Palestine Journal of Mathematics

Vol. 2(1) (2013) , 1–5

Tamely ramified extensions and cyclotomic fields in characteristic p

Julio Cesar Salas–Torres, Martha Rzedowski–Calderón and Gabriel Villa–Salvador

Communicated by Jose Luis Lopez-Bonilla

MSC 2010 Classifications: Primary 11R60; Secondary 11R20, 11R58.

Keywords and phrases: congruence function fields, global fields, Kronecker–Weber Theorem, cyclotomic function fields, quadratic extensions

Abstract. Let L be a finite abelian tamely ramified extension of a rational function field. In the spirit of the Kronecker–Weber Theorem, we present a construction of a cyclotomic function field and a constant field extension whose composite contains the given field L.

1 Introduction

The classical Kronecker–Weber Theorem establishes that every finite abelian extension of $\mathbb{Q}$, the field of rational numbers, is contained in a cyclotomic number field. In 1974, D. Hayes [2], defined the concept of cyclotomic function field and proved the analogous result for rational congruence function fields. The proof of this theorem uses class field theory.

In this note we present a proof of this result in the case of a finite abelian tamely ramified extension L of a rational function field k. More precisely, we show that L is contained in the composite of an explicit cyclotomic function field and a constant field extension. As a motivation, we study first quadratic extensions and in this case, we obtain explicitly the constant field extension.

2 Notation

First we give some notations and some results in the theory of cyclotomic function fields [4]. Let $k = \mathbb{F}_q(T)$ be a congruence rational function field, $\mathbb{F}_q$ denoting the finite field of $q = p^s$ elements, where p is the characteristic of the fields. Let $R_T = \mathbb{F}_q[T]$ be the ring of polynomials. For $N \in R_T \setminus \{0\}$, Λ_N denotes the N–torsion of the Carlitz module and $k(\Lambda_N)$ denotes the N–th cyclotomic function field. The degree of the extension $k(\Lambda_N)/k$ is $\Phi(N)$, where Φ, the phi Euler function for function fields, is multiplicative and for an irreducible polynomial P of degree d and $n \in \mathbb{N}$, $\Phi(P^n) = q^{(n-1)d}(q^d - 1)$. The extension $k(\Lambda_N)/k$ is geometric. We denote by $\mathfrak{p}_\infty$ the pole divisor of T in k. In $k(\Lambda_N)/k$, $\mathfrak{p}_\infty$ has ramification index $q-1$ and decomposes into $\frac{|G_N|}{q-1}$ different prime divisors of $k(\Lambda_N)$ of degree 1, where $G_N := \mathrm{Gal}(k(\Lambda_N)/k)$. We denote by R_T^+ the set of monic irreducible polynomials in R_T. The primes that ramify in $k(\Lambda_N)/k$ are $\mathfrak{p}_\infty$ and the polynomials $P \in R_T^+$ such that $P \mid N$, with the exception of the case $q = 2$ and $N \in \{T, T+1, T(T+1)\}$ since in these cases $k(\Lambda_N) = k$.

3 Quadratic Extensions

In this section we study quadratic extensions. This is a particular case of the general result but we include it since it is useful as a concrete example of the general case.

Since we are considering tamely ramified extensions, in this section we assume that the characteristic p of the fields is different from 2. We need a few lemmas.

Lemma 3.1. *Let F/k be a quadratic extension. Then $F = k(\sqrt{M})$, where $M = \alpha \prod_{i=1}^{r} P_i$ is a nonzero square-free polynomial, $\alpha \in \mathbb{F}_q^*$, $P_i \in R_T^+$ for $i \in \{1, ..., r\}$ with $P_i \neq P_j$ if $i \neq j$.*

Proof. Since the characteristic is different from 2, $F = k(y)$, where y satisfies $y^2 + b_1 y + b_0 = 0$, for some $b_0, b_1 \in k$. Then $y = \dfrac{-b_1 \pm \sqrt{b_1^2 - 4b_0}}{2}$ and therefore $F = k(\sqrt{b_1^2 - 4b_0}) =$

$k\left(\sqrt{\frac{f(T)}{g(T)}}\right) = k(\sqrt{f(T)g(T)}) = k(\sqrt{M})$, where M is a nonzero square-free polynomial that can be factored as above. □

Lemma 3.2. *Let $P \in R_T^+$ and $d = \deg P$. Then*

(a) *For d even we have $k(\sqrt{P}) \subseteq k(\Lambda_P)$,*

(b) *For d odd we have $k(\sqrt{-P}) \subseteq k(\Lambda_P)$.*

Proof. Since q is odd, $q-1 = 2l$ for some $l \in \mathbb{N}$. By [3, Exercise 5, page 303] we have two cases:

(a) For d even we have $k(\sqrt[q-1]{P}) \subseteq k(\Lambda_P)$, then $P^{\frac{1}{2}} = P^{\frac{l}{q-1}} = \left(P^{\frac{1}{q-1}}\right)^l$, then $k(\sqrt{P}) \subseteq k(\Lambda_P)$.

(b) For d odd we have $k(\sqrt[q-1]{-P}) \subseteq k(\Lambda_P)$, thus $(-P)^{\frac{1}{2}} = (-P)^{\frac{l}{q-1}} = \left((-P)^{\frac{1}{q-1}}\right)^l$, so that $k(\sqrt{-P}) \subseteq k(\Lambda_P)$.

□

Lemma 3.3. *Let $P \in R_T^+$. Then $k(\sqrt{P}) \subseteq k(\Lambda_P)\mathbb{F}_{q^2}$.*

Proof. For the case when d is odd, $k(\sqrt{P}) = k(\sqrt{-1}\sqrt{-P}) \subseteq k(\sqrt{-1}, \sqrt{-P}) = k(\sqrt{-1})k(\sqrt{-P}) \subseteq k\mathbb{F}_{q^2} \cdot k(\Lambda_P) = k(\Lambda_P)\mathbb{F}_{q^2}$ and for the case d even, we have $k(\sqrt{P}) \subseteq k(\Lambda_P) \subseteq k(\Lambda_P)\mathbb{F}_{q^2}$. □

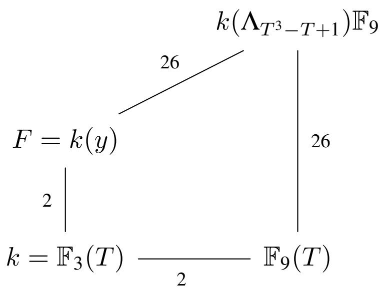
From the above lemmas we obtain explicitly, for a quadratic extension F/k, a composite of a cyclotomic function field and a constant field extension that contains F.

Proposition 3.4. *Let F/k be a quadratic extension. Then $F = k(\sqrt{M}) \subseteq k(\Lambda_M)\mathbb{F}_{q^2}$, where $M = \alpha \prod_{i=1}^{r} P_i$ is a nonzero square-free polynomial, $\alpha \in \mathbb{F}_q^*$, $P_i \in R_T^+$ for $i \in \{1, ..., r\}$ with $P_i \neq P_j$ if $i \neq j$.*

Proof. By Lemma 3.1 such nonzero square-free polynomial $M = \alpha \prod_{i=1}^{r} P_i$ exists. We take $\sqrt{M} = \sqrt{\alpha}\sqrt{P_1}\cdots\sqrt{P_r}$ and since by Lemma 3.3 we have $k(\sqrt{P_i}) \subseteq k(\Lambda_{P_i})\mathbb{F}_{q^2}$ for $i \in \{1, ..., r\}$, we have $k(\sqrt{M}) = k(\sqrt{\alpha}\sqrt{P_1}\cdots\sqrt{P_r}) \subseteq k(\sqrt{P_1})\cdots k(\sqrt{P_r})\mathbb{F}_{q^2} \subseteq k(\Lambda_{P_1})\cdots k(\Lambda_{P_r})\mathbb{F}_{q^2} = k(\Lambda_{P_1\cdots P_r})\mathbb{F}_{q^2} = k(\Lambda_{\alpha P_1\cdots P_r})\mathbb{F}_{q^2} = k(\Lambda_M)\mathbb{F}_{q^2}$. Therefore $F = k(\sqrt{M}) \subseteq k(\Lambda_M)\mathbb{F}_{q^2}$. □

Example 3.5. Let $k = \mathbb{F}_3(T)$ and $F = k(y)$, where $y^2 = T^3 - T + 1$. The polynomial $T^3 - T + 1$ is irreducible modulo 3. For the Kummer extension F/k we have

$$F \subseteq k(\Lambda_{T^3-T+1})\mathbb{F}_9.$$



4 The result

In this section we prove our main result. First we prove the following proposition.

Proposition 4.1. *Let L/k be a finite abelian extension, $P \in R_T^+$ and $d := \deg P$. Assume P is tamely ramified in L/k. If e denotes the ramification index of P in L/k, we have $e \mid q^d - 1$.*

Proof. First we consider in general a finite Galois extension L/k. Let $G_{-1} = D$ be the decomposition group of P, $G_0 = I$ be the inertia group and G_i, $i \geq 1$ be the ramification groups. Let $\mathfrak{P}$ be a prime divisor in L dividing P. Then if $\mathcal{O}_{\mathfrak{P}}$ denotes the valuation ring of $\mathfrak{P}$, we have

$$U^{(i)} = 1 + \mathfrak{P}^i \subseteq \mathcal{O}_{\mathfrak{P}}^* = \mathcal{O}_{\mathfrak{P}} \setminus \mathfrak{P}, i \geq 1, U^{(0)} = \mathcal{O}_{\mathfrak{P}}^*.$$

Let $l(\mathfrak{P}) := \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ be the residue field at $\mathfrak{P}$. The following are monomorphisms:

$$\begin{array}{ccc} G_i/G_{i+1} & \overset{\varphi_i}{\hookrightarrow} & U^{(i)}/U^{(i+1)} \cong \begin{cases} l(\mathfrak{P})^*, i = 0 \\ \mathfrak{P}^i/\mathfrak{P}^{i+1} \cong l(\mathfrak{P}), i \geq 1. \end{cases} \\ \overline{\sigma} & \mapsto & \sigma\pi/\pi \end{array}$$

where π denotes a prime element for $\mathfrak{P}$.

We will prove that if $G_{-1}/G_1 = D/G_1$ is abelian, then

$$\varphi = \varphi_0 \colon G_0/G_1 \longrightarrow U^{(0)}/U^{(1)} \cong \big(\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\big)^*$$

satisfies that $\operatorname{im}\varphi \subseteq \mathcal{O}_P/(P) \cong R_T/(P) \cong \mathbb{F}_{q^d}$. In particular it will follow that $\big|G_0/G_1\big| \mid \big|\mathbb{F}_{q^d}^*\big| = q^d - 1$.

To prove this statement, note that

$$\operatorname{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_P/(P))) \cong D/I = G_{-1}/G_0$$

(see [4, Corollary 5.2.12]).

Let $\sigma \in G_0$ and $\varphi(\bar{\sigma}) = \varphi(\sigma \bmod G_1) = [\alpha] = \alpha \bmod \mathfrak{P} \in \big(\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\big)^*$. Therefore $\sigma\pi \equiv \alpha\pi \bmod \mathfrak{P}^2$.

Let $\theta \in G_{-1} = D$ be arbitrary and let $\pi_1 := \theta^{-1}\pi$. Then π_1 is a prime element for $\mathfrak{P}$. Since φ is independent of the prime element, it follows that $\sigma\pi_1 \equiv \alpha\pi_1 \bmod \mathfrak{P}^2$, that is $\sigma\theta^{-1}\pi \equiv \alpha\theta^{-1}\pi \bmod \mathfrak{P}^2$. Since G_{-1}/G_1 is an abelian group, we have

$$\sigma\pi = (\theta\sigma\theta^{-1})(\pi) \equiv \theta(\alpha)\pi \bmod \mathfrak{P}^2.$$

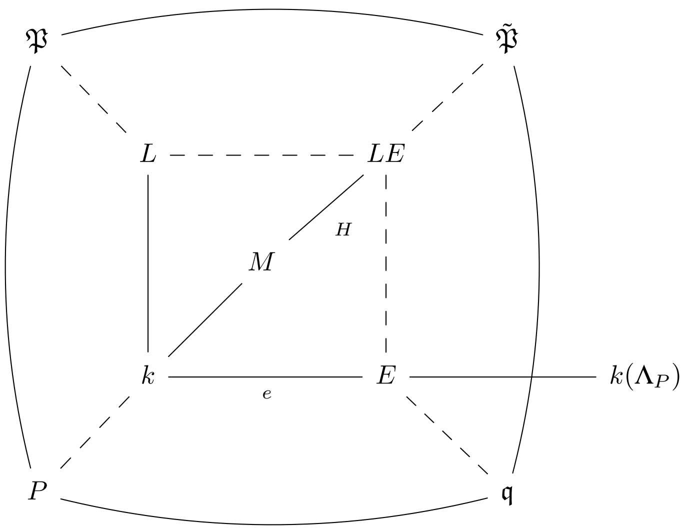
Thus $\sigma\pi \equiv \theta(\alpha)\pi \bmod \mathfrak{P}^2$ and $\sigma\pi \equiv \alpha\pi \bmod \mathfrak{P}^2$. It follows that $\theta(\alpha) \equiv \alpha \bmod \mathfrak{P}$ for all $\theta \in G_{-1}$.

If we write $\tilde{\theta} = \theta \bmod G_0$, $\tilde{\theta}[\alpha] = [\alpha]$, that is, $[\alpha]$ is a fixed element under the action of the group $G_{-1}/G_0 \cong \operatorname{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_P/(P)))$. We obtain that $[\alpha] \in \mathcal{O}_P/(P)$. Therefore $\operatorname{im}\varphi \subseteq \big(\mathcal{O}_P/(P)\big)^*$ and $\big|G_0/G_1\big| \mid \big|\big(\mathcal{O}_P/(P)\big)^*\big| = q^d - 1$.

Finally, since L/k is abelian and P is tamely ramified, $G_1 = \{1\}$, it follows that $e = |G_0| = |G_0/G_1| \mid q^d - 1$. □

Now consider a finite abelian tamely ramified extension L/k where $P_1, \ldots, P_r$ are the finite ramified primes. Set $P = P_1$ and $d = \deg P$. Let e be the ramification index of P in L. Then by Proposition 4.1 we have $e \mid q^d - 1$. Now P is totally ramified in $k(\Lambda_P)/k$ with ramification index $q^d - 1$. In this extension $\mathfrak{p}_\infty$ has ramification index equal to $q - 1$.

Let $k \subseteq E \subseteq k(\Lambda_P)$ with $[E : k] = e$. Set $\tilde{\mathfrak{P}}$ a prime divisor in LE dividing P. Let $\mathfrak{q} := \tilde{\mathfrak{P}}|_E$ and $\mathfrak{P} := \tilde{\mathfrak{P}}|_L$.



We have $e = e_{L/k}(\mathfrak{P}|P) = e_{E/k}(\mathfrak{q}|P)$. By Abhyankar's Lemma [4, Theorem 12.4.4], we obtain

$$e_{LE/k}(\tilde{\mathfrak{P}}|P) = \text{mcm}[e_{L/k}(\mathfrak{P}|P), e_{E/k}(\mathfrak{q}|P)] = \text{mcm}[e, e] = e.$$

Let $H \subseteq \text{Gal}(LE/k)$ be the inertia group of $\tilde{\mathfrak{P}}/P$. Set $M := (LE)^H$. Then P is unramified in M/k. We want to see that $L \subseteq k(\Lambda_P)M$. Indeed we have $[LE : M] = e$ and $E \cap M = k$ since P is totally ramified in E/k and unramified in M/k. It follows that $[ME : k] = [M : k][E : k]$. Therefore

$$[LE : k] = [LE : M][M : k] = e\frac{[ME : k]}{[E : k]} = e\frac{[ME : k]}{e} = [ME : k].$$

Since $ME \subseteq LE$ it follows that $LE = ME = EM \subseteq k(\Lambda_P)M$. Thus $L \subseteq k(\Lambda_P)M$.

In M/k the finite ramified primes are at most the elements of $\{P_2, \cdots, P_r\}$. In case $r - 1 \geq 1$, we may apply the above argument to M/k and we obtain M_2/k such that at most $r - 2$ finite primes are ramified and $M \subseteq k(\Lambda_{P_2})M_2$, so that $L \subseteq k(\Lambda_{P_1})M \subseteq k(\Lambda_{P_1})k(\Lambda_{P_2})M_2 = (\Lambda_{P_1P_2})M_2$.

Performing the above process at most r times we have

$$L \subseteq k(\Lambda_{P_1P_2\cdots P_r})M_0 \tag{4.1}$$

where in M_0/k the only ramified prime is $\mathfrak{p}_\infty$.

We also have

Proposition 4.2. *Let L/k be an abelian extension where at most a prime divisor $\mathfrak{p}_0$ of degree 1 is ramified and the extension is tamely ramified. Then L/k is a constant extension.*

Proof. By Proposition 4.1 we have $e := e_{L/k}(\mathfrak{p}_0)|q - 1$. Let H be the inertia group of $\mathfrak{p}_0$. Then $|H| = e$ and $\mathfrak{p}_0$ is unramified in $E := L^H/k$. Therefore E/k is an unramified extension. Thus E/k is a constant extension.

Let $[E : k] = m$. Then if $\mathfrak{P}_0$ is a prime divisor in E dividing $\mathfrak{p}_0$ then the relative degree $d_{E/k}(\mathfrak{P}_0|\mathfrak{p}_0)$ is equal to m, the number of prime divisors in E/k is 1 and the degree of $\mathfrak{P}_0$ is 1 (see [4, Theorem 6.2.1]). Therefore $\mathfrak{P}_0$ is the only prime divisor ramified in L/E and it is of degree 1 and totally ramified. Furthermore $[L : E] = e \mid q - 1 = |\mathbb{F}_q^*|$.

The $(q - 1)$-th roots of unity belong to $\mathbb{F}_q \subseteq k$. Hence k contains the e–th roots of unity and L/E is a Kummer extension, say $L = E(y)$ with $y^e = \alpha \in E = k\mathbb{F}_{q^m} = \mathbb{F}_{q^m}(T)$. We write α in a normal form as prescribed by Hasse [1]: $(\alpha)_E = \frac{\mathfrak{P}_0^a \mathfrak{a}}{\mathfrak{b}}$, $0 < a < e$. Now since $\deg(\alpha)_E = 0$ it follows that $\deg_E \mathfrak{a}$ or $\deg_E \mathfrak{b}$ is not a multiple of e. This contradicts that $\mathfrak{p}_0$ is the only ramified prime. Therefore L/k is a constant extension. □

Finally, we obtain our main result.

Theorem 4.3. *If L/k is a finite abelian tamely ramified extension, where $P_1, \ldots, P_r \in R_T^+$ and possibly $\mathfrak{p}_\infty$ are the ramified primes, then $L \subseteq k(\Lambda_{P_1\cdots P_r})\mathbb{F}_{q^m}$ for some $m \in \mathbb{N}$.*

Proof. From (4.1) we have $L \subseteq k(\Lambda_{P_1P_2\cdots P_r})M_0$, for a finite abelian tamely ramified extension M_0/k ramified at most at $\mathfrak{p}_\infty$. By Proposition 4.2 we have that $M_0 = k\mathbb{F}_{q^m}$ is a constant extension. It follows that $L \subseteq k(\Lambda_{P_1\cdots P_r})\mathbb{F}_{q^m}$ for some $m \in \mathbb{N}$.

□

References

[1] Helmut Hasse, *Theorie der relativ–zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantenkörper*, J. Reine Angew. Math. **172**, 37–54, (1934).

[2] David Hayes, *Explicit Class Field Theory for Rational Function Fields*, Trans. Amer. Math. Soc. **189**, 77–91, (1974).

[3] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002.

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

Author information

Julio Cesar Salas–Torres, Universidad Autónoma de la Ciudad de México, Academia de Matemáticas. Plantel San Lorenzo Tezonco., México.
E-mail: cesar.salas@uacm.edu.mx

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

Gabriel Villa–Salvador, Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N., México.
E-mail: gvillasalvador@gmail.com

Received: April 28, 2012

Accepted: July 8, 2012