Palestine Journal of Mathematics

Vol. 5(1) (2016) , 159–165

CONGRUENCE FUNCTION FIELDS WITH CLASS NUMBER ONE

Martha Rzedowski–Calderón and Gabriel Villa–Salvador

Communicated by Jose Luis Lopez-Bonilla

To the memory of Prof. Manohar L. Madan

MSC 2010 Classifications: Primary 11R29; Secondary 11R32, 11R58, 11R60.

Keywords and phrases: Class number one; congruence function fields; cyclotomic number fields; ramification.

Abstract. We prove that there exists, up to isomorphism, exactly one function field over the finite field of two elements of class number one and genus four. This result, together with the ones of MacRae, Madan, Leitzel, Queen and Stirpe, establishes that there exist eight non-isomorphic congruence function fields of genus larger than zero and class number one.

1 Introduction

Let K be a congruence function field with exact field of constants $\mathbb{F}_q$, the finite field of q elements. Consider the class group of divisors of degree zero of K: C_{0K}. It is a finite abelian group with h_K elements, h_K is called *the class number of* K. When K is a function field of genus 0, we have $h_K = 1$. Thus, we consider K of genus $g_K \geq 1$. When $q \geq 5$ and $g_K \geq 1$ we have $h_K > 1$. In [2] R. MacRae found all the congruence function fields with class number one in the particular case that K is a quadratic extension of the rational function field $k = \mathbb{F}_q(T)$ and K contains a prime divisor of degree one. He proved that there are four quadratic fields with class number one which have a prime of degree one. M. Madan and C. Queen continued the study of this problem in [3]. They showed that if $q = 2$ and $g_K > 4$, or $q = 3$ and $g_K > 2$ then $h_K \neq 1$. Finally, they proved that except for the case $q = 2$ and $g_K = 4$ there exist exactly seven congruence function fields with class number one and genus larger than zero. The case $q = 2$, $g_K = 4$ was not settled.

In [1] J. Leitzel, M. Madan and C. Queen considered the case $q = 2$ and $g_K = 4$ and claimed that there is no field of class number one over the finite field of two elements and genus four. However C. Stirpe [5] found a counterexample to this claim. The example runs as follows. Let $\mathfrak{m}$ be the place associated to the irreducible polynomial $T^4+T+1 \in \mathbb{F}_2[T]$ and let S be the place associated to the irreducible polynomial T^7+T^4+1. Let $K_S^{\mathfrak{m}}$ be the ray class field of conductor $\mathfrak{m}$ and such that S splits in $K_S^{\mathfrak{m}}/\mathbb{F}_2(T)$. Stirpe established that the subfield of degree five over $\mathbb{F}_2(T)$ satisfies that $h_K = 1$ and $g_K = 4$. Furthermore, Stirpe claims that $T^7 + T^4 + 1$ is not unique. For instance, he remarks that we may take S_1 to be the place associated to $T^7 + T^3 + 1$ and the unique subfield K_1 of $K_{S_1}^{\mathfrak{m}}$ of degree five over $\mathbb{F}_2(T)$ also satisfies that $h_{K_1} = 1$ and $g_{K_1} = 4$.

In [6], P. Mercuri and C. Stirpe proved that the two fields found by Stirpe in [5] are in fact isomorphic. Furthermore, they showed that, up to isomorphism, there is only one field of genus 4 and class number one. This result together with the results of Madan, Leitzel, Queen and Stirpe, shows that, up to isomorphism, there are exactly eight congruence function fields K of genus larger than zero and class number one.

In this paper we present another proof that, up to isomorphism, there is only one field of genus four and class number one. We do not use the examples found by Stirpe in [5]. Our approach uses the theory of cyclotomic function fields of Carlitz–Hayes. First, we consider a field K over $\mathbb{F}_2$ such that $h_K = 1$ and $g_K = 4$. We show that K has a unique rational function subfield $k := \mathbb{F}_2(T)$ such that $[K : k] = 5$ and that the extension K/k is cyclic. There is only one prime of k ramified in K and this place is of degree four. From the result

of Madan and Queen [3] that states that a function field K over $\mathbb{F}_2$ satisfies that $h_K = 1$ and $g_K = 4$ if and only if $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$ where N_i denotes the number of prime divisors in K of degree i, we deduce that, up to isomorphism, necessarily $K \subseteq k(\Lambda_M)\mathbb{F}_{2^5}$ where $M = T^4+T+1$ and $k(\Lambda_M)$ is the cyclotomic function field corresponding to the Carlitz module Λ_M. Finally, we prove that there are precisely two fields K over k contained in $k(\Lambda_M)\mathbb{F}_{2^5}$ such that $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$. In one of them $T^7 + T^4 + 1$ splits and $T^7 + T^3 + 1$ is inert and in the other $T^7 + T^4 + 1$ is inert and $T^7 + T^3 + 1$ splits. Both fields are isomorphic.

One of the key facts in our proof is that if $[K : k] = 5$ and $\mathfrak{p}$ is the divisor of degree four in K, then the different of K/k is $\mathfrak{p}^4$ and $\mathfrak{p}$ is totally ramified. This was proved by Mercuri and Stirpe in [6].

2 The field K

Let K be a congruence function field with exact field of constants the finite field of q elements $\mathbb{F}_q$. Let N_i denote the number of prime divisors of degree i in K, $i \geq 1$. Let A_i be the number of integral divisors in K of degree i, $i \geq 0$. The genus of K will be denoted by g and the class number of K by h. Let $k = \mathbb{F}_q(T)$ be a rational congruence function field and let $R_T = \mathbb{F}_q[T]$ be its ring of integers. $\mathfrak{p}_\infty$ will denote the pole divisor of T in k. For the standard results on congruence function fields and cyclotomic function fields we refer to [7].

For any divisor $\mathfrak{q}$ in K we denote by $d_K(\mathfrak{q})$ its degree. If $P_K(u) = a_0 + a_1u + \cdots + a_{2g}u^{2g}$ is the numerator of the zeta function of K, where $u = q^{-s}$, we have the following relations ([7, Theorems 6.3.5 and 6.4.1])

$$\begin{gathered} a_0 = 1, \quad a_{2g} = q^g, \quad a_{2g-i} = a_i q^{g-i}, \quad 0 \leq i \leq 2g, \\ a_i = A_i - (q+1)A_{i-1} + qA_{i-2}, \quad 0 \leq i \leq 2g, \quad \text{with} \quad A_{-1} = A_{-2} = 0, \qquad (2.1) \\ P_K(1) = h, \quad A_n = h\Big(\frac{q^{n-g+1}-1}{q-1}\Big) \quad \text{for} \quad n > 2g-2. \end{gathered}$$

From now on, K will denote a field over $\mathbb{F}_2$ such that $g = 4$ and $h = 1$. This condition is equivalent to $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$ ([3, Theorem 2 (v)]). From that paper we know that the numerator of the zeta function of K is $P_K(u) = 1 - 3u + 2u^2 + u^4 + 8u^6 - 24u^7 + 16u^8$. Let $\mathfrak{p}$ denote the only prime divisor of degree four in K.

In this case, from (2.1) we obtain that $A_0 = 1$, $A_i = N_i = 0$, $0 \leq i \leq 3$, $A_4 = N_4 = 1$ and $A_5 = N_5 = 3$. Let $\mathfrak{C}_i$, $1 \leq i \leq 3$ be the three places of degree five in K. Therefore $\ell(\mathfrak{C}_1^{-1}) = 2$, $L(\mathfrak{C}_1^{-1}) = \{0, 1, T, T+1\}$ where $(T)_K = \frac{\mathfrak{C}_2}{\mathfrak{C}_1}$ and $(T+1)_K = \frac{\mathfrak{C}_3}{\mathfrak{C}_1}$ where $(y)_K$ denotes the divisor in K of $y \in K^*$. We have $[K : k] = 5$. Since $L(\mathfrak{p}^{-1}) = \mathbb{F}_2$, it follows that the minimal n such that there exists $y \in K$ with $[K : \mathbb{F}_2(y)] = n$ is $n = 5$ and that k is unique satisfying this property.

Remark 2.1. Every proper subfield $\mathbb{F}_2 \subsetneqq E \subsetneqq K$ such that K/E is separable, is of genus 0. Indeed, for any finite subextension E of K, the differential exponent of every prime appearing in the different $\mathfrak{D}_{K/E}$ of the extension is greater than or equal to 2 and since the minimum degree of a prime in K is 4, the degree of d of $\mathfrak{D}_{K/E}$ is greater than of equal to 8 except in the case that K/E is unramified. From the Riemann-Hurwitz formula, if $g_E \geq 1$ and K/E ramified, we obtain

$$6 = 2g_K - 2 = [K : E](2g_E - 2) + d \geq d \geq 8.$$

Thus, if $g_E \geq 1$, K/E is unramified, $[K : E] = 3$, and $g_E = 2$. If K/E is normal, let $\mathfrak{t} = \mathfrak{p} \cap E$. Then since $[K : E] = 3$ is relatively prime to $\deg_K \mathfrak{p} = 4$, it follows that $\mathfrak{t}$ decomposes fully in K/E and in particular K would contain at least 3 primes of degree four. Therefore K/E is non-normal. Let $\tilde{K}$ be the Galois closure of K/E. Then $[\tilde{K} : K] = 2$ and since $\tilde{K}/K$ is unramified, it follows that $\tilde{K} = K\mathbb{F}_4$. We have that $\tilde{K}/E\mathbb{F}_4$ is a normal extension of degree 3. Since $\deg_K \mathfrak{p} = 4$ and $\tilde{K}/K$ is an extension of constants of degree 2, we obtain that $\mathfrak{p}$ decomposes into two primes of degree 2 in $\tilde{K}$ (see [7, Theorem 6.2.1]). Thus $\tilde{K}$ has exactly two primes of degree 2. Let $\tilde{\mathfrak{p}}$ be one of them and let $\tilde{\mathfrak{t}} = \tilde{\mathfrak{p}} \cap E\mathbb{F}_4$. As above we obtain that $\tilde{\mathfrak{t}}$ decomposes fully in $\tilde{K}/E\mathbb{F}_4$ and in particular we have at least three primes in $\tilde{K}$ of degree 2. This contradiction shows that $g_E = 0$.

Remark 2.2. Let $\theta \in \mathcal{G} := \mathrm{Aut}_{\mathbb{F}_2} K$. Since θ permutes the three divisors $\mathfrak{C}_i$, $1 \leq i \leq 3$, we have that $\theta|_k \in \mathrm{Aut}_{\mathbb{F}_2} k \cong \mathrm{PSL}(2, \mathbb{F}_2) \cong S_3$ where $k = \mathbb{F}_2(T)$ and S_3 is the symmetric group in three elements. Therefore $K^{\mathcal{G}} \supseteq k^{S_3}$. Therefore $|\mathcal{G}|$ divides 30. If 5 divides $|\mathcal{G}|$, then the field fixed by an element of order 5 of $\mathcal{G}$ is necessarily k and K/k is normal. If K/k is not normal then $\mathcal{G}$ is trivial since otherwise for each non–trivial subgroup of $\mathcal{G}$, the fixed field is of genus 0 but one of them is of degree less than five. This contradicts that five is the minimum degree of a proper subfield of K. Therefore, we have that K/k is normal if and only if $\mathrm{Aut}_{\mathbb{F}_2} K \neq \{\mathrm{Id}\}$.

One of the key facts to prove the uniqueness of K is the following theorem.

Theorem 2.3. *The extension K/k is normal.*

Proof. Stirpe and Mercuri [6] proved that $\mathfrak{p}$ is fully ramified in K/k and in particular $\mathfrak{D}_{K/k} = \mathfrak{p}^4$, where $\mathfrak{D}_{K/k}$ denotes the different of the extension K/k.

Assume that K/k is not normal. Let $\tilde{K}$ be the Galois closure of K/k, $G := \mathrm{Gal}(\tilde{K}/k)$ and $H := \mathrm{Gal}(\tilde{K}/K)$. Then G is a transitive subgroup of S_5, the symmetric group in five elements and H is a subgroup of S_4. The field of constants of $\tilde{K}$ is $\mathbb{F}_2$ because otherwise, since the primes of degree one are inert in K/k, we would have an element in G of order $5r$ with $r \geq 2$ contrary to the fact that the elements in S_5 are of order less than or equal to six.

From Abhyankar Lemma we obtain that $\tilde{K}/K$ is unramified. Let H_1 be a proper normal subgroup of H such that H/H_1 is abelian. Then we obtain a non–trivial unramified abelian extension of K and since the class number of K is one, this extension would be a constant extension. This contradiction proves that K/k is normal. □

We have $\mathfrak{D}_{K/k} = \mathfrak{p}^4$. Since $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$, we obtain that all prime divisors of k of degree less than or equal to four, except for one of degree four, are inert in K/k and one prime divisor of degree four is ramified.

In k we have three prime divisors of degree four, namely the ones corresponding to T^4+T+1, $T^4 + T^3 + 1$ and $T^4 + T^3 + T^2 + T + 1$.

Remark 2.4. We may assume without loss of generality that the ramified prime of degree four $\mathfrak{m}$ is the place corresponding to $M = T^4+T+1$ for if $\mathfrak{m}_1$ is the place corresponding to T^4+T^3+1 (resp. $T^4 + T^3 + T^2 + T + 1$), then $\sigma\colon k \to k$ given by $\sigma(T) = \frac{1}{T}$ (resp. $\sigma(T) = \frac{1}{T+1}$) satisfies $\sigma(T^4 + T + 1) = \frac{T^4+T^3+1}{T^4}$ (resp. $\sigma(T^4 + T + 1) = \frac{T^4+T^3+T^2+T+1}{(T+1)^4}$) so that $\sigma(\mathfrak{m}) = \mathfrak{m}_1$ and extending σ to $\tilde{\sigma}\colon K \to \overline{k}$ we obtain $\tilde{\sigma}(K) \cong K$ and $\sigma(k) = k$. In $\tilde{\sigma}(K)/k$, the prime $\mathfrak{m}_1$ is the ramified one.

The extension K/k is a cyclic extension such that all the primes of degree one, two and three in k ($\{\mathfrak{p}_\infty, T, T+1, T^2+T+1, T^3+T+1, T^3+T^2+1\}$) and the primes of degree four associated to $T^4 + T^3 + 1$ and $T^4 + T^3 + T^2 + T + 1$ are inert. The prime $\mathfrak{m}$ associated to $T^4 + T + 1$ is ramified.

Since $\mathfrak{p}_\infty$ is unramified in K/k, in fact $\mathrm{con}_{k/K}\, \mathfrak{p}_\infty = \mathfrak{C}_1$, and $\mathfrak{m}$ is the only ramified prime in K and it is tamely ramified we have that $K \subseteq k(\Lambda_M)\mathbb{F}_{2^5}$ (see [4, Proposition 3.4]) and $[K : k] = 5$.

The key step for the main result of this paper is the following theorem.

Theorem 2.5. *Up to isomorphism, there exists only one field K with $k \subseteq K \subseteq k(\Lambda_M)\mathbb{F}_{2^5}$ such that $g = 4$ and $h = 1$.*

Proof. To start, let $\mathfrak{t}$ be any prime divisor of k such that $\mathfrak{t} \neq \mathfrak{p}_\infty, \mathfrak{m}$, and let $P \in R_T := \mathbb{F}_2[T]$ be the monic irreducible polynomial associated to $\mathfrak{t}$. Then the Frobenius map φ_P of P in the extension $k(\Lambda_M)/k$ is given by $\varphi_P(\lambda) = \lambda^P$ where λ is a generator of Λ_M (see [7, Theorem 12.5.1]). In particular for $\mathfrak{t} \neq \mathfrak{p}_\infty, \mathfrak{m}$ we have that the decomposition group of $\mathfrak{t}$ is $D_P = \langle \varphi_P \rangle$ and $|D_P| = o(P \bmod M)$.

We have that $G_M := \mathrm{Gal}(k(\Lambda_M)/k) \cong C_{15}$, the cyclic group of 15 elements, and let L be

the subfield of $k(\Lambda_M)$ such that $[L : k] = 5$.

$$\begin{array}{ccc} k(\Lambda_M) & \longrightarrow & k(\Lambda_M)\mathbb{F}_{2^5} \\ {\scriptstyle 3}\,\big|\,{\scriptstyle \langle\tau^5\rangle} & & \big| \\ L & \longrightarrow & L\mathbb{F}_{2^5} \\ {\scriptstyle 5}\,\big|\,{\scriptstyle \langle\tau^3\rangle} & & \big| \\ k & \longrightarrow & k\mathbb{F}_{2^5} \end{array}$$

From the isomorphism $G_M \cong \left(R_T/(M)\right)^*$ we have that τ, given by $\tau(\lambda) = \lambda^T$, is a generator of G_M. Therefore $\mathrm{Gal}(L/k) \cong \langle \tau \bmod \langle\tau^5\rangle\rangle \cong \langle\tau^3\rangle$.

Note that P is inert in L/k if and only if $o(\varphi_P) \in \{5, 15\}$. Direct computations give

$$\begin{gathered} T^1 \equiv T \bmod M, \quad T^2 \equiv T^2 \bmod M, \quad T^3 \equiv T^3 \bmod M, \quad T^4 \equiv T+1 \bmod M, \\ T^5 \equiv T^2+T \bmod M, \quad T^6 \equiv T^3+T^2 \bmod M, \quad T^7 \equiv T^3+T+1 \bmod M, \\ T^8 \equiv T^2+1 \bmod M, \quad T^9 \equiv T^3+T \bmod M, \quad T^{10} \equiv T^2+T+1 \bmod M, \\ T^{11} \equiv T^3+T^2+T \bmod M, \quad T^{12} \equiv T^3+T^2+T+1 \bmod M, \\ T^{13} \equiv T^3+T^2+1 \bmod M, \quad \text{and} \quad T^{14} \equiv T^3+1 \bmod M, \\ \text{and} \quad T^4+T^3+1 \equiv T^3+T \bmod M, \quad T^4+T^3+T^2+T+1 \equiv T^3+T^2 \bmod M. \end{gathered} \tag{2.2}$$

From (2.2) we may compute the order of φ_P:

$$\begin{gathered} o(\varphi_T) = 15, \quad o(\varphi_{T+1}) = 15, \quad o(\varphi_{T^2+T+1}) = 3, \quad o(\varphi_{T^3+T^2+1}) = 15, \\ o(\varphi_{T^3+T+1}) = 15, \quad o(\varphi_{T^4+T^3+1}) = 5, \quad o(\varphi_{T^4+T^3+T^2+T+1}) = 5, \end{gathered}$$

and we also have that $\mathfrak{p}_\infty$ is fully decomposed in $k(\Lambda_M)/k$ (see [7, Theorem 12.4.6]), that is $o(\varphi_{\mathfrak{p}_\infty}) = 1$ where $\varphi_{\mathfrak{p}_\infty}$ denotes the Frobenius of $\mathfrak{p}_\infty$ in $k(\Lambda_M)/k$. Therefore, the decomposition groups of P in $k(\Lambda_M)/k$ are given by

$$\begin{gathered} D_T = D_{T+1} = D_{T^3+T^2+1} = D_{T^3+T+1} = G_M = \langle\tau\rangle, \\ D_{\mathfrak{p}_\infty} = \{\mathrm{Id}\}, \quad D_{T^2+T+1} = \langle\tau^5\rangle, \\ D_{T^4+T^3+1} = D_{T^4+T^3+T^2+T+1} = \langle\tau^3\rangle. \end{gathered} \tag{2.3}$$

In particular $\mathfrak{p}_\infty$ and T^2+T+1 are decomposed in L/k and $T, T+1, T^3+T^2+1, T^3+T+1, T^4+T^3+1$ and $T^4+T^3+T^2+T+1$ are inert in L/k.

Now, in the extension of constants $k_5 := k\mathbb{F}_{2^5}$ over k, all the primes of degree i, $1 \le i \le 4$, are inert ([7, Theorem 6.2.1]). We have that $\mathrm{Gal}(k_5/k) = \langle\chi\rangle$ where χ is induced by the Frobenius map of the extension $\mathbb{F}_{2^5}/\mathbb{F}_2$. More precisely, if $Q(T) = \sum_{i=0}^{d} a_i T^i \in \mathbb{F}_{2^5}[T]$, then $\chi(Q(T)) = \sum_{i=0}^{d} a_i^2 T^i$.

Let $P(T) \in R_T$ be a prime of degree i, $0 \le i \le 4$. Then the residue fields in k_5/k are isomorphic to $\mathbb{F}_{2^{5i}}/\mathbb{F}_{2^i}$ and the Frobenius map δ of $\mathbb{F}_{2^{5i}}/\mathbb{F}_{2^i}$ is given by $\delta(\alpha) = \alpha^{2^i}$ for $\alpha \in \mathbb{F}_{2^{5i}}$. Therefore the Frobenius map of $P(T)$ in k_5/k corresponds to $\langle\chi^i\rangle \in \mathrm{Gal}(k_5/k)$.

To find the Frobenius map of an arbitrary $P \in R_T$ in the extensions Lk_5 and $k(\Lambda_M)k_5$ we consider the following general situation. Let $E/F, J/F$ be Galois extensions of global or local fields such that $E \cap J = F$. Let $S := EJ$.

$$\begin{array}{ccc} E & \longrightarrow & EJ = S \\ \big| & & \big| \\ F & \longrightarrow & J \end{array}$$

We have the isomorphism

$$\Phi\colon\ \mathrm{Gal}(S/F) \to \mathrm{Gal}(E/F) \times \mathrm{Gal}(J/F)$$
$$\Phi(\theta) = \big(\theta|_E, \theta|_J\big),$$

and the inverse of Φ is given by

$$\Psi\colon\ \mathrm{Gal}(E/F) \times \mathrm{Gal}(J/F) \to \mathrm{Gal}(S/F)$$
$$\Psi(\alpha, \beta) = \tilde{\alpha}\tilde{\beta},$$

where $\tilde{\alpha}\colon S \to S$ and $\tilde{\beta}\colon S \to S$ are defined, for $z = \sum_{i=1}^{t} x_i y_i \in S$ with $x_i \in E$ and $y_i \in J$, by

$$\tilde{\alpha}\big(\sum_{i=1}^{t} x_i y_i\big) = \sum_{i=1}^{t} \alpha(x_i) y_i$$

and

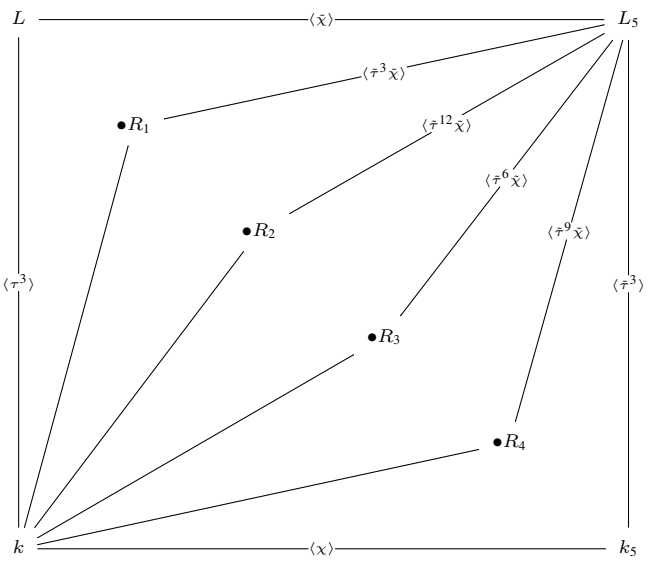
$$\tilde{\beta}\big(\sum_{i=1}^{t} x_i y_i\big) = \sum_{i=1}^{t} x_i \beta(y_i).$$

Let $\mathcal{P}$ be a prime in F, $\mathfrak{P}$ be a prime in S above $\mathcal{P}$ and let $\mathfrak{q} := \mathfrak{P} \cap J$ and $\mathfrak{t} := \mathfrak{P} \cap E$. Assume that $\mathcal{P}$ is unramified in S/F. Let $\left[\frac{S/F}{\mathfrak{P}}\right] \in \mathrm{Gal}(S/F)$ be the Frobenius map of $\mathfrak{P}/\mathcal{P}$. Then $\left[\frac{S/F}{\mathfrak{P}}\right]\Big|_E = \left[\frac{E/F}{\mathfrak{t}}\right]$ and $\left[\frac{S/F}{\mathfrak{P}}\right]\Big|_J = \left[\frac{J/F}{\mathfrak{q}}\right]$. Therefore

$$\left[\frac{S/F}{\mathfrak{P}}\right] = \widetilde{\left[\frac{E/F}{\mathfrak{t}}\right]}\widetilde{\left[\frac{J/F}{\mathfrak{q}}\right]}. \tag{2.4}$$

We will apply formula (2.4) to our case $(F =)k = \mathbb{F}_2(T)$, $(E =)L$, $(J =)k_5$ and $(S =)Lk_5$. There exist exactly four extensions R_j, $1 \le j \le 4$ of degree five over k contained in $L_5 := Lk_5$ other than L and k_5. The fields K we are looking for are, if any, among the fields R_j such that all the primes $P(T)$ in k of degree less than or equal to four other than M are inert in K/k. Note that since k_5/k is unramified and the only ramified prime in L/k is $\mathfrak{m}$, the only ramified prime in each R_j is $\mathfrak{m}$.

We have $\mathrm{Gal}(L_5/k) \cong C_5 \times C_5$ and the decomposition group of any unramified prime is cyclic since the characteristic is $2 \neq 5$. Thus, any prime of degree i with $i \le 4$ other than $\mathfrak{m}$ is decomposed in exactly one field among L, R_j, $1 \le j \le 4$, namely, in the fixed field L_5^H where H denotes the decomposition group of the prime in L_5/k. Now, $\mathfrak{p}_\infty$ and T^2+T+1 are decomposed in L/k so they are inert in every R_j, $1 \le j \le 4$.



Next we compute the decomposition group $\mathcal{D}_P$ in $k(\Lambda_M)k_5/k$ for $P \in \{T, T+1, T^3+T^2+1, T^3+T+1, T^4+T^3+1, T^4+T^3+T^2+T+1\}$ using formula (2.4). We denote by ξ_P the Frobenius of P in k_5/k and by φ_P the Frobenius of P in $k(\Lambda_M)/k$ (see (2.3)). Therefore, the Frobenius θ_P of P in $k(\Lambda_M)k_5/k$ is given by $\theta_P = \tilde{\varphi}_P\tilde{\xi}_P$.

From (2.2) and from the fact that the Frobenius $\tilde{\xi}_P$ of any P of degree i in k_5/k corresponds to $\langle\chi^i\rangle$, we obtain θ_P and the decomposition group $\mathcal{D}_P = \langle\theta_P\rangle$ for each P in $k(\Lambda_M)k_5$ as follows

$$\theta_T = \tilde{\tau}\tilde{\chi}, \quad \theta_{T+1} = \tilde{\tau}^4\tilde{\chi}, \quad \theta_{T^3+T^2+1} = \tilde{\tau}^{13}\tilde{\chi}^3,$$
$$\theta_{T^3+T+1} = \tilde{\tau}^7\tilde{\chi}^3, \quad \theta_{T^4+T^3+1} = \tilde{\tau}^9\tilde{\chi}^4, \quad \theta_{T^4+T^3+T^2+T+1} = \tilde{\tau}^6\tilde{\chi}^4.$$

Now let H_P be the subgroup of $\mathcal{D}_P$ of order 5. We obtain

$$H_T = H_{T^3+T^2+1} = H_{T^4+T^3+1} = \langle\tilde{\tau}^6\tilde{\chi}\rangle, \tag{2.5}$$
$$H_{T+1} = H_{T^3+T+1} = H_{T^4+T^3+T^2+T+1} = \langle\tilde{\tau}^9\tilde{\chi}\rangle,$$

and note that $\langle\tilde{\tau}^6\tilde{\chi}\rangle \neq \langle\tilde{\tau}^9\tilde{\chi}\rangle$.

Let $R_3 = L_5^{\langle\tilde{\tau}^6\tilde{\chi}\rangle}$ and $R_4 = L_5^{\langle\tilde{\tau}^9\tilde{\chi}\rangle}$. From (2.5) we have that in R_3/k, T, T^3+T^2+1 and T^4+T^3+1 split and in R_4/k, $T+1, T^3+T+1$ and $T^4+T^3+T^2+T+1$ split. Therefore all the primes of degree i with $1 \leq i \leq 4$ other than $\mathfrak{m}$ are inert in R_1/k and in R_2/k, where $R_1 = L_5^{\langle\tilde{\tau}^3\tilde{\chi}\rangle}$ and $R_2 = L_5^{\langle\tilde{\tau}^{12}\tilde{\chi}\rangle}$ and we have $\langle\tilde{\tau}^3\tilde{\chi}\rangle \neq \langle\tilde{\tau}^{12}\tilde{\chi}\rangle$. The fields R_1 and R_2 are of genus four and class number one.

Finally, we will prove that $R_1 \cong R_2$. Let $\sigma\colon k \to k$ be given by $\sigma(T) = \frac{1}{T}$ and extend σ to $\tilde{\sigma}\colon R_1 \to \bar{k}$. Since R_1 and R_2 are the only subfields of L_5 of genus four and class number one, necessarily we have $\sigma(R_1) = R_1$ or R_2. Now consider the primes T^7+T^4+1 and T^7+T^3+1. Since $T^7+T^4+1 \equiv T^3+1 \bmod M$ we have that $H_{T^7+T^4+1} = \langle\tilde{\tau}^{12}\tilde{\chi}\rangle$. Therefore T^7+T^4+1 splits in R_2 and is inert in R_1.

Now consider the prime T^7+T^3+1. Since $T^7+T^3+1 \equiv T \bmod M$, it follows that $H_{T^7+T^3+1} = \langle\tilde{\tau}^3\tilde{\chi}\rangle$ so that T^7+T^3+1 splits in R_1 and is inert in R_2. Since $\sigma(T^7+T^4+1) = \frac{T^7+T^3+1}{T^7}$ it follows that $\sigma(R_1) = R_2$ and $R_1 \cong R_2$. This proves Theorem 2.5. □

Remark 2.6. The fields R_1 and R_2 are the fields described by C. Stirpe in [5].

The main result of this paper is a consequence of Theorem 2.3, Remark 2.4 and Theorem 2.5.

Theorem 2.7. *Up to isomorphism, there exists exactly one function field over the finite field of two elements of class number one and genus four.*

Remark 2.8. The field K (equal to either R_1 or R_2) satisfies that $\mathcal{G} = \mathrm{Aut}_{\mathbb{F}_2} K = \mathrm{Aut}_k K = \mathrm{Gal}(K/k) \cong C_5$. Indeed, if $|\mathcal{G}| > 5$, there would exist an element of order 2 or 3 in $\mathcal{G}$ and if S were the group generated by this element, we would have $1 < [K : K^S] = |S| < 5$, thus K^S would be of genus 0 (see Remark 2.1). This contradicts that five is the minimum degree of a proper subfield of K.

References

[1] Leitzel, James R.C.; Madan, Manohar L.; Queen, Clifford S., *Algebraic function fields with small class number*, Journal of Number Theory **7**, 11–27, (1975).

[2] MacRae, Robert E., *On unique factorization in certain rings of algebraic functions*, Journal of Algebra **17**, 243–261, (1971).

[3] Madan, Manohar L.; Queen, Clifford S., *Algebraic function fields of class number one*, Acta Arithmetica **20**, 423–432–375, (1972).

[4] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus fields of abelian extensions of rational congruence function fields*, Finite Fields Appl. **20**, 40–54, (2013).

[5] Stirpe, Claudio, *A counterexample to 'Algebraic function fields with small class number'*, Journal of Number Theory **143**, 402–404, (2014).

[6] Mercuri, Pietro; Stirpe, Claudio, *Classification of Algebraic Function Fields with Class Number One*, arXiv:1406.5365v3, December 2 (2014).

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

Author information

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, gvilla@ctrl.cinvestav.mx

Received: March 22, 2015.

Accepted: April 21, 2015