, we must find the idèle subgroup of J_k corresponding to E_P. Now, since E_P is cyclotomic and P is the only finite prime ramified, there exists $t \in \mathbb{N}$ such that $E_P \subseteq k(\Lambda_{P^t})$. Therefore, the idèle group corresponding to E_P contains the idèle group corresponding to $k(\Lambda_{P^t})$.

Theorem 3.5. *Let* $N \in R_T$, $N = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ *with* $P_1, \ldots, P_r \in R_T^+$ *distinct. Set* $R_T' := R_T^+ \setminus \{P_1, \ldots, P_r\}$. *Then, the idèle group corresponding to* $k(\Lambda_N)$ *is*

$$\mathcal{X}_N = \prod_{i=1}^{r} U_{P_i}^{(\alpha_i)} \times \prod_{P \in R_T'} U_P \times [(\pi) \times U_\infty^{(1)}],$$

where $\pi = 1/T$ *is a uniformizing element for* $\mathfrak{p}_\infty$.

Proof. Let $U' := \prod_{Q \in R_T^+} U_Q \times [(\pi) \times U_\infty^{(1)}]$. We will give an epimorphism

$$\psi_N \colon U' \longrightarrow \operatorname{Gal}(k(\Lambda_N)/k) =: G_N$$

such that $\ker \psi_N = \mathcal{X}_N$ and hence, $U'/\mathcal{X}_N \cong G_N$.

Let $\vec{\xi} \in U'$. Then $\xi_{P_i} \in U_{P_i} = \{\sum_{j=0}^{\infty} a_j P_i^j \mid a_j \in R_T/\langle P_i \rangle\}$, $1 \le i \le r$. Since k is dense in the local field k_{P_i}, there exists $Q_i \in R_T$ such that $Q_i \equiv \xi_{P_i} \bmod P_i^{\alpha_i}$. By the Chinese Residue Theorem, we have that there exists $C \in R_T$ such that $C \equiv Q_i \bmod P_i^{\alpha_i}$, $1 \le i \le r$ and so $C \equiv \xi_{P_i} \bmod P_i^{\alpha_i}$, $1 \le i \le r$

Now, if $C_1 \in R_T$ satisfies $C_1 \equiv \xi_{P_i} \bmod P_i^{\alpha_i}$, $1 \le i \le r$, we have that $P_i^{\alpha_i} | C - C_1$ for $1 \le i \le r$. It follows that $N | C - C_1$ and thus $C \in R_T$ is unique modulo N. On the other hand, $v_{P_i}(\xi_{P_i}) = 0$, so that $P_i \nmid \xi_{P_i}$ and so we obtain that $\gcd(C, N) = 1$. In this way we have that $C \bmod N$ defines an element of $G_N = \operatorname{Gal}(k(\Lambda_N)/k)$.

Given $\sigma \in G_N$, there exists $C \in R_T$ such that $\sigma\lambda_N = \lambda_N^C$ where λ_N is a generator de Λ_N. Let $\vec{\xi} \in U'$ with $\xi_{P_i} = C$, $1 \le i \le r$ and $\xi_P = 1 = \xi_\infty$ for all $P \in R_T'$. Therefore $\vec{\xi} \mapsto C \bmod N$ and ψ_N is onto. Finally, $\ker \psi_N = \{\vec{\xi} \in U' \mid \xi_{P_i} \equiv 1 \bmod P_i^{\alpha_i}, 1 \le i \le r\} = \mathcal{X}_N$. So we have that ψ_N is an epimorphism and $\ker \psi_N = \mathcal{X}_N$.

We will show that $U'/\mathcal{X}_N \cong J_k/\mathcal{X}_N k^*$. We have the composition

$$U' \hookrightarrow J_k \twoheadrightarrow J_k/\mathcal{X}_N k^*, \quad \mu \colon U' \to J_k/\mathcal{X}_N k^*$$

with $\operatorname{im}\mu = U'\mathcal{X}_N k^*/\mathcal{X}_N k^*$ and $\ker\mu = U' \cap \mathcal{X}_N k^*$.

Now, $\mathcal{X}_N \subseteq U'$ so that $\mathcal{X}_N \subseteq U' \cap \mathcal{X}_N k^*$. Conversely, if $\vec{\xi} \in U' \cap \mathcal{X}_N k^*$, the components of $\vec{\xi}$ are given as

$$\xi_P = a \cdot \beta_P, \quad P \in R_T, \quad \vec{\beta} \in \mathcal{X}_N, \quad a \in k^*,$$

$$\xi_\infty = a \cdot \beta_\infty, \quad \beta_\infty \in (\pi) \times U_\infty^{(1)}.$$

Since $\xi_P, \beta_P \in U_P$ we have $v_P(\xi_P) = v_P(\beta_P) = 0$ for all $P \in R_T$. It follows that $v_P(a) = 0$ for all $P \in R_T$. Furthermore, since $\deg a = 0$ we have $v_\infty(a) = 0$ and so $a \in \mathbb{F}_q^*$.

Now $\xi_\infty, \beta_\infty \in (\pi) \times U_\infty^{(1)} = \ker\phi_\infty$, where $\phi_\infty \colon k_\infty^* \longrightarrow \mathbb{F}_q^*$ is the sign function of k_∞^* defined as $\phi_\infty(\lambda\pi^n u) = \lambda$ where $\lambda \in \mathbb{F}_q^*$, $n \in \mathbb{N}$ and $u \in U_\infty^{(1)}$. Thus $1 = \phi_\infty(\xi_\infty) = \phi_\infty(a)\phi_\infty(\beta_\infty) = \phi_\infty(a)$ and so $a = 1$. It follows that $\vec{\xi} \in \mathcal{X}_N$. Therefore $\ker\mu = \mathcal{X}_N$ and we obtain a monomorphism $U'/\mathcal{X}_N \overset{\theta}{\hookrightarrow} J_k/\mathcal{X}_N k^*$.

It remains to prove that θ is surjective. So, we must prove that $J_k = U'\mathcal{X}_N k^* = U'k^*$. We have that U' corresponds to the maximum unramified extension at every finite prime. Let L/k be this extension. Since $U_\infty^{(1)}$ corresponds to the first ramification group, and in this way it corresponds to the wild ramification of $\mathfrak{p}_\infty$, it follows that in L/k there is at most a ramified prime ($\mathfrak{p}_\infty$), being tamely ramified and of degree 1. From [16, Proposición 10.4.11], we obtain that L/k is an extension of constants.

Finally, since $1 = \min\{n \in \mathbb{N} \mid \deg\vec{\alpha} = n, \vec{\alpha} \in U'\}$, the field of constants of L is $\mathbb{F}_q$ (see [16, Teorema 17.8.6]) and therefore $L = k$. It follows that $C_k \cong U'$, that is, $J_k/k^* \cong U'$ and thus $J_k = U'k^*$. □

Corollary 3.6. *With the above notations, we have that for a cyclotomic field $k \subseteq F \subseteq k(\Lambda_N)$, the idèle group corresponding to F is of the form $R_F \times \prod_{Q\in R'_T} U_Q \times [(\pi) \times U_\infty^{(1)}]$ with R_F a group satisfying $\prod_{i=1}^r U_{P_i}^{(\alpha_i)} \subseteq R_F \subseteq \prod_{i=1}^r U_{P_i}$.*

Proof. Let Δ be the idèle group corresponding to F. Thus $\Delta \supseteq \mathcal{X}_N$. Now

$$\frac{\prod_{i=1}^r U_{P_i}}{\prod_{i=1}^r U_{P_i}^{(\alpha_i)}} \cong \big(R_T/\langle N\rangle\big)^* \cong \operatorname{Gal}(k(\Lambda_N)/k).$$

Therefore $\operatorname{Gal}(k(\Lambda_N)/F) \cong \frac{\Theta}{\prod_{i=1}^r U_{P_i}^{(\alpha_i)}} < \operatorname{Gal}(k(\Lambda_N)/k)$ for a group $\Theta \subseteq \prod_{i=1}^r U_{P_i}$. The group Θ corresponds to R_F. The result follows. □

Corollary 3.7. *Let $P \in R_T^+$. Then the idèle group corresponding to E_P is of the form*

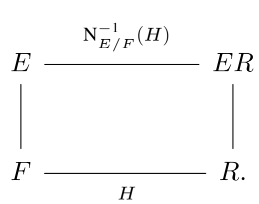
$$\Delta_P = H_P \times \prod_{\substack{Q\neq P\\ Q\in R_T^+}} U_Q \times [(\pi) \times U_\infty^{(1)}],$$

where $U_P^{(t)} \subseteq H_P \subseteq U_P$ for some $t \in \mathbb{N}$.

Proof. Since E_P is cyclotomic and the only finite prime ramified is P, there exists $t \in \mathbb{N}$ such that $E_P \subseteq k(\Lambda_{P^t})$. The result follows from Corollary 3.6 □

For each $P \in R_T^+$, k_P denotes the completion of k at P and k_∞ denotes the completion of k at $\mathfrak{p}_\infty$. We recall the following result of class field theory.

Theorem 3.8. *Let F be a global field and let R/F be the class field extension corresponding to H, that is, H is the open subgroup of C_F such that $H = \mathrm{N}_{R/F}\, C_R$ and $\operatorname{Gal}(R/F) \cong C_F/H$. Let E/F be a finite separable extension. Then ER/E is the class field extension corresponding to the subgroup $\mathrm{N}_{E/F}^{-1}(H)$ of C_E.*



Proof. We have that if E/F and E'/F' are two finite abelian extensions of global fields with $F \subseteq F'$ and $E \subseteq E'$ of global fields, and if $\psi_{E/F}$ denotes the Artin map of the extension E/F then we have the following commutative diagram

$$\begin{array}{ccc} C_{F'} & \xrightarrow{\psi_{E'/F'}} & \mathrm{Gal}(E'/F') \\ \downarrow {\scriptstyle \mathrm{N}_{F'/F}} & & \downarrow {\scriptstyle \text{rest}} \\ C_F & \xrightarrow[\psi_{E/F}]{} & \mathrm{Gal}(E/F) \end{array}$$

where rest denotes the restriction map (see [16, Proposición 17.6.39]).

We apply this result to our situation, that is, we have the commutative diagram

$$\begin{array}{ccc} C_{E} & \xrightarrow{\psi_{ER/E}} & \mathrm{Gal}(ER/E) \\ \downarrow {\scriptstyle \mathrm{N}_{E/F}} & & \downarrow {\scriptstyle \text{rest}} \\ C_F & \xrightarrow[\psi_{R/F}]{} & \mathrm{Gal}(R/F) \end{array}$$

Let $\psi_{ER/E}\colon C_E \longrightarrow \mathrm{Gal}(ER/E)$ be the Artin map. The norm group corresponding to ER/E is $\ker \psi_{ER/E}$, that is, $C_E/\ker \psi_{ER/E} \cong \mathrm{Gal}(ER/E)$. Now the restriction map is injective and we have

$$\text{rest} \circ \psi_{ER/E} = \psi_{R/F} \circ \mathrm{N}_{E/F}\,.$$

Therefore

$$\begin{gathered} \vec{x} \in \ker \psi_{ER/E} \iff \psi_{ER/E}(\vec{x}) = 1 \iff \\ \iff \text{rest} \circ \psi_{ER/E}(\vec{x}) = 1 = \psi_{R/F} \circ \mathrm{N}_{E/F}(\vec{x}) \iff \\ \iff \mathrm{N}_{E/F}(\vec{x}) \in \ker \psi_{R/F} = H \iff \vec{x} \in \mathrm{N}_{E/F}^{-1}(H). \end{gathered}$$

□

We apply Theorem 3.8 to the diagram

$$\begin{array}{ccc} K & \text{———} & KE_P \\ | & & | \\ k & \text{———} & E_P \end{array}$$

that is, KE_P is the class field of $\mathrm{N}_{K/k}^{-1}(\Delta_P)$. Since E_P is maximum in the sense that P is the only finite prime ramified in E_P/k and KE_P/K unramified at every finite prime, we have that Δ_P satisfies

$$\mathrm{N}_{K/k}^{-1}(\Delta_P) \subseteq \prod_{Q \in R_T^+} \prod_{\mathfrak{p}|Q} U_{\mathfrak{p}} \times \prod_{\mathfrak{P}_\infty | \mathfrak{p}_\infty} K_{\mathfrak{P}_\infty}^* \subseteq J_K,$$

or, equivalently,

$$\Delta_P \subseteq \mathrm{N}_{K/k}\Big(\prod_{Q \in R_T^+} \prod_{\mathfrak{p}|Q} U_{\mathfrak{p}} \times \prod_{\mathfrak{P}_\infty | \mathfrak{p}_\infty} K_{\mathfrak{P}_\infty}^* \Big).$$

Let $\vec{\alpha} \in \prod_{Q\in R_T^+}\prod_{\mathfrak{p}|Q} U_{\mathfrak{p}} \times \prod_{\mathfrak{P}_\infty|\mathfrak{p}_\infty} K_{\mathfrak{P}_\infty}^*$, $\vec{\alpha} = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$. Then

$$\mathrm{N}_{K/k}\,\vec{\alpha} = \prod_{Q\in R_T^+}\Big(\prod_{\mathfrak{p}|Q}\mathrm{N}_{K_{\mathfrak{p}}/k_Q}\,\alpha_{\mathfrak{p}}\Big)\cdot\prod_{\mathfrak{P}_\infty|\mathfrak{p}_\infty}\mathrm{N}_{K_{\mathfrak{P}_\infty}/k_\infty}\,\alpha_{\mathfrak{P}_\infty}.$$

For $Q \neq P$, Q is unramified in L_P/k, therefore, for $\mathfrak{Q}|Q$, $K_{\mathfrak{Q}}/k_Q$ is unramified and in particular it is a cyclic extension. Then $\mathrm{N}_{K_{\mathfrak{Q}}/k_Q}\,U_{\mathfrak{Q}} = U_Q$ (see [16, Teorema 17.2.17]).

For $Q = P$, we have

$$\prod_{\mathfrak{p}|P}\mathrm{N}_{K_{\mathfrak{p}}/k_P}\,\alpha_{\mathfrak{p}} = \prod_{j=1}^{m_P}\mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,\alpha_{\mathfrak{p}_j},$$

where $\mathrm{con}_{k/K}\,P = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_{m_P}^{e_{m_P}}$.

It follows that $\prod_{j=1}^{m_P}\mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,\alpha_{\mathfrak{p}_j} \in H_P$. In other words, if

$$S_j := \mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j} \times \prod_{\substack{Q\in R_T^+\\ Q\neq P}} U_Q \times [(\pi)\times U_\infty^{(1)}] \subseteq U_P \times \prod_{\substack{Q\in R_T^+\\ Q\neq P}} U_Q \times [(\pi)\times U_\infty^{(1)}],$$

we have

$$\Delta_P = \prod_{j=1}^{m_P} S_j \quad \text{and} \quad H_P = \prod_{j=1}^{m_P}\mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j}.$$

Now, if S_j is the norm group of the field $R_j \subseteq {}_nk(\Lambda_{P^{c_j}})_m$ for some $n \in \mathbb{N}\cup\{0\}, m \in \mathbb{N}$ and $c_j \in \mathbb{N}$, then $\prod_{j=1}^{m_P} S_j$ is the norm group of $\cap_{j=1}^{m_P} R_j$.

It follows that $[C_k : k^* S_j] = [U_P : \mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j}]$ and $\mathrm{Gal}(R_j/k) \cong C_k/k^*S_j$. Therefore $[R_j : k] = [C_k : k^*S_j] = [U_P : \mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j}]$. Finally, we have

$$E_P = \bigcap_{j=1}^{m_P} R_j, \quad [E_P : k] = \Big[\bigcap_{j=1}^{m_P} R_j : k\Big] = \Big[U_P : \prod_{j=1}^{m_P}\mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j}\Big].$$

We have proved our main result.

Theorem 3.9. *Let K/k be a finite and separable extension, where $k = \mathbb{F}_q(T)$. With the notations as above, let $K_{\mathfrak{gex}} = KL$. Then $L = \prod_{P\in R_T^+} L_P$ where $L_P = E_P S$, $S = L\cap M$ and $k \subseteq E_P \subseteq k(\Lambda_{P^{c_P}})$ corresponds to $\prod_{j=1}^{m_P}\mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j}$. In particular*

$$[E_P : k] = \Big[U_P : \prod_{j=1}^{m_P}\mathrm{N}_{K_{\mathfrak{p}_j}/k_P}\,U_{\mathfrak{p}_j}\Big],$$

where $\mathrm{con}_{k/K}\,P = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_{m_P}^{e_{m_P}}$.

The tamely ramified part of L_P/k is given by

$$e^{\text{tame}}(P) = \gcd(e_1,\ldots,e_{m_P}, q^{d_P}-1),$$

with $d_P = \deg_k P$. □

3.1 The field S

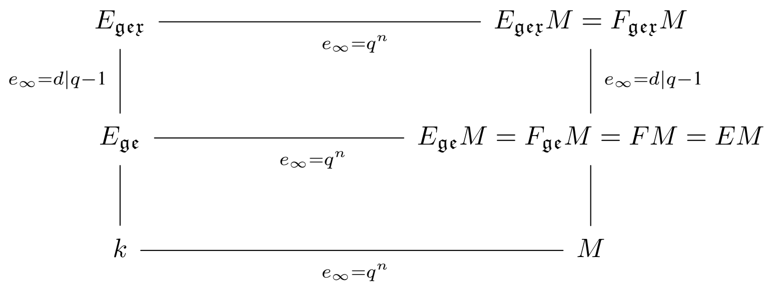
To study S, recall that for a finite extension K/k, the genus field is $K_{\mathfrak{ge}} = KF$ where F/k is the maximum abelian extension contained in the Hilbert class field and the extended genus field is $K_{\mathfrak{gex}} = KL$, where L satisfies $L_{\mathfrak{gex}} = L$, L/k is abelian and L is the maximum with respecto to this property. We have $F_{\mathfrak{ge}} = F$, $L = F_{\mathfrak{gex}}$ and $L_{\mathfrak{gex}} = L$. Let $L \subseteq {}_nk(\Lambda_N)_m$ with (m, N, n) the conductor of L. Then $M = L_n k_m$ and $S = L\cap M$.

Proposition 3.10. *We have that L/F is totally ramified at the infinite primes, unramified at the finite primes and $[L : F]|q-1$. In particular, L/F is tamely ramified.*

Proof. We have that F/k is abelian. Let $F \subseteq {}_nk(\Lambda_N)_m$ and $E = FM \cap k(\Lambda_N)$. Then $E_{\mathfrak{ge}}M = F_{\mathfrak{ge}}M = FM = EM$ (see [2]) and therefore $E_{\mathfrak{ge}} = E$.

Since $e_\infty(E_{\mathfrak{gex}}|E_{\mathfrak{ge}})|q-1$ and $e_\infty(M|k) = q^n$, it follows that

$$e_\infty(E_{\mathfrak{gex}}M|E_{\mathfrak{ge}}M) = e_\infty(E_{\mathfrak{gex}}|E_{\mathfrak{ge}}) = [E_{\mathfrak{gex}} : E_{\mathfrak{ge}}].$$



Hence,

$$\begin{aligned} e_\infty(F_{\mathfrak{gex}}|F_{\mathfrak{ge}}) &= e_\infty(F_{\mathfrak{gex}}M|F_{\mathfrak{ge}}M) = e_\infty(E_{\mathfrak{gex}}M|E_{\mathfrak{ge}}M) \\ &= [E_{\mathfrak{gex}} : E_{\mathfrak{ge}}] = [E_{\mathfrak{gex}}F : E_{\mathfrak{ge}}F] = [F_{\mathfrak{gex}} : F_{\mathfrak{ge}}]. \end{aligned}$$

So, the infinite primes are total and tamely ramified in $L = F_{\mathfrak{gex}}/F_{\mathfrak{ge}} = F$.

On the other hand, $E_{\mathfrak{gex}}/E_{\mathfrak{ge}}$ is unramified at the finite primes, thus $E_{\mathfrak{gex}}F = F_{\mathfrak{gex}} = L/F = F_{\mathfrak{ge}} = E_{\mathfrak{ge}}F$ is unramified at the finite primes. □

Proposition 3.11. *We have*

$$e_\infty^{wild}(L|k) = e_\infty^{wild}(F|k) = e_\infty^{wild}(S|k) = e_\infty(S|k).$$

Furthermore, $S = L \cap M = F \cap M$.

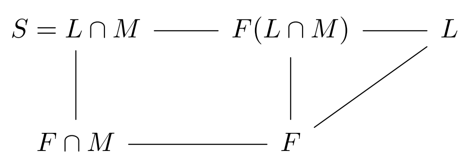
Proof. We have $e_\infty^{\text{wild}}(L|k) = e_\infty^{\text{wild}}(L|K) = e_\infty^{\text{wild}}(L|F)e_\infty^{\text{wild}}(F|k) = e_\infty^{\text{wild}}(F|k)$.

By the definition of S, we have $e_\infty^{\text{wild}}(S|k) = e_\infty(S|k)$ since $e_\infty(S|k)|q^n$. Now, $L = E_{\mathfrak{gex}}S$, $E_{\mathfrak{gex}} \cap S = k$ and $e_\infty^{\text{wild}}(E_{\mathfrak{gex}}|k) = 1$. Therefore

$$e_\infty^{\text{wild}}(L|k) = e_\infty^{\text{wild}}(E_{\mathfrak{gex}}S|S)e_\infty^{\text{wild}}(S|k) = e_\infty^{\text{wild}}(S|k)$$

since $e_\infty^{\text{wild}}(E_{\mathfrak{gex}}S|S)|e_\infty^{\text{wild}}(E_{\mathfrak{gex}}|k) = 1$.

We have $F \cap M \subseteq L \cap M = S$ and $F \cap (L \cap M) = F \cap M$.



It follows that $[L \cap M : F \cap M] = [F(L \cap M) : F] | [L : F] | q-1$. We have that L/F is totally ramified at the infinite primes and therefore $F(L \cap M)/F$ is also fully ramified at the infinite primes. It follows that $S = L \cap M/F \cap M$ is fully ramified at the infinite primes (see [16, Corolario 10.4.15]). Thus, $[S : F \cap M]|q^n$ and $[S : F \cap M]|q-1$ so that $[S : F \cap M] = 1$ and $F \cap M = L \cap M$. □

Proposition 3.12. *The field of constants of* S*, of* L *and of* F *is the same.*

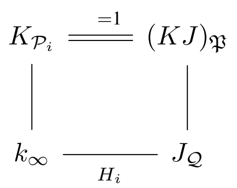
Proof. If $\mathbb{F}_{q^{t_0}}$ is the field of constants of L then $\mathbb{F}_{q^{t_0}} \subseteq S = L \cap M$ and since $S \subseteq F \subseteq L$, the result follows. □

Proposition 3.13. *Let* $\operatorname{con}_{k/K} \mathfrak{p}_\infty = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$ *and let* $t_i = \deg_K(\mathcal{P}_i)$*. Then the field of constants of* $K_{\mathfrak{ge}}$ *is* $\mathbb{F}_{q^{t_0}}$*, where* $t_0 = \gcd(t_1, \ldots, t_r)$.

Proof. See [13]. □

Corollary 3.14. *The field of constants of S, L and F is $\mathbb{F}_{q^{t_0}}$.* □

Now we consider a finite abelian extension J/k such that KJ/K is unramified and the infinite primes decompose fully. Let $\mathfrak{P}|\mathfrak{p}_\infty$ be a prime divisor of KJ, $\mathfrak{P} \cap K = \mathcal{P}_i$ for some $1 \le i \le r$ and $\mathfrak{P} \cap J = \mathfrak{Q}$. Taking the completions we have



Let $H_i := \mathrm{N}_{J_{\mathcal{Q}}/k_\infty} J_{\mathcal{Q}}^*$, that is, H_i is the norm group of $J_{\mathcal{Q}}$. Therefore, the norm group corresponding to $(KJ)_{\mathfrak{P}} = K_{\mathcal{P}_i}$ is $\mathrm{N}^{-1}_{K_{\mathcal{P}_i}/k_\infty}(H_i)$ (see Theorem 3.8). Hence $\mathrm{N}^{-1}_{K_{\mathcal{P}_i}/k_\infty}(H_i) = K^*_{\mathcal{P}_i}$. That is, $H_i = \mathrm{N}_{K_{\mathcal{P}_i}/k_\infty}(K^*_{\mathcal{P}_i})$. The maximum global abelian extension J/k satisfying that KJ/K is unramified and the infinite primes decompose fully, satisfies, locally at ∞, that its norm gorup is

$$\prod_{i=1}^r H_i = \prod_{i=1}^r \mathrm{N}_{K_{\mathcal{P}_i}/k_\infty}(K^*_{\mathcal{P}_i}).$$

In this way, if R/k_∞ is the maximum abelian extension with $(KR)_{\mathfrak{P}} = K_{\mathcal{P}_i}$ for some i. Thus R corresponds to $\prod_{i=1}^r H_i$, that is, $\mathrm{Gal}(R/k_\infty) = k^*_\infty/(\prod_{i=1}^r H_i)$ and $[R : k_\infty] = [k^*_\infty : \prod_{i=1}^r H_i]$.

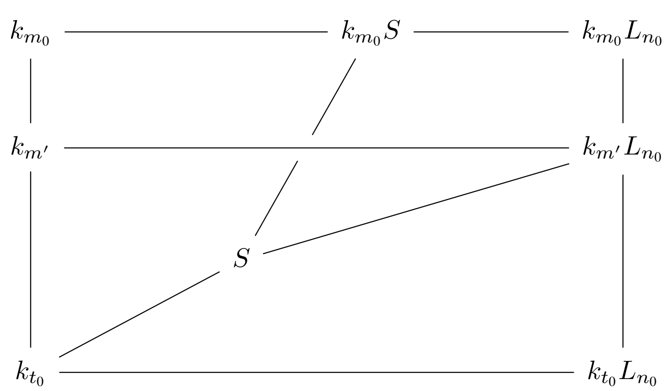
Let $[R : k_\infty] = p^\alpha a$ with $\alpha \in \mathbb{N} \cup \{0\}$ and $p \nmid a$. Since S is the maximum abelian extension of k such that the only ramified prime is $\mathfrak{p}_\infty$, it is fully ramified and $S \subseteq L$, and since $f_\infty(L|S) = 1$, it follows that if $\mathcal{P}_\infty$ is the only prime in S dividing $\mathfrak{p}_\infty$ (recall that the number of primes in S that lie above $\mathfrak{p}_\infty$ is $h_\infty(S|k) = 1$), then $[S_{\mathcal{P}_\infty} : k_\infty] = [S : k] = p^\alpha$. In particular, the norm group corresponding to $S_\infty = S_{\mathcal{P}_\infty}$ in k_∞ is the group $\mathfrak{G} \supseteq \prod_{i=1}^r H_i$, which is the minimum such that $[k^*_\infty : \mathfrak{G}] = p^\alpha$ is a p–group.

The conductor $\mathfrak{p}_\infty^{n_0}$ of S_∞ is such that n_0 is the minimum nonnegative integer such that $U_\infty^{(n_0)} \subseteq \mathfrak{G}$. The conductor of constants m_0 of S, that is, m_0 is the minimum natural number such that $S \subseteq k_{m_0} L_{n_0}$ is given as follows (see [2]). Let $t = f_\infty(S|k)$, $d^* = f_\infty(R'S|S)$ where $R' = S_{m_0} \cap L_{n_0}$ and $d^* = e_\infty(S|F')$ where $F' = S \cap {}_{n_0}k(\Lambda_1) = S \cap L_{n_0}$. Therefore

$$m_0 = f_\infty(S|k) e_\infty(S|S \cap L_{n_0}).$$

Proposition 3.15. *Let $f_\infty(S|k) = t$. Then $\mathbb{F}_{q^t}$ is the field of constants of S. That is, $t = t_0$.*

Proof. We have $\mathbb{F}_{q^{t_0}}(T) = k_{t_0} \subseteq S$. Let m_0, n_0 be minimum such that $S \subseteq k_{m_0} L_{n_0}$. Then $S \cap k_{m_0} = k_{t_0}$.



We have $Sk_{t_0}L_{n_0} = SL_{n_0}$, $k_{t_0}L_{n_0} \subseteq SL_{n_0} \subseteq k_{m_0}L_{n_0}$. Let $SL_{n_0} \cap k_{m_0} = k_{m'}$. From the Galois correspondence we obtain that $k_{m'}k_{t_0}L_{n_0} = k_{m'}L_{n_0} = SL_{n_0} \supseteq S$. It follows that $m' \ge m_0$. Hence $m' = m_0$ and $SL_{n_0} = k_{m_0}L_{n_0}$.

Now $e_\infty(k_{m_0}L_{n_0}|k_{t_0}) = q^n$ and $k_{m_0} \subseteq k_{m_0}S \subseteq k_{m_0}L_{n_0}$. Then

$$e_\infty(k_{m_0}L_{n_0}|S) = e_\infty(k_{m_0}L_{n_0}|k_{m_0}S) = \frac{q^{n_0}}{[k_{m_0}S : k_{m_0}]} = \frac{q^{n_0}}{[S : S \cap k_{m_0}]} = \frac{q^{n_0}}{[S : k_{t_0}]}.$$

Thus

$$e_\infty(S|k_{t_0}) = \frac{e_\infty(k_{m_0}L_{n_0}|k_{t_0})}{e_\infty(k_{m_0}L_{n_0}|S)} = \frac{q^{n_0}}{q^{n_0}/[S : k_{t_0}]} = [S : k_{t_0}].$$

It follows that S/k_{t_0} is fully ramified at the infinite prime. In particular $f_\infty(S|k_{t_0}) = 1$ so that $f_\infty(S|k) = f_\infty(S|k_{t_0})f_\infty(k_{t_0}|k) = f_\infty(k_{t_0}|k) = t_0$. □

We collect the above discussion in the following theorem.

Theorem 3.16. *Let $S = L \cap M$. Let $\operatorname{con}_{k/K} \mathfrak{p}_\infty = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$, let $t_i = \deg_K(\mathcal{P}_i)$, $1 \leq i \leq r$ and let $t_0 = \gcd(t_1, \ldots, t_r)$. Then the field of constants of S is $\mathbb{F}_{q^{t_0}}$.*

Let n_0 be the minimum nonnegative integer with $U_\infty^{(n_0)} \subseteq \mathfrak{S}$, where $\mathfrak{S}$ is a group that satisfies that $\mathfrak{S} \supseteq \prod_{i=1}^r H_i = \prod_{i=1}^r \mathrm{N}_{K_{\mathcal{P}_i}/k_\infty}(K_{\mathcal{P}_i}^*)$ and that $\mathfrak{S}$ is the minimum such that $[k_\infty^* : \mathfrak{S}] = p^\alpha$ is a p–group. Then the conductor of constants of S is $m_0 = f_\infty(S|k)e_\infty(S|S \cap L_{n_0}) = t_0 e_\infty(S|S \cap L_{n_0})$ and $\mathfrak{S}$ is the local norm group corresponding to S. In particular $\mathbb{F}_{q^{t_0}} \subseteq S \subseteq k_{m_0}L_{n_0}$. □

4 Number fields

The results of Section 3 can be developed in the number field case. In fact, for a number field, the extended genus field is more transparent than in the function field case.

Definition 4.1. Let K be an arbitrary number field, that is, a finite extension of the rational field $\mathbb{Q}$. Let K_{H^+} be the extended or narrow Hilbert class field of K, that is, K_{H^+} is the maximum abelian extension of K unramified at every finite prime of K. We define the *extended genus field* $K_{\mathfrak{ger}}$ of K as the maximum extension of K contained in K_{H^+} such that it is of the form KL with $L/\mathbb{Q}$ abelian.

Equivalently, if L is the maximum abelian extension of $\mathbb{Q}$ contained in K_{H^+}, the extended genus field of K is $K_{\mathfrak{ger}} = KL$.

Again, we stress that we choose L maximum.

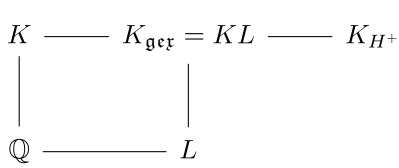
As in the function field case, we have

Proposition 4.2. *Let $K/\mathbb{Q}$ be a finite abelian extension and let X be the group of Dirichlet characters corresponding to K. Then $Y := \prod_{p\ prime} X_p$ is the group of Dirichlet characters corresponding to $K_{\mathfrak{ger}}$.* □

In particular, if $K/\mathbb{Q}$ is any finite extension and $K_{\mathfrak{ger}} = KL$, then $L = L_{\mathfrak{ger}}$. We want to describe $K_{\mathfrak{ger}}$ for a general number field K. Let $K/\mathbb{Q}$ be a finite extension. Let p be a prime in $\mathbb{Q}$ and let

$$\operatorname{con}_{\mathbb{Q}/K} p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

that is, $e_i = e_{K|\mathbb{Q}}(\mathfrak{p}_i|p)$, $1 \leq i \leq r$. Let $K_{\mathfrak{p}_1}, \ldots, K_{\mathfrak{p}_r}$ be the completions of K at the primes above p. Let $K_{\mathfrak{ger}} = KL$ with $L/\mathbb{Q}$ the maximum abelian extension such that $K \subseteq K_{\mathfrak{ger}} \subseteq K_{H^+}$.



Since $L = L_{\mathfrak{ger}}$, we let L_p be the field corresponding to X_p. We have that $L = \prod_{p \text{ prime}} L_p$ and $L_p \cap L_q = \mathbb{Q}$ for any primes p, q such that $p \neq q$. We have that L_p is the maximum abelian extension of $\mathbb{Q}$ with p the only possible finite prime ramified and such that KL_p/K is unramified at every finite prime.

Let p be a fixed prime and let $L_p \subseteq \mathbb{Q}(\zeta_{p^{m_p}})$. For any $n \in \mathbb{N}$, the idèle group corresponding to $\mathbb{Q}(\zeta_n)$ is

$$\mathcal{X}_n = \prod_{i=1}^{t} U_{p_i}^{(\alpha_i)} \times \prod_{\substack{q \text{ prime} \\ q \notin \{p_1, \dots, p_t\}}} U_q \times \mathbb{R}^+,$$

where $n = \prod_{i=1}^{t} p_i^{\alpha_i}$. As in the case of function fields, it follows that the idèle group corresponding to L_p is of the form

$$\Delta_p = H_p \times \prod_{\substack{q \text{ prime} \\ q \neq p}} U_q \times \mathbb{R}^+,$$

where $U_p^{(m_p)} \subseteq H_p \subseteq U_p$.

We have $e_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} = e_{K/\mathbb{Q}}(\mathfrak{p}_i|p) = e_i$. The extension $L_p/\mathbb{Q}$ is totally ramified at p and even we could mix up L_p with the completion of L at p. We have, with both meanings of L_p, that $[L_p : \mathbb{Q}] = [L_p : \mathbb{Q}_p] = e_p(L_p|\mathbb{Q})$.

By Theorem 3.8 we have that the norm group of the abelian extension KL_p/K is $\mathrm{N}_{K/\mathbb{Q}}^{-1}(\Delta_p)$. Since L_p is maximum, we want Δ_p to be such that (see [16, Corolario 17.6.47])

$$\mathrm{N}_{K/\mathbb{Q}}^{-1}(\Delta_p) \subseteq \prod_{\mathfrak{p} \text{ finite}} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \text{ real}} K_{\mathfrak{p}}^* = \prod_{\mathfrak{p} \text{ finite}} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^* \subseteq J_K,$$

or

$$\Delta_p \subseteq \mathrm{N}_{K/\mathbb{Q}}\Big(\prod_{\mathfrak{p} \text{ finite}} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^* \Big).$$

Let $\vec{\alpha} \in \prod_{\mathfrak{p} \text{ finite}} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^* \subseteq J_K$, $\vec{\alpha} = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$. Then

$$\mathrm{N}_{K/\mathbb{Q}}\, \vec{\alpha} = \prod_{q \text{ finite}} \Big(\prod_{\mathfrak{p}|q} \mathrm{N}_{K_{\mathfrak{p}}/\mathbb{Q}_p}\, \alpha_{\mathfrak{p}} \Big) \Big(\prod_{\mathfrak{p} \text{ real}} \mathrm{N}_{\mathbb{R}/\mathbb{R}}\, \alpha_{\mathfrak{p}} \Big).$$

As in the case of function fields we obtain that

$$H_p = \prod_{\mathfrak{p}|p} \mathrm{N}_{K_{\mathfrak{p}}/\mathbb{Q}_p} U_{\mathfrak{p}} \quad \text{and} \quad \Delta_p = \prod_{\mathfrak{p}|p} \mathrm{N}_{K_{\mathfrak{p}}/\mathbb{Q}_p} U_{\mathfrak{p}} \times \prod_{\substack{q \text{ prime} \\ q \neq p}} U_q \times \mathbb{R}^+.$$

In other words, let

$$S_i = \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i} \times \prod_{\substack{q \text{ prime} \\ q \neq p}} U_q \times \mathbb{R}^+ \subseteq U_p \times \prod_{\substack{q \text{ prime} \\ q \neq p}} U_q \times \mathbb{R}^+.$$

We have

$$\Delta_p = \prod_{i=1}^{r} S_i.$$

Now S_i corresponds to a field $R_i \subseteq \mathbb{Q}(\zeta_{p^{n_p}})$ and from [16, Teorema 17.6.49] it follows that $\prod_{i=1}^{r} S_i$ corresponds to $\bigcap_{i=1}^{r} R_i$. Thus $L_p = \bigcap_{i=1}^{r} R_i$. Furthermore, since R_i corresponds to S_i, we have

$$[C_{\mathbb{Q}} : \mathbb{Q}^* S_i] = [R_i : \mathbb{Q}] \quad \text{and} \quad \mathrm{Gal}(R_i/\mathbb{Q}) \cong C_{\mathbb{Q}}/\mathbb{Q}^* S_i.$$

Since in each field $R_i/\mathbb{Q}$, $1 \leq i \leq r$, the only finite prime ramified is p and it is totally ramified, the global and the local degrees are equal so that $[R_i : \mathbb{Q}] = [(R_i)_{\mathfrak{p}_i} : \mathbb{Q}_p]$. On the other hand, since $(R_i)_{\mathfrak{p}_i}/\mathbb{Q}_p$ is fully ramified we have

$$[(R_i)_{\mathfrak{p}_i} : \mathbb{Q}_p] = [U_p : \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}]$$

(see [16, Proposición 17.2.15]). Thus

$$[R_i : \mathbb{Q}] = [C_{\mathbb{Q}} : \mathbb{Q}^* S_i] = [U_p : \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}],$$

$$[L_p : \mathbb{Q}] = \Big[\bigcap_{i=1}^{r} R_i : \mathbb{Q}\Big] = \Big[U_p : \prod_{i=1}^{r} \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}\Big].$$

When $p \geq 3$, we have that $\mathbb{Q}(\zeta_{p^m})$ is cyclic for every $m \in \mathbb{N}$, however, when $p = 2$, $\mathbb{Q}(\zeta_{2^m})$ is not cyclic for $m \geq 3$. We study the two cases.

Let $G = \langle \sigma \rangle \cong C_n$ be a finite cyclic group of order $n \in \mathbb{N}$ and let $H_i = \langle \sigma^{j_i} \rangle < G$ where $j_i | n$, $i = 1, 2$. Let $H_1 \cap H_2 = \langle \sigma^t \rangle$ and $H_1 H_2 = \langle \sigma^s \rangle$ with $s, t | n$.

We have $\sigma^t \in H_i$, $i = 1, 2$ so that there exist $a_i \in \mathbb{Z}$ such that $\sigma^t = \sigma^{j_i a_i}$, $i = 1, 2$. Therefore $t \equiv j_i a_i \bmod n$, $i = 1, 2$, that is, $t = j_i a_i + l_i n$, $i = 1, 2$. Hence $j_i | t$, $i = 1, 2$ so that $\operatorname{lcm}[j_1, j_2] | t$.

Let $u = \operatorname{lcm}[j_1, j_2]$, $j_i | u$. Set $u = j_i b_i$. Then $\sigma^u = \sigma^{j_i b_i} \in H_i$, $i = 1, 2$. Thus $\sigma^u \in H_1 \cap H_2 = \langle \sigma^t \rangle$ and $\sigma^u = \sigma^{tc}$ for some c and $u = tc + ln$. It follows that $t | u = \operatorname{lcm}[j_1, j_2]$. Therefore $t = u$.

In other words, $H_1 \cap H_2 = \langle \sigma^{\operatorname{lcm}[j_1, j_2]} \rangle$.

Now, $H_1 H_2 = \langle \sigma^s \rangle$, $\frac{n}{s} = |H_1 H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = \frac{\frac{n}{j_1}\frac{n}{j_2}}{\frac{n}{t}} = \frac{nt}{j_1 j_2}$. Therefore $st = j_1 j_2$ and $j_1 j_2 = \gcd(j_1, j_2) \operatorname{lcm}[j_1, j_2] = \gcd(j_1, j_2) t = st$. Hence $s = \gcd(j_1, j_2)$.

In short, we have

Proposition 4.3. *Let $G = \langle \sigma \rangle$ be a cyclic group of order n and let $H_i = \langle \sigma^{j_i} \rangle$ with $j_i | n$, $i = 1, 2$ be two subgroups of G. Then*

$$H_1 \cap H_2 = \langle \sigma^{\operatorname{lcm}[j_1, j_2]} \rangle, \quad H_1 H_2 = \langle \sigma^{\gcd(j_1, j_2)} \rangle. \qquad \square$$

Corollary 4.4. *With the conditions of Proposition 4.3, we have*

$$|H_1 \cap H_2| = \frac{|G|}{\operatorname{lcm}[j_1, j_2]}, \quad [G : H_1 \cap H_2] = \operatorname{lcm}[j_1, j_2] = \operatorname{lcm}\Big[\frac{|G|}{|H_1|}, \frac{|G|}{|H_2|}\Big],$$

$$|H_1 H_2| = \frac{|G|}{\gcd(j_1, j_2)},$$

$$[G : H_1 H_2] = \frac{|G|}{|H_1 H_2|} = \gcd(j_1, j_2) = \gcd\big([G : H_1], [G : H_2]\big). \qquad \square$$

Corollary 4.5. *If $p > 2$ is a prime number and $H_i < \mathbb{Z}_p^*$, $i = 1, 2$ are two subgroups of finite index, then $[\mathbb{Z}_p^* : H_1 H_2] = \gcd\big([\mathbb{Z}_p^* : H_1], [\mathbb{Z}_p^* : H_2]\big)$.*

Proof. We have that $\mathbb{Z}_p^* \cong C_{p-1} \times \mathbb{Z}_p$ where C_{p-1} is the cyclic group of order $p - 1$. Let $H_i = H_i' \times p^{n_i} \mathbb{Z}_p$ where H_i' is the torsion of H_i, $i = 1, 2$. Then $H_1 H_2 = H_1' H_2' \times p^{\min\{n_1, n_2\}} \mathbb{Z}_p$. Therefore

$$\begin{aligned} [\mathbb{Z}_p^* : H_1 H_2] &= [C_{p-1} : H_1' H_2'] p^{\min\{n_1, n_2\}} \\ &= \gcd\big([C_{p-1} : H_1'], [C_{p-1} : H_2']\big) p^{\min\{n_1, n_2\}} \\ &= \gcd\big([\mathbb{Z}_p^* : H_1], [\mathbb{Z}_p^* : H_2]\big). \end{aligned}$$

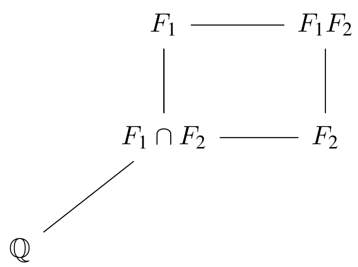
$\square$

We apply the previous discussion to the case $p > 2$.

Proposition 4.6. *If $p > 2$, $\mathbb{Q}(\zeta_{p^{m_p}})/\mathbb{Q}$ is a cyclic extension and $L_p/\mathbb{Q}$ is a cyclic extension. For F_1, F_2 contained in $\mathbb{Q}(\zeta_{p^{m_p}})$, we have*

$$[F_1 \cap F_2 : \mathbb{Q}] = \gcd\big([F_1 : \mathbb{Q}], [F_2 : \mathbb{Q}]\big).$$

Proof. We consider $F_1F_2/\mathbb{Q}$ which is cyclic since $\mathbb{Q}(\zeta_{p^{m_p}})/\mathbb{Q}$ is a cyclic extension. We have



Let $a = [F_1 \cap F_2 : \mathbb{Q}]$, $b = [F_1 : \mathbb{Q}]$ and $c = [F_2 : \mathbb{Q}]$. We have that $a|b$ and $a|c$ so that $a|\gcd(b,c)$. Now, since $\gcd(b,c)|b$ and $\gcd(b,c)|c$, there exists a unique field F_0 satisfying $[F_0 : \mathbb{Q}] = \gcd(b,c)$, $F_0 \subseteq F_1$ and $F_0 \subseteq F_2$. Hence $F_0 \subseteq F_1 \cap F_2$. This implies $\gcd(b,c) = [F_0 : \mathbb{Q}]|[F_1 \cap F_2 : \mathbb{Q}] = a$. Thus $a = \gcd(b,c)$. □

Corollary 4.7. *With the conditions of Proposition 4.6, if $p > 2$ and $F_1, \dots, F_t \subseteq \mathbb{Q}(\zeta_{p^{m_p}})$, we have*

$$\Big[\bigcap_{i=1}^{t} F_i : \mathbb{Q}\Big] = \gcd_{1\le i\le t}\big([F_i : \mathbb{Q}]\big).$$

Proof. Use induction. □

Remark 4.8. If $p = 2$, Proposition 4.6 is no longer true. For instance, if $F_1 = \mathbb{Q}(\sqrt{2})$, $F_2 = \mathbb{Q}(i)$, then $[F_1 : \mathbb{Q}] = [F_2 : \mathbb{Q}] = 2$ and since $F_1 \cap F_2 = \mathbb{Q}$, we have $[F_1 \cap F_2 : \mathbb{Q}] = 1$.

Remark 4.9. Since

$$\Big[\bigcap_{i=1}^{r} R_i : \mathbb{Q}\Big] = [L_p : \mathbb{Q}] = \Big[\mathbb{Q}_p^* : \prod_{i=1}^{r} \mathrm{N}_{(R_i)_{\mathfrak{p}_i}/\mathbb{Q}_p}(R_i)_{\mathfrak{p}_i}^*\Big] = \Big[U_p : \prod_{i=1}^{r} \mathrm{N}_{(R_i)_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}\Big],$$

for $p > 2$, we have

$$[L_p : \mathbb{Q}] = \gcd_{1\le i\le r}\big([R_i : \mathbb{Q}]\big) = \gcd_{1\le i\le r}\Big([U_{\mathfrak{p}_i} : \prod_{i=1}^{r} \mathrm{N}_{(R_i)_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}]\Big).$$

The main result on number fields is the following.

Theorem 4.10. *Let $K/\mathbb{Q}$ be a finite extension. With the above notations, we have $K_{\mathfrak{gex}} = KL$ where $L = \prod_{p \text{ finite}} L_p$ and L_p is a subfield of $\mathbb{Q}(\zeta_{p^{m_p}})$ satisfying*

$$[L_p : \mathbb{Q}] = \Big[U_p : \prod_{i=1}^{r} \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}\Big],$$

where $\operatorname{con}_{\mathbb{Q}/K} p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

Furthermore, if $p > 2$,

$$[L_p : \mathbb{Q}] = \gcd_{1\le i\le r} [U_p : \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i}],$$

L_p is determined by its degree $[L_p : \mathbb{Q}]$ and L_p is the class field of

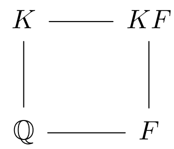
$$\prod_{i=1}^{r} \mathrm{N}_{K_{\mathfrak{p}_i}/\mathbb{Q}_p} U_{\mathfrak{p}_i} \times \prod_{\substack{q \text{ prime} \\ q \neq p}} U_q \times \mathbb{R}^+.$$

The tame ramification degree of the extension $[L_p : \mathbb{Q}]$ is

$$e^{\text{tame}} = \gcd(e_1, \dots, e_r, p-1).$$

Proof. It remains to find e^{tame}. Note that necessarily, $p \geq 3$. Let L'_p be the subfield of L_p of degree b_p where $[L_p : \mathbb{Q}] = p^{a_p} b_p$ and $\gcd(p, b_p) = 1$.

For any $F \subseteq \mathbb{Q}(\zeta_{p^{m_p}})$ with $[F : \mathbb{Q}] = d$ and $\gcd(p, d) = 1$, $F/\mathbb{Q}$ is tamely ramified. Assume that KF/K is unramified at p.



By Abhyankar Lemma, if $\mathfrak{P}$ is a prime in KF with $\mathfrak{P} \cap \mathbb{Q} = (p)$, $\mathfrak{P} \cap K = \mathfrak{p}_i$, $\mathcal{Q} = \mathfrak{P} \cap F$, then

$$e(\mathfrak{P}|p) = \operatorname{lcm}[e(\mathfrak{p}_i|p), e(\mathcal{Q}|p)] = \operatorname{lcm}[e_i, d].$$

Therefore $e(\mathfrak{P}|\mathfrak{p}_i) = \frac{e(\mathfrak{P}|p)}{e(\mathfrak{p}_i|p)} = \frac{e(\mathfrak{P}|p)}{e_i}$, that is, $\mathfrak{P}$ is unramified in KF/K if and only if $e(\mathfrak{P}|\mathfrak{p}_i) = 1$ if and only if $e(\mathfrak{P}|p) = e_i$ if and only if $d|e_i$. Hence, KF/K is unramifed at every finite prime, if and only if $d|e_i$ for $1 \leq i \leq r$ if and only if $d| \gcd(e_1, \ldots, e_r)$. Since $d|p-1$, this is equivalent to $d| \gcd(e_1, \ldots, e_r, p-1)$. It follows that $b_p = \gcd(e_1, \ldots, e_r, p-1)$. □

Remark 4.11. Theorem 4.10 was proved by M. Bhaskaran in [4] and by X. Zhang in [18].

4.1 Remarks on L_2

For any finite extension $K/\mathbb{Q}$, we have that if $K_{\mathfrak{gex}} = KL$ with $L/\mathbb{Q}$ the maximum abelian extension contained in K_{H^+}, we have proved that if $L = \prod_{q \text{ prime}} L_q$, then for $p \geq 3$, L_p is completely determined by

$$[L_p : \mathbb{Q}] = \Big[U_p : \prod_{\mathfrak{p}|p} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_p} U_\mathfrak{p}\Big] = \gcd_{\mathfrak{p}|p}[U_p : \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_p} U_\mathfrak{p}].$$

This is not so for $p = 2$. We want to study L_2.

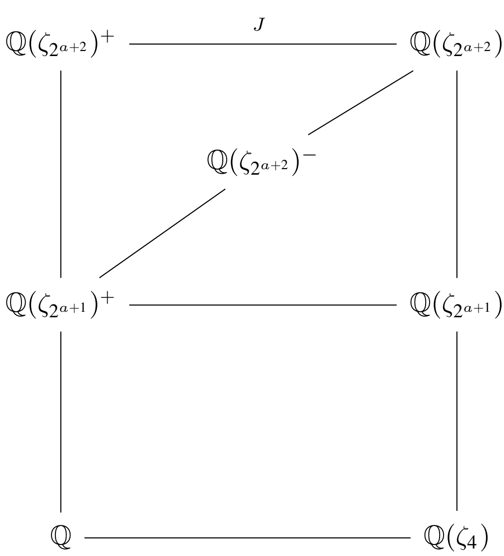
Let $[L_2 : \mathbb{Q}] = 2^a$, $a \geq 1$. For $a \geq 2$, there are three possible L_2, namely

$$\mathbb{Q}(\zeta_{2^{a+1}}), \quad \mathbb{Q}(\zeta_{2^{a+2}})^+ = \mathbb{Q}(\zeta_{2^{a+2}} + \zeta_{2^{a+2}}^{-1}) \quad \text{and} \quad \mathbb{Q}(\zeta_{2^{a+2}})^- := \mathbb{Q}(\zeta_{2^{a+2}} - \zeta_{2^{a+2}}^{-1}),$$

see [16, §5.3.1].

If L_2 is real, then $L_2 = \mathbb{Q}(\zeta_{2^{a+2}})^+$. If L_2 has conductor 2^{a+1} then $L_2 = \mathbb{Q}(\zeta_{2^{a+1}})$. In other words, L_2 can be determined by means of its conductor and whether it is real or not.

If $K(\zeta_{2^{a+1}})/K$ is unramified, we have $L_2 = \mathbb{Q}(\zeta_{2^{a+1}})$. In any case $\mathbb{Q}(\zeta_{2^{a+1}})^+ \subseteq L_2$, and therefore $K\mathbb{Q}(\zeta_{2^{a+1}})^+/K$ is unramified.



$\operatorname{Gal}\left(\mathbb{Q}(\zeta_{2^{a+2}})/\mathbb{Q}(\zeta_{2^{a+1}})^+\right) \cong C_2 \times C_2$

We need to determine the group of idèles corresponding to each extension L_2, where $L_2 \in \{\mathbb{Q}(\zeta_{2^{a+1}}), \mathbb{Q}(\zeta_{2^{a+2}})^+, \mathbb{Q}(\zeta_{2^{a+2}})^-\}$.

Recall that for a local field K we have $K^* \cong \mathbb{F}_q^* \times U_{\mathfrak{p}}^{(1)} \times (\pi)$, where π is a uniformizing element, $v_{\mathfrak{p}}(\pi) = 1$, $U_{\mathfrak{p}}$ are the units of K^*, $U_{\mathfrak{p}}^{(1)}$ are the units modulo 1, that is, $U_{\mathfrak{p}}^{(1)} = \{\xi \in U_{\mathfrak{p}} \mid \xi - 1 \in (\pi)\} = 1 + \pi\mathcal{O}_K = 1 + \mathfrak{p}$, and $U_{\mathfrak{p}}^{(1)} \times \mathbb{F}_q^* = U_{\mathfrak{p}}$ where $\mathbb{F}_q$ is the residue field.

In the particular case of $K = \mathbb{Q}_p^*$, $q = p$, $\mathbb{F}_p^* \cong C_{p-1} = \mathbb{Z}/(p-1)\mathbb{Z}$ and $U_p = \Big\{ \sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0, a_i \in \{0, 1, \dots, p-1\} \text{ for all } i \Big\} \cong \mathbb{Z}_p^*$, where $\mathbb{Z}_p$ denotes the ring of p–adic integers and $\mathbb{Z}_p^*$ is the multiplicative group of $\mathbb{Z}_p$.

We have

Proposition 4.12. (1) *If $p > 2$, $\mathbb{Z}_p^* \cong C_{p-1} \times \mathbb{Z}_p$ as groups.*

(2) *If $p = 2$, $1 + 2\mathbb{Z}_2 \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$ and $1 + 4\mathbb{Z}_2 \cong \mathbb{Z}_2$. In particular,*

$$U_2 = U_2^{(1)} = \mathbb{Z}_2^* \cong 1 + 2\mathbb{Z} \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \cong \{\pm 1\} \times \mathbb{Z}_2. \qquad \square$$

We are going to identify complex conjugation J with -1 since $J(\zeta_{2^n}) = \zeta_{2^n}^{-1}$ for all n.

The non–zero closed subgroups of $U_2 = \mathbb{Z}_2^* \cong \{\pm 1\} \times \mathbb{Z}_2$ are: $\{\pm 1\} \times 2^n\mathbb{Z}_2$, $2^n\mathbb{Z}_2$ and $\{\pm 1\} \cdot 2^n\mathbb{Z}_2$ with $n \in \mathbb{N} \cup \{0\}$.

The quotient groups are respectively

- $\frac{\{\pm 1\} \times \mathbb{Z}_2}{\{\pm 1\} \times 2^n\mathbb{Z}_2} \cong \frac{\mathbb{Z}_2}{2^n\mathbb{Z}_2} \cong C_{2^n}$,
- $\frac{\{\pm 1\} \times \mathbb{Z}_2}{2^n\mathbb{Z}_2} \cong \{\pm 1\} \times \frac{\mathbb{Z}_2}{2^n\mathbb{Z}_2} \cong \{\pm 1\} \times C_{2^n}$,
- $\frac{\{\pm 1\} \times \mathbb{Z}_2}{\{\pm 1\} \cdot 2^n\mathbb{Z}_2} \cong \mathcal{H}$.

Let us study $\mathcal{H}$. Consider $b := 1 \in \mathbb{Z}_2$. Then b is a topological generator of $\mathbb{Z}_2$. Let $a := -1$ be the unique torsion element of $\mathbb{Z}_2^*$ of order 2. Let $\mathcal{H}$ be the procyclic group with topological generator ab^{2^n}: $\mathcal{H} = \overline{\langle ab^{2^n} \rangle}$ (topological closure). Denote by $\tilde{a}$ and $\tilde{b}$ the classes of a and b modulo $\mathcal{H}$ respectively: $\tilde{a} = a \bmod \mathcal{H}$; $\tilde{b} = b \bmod \mathcal{H}$.

We have $\mathcal{G}/\mathcal{H} = \langle \tilde{a}, \tilde{b} \rangle$ where $\mathcal{G} = \{\pm 1\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2^*$. Since $ab^{2^n} \in \mathcal{H}$, $\tilde{b}^{2^n} = \tilde{a}^{-1} \bmod \mathcal{H}$ and $\tilde{a}^{-1} = \tilde{a} \bmod \mathcal{H}$ (indeed, $a^{-1} = a = -1$). Therefore $\mathcal{G}/\mathcal{H} = \langle \tilde{b} \rangle$ since $\tilde{a} = \tilde{b}^{2^n} \in \langle \tilde{b} \rangle$ so that $\mathcal{G}/\mathcal{H}$ is a cyclic group.

Note that $b^{2^n} \notin \mathcal{H}$ since otherwise $a \in \mathcal{H}$ but a is a torsion element and $\mathcal{H}$ is torsion free. Therefore $b^{2^n} \notin \mathcal{H}$. On the other hand $b^{2^{n+1}} = b^{2^n} b^{2^n} \equiv ab^{2^n} \bmod \mathcal{H}$ so that $b^{2^{n+1}} \in \mathcal{H}$. It follows that $o(\tilde{b}) = 2^{n+1}$. Thus $\mathcal{G}/\mathcal{H}$ is a cyclic group of order 2^{n+1}.

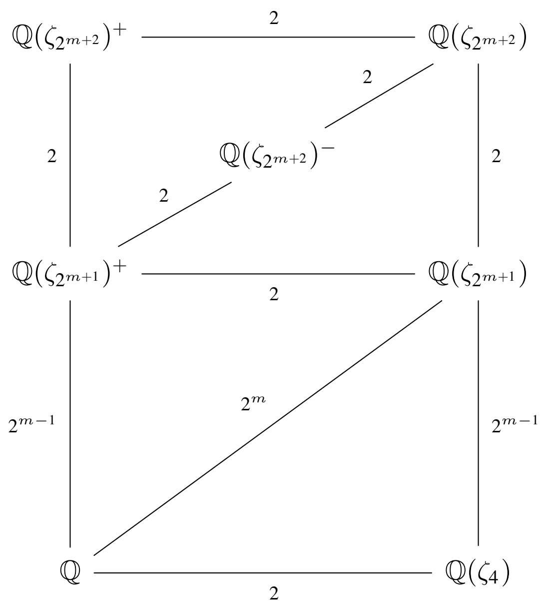
Uniformizing the indexes, we have

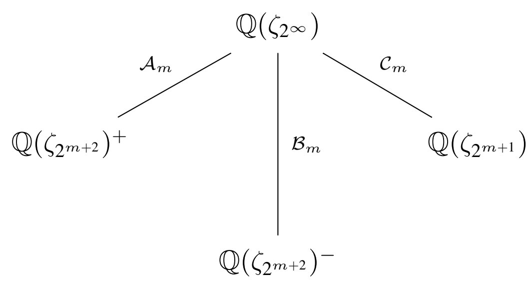
- $\frac{\{\pm 1\} \times \mathbb{Z}_2}{\{\pm 1\} \times 2^m\mathbb{Z}_2} = \frac{\overline{\langle a,b \rangle}}{\overline{\langle a,b^{2^m} \rangle}} = \langle b \bmod b^{2^m} \rangle \cong C_{2^m}$,
- $\frac{\{\pm 1\} \times \mathbb{Z}_2}{2^{m-1}\mathbb{Z}_2} = \frac{\overline{\langle a,b \rangle}}{\overline{\langle b^{2^{m-1}} \rangle}} = \langle \tilde{a}, \tilde{b} \rangle \bmod b^{2^{m-1}} \cong C_2 \times C_{2^{m-1}}$,
- $\frac{\{\pm 1\} \times \mathbb{Z}_2}{\{\pm 1\} \cdot 2^m\mathbb{Z}_2} = \frac{\overline{\langle a,b \rangle}}{\overline{\langle ab^{2^m} \rangle}} = \langle \tilde{b} \rangle \bmod \mathcal{H} \cong C_{2^m}$.

Define $\mathcal{A}_m := \{\pm 1\} \times 2^m\mathbb{Z}_2$; $\mathcal{B}_m := 2^{m-1}\mathbb{Z}_2$; $\mathcal{C}_m := \{\pm 1\}2^{m-1}\mathbb{Z}_2$.

We have

- $\mathcal{R}_m := \mathcal{G}/\mathcal{A}_m \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{2^{m+2}})^+/\mathbb{Q}) \cong C_{2^m}$ since $-1 \in \mathcal{A}_m$,
- $\mathcal{S}_m := \mathcal{G}/\mathcal{B}_m \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{2^{m+1}})/\mathbb{Q}) \cong C_2 \times C_{2^{m-1}}$ since $\mathcal{G}/\mathcal{B}_m$ is noncyclic and $-1 \notin \mathcal{B}_m$,
- $\mathcal{T}_m := \mathcal{G}/\mathcal{C}_m \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{2^{m+2}})^-/\mathbb{Q}) \cong C_{2^m}$ since it is cyclic and $-1 \notin \mathcal{C}_m$.





Since $[L_2 : \mathbb{Q}] = 2^m$ and $\big[U_2 : \prod_{\mathfrak{p}|2} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}\big] = 2^m$, it follows the following theorem.

Theorem 4.13. *If* $[L_2 : \mathbb{Q}] = 2^m$, *then*

(1) $L_2 = \mathbb{Q}(\zeta_{2^{m+2}})^+ \iff$ *for every place* $\mathfrak{p}$ *of* K *with* $\mathfrak{p}|2$ *we have* $-1 \in \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}$, *that is,* $-1 \in \bigcap_{\mathfrak{p}|2} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}$.

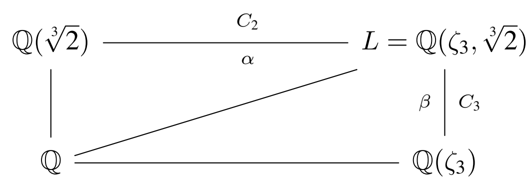
(2) $L_2 = \mathbb{Q}(\zeta_{2^{m+1}}) \iff \bigcap_{\mathfrak{p}|2} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}$ *is not cyclic (automatically we have that* $-1 \notin \bigcap_{\mathfrak{p}|2} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}$*).*

(3) $L_2 = \mathbb{Q}(\zeta_{2^{m+2}})^- \iff \bigcap_{\mathfrak{p}|2} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}$ *is cyclic and* $-1 \notin \bigcap_{\mathfrak{p}|2} \mathrm{N}_{K_\mathfrak{p}/\mathbb{Q}_2} U_\mathfrak{p}$. □

5 Some remarks on genus fields of number fields

Let $L/\mathbb{Q}$ be a finite Galois extension. Since $L/\mathbb{Q}$ is normal, L is either totally real or totally imaginary. Let $J\colon \mathbb{C} \longrightarrow \mathbb{C}$ be the complex conjugation. Since $J|_\mathbb{Q} = \mathrm{Id}_\mathbb{Q}$ and $L/\mathbb{Q}$ is normal, we have $J(L) = L = \bar{L}$. Hence $J|_L \in G := \mathrm{Gal}(L/\mathbb{Q})$. Furthermore $J|_L$ has order $o(J|_L) = 1$ or 2. Let L^J be the fixed field of L under the action of J. We have $\mathrm{Gal}(L|L^J) = \langle J|_L\rangle \cong \{1\}$ or C_2, the cyclic group of order 2 and $[L : L^J]|2$. Furthermore, $L^J \subseteq \mathbb{R}$.

Note that L^J is neither necessarily normal over $\mathbb{Q}$ nor totally real. For instance, if $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$.



Then $\operatorname{Gal}(L/\mathbb{Q}) = \langle \alpha, \beta \rangle = C_2 \ltimes C_3 \cong S_3$, the symmetric group in 3 elements. L is totally imaginary and $L^J = \mathbb{Q}(\sqrt[3]{2})$, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal and the 3 embeddings are $\sqrt[3]{2} \longrightarrow \begin{cases} \sqrt[3]{2} \\ \zeta_3\sqrt[3]{2} \\ \zeta_3^2\sqrt[3]{2} \end{cases}$. In other words, with the usual meaning, $r_1 = 1$ and $r_2 = 1$.

When $L/\mathbb{Q}$ is abelian, then $\langle J|_L \rangle \lhd G$, $L^J/\mathbb{Q}$ is a Galois extension and L^J is totally real.

In the case of genus fields, we consider $K/\mathbb{Q}$ a finite extension and let K_H and K_{H^+} be the Hilbert class field and the Hilbert extended (narrow) class field of K respectively. Then the genus field $K_{\mathfrak{ge}}$ is the maximum extension such that $K \subseteq K_{\mathfrak{ge}} \subseteq K_H$ with $K_{\mathfrak{ge}} = KF$, $F/\mathbb{Q}$ abelian. In particular, $F = F_{\mathfrak{ge}}$. The extended or narrow genus field $K_{\mathfrak{gex}}$ of K is the maximum extension such that $K \subseteq K_{\mathfrak{gex}} \subseteq K_{H^+}$ with $K_{\mathfrak{gex}} = KL$ and $L/\mathbb{Q}$ is abelian. In particular, $L_{\mathfrak{gex}} = L$. Recall that $L_{\mathfrak{gex}}$ is the maximum abelian extension of $\mathbb{Q}$ such that $L_{\mathfrak{gex}}/L$ is unramfied at every finite prime and $F_{\mathfrak{ge}}$ is the maximum abelian extension of $\mathbb{Q}$ with $F_{\mathfrak{ge}}/K$ unramified at every prime.

From the remarks above, it follows that $[K_{\mathfrak{gex}} : K_{\mathfrak{ge}}] = 1$ or 2 for every finite abelian extension $K/\mathbb{Q}$. Now, we have $K_H \subseteq K_{H^+}$ and in fact $\operatorname{Gal}(K_{H^+}/K_H) \cong C_2^r$ for some $r \in \mathbb{N} \cup \{0\}$. In our notation, we have that $F \subseteq L$ since KF/K is unramified and $F/\mathbb{Q}$ is abelian. On the other hand, L^J is totally real, $L^J/\mathbb{Q}$ is abelian and KL^J/K is unramified at every prime. It follows that

$$L^J \subseteq F \subseteq L.$$

Since $F = F_{\mathfrak{ge}}$ it follows that $[L : F]|2$ and therefore

$$[K_{\mathfrak{gex}} : K_{\mathfrak{ge}}] = [KL : KF]|[L : F] = 1 \text{ or } 2.$$

In short, we have

Proposition 5.1. *For a finite extension $K/\mathbb{Q}$, we have $[K_{\mathfrak{gex}} : K_{\mathfrak{ge}}]|2$.* □

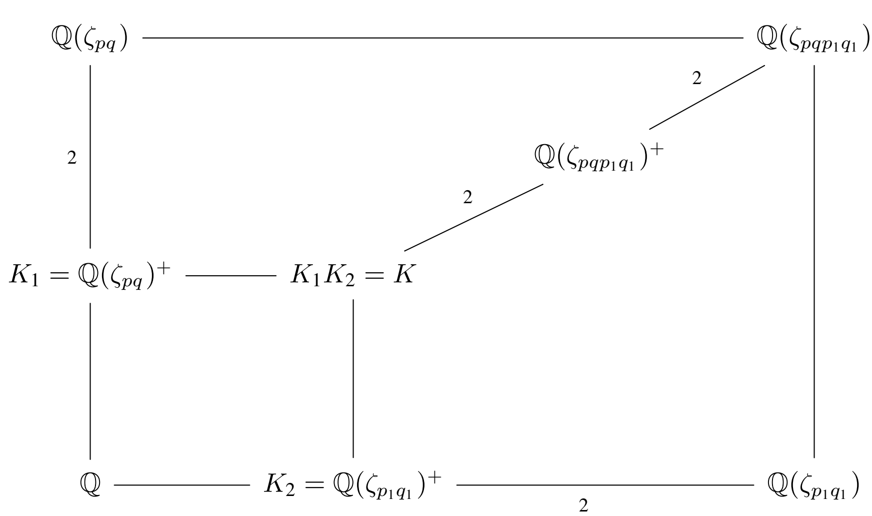
Now consider $K_i/\mathbb{Q}$, $i = 1, 2$, two finite extensions and let $K = K_1K_2$. We have $K_i \subseteq K$ for $i = 1, 2$. On the other hand the extension $(K_1)_{\mathfrak{ge}}/K_1$ is unramified and abelian, it follows that $K(K_1)_{\mathfrak{ge}}/KK_1 = K$ is unramified and abelian. Hence $K(K_1)_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}$. It follows that $(K_1)_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}$. Similarly $(K_2)_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}$. Therefore $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}$.

Remark 5.2. Not necessarily $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = K_{\mathfrak{ge}}$.

Example 5.3. Let p, q, p_1, q_1 be four odd distinct primes. Let $K_1 = \mathbb{Q}(\zeta_{pq})^+$, $K_2 = \mathbb{Q}(\zeta_{p_1q_1})^+$. Then, using Dirichlet characters, we have that $(K_1)_{\mathfrak{ge}} \subseteq \mathbb{Q}(\zeta_{pq})$ and $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_{pq})^+$ is ramified at ∞, it follows that $(K_1)_{\mathfrak{ge}} = K_1$. Similarly $(K_2)_{\mathfrak{ge}} = K_2$.

Furthermore, since $p \neq q$ (respectively $p_1 \neq q_1$), $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_{pq})^+$ is ramified only at ∞, that is, $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_{pq})^+$ is unramified at every finite prime ([16, Teorema 5.3.2]).

Now $K_1K_2 = K = \mathbb{Q}(\zeta_{pq})^+\mathbb{Q}(\zeta_{p_1q_1})^+ \subseteq \mathbb{Q}(\zeta_{pqp_1q_1})$.



We have that $\mathbb{Q}(\zeta_{pqp_1q_1})^+/K$ is unramified since p is unramified in $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_{pq})^+$ and thus

$$e_p(\mathbb{Q}(\zeta_{pqp_1q_1})|\mathbb{Q}) = p-1 = e_p(\mathbb{Q}(\zeta_{pq})^+|\mathbb{Q}) = e_p(K|\mathbb{Q}).$$

The same holds for q, p_1 and q_1. Now, ∞ is ramified in $\mathbb{Q}(\zeta_{pqp_1q_1})/\mathbb{Q}(\zeta_{pqp_1q_1})^+$. It follows that $K_{\mathfrak{ge}} = \mathbb{Q}(\zeta_{pqp_1q_1})^+$ and that $[K_{\mathfrak{ge}} : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}] = 2 > 1$.

Remark 5.4. For extended genus fields, we have that for any two finite abelian extensions $K_i/\mathbb{Q}$, $i = 1,2$ we have $K_{\mathfrak{gex}} = (K_1)_{\mathfrak{gex}}(K_2)_{\mathfrak{gex}}$ where $K = K_1K_2$ (see [2]).

Theorem 5.5. *Let $K_i/\mathbb{Q}$, $i = 1,2$ be two finite abelian extensions and let $K = K_1K_2$. Then*

$$[K_{\mathfrak{ge}} : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}]|2.$$

Proof. In general we consider a finite abelian extension $K/\mathbb{Q}$. Let $L = K_{\mathfrak{gex}}$. We have $K_{\mathfrak{ge}} = L^+K$ (see [2]). Let $K = K_1K_2$. Then $K_{\mathfrak{gex}} = (K_1)_{\mathfrak{gex}}(K_2)_{\mathfrak{gex}}$. Therefore $L = L_1L_2$ and $K_{\mathfrak{ge}} = L^+K$, $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = L_1^+K_1L_2^+K_2 = L_1^+L_2^+K$. Hence

$$[K_{\mathfrak{ge}} : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}] = [L^+K : L_1^+L_2^+K]|[L^+ : L_1^+L_2^+].$$

To prove the result, it suffices to show that for two finite abelian extensions $L_i/\mathbb{Q}$, $i = 1,2$, and for $L = L_1L_2$, we have $[L^+ : L_1^+L_2^+]|2$.

In general, we have $L^+ = L \cap \mathbb{Q}(\zeta_n)^+ = L \cap \mathbb{Q}(\zeta_n)^J$ for $L \subseteq \mathbb{Q}(\zeta_n)$. In particular, if $S := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$, $L^+ = L \cap \mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n)^S \cap \mathbb{Q}(\zeta_n)^I = \mathbb{Q}(\zeta_n)^{SI}$ where $I = \langle J \rangle$ and thus $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L^+) = SI$.

Let $S_i := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/L_i)$, $i = 1,2$. Since $L = L_1L_2$, we have $S = S_1 \cap S_2$. We also have

$$L_1^+L_2^+ = \mathbb{Q}(\zeta_n)^{S_1I}\mathbb{Q}(\zeta_n)^{S_2I} = \mathbb{Q}(\zeta_n)^{S_1I \cap S_2I} \subseteq L^+ = \mathbb{Q}(\zeta_n)^{SI}.$$

Therefore

$$\mathrm{Gal}(L^+/L_1^+L_2^+) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L_1^+L_2^+)}{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L^+)} \cong \frac{S_1I \cap S_2I}{SI} = \frac{S_1I \cap S_2I}{(S_1 \cap S_2)I}. \tag{5.1}$$

Now

$$|S_1I \cap S_2I| = \frac{|S_1I||S_2I|}{|S_1S_2I|} = \frac{\frac{|S_1||I|}{|S_1\cap I|}\frac{|S_2||I|}{|S_2\cap I|}}{\frac{|S_1S_2||I|}{|S_1S_2\cap I|}} = \frac{\frac{|S_1||S_2||I|^2}{|S_i\cap I||S_2\cap I|}}{\frac{|S_1||S_2|}{|S_1\cap S_2|}\frac{|I|}{|S_1S_2\cap I|}}$$
$$= \frac{|S_1 \cap S_2||S_1S_2 \cap I|}{|S_1 \cap I||S_2 \cap I|}|I|.$$

On the other hand $|(S_1 \cap S_2)I| = |SI| = \frac{|S||I|}{|S\cap I|}$. It follows that

$$[S_1I \cap S_2I : (S_1 \cap S_2)I] = \frac{|S_1 \cap S_2||S_1S_2 \cap I|}{|S_1 \cap I||S_2 \cap I|}\frac{|S \cap I|}{|S||I|}|I| = \frac{|S_1S_2 \cap I||S \cap I|}{|S_1 \cap I||S_2 \cap I|}.$$

Now $S \cap I \subseteq S_2 \cap I$. Let $\alpha = [S_2 \cap I : S \cap I] \in \mathbb{N}$. Then

$$[S_1I \cap S_2I : (S_1 \cap S_2)I] = \frac{1}{\alpha}\frac{|S_1S_2 \cap I|}{|S_1 \cap I|} = \frac{1}{\alpha}\frac{\frac{|S_1S_2||I|}{|S_1S_2I|}}{\frac{|S_1||I|}{|S_1I|}} = \frac{1}{\alpha}\frac{|S_1S_2||S_1I|}{|S_1S_2I||S_1|}.$$

We have $S_1S_2 \subseteq S_1S_2I$. Let $\beta = [S_1S_2I : S_1S_2] \in \mathbb{N}$. It follows that

$$[S_1I \cap S_2I : (S_1 \cap S_2)I] = \frac{1}{\alpha\beta}\frac{|S_1I|}{|S_1|} = \frac{1}{\alpha\beta}\frac{|S_1||I|}{|S_1||S_1 \cap I|} = \frac{1}{\alpha\beta}\frac{|I|}{|S_1 \cap I|} = \frac{\gamma}{\alpha\beta},$$

with $\gamma = [I : S_1 \cap I]||I|$. Therefore $[S_1I \cap S_2I : (S_1 \cap S_2)I] = \frac{\gamma}{\alpha\beta} \in \mathbb{N}$ and $[S_1I \cap S_2I : (S_1 \cap S_2)I]||I| = 1$ or 2. It follows that

$$[L^+ : L_1^+L_2^+]|2 \quad \text{and} \quad [K_{\mathfrak{ge}} : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}]|2.$$

□

References

[1] Anglès, Bruno; Jaulent, Jean–François, *Théorie des genres des corps globaux*, Manuscripta Math. **101**, no. 4, 513–532 (2000).

[2] Barreto–Castañeda, Jonny Fernando; Montelongo–Vázquez, Carlos; Reyes–Morales Carlos Daniel; Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel Daniel, *Genus fields of abelian extensions of rational congruence function fields II*, Rocky Mountain Journal of Mathematics, **48**, no. 7, 2099–2133 (2018).

[3] Bae, Sunghan; Koo, Ja Kyung, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60**, no. 3, 301–310 (1996).

[4] Bhaskaran M. *Construction of Genus Field and Some Applications*, Journal of Number Theory **11**, 488–497 (1979).

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

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

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

[8] Gauss, Carl Friedrich, *Disquisitiones arithmeticae*, 1801.

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

[10] Hu, Su; Li, Yan, *The genus fields of Artin–Schreier extensions*, Finite Fields Appl. **16**, no. 4, 255–264 (2010).

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

[12] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Genus Fields of Abelian Extensions of Congruence Rational Function Fields*, Finite Fields Appl. **20**, 40–54 (2013).

[13] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Genus Fields of Congruence Function Fields*, Finite Fields Appl. **44**, 56–75 (2017).

[14] Peng, Guohua, *The genus fields of Kummer function fields*, J. Number Theory **98** , no. 2, 221–227 (2003).

[15] Rosen, Michael, *The Hilbert class field in function fields*, Exposition. Math. **5**, no. 4, 365–378 (1987).

[16] Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Campos ciclotómicos numéricos y de funciones (segunda versión)*, `https://arxiv.org/abs/1407.3238`.

[17] Villa–Salvador, Gabriel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

[18] Zhang, Xianke, *Counterexample and Correction about Genus Fields of Number Fields*, Journal of Number Theory **23**, 318–321 (1986).

Author information

Elizabeth Ramírez–Ramírez, Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N., Ciudad de México, C.P. 07340, México.
E-mail: `eramirez@ctrl.cinvestav.mx`

Martha Rzedowski–Calderón, Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N., Ciudad de México, C.P. 07340, México.
E-mail: `mrzedowski@ctrl.cinvestav.mx`

Gabriel Villa–Salvador, Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N., Ciudad de México, C.P. 07340, México.
E-mail: `gvillasalvador@gmail.com, gvilla@ctrl.cinvestav.mx`

Received: October 23, 2018.
Accepted: December 28, 2018.