ISRAEL JOURNAL OF MATHEMATICS **144** (2004), 61–92

FINITE MODULES OVER NON-SEMISIMPLE GROUP RINGS

BY

Cristian D. Gonzalez-Aviles[*]

Av. Chile-España 210, Apt. 404, Ñuñoa, Santiago, Chile
gonzomat2002@yahoo.es

ABSTRACT

Let G be an abelian group of order n and let R be a commutative ring which admits a homomorphism $\mathbb{Z}[\zeta_n] \to R$, where ζ_n is a (complex) primitive n-th root of unity. Given a finite $R[G]$-module M, we derive a formula relating the order of M to the product of the orders of the various isotypic components M^χ of M, where χ ranges over the group of R-valued characters of G. For G cyclic, we give conditions under which the order of M is exactly equal to the product of the orders of the M^χ. To derive these conditions, we build on work of Aljadeff and Ginosar and obtain, in particular, a new criterion for cohomological triviality which improves upon the well-known criterion of T. Nakayama. We also give applications to abelian varieties and to ideal class groups of number fields, obtaining in particular some new class number relations. In an Appendix to the paper, we use étale cohomology to obtain some additional class number relations. Our results also have applications to "non-semisimple" Iwasawa theory, but we do not develop these here. In general, the results of this paper could be used to strengthen a variety of known results involving finite $R[G]$-modules whose hypotheses include (an equivalent form of) the following assumption: "the order of G is invertible in R".

0. Introduction

Let A be an abelian variety defined over a global field F and let K/F be a quadratic extension with Galois group G. Write A^{t} for the abelian variety dual to A. For each of the two characters χ of G, let A^χ (resp. $(A^{\mathrm{t}})^\chi$) be the twist of A (resp. A^{t}) by χ. In [8] the following result was established.

[*] Supported by Fondecyt grant 1000814.
Received May 2, 2002 and in revised form October 10, 2003

THEOREM 0.1 ([8, Corollary 4.6]): *With the above notations, assume that the following conditions hold.*

(i) *The Tate–Shafarevich group $Ш(A_K)$ of A_K is finite.*

(ii) $\widehat{H}^i(G, A^\chi(K)) = \widehat{H}^i(G, (A^{\mathrm{t}})^\chi(K)) = 0$ *for all integers i and all characters χ of G.*

(iii) *Both $A(F_v)$ and $A^{\mathrm{t}}(F_v)$ are connected for all real primes v of F.*

Then

$$[Ш(A_K)] = [Ш(A_F)][Ш(A_F^\chi)] \cdot \prod_{v \in T} [H^1(G_w, A(K_w))],$$

where T is the set of primes of F which ramify in K/F or where A_F has bad reduction, w is a fixed prime of K lying above v (for each $v \in T$), and $G_w = \mathrm{Gal}(K_w/F_v)$.

In attempting to generalize the above theorem to extensions of degree greater than 2, we were led to the following general problem. Given a finite abelian group G and a finite $R[G]$-module M (where R is a commutative ring which contains the values of all characters of G, e.g. $R = \mathbb{Z}[\zeta_n]$, where ζ_n is a complex n-th root of unity), find a formula for the order of M in terms of the orders of the various isotypic components M^χ of M, where χ runs over the group of characters $\widehat{G}$ of G and $M^\chi = \{m \in M \colon \sigma m = \chi(\sigma)m \text{ for all } \sigma \in G\}$. If n denotes the order of G and one considers $R_* = \mathbb{Z}[1/n] \otimes_{\mathbb{Z}} R$, then it is easy to find a formula of the desired type for the order of $M_* = \mathbb{Z}[1/n] \otimes_{\mathbb{Z}} M$ (which we regard as an $R_*[G]$-module in the natural way), since there is an isomorphism

$$M_* \simeq \bigoplus_\chi M_*^\chi = \bigoplus_\chi \varepsilon'_\chi M_*,$$

where $\varepsilon'_\chi = (1/n) \otimes \sum_{\sigma \in G} \overline{\chi}(\sigma)\sigma$ is the idempotent of the group ring $R_*[G]$ corresponding to $\chi \in \widehat{G}$ (here $\overline{\chi}$ denotes the inverse of χ). However, if for example $nM = 0$, then $M_* = 0$ and no information is gained on the order of M. A different approach involves the "quasi-idempotents"

$$\varepsilon_\chi = \sum_{\sigma \in G} \overline{\chi}(\sigma)\sigma \in R[G],$$

which satisfy $\varepsilon_\chi^2 = n\varepsilon_\chi$. Since $\varepsilon_\chi M$ no longer equals M^χ, it is natural to expect that the modules $M^\chi/\varepsilon_\chi M$ will play a role in our considerations. For $\chi = \chi^0$ (the trivial character of G), $M^\chi/\varepsilon_\chi M$ is the familiar Tate cohomology module $M^G/N_G M = \widehat{H}^0(G, M)$, where $N_G = \sum_{\sigma \in G} \sigma$ is the norm element of $R[G]$. In general, $\widehat{H}^0_\chi(G, M) \overset{\mathrm{def}}{=} M^\chi/\varepsilon_\chi M = \widehat{H}^0(G, M_{\overline{\chi}})$, where $M_{\overline{\chi}}$ is the $\overline{\chi}$-twist of M

(see Section 1 for definitions). Then the solution to the general problem stated abo ve is given by

THEOREM 0.2: *If G is cyclic and M is a finite $R[G]$-module, then*

$$[M]\cdot\prod_{\chi\in\widehat{G}}[\widehat{H}^0_\chi(G,M)/S_\chi(M)]=\prod_{\chi\in\widehat{G}}[M^\chi],$$

where $S_\chi(M)$ ($\chi\in\widehat{G}$) is the submodule of $\widehat{H}^0_\chi(G,M)$ defined in Section 2, formula (6). Equivalently,

$$[M]=\prod_{\chi\in\widehat{G}}[\varepsilon_\chi M]\cdot\prod_{\chi\in\widehat{G}}[S_\chi(M)].$$

(Analogous formulas exist for any finite abelian group G. See Theorem 3.1.)

If M is n-divisible, i.e., has no n-torsion, then the modules $\widehat{H}^0_\chi(G,M)$, and therefore also the modules $S_\chi(M)$, vanish. In this case the formulas of the theorem read

$$[M]=\prod_{\chi\in\widehat{G}}[M^\chi]=\prod_{\chi\in\widehat{G}}[\varepsilon_\chi M]. \tag{1}$$

However, w e could have obtained these formulas using the arguments given before the statement of the theorem. The interest of Theorem 0.2 is that there may exist other instances (besides that in which M is n-divisible) where the modules $\widehat{H}^0_\chi(G,M)=\widehat{H}^0(G,M_{\overline{\chi}})$ vanish, and therefore (1) holds. Regarding the vanishing of $\widehat{H}^0(G,M)$ for an arbitrary G-module M, w e use in Section 4 the impressive results of E. Aljadeff and Y. Ginosar [1], [2] to establish the follo wing theorem.

THEOREM 0.3: *Let G be a finite group such that all Sylow subgroups of G are cyclic*[1] *and let M be a finite G-module. Suppose that $\widehat{H}^0(H,M)=0$ for all subgroups H of G of* **prime** *order. Then $\widehat{H}^0(H,M)=0$ for all subgroups H of G.*

The above theorem is in fact a corollary of the following striking criterion for cohomological triviality.

THEOREM 0.4: *Let G be a finite group and let M be a G-module. Then M is cohomologically trivial if and only if $\widehat{H}^{i_p}(H,M)=\widehat{H}^{i_p+1}(H,M)=0$ for every p-elementary abelian subgroup H of G, where i_p is an integer (which may*

[1] See Section 4 for a description of these groups.

depend on p). In particular, if every Sylow subgroup of G is either cyclic or is a generalized quaternion group[2]*, then M is cohomologically trivial if and only if $\widehat{H}^{-1}(H,M)=\widehat{H}^{0}(H,M)=0$ for all subgroups H of G of prime order.*

(We remind the reader that a G-module M is said to be **cohomologically trivial** if $\widehat{H}^{i}(H,M)=0$ for all integers i and all subgroups H of G.)

The above theorem is a significant improvement of the well-known criterion for cohomological triviality established by T. Nakayama in the mid 1950's (see [23, Theorem IX.5.8 (i)⇔(ii), p. 145]; see also the remarks following the statement of Corollary 4.4 below).

Using the above criterion, we obtain results of the following type.

Theorem 0.5: *Let G be a cyclic group of order n and let M be a finite $R[G]$-module, where $R=\mathbb{Z}[\zeta_n]$. Assume that $\widehat{H}^{0}_{\chi}(H,M)=0$ for every subgroup H of G of prime order and every character χ of H. Then $\widehat{H}^{0}_{\psi}(G,M)=0$ for all characters ψ of G and*

$$[M]=\prod_{\psi\in\widehat{G}}[M^{\psi}]=\prod_{\psi\in\widehat{G}}[\varepsilon_{\psi}M].$$

If G is a cyclic 2-group and M is a G-module, set $M^{+}=\{m\in M\colon \tau m=m\}$, where τ is the unique element of order 2 in G.

Corollary 0.6: *Let G be a cyclic group of order 2^n, where $n\geq 1$, and let M be a finite $R[G]$-module, where $R=\mathbb{Z}[\zeta_{2^n}]$. Assume that $M^{+}=(1+\tau)M$. Then*

$$[M]=\prod_{\chi\in\widehat{G}}[M^{\chi}]=\prod_{\chi\in\widehat{G}}[\varepsilon_{\chi}M].$$

In Section 5 we apply the results of the preceding sections to Tate–Shafarevich groups of abelian varieties. The main result obtained is the following generalization of Theorem 0.1.

Theorem 0.7: *Let K/F be a cyclic Galois extension of global fields with Galois group G of order n and let A be an abelian variety defined over F with complex multiplication by $\mathbb{Z}[\zeta_n]$. Assume that the following conditions hold.*

(i) *The Tate–Shafarevich group $\text{Ш}(A_K)$ of A_K is finite.*

(ii) *$\widehat{H}^{i}_{\chi}(G,A(K))=\widehat{H}^{i}_{\chi}(G,A^{\mathrm{t}}(K))=0$ for all i and all $\chi\in\widehat{G}$.*

(iii) *$A(F_v)$ is connected for all real primes v of F.*

[2] Such groups G have the property that every abelian subgroup of G is cyclic. See [3, Theorem XII.11.6, p. 262].

Then

$$[\text{Ш}(A_K)] = \prod_{\chi\in\widehat{G}} [\text{Ш}(A_F^{\chi})] \cdot \prod_{\chi\in\widehat{G}} [S_\chi(\text{Ш}(A_K))],$$

where, for each $\chi \in \widehat{G}$, $S_\chi(\text{Ш}(A_K))$ is the submodule of $\widehat{H}^0_\chi(G, \text{Ш}(A_K))$ defined in Section 2, formula (6). Further, for each $\chi \in \widehat{G}$, $[S_\chi(\text{Ш}(A_K))]$ divides

$$\prod_{v\in T_{\overline{\chi}}} [\widehat{H}^0_{\chi_w}(G_w, A(K_w))],$$

where $T_{\overline{\chi}}$ and χ_w are as in the statement of Corollary 5.6 below.

In Section 6 we apply the results of the preceding Sections to study ideal class groups of number fields. The following results are obtained.

For any number field F and any finite Galois extension K of F with Galois group G and unit group U_K, we write $\text{Ш}^i(G, U_K)$ (resp. $\text{b}^i(G, U_K)$) for the kernel (resp. cokernel) of the map $H^i(G, U_K) \to \prod_v H^i(G_w, U_w)$, where, for each prime v of F, w denotes a fixed prime of K lying above v and G_w is the decomposition group of w in G. Further, we write C_K and h_K for the ideal class group and ideal class number of K, respectively. Similar notations apply to F.

Theorem 0.8: *Let K/F be a finite Galois extension of number fields with Galois group G of exponent e. Then there exists a rational number r, whose numerator and denominator are divisible only by primes that divide e, such that*

$$[C_K^G] = r \cdot h_F.$$

In particular, a prime $p \nmid e$ divides $[C_K^G]$ if and only if it divides h_F.

Theorem 0.9: *Let K/F be a finite Galois extension of number fields with Galois group G such that all Sylow subgroups of G are either cyclic or generalized quaternion. Assume, in addition, that the following conditions hold for each subextension L/F of K/F of prime index.*

(a) *K/L is ramified at some prime, and*

(b) $\text{b}^1(H, U_K) = \text{Ш}^2(H, U_K) = 0$, *where* $H = \text{Gal}(K/L)$.

Then the G-module C_K is cohomologically trivial.

Theorem 0.10: *Let K/F be a finite Galois extension of exponent 2. Then there exists an integer t such that*

$$h_K/h_F = 2^t \cdot \prod_{\chi\neq\chi^0} [\varepsilon_\chi C_K],$$

where C_K is the ideal class group of K, h_K (resp. h_F) denotes the order of C_K (resp. C_F), and the product extends over all non-trivial characters of G.

If K/F does not have exponent 2, then we need to extend scalars. Set $\overline{C}_K = \mathbb{Z}[\zeta_e]\otimes_{\mathbb{Z}} C_K$, where e denotes the exponent of K/F, and define $\varphi(e) = [(\mathbb{Z}/e\mathbb{Z})^\times]$. Then the following holds.

Theorem 0.11: *Let K/F be an abelian extension of number fields with Galois group G of exponent e. Then there exists a rational number r, whose numerator and denominator are divisible only by primes that divide e, such that*

$$(h_K/h_F)^{\varphi(e)} = r\cdot\prod_{\chi\neq\chi^0}[\varepsilon_\chi\overline{C}_K].$$

Corollary 0.12: *Let p be an odd prime and let $K=\mathbb{Q}(\zeta_p)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_p)$. Write h^+ for the class number of K and G for the Galois group of $K/\mathbb{Q}$. Then there exists a rational number r, whose numerator and denominator are divisible only by primes that divide $(p-1)/2$, such that*

$$(h^+)^{\varphi(\frac{p-1}{2})} = r\cdot\prod_{\chi\in\widehat{G}}[\varepsilon_\chi\overline{C}_K].$$

In particular, p divides h^+ if and only if p divides $[\varepsilon_\chi\overline{C}_K]$ for some character χ of G.

The preceding results (0.10-0.12) cannot be considered satisfactory, because they give no information on the integers $[\varepsilon_\chi\overline{C}_K]$[3]. However, there exist clear indications that the integers $[\varepsilon_\chi\overline{C}_K]$ are related to the class numbers of the various subextensions of K/F. See the Example and Remarks following the statement of Corollary 6.7 below. Regarding the last assertion of Corollary 0.12, it is of course an allusion to Vandiver's conjecture, which asserts that h^+ is never divisible by p. Concerning this well-known conjecture, the results of this paper seem to suggest that the following statement is true: Vandiver's conjecture holds for p if and only if p does not divide h_L for every subextension $L/\mathbb{Q}$ of $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$ of **prime** degree.

In an Appendix to the paper, we use étale cohomology to obtain certain variants of Theorem 0.8 above. See Theorem A.4 and Corollary A.5 below. We

[3] B. de Smit [6] has obtained a **precise** formula similar to that of Theorem 0.10 for any elementary abelian extension of number fields. See the remarks following Corollary 6.7 below. I'm indebted to F. Lemmermeyer for calling my attention to de Smit's work.

also note that the results of this paper have applications to "non-semisimple" Iwasawa theory, which we hope to develop in a future publication.

Acknowledgement: I am very grateful to E. Aljadeff for having explained to me his results on the norm map and for providing me with copies of his papers [1] and [2]. I am also very grateful to J. Carlson for pointing out an error in an earlier version of the paper, and to the referee for questioning the validity of the original (wrong) statement of Theorem 6.6. The referee's question led to the writing of the Appendix, which I hope some readers will find interesting. Further, I am indebted to F. Lemmermeyer for calling my attention to the work of B. de Smit. *Je remercie également l'Officine pour la Cooperation Reǵionale de l'Ambassade de France au Chili, et très particulièrement Mme. Annie Pauget, pour le financement de mon voyage à Sierra de La Ventana, Argentine, oú une version préliminaire de ce travail a eté presenté le 30 d'Octobre 2001, dans le cadre du* Coloquio Internacional de Homología y Representaciones de Algebras.

1. Preliminaries

Let G be a finite group of exponent e and let $\chi\colon G \to F$ be a character (one-dimensional representation) of G with values in a field F containing a primitive e-th root of unity ζ_e (e.g., $F = \mathbb{C}$). A commutative ring with unit R is said to be **sufficiently large** for G if there exists a ring homomorphism $\mathbb{Z}[\zeta_e] \to R$. For example, $\mathbb{Z}[\zeta_e]$ and $\mathbb{F}_p[x]/(x^{p^m})$ (when $e = p^m$ is a prime power) are sufficiently large for G. Since $\chi\colon G \to F$ factors through $\mathbb{Z}[\zeta_e]$, we may compose χ with the given homomorphism $\mathbb{Z}[\zeta_e] \to R$ to obtain a multiplicative map $G \to R$. This map will also be denoted by χ. Thus $\chi\colon G \to R$ is an "R-valued character of G". Clearly, the values of χ lie in $R^\times$ (the group of units of R), so χ is an element of $\widehat{G} \overset{\text{df.}}{=} \operatorname{Hom}(G, R^\times)$.

Now let R be sufficiently large for G and let M be an $R[G]$-module. Consider the augmentation homomorphism

$$\alpha_\chi\colon R[G] \to R, \quad \sum_{\sigma\in G} r_\sigma \sigma \mapsto \sum_{\sigma\in G} r_\sigma \chi(\sigma).$$

For each $i \geq 0$, consider further the R-module

$$H^i_\chi(G, M) = \operatorname{Ext}^i_{R[G]}(R, M),$$

where R is being regarded as an $R[G]$-module through the map α_χ. For $i = 0$ we have

$$H^0_\chi(G, M) = \operatorname{Hom}_{R[G]}(R, M) = M^\chi,$$

where $M^{\chi} \overset{\text{df.}}{=} \{m \in M\colon \sigma m = \chi(\sigma)m \text{ for all } \sigma \in G\}$.

Next consider the element

$$\varepsilon_{\chi} = \sum_{\sigma \in G} \overline{\chi}(\sigma)\sigma \in R[G],$$

where $\overline{\chi}$ is the character inverse to χ, i.e., $\overline{\chi}(\sigma) = \chi(\sigma)^{-1}$ for all $\sigma \in G$. It is not difficult to check that $\varepsilon_{\chi}M \subset M^{\chi}$. Set

$$\widehat{H}^0_{\chi}(G, M) = M^{\chi}/\varepsilon_{\chi}M.$$

We note that if M is a $\mathbb{Z}[G]$-module and χ is the trivial character of G, then the $\mathbb{Z}$-modules $H^i_{\chi}(G, M)$ and $\widehat{H}^0_{\chi}(G, M)$ defined above are the well-known groups $H^0(G, M) = M^G$ and $\widehat{H}^0(G, M) = M^G/N_G M$ in group cohomology. In general, the R-modules $H^i_{\chi}(G, M)$ and $\widehat{H}^0_{\chi}(G, M)$ are "usual" cohomology modules of a twisted form of M. Indeed, let $M_{\overline{\chi}}$ denote the R-module M endowed with the new G-action

$$\sigma \cdot m = \overline{\chi}(\sigma)\sigma m \quad (\sigma \in G, m \in M).$$

Then

$$\widehat{H}^i_{\chi}(G, M) = \widehat{H}^i(G, M_{\overline{\chi}})$$

for all $i \geq 0$. The above formula follows in a standard way from the fact that the functor $M \mapsto M^{\chi}$ is the composite of the functors $M \mapsto M^{\chi^0}$, where χ^0 is the trivial character of G, and $M \mapsto M_{\overline{\chi}}$, the second of which is **exact** and right adjoint to an exact functor, namely $M \mapsto M_{\chi}$.

2. Cyclic groups

We assume now that G is a finite cyclic group of order n. Let M be a finite $R[G]$-module, where R is sufficiently large for G. Then there exists a ring homomorphism $\mathbb{Z}[\zeta_n] \to R$, where ζ_n is a primitive (complex) n-th root of unity. We will continue towrite ζ_n for the image of ζ_n in R under the above homomorphism (this should not be cause for confusion). We now choose and fix a generator τ of G and define a character $\chi\colon G \to R^{\times}$ by $\chi(\tau) = \zeta_n$. Then any other character of G has the form χ^i, where $0 \leq i \leq n-1$ (by convention χ^0 is the trivial character of G, i.e., $\chi^0(\sigma) = 1$ for all $\sigma \in G$).

Now recall the elements $\varepsilon_{\chi^i} = \sum_{\sigma \in G} \overline{\chi}^i(\sigma)\sigma \in R[G]$, where $0 \leq i \leq n-1$.

We have

$$\begin{aligned}\varepsilon_{\chi^i} = \sum_{j=0}^{n-1} \overline{\zeta}_n^{ij}\tau^j &= \prod_{j=1}^{n-1}(\overline{\zeta}_n^{i}\tau - \zeta_n^j)\\ &= \overline{\zeta}_n^{(n-1)i}\prod_{j=1}^{n-1}(\tau - \zeta_n^{i+j}) = \zeta_n^i \prod_{\substack{j=0\\ j\neq i}}^{n-1}(\tau - \zeta_n^j).\end{aligned}$$

In particular the norm element $\varepsilon_{\chi^0} = \sum_{\sigma\in G}\sigma \in R[G]$ factors as

$$\varepsilon_{\chi^0} = \prod_{j=1}^{n-1}(\tau - \zeta_n^j).$$

Our objective now is to derive a formula connecting the order of M to the orders of the various isotypic components M^{χ^i} of M. To this end, we fix the following notation. The order of a finite module M will be denoted by $[M]$. Further, if a is an element of $R[G]$, $\operatorname{Ker} a$ will denote the kernel of multiplication by a on M (this nonstandard notation for the a-torsion submodule of M is a convenient one, as will become apparent below). Observe that $M^{\chi^i} = \{m \in M \colon \tau m = \zeta_n^i m\} = \operatorname{Ker}(\tau - \zeta_n^i)$. Now, in order to make our general argument more transparent, we will begin by examining the simplest case, that in which $n = 2$. Consider the following exact sequence (which is available for any n)

$$(2) \qquad 0 \to \operatorname{Ker}\varepsilon_{\chi^0} \to M \xrightarrow{\varphi_0} M^{\chi^0} \to \widehat{H}^0_{\chi^0}(G, M) \to 0$$

where φ_0 is the multiplication by ε_{χ^0} map. When $n = 2$, $\operatorname{Ker}\varepsilon_{\chi^0} = \operatorname{Ker}(1+\tau) = \operatorname{Ker}(\tau - (-1)) = M^{\chi}$ (see above), so we immediately obtain from (2)

$$[M][\widehat{H}^0_{\chi^0}(G, M)] = [M^{\chi^0}][M^{\chi}].$$

This is the desired result for $n = 2$.

When $n = 3$ the situation is more complicated, because $\varepsilon_{\chi^0} = (\tau - \zeta_3)(\tau - \zeta_3^2)$ is the product of two linear factors, and therefore $\operatorname{Ker}\varepsilon_{\chi^0}$ is not equal to M^{χ^i} for any i. However, we can relate $\operatorname{Ker}\varepsilon_{\chi^0}$ to modules of the form M^{χ^i} by means of the exact sequence

$$0 \to M^{\chi^2} = \operatorname{Ker}(\tau - \zeta_3^2) \to \operatorname{Ker}\varepsilon_{\chi^0} \xrightarrow{\varphi_1} M^{\chi} \to Q_1 \to 0,$$

where φ_1 is the multiplication by $(\tau - \zeta_3^2)$ map and

$$Q_1 = \operatorname{Coker}\varphi_1 = M^{\chi}/(\tau - \zeta_3^2)\operatorname{Ker}\varepsilon_{\chi^0}.$$

Now since

$$(\tau-\zeta_3^2)\operatorname{Ker}\varepsilon_{\chi^0}=M^{\chi}\cap(\tau-\zeta_3^2)M,$$

we have

$$Q_1\simeq\widehat{H}^0_{\chi}(G,M)/S_1(M),$$

where

$$S_1(M)=M^{\chi}\cap(\tau-\zeta_3^2)M/\varepsilon_{\chi}M.$$

Thus, writing $S_0(M)=\{0\}$, we obtain

$$[M][\widehat{H}^0_{\chi^0}(G,M)/S_0(M)][\widehat{H}^0_{\chi}(G,M)/S_1(M)]=[M^{\chi^0}][M^{\chi}][M^{\chi^2}],$$

which is the desired result for $n=3$.

We now present the general argument.

For each $i\in\{0,1,\dots,n-2\}$, there is an exact sequence

$$0\to\operatorname{Ker}\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)\to\operatorname{Ker}\prod_{j=i}^{n-1}(\tau-\zeta_n^j)\xrightarrow{\varphi_i}M^{\chi^i}\to Q_i\to 0 \tag{3}$$

in which φ_i is the multiplication by $\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)$ map and

$$Q_i=\operatorname{Coker}\varphi_i=M^{\chi^i}\Big/\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)\operatorname{Ker}\prod_{j=i}^{n-1}(\tau-\zeta_n^j).$$

Note that (3) for $i=0$ is precisely the exact sequence (2), because $\prod_{j=0}^{n-1}(\tau-\zeta_n^j)=\tau^n-1=0$ and, therefore, $\operatorname{Ker}\prod_{j=0}^{n-1}(\tau-\zeta_n^j)=M$. Also note that, since

$$\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)\operatorname{Ker}\prod_{j=i}^{n-1}(\tau-\zeta_n^j)=M^{\chi^i}\cap\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)M,$$

we have

$$Q_i\simeq\widehat{H}^0_{\chi^i}(G,M)/S_i(M), \tag{4}$$

where $S_i(M)$ is the submodule of $\widehat{H}^0_{\chi^i}(G,M)$ given by

$$S_i(M)=\Bigl(M^{\chi^i}\cap\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)M\Bigr)\Big/\varepsilon_{\chi^i}M. \tag{5}$$

Now, by (3),

$$\frac{[\operatorname{Ker}\prod_{j=i}^{n-1}(\tau-\zeta_n^j)]}{[\operatorname{Ker}\prod_{j=i+1}^{n-1}(\tau-\zeta_n^j)]}=\frac{[M^{\chi^i}]}{[Q_i]}$$

for $i = 0, 1, \ldots, n-2$. Multiplying these equalities together we obtain, since the product of the left-hand side terms **telescopes**,

$$\frac{[M]}{[M^{\chi^{n-1}}]} = \frac{\prod_{i=0}^{n-2}[M^{\chi^i}]}{\prod_{i=0}^{n-2}[Q_i]}.$$

Thus, by (4), the following holds.

Theorem 2.1: *We have*

$$[M] \cdot \prod_{i=0}^{n-2}[\widehat{H}^0_{\chi^i}(G, M)/S_i(M)] = \prod_{i=0}^{n-1}[M^{\chi^i}],$$

where $S_i(M)$ ($i = 0, 1, \ldots, n-2$) is the submodule of $\widehat{H}^0_{\chi^i}(G, M)$ given by (5).

We will now restate the above theorem in a form which is more suitable for generalization. Set $\prod_{j=i+1}^{n-1}(\tau - \zeta_n^j)M = M$ if $i = n-1$. Now, for $\psi = \chi^i \in \widehat{G}$, $0 \leq i \leq n-1$, define

$$S_\psi(M) = S_i(M) = \left(M^{\chi^i} \cap \prod_{j=i+1}^{n-1}(\tau - \zeta_n^j)M\right) \Big/ \varepsilon_{\chi^i} M. \tag{6}$$

Then Theorem 2.1 may be restated as follows.

Theorem 2.2: *If G is a cyclic group and M is a finite $R[G]$-module, then*

$$[M] \cdot \prod_{\psi \in \widehat{G}}[\widehat{H}^0_\psi(G, M)/S_\psi(M)] = \prod_{\psi \in \widehat{G}}[M^\psi],$$

where $S_\psi(M)$ (for $\psi \in \widehat{G}$) is the submodule of $\widehat{H}^0_\psi(G, M)$ given by (6). An equivalent statement is

$$[M] = \prod_{\psi \in \widehat{G}}[\varepsilon_\psi M] \cdot \prod_{\psi \in \widehat{G}}[S_\psi(M)].$$

3. Abelian groups

In this section we extend Theorem 2.2 to arbitrary finite abelian groups. We will consider first abelian groups which are the direct product of two cyclic groups.

Let K_1 and K_2 be (finite) cyclic groups and let $G = K_1 \times K_2$ be the direct product of K_1 and K_2. Let M be a finite $R[G]$-module, where R is sufficiently large for G (for example $R = \mathbb{Z}[\zeta_e]$, where e is the exponent of G and ζ_e is a fixed complex e-th root of unity). Write M_{K_i} for the $R[G]$-module M regarded as an $R[K_i]$-module ($i = 1, 2$). Note that, since $\widehat{G} = \widehat{K}_1 \times \widehat{K}_2$, each character $\chi \in \widehat{G}$ may be written uniquely as $\chi = \chi_1 \cdot \chi_2$, where $\chi_1 \in \widehat{K}_1$ and $\chi_2 \in \widehat{K}_2$. We have

$$M^{\chi} = (M^{\chi_1}_{K_1})^{\chi_2}_{K_2}$$

(note that since $M^{\chi_1}_{K_1}$ is an $R[G]$-module in a natural way, it is meaningful to consider the restricted module $(M^{\chi_1}_{K_1})_{K_2}$). To ease notation, we will write the above equality as "$M^{\chi} = (M^{\chi_1})^{\chi_2}$". (The reader should bear in mind, however, that in an expression of the form "M^{χ_1}" (resp. "N^{χ_2}"), M (resp. N) is being regarded as a K_1-module (resp. K_2-module).) Now we have

$$\prod_{\chi \in \widehat{G}} [M^{\chi}] = \prod_{\chi_1 \in \widehat{K}_1} \prod_{\chi_2 \in \widehat{K}_2} [(M^{\chi_1})^{\chi_2}].$$

Next, by Theorem 2.2,

$$\prod_{\chi_2 \in \widehat{K}_2} [(M^{\chi_1})^{\chi_2}] = [M^{\chi_1}] \cdot \prod_{\chi_2 \in \widehat{K}_2} [\widehat{H}^0_{\chi_2}(K_2, M^{\chi_1}) / S_{\chi_2}(M^{\chi_1})],$$

where $S_{\chi_2}(M^{\chi_1})$ is given by (6) with $\psi = \chi_2$ and $M = M^{\chi_1}$ in that formula. Applying Theorem 2.2 once again, we obtain

$$[M] \cdot \prod_{\chi_1 \in \widehat{K}_1} [\widehat{H}^0_{\chi_1}(K_1, M) / S_{\chi_1}(M)] \prod_{\substack{\chi_2 \in \widehat{K}_2 \\ \chi_1 \in \widehat{K}_1}} [\widehat{H}^0_{\chi_2}(K_2, M^{\chi_1}) / S_{\chi_2}(M^{\chi_1})] = \prod_{\chi \in \widehat{G}} [M^{\chi}].$$

In general, the following holds.

Theorem 3.1: *Let G be a finite abelian group and let M be a finite $R[G]$-module. Let $G = K_1 \times \cdots \times K_r$ ($r \geq 1$) be a decomposition of G into a direct product of cyclic groups. For $0 \leq i \leq r-1$, set $G_i = K_1 \times \cdots \times K_i$, where G_0 is defined to be 0. Then*

$$[M] \cdot \prod_{i=1}^{r} \prod_{\substack{\chi_i \in \widehat{K}_i \\ \psi \in \widehat{G}_{i-1}}} [\widehat{H}^0_{\chi_i}(K_i, M^{\psi}) / S_{\chi_i}(M^{\psi})] = \prod_{\chi \in \widehat{G}} [M^{\chi}].$$

Proof: This may be proved without difficulty by induction, writing $G = (K_1 \times \cdots \times K_{r-1}) \times K_r$ and arguing as in the case $r = 2$ above. ∎

4. A criterion for cohomological triviality

In this section we establish a criterion for cohomological triviality using an important result of E. Aljadeff and Y. Ginosar. We then apply this criterion to derive sufficient conditions under which the order of a finite $R[G]$-module M (where G is cyclic and R is sufficiently large for G) equals the product of the orders of the various isotypic components M^χ of M as χ ranges over $\widehat{G}$. In this section "G-module" means $\mathbb{Z}[G]$-module.

We begin with

Theorem 4.1 (Aljadeff): *Let G be a finite group and let M be a G-module which is also a commutative ring with unit. Assume that $\widehat{H}^0(H,M)=0$ for every subgroup H of G of prime order. Then $\widehat{H}^0(H,M)=0$ for every subgroup H of G.*

Proof: See [1, Corollary 0.2]. The proof uses a tensor induction argument for skew group rings M_tH, where H is a subgroup of G and $t\colon G\to \mathrm{Aut}(M)$ is the map defining the action of G on M. ∎

Remark: The commutativity assumption of the theorem is crucial. See [1] for an example of a group G and a non-commutative ring M for which the theorem fails. The following is the correct generalization of Theorem 4.1 when M is a non-commutative ring with unit: if $\widehat{H}^0(H,M)=0$ for every elementary abelian subgroup H of G, then $\widehat{H}^0(H,M)=0$ for every subgroup H of G. See [2, Theorem 1].

Our objective now is to extend the class of G-modules M to which Theorem 4.1 applies (at the expense of restricting the class of groups G, as it will turn out). We need the following result.

Theorem 4.2 (Aljadeff–Ginosar): *Let R be a ring with unit, let G be a finite group and let M be a module over a crossed product algebra $R*G$. Then*

$$\text{proj.dim.}_{R*G}M=\sup\{\text{proj.dim.}_{R*H}M\colon H\le G \textit{ elementary abelian}\}.$$

Proof: See [2, Theorem 3]. ∎

Remark: Theorem 4.2 is a corollary of the following generalization (due to Aljadeff and Ginosar) of a well-known theorem of Chouinard [5]: an $R*G$-module M is weakly projective (resp. projective) if and only if M is $R*H$-weakly projective (resp. projective) for every elementary abelian subgroup H of G. See [2, Theorem 2].

We now hav e

THEOREM 4.3: *Let G be a finite group and let M be a G-module. Then M is cohomologically trivial if and only if $\widehat{H}^{i_p}(H,M) = \widehat{H}^{i_p+1}(H,M) = 0$ for every p-elementary abelian subgroup H of G, where i_p is an integer (which may depend on the prime p).*

Proof: By the Nakayama–Rim theorem [23, Theorem IX.5.8, (ii)⇔(iv), p. 145], a G-module M is cohomologically trivial if and only if the $\mathbb{Z}[G]$-projective dimension of M is ≤ 1. Now Theorem 4.2 shows that M is cohomologically trivial if and only if M is H-cohomologically trivial for every p-elementary abelian subgroup H of G. Nakayama's criterion [23, Theorem IX.5.8, (i)⇔(ii), p. 145] now completes the proof. ∎

COROLLARY 4.4: *Let G be a finite group such that all Sylow subgroups of G are either cyclic or generalized quaternion, and let M be a G-module. Assume that $\widehat{H}^{-1}(H,M) = \widehat{H}^{0}(H,M) = 0$ for all subgroups H of G of prime order. Then M is cohomologically trivial.*

Proof: The class of groups G which satisfies the hypothesis of the corollary is exactly the class of groups G which ha vethe property that ev ery abelian subgroup of G is cyclic. See [3, Theorem XII.11.6, p. 262]. The corollary now follo ws from the theorem and the periodicity of the cohomology of cyclic groups. ∎

Remarks: (a) The corollary applies in particular to $G = Q_{2^n}$, the generalized quaternion group of order 2^n ($n \geq 3$). Note that this group has a **unique** subgroup H of order 2.

(b) The classical Hölder–Burnside–Zassenhaus theorem asserts that a group G has the property that all its Sylo w subgroups arecyclic if and only if G is a split extension (i.e., a semi-direct product) of tw o cyclic groups whose orders are relatively prime. See [21, Theorem 10.26, p. 246] and [29, Theorem V.3.11, p. 175]. Thus Corollary 4.4 applies to all cyclic groups (but not to other types of abelian groups) and to certain types of non-abelian finite groups (other than Q_{2^n}), for example the dihedral groups of order $2n$ for every **odd** integer $n \geq 3$.

(c) Theorem 4.3 and Corollary 4.4 represent a significant improvement of the w ell-known criterion for cohomological triviality established by T. Nakayama in the mid 1950's (see [23, Theorem IX.5.8 (i)⇔(ii), p. 145]). F or example, if$G$ is a cyclic group of order p^n (where p is a prime and $n \geq 1$) and M is a G-module, then by Corollary 4.4 the cohomological triviality of M may be checked "at the first layer", i.e., by checking whether $\widehat{H}^i(H,M)$ vanishes for $i=-1,0$ and H equal to the unique subgroup of G of order p. By contrast, Nakayama's criterion requires checking the vanishing of these cohomology groups for the full group (i.e., for $H=G$), a verification which depends on the (possibly very large) value of n.

Recall now that if H is a finite cyclic group and M is an H-module such that the cohomology groups $\widehat{H}^i(H,M)$, $i=0,1$, are **finite**, then the Hebrand quotient $h(M)$ of M is defined by

$$h(M)=[\widehat{H}^0(H,M)]/[H^1(H,M)].$$

It is a well-known fact that the Herbrand quotient of a finite module is 1. Now Corollary 4.4 yields the following variant of Theorem 4.1.

Corollary 4.5: *Let G be a finite group satisfying the hypothesis of Corollary 4.4 and let M be a G-module. Assume that for each subgroup H of G of prime order the Herbrand quotient of M, when regarded as an H-module, is defined and equal to 1 (for example, M may be a finite G-module). Assume further that $\widehat{H}^0(H,M)=0$ for all subgroups H of prime order. Then M is cohomologically trivial. In particular $\widehat{H}^0(H,M)=0$ for all subgroups H of G.*

Remark: The above corollary will be applied in the next section to establish an interesting fact concerning abelian varieties defined over local fields. See Theorem 5.3 below.

Next, we will combine Theorem 2.2 and Corollary 4.5 to obtain conditions which will ensure that the order of a finite $R[G]$-module M, where G is cyclic and R is sufficiently large for G, equals the product of the orders of the various isotypic components M^χ of M as χ ranges over $\widehat{G}$.

Theorem 4.6: *Let G be a finite cyclic group and let M be a finite $R[G]$-module, where R is sufficiently large for G. Assume that $\widehat{H}^0_\chi(H,M)=0$ for every subgroup H of G of prime order and every character χ of H. Then $\widehat{H}^0_\psi(G,M)=0$ for all characters ψ of G, and*

$$[M]=\prod_{\psi\in\widehat{G}}[M^\psi]=\prod_{\psi\in\widehat{G}}[\varepsilon_\psi M].$$

Proof: The stated formula will follow from Theorem 2.2 once we prove the first assertion. Let ψ be any character of G and let $M_{\overline{\psi}}$ be the twist of M by

$\overline{\psi}$ (see §1). Let H be a subgroup of G of prime order. As an $R[H]$-module, $M_{\overline{\psi}}$ is canonically isomorphic to $M_{\overline{\chi}}$, where $\overline{\chi} = \overline{\psi}|_H$ is the restriction of $\overline{\psi}$ to H. Therefore $\widehat{H}^0(H, M_{\overline{\psi}}) \simeq \widehat{H}^0(H, M_{\overline{\chi}}) \simeq \widehat{H}^0_{\chi}(H, M) = 0$. Now Corollary 4.5 shows that $\widehat{H}^0(G, M_{\overline{\psi}})$ is zero, whence $\widehat{H}^0_{\psi}(G, M)$ is zero and the proof is complete. ∎

Remarks: (a) By Theorem 4.1, a result analogous to Theorem 4.6 holds true if G is an y finite abelian group and the finite$R[G]$-module M has the structure of a commutativ e ring with unit.

(b) If G is a cyclic group of order p^n, where p is a prime and $n \geq 1$, the number of conditions to be check ed in order to apply Theorem 4.6 is **independent** of n. See the remarks following the proof of Corollary 4.4.

Now let G be a cyclic 2-group and let τ denote the unique element of G of order 2. For any finite $R[G]$-module M, define

$$M^+ = \{m \in M \colon \tau m = m\}. \tag{7}$$

Then M^+ is a submodule of M con taining $(1 +\tau)M$.

Theorem 4.6 has the following satisfying corollary.

Corollary 4.7: *Let G be a cyclic group of order 2^n, where $n \geq 1$, and let M be a finite $R[G]$-module. Assume that $M^+ = (1+\tau)M$, where M^+ is given b y (7) and τ is the unique element of G of order 2. Then*

$$[M] = \prod_{\psi \in \widehat{G}} [M^{\psi}] = \prod_{\psi \in \widehat{G}} [\varepsilon_{\psi} M].$$

Proof: This will follow from Theorem 4.6 once we check that $\widehat{H}^0_{\chi}(H, M) = 0$ for $H = \langle \tau \rangle$ and χ equal to the nontrivial c haracter of$H$. But

$$\widehat{H}^0_{\chi}(H, M) = {}_{(1+\tau)}M/(1-\tau)M = \widehat{H}^{-1}(H, M)$$

has the same order as $\widehat{H}^0(H, M) = M^+/(1+\tau)M$, which is zero b y hypothesis. ∎

5. Applications to abelian v arieties

Let F be a global field, i.e., F is a finite extension of $\mathbb{Q}$ (the "number field case") or is finitely generated and of transcendence degree 1 ov er a finite field (the "function field case"). The following notations will remain in force throughout the rest of the paper. Let $\bar{F}$ denote a fixed separable algebraic closure of

F. We will write Γ for the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$ and p for the characteristic exponent of F. For each prime v of F, we choose once and for all a prime $\overline{v}$ of $\bar{F}$ lying above v and write Γ_v for the decomposition group of $\overline{v}$ in Γ, i.e., $\Gamma_v = \{\sigma \in \Gamma\colon \sigma(\overline{v}) = \overline{v}\}$. Then $\bar{F}_v := \bar{F}_{\overline{v}}$ is a separable algebraic closure of F_v and Γ_v may be identified with $\mathrm{Gal}(\bar{F}_v/F_v)$. Given a (discrete, continuous) Γ-module M, $H^i(F,M)$ will denote the i-th Galois cohomology group $H^i(\Gamma, M)$. For $i = 1$ or 2, we set

$$\text{Ш}^i(F,M) = \mathrm{Ker}\left[H^i(F,M) \to \prod_{\text{all } v} H^i(F_v, M)\right]$$

and

$$\mathrm{b}^i(F,M) = \mathrm{Coker}\left[H^i(F,M) \to \prod_{\text{all } v} H^i(F_v, M)\right],$$

where the products extend over all primes v of F.

Let A be an abelian variety defined over F and let K/F be a finite Galois subextension of $\bar{F}/F$ with Galois group G. We will write A_F (resp. A_K) for the abelian variety A regarded as an abelian variety over F (resp. K). Further, A^{t} will denote the dual (Picard) variety of A. For each prime w of K lying above a prime v of F, we will write G_w for $\mathrm{Gal}(K_w/F_v)$ and identify it with the decomposition group of w in G.

Proposition 5.1: *Let w be any prime of K, let v be the prime of F lying below w and let L/F_v be a subextension of K_w/F_v such that $H = \mathrm{Gal}(K_w/L)$ is cyclic. Then the Herbrand quotient of the H-module $A(K_w)$ is 1.*

Proof: Let $f\colon A \to A^{\mathrm{t}}$ be an isogeny and let A_f be the kernel of f. Then there exists a natural exact sequence

$$0 \to A_f(\overline{K}_w) \to A(\overline{K}_w) \to A^{\mathrm{t}}(\overline{K}_w) \to 0,$$

where $\overline{K}_w$ is a separable algebraic closure of K_w. Taking $\mathrm{Gal}(\overline{K}_w/K_w)$-invariants of the above exact sequence, we conclude that there exists an H-module homomorphism $A(K_w) \to A^{\mathrm{t}}(K_w)$ with finite kernel and cokernel. Therefore $h(A(K_w)) = h(A^{\mathrm{t}}(K_w))$, where $h(M)$ denotes the Herbrand quotient of the H-module M. On the other hand, local duality [16, I.3.4, 3.7; III.7.8] (see also [15, Proposition 4.2]) implies that $h(A(K_w))h(A^{\mathrm{t}}(K_w)) = 1$. Therefore $h(A(K_w))^2 = 1$, whence the result follows. ∎

Remark: When K_w is non-archimedean of characteristic zero, there is an alternative proof of Proposition 5.1 which makes use of a well-known theorem of Mattuck. This proof (therefore) depends on the theory of the logarithm. See [25, §4, (14)].

COROLLARY 5.2: *Let v be a real prime of F. Then $A(F_v)$ is connected if and only $A^{\mathrm{t}}(F_v)$ is connected.*

Proof: By [16, I.3.7], $A(F_v)$ is connected if and only if $\widehat{H}^0(F_v, A) = 0$ or, equivalently by duality, if and only if $H^1(F_v, A^{\mathrm{t}}) = 0$. The proposition (applied to A^{t} and to some totally imaginary finite Galois extension K of F) shows that the latter is equivalent to the vanishing of $\widehat{H}^0(F_v, A^{\mathrm{t}})$, i.e., to the connectedness of $A^{\mathrm{t}}(F_v)$. ∎

Remark: Corollary 5.2 was known to Yu. Zarhin in 1972. See [28, §3].

THEOREM 5.3: *Let v be a prime of F and let w be a fixed prime of K lying abo vev. Assume that the decomposition group $G_w = \mathrm{Gal}(K_w/F_v)$ satisfies the h ypothesis of Corollary 4.4. Assume further that $A(L) = N_{K_w/L}A(K_w)$ for every subextension L/F_v of K_w/F_v of prime index. Then the G_w-module $A(K_w)$ is cohomologically trivial.*

Proof: This follows at once from Proposition 5.1 and Corollary 4.5. ∎

Remarks: (a) If $G = \mathrm{Gal}(K/F)$ satisfies the hypothesis of Corollary 4.4, then so does G_w for any w. On the other hand, let p denote the characteristic of the residue field of F_v and let e and f denote, respectively, the ramification index and residue degree of w in K/F. Further, let G_0 and G_1 denote the inertia and first ramification subgroup of G_w, respectively. There exist group extensions

$$0 \to G_0 \to G_w \to G_w/G_0 \to 0$$

and

$$0 \to G_1 \to G_0 \to G_0/G_1 \to 0,$$

where G_w/G_0 is cyclic of order f, G_0/G_1 is cyclic of order prime to p and G_1 is a p-group. See [23, pp. 67–68]. It follo ws that if G_1 is either cyclic or generalized quaternion and f is **prime to the ramification index** $e = [G_0]$, then G_w satisfies the h ypothesis of Corollary 4.4. (See [23, Ex. IV.2.3, p. 71] for conditions that will insure that G_1 is cyclic.)

(b) Notations being as in the theorem, let K_w/L be a ramified extension of prime degree p. Write $\mathfrak{l}$ for the residue field of L. Further, let $\mathcal{A}$ denote the Neŕon model of A_L and let $\widehat{\mathcal{A}}$ be the formal completion of $\mathcal{A}$ along its zero section. Then there exists a natural exact sequence

$$A(\mathfrak{l})_p \to \widehat{H}^0(H, \widehat{\mathcal{A}}(K_w)) \to \widehat{H}^0(H, A(K_w)) \to A(\mathfrak{l})/pA(\mathfrak{l}) \to 0,$$

where $A(\mathfrak{l})_p$ denotes the p-torsion subgroup of the finite group $A(\mathfrak{l})$ (see [15, Corollary 4.6]). It follows that the vanishing of $\widehat{H}^0(H, A(K_w))$ is equivalent to the vanishing of both $A(\mathfrak{l})_p$ and $\widehat{H}^0(H, \widehat{\mathcal{A}}(K_w))$. Regarding the vanishing of $\widehat{H}^0(H, \widehat{\mathcal{A}}(K_w))$, it seems likely that the methods of [15, §4] are strong enough for finding sufficient conditions under which $\widehat{H}^0(H, \widehat{\mathcal{A}}(K_w))$ vanishes. However, we do not pursue this matter here.

Next we recall the main theorem of [8]. Let T be the set of primes of F which is formed by collecting together the primes that ramify in K/F and the primes where A has bad reduction.

Theorem 5.4: *Notations being as above, suppose that the following conditions hold.*

(i) *The Tate–Shafarevich group $\text{Ш}(A_K)$ of A_K is finite.*

(ii) *$\widehat{H}^i(G, A(K)) = \widehat{H}^i(G, A^{\text{t}}(K)) = 0$ for all integers i.*

(iii) *$A(F_v)$ is connected for all real primes v of F.*

Then

$$[\text{Ш}(A_K)^G] = [\text{Ш}(A_F)] \cdot \prod_{v \in T} [H^1(G_w, A(K_w))]$$

and

$$[H^1(G, \text{Ш}(A_K))] = \prod_{v \in T} [H^2(G_w, A(K_w))],$$

where, for each prime $v \in T$, w is a fixed prime of K lying above v.

Proof: See [8], Theorem 4.4. ∎

Remarks: (a) The above result, which was established in [8] for number fields only, is in fact valid for arbitrary global fields. This holds because [16], which was the main reference for [8], covers both the number field and function field cases (one only needs to supplement some of the references made in [8] to results from Chapter I of [16] with references to Chapter III of the same book).

(b) As pointed out by the referee of [8], the conditions of the theorem “[seem] rather stringent but hold in fact quite often”. The results of Aljadeff and Ginosar explain why this is so. Consider, for example, the case of a cyclic p-group G, where p is a prime number. Then condition (ii) of the theorem is equivalent to the cohomological trivialit y of both $A(K)$ and $A^{\mathrm{t}}(K)$. By Corollary 4.4, the latter is equivalen t to the vanishing of $\widehat{H}^i(H, A(K))$ and $\widehat{H}^i(H, A^{\mathrm{t}}(K))$ for $i=-1$ and 0, where H is the unique subgroup of G of order p. These conditions do not seem stringent at all. (Note, furthermore, that if there exists an isogeny $f\colon A \to A^{\mathrm{t}}$ of degree prime to p, then $\widehat{H}^i(H, A^{\mathrm{t}}(K))=0$ for all i if and only if $\widehat{H}^i(H, A(K))=0$ for all i. See the proof of Proposition 5.1 above.)

(c) Condition (iii) of the theorem is vacuous if F has no real primes. F urthermore, Corollary 5.2 shows that it is equivalent to condition (B) of [8].

Henceforth, we will assume that K/F is a **cyclic** extension.

Corollary 5.5: *Assume that G is cyclic. Then, with the hypotheses and notations of Theorem 5.4,*

$$[\text{Ш}(A_K)^G] = [\text{Ш}(A_F)][\widehat{H}^0(G, \text{Ш}(A_K))]$$

and

$$[\widehat{H}^0(G, \text{Ш}(A_K))] = \prod_{v\in T}[\widehat{H}^0(G_w, A(K_w))].$$

Proof: This is immediate from Theorem 5.4, using Proposition 5.1, the periodicity of the cohomology of cyclic groups and the fact that the Herbrand quotient of a finite module is 1. ∎

We now write n for the order of G and assume that A has **complex multiplication** b y the ring of in tegers $R = \mathbb{Z}[\zeta_n]$ of $\mathbb{Q}(\zeta_n)$. Then $\text{Ш}(A_K)$ is an $R[G]$-module in a natural way, and we may apply to it the results of the preceding sections. F or each character χ of G we will write A^χ for the χ-twist of A† (see [17, §2]). Then there are isomorphisms

$$\text{Ш}(A_K)^\chi \simeq (\text{Ш}(A_K)_{\overline{\chi}})^G \simeq \text{Ш}(A_K^{\overline{\chi}})^G.$$

The next corollary results from applying Corollary 5.5 to the twisted abelian variet y $A^{\overline{\chi}}$.

† This is a standard notation for the χ-twist of an abelian variety. We have adopted it in spite of the fact that some readers may be confused by it, in view of the notations introduced earlier. It may help clarify matters to note that $A^\chi(K)$ is an $R[G]$-module which is isomorphic to the twisted $R[G]$-module $A(K)_\chi$ defined in §1, whereas $A(K)^\chi$ (whic h w e primarily regard as an R-module) is isomorphic to the R-module $A^{\overline{\chi}}(F)$, where $\overline{\chi}$ is the inverse character of χ.

COROLLARY 5.6: *Suppose G is cyclic and let χ be a character of G. Assume that the conditions of Theorem 5.4 hold for the twisted abelian variety $A_K^{\overline{\chi}}$. Then*

$$[\text{Ш}(A_K)^{\chi}] = [\text{Ш}(A_F^{\overline{\chi}})][\widehat{H}_{\chi}^{0}(G, \text{Ш}(A_K))]$$

and

$$[\widehat{H}_{\chi}^{0}(G, \text{Ш}(A_K))] = \prod_{v \in T_{\overline{\chi}}} [\widehat{H}_{\chi_w}^{0}(G_w, A(K_w))],$$

where $T_{\overline{\chi}}$ is the set of primes of F which ramify in K/F or where $A_F^{\overline{\chi}}$ has bad reduction, and χ_w is the restriction of χ to G_w.

We now combine the above corollary with Theorem 2.2 to establish the main result of this section.

THEOREM 5.7: *Let K/F be a cyclic Galois extension of global fields with Galois group G of order n and let A be an abelian variety over F with complex multiplication by the ring of integers of $\mathbb{Q}(\zeta_n)$. Assume that the following conditions hold.*

(i) *The Tate-Shafarevich group $\text{Ш}(A_K)$ of A_K is finite.*
(ii) *$\widehat{H}_{\chi}^{i}(G, A(K)) = \widehat{H}_{\chi}^{i}(G, A^{\mathrm{t}}(K)) = 0$ for all i and all $\chi \in \widehat{G}$.*
(iii) *$A(F_v)$ is connected for all real primes v of F.*

Then

$$[\text{Ш}(A_K)] = \prod_{\chi \in \widehat{G}} [\text{Ш}(A_F^{\chi})] \cdot \prod_{\chi \in \widehat{G}} [S_{\chi}(\text{Ш}(A_K))],$$

where, for each $\chi \in \widehat{G}$, $S_{\chi}(\text{Ш}(A_K))$ is the submodule of $\widehat{H}_{\chi}^{0}(G, \text{Ш}(A_K))$ given by (6). Further, for each $\chi \in \widehat{G}$, $[S_{\chi}(\text{Ш}(A_K))]$ divides

$$\prod_{v \in T_{\overline{\chi}}} [\widehat{H}_{\chi_w}^{0}(G_w, A(K_w))],$$

where $T_{\overline{\chi}}$ and χ_w are as in the statement of Corollary 5.6.

Remarks: (a) Since A and A^{χ} are isomorphic over K, the finiteness of $\text{Ш}(A_K^{\chi})$ is equivalent to that of $\text{Ш}(A_K)$. Thus condition (i) of Theorem 5.7 implies that condition (i) of Theorem 5.4 holds for all twists of A.

(b) Similarly, condition (iii) of Theorem 5.7 implies that condition (iii) of Theorem 5.4 holds for all twists of A. Indeed, let v be a real prime of F and let K be a totally imaginary extension of F. By [16, I.3.7], $A^{\chi}(F_v)$ is connected if and only if $\widehat{H}^{0}(G_w, A^{\chi}(K_w)) \simeq \widehat{H}_{\overline{\chi}_w}^{0}(G_w, A(K_w))$ is zero. On the other hand, since K_w/F_v is quadratic,

$$[\widehat{H}_{\overline{\chi}_w}^{0}(G_w, A(K_w))] = [\widehat{H}^{-1}(G_w, A(K_w))] = [\widehat{H}^{0}(G_w, A(K_w))],$$

by the proof of Corollary 4.7 and Proposition 5.1. Thus $A^{\chi}(F_v)$ is connected if and only if $\widehat{H}^0(G_w, A(K_w))$ is zero, i.e., if and only if $A(F_v)$ is connected.

(c) If G is a cyclic p-group, where p is a prime, and H is the unique subgroup of G of order p, then condition (ii) of Theorem 5.7 is equivalent to the condition:
(ii)′ $\widehat{H}^i_{\chi}(H, A(K)) = \widehat{H}^i_{\chi}(H, A^{\mathrm{t}}(K)) = 0$ for $i = -1, 0$ and all $\chi \in \widehat{H}$.

See the remark following the statement of Theorem 5.4. When $p = 2$, the above condition needs only be checked for $\chi = \chi^0$, the trivial character of H.

(d) Theorem 5.7 generalizes Corollary 4.6 of [8]. As noted in the introduction, the search for such a generalization motivated the writing of this paper.

6. Applications to ideal class groups of number fields

Let F be a number field, let $\bar{F}$ be a fixed algebraic closure of F and let $\Gamma = \mathrm{Gal}(\bar{F}/F)$. We will write $\mathcal{O}_F$ for the ring of integers of F, U_F for its group of units and $\mathcal{I}_F$ for the group of fractional ideals of F. The subgroup of $\mathcal{I}_F$ of principal fractional ideals will be denoted by $\mathcal{P}_F$ and identified with F^*/U_F via the canonical map. In addition, we will write C_F for the ideal class group $\mathcal{I}_F/\mathcal{P}_F$ of F and h_F for its order. The group of units in $\bar{F}$ will be denoted by $\bar{U}$. Further, we will write S_∞ for the set of archimedean primes of F. For $v \notin S_\infty$, U_v (resp. $\bar{U}_v$) will denote the group of units in F_v (resp. $\bar{F}_v$). If $v \in S_\infty$, we set $U_v = F_v^*$ (resp. $\bar{U}_v = \bar{F}_v^*$). We now recall that the invariant map $\mathrm{inv}_v \colon \mathrm{Br}(F_v) \to \mathbb{Q}/\mathbb{Z}$ of local class field theory induces isomorphisms $\mathrm{Br}(F_v) \simeq \mathbb{Q}/\mathbb{Z}$ if v is non-archimedean, $\mathrm{Br}(F_v) \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if v is real, and $\mathrm{Br}(F_v) = 0$ if v is complex. Now let K/F be a finite Galois subextension of $\bar{F}/F$ with Galois group G. For each prime v of F, we will write w for the prime of K lying below the prime $\overline{v}$ of $\bar{F}$ chosen previously.

Lemma 6.1: *There exists a canonical isomorphism of G-modules*

$$C_K = \text{Ш}^1(K, \bar{U}).$$

Proof (After B. Poonen [20]): Set $\Delta = \mathrm{Gal}(\bar{F}/K)$. Taking Δ-cohomology of the natural exact sequence

$$0 \to \bar{U} \to \bar{F}^* \to \bar{F}^*/\bar{U} \to 0$$

and using Hilbert's Theorem 90, we obtain a natural exact sequence

$$0 \to U_K \to K^* \to (\bar{F}^*/\bar{U})^{\Delta} \xrightarrow{\partial} H^1(K, \bar{U}) \to 0,$$

where ∂ is the usual connecting homomorphism in Galois cohomology. Using the identification $K^*/U_K = \mathcal{P}_K$, we conclude that ∂^{-1} induces an isomorphism

$$H^1(K, \bar{U}) = (\bar{F}^*/\bar{U})^{\Delta}/\mathcal{P}_K.$$

Now, since $H^1(K,\bar{U})$ is torsion and $(\bar{F}^*/\bar{U})^\Delta$ is uniquely divisible, $(\bar{F}^*/\bar{U})^\Delta/\mathcal{P}_K$ is canonically isomorphic to $(\mathcal{P}_K\otimes\mathbb{Q})/\mathcal{P}_K$ (via the map $[a]\mapsto[(ma)\otimes(1/m)]$, where m is the order of the coset $[a]$). On the other hand, since $\mathcal{P}_K\otimes\mathbb{Q}=\mathcal{I}_K\otimes\mathbb{Q}$ by the finiteness of $\mathcal{I}_K/\mathcal{P}_K$, we conclude that there exists a natural isomorphism

$$H^1(K,\bar{U})=(\mathcal{I}_K\otimes\mathbb{Q})/\mathcal{P}_K.$$

Similarly, for every finite prime w of K, there exists a canonical isomorphism

$$H^1(K_w,\bar{U}_w)=(\mathbb{Z}\otimes\mathbb{Q})/\mathbb{Z}=\mathbb{Q}/\mathbb{Z}$$

(the reader may ignore the archimedean primes of K since they play no role in this proof). Now it is not difficult to see, by tracing through definitions, that the localization map $H^1(K,\bar{U})\to H^1(K_w,\bar{U}_w)$ corresponds, under the above isomorphisms, to the map $(\mathcal{I}_K\otimes\mathbb{Q})/\mathcal{P}_K\to\mathbb{Q}/\mathbb{Z}$ which is induced by the w-adic valuation map $\mathcal{I}_K\to\mathbb{Z}$, i.e., by the map which assigns to a fractional ideal $\mathfrak{a}\in\mathcal{I}_K$ the exponent of w in its factorization. It now follows easily that the subgroup $\text{Ш}^1(K,\bar{U})$ of $H^1(K,\bar{U})$ is canonically isomorphic to the subgroup $C_K=\mathcal{I}_K/\mathcal{P}_K$ of $(\mathcal{I}_K\otimes\mathbb{Q})/\mathcal{P}_K$. ∎

There exists an exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(G,U_K) \arrow[r] \arrow[d] & H^1(F,\bar{U}) \arrow[r] \arrow[d] & H^1(K,\bar{U})^G \arrow[r] \arrow[d] & H^2(G,U_K) \arrow[d] \\
0 \arrow[r] & \prod_v H^1(G_w,U_w) \arrow[r] & \prod_v H^1(F_v,\bar{U}_v) \arrow[r] & \prod_v H^1(K_w,\bar{U}_w)^{G_w} \arrow[r] & \prod_v H^2(G_w,U_w)
\end{tikzcd}$$

in which the rows are (induced by) the inflation-restriction exact sequences, the products extend over all primes v of F and, for each such prime v, w is the prime of K lying above v fixed previously (note that we have used "semilocal theory" [4, §2.1]). An application of a variant of the snake lemma [10, Lemma 1.7] to the above diagram, together with Lemma 6.1, yields

Theorem 6.2: *Let K/F be a finite Galois extension of number fields with Galois group G. Then there exists a natural complex of finite abelian groups*

$$0\to\text{Ш}^1(G,U_K)\to C_F\to C_K^G\to\text{Ш}^2(G,U_K)$$

which is exact except perhaps at C_K^G, where its homology is a (finite) subgroup of $\mathrm{b}^1(G,U_K)$. ∎

As immediate consequences of the theorem, we have

Corollary 6.3: *Let K/F be a finite Galois extension of number fields with Galois group G of exponent e. Then there exists a rational number r_0, wbse numerator and denominator are divisible only by primes that divide e, such that*

$$[C_K^G] = r_0 \cdot h_F.$$

In particular, a prime $p \nmid e$ divides $[C_K^G]$ if and only if it divides h_F.

Corollary 6.4: *Let K/F be a finite Galois extension of number fields with Galois group G. Assume that $\mathrm{b}^1(G, U_K) = \text{Ш}^2(G, U_K) = 0$. Then the canonical map $C_F \to C_K^G$ is surjective.*

Corollary 6.5: *Let K/F be a finite Galois extension of number fields with Galois group G. Assume that $\text{Ш}^1(G, U_K) = 0$. Then h_F divides h_K.*

Remarks: (a) For each finite prime v of F, $H^1(G_w, U_w)$ is a (cyclic) group of order $e(w/v)$, where $e(w/v)$ denotes the ramification index of K_w/F_v. See [24, Proposition 47, p. 154]. It follows that $\mathrm{b}^1(G, U_K)$ is a **finite** group of order dividing $\prod_{v \notin S_\infty} e(w/v)$.

(b) If K/F has the property that K_w/F_v is cyclic for every finite prime v of F, then $\prod_v H^2(G_w, U_w)$ is a finite group of order

$$\prod_v [H^2(G_w, U_w)] = 2^{r_\infty(K/F)} \cdot \prod_{v \notin S_\infty} e(w/v),$$

where $r_\infty(K/F)$ denotes the number of real primes of F which ramify in K. See [13, Lemma IX.3.4, p. 188]. In particular, if K/F is **unramified at all primes** of F, then, by (a) and the theorem, there exists a natural exact sequence of finite groups

$$0 \to H^1(G, U_K) \to C_F \to C_K^G \to H^2(G, U_K).$$

See the Appendix for a generalization of this fact. The preceding exact sequence has the following "amusing" consequence. Let K be the Hilbert class field of F. Then, by the Principal Ideal Theorem [19, Theorem 8.6, p. 107], the canonical map $C_F \to C_K^G$ is zero. Consequently, the above exact sequence yields a canonical isomorphism

$$C_F = H^1(G, U_K).$$

Therefore every ideal class in F may be represented by a 1-G-cocycle with values in the group of units of the Hilbert class field K of F, where $G = \mathrm{Gal}(K/F)$.

(c) Let T be the F-torus corresponding to the free and finitely generated Γ-module U_K/tors, and assume (for simplicity) that $H^2(G, U_{K,\mathrm{tors}}) = 0$ (this holds, for example, if the order of $U_{K,\mathrm{tors}}$, i.e., the number of roots of unity contained in K, is prime to the order of G). Then there exists a canonical injection

$$Ш^2(G, U_K) \hookrightarrow Ш^2(G, U_K/\mathrm{tors}).$$

On the other hand, by Nakayama–Tate duality, $Ш^2(G, U_K/\mathrm{tors})$ is canonically isomorphic to the dual of $Ш^1(F, T)$ (see [22, Lemma 1.9, p. 19]). Consequently $Ш^2(G, U_K) = 0$ if $Ш^1(F, T) = 0$. The latter holds, for example, if G is **metacyclic** ([22, Corollary 5.3, p. 34]).

Now let G be any finite group and let M be a finite $\mathbb{Z}[G]$-module. Since $\mathbb{Z}$ is not sufficiently large for G, the results of §§3 and 4 do not immediately apply to M. Consequently, we need to "extend scalars". Let $R = \mathbb{Z}[\zeta_e]$, where e is the exponent of G and ζ_e is a fixed (complex) e-th root of unity. Clearly, $R = \mathbb{Z}[\zeta_e]$ is a free $\mathbb{Z}$-module of rank $\varphi(e)$, where φ is Euler's function. Define

$$\overline{M} = M \otimes_{\mathbb{Z}} R.$$

Then $\overline{M}$ is a finite $R[G]$-module (with G acting trivially on R), of order $[M]^{\varphi(e)}$. More precisely, let $\mathcal{B} = \{\zeta_e^i \colon 0 \leq i \leq \varphi(e) - 1\}$. Then the elements of $\overline{M}$ may be regarded as formal linear combinations of elements of M with coefficients in $\mathcal{B}$, i.e., an y$x \in \overline{M}$ may be written, uniquely, in the form

$$x = \sum_{i=0}^{\varphi(e)-1} m_i \zeta_e^i, \tag{8}$$

where the $m_i \in M$.

We now apply Theorem 3.1 to the $R[G]$-module $\overline{C}_K = C_K \otimes_{\mathbb{Z}} R$. Using Corollary 6.3, we obtain the following result.

Theorem 6.6: *Let K/F be an abelian extension of number fields with Galois group G of exponent e. Then there exists a rational number r, whose numerator and denominator are divisible only by primes that divide e, such that*

$$(h_K/h_F)^{\varphi(e)} = r \cdot \prod_{\substack{\chi \in \widehat{G} \\ \chi \neq \chi^0}} [\overline{C}_K^{\chi}].$$

Writing each factor $[\overline{C}_K^{\chi}]$ in the formula of the theorem as $[\varepsilon_\chi \overline{C}_K][\widehat{H}_\chi^0(G, \overline{C}_K)]$, w e concludethat there exists a rational number r', whose n umerator and denominator are divisible only by primes that divide e, such that

$$(9) \qquad (h_K/h_F)^{\varphi(e)} = r' \cdot \prod_{\chi\neq\chi^0} [\varepsilon_\chi \overline{C}_K].$$

For example, if G is a p-elementary abelian group for some prime p, then (9) is an identity of the type

$$(h_K/h_F)^{p-1} = p^t \cdot \prod_{\chi\neq\chi^0} [\varepsilon_\chi \overline{C}_K],$$

where t is an integer which may be positive, negative or zero. When $p = 2$, the situation is particularly simple, since in this case there is no need to extend scalars ($R = \mathbb{Z}$). We have

Corollary 6.7: *Let K/F be a finite Galois extension of exponent 2. Then there exists an integer t such that*

$$h_K/h_F = 2^t \cdot \prod_{\chi\neq\chi^0} [\varepsilon_\chi C_K],$$

where the product extends over all non-trivial characters of G.

Regarding the formula of the corollary, the factors $[\varepsilon_\chi C_K]$ which appear on the right-hand side seem to be related to the class numbers of the various subextensions of K/F. See below.

Example (Cf. [27, Theorem 10.10, p. 191]): Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a biquadratic extension of the rational field, where d_1 and d_2 are squarefree integers. Let χ_j ($j = 1, 2, 3$) be the nontrivial characters of $G = \mathrm{Gal}(K/F)$, numbered so that $L_j = \mathrm{Fix}(\mathrm{Ker}\,\chi_j) = \mathbb{Q}(\sqrt{d_j})$, where $d_3 = d_1 d_2$. Write

$$\{1, \tau\} = \mathrm{Gal}(K/L_1), \quad \{1, \sigma\} = \mathrm{Gal}(K/L_2), \quad \{1, \sigma\tau\} = \mathrm{Gal}(K/L_3),$$

and set $\varepsilon_{\chi_j} = \varepsilon_j$ ($j = 1, 2, 3$). Then $\varepsilon_1 = (1-\sigma)(1+\tau)$, $\varepsilon_2 = (1-\tau)(1+\sigma)$ and $\varepsilon_3 = (1-\tau)(1-\sigma)$. We have $\varepsilon_1 C_K = (1-\sigma)N_{K/L_1} C_K$. Further, σ acts on $N_{K/L_1} C_K$ as multiplication by -1 since

$$(1+\sigma)N_{K/L_1} C_K = N_{L_1/\mathbb{Q}} N_{K/L_1} C_K = 0.$$

It follows that $[\varepsilon_1 C_K]$ differs from $h_1 \overset{\text{def}}{=} [C_{L_1}]$ by a power of 2. Similarly, $[\varepsilon_2 C_K]$ differs from $h_2 = [C_{L_2}]$ by a power of 2. On the other hand, $\varepsilon_3 C_K = (1-\tau)(1+\sigma\tau)C_K = (1-\tau)N_{K/L_3} C_K$, and we conclude as before that $[\varepsilon_3 C_K]$ differs from $h_3 = [C_{L_3}]$ by a power of 2. Summarizing, there exists an integer t such that

$$h_K = 2^t \cdot h_1 h_2 h_3.$$

Remarks: (a) The formula of the example is not new. A precise version of it [7, Theorem 74, p. 320] follows from the classical Brauer relations [7, Theorem 73, p. 315]. More generally, if K/F is any Galois extension of number fields of type $(2,2)$, F. Lemmermeyer [14] has obtained a formula of the type

$$h_K = 2^t h_1 h_2 h_3 / h_F^2,$$

where t is an integer whose precise value is given in [14, p. 247]. Lemmermeyer's formula has been recently generalized by B. de Smit [6], who used a certain "Brauer relation" to obtain the following result. Let K/F be a finite abelian extension of number fields with Galois group $G \simeq (\mathbb{Z}/p\mathbb{Z})^m$, where p is a prime and $m \geq 2$. Then there exists an integer t such that

$$h_K h_F^{g-1} = p^t \prod_{[L:F]=p} h_L, \tag{10}$$

where $g = (p^m - 1)/(p-1)$ is the number of subgroups of G of index p (for the precise value of t, see [6, p. 140]). Note that the preceding formula may be written as

$$h_K/h_F = p^t \prod_{[L:F]=p} (h_L/h_F),$$

so it seems likely that (10) may also be obtained by repeated application of Theorem 6.6 above. When $F = \mathbb{Q}$, (10) has the following interesting consequence: a prime $q \neq p$ divides h_K if and only if q divides h_L for some subextension $L/\mathbb{Q}$ of $K/\mathbb{Q}$ of degree p.

(b) As mentioned earlier, the factors $[\overline{C}_K^{\chi}]$ intervening in the formula of Theorem 6.6 appear to be related to the class numbers of the various subextensions of K/F. Further, the actual computation of $[\overline{C}_K^{\chi}]$ in terms of class numbers of subextensions of K/F seems to be a problem in linear algebra. For example, if τ is a fixed generator of G and χ is given by $\chi(\tau) = \zeta_n$, then there exists a natural isomorphism

$$\overline{C}_K^{\chi} \simeq \{\mathbf{m} \in C_K^{\varphi(n)} \colon \tau\mathbf{m} = A\mathbf{m}\},$$

where A is the **companion matrix**[4] of the n-th cyclotomic polynomial $\Phi_n(x)$ (this follows from (8)). However, we do not yet know if $\overline{C}_K^{\chi^i}$ $(2 \leq i \leq n-1)$ admits a similar description. In any case, it seems likely that the identity

$$N_{K/L} = \prod_{\substack{d \mid [K:L] \\ d>1}} \Phi_d(\tau^{[L:F]})$$

[4] Or the **transpose** of the companion matrix, depending upon which definition of "companion matrix" one adopts.

will play a role in the computation of $[\overline{C}_K^{\chi^i}]$ in terms of the class numbers of the various subextensions of K/F.

(c) Let p be an odd prime and let $K = \mathbb{Q}(\zeta_p)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_p)$. Let h^+ be the class number of K. Then formula (9) (for $F = \mathbb{Q}$) is

$$(h^+)^{\varphi(\frac{p-1}{2})} = r' \cdot \prod_{\chi \neq \chi^0} [\varepsilon_\chi \overline{C}_K],$$

where r' is a rational number whose numerator and denominator are divisible only by primes that divide $(p-1)/2$. In particular, p divides h^+ if and only if p divides $[\varepsilon_\chi \overline{C}_K]$ for some (non-trivial) character χ of G, i.e., Vandiver's conjecture holds for p if and only if p does not divide $[\varepsilon_\chi \overline{C}_K]$ for every non-trivial character χ of G. Regarding this well-known conjecture, the results of this paper seem to indicate that the following statement is true: p does not divide h^+ if and only if p does not divide h_L for every subextension $L/\mathbb{Q}$ of $K/\mathbb{Q}$ of **prime** degree.

THEOREM 6.8: *Let K/F be a finite Galois extension of number fields with Galois group G such that every Sylow subgroup of G is either cyclic or generalized quaternion. Assume, in addition, that the following conditions hold for each subextension L/F of K/F of prime index.*

(a) *K/L is ramified at some prime, and*

(b) *$\text{b}^1(H, U_K) = \text{Ш}^2(H, U_K) = 0$, where $H = \text{Gal}(K/L)$.*

Then the G-module C_K is cohomologically trivial.

Proof: Hypothesis (a) implies that $K \cap \mathcal{H}_L = L$, where $\mathcal{H}_L$ is the Hilbert class field of L. Now a well-known consequence of class field theory [12, Lemma on p. 83] shows that the canonical map $C_K \to C_L, \{\mathfrak{a}\} \mapsto \{N_{K/L}\mathfrak{a}\}$, is surjective. On the other hand, by Corollary 6.4, hypothesis (b) implies that the natural map $C_L \to C_K^H$ is surjective. We conclude that the norm map $N_{K/L}\colon C_K \to C_K^H$ is surjective, i.e., $\widehat{H}^0(H, C_K) = 0$. The theorem now follows from Corollary 4.5. ∎

Remarks: (a) Condition (a) of the theorem holds if K/F is ramified at some prime and its Galois group is cyclic of p-power order, where p is a prime. Indeed, let v be a prime of F having a nontrivial inertia group $I(v, K/F)$. Then $I(v, K/F)$ contains $\text{Gal}(K/L)$, where L/F is the unique subextension of K/F of index p. It follows that K/L ramifies at a prime of L lying above v.

(b) Regarding condition (b) of the theorem, see Remark (c) following the statement of Corollary 6.5.

Appendix

In this Appendix we use étale cohomology to establish certain variants of Corollary 6.3 above. See Theorem A.4 and Corollary A.5 below.

We keep the notations introduced in Section 6. In particular, K/F is a finite Galois extension of number fields with Galois group G and, for each prime v of F, w is a fixed prime of K lying above v. We will also need the following notations: S will denote the set of primes of F formed by collecting together the archimedean primes of F and the primes that ramify in K/F, S_K will denote the set of primes of K lying above the primes in S and, for any prime v of F, n_v will denote the local degree $[K_w\colon F_v]$. Further, we will write N_S for the **least common multiple** of the integers n_v $(v \in S)$. The notations $\mathcal{O}_{F,S}$, $U_{F,S}$, $C_{F,S}$ and $h_{F,S}$ will refer to the ring of S-integers, the group of S-units, the S-ideal class group and the S-class number of F, respectively. When $S = S_\infty$, i.e., when K/F is unramified at all finite primes of F, we have $\mathcal{O}_{F,S} = \mathcal{O}_F$, $U_{F,S} = U_F$, $C_{F,S} = C_F$ and $N_S = 2^{\min(1, r_\infty(K/F))}$, where $r_\infty(K/F)$ denotes the number of real primes of F which ramify in K/F.

We begin by observing that the natural map $\operatorname{Spec}\mathcal{O}_{K,S_K} \to \operatorname{Spec}\mathcal{O}_{F,S}$ is a finite, étale and surjective morphism of degree $[K\colon F]$, i.e., it is a Galois covering with Galois group G. Now the Hochschild–Serre spectral sequence in étale cohomology

$$H^p(G, H^q_{\text{ét}}(\operatorname{Spec}\mathcal{O}_{K,S_K}, \mathbb{G}_m)) \Longrightarrow H^{p+q}_{\text{ét}}(\operatorname{Spec}\mathcal{O}_{F,S}, \mathbb{G}_m),$$

where $\mathbb{G}_m$ is the multiplicative group scheme, gives rise to the following exact sequence of finite groups, known as the **Picard–Brauer exact sequence**:

(11)
$$\begin{aligned}0 &\to H^1(G, U_{K,S_K}) \to C_{F,S} \to C_{K,S_K}^G \to H^2(G, U_{K,S_K}) \to \mathrm{B}(\mathcal{O}_{F,S}, \mathcal{O}_{K,S_K})\\ &\to H^1(G, C_{K,S_K}) \to H^3(G, U_{K,S_K}),\end{aligned}$$

where

$$\mathrm{B}(\mathcal{O}_{F,S}, \mathcal{O}_{K,S_K}) = \operatorname{Ker}[\operatorname{Br}(\mathcal{O}_{F,S}) \to \operatorname{Br}(\mathcal{O}_{K,S_K})^G].$$

See [18, p. 309] and [16, Proposition II.2.1, p. 201], and note that we have identified $\operatorname{Pic}(\mathcal{O}_{F,S})$ and $\operatorname{Pic}(\mathcal{O}_{K,S_K})$ with $C_{F,S}$ and C_{K,S_K}, respectively (cf. [11, Example II.6.3.2, p. 132, and Corollary II.6.16, p. 145]).

Lemma A.1: *We have*

$$[\mathrm{B}(\mathcal{O}_{F,S}, \mathcal{O}_{K,S_K})] = \frac{1}{N_S}\prod_{v\in S} n_v,$$

where N_S is the least common multiple of the integers n_v $(v \in S)$.

Proof: By [16, Proposition II.2.1, p. 201] and "semilocal theory" [4, §2.1] (see also [26, §11, (7), p. 194]), there exists an exact commutativ e diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Br}\,(\mathcal{O}_{F,S}) \arrow[r] \arrow[d] & \bigoplus_{v\in S} \mathrm{Br}(F_v) \arrow[r, "\sum \mathrm{inv}_v"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[d] \\
0 \arrow[r] & \mathrm{Br}(\mathcal{O}_{K,S_K})^G \arrow[r] & \bigoplus_{v\in S} \mathrm{Br}(K_w)^{G_w} \arrow[r, "\sum \mathrm{inv}_w"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Consequently, $\mathrm{B}(\mathcal{O}_{F,S}, \mathcal{O}_{K,S_K})$ is isomorphic to the kernel of the map

$$\sum \mathrm{in\,v}_v : \bigoplus_{v\in S} H^2(G_w, K_w^*) \to \mathbb{Q}/\mathbb{Z}$$

(see [23, Corollary, p. 156]). On the other hand, local class field theory allows us to identify the latter map with the summation map Σ: $\bigoplus_{v\in S} n_v^{-1}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$. Now [9, Lemma 1.2] completes the proof. ∎

Proposition A.2: *Let K/F be a finite Galois extension of number fields with Galois group G. Assume that K/F is unramified at all finite primes of F. Then there exists a natural exact sequence of finite groups*

$$0 \to H^1(G, U_K) \to C_F \to C_K^G \to H^2(G, U_K) \to \mathrm{B}(\mathcal{O}_F, \mathcal{O}_K),$$

in which $\mathrm{B}(\mathcal{O}_F, \mathcal{O}_K)$ is a group of order $2^{\max\,(0, r_\infty(K/F)-1)}$, where $r_\infty(K/F)$ denotes the number of real primes of F which ramify in K/F. In particular, if at most one real prime of F ramifies in K/F, then there exists a natural exact sequence[5]

$$0 \to H^1(G, U_K) \to C_F \to C_K^G \to H^2(G, U_K) \to 0.$$

Proof: This follows by setting $S = S_\infty$ in (11) and using Lemma A.1. ∎

Corollary A.3: *Let F be a number field and let K be the Hilbert class field of F. Write $G = \mathrm{Gal}(K/F)$. Then there exist canonical isomorphisms*

$$C_F = H^1(G, U_K) \quad \textit{and} \quad C_K^G = H^2(G, U_K).$$

Proof: As already noted (cf. Remark (b) following the statement of Corollary 6.5), the Principal Ideal Theorem [19, Theorem 8.6, p. 107] implies that the natural map $C_F \to C_K^G$ is zero. The result is now immediate from the proposition. ∎

[5] Cf. Remark (b) following the statement of Corollary 6.5.

Theorem A.4: *Let K/F be a cyclic Galois extension of number fields with Galois group G of order n. Then there exists an integer d, which divides the order of $H^1(G, C_{K,S_K})$, such that*

$$(n/N_S) \cdot [C_{K,S_K}^G] = d \cdot h_{F,S}.$$

Proof: This follows at once from Lemma A.1 and the exactness of (11), using the fact that the Herbrand quotient of U_{K,S_K} equals $(1/n)\prod_{v \in S} n_v$ (see, for example, [19, Theorem 1.3, p. 74]). ∎

Corollary A.5: *Let K/F be a cyclic Galois extension of number fields with Galois group G of order n. Assume that K/F is unramified at all finite primes of F. Then there exists an integer d, which divides the order of $\widehat{H}^0(G, C_K)$, such that*

$$n \cdot [C_K^G] = d \cdot 2^{\min\ (1,r_\infty(K/F))} h_F.$$

In particular, if $\widehat{H}^0(G, C_K) = 0$ (cf. Theorem 6.8), then

$$n \cdot [C_K^G] = 2^{\min(1,r_\infty(K/F))} h_F. \qquad ∎$$

References

[1] E. Aljadeff, *On the surjectivity of some trace maps*, Israel Journal of Mathematics **86** (1994), 221–232.

[2] E. Aljadeff and Y. Ginosar, *Induction from elementary abelian subgroups*, Journal of Algebra **179** (1996), 599–606.

[3] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, 1956.

[4] C. Chamfy, *Modules semi-locaux*, in *Cohomologie Galoisienne des Modules Finis* (Sém. Poitou), Dunod, Paris, 1967.

[5] L. Chouinard, *Projectivity and relative projectivity over rings*, Journal of Pure and Applied Algebra **7** (1976), 287–302.

[6] B. de Smit, *Brauer–Kuroda relations for S-class numbers*, Acta Arithmetica **98** (2001), 133–146.

[7] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, 1991.

[8] C. D. Gonzalez-Avilés, *On Tate–Shafarevich groups of abelian varieties*, Proceedings of the American Mathematical Society **128** (2000), 953–961.

[9] C. D. Gonzalez-Avilés, *Brauer groups and Tate–Shafarevich groups*, Journal of Mathematical Sciences of the University of Tokyo **10** (2003), 391–419.

[10] C. D. Gonzalez-Avilés, *Brauer groups and Tate–Shafarevich groups, II*, Available from http://arxiv.org/abs/math.NT/0306231 (submitted).

[11] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, Berlin, 1977.

[12] S. Lang, *Introduction to Cyclotomic Fields*, Springer-Verlag, Berlin, 1978.

[13] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1986.

[14] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arithmetica **66** (1994), 245–260.

[15] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inventiones Mathematicae **18** (1972), 183–266.

[16] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Mathematics, Vol. 1, Academic Press, Orlando, 1986.

[17] J. S. Milne, *On the arithmetic of abelian varieties*, Inventiones Mathematicae **17** (1972), 177–190.

[18] J. S. Milne, *Étale Cohomology*, Princeton University Press, Princeton, N.J., 1980.

[19] J. Neukirch, *Class Field Theory*, Springer-Verlag, Berlin–New York–Tokyo, 1986.

[20] B. Poonen, *The class group of a number field is the Tate–Shafarevich group of the units*, Unpublished typescript.

[21] J. S. Rose, *A Course on Group Theory*, Cambridge University Press, Cambridge, 1978.

[22] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, Journal für die reine und angewandte Mathematik **327** (1981), 12–80.

[23] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, Vol. 67, Springer-Verlag, New York, 1979.

[24] S. Shatz, *Profinite Groups, Arithmetic, and Geometry*, Annals of Mathematics Studies, Vol. 67, Princeton University Press, Princeton, 1972.

[25] J. Tate, *WC-groups over $\mathfrak{p}$-adic fields*, Séminaire Bourbaki, Exposé **156** (1957/58).

[26] J. Tate, *Global Class Field Theory*, in *Algebraic Number Theory* (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, London, 1967, pp. 162–203.

[27] L. Washington, *Introduction to Cyclotomic Fields*, 2nd Edition, Springer-Verlag, Berlin, 1997.

[28] Yu. Zarhin, *Néron pairings and quasicharacters*, Mathematics of the USSR-Izvestiya **6** (1972), no. 3, 491–503.

[29] H. J. Zassenhaus, *The Theory of Groups*, 2nd Edition, Chelsea, New York, 1958.