Can. J. Math. Vol. **50** (6), 1998 pp. 1253–1272.

INTEGRAL REPRESENTATION OF p-CLASS GROUPS IN $\mathbb{Z}_p$-EXTENSIONS AND THE JACOBIAN VARIETY

PEDRO RICARDO LÓPEZ-BAUTISTA AND
GABRIEL DANIEL VILLA-SALVADOR

ABSTRACT. For an arbitrary finite Galois p-extension L/K of $\mathbb{Z}_p$-cyclotomic number fields of CM-type with Galois group $G = \mathrm{Gal}(L/K)$ such that the Iwasawa invariants μ_K^-, μ_L^- are zero, we obtain unconditionally and explicitly the Galois module structure of ${C_L}^-(p)$, the minus part of the p-subgroup of the class group of L. For an arbitrary finite Galois p-extension L/K of algebraic function fields of one variable over an algebraically closed field k of characteristic p as its exact field of constants with Galois group $G = \mathrm{Gal}(L/K)$ we obtain unconditionally and explicitly the Galois module structure of the p-torsion part of the Jacobian variety $J_L(p)$ associated to L/k.

1. **Introduction.** Let L be an algebraic number field L. It is said to be of CM-type if it is a totally imaginary quadratic extension of a totally real field. It is called a cyclotomic $\mathbb{Z}_p$-field if $L = L_0\mathbb{Q}_\infty$ where L_0 is a finite extension of $\mathbb{Q}$, the field of rational numbers, $\mathbb{Z}_p$ is the ring of the p-adic integers and $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For an odd prime p we will denote by L/K a finite Galois p-extension of $\mathbb{Z}_p$-cyclotomic number fields of CM-type with Galois group $G = \mathrm{Gal}(L/K)$ such that the Iwasawa invariants μ_K^-, μ_L^- are zero (a conjecture of Iwasawa states that the p-part of the class group is divisible. It implies $\mu_K^- = 0 = \mu_L^-$). Let L_n be the intermediate fields associated to the extension L/L_0. Let I_{L_n} be the group of ideals, P_{L_n} the group of principal ideals and C_{L_n} the group of ideal classes of L_n. It is well-known that, if $C_L(p)$ denotes the set of p-torsion elements of C_L, then, as groups, $C_L \cong \varinjlim C_{L_n}$, $C_L(p) \cong \varinjlim C_{L_n}(p)$ and $C_L = \oplus_q C_L(q)$ where q runs over the rational primes. We also have $C_L(p) \cong {C_L}^-(p) \oplus {C_L}^+(p)$ and that, as $\mathbb{Z}_p$-modules, ${C_L}^-(p) \cong R^{\lambda_L^-}$, where $C_L(p)^\pm := \{a \mid a \in C_L(p),\ a^J = \pm a\}$, J denoting complex conjugation, λ_L^- is the minus pariant λ_L of the field L and $R := \mathbb{Q}_p/\mathbb{Z}_p$, where $\mathbb{Q}_p$ is the field of the p-adic numbers. We have that G acts naturally on the $\mathbb{Z}_p$-module $C_L(p)$, so that ${C_L}^-(p)$, the minus part of the p-subgroup of the class group of L, has structure of $\mathbb{Z}_p[G]$-module. Here $\mathbb{Z}_p[G]$ denotes the group ring with coefficients in $\mathbb{Z}_p$. Iwasawa obtained [7] the $\mathbb{Q}_p[G]$-module structure of $\mathrm{Hom}_{\mathbb{Z}_p}\big({C_L}^-(p), R\big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Using this result, he gave a new proof of the Kida-Kuzmin formula which, in this context, is analogous to the Deuring-Šafarevič formula in theory of algebraic function fields of one variable.

We are interested in the explicit Galois module structure of ${C_L}^-(p)$ as $\mathbb{Z}_p[G]$-module.

Received by the editors March 5, 1998; revised July 7, 1998.

The second author's work was partially supported by CONACyT, project no. 25063-E.

AMS subject classification: Primary: 11R33; secondary: 11R23, 11R58, 14H40.

Key words and phrases: $\mathbb{Z}_p$-extensions, Iwasawa's theory, class group, integral representation, fields of algebraic functions, Jacobian variety, Galois module structure.

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

The explicit Galois module structure of ${C_L}^-(p)$ is known in some cases. The cases known before this work are the following: when G is a cyclic group of order p or p^2 (Gold-Madan [4]); when L/K is an extension unramified (Villa-Madan [17]); when the p-th roots of unity are not present in K (Villa-Madan [18]); when K contains the p-roots of unity and there exists a unique maximal decomposition group and this is normal in G (Villa-Madan [18]). This last family has as particular cases: L/K has a fully ramified prime or G is a cyclic group.

The following exact sequence of $\mathbb{Z}_p[G]$-modules was established in [18]:

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{r} R[G/G_i]}{\mathrm{Re}^*} \longrightarrow R[G]^{r-1+\lambda_K^-} \longrightarrow {C_L}^-(p) \longrightarrow 0.$$

This sequence determines implicitly the Galois module structure of ${C_L}^-(p)$ and we have that, as $\mathbb{Z}_p[G]$-modules,

$$(\alpha) \qquad {C_L}^-(p) \cong R[G]^u \oplus \Omega^{\#}\left(\frac{\bigoplus_{i=1}^{r} R[G/G_i]}{\mathrm{Re}^*}\right)$$

where u is a nonnegative integer to be determined, $\Omega^{\#}$ is the dual of the Heller's loop-space operation, $G_1, \ldots, G_r$ are the decomposition groups of the prime divisors $P_1, \ldots, P_r$ of K ramified in L and $\mathrm{Re}^* = \{(\sum_{\sigma\in G/G_1} x\sigma, \ldots, \sum_{\sigma\in G/G_r} x\sigma) \in \bigoplus_{i=1}^{r} R[G/G_i] \mid x \in R\}$.

As our first main result in this paper we obtain unconditionally and explicitly the Galois module structure of ${C_L}^-(p)$ (Theorem 1).

The integer u in (α) is given in terms of λ_K^-, the minus λ Iwasawa invariant of K and the minimum number of generators of the group $G/\hat{H}$, where $\hat{H}$ is the composite of the normal closure of the $G_i's$ in G, (Propositions 2 and 4). The decomposition in (α) of the second summand in terms of indecomposable modules is given in Propositions 5 and 10.

It has been known since the days of Gauss that there is a strong analogy between the theory of algebraic functions of one variable and the theory of algebraic numbers. In fact, Iwasawa laid the foundations of his theory in number fields, in an attempt to find an analog of the group of divisor classes of degree 0 in algebraic functions. Section 4 is devoted to algebraic function fields.

Let L/K be a finite Galois p-extension of algebraic function fields of one variable with Galois group $G = \mathrm{Gal}(L/K)$ and field of constants k, an algebraically closed field of characteristic p, where p is an arbitrary rational prime number.

The group G acts naturally on several $\mathbb{Z}_p$-modules associated to L. Let J_L be the Jacobian variety associated to L. Then G acts on J_L and, by restriction, on ${}_{p^n}J_L$, the group of points of order dividing p^n. Let $J_L(p) = \varinjlim {}_{p^n}J_L$ the p-torsion part of the Jacobian variety associated to the function field L/k. We have that $J_L(p)$ is naturally G-isomorphic to $C_{0,L}(p)$, the p-subgroup of $C_{0,L}$, the group of divisor classes of degree 0 of L. It is well-known that, as $\mathbb{Z}_p$-modules, $C_{0,L}(p) \cong R^{\tau_L}$, where τ_L is the Hasse-Witt invariant of field L.

We are interested in the explicit Galois module structure of $J_L(p)$ as $\mathbb{Z}_p[G]$-module.

In the classical case, that is, when k is the field of complex numbers, the structure of the group of divisor classes of degree 0 is given by the classical theorem of Abel and Jacobi.

The explicit Galois module structure of $J_L(p)$ is known in some cases. One of the cases is when there exists a unique maximal decomposition group and this is normal in G. This family has as particular cases: when L/K has a fully ramified prime or when L/K is a cyclic extension [18]. In that paper the following $\mathbb{Z}_p[G]$-exact sequence was obtained:

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{r} R[G/G_i]}{\mathrm{Re}^*} \longrightarrow R[G]^{r-1+\tau_K} \longrightarrow J_L(p) \longrightarrow 0.$$

This sequence determines implicitly the Galois module structure of $J_L(p)$. It was proved that, as $\mathbb{Z}_p[G]$-modules,

$$(\beta) \qquad J_L(p) \cong R[G]^v \bigoplus \Omega^{\#}\left(\frac{\bigoplus_{i=1}^{r} R[G/G_i]}{Re^*}\right),$$

where v is a nonnegative integer number to be determined and $G_1, \ldots, G_r$ are the decomposition groups of the prime divisors $P_1, \ldots, P_r$ of K ramified in L.

For a finite Galois p-extension L/K we obtain unconditionally and explicitly the Galois module structure of $J_L(p)$ (Theorem 2).

The integer v in (β) is given in terms of τ_K the Hasse-Witt invariant of K and the minimum number of generators of the group $G/\hat{H}$, where $\hat{H}$ is the composite of the normal closure of the G_i's in G, (analogue of Propositions 2 and 4). The decomposition in (β) of the second summand in terms of indecomposable modules is given as in Propositions 5 and 10.

ACKNOWLEDGMENT. The authors are grateful to Professor A. Weiss for the help they received from him during the preparation of this work.

2. **Notations.** We will denote by $\mathbb{F}_p$ the finite field with p elements, C_p the cyclic group of order p, $\mathbb{R}$ the field of real numbers, $\mathbb{N} := \{1, 2, 3, \ldots\}$ and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. For $n \in \mathbb{N}$ we set $W_n := \{\xi \in \mathbb{C} \mid \xi^n = 1\}$, $W(p) := \bigcup_{n=0}^{\infty} W_{p^n}$. We have that $R \cong W(p)$.

We will denote the disjoint union of the sets $X_1, \ldots, X_n$ by $\biguplus_{i=1}^{n} X_i$.

Let G be a finite p-group. For a $\mathbb{Z}_p[G]$-module M we write $M = M^{(0)} \oplus M^{(1)}$, where $M^{(0)}$ is $\mathbb{Z}_p[G]$-injective and $M^{(1)}$ has no injective $\mathbb{Z}_p[G]$-components. If $0 \longrightarrow M \longrightarrow Y \longrightarrow N \longrightarrow 0$ is a $\mathbb{Z}_p[G]$-exact sequence with Y injective then the dual of the Heller's loop-space operation is defined by $\Omega^{\#}(M) \cong N^{(1)}$.

We denote by M^G the set $\{m \in M \mid gm = m \; \forall g \in G\}$, $I_G := \langle g - 1 \mid g \in G \rangle \subseteq \mathbb{Z}[G] \subseteq \mathbb{Z}_p[G]$.

$I(M)$ will denote the only injective $\mathbb{Z}_p[G]$-envelope of M, up to isomorphism, and $P(M)$ will denote the only projective $\mathbb{Z}_p[G]$-cover of M, up to isomorphism, if such cover exists.

For $n \in \mathbb{N}$, we define the $\mathbb{Z}_p[G]$-homomorphism $p^n\colon M \longrightarrow M$ such that $p^n(m) = p^n m$ $\forall m \in M$. We set ${}_{p^n}M := \ker(p^n)$. Then ${}_{p^n}M$ is the subgroup of elements in M of order dividing p^n.

Let H be a subgroup of G. A subset X of G that contains exactly one element of each left coset of H in G is called a *left transversal of H in G*. If X is a left transversal of H in G and M is a $\mathbb{Z}_p[G]$-module, we define the map $\mathrm{Tr}_{G/H}\colon M^H \longrightarrow M^G$ such that $\mathrm{Tr}_{G/H}(m) = \sum_{g_i \in X} g_i m$. $\mathrm{Tr}_{G/H}$ will be called *the transversal trace of H in G*.

In general, if A is a G-module then $H^n(G, A)$ will denote the *n-th cohomology group of G with coefficients in the module A*. We write $H^n(A) := H^n(G, A)$ if the underlying group G is clear. The trivial cohomology group will be denoted by 0, whether the group structure of the module A is multiplicative or additive.

3. **Integral representation of p-class groups.** We will denote by p an odd rational prime number, L/K a finite Galois p-extension of cyclotomic $\mathbb{Z}_p$-fields of CM-type with Galois group $G = \mathrm{Gal}(L/K)$ that satisfies $\mu_L^- = 0$, $\mu_K^- = 0$. We assume $W(p) \subseteq K$. The case $W(p) \nsubseteq K$ has been considered in [18]. Let $P_1^+, \ldots, P_r^+$ be the primes in $K^+ := K \cap \mathbb{R}$ ramified in $L^+ := L \cap \mathbb{R}$ split in K and such that they are non-p primes, that is, $P_i^+{}_{|_{\mathbb{Q}}} \neq p$. Let $M_0 := \mathrm{Con}_{K^+|K}(P_1^+ \cdots P_r^+) = P_1 P_1^J \cdots P_r P_r^J$ where $\mathrm{Con}_{K^+|K}$ is the conorm map. Let $S := \{P_1, P_2, \ldots, P_r\}$, and $\hat{S} := \{Q_t^{(i)} \mid i \in [\![1, r]\!],\ t \in [\![1, g_i]\!]\}$, where $\hat{S}$ is the set consisting of the prime divisors $Q_t^{(i)}$ of L such that $Q_t^{(i)}$ divides the prime divisor P_i and g_i is the decomposition number of the prime divisor P_i. If $Q_t^{(i)} \in \hat{S}$ we define $G_t^{(i)} := \{\sigma \in G \mid Q_t^{(i)\sigma} = Q_t^{(i)}\} = \mathrm{Dec}(Q_t^{(i)} \mid P_i)$ the decomposition group of the prime divisor $Q_t^{(i)}$. If $t \in [\![1, g_i]\!]$ we set $Q_i := Q_t^{(i)}$ and $G_i := \{\, \sigma \in G \mid Q_i^\sigma = Q_i \,\} = \mathrm{Dec}(Q_i \mid P_i)$. We will say that G_i is the decomposition group of the prime divisor P_i. If P_i is any of the previous primes, we define

$$H_i^{p^{e_i}} := \mathrm{Con}_{K|L}(P_i) = (Q_1^{(i)} \cdots Q_{g_i}^{(i)})^{p^{e_i}}$$

where p^{e_i} is the ramification index and g_i is the decomposition number of the prime P_i in L/K. Let $\mathcal{N} := \prod_{i=1}^r H_i H_i^J$. We define $P_{\mathcal{N}} := \{(\alpha) \mid \alpha \in L^*,\ \alpha \equiv 1 \bmod \mathcal{N}\}$, $I_{\mathcal{N}} := \{\mathcal{O} \mid \mathcal{O}$ is divisor of L relatively prime to $\mathcal{N}\}$, $C_{\mathcal{N}} := I_{\mathcal{N}}/P_{\mathcal{N}}$ the ray class group, $T_{\mathcal{N}} := \{(\alpha) \mid \alpha \in L^*,\ (\alpha)$ is relatively prime to $\mathcal{N}\}$.

The $\mathbb{Z}_p[G]$-module structure of $C_L{}^-(p)$ is obtained implicitly in [17] and [18]. We have the $\mathbb{Z}_p[G]$-exact sequence [17, p. 332],

$$0 \longrightarrow (T_{\mathcal{N}}/P_{\mathcal{N}})^-(p) \longrightarrow C_{\mathcal{N}}^-(p) \longrightarrow C_L^-(p) \longrightarrow 0.$$

We have that, as groups, $(T_{\mathcal{N}}/P_{\mathcal{N}})^-(p) \cong W(p)^{t-\delta_K}$ where $t = \sum_{i=1}^r g_i$, and $\delta_K = 1$ if $W(p) \subseteq K$ and $\delta_K = 0$ otherwise.

In [17, Theorem 5] is shown that as $\mathbb{Z}_p[G]$-modules $(T_{\mathcal{N}}/P_{\mathcal{N}})^-(p) \cong \frac{\bigoplus_{i=1}^r R[G/G_i]}{(\mathrm{Re}^*)^{\delta_K}}$ and in [18, Proposition 3] as $\mathbb{Z}_p[G]$-modules $C_{\mathcal{N}}^-(p) \cong R[G]^{r-\delta_K+\lambda_K^-}$.

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

We set $T := \frac{\bigoplus_{i=1}^r R[G/G_i]}{\mathrm{Re}^*}$. Since $\delta_K = 1$ we obtain the $\mathbb{Z}_p[G]$-exact sequence [18, Theorem 1]

$$0 \longrightarrow T \longrightarrow R[G]^{r-1+\lambda_K^-} \longrightarrow C_L{}^-(p) \longrightarrow 0.$$

Since $R[G]^{r-1+\lambda_K^-}$ is an injective $\mathbb{Z}_p[G]$-module we obtain that there exists some $u \geq 0$ such that as $\mathbb{Z}_p[G]$-modules [18, Theorem 2],

$$(1) \qquad C_L{}^-(p) \cong C_L{}^-(p)^{(0)} \oplus C_L{}^-(p)^{(1)} \cong R[G]^u \oplus \Omega^\#\left(\frac{\bigoplus_{i=1}^r R[G/G_i]}{\mathrm{Re}^*}\right) = R[G]^u \oplus \Omega^\#(T),$$

where $C_L{}^-(p)^{(0)}$ is the injective part of $C_L{}^-(p)$ and $C_L{}^-(p)^{(1)}$ does not have injective components. The implicit $\mathbb{Z}_p[G]$-module structure of $C_L{}^-(p)$ is given in (1). To find explicitly the structure of $C_L{}^-(p)$ we will calculate the value of u and we will find the indecomposable $\mathbb{Z}_p[G]$-components of the second summand. Our first step is the following

PROPOSITION 1. *Let c be the minimum natural number such that there exists a $\mathbb{Z}_p[G]$-monomorphism $\phi: T \longrightarrow R[G]^c$. Then $R[G]^c$ is the injective $\mathbb{Z}_p[G]$-envelope of T and there exists a $\mathbb{Z}_p[G]$-exact sequence $0 \longrightarrow T \longrightarrow R[G]^c \longrightarrow \Omega^\#(T) \longrightarrow 0$.*

PROOF. Let $\big(I(T), h\big)$ be the injective $\mathbb{Z}_p[G]$-envelope of T. It follows that $R[G]^c \cong I(T) \oplus W$ for some $\mathbb{Z}_p[G]$-module W. It follows that $I(T) \cong R[G]^d$ for some $d \leq c$. Therefore we have a $\mathbb{Z}_p[G]$-monomorphism $\phi: T \longrightarrow R[G]^d$. Since c is minimum it follows that $d = c$. Since ${}_p(R[G]^c/T) \cong \frac{\mathbb{F}_p[G]^c}{{}_pT}$ and this module does not have $\mathbb{F}_p[G]$-injective components, it follows from [11, Lemma 3] that $R[G]^c/T$ does not have $\mathbb{Z}_p[G]$-injective components. ∎

PROPOSITION 2. *Let $(R[G]^c, h)$ be the injective $\mathbb{Z}_p[G]$-envelope of T and $u \in \mathbb{N}_0$ such that $C_L{}^-(p)^{(0)} \cong R[G]^u$. Then there exists an $\mathbb{F}_p[G]$-exact sequence*

$$0 \longrightarrow {}_pT \xrightarrow{\hat{h}} \mathbb{F}_p[G]^c \longrightarrow \Omega^\#({}_pT) \longrightarrow 0.$$

Furthermore, the integer u is given by $u = r - 1 - c + \lambda_K^-$ and $c = \dim_{\mathbb{F}_p}\big(({}_pT)^G\big)$.

PROOF. Since T is a p-divisible module we obtain the $\mathbb{F}_p[G]$-exact sequence

$$0 \longrightarrow {}_pT \xrightarrow{\hat{h}} \mathbb{F}_p[G]^c \longrightarrow {}_p\Omega^\#(T) \longrightarrow 0.$$

It follows from [9, Proposition 2.11] that $\Omega^\#({}_pT) \cong {}_p\Omega^\#(T)$.

Since $R[G]^c$ and $R[G]^{r-1+\lambda_K^-}$ are injective $\mathbb{Z}_p[G]$-modules, we obtain the $\mathbb{Z}_p[G]$-exact sequence

$$0 \longrightarrow T \longrightarrow R[G]^{r-1+\lambda_K^-} \longrightarrow R[G]^u \oplus \Omega^\#(T) \longrightarrow 0.$$

From Proposition 1 and Schanuel's Lemma for injective modules we have that

$$R[G]^c \oplus R[G]^u \oplus \Omega^\#(T) \cong \Omega^\#(T) \oplus R[G]^{r-1+\lambda_K^-}.$$

Therefore $u = r - 1 - c + \lambda_K^-$.

Let $c' := \dim_{\mathbb{F}_p}\big(({}_pT)^G\big)$. From the $\mathbb{F}_p[G]$-exact sequence

$$0 \longrightarrow ({}_pT)^G \xrightarrow{\hat{h}} \big(\mathbb{F}_p[G]^c\big)^G \longrightarrow \big({}_p\Omega^\#(T)\big)^G,$$

we obtain a $\mathbb{F}_p[G]$-monomorphism $({}_pT)^G \xrightarrow{\hat{f}} \mathbb{F}_p^c$. Thus $c' \leq c$.

We have that $(\mathbb{F}_p[G]^c, \hat{f})$ is the injective $\mathbb{F}_p[G]$-envelope of ${}_pT$. Therefore c is the minimum nonnegative integer such that there exists an $\mathbb{F}_p[G]$-monomorphism $\hat{h}\colon {}_pT \longrightarrow \mathbb{F}_p[G]^c$.

Since $({}_pT)^G \cong \mathbb{F}_p^{c'} \subseteq \mathbb{F}_p[G]^{c'}$, we have that there exists an $\mathbb{F}_p[G]$-monomorphism

$$\rho\colon ({}_pT)^G \longrightarrow \mathbb{F}_p[G]^{c'}.$$

Since $\mathbb{F}_p[G]^{c'}$ is an injective $\mathbb{F}_p[G]$-module and the inclusion map $i\colon ({}_pT)^G \longrightarrow {}_pT$ is an $\mathbb{F}_p[G]$-monomorphism, it follows that there exists $\hat{\rho}\colon {}_pT \longrightarrow \mathbb{F}_p[G]^{c'}$, an $\mathbb{F}_p[G]$-homomorphism such that $\rho = \hat{\rho} \circ i$. We have that $\hat{\rho}$ is a $\mathbb{F}_p[G]$-monomorphism because otherwise if $\ker(\hat{\rho}) \neq (0)$, then, since $\mathbb{F}_p$ is a field of characteristic p and G is a finite p-group we would have that $\big(\ker(\hat{\rho})\big)^G \neq 0$. Now, $\big(\ker(\hat{\rho})\big)^G = \ker(\hat{\rho}) \cap ({}_pT)^G = \ker(\rho) = 0$. Therefore $\hat{\rho}$ is an $\mathbb{F}_p[G]$-monomorphism. Thus $c \leq c'$. ∎

We now calculate $\dim_{\mathbb{F}_p}\big(({}_pT)^G\big)$. Let $H_1, \dots, H_r$ be arbitrary subgroups of G and let $T_t := \frac{\bigoplus_{i=1}^t R[G/H_i]}{\mathrm{Re}^*_{(t)}}$, $t \in [\![1, r]\!]$ where $\mathrm{Re}^*_{(t)}$ is the diagonal submodule of $\bigoplus_{i=1}^t R[G/H_i]$. We have that ${}_pT_t = \frac{\bigoplus_{i=1}^t \mathbb{F}_p[G/H_i]}{\mathbb{F}_p e^*_{(t)}}$, where $\mathbb{F}_p e^*_{(t)}$ is the diagonal submodule of $\bigoplus_{i=1}^t \mathbb{F}_p[G/H_i]$. First, we will calculate $\dim_{\mathbb{F}_p}\big(({}_pT_1)^G\big)$.

PROPOSITION 3. *Let G be a finite p-group, H an arbitrary subgroup of G, $\psi \in \mathrm{Hom}(G, C_p)$, $\hat{H} := \langle gHg^{-1} \mid g \in G\rangle$ the normal closure of H in G, $d_{G/\hat{H}}$ the minimum number of generators of the group $G/\hat{H}$. Let $\alpha_1\colon \mathbb{F}_p e^*_{(1)} \longrightarrow \mathbb{F}_p[G/H]$ be the $\mathbb{F}_p[G]$-homomorphism given by $\alpha_1(x) = \sum_{\sigma \in G/H} x\sigma$, and let $\alpha_1^*\colon H^1(G, \mathbb{F}_p e^*_{(1)}) \longrightarrow H^1(G, \mathbb{F}_p[G/H])$ be the map induced by α_1 on the cohomology groups. Then*

(a) $\dim_{\mathbb{F}_p}\big(({}_pT_1)^G\big) = \dim_{\mathbb{F}_p}\left(\left(\frac{\mathbb{F}_p[G/H]}{\mathbb{F}_p e^*_{(1)}}\right)^G\right) = \dim_{\mathbb{F}_p}\big(\ker(\alpha_1^*)\big)$.

(b) $\psi \in \ker(\alpha_1^*)$ *if and only if* $\hat{H} \leq \ker(\psi)$.

(c) $\ker(\alpha_1^*) \cong \mathrm{Hom}(G/\hat{H}, C_p)$.

(d) $\dim_{\mathbb{F}_p}\big(\ker(\alpha_1^*)\big) = d_{G/\hat{H}}$. *Therefore* $\dim_{\mathbb{F}_p}\big(({}_pT_1)^G\big) = \dim_{\mathbb{F}_p}\left(\left(\frac{\mathbb{F}_p[G/H]}{\mathbb{F}_p e^*_{(1)}}\right)^G\right) = d_{G/\hat{H}}$.

PROOF. (a) From the $\mathbb{F}_p[G]$-exact sequence

$$0 \longrightarrow \mathbb{F}_p e^*_{(1)} \xrightarrow{\alpha_1} \mathbb{F}_p[G/H] \xrightarrow{\pi} \frac{\mathbb{F}_p[G/H]}{\mathbb{F}_p e^*_{(1)}} \longrightarrow 0,$$

we obtain the long exact sequence in cohomology,

$$\begin{aligned} 0 \longrightarrow (\mathbb{F}_p e^*_{(1)})^G \longrightarrow \big(\mathbb{F}_p[G/H]\big)^G \longrightarrow ({}_pT_1)^G \longrightarrow H^1(\mathbb{F}_p e^*_{(1)}) \longrightarrow \\ \longrightarrow H^1\big(\mathbb{F}_p[G/H]\big) \longrightarrow H^1({}_pT_1) \longrightarrow \cdots. \end{aligned}$$

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

Since $(\mathbb{F}_p[G/H])^G \cong \mathbb{F}_p \cong \mathbb{F}_p e^*_{(1)}$ we have the exact sequence of groups

$$0 \longrightarrow \mathbb{F}_p e^*_{(1)} \xrightarrow{\varphi_3} \mathbb{F}_p e^*_{(1)} \xrightarrow{\varphi_2} ({}_pT_1)^G \xrightarrow{\varphi_1} H^1(\mathbb{F}_p e^*_{(1)}) \longrightarrow \cdots.$$

It follows that φ_1 is injective. Then we have the exact sequence of groups

$$0 \longrightarrow ({}_pT_1)^G \longrightarrow H^1(\mathbb{F}_p e^*_{(1)}) \xrightarrow{\alpha_1^*} H^1\bigl(\mathbb{F}_p[G/H]\bigr) \longrightarrow \cdots.$$

Since G acts trivially on the module $\mathbb{F}_p e^*_{(1)}$, we obtain the exact sequence

$$0 \longrightarrow ({}_pT_1)^G \xrightarrow{\varphi_1} \operatorname{Hom}(G, C_p) \xrightarrow{\alpha_1^*} H^1\bigl(\mathbb{F}_p[G/H]\bigr) \longrightarrow \cdots.$$

So, $\ker(\alpha_1^*) = \operatorname{im}(\varphi_1) \cong ({}_pT_1)^G = \left(\frac{\mathbb{F}_p[G/H]}{\mathbb{F}_p e^*_{(1)}}\right)^G$.

(b) The map $\alpha_1^*\colon \operatorname{Hom}(G, C_p) \longrightarrow H^1(\mathbb{F}_p[G/H])$ is given by

$$\alpha_1^*(\psi) = \alpha_1 \circ \psi + B^1\bigl(G, \mathbb{F}_p[G/H]\bigr), \quad \text{where} \quad \alpha_1 \circ \psi(g) = \sum_{\sigma \in G/H} \psi(g)\sigma \quad \forall g \in G.$$

We have the following equivalences

$$\begin{aligned} \psi \in \ker(\alpha_1^*) &\iff \alpha_1^*(\psi) = \alpha_1 \circ \psi + B^1\bigl(G, \mathbb{F}_p[G/H]\bigr) = B^1\bigl(G, \mathbb{F}_p[G/H]\bigr) \\ &\iff \alpha_1 \circ \psi \in B^1\bigl(G, \mathbb{F}_p[G/H]\bigr) \\ &\iff \exists\, \varepsilon \in \mathbb{F}_p[G/H] \text{ such that } \alpha_1 \circ \psi(g) = (g-1)\varepsilon, \forall\, g \in G. \end{aligned}$$

From these equivalences it follows that $\psi \in \ker(\alpha_1^*) \Rightarrow \hat{H} \leq \ker(\psi)$. For the opposite implication we assume that $\hat{H} \leq \ker(\psi)$. We will prove that $\psi \in \ker(\alpha_1^*)$. For this, it suffices to show the existence of an element $\varepsilon \in \mathbb{F}_p[G/H]$ such that $\alpha_1 \circ \psi(g) = (g-1)\varepsilon$ for all $g \in G$.

We set $\varepsilon := \sum_{\sigma \in G/H} s_\sigma \sigma \in \mathbb{F}_p[G/H]$. As candidates for the s_σ we set $s_{gH} := s_H - \psi(g)$. The definition of $s_\sigma = s_{gH}$ does not depend on the representative of the class σ. Thus, if $\varepsilon = \sum_{\sigma \in G/H} s_\sigma \sigma = \sum_{xH \in G/H} \bigl(s_H - \psi(x_\sigma)\bigr)\sigma$, where x_σ is any representative of the class σ then ε satisfies $\alpha_1 \circ \psi(g) = (g-1)\varepsilon$, for all $g \in G$. Therefore $\psi \in \ker(\alpha_1^*) \Leftrightarrow \hat{H} \leq \ker(\psi)$.

(c) Let $\psi \in \ker(\alpha_1^*) \subseteq \operatorname{Hom}(G, C_p)$. We have that $\psi \in \ker(\alpha_1^*) \Leftrightarrow \hat{H} \leq \ker(\psi)$ with $\hat{H} \trianglelefteq G$. Therefore, for each $\psi \in \ker(\alpha_1^*)$, there exists a unique $\hat{\psi} \in \operatorname{Hom}(G/\hat{H}, C_p)$ such that $\hat{\psi}(g\hat{H}) = \psi(g)$ for all $g \in G$. Let $\rho\colon \ker(\alpha_1^*) \longrightarrow \operatorname{Hom}(G/\hat{H}, C_p)$ be given by $\rho(\psi) = \hat{\psi}$. We have that ρ is an isomorphism.

(d) Since $G/\hat{H}$ is a finite p-group we have that $\operatorname{Hom}_{\mathbb{Z}}(G/\hat{H}, C_p) \cong \operatorname{Hom}_{\mathbb{Z}}\left(\frac{G/\hat{H}}{\Phi(G/\hat{H})}, C_p\right)$ where $\Phi(G/\hat{H})$ is the Frattini subgroup of $G/\hat{H}$. From (c) and from [15, Theorem 1.16] it follows that

$$\dim_{\mathbb{F}_p}\bigl(\ker(\alpha_1^*)\bigr) = \dim_{\mathbb{F}_p}\left(\operatorname{Hom}_{\mathbb{Z}}\left(\frac{G/\hat{H}}{\Phi(G/\hat{H})}, C_p\right)\right) = d_{G/\hat{H}}. \qquad \blacksquare$$

Now, we calculate $\dim_{\mathbb{F}_p}\bigl(({}_pT_r)^G\bigr)$ for $r \geq 2$.

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

PROPOSITION 4. *Let G be a finite p-group, $H_1,\ldots,H_r$ arbitrary subgroups of G. For each $i\in[\![1,r]\!]$, let $\hat{H}_i:=\langle gH_ig^{-1}\mid g\in G\rangle$ be the normal closure of the subgroup H_i in G. We set $\hat{H}:=\hat{H}_1\cdots\hat{H}_r$ and let $d_{G/\hat{H}}$ be the minimum number of generators of the group $G/\hat{H}$. Then $\dim_{\mathbb{F}_p}\big(({}_pT_r)^G\big)=r-1+d_{G/\hat{H}}$.*

PROOF. For each $i\in[\![1,r]\!]$ we consider the maps $\alpha_i\colon \mathbb{F}_pe_i^*\longrightarrow\mathbb{F}_p[G/H_i]$ such that $\alpha_i(x)=\sum_{\sigma\in G/H_i}x\sigma$, where $\mathbb{F}_pe_i^*$ is the diagonal submodule of $\mathbb{F}_p[G/H_i]$. Since the group G acts trivially on $\mathbb{F}_pe_i^*$ we have that $H^1(G,\mathbb{F}_pe_i^*)\cong\operatorname{Hom}(G,C_p)$. Let α_i^* be the map induced by α_i on the cohomology groups, that is

$$\alpha_i^*\colon\operatorname{Hom}(G,C_p)\longrightarrow H^1\big(G,\mathbb{F}_p[G/H_i]\big)$$

such that, for each $\psi\in\operatorname{Hom}(G,C_p)$, $\alpha_i^*(\psi)=\alpha_i\circ\psi+B^1(G,\mathbb{F}_p[G/H_i])$, where $\alpha_i\circ\psi(g)=\sum_{\sigma\in G/H_i}\psi(g)\sigma\forall g\in G$. We set $\mathbb{F}_pe^*:=\mathbb{F}_pe^*_{(r)}$. We consider the $\mathbb{F}_p[G]$-exact sequence

$$0\longrightarrow\mathbb{F}_pe^*\xrightarrow{\alpha}\bigoplus_{i=1}^r\mathbb{F}_p[G/H_i]\xrightarrow{\pi}\frac{\bigoplus_{i=1}^r\mathbb{F}_p[G/H_i]}{\mathbb{F}_pe^*}\longrightarrow 0,$$

where $(x,\ldots,x)\xrightarrow{\alpha}(\sum_{\sigma\in G/H_1}x\sigma,\ldots,\sum_{\sigma\in G/H_r}x\sigma)$. Therefore $\alpha=(\alpha_1,\ldots,\alpha_r)$. We obtain the long exact sequence in cohomology,

$$\begin{gathered}0\longrightarrow(\mathbb{F}_pe^*)^G\xrightarrow{\varphi_3}\Big(\bigoplus_{i=1}^r\mathbb{F}_p[G/H_i]\Big)^G\xrightarrow{\varphi_2}({}_pT_r)^G\xrightarrow{\varphi_1}H^1(G,\mathbb{F}_pe^*)\xrightarrow{\alpha^*}\\ \xrightarrow{\alpha^*}\bigoplus_{i=1}^rH^1\big(G,\mathbb{F}_p[G/H_i]\big)\longrightarrow H^1({}_pT_r)\longrightarrow\cdots,\end{gathered}$$

where for each $\psi\in\operatorname{Hom}(G,C_p)$ we have $\alpha^*(\psi)=\big(\alpha_1^*(\psi),\ldots,\alpha_r^*(\psi)\big)$. Since the group G acts trivially on $\mathbb{F}_pe^*$, we obtain the exact sequence

$$\begin{gathered}0\longrightarrow\mathbb{F}_pe^*\xrightarrow{\varphi_3}(\mathbb{F}_pe^*)^r\xrightarrow{\varphi_2}({}_pT_r)^G\xrightarrow{\varphi_1}\operatorname{Hom}(G,C_p)\xrightarrow{\alpha^*}\\ \xrightarrow{\alpha^*}\bigoplus_{i=1}^rH^1\big(G,\mathbb{F}_p[G/H_i]\big)\longrightarrow H^1({}_pT_r)\longrightarrow\cdots.\end{gathered}\tag{2}$$

Since $\ker(\alpha^*)=\operatorname{im}(\varphi_1)$, from (2) we obtain the $\mathbb{F}_p$-exact sequence

$$0\longrightarrow\mathbb{F}_pe^*\xrightarrow{\varphi_3}(\mathbb{F}_pe^*)^r\xrightarrow{\varphi_2}({}_pT_r)^G\xrightarrow{\varphi_1}\ker(\alpha^*)\longrightarrow 0.\tag{3}$$

Therefore, $r=\dim_{\mathbb{F}_p}\big(\ker(\varphi_2)\big)+\dim_{\mathbb{F}_p}\big(\operatorname{im}(\varphi_2)\big)=1+\dim_{\mathbb{F}_p}\big(\ker(\varphi_1)\big)$. It follows that $\dim_{\mathbb{F}_p}\big(\ker(\varphi_1)\big)=r-1$. From (3) we obtain the $\mathbb{F}_p$-exact sequence

$$0\longrightarrow(\mathbb{F}_pe^*)^{r-1}\longrightarrow({}_pT_r)^G\longrightarrow\ker(\alpha^*)\longrightarrow 0.\tag{4}$$

Since $(\mathbb{F}_pe^*)^{r-1}$ is $\mathbb{F}_p$-injective, we have that $\dim_{\mathbb{F}_p}\big(({}_pT_r)^G\big)=r-1+\dim_{\mathbb{F}_p}\big(\ker(\alpha^*)\big)$.

From Proposition 3 (b) it follows that for each $i \in [\![1, r]\!]$ the map ψ is characterized by $\psi \in \ker(\alpha_i^*) \Leftrightarrow \hat{H}_i \leq \ker(\psi)$. Since $\alpha^*(\psi) = \big(\alpha_1^*(\psi), \ldots, \alpha_r^*(\psi)\big)$, we have that

$$\begin{aligned} \psi \in \ker(\alpha^*) &\iff \psi \in \ker(\alpha_i^*) \quad \forall\, i \in [\![1, r]\!], \\ &\iff \hat{H}_i \leq \ker(\psi) \quad \forall\, i \in [\![1, r]\!], \\ &\iff \hat{H} = \hat{H}_1 \cdots \hat{H}_r \leq \ker(\psi). \end{aligned}$$

In a similar fashion, as in the proof of Proposition 3 (c), it can be proven that $\ker(\alpha^*) \cong \operatorname{Hom}(G/\hat{H}, C_p)$. Therefore $\dim_{\mathbb{F}_p}\big(\ker(\alpha^*)\big) = d_{G/\hat{H}}$. ■

PROPOSITION 5. *Let L/K be a finite Galois p-extension of cyclotomic $\mathbb{Z}_p$-fields of CM-type with Galois group $G = \operatorname{Gal}(L/K)$ such that $\mu_K^- = 0$, $\mu_L^- = 0$. Let $H_1, \ldots, H_r$ be arbitrary subgroups of G. Reordering the indices and taking conjugates, if necessary, let $1 \leq i_1 < i_2 < \cdots < i_{s-1} < i_s = r$ be such that*

$$\begin{gathered} H_1, \ldots, H_{i_1-1} \subseteq H_{i_1} \\ H_{i_1+1}, \ldots, H_{i_2-1} \subseteq H_{i_2} \\ \vdots \\ H_{i_{s-1}+1}, \ldots, H_{i_s-1} \subseteq H_{i_s} = H_r \end{gathered}$$

and that the subgroups $H_{i_1}, H_{i_2}, \ldots, H_{i_s}$ satisfy the condition: If for $1 \leq j, k \leq s$, there exists some $g \in G$ such that $H_{i_j}^g = gH_{i_j}g^{-1} \subseteq H_{i_k}$, then $j = k$. Let $A_2 := \{i_1, i_2, \ldots, i_s\}$ and $A_1 := [\![1, r]\!] - A_2$. Then

$$\frac{\bigoplus_{i=1}^{r} R[G/H_i]}{\mathrm{Re}^*} \cong \bigoplus_{i \in A_1} R[G/H_i] \bigoplus \frac{\bigoplus_{i \in A_2} R[G/H_i]}{\mathrm{Re}^*_{A_2}},$$

where $\mathrm{Re}^*_{A_2} := \{(\sum_{\sigma \in G/H_{i_1}} x\sigma, \ldots, \sum_{\sigma \in G/H_{i_s}} x\sigma) \in \oplus_{i \in A_2} R[G/H_i] \mid x \in R\}$.

PROOF. For each $j \in [\![1, s]\!]$, we set

$$\Lambda_{\hat{\imath}_j} \colon R[G/H_{i_j}] \longrightarrow R[G/H_{\hat{\imath}_j}], \qquad \sum_{\psi \in G/H_{i_j}} a_\psi \psi \longrightarrow \sum_{\psi \in G/H_{i_j}} a_\psi \sum_{\substack{\sigma \subseteq \psi \\ \sigma \in G/H_{\hat{\imath}_j}}} \sigma,$$

where $\hat{\imath}_j \in [\![i_{j-1} + 1, i_j - 1]\!]$, $i_0 = 0$. We have that $\Lambda_{\hat{\imath}_j}$ is a $\mathbb{Z}_p[G]$-monomorphism. We set

$$\begin{aligned} \Lambda \colon \bigoplus_{i=1}^{r} R[G/H_i] &\longrightarrow \frac{\bigoplus_{i=1}^{r} R[G/H_i]}{\mathrm{Re}^*}, \\ (\xi_1, \ldots, \xi_{i_j}, \ldots, \xi_r) &\longrightarrow \overline{(c_1, \ldots, c_{r-1}, c_r)}, \end{aligned}$$

where

$$c_t = \begin{cases} \xi_t + \Lambda_t(\xi_{i_j}) & \text{if } t \in [\![i_{j-1} + 1, i_j - 1]\!] \\ \xi_{i_j} & \text{if } t = i_j. \end{cases}$$

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

The map Λ is a $\mathbb{Z}_p[G]$-epimorphism and $\ker(\Lambda) = D \cong \mathrm{Re}^*_{A_2}$, with $D \subseteq \oplus_{i=1}^r R[G/H_i]$,

$$D := \Big\{ \Big(0, \ldots, 0, \sum_{\psi \in G/H_{i_1}} x\psi, 0, \ldots, 0, \sum_{\psi \in G/H_{i_2}} x\psi, 0, \ldots, 0, \sum_{\psi \in G/H_{i_s}} x\psi\Big) \;\Big|\; x \in R \Big\}. \qquad \blacksquare$$

In (1), from Proposition 5 it follows that

$$\Omega^{\#}\left(\frac{\overset{r}{\underset{i=1}{\oplus}} R[G/G_i]}{\mathrm{Re}^*}\right) \cong \bigoplus_{i \in A_1} \frac{R[G]}{R[G/G_i]} \bigoplus \Omega^{\#}\left(\frac{\underset{i\in A_2}{\oplus} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right).$$

An essential part in the demonstration of the $\mathbb{Z}_p[G]$-indecomposability of the module $\Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right)$ is the $\mathbb{F}_p[G]$-indecomposability of the $\mathbb{F}_p[G]$-module $p\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right) \cong \frac{\bigoplus_{i\in A_2} \mathbb{F}_p[G/G_i]}{\mathbb{F}_p e^*_{A_2}}$.

If F is a field and X is a finite set, we set $\hat{X} := \sum_{x\in X} x \in F[X]$.

PROPOSITION 6. *Let G be a finite p-group and let $H_1, \ldots, H_r$ be subgroups of G. Consider the natural action of G on the set $S := \biguplus_{i=1}^r G/H_i$. Then, as $\mathbb{F}_p[G]$-modules, $\oplus_{i=1}^r \mathbb{F}_p[G/H_i] \cong \mathbb{F}_p\big[\biguplus_{i=1}^r G/H_i\big]$ and, therefore, $\frac{\bigoplus_{i=1}^r \mathbb{F}_p[G/H_i]}{\mathbb{F}_p e^*} \cong \frac{\mathbb{F}_p[S]}{\mathbb{F}_p\hat{S}}$ as $\mathbb{F}_p[G]$-modules.*

PROOF. The mapping $\phi\colon \oplus_{i=1}^r \mathbb{F}_p[G/H_i] \longrightarrow \mathbb{F}_p\big[\biguplus_{i=1}^r G/H_i\big]$, such that

$$\phi\Big(\Big(\sum_{\sigma_1\in G/H_1} a_{\sigma_1}\sigma_1, \cdots, \sum_{\sigma_r \in G/H_r} a_{\sigma_r}\sigma_r\Big)\Big) = \sum_{i=1}^r \sum_{\sigma_i \in G/H_i} a_{\sigma_i}\sigma_i$$

is an $\mathbb{F}_p[G]$-isomorphism. $\blacksquare$

Kindly, Professor Alfred Weiss supplied the proof that the $\mathbb{F}_p[G]$-module $\frac{\mathbb{F}_p[\mathbb{S}]}{\mathbb{F}_p\hat{\mathbb{S}}}$ is $\mathbb{F}_p[G]$-indecomposable, where $\mathbb{S} := \biguplus_{i\in A_2} G/G_i$. Moreover, Professor Weiss proves that the $F[G]$-module $\frac{F[S]}{F\hat{S}}$ is an indecomposable $F[G]$-module, where F is an arbitrary field of characteristic p, G a finite p-group and $S := \bigcup_{i=1}^r G/H_i$ with H_i arbitrary subgroups of G subject to the condition that $H_i^g = gH_ig^{-1} \subseteq H_j$ for some $g \in G \Leftrightarrow i = j$.

PROPOSITION 7 (WEISS). *Let G be a finite p-group, F a field of characteristic p, S a finite set, such that G acts on S, H a subgroup of G acting by restriction on S and B an $F[G]$-module. Then*

(a) The set $\mathbf{S} := \{\hat{X} \mid X$ is a H-orbit in $S\}$ is an F-base of the module $(F[S])^H$. In particular, the set $\bar{\mathbf{S}} := \{\hat{X} + F\hat{S} \mid \hat{X} \in \mathbf{S}\}$ is F-generator of the module $\frac{(F[S])^H}{F\hat{S}}$.

(b) Every $f \in \mathrm{End}_{F[G]}(B)$ induces an map $\hat{f} \in \mathrm{End}_F\left(\frac{B}{I_GB}\right)$ given by $\hat{f}(b + I_GB) = f(b) + I_GB$.

(c) We consider the homomorphism of F-algebras $\psi\colon \mathrm{End}_{F[G]}(B) \longrightarrow \mathrm{End}_F\left(\frac{B}{I_GB}\right)$ such that $\psi(f) = \hat{f}$ and let $A := \psi\big(\mathrm{End}_{F[G]}(B)\big)$. Then $\frac{A}{\mathrm{rad}(A)} \cong \frac{\mathrm{End}_{F[G]}(B)}{\mathrm{rad}(\mathrm{End}_{F[G]}(B))}$, where $\mathrm{rad}(A)$ denotes the Jacobson radical of A.

(d) $\frac{F[S]}{F\hat{S}}$ is an indecomposable $F[G]$-module if and only if A is a local ring.

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

PROOF. (a) Let $x = \sum_{s \in S} r_s s \in (F[S])^H$. If X_i, $i \in [\![1,t]\!]$ are the H-orbits over S, we have that $x = \sum_{i=i}^{t} r_i \sum_{s \in X_i} s = \sum_{i=1}^{t} r_i \hat{X}_i$. It follows that the set $\mathbf{S}$ is an F-generator of $(F[S])^H$. If $\sum_{i=i}^{t} b_i \hat{X}_i = 0$ then $b_i = 0 \; \forall\, i \in [\![1,t]\!]$. It follows that $\mathbf{S}$ is an F-base.

(b) We have that $f(I_G B) = I_G f(B)$ and $I_G B \subseteq \ker(\pi \circ f)$, where π is the canonical projection. So, there exists a unique $\hat{f} \in \mathrm{End}_{F[G]}\left(\frac{B}{I_G B}\right)$ as is required. Since G acts trivially on $\frac{B}{I_G B}$, $\mathrm{End}_{F[G]}\left(\frac{B}{I_G B}\right) \cong \left(\mathrm{End}_F\left(\frac{B}{I_G B}\right)\right)^G \cong \mathrm{End}_F\left(\frac{B}{I_G B}\right)$.

(c) From [12, Lemma 2.21], we have that I_G is a nilpotent ideal. It follows that $\ker(\psi) = \{ f \in \mathrm{End}_{F[G]}(B) \mid f(B) \subseteq I_G B\}$ is a nilpotent ideal. From [1, Corollary 15.10] we obtain that $\ker(\psi) \subseteq \mathrm{rad}\big(\mathrm{End}_{F[G]}(B)\big)$. From [3, Proposition 5.1-iii] it follows that $\mathrm{rad}\left(\frac{\mathrm{End}_{F[G]}(B)}{\ker(\psi)}\right) \cong \frac{\mathrm{rad}\left(\mathrm{End}_{F[G]}(B)\right)}{\ker(\psi)}$. Since $\psi \colon \mathrm{End}_{F[G]}(B) \longrightarrow A$ is an epimorphism, we have that $\frac{\mathrm{End}_{F[G]}(B)}{\ker(\psi)} \cong A$.

(d) It follows from [3, Proposition 6.10]; [3, Proposition 5.21] and (c). ∎

Let G be a finite p-group, H a subgroup of G such that G acts on a finite set S and let X be an H-orbit of S. We say that X is a Weiss H-orbit over S if X contains some $s \in S$ such that the stabilizer G_s satisfies $G_s \le H$. We have that X is a Weiss H-orbit over S if and only if $G_s = H_s$ for some $s \in X$ if and only if $G_s \subseteq H$ for some $s \in X$.

PROPOSITION 8 (WEISS). *Let G be a finite p-group, F a field of characteristic p, S a finite set such that G acts on S, H a subgroup of G acting by restriction on S. Then $\mathcal{B} := \{\mathrm{Tr}_{G/H}(\hat{X}) \mid X$ a Weiss H-orbit$\}$ is an F-base of the module $\mathrm{Tr}_{G/H}(F[S]^H)$.*

PROOF. Let $\varepsilon \in \mathrm{Tr}_{G/H}(F[S]^H)$. Then $\varepsilon = \mathrm{Tr}_{G/H}(\sum_{i=1}^{t} r_i \hat{X}_i) = \sum_{i=1}^{t} r_i \mathrm{Tr}_{G/H}(\hat{X}_i)$ where $r_i \in F$ and X_i, $i \in [\![1,t]\!]$ are the H-orbits over S. Let $s \in S$ and let X_i be an H-orbit over S such that $s \in X_i$. We have that if $H = \biguplus_{i=1}^{[H:H_s]} h_i H_s$, then $X_i = \{h_i s \mid i \in [\![1,[H:H_s]]\!]\}$. So, $\mathrm{Tr}_{G/H}(\hat{X}_i) = \mathrm{Tr}_{G/H}\mathrm{Tr}_{H/H_s}(s) = \mathrm{Tr}_{G/H_s}(s) = \mathrm{Tr}_{G/G_s}\mathrm{Tr}_{G_s/H_s}(s) = \mathrm{Tr}_{G/G_s}([G_s : H_s]s) = [G_s : H_s]\mathrm{Tr}_{G/G_s}(s) = \begin{cases} \hat{O}_s & \text{if } G_s = H_s \\ 0 & \text{otherwise,} \end{cases}$ where $\hat{O}_s$ is the G-orbit over S containing s. Hence $\varepsilon = \sum_{i=1}^{t} r_i [G_s : H_s]\mathrm{Tr}_{G/G_s}(s) = \sum_{i=1}^{t} r_i \mathrm{Tr}_{G/H}(\hat{X}_i)$, where the $X_i's$ are Weiss H-orbits over S.

Clearly $\mathcal{B}$ is an F-linearly independent set. ∎

PROPOSITION 9 (WEISS). *Let G be a finite p-group, F a field of characteristic p, $H_1, \ldots, H_r$ subgroups of G satisfying the condition*

$$(*) \qquad H_i^g = gH_ig^{-1} \subseteq H_j \quad \textit{for some } g \in G \iff i = j$$

and such that G acts in a natural way on the set $S := \biguplus_{i=1}^{r} G/H_i$. Then $B := \frac{F[S]}{F\hat{S}}$ is an indecomposable $F[G]$-module.

PROOF. Let $A := \{\hat{f} \mid f \in \mathrm{End}_{F[G]}(B)\}$, where $\hat{f} \in \mathrm{End}_F\left(\frac{B}{I_G B}\right)$ and $\hat{f}(x + I_G B) = f(x) + I_G B$. In order to prove the $F[G]$-indecomposability of the module B, it suffices to prove that A is a local ring. Let $v_j := \pi(H_j + F\hat{S})$, $j \in [\![1,r]\!]$, where $\pi \colon B \longrightarrow \frac{B}{I_G B}$ is the canonical projection. We have that $V := \{v_j \mid j \in [\![1,r]\!]\}$ is an F-generator set of the module $\frac{B}{I_G B}$. The map $\rho\colon I_G F[S] \longrightarrow I_G\left(\frac{F[S]}{F\hat{S}}\right)$ given by $\sum_{i=1}^n x_i y_i \longrightarrow \sum_{i=1}^n x_i(y_i + F\hat{S})$ is an $F[G]$-epimorphism with $\ker(\rho) \cong F\hat{S}$. Thus $I_G B \cong \frac{I_G F[S]}{F\hat{S}}$.

We consider $x = \sum_{i=1}^n x_i y_i \in I_G F[S]$, where $x_i \in I_G$, $y_i \in F[S]$. We have that

$$x_i y_i = \Bigl(\sum_{g\in G} r_g g\Bigr)\Bigl(\sum_{j=1}^{r}\sum_{\sigma_j\in G/H_j} a_{\sigma_j}\sigma_j\Bigr) = \sum_{j=1}^{r}\sum_{\sigma_j\in G/H_j}\sum_{g\in G}(r_g a_{\sigma_j})\sigma_j. \tag{5}$$

Therefore, for each $\sigma_j \in G/H_j$ and for each $j \in [\![1, r]\!]$ the coefficients in $\sum_{g\in G}(r_g a_{\sigma_j} g)\sigma_j$ satisfy $\sum_{g\in G} r_g a_{\sigma_j} = 0$. Given $\sum_{i=1}^r a_i v_i$, any linear F-combination of the v_i, equal to zero, it follows that $(a_1 H_1 + \cdots + a_r H_r) + F\hat{S} \in I_G B$; so $a_i = 0\ \forall\, i \in [\![1, r]\!]$. Therefore V is an F-base of $\frac{B}{I_G B}$.

Since $f(H_j + F\hat{S}) \in \frac{F[S]^{H_j}}{F\hat{S}}$, from Proposition 7 (b), it follows that $f(H_j + F\hat{S}) = \bigl(\sum_{X\in S/H_j} a_j(X)\hat{X}\bigr) + F\hat{S}$, where $a_j(X) \in F$ and S/H_j represents the set of H_j-orbits over S.

Since $F\hat{S} = \hat{S} + F\hat{S}$, we have that

$$F\hat{S} = f(\hat{S} + F\hat{S}) = f\Bigl(\sum_{j=1}^{r}\operatorname{Tr}_{G/H_j}(H_j + F\hat{S})\Bigr) = \sum_{j=1}^{r}\sum_{X\in S/H_j} a_j(X)\operatorname{Tr}_{G/H_j}(\hat{X}) + F\hat{S}.$$

If X is not a Weiss H_j-orbit, it follows from Proposition 8 that $\operatorname{Tr}_{G/H_j}(\hat{X}) = 0$. Therefore

$$\sum_{j=1}^{r}\sum_{X\in S/H_j} a_j(X)\operatorname{Tr}_{G/H_j}(\hat{X}) + F\hat{S} = \sum_{j=1}^{r}\sum_{X\in U} a_j(X)\operatorname{Tr}_{G/H_j}(\hat{X}) + F\hat{S},$$

where U is the set of Weiss H_j-orbits over S. Since X is an H_j-orbit over S, we have that for some $i \in [\![1, r]\!]$, $X = \{gg'H_i \mid g \in H_j\}$.

Since X is a Weiss H-orbit over S, it follows that there exists some $xg'H_i \in X$ such that $G_{xg'H_j} \subseteq H_j$. We have that $G_{xg'H_i} = H_i^{xg'}$. Therefore $H_i^{xg'} \subseteq H_j$. Hence, from condition $(*)$ it follows that $i = j$. Therefore $g' \in N_G(H_j)$. Thus $X = \{g'H_j\}$. Hence

$$\sum_{j=1}^{r}\sum_{g'\in N_G(H_j)} a_j\bigl(\{g'H_j\}\bigr)\operatorname{Tr}_{G/H_j}(g'H_j) \in F\hat{S}.$$

Since $\operatorname{Tr}_{G/H_j}(g'H_j) = \sum_{z\in G/H_j} zH_j$, it follows that

$$\sum_{j=1}^{r}\sum_{z\in G/H_j}\sum_{g'\in N_G(H_j)} a_j\bigl(\{g'H_j\}\bigr) zH_j \in F\hat{S}.$$

So,

$$\sum_{g'\in N_G(H_j)} a_j\bigl(\{g'H_j\}\bigr) = \sum_{g'\in N_G(H_t)} a_t\bigl(\{g'H_t\}\bigr) \quad \forall\, t, j \in [\![1, r]\!].$$

Thus, the element

$$a(f) := \sum_{g'\in N_G(H_j)} a_j\bigl(\{g'H_j\}\bigr)$$

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

is independent of j. Thus,

$$\hat{f}(v_j) = \pi\big(f(H_j + F\hat{S})\big) = \sum_{g' \in N_G(H_j)} a_j\big(\{g'H_j\}\big)\pi(g'H_j + F\hat{S}) = a(f)v_j.$$

So, $\hat{f}$ is the multiplication by the constant $a(f)$. Hence $A \cong \{a(f) \mid f \in \mathrm{End}_{F[G]}(B)\}$. Therefore A is a local ring. ■

PROPOSITION 10. *Let G be a finite p-group and M a p-torsion $\mathbb{Z}_p[G]$-module.*

(a) If ${}_pM$ is an indecomposable $\mathbb{F}_p[G]$-module, then M is an indecomposable $\mathbb{Z}_p[G]$-module.

(b) Let M be a p-divisible $\mathbb{Z}_p[G]$-module such that ${}_pM$ is an indecomposable $\mathbb{F}_p[G]$-module. Then $(R[G]^b, h)$ is the injective $\mathbb{Z}_p[G]$-envelope of M for some $b \in \mathbb{N}_0$, $\mathrm{coker}(h)$ does not have injective $\mathbb{Z}_p[G]$-components and $\Omega^{\#}(M)$ is an indecomposable $\mathbb{Z}_p[G]$-module.

PROOF. [9, Proposition 2.25]. ■

PROPOSITION 11. *With the conditions and notations in Proposition 5, let $H_i = G_i$. Then $\Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right)$ is an indecomposable $\mathbb{Z}_p[G]$-module. Furthermore, as $\mathbb{Z}_p[G]$-modules*

$$\Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right) \cong \frac{R[G]^{|A_2|-1+d_{G/\hat{H}}}}{\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}}$$

and as $\mathbb{Z}_p$-modules

$$\Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right) \cong R^a,$$

where $a = |G|d_{G/\hat{H}} + \sum_{i\in A_2}\left(|G| - \frac{|G|}{|G_i|}\right) + 1 - |G|$.

PROOF. From Proposition 5 follows the existence of a $\mathbb{Z}_p[G]$-monomorphism $f\colon M \longrightarrow T$, where $M := \frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}$ and $T := \frac{\bigoplus_{i=1}^{r} R[G/G_i]}{\mathrm{Re}^*}$.

From Proposition 1, it follows that $(R[G])^c$ is the injective $\mathbb{Z}_p[G]$-envelope of T, where $c = \dim_{\mathbb{F}_p}\big(({}_pT)^G\big)$. From [9, Proposition 1.11], we have that the injective $\mathbb{Z}_p[G]$-envelope of M is $(R[G]^t, \rho)$ for some $t \in \mathbb{N}_0$. As in the proof of Proposition 1, we have that $\mathrm{coker}(\rho)$ does not have injective $\mathbb{Z}_p[G]$-components. From Proposition 10 follows that $\Omega^{\#}(M)$ is an indecomposable $\mathbb{Z}_p[G]$-module. From Propositions 1, 2 and 4, follows that the $\mathbb{Z}_p[G]$-sequence

$$0 \longrightarrow M \longrightarrow R[G]^{|A_2|-1+d_{G/\hat{H}}} \longrightarrow \Omega^{\#}(M) \longrightarrow 0$$

is exact. Hence, $\Omega^{\#}(M) \cong \frac{R[G]^{|A_2|-1+d_{G/\hat{H}}}}{\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}}$. So, we obtain the $\mathbb{Z}_p[G]$-module structure of $\Omega^{\#}(M)$ and the value of a. ■

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

The first main result of this paper is the following

THEOREM 1. *Let L/K be a finite Galois p-extension of cyclotomic $\mathbb{Z}_p$-fields of* CM-*type with Galois group $G = \mathrm{Gal}(L/K)$, such that $\mu_K^- = 0$, $\mu_L^- = 0$. Let $P_1, \ldots, P_r$ be the ramified prime divisors in L/K with $G_1, \ldots, G_r$ their decomposition groups respectively. For each $i \in [\![1, r]\!]$ let $\hat{G}_i := \langle gG_ig^{-1} \mid g \in G\rangle$ be the normal closure of the subgroup G_i in G. We set $\hat{H} := \hat{G}_1 \cdots \hat{G}_r$ and $d_{G/\hat{H}}$ the minimum number of generators of the group $G/\hat{H}$. Let $C_L{}^-(p)$ be the minus part of the p-subgroup of the class group of L. Reordering the indices and taking conjugates, if necessary, let $1 \le i_1 < i_2 < \cdots < i_{s-1} < i_s = r$ such that*

$$\begin{gathered} G_1, \ldots, G_{i_1-1} \subseteq G_{i_1} \\ G_{i_1+1}, \ldots, G_{i_2-1} \subseteq G_{i_2} \\ \vdots \\ G_{i_{s-1}+1}, \ldots, G_{i_s-1} \subseteq G_{i_s} = G_r \end{gathered}$$

and that they satisfy the condition: If for $1 \le j, k \le s$, there exists some $g \in G$ such that $G_{i_j}^g = gG_{i_j}g^{-1} \subseteq G_{i_k}$, then $j = k$. Let $A_2 := \{i_1, i_2, \ldots, i_s\}$ and $A_1 := [\![1, r]\!] - A_2$. Then the modular decomposition of $C_L{}^-(p)$ in terms of indecomposable $\mathbb{Z}_p[G]$-modules is given by

$$C_L{}^-(p) \cong R[G]^{\lambda_K^- - d_{G/\hat{H}}} \bigoplus \bigoplus_{i \in A_1} \frac{R[G]}{R[G/G_i]} \bigoplus \Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right),$$

where $\mathrm{Re}^*_{A_2} = \{(\sum_{\sigma \in G/G_{i_1}} x\sigma, \ldots, \sum_{\sigma\in G/G_{i_s}} x\sigma) \in \oplus_{i\in A_2} R[G/G_i] \mid x \in R\}$.

As $\mathbb{Z}_p[G]$-modules we have that

$$W := \Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right) \cong \frac{R[G]^{|A_2|-1+d_{G/\hat{H}}}}{\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}};$$

W is an indecomposable $\mathbb{Z}_p[G]$-module and as $\mathbb{Z}_p$-module $W \cong R^a$, where $a = |G|d_{G/\hat{H}} + \sum_{i\in A_2}\left(|G| - \frac{|G|}{|G_i|}\right) + 1 - |G|$.

PROOF. From (1) we have that

$$C_L{}^-(p) \cong C_L{}^-(p)^{(0)} \oplus C_L{}^-(p)^{(1)} \cong R[G]^u \oplus \Omega^{\#}(T).$$

From Proposition 2 it follows that

$$C_L{}^-(p)^{(0)} \cong R[G]^{r-1-c+\lambda_K^-},$$

where $c = \dim_{\mathbb{F}_p}\left(({}_pT)^G\right)$. From Proposition 4 we obtain that

$$\dim_{\mathbb{F}_p}\left(({}_pT)^G\right) = \dim_{\mathbb{F}_p}\left(({}_pT_r)^G\right) = r - 1 + d_{G/\hat{H}}.$$

If C is a subgroup of G in [18, Proposition 4] is shown that as $\mathbb{Z}_p[G]$-modules $\Omega^{\#}(R[G/C]) \cong \frac{R[G]}{R[G/C]}$. Moreover, the $\mathbb{Z}_p[G]$-modules $R[G/C]$ and $\frac{R[G]}{R[G/C]}$ are indecomposable $\mathbb{Z}_p[G]$-modules. Therefore,

$$\bigoplus_{i\in A_1} \Omega^{\#}(R[G/G_i]) \cong \bigoplus_{i\in A_1} \frac{R[G]}{R[G/G_i]}.$$

Hence, from Proposition 5 we obtain that the modular decomposition of $C_L{}^{-}(p)^{(1)}$ is given by

$$C_L{}^{-}(p)^{(1)} \cong \Omega^{\#}(T) \cong \bigoplus_{i\in A_1} \frac{R[G]}{R[G/G_i]} \oplus W.$$

Finally, from Proposition 11 we obtain that W is an indecomposable $\mathbb{Z}_p[G]$-module, as well as we obtain its $\mathbb{Z}_p$-module structure. ∎

4. **Jacobian variety.** For a function field L over k, in addition to the notation introduced earlier, we denote by $\mathbb{P}_L$ and D_{0L}, respectively, the group of principal divisors and the group of divisors of degree 0. The p-subgroup $C_{0,L}(p)$ of the group of divisor classes of degree 0 in L has structure of $\mathbb{Z}_p$-module with action given by $(\sum_{i=0}^{\infty} a_i p^i)(\mathcal{O}P_L) = \mathcal{O}^a P_L$, where $a = \sum_{i=0}^{n_0} a_i p^i$ and $n_0 \in \mathbb{N}$ satisfies $\mathcal{O}^{p^m} \in P_L\ \forall\, m \geq n_0$. Let G be a finite subgroup of $\mathrm{Aut}_K(L)$. Then $C_{0,L}(p)$ has structure of G-module with the action of G on $C_{0,L}(p)$ given by $\sigma(\mathcal{O}P_L) = \mathcal{O}^{\sigma} P_L$, $\sigma \in G$. Therefore $C_{0,L}(p)$ has the structure of $\mathbb{Z}_p[G]$-module.

A formal product $\mathcal{M} = \prod_{P\in\mathbb{P}_L} P^{n_{\mathcal{M}}(P)}$ where $n_{\mathcal{M}}(P) \in \mathbb{N}_0$ and $n_{\mathcal{M}}(P) = 0$, except for a finite number of prime divisors of L, will be called *a modulus over L*. We will denote by $D_{0L,\mathcal{M}}$ the group of divisors of L of degree zero relatively prime to $\mathcal{M}$, $P_{L,\mathcal{M}}$ will denote the group of principal divisors (α) such that $\alpha \equiv 1 \bmod \mathcal{M}$ and $C_{0L,\mathcal{M}} := \frac{D_{0L,\mathcal{M}}}{P_{L,\mathcal{M}}}$ will denote the group of classes of degree zero associated to the modulus $\mathcal{M}$.

For any modulus $\mathcal{M}$ over L we have a commutative algebraic group, denoted by $J_{L,\mathcal{M}}$ called the *generalized Jacobian of L corresponding to the modulus $\mathcal{M}$* (for the definition and results about Jacobians we refer to Serre [14]). As groups we have $C_{0L,\mathcal{M}} \cong J_{L,\mathcal{M}}$ [14, Theorem 1, p. 88]. For $\mathcal{M} = \eta$, where η is the unit divisor of L we have that $J_{L,\eta} = J_L$, where J_L is the Jacobian variety associated to the function field L [14, p. 90].

Let $\mathcal{M}$ and $\mathcal{M}'$ be modulii over L. We say that $\mathcal{M}'$ divides $\mathcal{M}$, denoted by $\mathcal{M}' \mid \mathcal{M}$, if we have that $n_{\mathcal{M}}(P) \geq n_{\mathcal{M}'}(P)\ \forall P \in \mathbb{P}_L$. Let $\mathcal{M}$, $\mathcal{M}'$ be modulii over L such that $\mathcal{M}' \mid \mathcal{M}$. Then there exists a unique epimorphism $\varphi\colon J_{L,\mathcal{M}} \longrightarrow J_{L,\mathcal{M}'}$ such that $H_{\mathcal{M}'|\mathcal{M}} := \ker(\varphi)$ is a connected subgroup of $J_{L,\mathcal{M}}$ [14, Proposition 6, p. 91]. We set $\tau_{L,\mathcal{M}} := \dim_{\mathbb{F}_p}\big({}_pJ_{L,\mathcal{M}}(p)\big)$. The number $\tau_{L,\mathcal{M}}$ is the *p-rank of the generalized Jacobian* $J_{L,\mathcal{M}}$ and $\tau_L^{\cdot} = \dim_{\mathbb{F}_p}\big({}_pJ_L(p)\big)$, the *$p$-rank of the Jacobian variety* associated to L/k, is called the Hasse-Witt invariant of L.

We will denote by p an arbitrary rational prime number. Let L/K be a finite Galois p-extension of algebraic function fields of one variable with Galois group $G = \mathrm{Gal}(L/K)$ and field of constants k, an algebraically closed field of characteristic p. Let

$$S := \{P_1, P_2, \ldots, P_r\}, \quad \hat{S} := \left\{Q_t^{(i)} \mid i \in [\![1, r]\!], t \in [\![1, p^{s_i}]\!]\right\}, \tag{6}$$

where S is the set consisting of the prime divisors P_i of K which are ramified in L, $\hat{S}$ is the set consisting of the prime divisors $Q_t^{(i)}$ of L such that the $Q_t^{(i)}$ are the divisors in L above P_i and p^{s_i} is the decomposition number of the prime divisor P_i. If $Q_t^{(i)} \in \hat{S}$ we define $G_t^{(i)} := \{\sigma \in G \mid Q_t^{(i)\sigma} = Q_t^{(i)}\} = \mathrm{Dec}(Q_t^{(i)} \mid P_i)$, the decomposition group of the prime divisor $Q_t^{(i)}$. We have that if $Q_{t'}^{(i)}$ is any other prime divisor of L dividing the prime divisor P_i, then the groups $G_{t'}^{(i)}$ and $G_t^{(i)}$ are conjugate. It follows that as $\mathbb{Z}_p[G]$-modules $R[G/G_t^{(i)}] \cong R[G/G_{t'}^{(i)}]$. If $t \in [\![1, p^{s_i}]\!]$, we choose G_i, one representative in the conjugacy class of $G_t^{(i)}$ and we define $Q_i := Q_t^{(i)}$; so $G_i := \{\sigma \in G \mid Q_i^\sigma = Q_i\} = \mathrm{Dec}(Q_i \mid P_i)$. We define the following modulii over L and over K

$$\mathcal{N} := \prod_{Q\in\hat{S}} Q, \quad \mathcal{M} := \prod_{P\in S} P \tag{7}$$

where $S, \hat{S}$ are the sets given in (6). Let $J_{L,\mathcal{N}}$, $J_{K,\mathcal{M}}$ be the generalized Jacobians of L and of K associated to the modulus $\mathcal{N}$ and $\mathcal{M}$, respectively.

Since k is an algebraically closed field, we have that the inertia degree f_Q of every prime divisor Q of L and of K is 1. It follows that the degree of the modulus $\mathcal{N}$ is $\deg(\mathcal{N}) = \sum_{i=1}^r p^{s_i} = \sum_{i=1}^r \frac{|G|}{|G_i|}$. We also have $\deg(\mathcal{M}) = r$.

PROPOSITION 12. *Let L/K be a finite Galois p-extension of algebraic function fields of one variable with field of constants k, an algebraically closed field of characteristic p and Galois group $G = \mathrm{Gal}(L/K)$. Let S, $\hat{S}$ be the sets of primes given in* (6) *and $G_1, \ldots, G_r$ the decomposition groups of the prime divisors of L that divide the ramified prime divisors of K given in* (4). *Let*

$$\mathcal{N} := \prod_{Q\in\hat{S}} Q, \quad \mathcal{M} := \prod_{P\in S} P \tag{8}$$

and $J_{L,\mathcal{N}}$, $J_{K,\mathcal{M}}$ be the respective generalized Jacobians. Let $J_L(p)$ be the p-torsion part of the Jacobian variety associated to L/k. Then

(a) ${}_pJ_{L,\mathcal{N}}(p)$ *is a free* $\mathbb{F}_p[G]$*-module. Moreover* ${}_pJ_{L,\mathcal{N}}(p) \cong \mathbb{F}_p[G]^{r-1+\tau_K}$.

(b) $\dim_{\mathbb{F}_p}\left({}_p\big(J_{L,\mathcal{N}}(p)^G\big)\right) = r - 1 + \tau_K$.

(c) *There exists a* $\mathbb{Z}_p[G]$*-exact sequence* $0 \longrightarrow H_{\eta/\mathcal{N}}(p) \longrightarrow J_{L,\mathcal{N}}(p) \longrightarrow J_L(p) \longrightarrow 0$.

(d) *As* $\mathbb{Z}_p[G]$*-modules* $H_{\eta/\mathcal{N}}(p) \cong \frac{\bigoplus_{i=1}^r R[G/G_i]}{\mathrm{Re}^*}$, *and* $H_{\eta/\mathcal{N}}(p) \cong R^{\deg(\mathcal{N})-1}$ *as* $\mathbb{Z}_p$*-modules.*

(e) $\dim_{\mathbb{F}_p}\left({}_pJ_{K,\mathcal{M}}(p)\right) \geq \dim_{\mathbb{F}_p}\left({}_p\big(J_{L,\mathcal{N}}(p)\big)^G\right)$.

(f) $J_{L,\mathcal{N}}(p) \cong R[G]^{r-1+\tau_K}$.

(g) *There exists a* $\mathbb{Z}_p[G]$*-exact sequence*

$$0 \longrightarrow \frac{\bigoplus_{i=1}^r R[G/G_i]}{\mathrm{Re}^*} \longrightarrow R[G]^{r-1+\tau_K} \longrightarrow J_L(p) \longrightarrow 0, \tag{9}$$

and for some $\nu \in \mathbb{N}_0$,

$$J_L(p) \cong J_L(p)^{(0)} \oplus J_L(p)^{(1)} \cong R[G]^\nu \oplus \Omega^\#\left(\frac{\bigoplus_{i=1}^r R[G/G_i]}{\mathrm{Re}^*}\right) = R[G]^\nu \oplus \Omega^\#(\mathbf{T}), \tag{10}$$

where $\mathbf{T} := \frac{\bigoplus_{i=1}^{r} R[G/G_i]}{Re^*}$.

PROOF. (a) It follows using the Deuring-Šafarevič formula and proceeding as in [17, Proposition 8].

(b) In general we have that if M is a $\mathbb{Z}_p[G]$-module then, as $\mathbb{Z}_p[G]$-modules $({}_pM)^G \cong {}_p(M^G)$. From (a) it follows that as $\mathbb{F}_p[G]$-modules $\big({}_pJ_{L,N}(p)\big)^G \cong \mathbb{F}_p^{r-1+\tau_K}$. Therefore $\dim_{\mathbb{F}_p}\Big({}_p\big(J_{L,N}(p)^G\big)\Big) = \dim_{\mathbb{F}_p}\Big(\big({}_pJ_{L,N}(p)\big)^G\Big) = r-1+\tau_K$.

(c) From [14, Proposition 6, p. 91] applied to the modulus N, η over L follows the existence of a unique epimorphism $\varphi: J_{L,N} \longrightarrow J_{L,\eta}$ such that $H_{\eta|N} := \ker(\varphi)$ is a connected subgroup of $J_{L,N}$. Therefore there exists an exact sequence of groups

$$0 \longrightarrow H_{\eta|N} \longrightarrow J_{L,N} \xrightarrow{\varphi} J_L \longrightarrow 0. \tag{11}$$

Since the torsion of $H_{\eta|N}$ is p^n-divisible for all $n \in \mathbb{N}$, we have that there exists a $\mathbb{Z}_p[G]$-exact sequence

$$0 \longrightarrow {}_{p^n}H_{\eta|N} \longrightarrow {}_{p^n}J_{L,N} \longrightarrow {}_{p^n}J_L \longrightarrow 0. \tag{12}$$

In general, if A is an abelian group we have that $A(p) \cong \varinjlim {}_{p^m}A \cong \bigcup_{m=1}^{\infty} {}_{p^m}A$. Therefore, from (12), we obtain the $\mathbb{Z}_p$-exact sequence

$$0 \longrightarrow H_{\eta|N}(p) \longrightarrow J_{L,N}(p) \longrightarrow J_L(p) \longrightarrow 0. \tag{13}$$

Moreover, since G acts in a natural way on these modules, we have that (13) is a $\mathbb{Z}_p[G]$-exact sequence.

(d) [18, p. 267].

(e) From [18, Proposition 9], we have that the conorm map $\phi: J_{K,M}(p) \longrightarrow \big(J_{L,N}(p)\big)^G$ is surjective. Therefore,

$$\tau_{K,M} = \dim_{\mathbb{F}_p}\Big({}_p\big(J_{K,M}(p)\big)\Big) \geq \dim_{\mathbb{F}_p}\Big({}_p\big(J_{L,N}(p)\big)^G\Big).$$

(f) From (e), we obtain that

$$\dim_{\mathbb{F}_p}\Big({}_p\big(J_{K,M}(p)\big) = \tau_{K,M} = r-1+\tau_K \geq \dim_{\mathbb{F}_p}\Big({}_p\big(J_{L,N}(p)\big)^G\Big).$$

Now, we have that $\tau_{L,N} = \dim_{\mathbb{F}_p}\big({}_pJ_{L,N}(p)\big) = \tau_L + \sum_{i=1}^{r}\frac{|G|}{|G_i|} - 1$. Therefore, from the Deuring-Šafarevič formula, we obtain that $\tau_{L,N} = |G|(r-1+\tau_K) = |G|\tau_{K,M}$. It follows that $\dim_{\mathbb{F}_p}\big({}_pJ_{L,N}(p)\big) \geq |G| \dim_{\mathbb{F}_p}\Big({}_p\big(J_{L,N}(p)\big)^G\Big)$. From Kato's Lemma [10, Proposition 2], we obtain that ${}_pJ_{L,N}(p) \cong \mathbb{F}_p[G]^{r-1+\tau_K}$. Finally, as in [18, Theorem 9] we obtain that as $\mathbb{Z}_p[G]$-modules $J_{L,N}(p) \cong R[G]^{r-1+\tau_K}$.

(g) It follows from (d), (f) and (13).

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

The sequence (9) is similar to the $\mathbb{Z}_p[G]$-exact sequence in [18, Theorem 4] for number fields, so the $\mathbb{Z}_p[G]$-exact sequence (9) determines uniquely the $\mathbb{Z}_p[G]$-module structure of $J_L(p)$. Similarly, as in [18, Theorem 2], we have that for some $v \in \mathbb{N}_0$

$$J_L(p) \cong R[G]^v \bigoplus \Omega^\# \left(\frac{\bigoplus_{i=1}^{r} R[G/G_i]}{\mathrm{Re}^*} \right). \tag{14}$$ ∎

The expression (14) gives us implicitly the structure of $J_L(p)$ as $\mathbb{Z}_p[G]$-module.

As analogous to Propositions 1, 2 and 4, we have that $R[G]^c$ is the injective $\mathbb{Z}_p[G]$-envelope of $\mathbf{T}$, where c is the minimum natural number such that there exists a $\mathbb{Z}_p[G]$-monomorphism $\phi\colon \mathbf{T} \longrightarrow R[G]^c$ and there exists an $\mathbb{Z}_p[G]$-exact sequence $0 \longrightarrow \mathbf{T} \longrightarrow R[G]^c \longrightarrow \Omega^\#(\mathbf{T}) \longrightarrow 0$.

For each $i \in [\![1, r]\!]$, let $\hat{G}_i := \langle gG_ig^{-1} \mid g \in G \rangle$ be the normal closure of the subgroup G_i in G and let $d_{G/\hat{G}_i}$ be the minimum number of generators of the group $G/\hat{G}_i$. We set $\hat{H} := \hat{G}_1 \cdots \hat{G}_r$. We have that $J_L(p)^{(0)} \cong R[G]^v$ for some $v \in \mathbb{N}_0$. Moreover $v = r - 1 - c + \tau_K$ and $c = \dim_{\mathbb{F}_p}\big(({}_p\mathbf{T})^G\big) = r - 1 + d_{G/\hat{H}}$ where $d_{G/\hat{H}}$ is the minimum number of generators of the group $G/\hat{H}$.

In (14), from Proposition 5 it follows that

$$\Omega^\# \left(\frac{\bigoplus_{i=1}^{r} R[G/G_i]}{\mathrm{Re}^*} \right) \cong \bigoplus_{i \in A_1} \frac{R[G]}{R[G/G_i]} \bigoplus \Omega^\# \left(\frac{\bigoplus_{i \in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}} \right).$$

From Proposition 11 we have that the indecomposable $\mathbb{Z}_p[G]$-module

$$\Omega^\# \left(\frac{\bigoplus_{i \in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}} \right) \cong \frac{R[G]^{|A_2|-1+d_{G/\hat{H}}}}{\frac{\bigoplus_{i \in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}}$$

and $W \cong R^a$ as $\mathbb{Z}_p$-modules, where $a = |G|d_{G/\hat{H}} + \sum_{i \in A_2} \left(|G| - \frac{|G|}{|G_i|} \right) + 1 - |G|$.

As the second main result of this paper, we obtain unconditionally and explicitly, the Galois module structure of $J_L(p)$.

THEOREM 2. *Let L/K be a finite Galois p-extension of algebraic function fields of one variable with field of constants k, an algebraically closed field of characteristic p and, let $G = \mathrm{Gal}(L/K)$. Let $P_1, \ldots, P_r$ be the ramified prime divisors in L/K with $G_1, \ldots, G_r$ their decomposition groups respectively and let $J_L(p)$ be the p-torsion part of the Jacobian variety associated to L/k. For each $i \in [\![1, r]\!]$, let $\hat{G}_i := \langle gG_ig^{-1} \mid g \in G \rangle$ be the normal closure of the subgroup G_i in G and let $d_{G/\hat{G}_i}$ be the minimum number of generators of the group $G/\hat{G}_i$. Let $\hat{H} := \hat{G}_1 \cdots \hat{G}_r$ and $d_{G/\hat{H}}$ be the minimum number of* *generators of the group $G/\hat{H}$. Reordering the indices and taking conjugates, if necessary, let $1 \le i_1 < i_2 < \cdots < i_{s-1} < i_s = r$ such that*

$$\begin{gathered} G_1, \ldots, G_{i_1-1} \subseteq G_{i_1} \\ G_{i_1+1}, \ldots, G_{i_2-1} \subseteq G_{i_2} \\ \vdots \\ G_{i_{s-1}+1}, \ldots, G_{i_s-1} \subseteq G_{i_s} = G_r \end{gathered}$$

and that they satisfy the condition: If for $1 \le j, k \le s$, there exists some $g \in G$ such that $G_{i_j}^g = gG_{i_j}g^{-1} \subseteq G_{i_k}$, then $j = k$. Let $A_2 := \{i_1, i_2, \ldots, i_s\}$ and $A_1 := [\![1, r]\!] - A_2$. Then the modular decomposition, in terms of indecomposable $\mathbb{Z}_p[G]$-modules of $J_L(p)$, is given by

$$J_L(p) \cong R[G]^{r_K} - d_{G/\hat{H}} \bigoplus \bigoplus_{i\in A_1} \frac{R[G]}{R[G/G_i]} \bigoplus \Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right),$$

where

$$\mathrm{Re}^*_{A_2} = \Big\{ \big(\sum_{\sigma\in G/G_{i_1}} x\sigma, \ldots, \sum_{\sigma\in G/G_{i_s}} x\sigma \big) \in \bigoplus_{i\in A_2} R[G/G_i] \mid x \in R \Big\}.$$

As $\mathbb{Z}_p[G]$-module we have that

$$W := \Omega^{\#}\left(\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}\right) \cong \frac{R[G]^{|A_2|-1+d_{G/\hat{H}}}}{\frac{\bigoplus_{i\in A_2} R[G/G_i]}{\mathrm{Re}^*_{A_2}}},$$

and W is an indecomposable $\mathbb{Z}_p[G]$-module and, as $\mathbb{Z}_p$-module, $W \cong R^a$ where $a = |G|d_{G/\hat{H}} + \sum_{i\in A_2} \left(|G| - \frac{|G|}{|G_i|}\right) + 1 - |G|$.

PROOF. Analogous to that of Theorem 1. ∎

From Theorem 1 and Theorem 2, we see that the Galois module structure of the p-torsion part of the Jacobian variety of an algebraic function field of one variable is analogous to that of the minus part of the p-class group of a cyclotomic $\mathbb{Z}_p$-extension of CM-type.

REFERENCES

1. F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*. Graduate Texts in Math. **13**, Springer-Verlag, Berlin-Heidelberg-New York, 1974.
2. C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys **6**, Amer. Math. Soc., 1951.
3. C. W. Curtis and I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders, Vol. I*. Pure and Appl. Math., Wiley-Interscience, New York, 1981.
4. R. Gold and M. Madan *Galois representation of Iwasawa modules*. Acta Arith. **46**(1986), 243–255.
5. K. Iwasawa, *On Γ-extensions of Algebraic Number Fields*. Bull. Amer. Math. Soc. **65**(1959), 183–226.
6. ———, *On $\mathbb{Z}_\ell$-extensions of Algebraic Number Fields*. Ann. of Math. **98**(1973), 246–326.

https://doi.org/10.4153/CJM-1998-061-8 Published online by Cambridge University Press

7. ______, *Riemann-Hurwitz Formula and p-adic Galois Representation for Number Fields*. Tôhoku Math. J. **33**(1981), 263–288.
8. G. Karpilovsky, *Group Representations, Vol. I*. North-Holland Mathematics Studies **175**, North-Holland, Amsterdam-London-New York-Tokyo, 1992.
9. R. López, *Ph.D. Dissertation*. Centro de Investigación y de Estudios Avanzados del I.P.N., February, 1998.
10. S. Nakajima, *Equivariant Form of the Deuring-Šafarevič Formula for Hasse-Witt Invariants*. Math. Z. **190**(1985), 559–566.
11. M. Rzedowski, G. Villa and M. Madan, *Galois module structure of Tate modules*. Math. Z. **224**(1997), 77–101.
12. Sudarshan K. Sehgal, *Topics in Group Rings*. Pure and Appl. Math. **50**, Marcel Dekker, Inc., New York, 1978.
13. J. P. Serre, *Local Fields*, Graduate Texts in Math. **67**, Springer-Verlag, New York, 1979.
14. ______, *Algebraic Groups and Class Fields*. Graduate Texts in Math. **117**, Springer-Verlag, Berlin-Heidelberg-New York, 1988.
15. M. Suzuki, *Group Theory I*. Grundlehren Math. Wiss. **247**, Springer-Verlag, Berlin-Heidelberg-New York, 1980.
16. R. Valentini, *Some p-adic Galois Representations for Curves in Characteristic p*. Math. Z. **192**(1986), 541–545.
17. G. Villa and M. Madan, *Structure of Semisimple Differentials and p-Class Groups in* $\mathbb{Z}_p$*-extensions*. Manuscripta Math. **57**(1987), 315–350.
18. ______, *Integral representations of p-class groups in* $\mathbb{Z}_p$*-extensions, semisimple differentials and Jacobians*. Arch. Math. **56**(1991), 254–269.

Departamento de Ciencias Básicas
Universidad Autónoma Metropolitana-Azcapotzalco
Av. San Pablo No. 180, Col. Reynosa Tamaulipas
Azcapotzalco D.F., C.P. 02200 México
email: rlopez@hp9000a1.uam.mx

Departamento de Matemáticas
Centro de Investigación y de Estudios Avanzados
del I.P.N.
Apartado Postal 14-740, 07000 México, D.F.
email: villa@math.cinvestav.mx