ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 48, Number 6, 2018

GENUS FORMULAS FOR ABELIAN p-EXTENSIONS

FAUSTO JARQUÍN-ZÁRATE, MARTHA RZEDOWSKI-CALDERÓN
AND GABRIEL VILLA-SALVADOR

ABSTRACT. We apply a result of Kani relating genera and Hasse-Witt invariants of Galois extensions to a family of abelian p-extensions. Our formulas generalize the case of elementary abelian p-extensions found by Garcia and Stichtenoth.

1. Introduction. Kani proved in [**2**] that, if L/K is a finite Galois extension of function fields with Galois group G, then any relation among idempotents of subgroups of G in $\mathbb{Q}[G]$ implies the same relation among the *quotient genera*. The quotient genus for a subgroup H of G is the genus of the field $K_H := L^H$.

In the same paper, Kani proved that, if the field of constants k of K is a field of positive characteristic $p > 0$, then any relation among the subgroups H of G implies the same relation among the Hasse-Witt invariants of the fields K_H.

In this paper, we consider an arbitrary field k of characteristic $p > 0$, a function field K with field of constants k, and a Galois extension L/K with Galois group isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^n$, where m and n are natural numbers. We find two formulas relating the genus g_L of L and the genera of a family of subextensions. The first is the family of all cyclic subextensions of K and the second is the family of all subextensions E with L/E cyclic. The same relations hold for the Hasse-Witt invariants. Our results generalize the formula found by Garcia and Stichtenoth [**1**] for elementary abelian p-extensions.

2010 AMS *Mathematics subject classification.* Primary 11R58, Secondary 111R29, 11R60.

Keywords and phrases. Function fields, Kani's formula, abelian p-extensions, Artin-Schreier-Witt extensions.

The third author is the corresponding author.

Received by the editors on August 29, 2017, and in revised form on December 30, 2017.

DOI:10.1216/RMJ-2018-48-6-1905

2. Results. Let k be any field of positive characteristic p, and let K be a function field with field of constants k. Let L/K be a Galois extension with Galois group isomorphic to $G = (\mathbb{Z}/p^m\mathbb{Z})^n$. Let $\mathcal{G}$ be the set of all subgroups of G. For each $H \in \mathcal{G}$, let K_H be the subfield of L fixed by H, that is, $K_H := L^H$. Let g_H be the genus of K_H, and let τ_H be the Hasse-Witt invariant of K_H. For $H \in \mathcal{G}$, let ϵ_H be the *norm idempotent of* H:

$$\epsilon_H := \frac{1}{|H|} \sum_{h \in H} h \in \mathbb{Q}[G].$$

In **[2]**, Kani proved the following result.

Theorem 2.1 ([**2**]). *Any relation*

$$\sum_{H \in \mathcal{G}} r_H \epsilon_H = 0 \quad \textit{with } r_H \in \mathbb{Q},$$

among the norm idempotents yields the following two relations:

$$\sum_{H \in \mathcal{G}} r_H g_H = 0 \quad \textit{and} \quad \sum_{H \in \mathcal{G}} r_H \tau_H = 0,$$

among the genera and among the Hasse-Witt invariants.

Let $\mathcal{H}_i$ be the set of all subgroups of G isomorphic to $\big(\mathbb{Z}/p^m\mathbb{Z}\big)^{n-1} \oplus \big(\mathbb{Z}/p^{m-i}\mathbb{Z}\big)$, $0 \le i \le m$. The set of the fields fixed by $H \in \mathcal{H}_i$ is the set $\mathcal{K}_i$ of all the subfields $K \subseteq E \subseteq L$ such that $\mathrm{Gal}(E/K) \cong (\mathbb{Z}/p^i\mathbb{Z})$, that is, the collection of all of the cyclic extensions of K of degree p^i contained in L. Our main result is:

Theorem 2.2. *We have the following relations*

$$g_L = -p\left(\frac{p^{n-1}-1}{p-1}\right) g_K - (p^{n-1}-1) \sum_{i=1}^{m-1} \sum_{E \in \mathcal{K}_i} g_E + \sum_{E \in \mathcal{K}_m} g_E,$$

and

$$\tau_L = -p\left(\frac{p^{n-1}-1}{p-1}\right) \tau_K - (p^{n-1}-1) \sum_{i=1}^{m-1} \sum_{E \in \mathcal{K}_i} \tau_E + \sum_{E \in \mathcal{K}_m} \tau_E.$$

Corollary 2.3 ([**1**]). *If L/K is an elementary abelian p-extension of degree p^n, we have*

$$g_L = -p\left(\frac{p^{n-1}-1}{p-1}\right)g_K + \sum_{E\in\mathcal{K}_1} g_E.$$

Now, let $\mathcal{T}_i$ be the set of cyclic subgroups of G of order p^i, $0 \le i \le m$. Let $\mathcal{L}_i$ be the set of subextensions $K \subseteq E \subseteq L$ such that L/E is a cyclic extension of degree p^i. We have $\mathcal{L}_i = \{E \mid E = L^H \text{ with } H \in \mathcal{T}_i\}$. Then,

Theorem 2.4. *We have the following relations*:

$$p\left(\frac{p^{n-1}-1}{p-1}\right)g_L = -p^{nm}g_K - (p^{n-1}-1)\sum_{i=1}^{m-1} p^i \sum_{E\in\mathcal{L}_i} g_E + p^m \sum_{E\in\mathcal{L}_m} g_E,$$

and

$$p\left(\frac{p^{n-1}-1}{p-1}\right)\tau_L = -p^{nm}\tau_K - (p^{n-1}-1)\sum_{i=1}^{m-1} p^i \sum_{E\in\mathcal{L}_i} \tau_E + p^m \sum_{E\in\mathcal{L}_m} \tau_E.$$

Remark 2.5. The genera of the subfields considered in Theorem 2.2 can be computed using the results of Schmid [**3**].

It is not easy to use Theorem 2.4 in applications since the family of fields considered is in the top of the extension; thus, the genera is difficult to find.

3. Proofs.

First, we consider

$$M_i := \sum_{H\in\mathcal{H}_i} \epsilon_H, \quad 0 \le i \le m. \tag{3.1}$$

Note that $M_0 = \sum_{H\in\mathcal{H}_0} \epsilon_H = \epsilon_G = (1/p^{nm})\sum_{\sigma\in G}\sigma$.

Fix an element $\sigma \in G$. Let $T(i,\sigma)$ be the number of distinct subgroups $H \in \mathcal{H}_i$ such that $\sigma \in H$, that is,

$$T(i,\sigma) := |\{H \in \mathcal{H}_i \mid \sigma \in H\}|.$$

Let s be a natural number $1 \leq s \leq m$, and let

$$G_s := \{\sigma \in G \mid o(\sigma) = p^s\}.$$

Note that, given any element $\sigma \in G_s$, there exists an element $\tau \in G$ of order p^m such that $\tau^{p^{m-s}} = \sigma$. If θ and σ are two elements of G_s, then there exists an automorphism $\Phi \in \mathrm{Aut}(G)$ such that $\Phi(\theta) = \sigma$. Thus, $T(i,\sigma) = T(i,\theta)$. Therefore, it makes sense to define

$$T(i,s) := T(i,\sigma), \tag{3.2}$$

where σ is any element of G_s.

Let $C_s := \sum_{\sigma \in G_s} \sigma \in \mathbb{Q}[G]$. Then,

$$\begin{aligned} M_i &= \sum_{H \in \mathcal{H}_i} \frac{1}{|H|} \sum_{h \in H} h \\ &= \frac{1}{p^{m(n-1)+(m-i)}} \sum_{s=0}^{m} T(i,s) \sum_{\sigma \in G_s} \sigma \\ &= \frac{1}{p^{nm-i}} \sum_{s=0}^{m} T(i,s) C_s. \end{aligned}$$

We must compute $T(i,s)$ for all $0 \leq i,\, s \leq m$. Towards this end, let e_s be the number of elements of G of order p^s. We have

$$e_s = q^s - q^{s-1}, \quad 1 \leq s \leq m, \text{ and } e_0 = 1,$$

where $q = p^n$. In particular, if h_i is the number of distinct cyclic subgroups of G of order p^i, it follows that

$$h_i = \frac{q^i - q^{i-1}}{p^i - p^{i-1}}, \quad 1 \leq i \leq m, \text{ and } h_0 = 1.$$

Since, in an abelian group, its lattice of subgroups is symmetric, that is, if B is a subgroup of a finite abelian group A, then A contains a subgroup isomorphic to A/B. It follows that

$$h_i = |\mathcal{H}_i|.$$

Let $H \in \mathcal{H}_i$, and let $L(H,s) = |H \cap G_s|$. Since all of the subgroups in the collection $\mathcal{H}_i$ are isomorphic, it makes sense to define

$$L(i,s) := L(H,s),$$

where H is any subgroup in $\mathcal{H}_i$.

Let $\mathcal{F} \subseteq \mathcal{H}_i \times G_s$ be defined by

$$\mathcal{F} := \{(H, \sigma) \mid \sigma \in H\}.$$

We can compute $|\mathcal{F}|$ either column-by-column or row-by-row, which gives us:

$$|\mathcal{F}| = h_i L(i,s) = T(i,s) e_s, \tag{3.3}$$

respectively, that is, to find $T(i,s)$, it suffices to find $L(i,s)$.

Now, fix $H \in \mathcal{H}_i$, and let $B_s := \{x \in H \mid x^{p^s} = \mathrm{Id}_G\} = \{x \in H \mid o(x) \text{ divides } p^s\}$. Then, $L(i,s) = |B_s| - |B_{s-1}|$ for $1 \leq s \leq m$ and $L(i,0) = |B_0| = 1$. Now, to find B_s, note that $B_s = \ker \Psi$, where $\Psi : H \to H$, $\Psi(x) = x^{p^s}$. The image of Ψ is H^{p^s}. Hence,

$$|B_s| = \frac{|H|}{|H^{p^s}|}.$$

Since $H \cong \left(\mathbb{Z}/p^m\mathbb{Z}\right)^{n-1} \oplus \left(\mathbb{Z}/p^{m-i}\mathbb{Z}\right)$, we have $H^{p^s} \cong (\mathbb{Z}/p^{m-s}\mathbb{Z})^{n-1} \oplus A$, where

$$A \cong \begin{cases} \left(\mathbb{Z}/p^{m-i-s}\mathbb{Z}\right) & \text{if } 1 \leq s \leq m-i \\ 0 & \text{if } m-i < s \leq m. \end{cases}$$

Therefore, we have

$$L(i,s) = \begin{cases} 1 & \text{if } s = 0,\ 0 \leq i \leq m, \\ p^{n(s-1)}(p^n - 1) & \text{if } 1 \leq s \leq m-i \\ & (0 \leq i \leq m-1), \\ p^{(n-1)(s-1)+(m-i)}(p^{n-1} - 1) & \text{if } m-i+1 \leq s \leq m \\ & (1 \leq i \leq m). \end{cases} \tag{3.4}$$

From (3.3) and (3.4), we obtain

$$T(i,s) = \begin{cases} 1 & \text{if } i = 0,\ 0 \leq s \leq m, \\ h_i & \text{if } s = 0, 0 \leq i \leq m, \\ \left(\dfrac{p^n - 1}{p-1}\right) p^{(n-1)(i-1)} & \text{if } 1 \leq s \leq m-i, \\ & (1 \leq i \leq m-1), \\ \left(\dfrac{p^{n-1} - 1}{p-1}\right) p^{(n-2)(i-1)+(m-s)} & \text{if } m-i+1 \leq s \leq m, \\ & (1 \leq i \leq m). \end{cases} \tag{3.5}$$

Thus, from (3.5), we obtain

$$M_i = \frac{p^i}{p^{nm}} h_i \operatorname{Id}_G + \frac{p^i}{p^{nm}} \sum_{s=1}^{m-i} \left(\frac{p^n - 1}{p-1}\right) p^{(n-1)(i-1)} C_s$$
$$+ \frac{p^i}{p^{nm}} \sum_{s=m-i+1}^{m} \left(\frac{p^{n-1} - 1}{p-1}\right) p^{(n-2)(i-1)+(m-s)} C_s,$$

for $1 \le i \le m$ and $M_0 = \epsilon_G$.

Now, in order to obtain a relation among the norm idempotents, since $M_0 = \epsilon_G$ and $\operatorname{Id}_G = \epsilon_{\operatorname{Id}_G}$, what we need is to find $x_1, \ldots, x_m \in \mathbb{Q}$ such that

$$\sum_{i=1}^{m} x_i M_i = y_0 \operatorname{Id}_G + \sum_{s=1}^{m} y_s C_s,$$

with $y_0 \in \mathbb{Q}$ and $y_1 = y_2 = \cdots = y_m \neq 0$.

Let $x_1, \ldots, x_m \in \mathbb{Q}$, and

$$\sum_{i=1}^{m} x_i M_i = \underbrace{\left(\sum_{i=1}^{m} \frac{p^i}{p^{nm}} x_i h_i\right)}_{y_0} \operatorname{Id}_G + \left(\frac{p^n - 1}{p-1}\right) \sum_{i=1}^{m-1} \sum_{s=1}^{m-i} x_i \frac{p^{(n-1)(i-1)+i}}{p^{nm}} C_s$$
$$+ \left(\frac{p^{n-1} - 1}{p-1}\right) \sum_{i=1}^{m} \sum_{s=m-i+1}^{m} x_i \frac{p^{(n-2)(i-1)+(m-s)+i}}{p^{nm}} C_s.$$

Changing the summation order (Fubini's Theorem), we obtain

$$\sum_{i=1}^{m} x_i M_i = y_0 \operatorname{Id}_G + \left(\frac{p^n - 1}{p-1}\right) \sum_{s=1}^{m-1} \sum_{i=1}^{m-s} x_i \frac{p^{(n-1)(i-1)+i}}{p^{nm}} C_s$$
$$+ \left(\frac{p^{n-1} - 1}{p-1}\right) \sum_{s=1}^{m} \sum_{i=m-s+1}^{m} x_i \frac{p^{(n-2)(i-1)+(m-s)+i}}{p^{nm}} C_s$$
$$= \sum_{s=0}^{m} y_s C_s.$$

We have, for $1 \le s \le m-1$,

$$y_s = \left(\frac{p^n - 1}{p-1}\right) \sum_{i=1}^{m-s} x_i \frac{p^{(n-1)(i-1)+i}}{p^{nm}} \tag{3.6}$$

$$+\left(\frac{p^{n-1}-1}{p-1}\right)\sum_{i=m-s+1}^{m} x_i\frac{p^{(n-2)(i-1)+(m-s)+i}}{p^{nm}}$$

and

$$y_m=\left(\frac{p^{n-1}-1}{p-1}\right)\sum_{i=1}^{m} x_i\frac{p^{(n-2)(i-1)+i}}{p^{nm}}. \tag{3.7}$$

Consider $1\le s\le m-2$. Our goal is to show that $x_1,\dots,x_m$ can be chosen so that $y_s=y_{s+1}$. From (3.6), we obtain

$$x_{m-s}=-\frac{p^{ns}(p^{n-1}-1)}{p^{nm}}\sum_{i=m-s+1}^{m} p^{(n-1)(i-1)+(m-s)}x_i,\quad 1\le s\le m-2. \tag{3.8}$$

Similarly, for $s=m-1$, we obtain from $y_{m-1}=y_m$, (3.6) and (3.7),

$$x_1=-(p^{n-1}-1)\sum_{i=2}^{m} p^{(n-1)(i-2)}x_i. \tag{3.9}$$

Taking $s=1$ in (3.8), we obtain

$$x_{m-1}=-(p^{n-1}-1)x_m. \tag{3.10}$$

From (3.10), taking $s=2$ in (3.8), we obtain $x_{m-2}=-(p^{n-1}-1)x_m$. By induction, we obtain

$$x_2=\cdots=x_{m-1}=-(p^{n-1}-1)x_m. \tag{3.11}$$

Finally, from (3.11) and (3.9), we get $x_1=-(p^{n-1}-1)x_m$.

We let $x_m=1$ and obtain $x_i=-(p^{n-1}-1)$ for $1\le i\le m-1$. Then, from (3.6) and (3.7), we have

$$y_1=\cdots=y_m=\left(\frac{p^{n-1}-1}{p-1}\right)\frac{1}{p^{nm-1}}.$$

Therefore,

$$\begin{aligned}(3.12)\qquad &-\sum_{i=i}^{m-1}\sum_{H\in\mathcal{H}_i}(p^{n-1}-1)\epsilon_H+\sum_{H\in\mathcal{H}_m}\epsilon_H\\ &\qquad=-(p^{n-1}-1)\sum_{i=1}^{m-1}M_i+M_m\end{aligned}$$

$$= y_0 \operatorname{Id}_G + \frac{1}{p^{nm-1}} \left(\frac{p^{n-1}-1}{p-1} \right) \sum_{s=1}^{m} C_s$$
$$= z_0 \epsilon_{\operatorname{Id}_G} + \frac{1}{p^{nm-1}} \left(\frac{p^{n-1}-1}{p-1} \right) p^{nm} \epsilon_G$$
$$= z_0 \epsilon_{\operatorname{Id}_G} + p \left(\frac{p^{n-1}-1}{p-1} \right) \epsilon_G,$$

where

$$z_0 = y_0 - \left(\frac{p^{n-1}-1}{p-1} \right) \frac{1}{p^{nm-1}}.$$

Since $y_0 = \sum_{i=1}^{m} (p^i/p^{nm}) x_i h_i$ with x_i as in (3.10) and (3.11) with $x_m = 1$, we obtain $z_0 = 1$. Theorem 2.2 is now a consequence of Theorem 2.1 and (3.12).

In order to prove Theorem 2.4, we now consider $\mathcal{T}_i$, $0 \le i \le m$. We have $|\mathcal{T}_i| = h_i$. Let

$$Q_i := \sum_{H \in \mathcal{T}_i} \epsilon_H.$$

Consider an element $\sigma \in G_s$. Let $N(i, \sigma)$ be the number of cyclic subgroups of G of order p^i containing σ. Since, for any two elements of G_s, there exists an automorphism of G sending one into the other, as in (3.2), it makes sense to define

$$N(i, s) := N(i, \sigma),$$

where σ is any element of G_s. Then,

$$Q_i = \frac{1}{p^i} \sum_{H \in \mathcal{T}_i} \sum_{\sigma \in H} \sigma \tag{3.13}$$
$$= \frac{1}{p^i} \sum_{s=0}^{m} N(i, s) \sum_{\sigma \in G_s} \sigma$$
$$= \frac{1}{p^i} \sum_{s=0}^{m} N(i, s) C_s.$$

First, we compute $N(m, s)$. Let $\{\tau_1, \ldots, \tau_n\}$ be a basis of G over $\mathbb{Z}/p^m\mathbb{Z}$. More precisely, $G = \langle \tau_1, \ldots, \tau_n \rangle$ and $o(\tau_j) = p^m$ for $1 \le j \le n$. Let $\mu \in G$, say $\mu = \tau_1^{\alpha_1} \cdots \tau_n^{\alpha_n}$. Then, $o(\mu) = p^m$ if and only if there exists a $1 \leq j \leq n$ such that $\gcd(\alpha_j, p) = 1$. Fix an element σ of G_s with $s \geq 1$. We can choose the basis $\{\tau_1, \ldots, \tau_n\}$ of G such that $\tau_1^{p^{m-s}} = \sigma$.

We have

$$h_m = \frac{q^m - q^{m-1}}{p^m - p^{m-1}}.$$

The different h_m cyclic subgroups of G of order p^m are

$$\langle \tau_1 \tau_2^{\alpha_2} \cdots \tau_n^{\alpha_n} \rangle, \; 0 \leq \alpha_j \leq p^m - 1, \; 2 \leq j \leq n,$$
$$\langle \tau_1^{p\alpha_1} \tau_2 \tau_3^{\alpha_3} \cdots \tau_n^{\alpha_n} \rangle, \; 0 \leq \alpha_1 \leq p^{m-1} - 1 \text{ and } 0 \leq \alpha_j \leq p^m - 1, \; 3 \leq j \leq n,$$
$$\vdots \qquad \vdots$$
$$\langle \tau_1^{p\alpha_1} \tau_2^{p\alpha_2} \cdots \tau_{k-1}^{p\alpha_{k-1}} \tau_k \tau_{k+1}^{\alpha_{k+1}} \cdots \tau_n^{\alpha_n} \rangle, \; 0 \leq \alpha_j \leq p^{m-1} - 1, \; 1 \leq j \leq k-1$$
$$\text{and } 0 \leq \alpha_j \leq p^m - 1, \; k+1 \leq j \leq n,$$
$$\vdots \qquad \vdots$$
$$\langle \tau_1^{p\alpha_1} \tau_2^{p\alpha_2} \cdots \tau_{n-1}^{p\alpha_{n-1}} \tau_n \rangle, \; 0 \leq \alpha_j \leq p^{m-1} - 1, \; 1 \leq j \leq n-1.$$

Note that σ does not belong to any subgroup of the form

$$\langle \tau_1^{p\alpha_1} \tau_2^{p\alpha_2} \cdots \tau_{k-1}^{p\alpha_{k-1}} \tau_k \tau_{k+1}^{\alpha_{k+1}} \cdots \tau_n^{\alpha_n} \rangle, \quad k \geq 2,$$

since $s \geq 1$. Otherwise, we would have

$$\sigma = \tau_1^{p^{m-s}} = \left(\tau_1^{p\alpha_1} \tau_2^{p\alpha_2} \cdots \tau_{k-1}^{p\alpha_{k-1}} \tau_k \tau_{k+1}^{\alpha_{k+1}} \cdots \tau_n^{\alpha_n} \right)^{\beta}$$

for some $0 \leq \beta \leq p^m - 1$. Since $\{\tau_1, \ldots, \tau_n\}$ is a basis of G, we would have that $p^m \mid \beta$, that is, $\beta = 0$, which is impossible since $\sigma \neq \mathrm{Id}_G$.

Similarly, we have $\sigma \in \langle \tau_1 \tau_2^{\alpha_2} \cdots \tau_n^{\alpha_n} \rangle$ if and only if $\alpha_j = p^s l_j$ with $0 \leq l_j \leq p^{m-s} - 1$, $2 \leq j \leq n$. For $s = 0$, we have $\sigma = \mathrm{Id}_G$ and $N(m, 0) = h_m$. Therefore, we have

$$N(m, s) = \begin{cases} p^{(m-s)(n-1)} & \text{if } 1 \leq s \leq m, \\ h_m & \text{if } s = 0. \end{cases} \tag{3.14}$$

Now, let $0 \leq i \leq m$. If $i < s$, then $|H| = p^i < p^s = o(\sigma)$ so that $\sigma \notin H$. Thus, $N(i, s) = 0$ if $i < s$. Now, let $s \leq i$. If $s = 0$, then $N(i, 0) = h_i$, since $\sigma = \mathrm{Id}_G$.

Next, we consider $s \geq 1$. Let $1 \leq t \leq m$ and $\phi_t\colon G \to G$, $\phi(x) = x^{p^t}$. Then, $\ker \phi_t = \{x \in G \mid x^{p^t} = 1\} = \{x \in G \mid o(x) \text{ divides } p^t\}$, and the image of ϕ_t is G^{p^t}. In particular, if $t = i$, then any $H \in \mathcal{T}_i$ satisfies $H \subseteq \ker \phi_i$. It is easy to see that $\ker \phi_i = G^{p^{m-i}} \cong (\mathbb{Z}/p^i\mathbb{Z})^n$. Therefore, from the case $i = m$, we have $N(i,s) = p^{(i-s)(n-1)}$ for $s \neq 0$ and $N(i,0) = h_i$. From (3.14), we obtain

$$N(i,s) = \begin{cases} h_i & \text{if } s = 0 \text{ and } 0 \leq i \leq m, \\ p^{(i-s)(n-1)} & \text{if } 1 \leq s \leq i \leq m, \\ 0 & \text{if } 0 \leq i < s \leq m. \end{cases} \tag{3.15}$$

From (3.13) and (3.15), we obtain

$$Q_i = \frac{1}{p^i} \sum_{s=0}^{i} N(i,s)\, C_s = \frac{1}{p^i}\, h_i \operatorname{Id}_G + \sum_{s=1}^{i} p^{(i-s)(n-1)-i} C_s.$$

Equivalently, we have

$$p^i Q_i = h_i \operatorname{Id}_G + \sum_{s=1}^{i} p^{(i-s)(n-1)} C_s, \quad 0 \leq i \leq m,\ Q_0 = \operatorname{Id}_G. \tag{3.16}$$

Let $x_1, \ldots, x_n \in \mathbb{Q}$ be such that $\sum_{i=1}^m x_i p^i Q_i = y_0 \operatorname{Id}_G + \sum_{s=1}^m y_s C_s$ with $y_0 \in \mathbb{Q}$ and $y_1 = y_2 = \cdots = y_m \neq 0$. Then, from (3.16), we have

$$\begin{aligned} \sum_{i=1}^m x_i p^i Q_i &= \left(\sum_{i=1}^m x_i h_i\right) \operatorname{Id}_G + \sum_{i=1}^m \sum_{s=1}^i x_i p^{(i-s)(n-1)} C_s \\ &= y_0 \operatorname{Id}_G + \sum_{s=1}^m \sum_{i=s}^m x_i p^{(i-s)(n-1)} C_s \\ &= y_0 \operatorname{Id}_G + \sum_{s=1}^m y_s C_s, \end{aligned}$$

where $y_0 = \sum_{i=1}^m x_i h_i$ and, for $s \geq 1$,

$$y_s = \sum_{i=s}^m x_i p^{(i-s)(n-1)} = x_s + \sum_{i=s+1}^m x_i p^{(i-s)(n-1)}.$$

From the condition $y_1 = \cdots = y_m$, we obtain, by induction on s, that

$$x_1 = x_2 = \cdots = x_{m-1} = -(p^{n-1} - 1)x_m.$$

We take $x_m = 1$ and get $x_i = -(p^{n-1} - 1)$, $1 \leq i \leq m-1$. With these values, we obtain $y_1 = y_2 = \cdots = y_m = 1$ and $y_0 = (p^n - 1)/(p-1)$.

Then, we finally obtain a relation among idempotents of $\mathcal{T}_i$, $0 \leq i \leq m$:

$$\begin{aligned} &-(p^{n-1}-1)\sum_{i=1}^{m-1}\sum_{H\in\mathcal{T}_i} p^i\epsilon_H + \sum_{H\in\mathcal{T}_m} p^m\epsilon_H \\ &= \left(\left(\frac{p^n-1}{p-1}\right) - 1\right)\epsilon_{\mathrm{Id}_G} + p^{nm}\epsilon_G \\ &= p\left(\frac{p^{n-1}-1}{p-1}\right)\epsilon_{\mathrm{Id}_G} + p^{nm}\epsilon_G. \end{aligned}$$

Theorem 2.4 follows from Kani's theorem (Theorem 2.1).

Acknowledgments. We thank the anonymous referee for the careful reading of the manuscript. His/her remarks improved the presentation of the article.

REFERENCES

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

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

3. Hermann Ludwig Schmid, *Zur Arithmetik der zyklischen p-Körper*, J. reine angew. Math. **176** (1936), 161–167.

Universidad Autónoma de la Ciudad de México, Academia de Matemáticas, Plantel San Lorenzo Tezonco, Prolongación San Isidro No. 151, Col. San Lorenzo, Iztapalapa, C.P. 09790, Ciudad de México, México
Email address: **fausto.jarquin@uacm.edu.mx**

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**