ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 48, Number 7, 2018

GENUS FIELDS OF ABELIAN EXTENSIONS OF RATIONAL CONGRUENCE FUNCTION FIELDS, II

JONNY FERNANDO BARRETO-CASTAÑEDA, CARLOS MONTELONGO-VÁZQUEZ, CARLOS DANIEL REYES-MORALES, MARTHA RZEDOWSKI-CALDERÓN AND GABRIEL VILLA-SALVADOR

ABSTRACT. In this paper, we find the genus field of finite abelian extensions of the global rational function field. We introduce the term conductor of constants for these extensions and determine it in terms of other invariants. We study the particular case of finite abelian p-extensions and give an explicit description of their genus field.

1. Introduction. It was Gauss [**11**] who first considered what now is known as the *genus field*. The work of Gauss was in the context of binary quadratic forms. Later, this concept was translated into the context of quadratic number fields. In this way, originally, the definition of genus field was given for a quadratic extension of $\mathbb{Q}$. We have that, for a quadratic number field K, the genus field of K is the maximal extension of K that is abelian over $\mathbb{Q}$ and which is unramified over K. The Galois group of $K_{\mathfrak{gc}}/K$, $K_{\mathfrak{gc}}$ denoting the genus field of K, is isomorphic to the maximal subgroup of exponent 2 of the ideal class group of K. It was proven by Gauss that, if s is the number of different positive finite rational primes dividing the discriminant δ_K of a quadratic number field K, then the 2-rank of the class group of K is $s-2$ if $\delta_K > 0$, and there exists a prime $p \equiv 3 \bmod 4$ dividing δ_K, and $s-1$ otherwise.

Genus theory using class field theory was introduced by Hasse [**12**] for the special case of quadratic number fields. Hasse translated Gauss's genus theory using characters. Leopoldt [**18**] generalized the results of Hasse, determining the genus field $K_{\mathfrak{gc}}$ of an absolute abelian

2010 AMS *Mathematics subject classification.* Primary 11R58, Secondary 11R29, 11R60.

Keywords and phrases. Global function fields, ramification, genus fields, abelian p-extensions.

Received by the editors on October 21, 2017, and in revised form on February 19, 2018.

DOI:10.1216/RMJ-2018-48-7-2099

number field K. Leopoldt used Dirichlet characters to develop genus theory of absolute abelian extensions and related the theory of Dirichlet characters to the arithmetic of K.

The concept of genus fields for an arbitrary finite extension of the field of rational numbers was introduced by Fröhlich [**7, 8, 9**]. Fröhlich defined the genus field $K_{\mathfrak{ge}}$ of an arbitrary finite number field $K/\mathbb{Q}$ as $K_{\mathfrak{ge}} := Kk^*$, where k^* is the maximal abelian number field such that Kk^*/K is unramified. We have that k^* is the maximal abelian number field contained in $K_{\mathfrak{ge}}$. The degree $[K_{\mathfrak{ge}} : K]$ is called the *genus number* of K, and the Galois group $\mathrm{Gal}(K_{\mathfrak{ge}}/K)$ is called the *genus group* of K.

We have that, if K_H denotes the *Hilbert class field* of K, then $K \subseteq K_{\mathfrak{ge}} \subseteq K_H$, and $\mathrm{Gal}(K_H/K)$ 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, that is, $\mathrm{Gal}(K_{\mathfrak{ge}}/K) \cong Cl_K/G_K$. The subgroup G_K is called the *principal genus* of K, and $|Cl_K/G_K|$ is equal to the genus number of K.

Zhang [**29**] gave a simple expression of $K_{\mathfrak{ge}}$ for any abelian extension K of $\mathbb{Q}$ using Hilbert ramification theory. Ishida [**15**] described the *narrow genus field* $K_{\mathfrak{ge}}$ of any finite extension of $\mathbb{Q}$, that is, Ishida allowed ramification at the infinite primes. Given a number field K, Ishida found two abelian number fields k_1^* and k_2^* such that

$$k^* = k_1^* k_2^* \quad \text{and} \quad k_1^* \cap k_2^* = \mathbb{Q}.$$

The field k_1^* is related to the finite primes p such that at least one prime in K above p is tamely ramified.

We are interested in genus theory for global function fields. There is no direct proper notion of Hilbert class field since all of the constant field extensions are abelian and unramified, and the maximal constant extension is infinite abelian and unramified. On the other extreme, if the class number of a congruence function field K is h_K, then there are exactly $h := h_K$ abelian extensions $K_1, \ldots, K_h$ of K such that K_i/K are maximal unramified with exact field of constants of each K_i, the same as that of K, $\mathbb{F}_q$ the finite field of q elements and $\mathrm{Gal}(K_i/K) \cong Cl_{K,0}$ the group of classes of divisors of degree zero [**2,** page 79, Chapter 8].

There have been different notions of genus fields according to different Hilbert class field definitions. Rosen [**24**] gave a definition of Hilbert class fields of K, fixing a nonempty finite set S_∞ of prime divisors of K.

Using Rosen's definition of the Hilbert class field, it is possible to give a proper concept of genus fields along the lines of number fields.

Clement [**6**] found a narrow genus field of a cyclic extension of $k = \mathbb{F}_q(T)$ of prime degree l dividing $q-1$. She used the concept of a Hilbert class field similar to that of a quadratic number field K: it is the finite abelian extension of K such that the prime ideals of the ring of integers $\mathcal{O}_K$ of K splitting there are precisely the principal ideals generated by an element whose norm is an l-power. Bae and Koo [**3**] were able to generalize the results of Clement with the methods developed by Fröhlich [**9**]. They defined the narrow genus field for general global function fields and developed the analogue of the classical genus theory. Anglès and Jaulent [**1**] used narrow S-class groups to establish the fundamental results, using class field theory, for the genus theory of finite extensions of global fields, where S is a finite set of places.

Peng [**23**] explicitly described the genus theory for Kummer extensions K of $k := \mathbb{F}_q(T)$ of prime degree l, based on the global function field analogue of Conner and Hurrelbrink's exact hexagon. Wittman [**28**] extended Peng's results to the case $l \nmid q\,(q-1)$ and used his results to study the l-part of the ideal class groups of cyclic extensions of prime degree l of k. Hu and Li [**14**] explicitly described the genus field of an Artin-Schreier extension of k.

In [**19, 20**], a theory of genus fields of congruence function fields was developed using Rosen's definition of Hilbert class field: given a finite nonempty set S of places of a global function field K, the Hilbert class field (relative to S) $K_{H,S}$ of K is defined as the maximal abelian unramified extension of K such that the places in S fully decompose in $K_{H,S}$. The genus field $K_{\mathfrak{ge}}$ of K is the maximal extension of K such that

$$K \subseteq K_{\mathfrak{ge}} \subseteq K_{H,S}$$

with $K_{\mathfrak{ge}} = Kk^*$ and such that k^*/k is an abelian extension. In the case where K/k is abelian, $K_{\mathfrak{ge}}$ simply is the maximal abelian unramified extension of k such that the primes in S fully decompose in $K_{\mathfrak{ge}}$. The methods used there were based on the ideas of Leopoldt using Dirichlet characters, and a general description of $K_{\mathfrak{ge}}$ in terms of Dirichlet characters was given. The genus field $K_{\mathfrak{ge}}$ was obtained for an abelian extension K of k and S the set of infinite primes. The method

was used to give $K_{\mathfrak{gc}}$ explicitly when K/k is a cyclic extension of prime degree $l \mid q-1$ (Kummer) or $l = p$ where p is the characteristic (Artin-Schreier) and also when K/k is a p-cyclic extension (Witt). Later on, the method was used in [**5**] to explicitly describe $K_{\mathfrak{gc}}$ when K/k is a cyclic extension of degree l^n, where l is a prime number and $l^n \mid q-1$.

In this paper, we consider a finite abelian extension K/k. We find the genus field of K with respect to k. Special consideration is given to the genus field of a finite abelian p-extension of k, where p is the characteristic.

The study of elementary abelian p-extensions, and more generally abelian p-extensions, has been considered by numerous authors. These extensions appear in several contexts. In [**22**], Ore considered additive polynomials using composition as multiplication. With this operation, these polynomials are known as *twisted polynomials*, and this is one of the bases for *Drinfeld modules*. Lachaud [**17**] obtained an analogue of the Carlitz-Uchiyama bound for geometric BCH codes and some consequences for cyclic codes. His results are part of the analysis of the L-function of Artin-Schreier extensions. Garcia and Stichtenoth [**10**] studied field extensions L/K given by an equation of the type

$$y^q - y = f(x) \in K(x),$$

where q is a power of p and $\mathbb{F}_q \subseteq K$. Using a result of Kani [**16**], they obtained a formula relating the genus of the extension and the genus of several subextensions of degree p. There are many fields of this kind having the maximum number of rational places allowed by Weil's bound, but they proved that, for fixed K, the number of rational places is asymptotically bad. They also used these extensions to find a family of fields whose Weierstrass gap sequences are nonclassical.

In [**4**], we considered an additive polynomial $f(X)$ whose roots belong to the base field, and we proved results analogous to those obtained by Garcia and Stichtenoth. More generally, we studied abelian extensions of type $C_{p^m}^n$, where C_j denotes a cyclic group of order j, and such that the base field contains the finite field $\mathbb{F}_q$, with $q = p^n$. For instance, given an additive polynomial $f(X)$, we have that, if the roots of f are in the base field, any elementary abelian p-extension can be obtained by means of an equation of the type $f(X) = u$. Furthermore, all the subextensions of degree p over the base field can be deduced from the equation $f(X) = u$.

We have studied genus fields in [**19, 20, 21**]. The general result we present here goes along the lines of the proof we presented in [**19**], but it is much simpler since, now, we consider in merely one step the tame and the wild ramifications of the infinite prime. In [**19**], we first studied the case of tame ramification of the infinite primes and then the general case. It turns out that it is possible to consider the general case in only one step and, in fact, this approach gives the genus field much faster and in a more transparent manner. Furthermore, in [**19**], we restricted ourselves to geometric extensions. Here, we consider general, not necessarily geometric, finite abelian extensions.

Our objective in this paper is to give a full solution to the genus field problem for finite abelian extensions K of k. We use this approach to study finite abelian p-extensions of k. Obtaining the genus field of this family of extensions is much more transparent than the manner in which it was obtained in [**19**].

We use the following notation. Let $k = \mathbb{F}_q(T)$ be a global rational function field of characteristic p. Let $R_T = \mathbb{F}_q[T]$ be the polynomial ring. Let R_T^+ denote the set of all monic irreducible polynomials in R_T. For $N \in R_T$, $k(\Lambda_N)$ denotes the Nth Carlitz cyclotomic function field. Let $\mathcal{P}_\infty$ be the pole of the principal divisor (T) in k, which we call the *infinite prime*. The maximal real subfield $k(\Lambda_N)^+$ of $k(\Lambda_N)$ is the decomposition field of the infinite prime. For any field L such that $k \subseteq L \subseteq k(\Lambda_N)$, the real subfield L^+ of L is

$$L^+ := k(\Lambda_N)^+ \cap L.$$

General results on cyclotomic function fields can be consulted in [**26,** Chapter 12]. Let K/k be a finite abelian extension. From the Kronecker-Weber theorem, we have that there exist $n, m \in \mathbb{N}$ and $N \in R_T$ such that

$$K \subseteq {}_nk(\Lambda_N)_m := L_nk(\Lambda_N)\mathbb{F}_{q^m},$$

where L_n denotes the subfield of $k(\Lambda_{1/T^{n+1}})$ of degree q^n and $k_m := \mathbb{F}_{q^m}(T)$ is the extension of constants of k of degree m. We have that $\mathcal{P}_\infty$ is totally and wildly ramified in L_n/k. We also have that $\mathcal{P}_\infty$ is totally inert in k_m/k.

For any finite abelian extension F of k, $S_\infty(F)$ denotes the set of prime divisors of F above $\mathcal{P}_\infty$. For any finite abelian field extension E/F, let $e_\infty(E/F)$, $f_\infty(E/F)$ and $h_\infty(E/F)$ denote the ramification

index, the inertia degree and the decomposition number of $S_\infty(F)$ in E, respectively. For $P \in R_T^+$, $e_P(E/F)$ denotes the ramification index of any prime in F above P in E/F. For any extension F/k, let $F_{\mathfrak{ge}}$ denote the genus field of F over k with $S = S_\infty(F)$. When F/k is a finite abelian extension, $F_{\mathfrak{ge}}$ is the maximal abelian extension contained in the Hilbert class field of F. The symbol C_d will denote the cyclic group of d elements.

Let $M := L_n k_m$. Then,

$$e_\infty(M/k) = q^n, \qquad f_\infty(M/k) = m \quad \text{and} \quad h_\infty(M/k) = 1. \tag{1.1}$$

We have $M \cap k(\Lambda_N) = k$.

Our first main result is stated later as Theorem 2.2.

Theorem 1.1. *Let K/k be a finite abelian extension with the above notation. Let*

$$E := KM \cap k(\Lambda_N).$$

Then,

$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1} K = (E_{\mathfrak{ge}} K)^H,$$

where H is the decomposition group of any prime in $S_\infty(K)$ in $E_{\mathfrak{ge}}K/K$, $H_1 := H|_{E_{\mathfrak{ge}}}$ and $H_2 := H_1|_E$.

Let $d := f_\infty(EK/K)$. We have

$$H \cong H_1 \cong H_2 \cong C_d$$

and $d \mid q-1$. We also have that $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ and $EK/E^{H_2}K$ are extensions of constants of degree d. Finally, the field of constants of $K_{\mathfrak{ge}}$ is $\mathbb{F}_{q^t}$, where t is the degree of $S_\infty(K)$ in K.

As a corollary, we obtain the general description of the genus field of abelian p-extensions in Theorem 2.3.

In the classical case, the analogue to Theorem 1.1 is the following.

Theorem 1.2. *Let K be an abelian extension of $\mathbb{Q}$, and let X be the group of Dirichlet characters corresponding to K. For any rational prime p and each Dirichlet character χ, let χ_p be the pth component of χ. Set*

$$X_p = \{\chi_p \mid \chi \in X\}.$$

Let

$$Y := \prod_{p \in \mathcal{P}} X_p,$$

where the product runs through the set of rational primes $\mathcal{P}$. Then, if L is the field corresponding to Y, L is the maximal abelian extension of $\mathbb{Q}$ containing K such that L/K is unramified at every finite rational prime.

Our second main result is the description of what we call the *conductor of constants* of an abelian extension K/k. The classical Kronecker-Weber theorem establishes that every finite abelian extension of $\mathbb{Q}$, the field of rational numbers, is contained in a cyclotomic field. Equivalently, the maximal abelian extension of $\mathbb{Q}$ is the union of all cyclotomic fields. In 1974, Hayes **[13]** proved the analogous result for rational congruence function fields. He proved that the maximal abelian extension of k is the composite of three linearly disjoint fields: the first is the union of all cyclotomic function fields; the second is the union of all constant extensions; and, the third is the union of all the subfields of the corresponding cyclotomic function fields, where the infinite prime is totally wildly ramified.

Given a finite abelian extension K/k, by the Kronecker-Weber theorem, we have

$$K \subseteq {}_n k(\Lambda_N)_m$$

for some $n, m \in \mathbb{N}$ and $N \in R_T$. The minimum N and n can be found by class field theory by means of the conductor related to the finite primes and the infinite prime, respectively. However, m does not belong to this category. In this paper, we define the *conductor of constants* as the minimum m satisfying this condition and describe m in terms of some other invariants of the extension. This is given in Theorem 3.1.

The third main result is the explicit description of genus fields of finite abelian p-extensions of rational function fields in the case where we have enough constants. This is given in Theorem 5.1. More precisely, in the notation of Witt vectors, if $k = \mathbb{F}_q(T)$ and if $\mathbb{F}_v \subseteq \mathbb{F}_q$, then any finite abelian p-extension K/k with Galois group of rank v can be given as $K(\vec{y})$ where $\vec{y}$ is given by a Witt equation of the form

$$\vec{y}^{p^v} \overset{\bullet}{-} \vec{y} = \vec{\beta} \in W_m(k).$$

When $\mathbb{F}_v \not\subseteq \mathbb{F}_q$, the field K cannot be described by this type of equation.

To describe the genus fields of finite abelian p-extensions of rational function fields without sufficient constants, we first prove a result on the genus field of a composite of finite abelian extensions of degree relatively prime to the order of the multiplicative group of the field of constants, which shows that the genus field of the composite is the composite of the respective genus fields. The description of the genus field of an arbitrary finite abelian extension of a global rational function field of degree relatively prime to the order of the multiplicative group of the field of constants is the final main result, Theorem 6.9.

2. The genus field. The general results on genus fields, as presented in the introduction, which are necessary throughout this paper, can be found in **[19, 20]**.

First, we present a new proof of the fact that, if $K \subseteq k(\Lambda_N)$, then $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. For a group of Dirichlet characters X, and for $P \in R_T^+$, we set

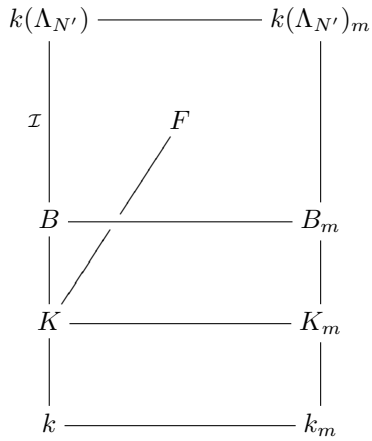
$$X_P = \{\chi_P \mid \chi \in X\},$$

where χ_P is the Pth component of χ. We refer to **[26,** Chapter 12] for the use of Dirichlet characters.

Theorem 2.1. *Let $k \subseteq K \subseteq k(\Lambda_N)$ for some $N \in R_T^+$. Then, $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Furthermore, if the group of Dirichlet characters of K is X, and, if L is the field associated to $Y = \prod_{P \in R_T^+} X_P$, then*

$$K_{\mathfrak{ge}} = KL^+.$$

Proof. Let F/K be an unramified abelian extension so that the elements of $S_\infty(K)$ are fully decomposed in F/K. In particular, $\mathcal{P}_\infty$ is tamely ramified. By the Kronecker-Weber theorem, we have $F \subseteq K(\Lambda_{N'})_m$ for some $N' \in R_T^+$, $m \in \mathbb{N}$. Let $\mathcal{I}$ be the inertia group of $S_\infty(K)$ in $k(\Lambda_{N'})/k$, and let $B = k(\Lambda_{N'})^{\mathcal{I}}$. Since the elements of $S_\infty(B)$ are of degree 1, they are fully inert in B_m/B. Furthermore, the elements of $S_\infty(B)$ are fully ramified in $k(\Lambda_{N'})/B$. Now, the elements of $S_\infty(K)$ are fully decomposed in B/K; thus, we obtain that B is the decomposition field of $S_\infty(K)$ in $k(\Lambda_{N'})_m/K$. It follows that $F \subseteq B \subseteq k(\Lambda_{N'})$.



Let Z be the group of Dirichlet characters associated to F. Since F/K is unramified, it follows that $X \subseteq Z \subseteq Y$, that is, $F \subseteq L$ since L is the maximal abelian extension contained in some cyclotomic function field such that L/K is unramified in the finite primes. In particular, we may take $N' = N$. Therefore, $K_{\mathfrak{ge}} = L^{\mathcal{D}}$, where $\mathcal{D}$ is the decomposition group of $S_\infty(K)$ in L/K. Now, $S_\infty(K)$ fully decompose in KL^+/K since $\mathcal{P}_\infty$ fully decomposes in L^+/k. Since L/K is unramified, we have

$$KL^+ \subseteq L$$

so that KL^+/K is unramified. Hence, $KL^+ \subseteq K_{\mathfrak{ge}}$, and we obtain that

$$KL^+ \subseteq K_{\mathfrak{ge}} \subseteq L.$$

Finally, we see that $S_\infty(KL^+)$ is fully ramified in the extension L/KL^+. In fact, this follows from the facts that $L^+ \subseteq KL^+ \subseteq L$, and $S_\infty(L^+)$ is totally ramified in L/L^+. Since $KL^+ \subseteq K_{\mathfrak{ge}} \subseteq L$, and $K_{\mathfrak{ge}}/KL^+$ is unramified, it follows that $K_{\mathfrak{ge}} = KL^+ \subseteq k(\Lambda_N)$. □

Our first main result is the following.

Theorem 2.2. *Let K/k be a finite abelian extension such that $K \subseteq {}_nk(\Lambda_N)_m$. Let $M = L_nk_m$, and let*

$$E := KM \cap k(\Lambda_N).$$

Then,

$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1} K = (E_{\mathfrak{ge}} K)^H,$$

where H is the decomposition group of any prime in $S_\infty(K)$ in $E_{\mathfrak{ge}}K/K$, $H_1 := H|_{E_{\mathfrak{ge}}}$ and $H_2 := H_1|_E$. Let $d := f_\infty(EK/K)$. We have $H \cong H_1 \cong H_2 \cong C_d$ and $d \mid q-1$. We also have that $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ and $EK/E^{H_2}K$ are extensions of constants of degree d. Finally, the field of constants of $K_{\mathfrak{ge}}$ is $\mathbb{F}_{q^t}$, where t is the degree of $S_\infty(K)$ in K.

Proof. The proof that the field of constants of $K_{\mathfrak{ge}}$ is $\mathbb{F}_{q^t}$ is the same as that in [**19,** Lemma 4.1]. We repeat the argument for the sake of completeness. Let K_r be the extension of constants of K of degree r. Since the degree of any element of $S_\infty(K)$ is t, the elements of $S_\infty(K)$ decompose into $\gcd(t,r)$ elements of K_r (see [**26,** Theorem 6.2.1]). Therefore, the elements of $S_\infty(K)$ fully decompose if and only if $\gcd(t,r) = r$ if and only if $r \mid t$. The assertion follows.

Since $k(\Lambda_N) \cap M = k$ and $E = KM \cap k(\Lambda_N)$, from the Galois correspondence, between $k(\Lambda_N)/k$ and $k(\Lambda_N)M/M$, E corresponds to KM. Hence, $KM = EM$ corresponds to E. Thus,

$$KM = EM.$$

Now,

$$\begin{aligned} E \cap K \subseteq E_{\mathfrak{ge}} \cap K \subseteq k(\Lambda_N) \cap K &= (KM \cap k(\Lambda_N)) \cap k(\Lambda_N) \cap K \\ &= E \cap k(\Lambda_N) \cap K = E \cap K. \end{aligned}$$

Therefore,

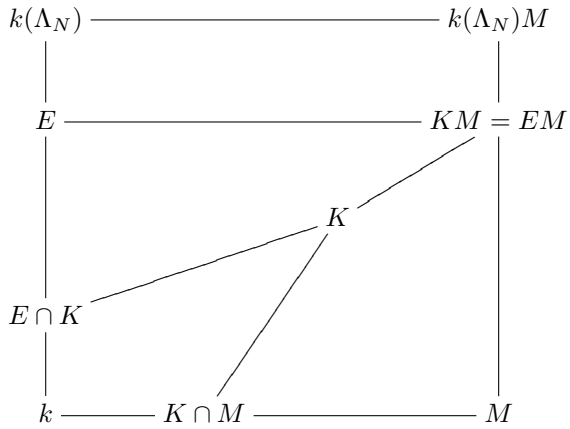
$$E \cap K = E_{\mathfrak{ge}} \cap K = k(\Lambda_N) \cap K.$$

We have $[E : k] = [EM : M] = [KM : M] = [K : K \cap M]$. Thus,

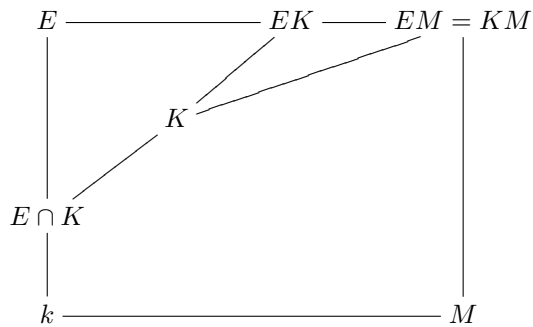
$$[K : k] = [E : k][K \cap M : k]. \tag{2.1}$$

Next, we prove that EK/K is unramified. First, note that

$$E \subseteq EK \subseteq EKM = E \cdot EM = EM.$$



In the extension M/k, $\mathcal{P}_\infty$ is the only ramified prime. Hence, in KM/E, the only possible ramified primes are those in $S_\infty(E)$. We also have that, in the extension KM/K, the only possible ramified primes are the elements of $S_\infty(K)$ and, since $K \subseteq EK \subseteq EM = KM$, the only possible ramified primes in EK/K are those in $S_\infty(K)$.



From (1.1), we have

$$e_\infty(EK/K) \mid e_\infty(M/K \cap M)$$

and

$$e_\infty(M/K \cap M) \mid e_\infty(M/k) = q^n.$$

On the other hand, we have

$$e_\infty(EK/K) \mid e_\infty(E/E \cap K)$$

and

$$e_\infty(E/E\cap K) \mid e_\infty(k(\Lambda_N)/k) = q-1.$$

Thus,

$$e_\infty(EK/K) \mid \gcd(q^n, q-1) = 1,$$

and EK/K is unramified.

Now, we have that

$$e_\infty(EK/K)f_\infty(EK/K) \mid e_\infty(E/E\cap K)f_\infty(E/E\cap K),$$

and $e_\infty(EK/K) = 1$, $f_\infty(E/E\cap K) = 1$. Hence,

$$f_\infty(EK/K) \mid e_\infty(E/E\cap K) \quad \text{and} \quad e_\infty(E/E\cap K) \mid q-1.$$

Thus, $f_\infty(EK/K) \mid q-1$. Therefore, we have that EK/K is unramified, the inertia degree of $S_\infty(K)$ in EK/K is $d = f_\infty(EK/K)$, and $d \mid q-1$. Since $E_{\mathfrak{ge}}/E$ is unramified and $S_\infty(E)$ fully decomposes in $E_{\mathfrak{ge}}/E$, the same holds in $E_{\mathfrak{ge}}K/EK$. In this way, we obtain that $E_{\mathfrak{ge}}K/K$ is an unramified extension, and the inertia degree of $S_\infty(K)$ is d.

Recall that H is the decomposition group of any prime in $S_\infty(K)$ in $E_{\mathfrak{ge}}K/K$, and let $H_1 := H|_{E_{\mathfrak{ge}}}$. Observe that $|H| = d$. Since $E_{\mathfrak{ge}}\cap K = E\cap K$, from the Galois correspondence, we obtain that $H \cong H_1$, $|H| = |H_1|$ and $E_{\mathfrak{ge}}^{H_1}K = (E_{\mathfrak{ge}}K)^H$. Analogously, $H_2 \cong H_1$. Furthermore, $H_1 \subseteq I_\infty(k(\Lambda_N)/k) \cong C_{q-1}$, where I_∞ denotes the inertia group of $\mathcal{P}_\infty$. Therefore, H is a cyclic group, $H \cong H_1 \cong H_2 \cong C_d$. Since $S_\infty(K)$ fully decomposes in $E_{\mathfrak{ge}}^{H_1}K/K$, it follows that

$$E_{\mathfrak{ge}}^{H_1}K \subseteq K_{\mathfrak{ge}}.$$

Let $E_1 := EE_{\mathfrak{ge}}^{H_1} \subseteq E_{\mathfrak{ge}}$. Now, $H_1 \subseteq I_\infty(E/E\cap K)$, so $S_\infty(E_{\mathfrak{ge}}^{H_1})$ is fully ramified in $E_{\mathfrak{ge}}/E_{\mathfrak{ge}}^{H_1}$. Therefore, $S_\infty(E_1)$ is fully ramified in $E_{\mathfrak{ge}}/E_1$. On the other hand, $S_\infty(E)$ fully decomposes in $E_{\mathfrak{ge}}/E$. Hence, $S_\infty(E_1)$ fully decomposes in $E_{\mathfrak{ge}}/E_1$, that is, $S_\infty(E_1)$ ramifies and fully decomposes in $E_{\mathfrak{ge}}/E_1$. Therefore,

$$E_{\mathfrak{ge}} = E_1 = EE_{\mathfrak{ge}}^{H_1}.$$

It follows that

$$(E_{\mathfrak{ge}}K)^H = E_{\mathfrak{ge}}^{H_1}K \subseteq K_{\mathfrak{ge}} \quad \text{and} \quad EE_{\mathfrak{ge}}^{H_1} = E_{\mathfrak{ge}}.$$

To prove the other containment, we define $C := K_{\mathfrak{ge}}M \cap k(\Lambda_N)$. We have

$$E \subseteq EM = KM \subseteq K_{\mathfrak{ge}}M, \quad E \subseteq k(\Lambda_N).$$

Therefore,

$$E \subseteq K_{\mathfrak{ge}}M \cap k(\Lambda_N) = C,$$

that is, $E \subseteq C$. Furthermore, $E_{\mathfrak{ge}}^{H_1} \subseteq E_{\mathfrak{ge}}^{H_1}K \subseteq K_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}M$ and $E_{\mathfrak{ge}}^{H_1} \subseteq E_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Thus, $E_{\mathfrak{ge}}^{H_1} \subseteq K_{\mathfrak{ge}}M \cap k(\Lambda_N) = C$. Hence, $E_{\mathfrak{ge}}^{H_1} \subseteq C$. Therefore,

$$E_{\mathfrak{ge}} = EE_{\mathfrak{ge}}^{H_1} \subseteq C. \tag{2.2}$$

Since $C = K_{\mathfrak{ge}}M \cap k(\Lambda_N)$, from the Galois correspondence, we have $CM = K_{\mathfrak{ge}}M$. Now, since $K_{\mathfrak{ge}}/K$ is unramified and $S_\infty(K)$ fully decomposes, it follows that

$$CM/KM \quad \text{is unramified and } S_\infty(KM) \text{ fully decomposes.} \tag{2.3}$$

We now prove that C/E is unramified. From (2.3), it follows that CM/KM is unramified. Now, in $KM = EM$ over E, the only ramified primes are those in $S_\infty(E)$, and they have ramification index equal to q^n. It follows that the only ramified primes in CM/E are those in $S_\infty(E)$. Hence, the only possible ramified primes in C/E are those in $S_\infty(E)$. Now,

$$e_\infty(C/E) \mid e_\infty(CM/E) = q^n$$

and

$$e_\infty(C/E) \mid e_\infty(k(\Lambda_N)/k) = q - 1,$$

so that

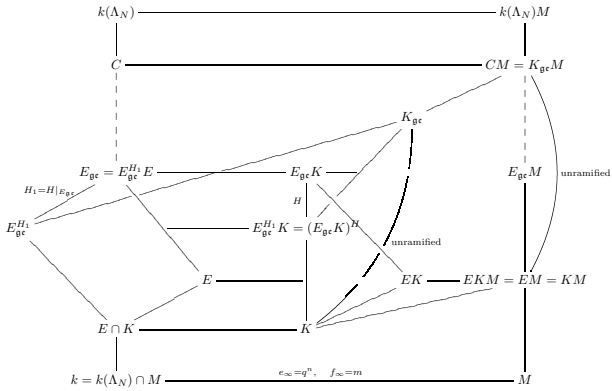
$$e_\infty(C/E) \mid \gcd(q^n, q-1) = 1.$$

Therefore, C/E is an unramified extension.

On the other hand, since $S_\infty(E)$ is unramified in C/E, $S_\infty(E)$ fully decomposes in C/E since $C \subseteq k(\Lambda_N)$. It follows that $C \subseteq E_{\mathfrak{ge}}$. From this and equation (2.2), we obtain

$$C = E_{\mathfrak{ge}} \quad \text{and} \quad E_{\mathfrak{ge}}M = CM = K_{\mathfrak{ge}}M.$$

We have $E_{\mathfrak{ge}}K \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}}$. Since $K_{\mathfrak{ge}}/K$ is unramified and $S_\infty(K)$ fully decomposes in $K_{\mathfrak{ge}}$, the same holds in $E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K$. In particular, $h_\infty(E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K) = [E_{\mathfrak{ge}}K_{\mathfrak{ge}} : E_{\mathfrak{ge}}K]$.

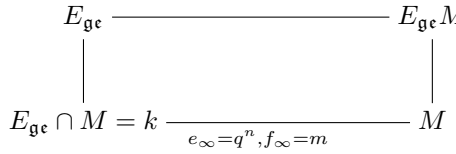


Now, in the extension $E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}$, the only ramified primes are those in $S_\infty(E_{\mathfrak{ge}})$, and we have

$$e_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}) = q^n \quad \text{and} \quad f_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}) = m$$

since $e_\infty(E_{\mathfrak{ge}}/k) \mid q-1$, which is relatively prime to q,

$$f_\infty(E_{\mathfrak{ge}}/k) = 1, e_\infty(M/k) = q^n \quad \text{and} \quad f_\infty(M/k) = m.$$



Let F_1 and F_2 be two fields such that $k \subseteq F_1 \subseteq F_2 \subseteq M$. Let $R_i = E_{\mathfrak{ge}}F_i$, $i = 1, 2$. Since $f_\infty(E_{\mathfrak{ge}}/k) = 1$ and $e_\infty(E_{\mathfrak{ge}}/k) \mid q-1$, it follows from the Galois correspondence between M/k and $E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}$ that $e_\infty(R_i/E_{\mathfrak{ge}}) = e_\infty(F_i/k)$ and $f_\infty(R_i/E_{\mathfrak{ge}}) = f_\infty(F_i/k)$, $i = 1, 2$. Therefore, $e_\infty(F_2/F_1) = e_\infty(R_2/R_1)$ and $f_\infty(F_2/F_1) = f_\infty(R_2/R_1)$.

Since $h_\infty(M/k) = 1$, we have $h_\infty(R_2/R_1) = 1$. In particular,

$$\begin{aligned} R_1 \neq R_2 &\iff F_1 \neq F_2 \iff e_\infty(F_2/F_1) > 1 \quad \text{or} \quad f_\infty(F_2/F_1) > 1 \\ &\iff e_\infty(R_2/R_1) > 1 \quad \text{or} \quad f_\infty(R_2/R_1) > 1. \end{aligned} \tag{2.4}$$

Also, since

$$E_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M,$$

$S_\infty(E_{\mathfrak{ge}}K)$ is unramified in $E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K$, and $S_\infty(E_{\mathfrak{ge}}K)$ fully decomposes; thus, we obtain that

$$e_\infty(E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K) = 1 \quad \text{and} \quad f_\infty(E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K) = 1.$$

From (2.4), it follows that

$$E_{\mathfrak{ge}}K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K.$$

Therefore, $K_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$. Since $E_{\mathfrak{ge}}K/K$ is unramified, if $\mathcal{D}$ is the decomposition group of $S_\infty(K)$ in $E_{\mathfrak{ge}}K/K$, we obtain that $K_{\mathfrak{ge}} = (E_{\mathfrak{ge}}K)^{\mathcal{D}}$. Then, we have

$$f_\infty(E_{\mathfrak{ge}}K/K) = f_\infty(E_{\mathfrak{ge}}K/EK)f_\infty(EK/K) = 1 \cdot d = d.$$

Hence, $\mathcal{D} = H$ and $K_{\mathfrak{ge}} = (E_{\mathfrak{ge}}K)^{\mathcal{D}} = (E_{\mathfrak{ge}}K)^H = E_{\mathfrak{ge}}^{H_1}K$.

Finally, it remains to show that $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ and $EK/E^{H_2}K$ are extensions of constants. Since $K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M$ and $E_{\mathfrak{ge}}K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$, we have

$$K_{\mathfrak{ge}} = (E_{\mathfrak{ge}}K)^H \subseteq E_{\mathfrak{ge}}K \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M.$$

Set $F_1 = K_{\mathfrak{ge}} \cap M$ and $F_2 = E_{\mathfrak{ge}}K \cap M$. We have

$$\begin{aligned} d &= [E_{\mathfrak{ge}}K : K_{\mathfrak{ge}}] = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}) = [F_2 : F_1] \\ &= e_\infty(F_2/F_1)f_\infty(F_2/F_1)h_\infty(F_2/F_1). \end{aligned}$$

Since $e_\infty(F_2/F_1) \mid q^n$ and $h_\infty(F_2/F_1) = 1$, it follows that

$$e_\infty(F_2/F_1) = e_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}) = 1$$

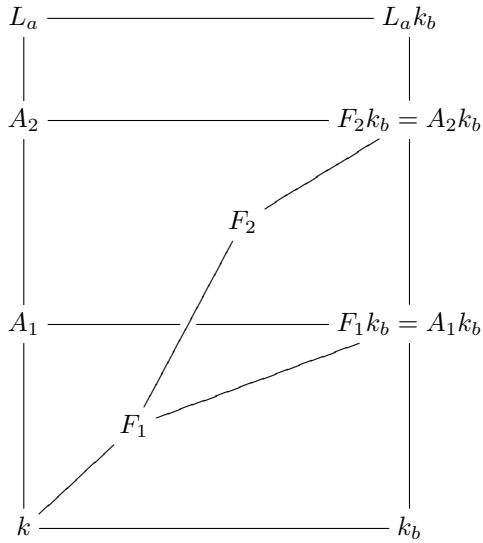
and

$$f_\infty(F_2/F_1) = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}) = d.$$

Therefore, $k \subseteq F_1 \subseteq F_2 \subseteq M$ and $e_\infty(F_2/F_1) = 1$.

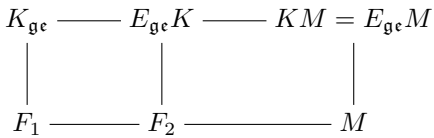
Let a and b be such that $F_2 \subseteq F_1k_bL_a$. Let $A_i = F_ik_b \cap L_a$, $i = 1, 2$. Note that, since $e_\infty(F_2/F_1) = 1$ and $F_ik_b = A_ik_b/A_i$, $i = 1, 2$, are extensions of constants, we have $e_\infty(A_2/A_1) = 1$. Since L_a/k is totally ramified at $\mathcal{P}_\infty$, it follows that $A_1 = A_2$. Therefore, $F_2k_b = F_1k_b$, and

F_2/F_1 is an extension of constants.



$$e_\infty(F_2k_b/F_1k_b) = e_\infty(F_2/F_1) = e_\infty(A_2/A_1) = 1.$$

Recall that $F_1 = K_{\mathfrak{ge}} \cap M$. We consider $K_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K \subseteq K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M$:



Therefore, $K_{\mathfrak{ge}} \subseteq F_2K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$. It follows that $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ is an extension of constants of degree $[E_{\mathfrak{ge}}K : K_{\mathfrak{ge}}] = |H| = d$. The proof that $EK/E^{H_2}K$ is an extension of constants is completely similar. This concludes the proof of the theorem. □

For the particular case of a finite abelian p-extension, we have that, on one hand, $d \mid q-1$ and, on the other hand, $d \mid [EK : K]$. Since K/k is a p-extension, we obtain from (2.1) that E/k is also a p-extension. Finally, since

$$\mathrm{Gal}(EK/k) \longrightarrow \mathrm{Gal}(E/k) \times \mathrm{Gal}(K/k), \quad \sigma \mapsto (\sigma|_E, \sigma|_K)$$

is injective, and it follows that EK/k is also a p-extension. Therefore, $d \mid p^a$ for some a. Thus, $d = 1$. We have proved the following.

Theorem 2.3. *With the above notation, let K/k be a finite abelian p-extension. Let*

$$E := KM \cap k(\Lambda_N).$$

Then, $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$ and $K_{\mathfrak{ge}}/k$ is an abelian p-extension.

Proof. The last assertion follows from the fact that $E_{\mathfrak{ge}}/k$ is also an abelian p-extension. □

With the same proof as that for Theorem 2.2, we obtain the following.

Theorem 2.4. *Let K/k be a finite abelian extension. Let*

$$R := K_m \cap {}_nk(\Lambda_N).$$

Then,

$$K_{\mathfrak{ge}} = R_{\mathfrak{ge}}^{\mathcal{H}_1}K = (R_{\mathfrak{ge}}K)^{\mathcal{H}},$$

where $\mathcal{H}$ is the decomposition group at infinity in $R_{\mathfrak{ge}}K/K$, $\mathcal{H}_1 := \mathcal{H}|_{R_{\mathfrak{ge}}}$ and $\mathcal{H}_2 := \mathcal{H}_1|_R$.

Let $d^* := f_\infty(RK/K)$. We have $\mathcal{H} \cong \mathcal{H}_1 \cong \mathcal{H}_2 \cong C_{d^*}$ and $d^* \mid q-1$. We also have that $R_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ and $RK/R^{\mathcal{H}_2}K$ are extensions of constants of degree d^*. Finally, the field of constants of $K_{\mathfrak{ge}}$ is $\mathbb{F}_{q^t}$, where t is the degree of $S_\infty(K)$ in K.

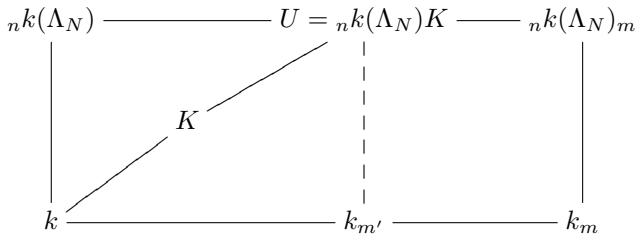
3. Conductor of constants. Let K be a finite abelian extension of k. By the Kronecker-Weber theorem, we have that there exist $n, m \in \mathbb{N}$ and $N \in R_T$ such that $K \subseteq {}_nk(\Lambda_N)_m$. The minima n and N satisfying this condition are given by class field theory using local conductors of the extension K/k: n for $\mathcal{P}_\infty$ and N for the finite primes.

In this section, we will determine the minimum m satisfying the above condition, and we will see that this m is related to the number d given in Theorem 2.2. The number m will be called the *conductor of constants* of the abelian extension K/k.

Note that, in general, $\mathbb{F}_{q^m}$ is neither the field of constants of K nor that of $K_{\mathfrak{ge}}$. For instance, let $q \equiv 3 \bmod 4$. Since $\sqrt{-1} \notin \mathbb{F}_q$, we have $k(\sqrt{-T}) \neq K := k(\sqrt{T})$. The field of constants of K is $\mathbb{F}_q$, and K is not cyclotomic. In fact, $K \subseteq k(\Lambda_T)\mathbb{F}_{q^2}$, and $m = 2$ is the conductor of constants of K. We also have, in this case, that $K_{\mathfrak{ge}} = K$.

Now, let $n, m \in \mathbb{N}$ and $N \in R_T$ be such that $K \subseteq {}_nk(\Lambda_N)_m$ and where m is the minimum with respect to this condition. Note that m may depend on n and N. Consider the following diagram of Galois extensions, that is, let $U := {}_nk(\Lambda_N)K$ and $k_{m'} := U \cap k_m$. From the Galois correspondence, we have that

$$U = {}_nk(\Lambda_N)K = {}_nk(\Lambda_N)k_{m'} = {}_nk(\Lambda_N)_{m'} \supseteq K.$$



Since m is minimal, we obtain that $m' = m$, that is, m is determined by the equality

$$ {}_nk(\Lambda_N)K = {}_nk(\Lambda_N)_m. \tag{3.1}$$

Now, we shall see that m is independent of n and N. Let $n_i \in \mathbb{N}$, $N_i \in R_T$ and $m_i \in \mathbb{N}$ be the minimum such that $K \subseteq {}_{n_i}k(\Lambda_{N_i})_{m_i}$, $i = 1, 2$. Let $n_0 := \max\{n_1, n_2\}$, $N_0 = \operatorname{lcm}[N_1, N_2]$ and $m_0 \in \mathbb{N}$ be minimum such that $K \subseteq {}_{n_0}k(\Lambda_{N_0})_{m_0}$. From (3.1), it follows that

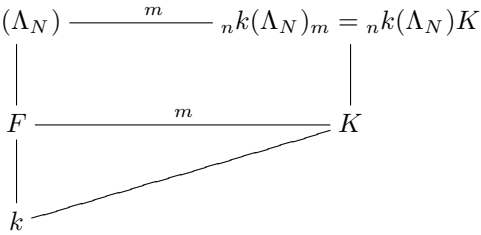
$$\begin{aligned} {}_{n_0}k(\Lambda_{N_0})K &= L_{n_0}\big({}_{n_i}k(\Lambda_{N_i})k(\Lambda_{N_0})\big)K = L_{n_0}\big({}_{n_i}k(\Lambda_{N_i})K\big)k(\Lambda_{N_0}) \\ &= L_{n_0}\big({}_{n_i}k(\Lambda_{N_i})_{m_i}k(\Lambda_{N_0})\big) = {}_{n_0}k(\Lambda_{N_0})_{m_i}, \end{aligned}$$

and

$$ {}_{n_0}k(\Lambda_{N_0})K = {}_{n_0}k(\Lambda_{N_0})_{m_0}.$$

Therefore, $m_1 = m_2 = m_0$.

Hence, we consider $K \subseteq {}_nk(\Lambda_N)_m$ with m the minimum. Let $F := K \cap {}_nk(\Lambda_N)$, and consider the following Galois square (see (3.1)):



Let t be the degree of $S_\infty(K)$ in K, that is, $t = f_\infty(K/k)$. We have

$$e_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) = 1,$$
$$f_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) = m.$$

In particular,

$$\{1\} = I_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) \subseteq I_\infty(K/F),$$
$$C_m \cong D_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) \subseteq D_\infty(K/F).$$

Since $[K : F] = m$ and $m \leq |D_\infty(K/F)| \leq [K : F] = m$, it follows that $|D_\infty(K/F)| = m$ and $D_\infty(K/F) \cong C_m$. In particular, we have $h_\infty(K/F) = 1$ and $h_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) = 1$.

On the other hand, we have

$$t = f_\infty(K/k) = f_\infty(K/F)f_\infty(F/k) = f_\infty(K/F) \cdot 1 = f_\infty(K/F),$$

that is, $f_\infty(K/F) = t$. Furthermore,

$$e_\infty(K/F)f_\infty(K/F)h_\infty(K/F) = e_\infty(K/F) \cdot t \cdot 1 = m,$$

so that $e_\infty(K/F) = m/t$. Hence,

$$\begin{aligned} m = [K : F] &= f_\infty(K/F)e_\infty(K/F) = te_\infty(K/F) \\ &= t\frac{e_\infty(K/k)}{e_\infty(F/k)}. \end{aligned} \tag{3.2}$$

Now, we shall investigate the relation between the numbers m and $d = f_\infty(E_{\mathfrak{gc}}K/K_{\mathfrak{gc}})$, given in Theorem 2.2. Recall that $M = L_nk_m$, $E = KM \cap k(\Lambda_N)$ and $EM = KM$. We have

$$E_{\mathfrak{gc}} \subseteq E_{\mathfrak{gc}}K \subseteq E_{\mathfrak{gc}}KL_n \subseteq E_{\mathfrak{gc}}KM = E_{\mathfrak{gc}}EM = E_{\mathfrak{gc}}M.$$

Let $A := E_{\mathfrak{ge}}K \cap M$ and $B := E_{\mathfrak{ge}}KL_n \cap M$. From the Galois correspondence, we have $E_{\mathfrak{ge}}K = E_{\mathfrak{ge}}A$ and $E_{\mathfrak{ge}}KL_n = E_{\mathfrak{ge}}B$.

$$\begin{array}{ccccccc} E_{\mathfrak{ge}} & \text{——} & E_{\mathfrak{ge}}K & \text{——} & E_{\mathfrak{ge}}KL_n & \text{——} & E_{\mathfrak{ge}}M \\ | & & | & & | & & | \\ k & \text{————} & A & \text{————} & B & \text{————} & M \end{array}$$

We also have $L_n \subseteq E_{\mathfrak{ge}}KL_n \cap M = B \subseteq M = L_nk_m$. Therefore, B/L_n is an extension of constants, say, $B = L_nk_{m'}$ with $m' \mid m$. From the Galois correspondence, we obtain

$$K \subseteq E_{\mathfrak{ge}}KL_n = E_{\mathfrak{ge}}B = E_{\mathfrak{ge}}L_nk_{m'} \subseteq k(\Lambda_N)L_nk_{m'} = {}_nk(\Lambda_n)_{m'}.$$

Since m is the minimum, $m' = m$, $B = M$ and $E_{\mathfrak{ge}}KL_n = E_{\mathfrak{ge}}M$.

Now, $E_{\mathfrak{ge}}(AL_n) = (E_{\mathfrak{ge}}A)L_n = (E_{\mathfrak{ge}}K)L_n = E_{\mathfrak{ge}}M$. Again, from the Galois correspondence, it follows that $AL_n = M$. We consider the following Galois square:

$$\begin{array}{ccc} L_n & \text{———} & AL_n = M = L_nk_m \\ | & & | \\ A \cap L_n & \text{—————} & A \end{array}$$

We have

$$f_\infty(AL_n/L_n) = f_\infty(M/L_n) = m$$

and

$$e_\infty(AL_n/L_n) = e_\infty(M/L_n) = 1.$$

Thus,

$$\{1\} = I_\infty(AL_n/L_n) \subseteq I_\infty(A/A \cap L_n)$$

and

$$C_m \cong D_\infty(AL_n/L_n) \subseteq D_\infty(A/A \cap L_n).$$

Due to the fact that $[A : A \cap L_n] = [M : L_n] = m$, it follows that

$$D_\infty(A/A \cap L_n) \cong C_m, \qquad e_\infty(A/A \cap L_n) = 1$$

and $f_\infty(A/A \cap L_n) = m$. Therefore,

$$f_\infty(E_{\mathfrak{ge}}K/k) = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}})f_\infty(K_{\mathfrak{ge}}/K)f_\infty(K/k) = d \cdot 1 \cdot t = dt = td.$$

Thus,

$$f_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}K) = \frac{f_\infty(E_{\mathfrak{ge}}M/k)}{f_\infty(E_{\mathfrak{ge}}K/k)} = \frac{m}{td}.$$

Finally,

$$\begin{aligned}\frac{m}{td} &= f_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}K)|[E_{\mathfrak{ge}}M : E_{\mathfrak{ge}}K] = [M : A] \\ &= [L_n : A \cap L_n]|[L_n : k] = q^n.\end{aligned}$$

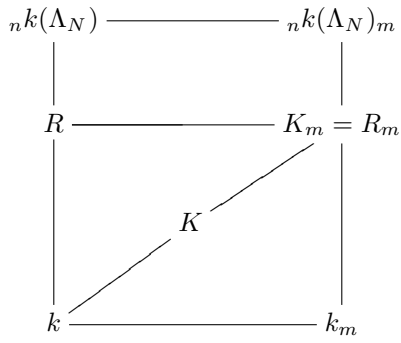
It follows that

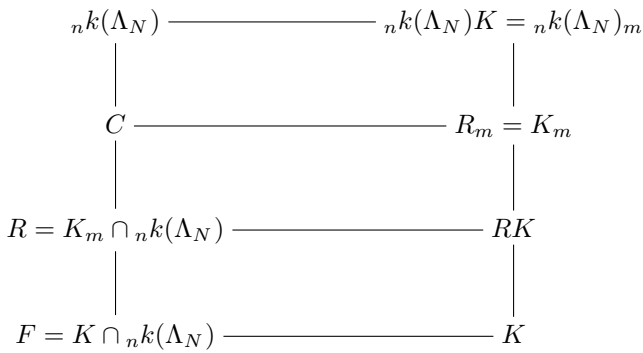
$$m = tdp^s,$$

for some $s \in \mathbb{N} \cup \{0\}$. Furthermore, $f_\infty(K_m/K) = m/t = e_\infty(K/F)$. Note that

$$td = f_\infty(K/k)f_\infty(EK/K) = f_\infty(EK/k).$$

We compute m in another way. Recall $F = K \cap_n k(\Lambda_N)$, and consider the following Galois squares:





Since $R = K_m \cap {}_nk(\Lambda_N)$, it follows that $K_m = R_m$. Now, $K, R \subseteq RK \subseteq K_m = R_m$.

Note that, in general, $R \neq F$. For instance, if $q \equiv 3 \bmod 4$, $\sqrt{-1} \notin \mathbb{F}_q^*$, and, if $K := k(\sqrt{T})$, then $n = 1, m = 2, N = T$ and

$$F = K \cap {}_nk(\Lambda_N) = k(\sqrt{T}) \cap k(\Lambda_T) = k,$$

$$R = K_m \cap {}_nk(\Lambda_N) = \mathbb{F}_{q^2}(\sqrt{T}) \cap k(\Lambda_T) = k(\sqrt{-T}) \neq k.$$

Let $C := K_m \cap {}_nk(\Lambda_N)$. Then, $C = R$, and, from the Galois correspondence, we have $RK = R_m = K_m$. It follows that the field of constants of RK is $\mathbb{F}_{q^m}$. The field of constants of $RK_{\mathfrak{ge}}$ is also $\mathbb{F}_{q^m}$. Now, the field of constants of $K_{\mathfrak{ge}}$ is $\mathbb{F}_{q^t}$.

On the other hand, we have that $RK_{\mathfrak{ge}}/R_{\mathfrak{ge}}^{\mathcal{H}_1}K = K_{\mathfrak{ge}}$ is an extension of constants of degree $d^* = |\mathcal{H}_1|$. Thus, the field of constants of $RK_{\mathfrak{ge}}$ is $\mathbb{F}_{q^{td^*}}$. It follows that $td^* = m$.

We have obtained the following.

Theorem 3.1 (Conductor of constants)**.** *Let K be a finite abelian extension of k. Let $n, m \in \mathbb{N}$ and $N \in R_T$ be such that $K \subseteq {}_nk(\Lambda_N)_m$ and m is minimum with this property. Then, m is independent of n and N. Let $t = f_\infty(K/k) = f_\infty(K/F)$ be the degree of the infinite primes of K.*

(a) *Let $M = L_nk_m$, $E = KM \cap k(\Lambda_N)$, $F = K \cap {}_nk(\Lambda_N)$ and $d = f_\infty(EK/K) = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}})$. Then,*

$$_nk(\Lambda_N)K = {}_nk(\Lambda_N)_m$$

and

$$m = [K : F] = te_\infty(K/F) = tdp^s = f_\infty(EK/k)p^s$$

for some $s \geq 0$. *In particular,*

$$e_\infty(K/F) = dp^s = f_\infty(K_m/K).$$

(b) *Let* $R = K_m \cap {}_nk(\Lambda_N)$ *and* $d^* = f_\infty(RK/K)$. *Then,*

$$m = te_\infty(K/F) = td^* = f_\infty(RK/k).$$

In particular,

$$d^* = f_\infty(RK/K) = e_\infty(K/F).$$

Remark 3.2. When $p \nmid m/t$, in particular, when K/k is tamely ramified at $\mathcal{P}_\infty$, we have $s = 0$ and $m = td$. When K/k is not tamely ramified, we may have $s \geq 1$.

Example 3.3. Let p be any prime, and let $q = p$. Let $X := 1/T$. We have $L_1 := k(\Lambda_{X^2})^{\mathbb{F}_p^*}$ and $[L_1 : k] = p$. We have that L_1/k is an Artin-Schreier extension. It is unnecessary to give the explicit description of L_1; however, for the sake of convenience, we give a generator of L_1. Let λ be a generator of Λ_{X^2} such that λ^{p-1} is a generator of $k(\Lambda_{X^2})^+ = L_1$. Now, λ is a root of the cyclotomic polynomial $\Psi_{X^2}(u)$ (see **[26,** Chapter 12]). We have that $\Psi_{X^2}(u) = \Psi_X(u^X)$, where u^X denotes the Carlitz action. Since $\Psi_X(u) = u^X/u = u^{p-1} + X$, it follows that $\Psi_{X^2}(\lambda) = (\lambda^p + X\lambda)^{p-1} + X$. Set $\mu := \lambda^{p-1}$ and $\xi := \mu + X$. Then, we obtain

$$\xi^p - X\xi^{p-1} + X = 0.$$

Finally, if $\delta := 1/\xi$, then $L_1 = k(\delta)$ with

$$\delta^p - \delta = -1/X = -T, \quad \delta = T/(T\lambda^{p-1} + 1).$$

Let α be a solution of $y^p - y = 1$. Then, $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^p}$, $k_p = \mathbb{F}_p(\alpha)(T) = \mathbb{F}_{p^p}(T)$ and $L_1k_p = k(\alpha, \delta)$. The $p + 1$ extensions K/k of degree p over k such that $k \subseteq K \subseteq L_1k_p$ are $\{k(\alpha + i\delta)\}_{i=0}^{p-1}$ and L_1. Set $K := k(\alpha + \delta)$. Then, $K \neq k_p$ and $K \neq L_1$. Hence, $K = k(z)$ with $z^p - z = 1 - T$.

Let $N \in R_T$ be arbitrary. Then, $K \subseteq L_1k_p \subseteq {}_1k(\Lambda_N)_p$ and $K \nsubseteq {}_1k(\Lambda_N)_1$. Therefore, $m = p$ and $M = L_1k_p$. We have $f_\infty(K/k) = 1$

and $e_\infty(K/k) = p$. We also have $E := KM \cap k(\Lambda_N) = M \cap k(\Lambda_N) = k$. Therefore, $E_{\mathfrak{ge}} = k$ and $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K = K$. It follows that $EK = K$ and $f_\infty(EK/K) = d = 1$. Hence, $td = 1 \neq m = p$. In this example, $s = 1$.

Remark 3.4. From Theorems 2.2 and 2.4, it follows that, if $K \subseteq {}_nk(\Lambda_N)_m$, then $K_{\mathfrak{ge}} \subseteq {}_nk(\Lambda_N)_m$. In particular, the conductors of constants of K and $K_{\mathfrak{ge}}$ are the same.

4. Genus fields of subfields of cyclotomic function fields. For an abelian extension K/k, the explicit description of $K_{\mathfrak{ge}}$, that is, a description in terms of the generating equation of $K_{\mathfrak{ge}}$, depends upon the explicit description of $E_{\mathfrak{ge}}$ (Theorem 2.2). In this section, we present some details in order to find $E_{\mathfrak{ge}}$. For results and notation regarding Dirichlet characters we use, the reader is referred to **[26,** Chapter 12]. Here, K denotes a field $k \subseteq K \subseteq k(\Lambda_N)$ for some $N \in R_T$ and $k = \mathbb{F}_q(T)$.

Remark 4.1. Let $k \subseteq K \subseteq k(\Lambda_N)$, and let X be the group of Dirichlet characters associated to K. If L is the field associated to $\prod_{P \in R_T^+} X_P$, then

$$K_{\mathfrak{ge}} = L^{\mathcal{D}},$$

where $\mathcal{D}$ is the decomposition group of any prime $\mathfrak{p} \in S_\infty(K)$ in L/K.

Proposition 4.2. *With the notation as above, let X be the group of Dirichlet characters corresponding to K. Fix $P \in R_T^+$. Let Y be a group of Dirichlet characters such that $Y = Y_P$, that is, for any $\chi \in Y$, the conductor of χ is a power of P: $\mathcal{F}_\chi = P^{\alpha_\chi}$ for some $\alpha_\chi \in \mathbb{N} \cup \{0\}$. Let L be the field associated to $\langle X, Y\rangle$, that is, if F is the field associated to Y, then $L = KF$. If KF/K is unramified at P, then $Y \subseteq X_P$.*

Proof. We have

$$|\langle X, Y\rangle_P| = e_P(KF/k) = e_P(KF/K)e_P(K/k) = e_P(K/k) = |X_P|.$$

Since $X_P \subseteq \langle X, Y\rangle_P$, it follows that $X_P = \langle X, Y\rangle_P$. In addition, since $Y_P \subseteq \langle X, Y\rangle_P$, the result follows. □

Corollary 4.3. *If $|Y| = |X_P|$, then $Y = X_P$.*

Next, we apply Proposition 4.2 to Kummer extensions of k and to finite abelian p-extensions of k.

4.1. Kummer extensions. From Proposition 4.2 and **[21,** subsection 5.2], we obtain the following.

Theorem 4.4. *Let X be the group of Dirichlet characters associated to $K = k\big(\sqrt[t]{\gamma D}\big)$ with $t \mid q-1$, $D \in R_T$ and is t-power free,*

$$D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}, \quad r \geq 1,\ 1 \leq \alpha_i \leq t-1,\ 1 \leq i \leq r,$$

$\gamma = (-1)^{\deg D}$. Let $d_i = \gcd(t, \alpha_i)$, $1 \leq i \leq r$. Then, the field associated to

$$\prod_{P \in R_T^+} X_P = \prod_{i=1}^{r} X_{P_i}$$

is $L = k(\xi_1, \ldots, \xi_r)$, where

$$\xi_i = \sqrt[t/d_i]{\gamma_i P_i^{\alpha_i/d_i}} \quad \text{and} \quad \gamma_i = (-1)^{\deg P_i^{\alpha_i/d_i}},$$

that is,

$$L = k\Big(\sqrt[t]{(-1)^{\deg P_1^{\alpha_1}} P_1^{\alpha_1}}, \ldots, \sqrt[t]{(-1)^{\deg P_r^{\alpha_r}} P_r^{\alpha_r}}\Big),$$

and the genus field of K is $K_{\mathfrak{gc}} = L^{\mathcal{D}}$, where $\mathcal{D}$ is the decomposition group of any prime $\mathfrak{p} \in S_\infty(K)$ in L/K.

4.2. Abelian p-extensions. For any field F, $W_v(F)$ denotes the ring of Witt vectors of length v. The Witt operations will be denoted by $\overset{\bullet}{+}$ and $\overset{\bullet}{-}$. We now consider $K = k(\vec{y})$, where

$$\vec{y}^{\,p^u} \overset{\bullet}{-} \vec{y} = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r,$$

with $\vec{\delta}_i = (\delta_{i,1}, \ldots, \delta_{i,v})$ for some $v \in \mathbb{N}$, $\delta_{i,j} = Q_{i,j}/P_i^{e_{i,j}}$, $e_{i,j} \geq 0$, $Q_{i,j} \in R_T$. Here, we assume that $\mathbb{F}_{p^u} \subseteq \mathbb{F}_q$ and $K \subseteq k(\Lambda_N)$ for some $N \in R_T$. Let X be the group of characters associated to K. According to Schmid **[25]**, the ramification index of P_i in K/k is determined by the first index j such that we may write $\delta_{i,j} = Q_{i,j}/P_i^{e_{i,j}}$ with $\gcd(Q_{i,j}, P_i) = 1$, $e_{i,j} > 0$ and $\gcd(e_{i,j}, p) = 1$, in other words, the ramification index of P_i at K/k depends only upon $\vec{\delta}_i$ and not upon

$\vec{\delta}_1, \ldots, \vec{\delta}_{i-1}, \vec{\delta}_{i+1}, \ldots, \vec{\delta}_r$. Therefore, if Y is the group of characters associated to

$$F_i = k(\vec{y}_i) \quad \text{with} \quad \vec{y}_i^{\,p^u} \overset{\bullet}{-} \vec{y}_i = \vec{\delta}_i, \quad 1 \leq i \leq r,$$

we have $|X_{P_i}| = |Y| = |Y_{P_i}|$. Furthermore, the extension

$$KF_i = k(\vec{y}, \vec{y}_i) = k(\vec{y}, \vec{y} \overset{\bullet}{-} \vec{y}_i) = K(\vec{y} \overset{\bullet}{-} \vec{y}_i)$$

is unramified at P_i over K. It follows that the field associated to

$$\prod_P X_P = \prod_{i=1}^r X_{P_i}$$

is $k(\vec{y}_1, \ldots, \vec{y}_r)$ (Proposition 4.2). Here, the decomposition group $\mathcal{D}$ is trivial. Then, we have (see Remark 4.1) the following.

Theorem 4.5. *With the conditions as above, if $K = k(\vec{y})$, then the field associated to $\prod_P X_{P \in R_T^+} = \prod_{i=1}^r X_{P_i}$ is*

$$L = k(\vec{y}_1, \ldots, \vec{y}_r),$$

and the genus field of K is also

$$K_{\mathfrak{ge}} = k(\vec{y}_1, \ldots, \vec{y}_r).$$

5. Explicit description of genus fields of abelian p-extensions. The reader may consult **[19, 27]** for the theory of Witt vectors. Let K/k be a finite abelian p-extension. Recall that $k = k_0(T)$ with $k_0 = \mathbb{F}_q$, say $q = p^l$. We will assume that $\mathbb{F}_{p^u} \subseteq k_0$, that is, $u \mid l$. Then, we have

$$\mathrm{Gal}(K/k) \cong \left(\mathbb{Z}/p^{\alpha_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p^{\alpha_u}\mathbb{Z}\right)$$

with $1 \leq \alpha_1 \leq \cdots \leq \alpha_u = v$. There exist $\vec{w}_1, \ldots, \vec{w}_u \in W_v(\overline{k})$ such that $\vec{w}_i^{\,p} \overset{\bullet}{-} \vec{w}_i = \vec{\xi}_i \in W_v(k)$, with $K = k(\vec{w}_1, \cdots, \vec{w}_v)$. We also have that there exists a $\vec{y}_0 \in W_v(\overline{k})$ such that $K = k(\vec{y}_0)$ with

$$\vec{y}_0^{\,p^u} \overset{\bullet}{-} \vec{y}_0 = \vec{\xi}_0 \quad \text{for some } \vec{\xi}_0 \in W_v(k)$$

(see **[4,** Theorem 8.5]). Here, $\overline{k}$ denotes an algebraic closure of k.

Let $P_1, \dots, P_r \in R_T^+$ be the finite primes in k ramified in K. From [**4,** Theorem 8.10] it follows that we may decompose $\vec{\xi}_0$ as

$$\vec{\xi}_0 = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r \overset{\bullet}{+} \vec{\gamma}, \tag{5.1}$$

where $\delta_{i,j} = Q_{i,j}/P_i^{e_{i,j}}$, $e_{i,j} \geq 0$, $Q_{i,j} \in R_T$ and, if $e_{i,j} > 0$, then

$$e_{i,j} = \lambda_{i,j} p^{m_{i,j}}, \qquad \gcd(\lambda_{i,j}, p) = 1, \quad 0 \leq m_{i,j} < n,$$

$\gcd(Q_{i,j}, P_i) = 1$ and $\deg(Q_{i,j}) < \deg(P_i^{e_{i,j}})$, and $\gamma_j = f_j(T) \in R_T$ with $\deg f_j = \nu_j p^{m_j}$ and $\gcd(q, \nu_j) = 1$, $0 \leq m_j < n$, when $f_j \notin k_0$. If the ramification index of P_i is $p^{a_i} < p^v$, we may write

$$\vec{\delta}_i = (\delta_{i,1}, \dots, \delta_{i,v}) = (0, \dots, 0, \delta_{i,(v-a_i+1)}, \dots, \delta_{i,v}),$$

in particular, $\mathcal{P}_\infty$ fully decomposes in $k(\vec{y}_i)/k$, where $\vec{y}_i^{\,p^u} \overset{\bullet}{-} \vec{y}_i = \vec{\delta}_i$ (see [**4,** Theorem 8.13]).

Let $\vec{z}^{\,p^u} \overset{\bullet}{-} \vec{z} = \vec{\gamma}$. In $k(\vec{z})/k$, the only possible ramified prime is $\mathcal{P}_\infty$. Note that, if

$$\vec{y} = \vec{y}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{y}_r,$$

then

$$\vec{y}^{\,p^u} \overset{\bullet}{-} \vec{y} = \vec{\xi}_0 \overset{\bullet}{-} \vec{\gamma} = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r,$$

and $\mathcal{P}_\infty$ fully decomposes in $k(\vec{y})/k$. We have $\vec{y}_0 = \vec{y} \overset{\bullet}{+} \vec{z}$, $k(\vec{z}) \subseteq M$ and $k(\vec{y} \overset{\bullet}{+} \vec{z}) \subseteq k(\vec{y})k(\vec{z})$.

The first main result of this section is the following.

Theorem 5.1. *With the above notation, let $E = KM \cap k(\Lambda_N)$. Then, $E = k(\vec{y})$, $E_{\mathfrak{ge}} = k(\vec{y}_1, \dots, \vec{y}_r)$, and*

$$K_{\mathfrak{ge}} = k(\vec{y}_1, \dots, \vec{y}_r, \vec{z}).$$

Proof. From the Galois correspondence, $EM = KM$. To prove $E = k(\vec{y})$ is equivalent to showing $k(\vec{y})M = KM$ since $k(\vec{y}) \subseteq k(\Lambda_N)$. Now, $k(\vec{z}) \subseteq M$ since $M = L_n \mathbb{F}_{q^m}(T)$ codifies all inertia and ramification, which is totally wild, of $\mathcal{P}_\infty$. We have

$$k(\vec{y})M = k(\vec{y})k(\vec{z})M \supseteq k(\vec{y} \overset{\bullet}{+} \vec{z})M = KM.$$

In addition,

$$KM = Kk(\vec{z})M = k(\vec{y}_0)k(\vec{z})M \supseteq k(\vec{y}_0 \overset{\bullet}{-} \vec{z})M = k(\vec{y})M.$$

Thus,

$$KM = k(\vec{y})M \quad \text{and} \quad E = k(\vec{y}).$$

From **[19]** (see also Theorem 4.5), we obtain $E_{\mathfrak{ge}} = k(\vec{y}_1, \ldots, \vec{y}_r)$. Finally,

$$\begin{aligned} K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K &= k(\vec{y}_1, \ldots, \vec{y}_r)k(\vec{y}_0) \\ &= k(\vec{y}_1, \ldots, \vec{y}_r)k(\vec{y}_0 \overset{\bullet}{-} \vec{y}_1 \overset{\bullet}{-} \cdots \overset{\bullet}{-} \vec{y}_r) \\ &= k(\vec{y}_1, \ldots, \vec{y}_r)k(\vec{z}) = k(\vec{y}_1, \ldots, \vec{y}_r, \vec{z}). \end{aligned}$$

This concludes the proof. □

Remark 5.2.

(a) Observe that, with the above conditions,

$$[k(\vec{y}_i) : k] = e_{P_i}(K/k)$$

and

$$[k(\vec{z}) : k] = e_{\infty}(K/k) \cdot f_{\infty}(K/k).$$

(b) Note that the proof of Theorem 5.1 works even in the case where $\vec{\delta}_i$ and $\vec{\gamma}$ are not in the reduced form described above. We only need that, in each extension $\vec{y}_i^{\,p^u} \overset{\bullet}{-} \vec{y}_i = \vec{\delta}_i$, $1 \le i \le r$, and $\vec{z}^{\,p^u} \overset{\bullet}{-} \vec{z} = \vec{\gamma}$, there is at most one ramifying prime.

From Theorem 2.3, the cases of Artin-Schreier and Witt extensions and elementary abelian p-extensions are an immediate consequence of Theorem 5.1.

Corollary 5.3 (**[19,** Theorems 5.4, 5.7]). *Let $E = F(T)$, where F is a finite field.*

(a) *Let $K = E(y)$ with*

$$y^p - y = \alpha = \sum_{i=1}^{r} \frac{Q_i}{P_i^{e_i}} + f(T),$$

where $P_i \in R_T^+$, $Q_i \in R_T$, $\gcd(P_i, Q_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\deg Q_i < \deg P_i^{e_i}$, $1 \le i \le r$, $f(T) \in R_T$, *with* $p \nmid \deg f$ *when* $f(T) \notin F$. *Then,*

$$K_{\mathfrak{gc}} = E(y_1, \dots, y_r, \beta),$$

where $y_i^p - y_i = Q_i/P^{e_i}$, $1 \le i \le r$ *and* $\beta^p - \beta = f(T)$.

(b) *Let* $K = E(\vec{y})$, *where*

$$\vec{y}^{\,p} \overset{\bullet}{-} \vec{y} = \vec{\beta} = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r \overset{\bullet}{+} \vec{\mu},$$

with $\delta_{i,j} = Q_{i,j}/P_i^{e_{i,j}}$, $e_{i,j} \ge 0$, $Q_{i,j} \in R_T$, $\gcd(Q_{i,j}, P_i) = 1$ *and, if* $e_{i,j} > 0$, *then* $p \nmid e_{i,j}$, $\deg(Q_{i,j}) < \deg(P_i^{e_{i,j}})$, *and* $\mu_j = f_j(T) \in R_T$ *with* $p \nmid \deg f_j$ *when* $f_j \notin F$. *Then,*

$$K_{\mathfrak{gc}} = E(\vec{y}_1, \dots, \vec{y}_r, \vec{z}),$$

where $\vec{y}_i^{\,p} \overset{\bullet}{-} \vec{y}_i = \vec{\delta}_i$, $1 \le i \le r$ *and* $\vec{z}^{\,p} \overset{\bullet}{-} \vec{z} = \vec{\mu}$.

(c) *Assume that* $\mathbb{F}_{p^u} \subseteq F$. *Let* $K = E(y)$, *with*

$$y^{p^u} - y = \alpha = \sum_{i=1}^{r} \frac{Q_i}{P_i^{e_i}} + f(T),$$

where $P_i \in R_T^+$, $Q_i \in R_T$ *and* $f(T) \in F[T]$. *Then,*

$$K_{\mathfrak{gc}} = E(y_1, \dots, y_r, z),$$

where $y_i^{p^u} - y_i = Q_i/P_i^{e_i}$, $1 \le i \le r$ *and* $z^{p^u} - z = f(T)$.

6. General finite abelian extensions of k. Up until now, we have given the explicit description of the genus fields of abelian p-extensions K of $k = k_0(T)$, where $k_0 = \mathbb{F}_q$ is such that $\mathbb{F}_{p^u} \subseteq k_0$, $K = k(\vec{y})$, and $\vec{y}$ is given by an equation of the form $\vec{y}^{\,p^u} \overset{\bullet}{-} \vec{y} = \vec{\beta} \in W_m(k)$. When $\mathbb{F}_{p^u} \not\subseteq k_0$, the field K cannot be given by this type of equation.

In this section, we explicitly give the description of $K_{\mathfrak{gc}}$, where K/k is a finite abelian extension of degree t with $\gcd(t, q-1) = 1$. The case $t \mid q-1$ is treated in subsection 4.1.

Remark 6.1. For any abelian extension K/k of degree t with $\gcd(t, q-1) = 1$, we have that, if $E = KM \cap k(\Lambda_N)$, then $[E : k] \mid t$, see (2.1). If X is the set of Dirichlet characters of E, we have $\gcd(|X|, q-1) = \gcd([E : k], q-1) = 1$. Since, for any $\chi \in X$ and

$P \in R_T^+$, we have that $\chi_P^{|X|} = 1$, we obtain that $\gcd([E_{\mathfrak{ge}} : k], q-1) = 1$. In particular, $H = \{1\}$. Therefore, $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$.

Remark 6.2. In general, if K_1 and K_2 are two finite extensions of k, we have

$$(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} \subseteq (K_1K_2)_{\mathfrak{ge}};$$

however, we may have $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} \subsetneq (K_1K_2)_{\mathfrak{ge}}$. In fact, let $q > 2$ and P, Q, R, $S \in R_T$ be four different monic polynomials in R_T. Set $L_1 := k(\Lambda_{PQ})^+$ and $L_2 := k(\Lambda_{RS})^+$. Then, $(L_i)_{\mathfrak{ge}} = L_i$, $i = 1, 2$. Therefore, $(L_1)_{\mathfrak{ge}}(L_2)_{\mathfrak{ge}} = L_1L_2$. On the other hand, $(L_1L_2)_{\mathfrak{ge}} = k(\Lambda_{PQRS})^+$ and $[L_{\mathfrak{ge}} : L] = q - 1 > 1$. Thus, $(L_1L_2)_{\mathfrak{ge}} = L_{\mathfrak{ge}} \neq L = (L_1)_{\mathfrak{ge}}(L_2)_{\mathfrak{ge}}$.

We will show that, for finite abelian extensions of k of degree relatively prime to $q - 1$, we have equality. In particular, if K_1 and K_2 are finite abelian p-extensions of k, we have equality.

For a subfield $K \subseteq k(\Lambda_N)$ for some $N \in R_T$, denote by $K'_{\mathfrak{ge}}$ the maximal abelian extension of K contained in $k(\Lambda_N)$, unramified at the finite primes. We have (see Remark 4.1):

$$K_{\mathfrak{ge}} = (K'_{\mathfrak{ge}})^{\mathcal{D}}, \tag{6.1}$$

where $\mathcal{D}$ is the decomposition group at infinity in $K'_{\mathfrak{ge}}/K$.

Consider $K_i \subseteq k(\Lambda_N)$, $i = 1, 2$, and let X_i be the group of Dirichlet characters associated to K_i. Therefore, $Y = X_1X_2 = \langle X_1, X_2\rangle$ is the group of Dirichlet characters associated to $L = K_1K_2$. Let $P \in R_T^+$. It is easy to see that

$$\langle X_1, X_2\rangle_P = \langle (X_1)_P, (X_2)_P\rangle,$$

so that we obtain

$$\prod_{P\in R_T^+} Y_P = \prod_{P\in R_T^+} \langle X_1, X_2\rangle_P = \Big(\prod_{P\in R_T^+} (X_1)_P\Big) \cdot \Big(\prod_{P\in R_T^+} (X_2)_P\Big).$$

It follows that

$$(K_1)'_{\mathfrak{ge}}(K_2)'_{\mathfrak{ge}} = (K_1K_2)'_{\mathfrak{ge}}.$$

We have proved the following.

Proposition 6.3. *For $K_i \subseteq k(\Lambda_N)$, $i = 1, 2$, we have*

$$(K_1)'_{\mathfrak{ge}}(K_2)'_{\mathfrak{ge}} = (K_1K_2)'_{\mathfrak{ge}}.$$

Corollary 6.4. *Let $K_i \subseteq k(\Lambda_N)$, $i = 1, 2$, be such that K_1/k and K_2/k are finite abelian extensions of degrees relatively prime to $q - 1$. Then, $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = (K_1K_2)_{\mathfrak{ge}}$.*

Proof. Since the decomposition groups of $\mathcal{P}_\infty$ in K_1/k, K_2/k and K_1K_2/k are the unit group, it follows from (6.1) that $(K_i)_{\mathfrak{ge}} = (K_i)'_{\mathfrak{ge}}$, $i = 1, 2$, and $(K_1K_2)_{\mathfrak{ge}} = (K_1K_2)'_{\mathfrak{ge}}$. The result follows from Proposition 6.3. □

Corollary 6.5. *Let K_i/k, $i = 1, 2$, be two finite abelian extensions of degrees relatively prime to $q - 1$. Then*

$$(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = (K_1K_2)_{\mathfrak{ge}}.$$

Proof. Let $k_0 = \mathbb{F}_{p^l}$, $K_i \subseteq L_nk(\Lambda_N)\mathbb{F}_{p^{lm}}(T)$, $i = 1, 2$, and let $M := L_n\mathbb{F}_{p^{lm}}(T)$. Set $E_i := K_iM \cap k(\Lambda_N)$, $i = 1, 2$, and $E := K_1K_2M \cap k(\Lambda_N)$. Using the Galois correspondence, it can be proven that $E = E_1E_2$. From Corollary 6.4, we have $E_{\mathfrak{ge}} = (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$. Therefore,

$$\begin{aligned}(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} &= (E_1)_{\mathfrak{ge}}K_1 \cdot (E_2)_{\mathfrak{ge}}K_2 = (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}} \cdot K_1K_2 \\ &= E_{\mathfrak{ge}} \cdot K_1K_2 = (K_1K_2)_{\mathfrak{ge}}.\end{aligned}$$

Thus, $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = (K_1K_2)_{\mathfrak{ge}}$. □

Corollary 6.6. *Let K_i/k, $i = 1, 2$ be two finite abelian p-extensions. Then,*

$$(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = (K_1K_2)_{\mathfrak{ge}}.$$

As a consequence, we obtain the description of the genus field of a finite abelian p-extension of k.

Corollary 6.7. *Let K/k be a finite abelian p-extension with Galois group*

$$\mathrm{Gal}(K/k) = G \cong G_1 \times \cdots \times G_s$$

with $G_i \cong \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$, $1 \le i \le s$. *Let* K *be the composite* $K = K_1 \cdots K_s$ *such that* $\mathrm{Gal}(K_i/k) \cong G_i$. *Let* $P_1, \ldots, P_r$ *be the finite primes ramified in* K/k. *Let* $K_i = k(\vec{w}_i)$ *be given by the equation*

$$\vec{w}_i^{\,p} \overset{\bullet}{-} \vec{w}_i = \vec{\xi}_i, \quad 1 \le i \le s.$$

Write each $\vec{\xi}_i$ *as in* (5.1), *that is,*

$$\vec{\xi}_i = \vec{\delta}_{i,1} \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_{i,r} \overset{\bullet}{+} \vec{\gamma}_i,$$

such that all of the components of $\vec{\delta}_{i,j}$ *are written so that the degree of the numerator is less than the degree of the denominator, the support of the denominator is at most* $\{P_j\}$, *and the components of* $\vec{\gamma}_i$ *are polynomials. Let*

$$\vec{w}_{i,j}^{\,p} \overset{\bullet}{-} \vec{w}_{i,j} = \vec{\delta}_{i,j}, \quad 1 \le i \le s,\ 1 \le j \le r$$

and

$$\vec{z}_i^{\,p} \overset{\bullet}{-} \vec{z}_i = \vec{\gamma}_i, \quad 1 \le i \le s.$$

Then

$$K_{\mathfrak{ge}} = k\big(\vec{w}_{i,j}, \vec{z}_i \mid 1 \le i \le s,\ 1 \le j \le r\big).$$

Proof. From Remark 5.2 (b), we obtain that the genus field $E_{\mathfrak{ge}}$ given in Theorem 5.1 can be obtained in the same way, even if the equation is not given in normal form. Thus, the result follows from Remarks 5.2 (b), Corollary 5.3 (b) and Corollary 6.6. □

Proposition 6.8. *Let* $E \subseteq k(\Lambda_N)$ *be a cyclic extension of* k *of degree* t *relatively prime to* $p(q-1)$. *Let* $P_1, \ldots, P_r \in R_T^+$ *be the primes in* k *ramifying in* E. *Then,*

$$E_{\mathfrak{ge}} = \prod_{j=1}^{r} F_j,$$

where $k \subseteq F_j \subseteq k(\Lambda_{P_j})$ *is the subfield of degree* a_j *over* k, a_j *is the order of* χ_{P_j}, *and* χ *is the character associated to* E.

Proof. We consider a cyclic extension K/k of degree t such that $\gcd(t, p(q-1)) = 1$. We have that $E = KM \cap k(\Lambda_N)$ satisfies that $[E : k]$ is relatively prime to $q-1$. From Remark 4.1, we have $E'_{\mathfrak{ge}} = E_{\mathfrak{ge}}$ and $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$.

The result follows from the fact that $X = \langle \chi \rangle$ is the group of Dirichlet characters associated to E, $E_{\mathfrak{ge}}$ is the field corresponding to $\prod_{j=1}^{r} X_{P_j}$, $X_{P_j} = \langle \chi_{P_j} \rangle$ (see Proposition 4.2) and F_j is the field associated to χ_{P_j}. □

Next is our final, main result.

Theorem 6.9. *Let K/k be an abelian extension of degree t with $\gcd(t, q-1) = 1$. Let $P_1, \ldots, P_r \in R_T^+$ be the primes in k ramifying in K. Let $E = KM \cap k(\Lambda_N) = E_0 E_1 \cdots E_s$, where E_i/k is a cyclic extension of degree t_i, $\gcd(t_i, p(q-1)) = 1$, $1 \leq i \leq s$, and E_0/k is an abelian p-extension. Then*

$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}} K, \quad \text{where } E_{\mathfrak{ge}} = (E_0)_{\mathfrak{ge}} (E_1)_{\mathfrak{ge}} \cdots (E_s)_{\mathfrak{ge}},$$

$(E_0)_{\mathfrak{ge}}$ is given by Corollary 6.7, and $(E_i)_{\mathfrak{ge}} = \prod_{j=1}^{r} F_{i,j}$ is given by Proposition 6.8, $1 \leq i \leq s$. Furthermore, let $b_{i,j} := [F_{i,j} : k]$. Then, $L_j := \prod_{i=1}^{s} F_{i,j}$ is the subfield of $k(\Lambda_{P_j})$ of degree $b_j := \operatorname{lcm}[b_{i,j}, 1 \leq i \leq s]$ over k. We have

$$K_{\mathfrak{ge}} = (E_0)_{\mathfrak{ge}} \left(\prod_{j=1}^{r} L_j \right) K.$$

Proof. The result follows from Theorem 2.2, Corollary 6.6 and Proposition 6.8. □

Acknowledgments. We thank the anonymous referee for his/her very thorough review of this work as well as his/her suggestions which improved the presentation of the article.

REFERENCES

1. B. Anglès and J.-F. Jaulent, *Théorie des genres des corps globaux*, Manuscr. Math. **101** (2000), 513–532.

2. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1967.

3. S. Bae and J.K. Sunghan, *Genus theory for function fields*, J. Australian Math. Soc. **60** (1996), 301–310.

4. J.F. Barreto-Castañeda, F. Jarquín-Zárate, M. Rzedowski-Calderón and G. Villa-Salvador, *Abelian p-extensions and additive polynomials*, Inter. J. Math. **28** (2017), 1750100-1–1750100-32.

5. V. Bautista-Ancona, M. Rzedowski-Calderón and G. Villa-Salvador, *Genus fields of cyclic l-extensions of rational function fields*, Inter. J. Num. Th. **9** (2013), 1249–1262.

6. R. Clement, *The genus field of an algebraic function field*, J. Num. Th. **40** (1992), 359–375.

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

8. ———, *The genus field and genus group in finite number fields*, II, Mathematika **6** (1959), 142–146.

9. ———, *Central extensions, Galois groups and ideal class groups of number fields*, Contemp. Math. **24** (1983).

10. A. Garcia and H. Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscr. Math. **72** (1991), 67–79.

11. C.F. Gauss, *Disquisitiones arithmeticae*, 1801.

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

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

14. S. Hu and Y. Li, *The genus fields of Artin-Schreier extensions*, Finite Fields Appl. **16** (2010), 255–264.

15. M. Ishida, *The genus fields of algebraic number fields*, Lect. Notes Math. **555** (1976).

16. E. Kani, *Relations between the genera and between the Hasse-Witt invariants of Galois coverings of curves*, Canadian Math. Bull. **28** (1985), 321–327.

17. G. Lachaud, *Artin-Schreier curves, exponential sums, and the Carlitz-Uchiyama bound for geometric codes*, J. Num. Th. **39** (1991), 18–40.

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

19. M. Maldonado-Ramírez, M. Rzedowski-Calderón and G. Villa-Salvador, *Genus fields of abelian extensions of congruence rational function fields*, Finite Fields Appl. **20** (2013), 40–54.

20. ———, *Corrigendum to Genus fields of abelian extensions of rational congruence function fields*, Finite Fields Appl. **20**, (2015), 283–285.

21. ———, *Genus fields of congruence function fields*, Finite Fields Appl. **44** (2017), 56–75.

22. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584.

23. G. Peng, *The genus fields of Kummer function fields*, J. Num. Th. **98** (2003), 221–227.

24. M. Rosen, *The Hilbert class field in function fields*, Expos. Math. **5** (1987), 365–378.

25. H.L. Schmid, *Zur Arithmetik der zyklischen p-Körpe*, J. reine angew. Math. **176** (1936), 161–167.

26. G.D. Villa-Salvador, *Topics in the theory of algebraic function fields*, Math. Th. Appl. (2006).

27. E. Witt, *Zyklische Körper und Algebren der Characteristik p von Grad p^n*, J. reine angew. Math. **176** (1936), 126–140.

28. C. Wittmann, *l-class groups of cyclic function fields of degree l*, Finite Fields Appl. **13** (2007), 327–347.

29. X. Zhang, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94** (1985), 393–395.

Centro de Investigación y de Estudios Avanzados del I.P.N., Departamento de Control Automático, Ciudad de México, México
Email address: **jbarreto@ctrl.cinvestav.mx**

Centro de Investigación y de Estudios Avanzados del I.P.N., Departamento de Control Automático, Ciudad de México, México
Email address: **cmontelongo@ctrl.cinvestav.mx**

Centro de Investigación y de Estudios Avanzados del I.P.N., Departamento de Control Automático, Ciudad de México, México
Email address: **mcenigm@gmail.com**

Centro de Investigación y de Estudios Avanzados del I.P.N., Departamento de Control Automático, Ciudad de México, México
Email address: **mrzedowski@ctrl.cinvestav.mx**

Centro de Investigación y de Estudios Avanzados del I.P.N., Departamento de Control Automático, Ciudad de México, México
Email address: **gvillasalvador@gmail.com, gvilla@ctrl.cinvestav.mx**