Journal of Pure and Applied Algebra 38 (1985) 39-63
North-Holland

A GENERALIZATION OF THE NORM RESIDUE SYMBOL

Stephen U. CHASE
Cornell University, Ithaca, NY 14853, USA

Communicated by A. Heller
Received 29 July 1983

Let k be a field containing n distinct n-th roots of 1, where n is a natural number relatively prime to the characteristic of k. The norm residue symbol (of degree n) is a homomorphism

$$\{\cdot,\cdot\}_n : k^* \otimes_{\mathbb{Z}} k^* \to \mathrm{Br}(k)_n \otimes_{\mathbb{Z}} \mu_n$$
$$a \otimes b \mapsto \{a,b\}_n$$

where k^* is the multiplicative group of k, $\mathrm{Br}(k)_n$ is the n-torsion subgroup of the Brauer group $\mathrm{Br}(k)$ of k, and μ_n is the cyclic group of order n consisting of all n-th roots of 1 in k. If k is a local field, then $\{\cdot,\cdot\}_n$ can be used together with the Hasse invariant isomorphism

$$\mathrm{Inv}_k : \mathrm{Br}(k) \xrightarrow{\approx} \mathbb{Q}/\mathbb{Z}$$

to construct the classical norm residue symbol (or 'local symbol')

$$(\cdot,\cdot)_n : k^* \otimes_{\mathbb{Z}} k^* \to \mu_n$$

for such fields, which is of great importance in local class field theory.

The norm residue symbol $\{\cdot,\cdot\}_n$ is often defined in terms of a more general pairing $\langle\cdot,\cdot\rangle_n$ into $\mathrm{Br}(k)_n$ for which the assumptions on k and n introduced above are unnecessary; see, e.g., Serre [16, p. 204]. This pairing is briefly reviewed in Section 1. If k and n satisfy the above hypotheses, then the norm residue symbol arises upon interpreting one of the terms in the pairing $\langle\cdot,\cdot\rangle_n$ by means of Kummer theory.

The purpose of this paper is to use, in just the same way, the generalized Kummer theory of the author and others to produce more general norm residue symbols which are meaningful without the presence of all n-th roots of 1 in the ground field k. Such considerations seem timely for two reasons. Merkur'ev and Suslin [13,14] have recently determined the image and kernel of the homomorphism $\{\cdot,\cdot\}_n$ for any field containing all n-th roots of 1, and it is natural to ask whether this deep and elegant theorem permits an extension to more general fields. In addition, our approach to the norm residue symbol leads to certain explicit formulae which are to some extent suggestive of the classical Stickelberger relations for the ideal class group of a cyclotomic field; see, e.g., Washington [18, Theorem 6.10, p. 94]. These relations and their variants have recently appeared also in the theory of Galois module structure of the ring of integers in a number field (Fröhlich [10], McCulloh [12], Childs [7]). The general norm residue symbols thus provide further evidence of the apparent ubiquity of these formulae in much of field theory and arithmetic.

In Section 2 we review the requisite Kummer theory and adapt it slightly to our purpose; for further details and generalizations see Chase [4,5], Waterhouse [19], or Takeuchi [17]. In Section 4 we apply it to obtain our norm residue symbols, which are homomorphisms

$$\{\cdot,\cdot\}_n : \mathrm{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)\otimes_{\mathbb{Z}} k^* \to \mathrm{Br}(k)_n \otimes_{\mathbb{Z}} \mu_n,$$

$$(\cdot,\cdot)_n : \mathrm{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)\otimes_{\mathbb{Z}} k^* \to \mu_n.$$

The first is defined for any field of characteristic prime to the given natural number n; the second for a local field satisfying these conditions. Here μ_n is the group of all n-th roots of 1 in a separable closure of k, $L=k(\mu_n)$, and Δ is the Galois group of the cyclotomic extension L/k. $(\mathbb{Z}/n\mathbb{Z})^t = \mathbb{Z}/n\mathbb{Z}$ viewed as a $\mathbb{Z}\Delta$-module via the canonical homomorphism $t:\Delta\to(\mathbb{Z}/n\mathbb{Z})^*$.

We shall interpret the elements of $\mathrm{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)$ as equivalence classes of $\mathbb{Z}\Delta$-module extensions

$$\xi:\quad 1\to L^*\to E\to(\mathbb{Z}/n\mathbb{Z})^t\to 1$$

as in, e.g., MacClane [11, Ch. III]. Since the $\mathbb{Z}\Delta$-module $(\mathbb{Z}/n\mathbb{Z})^t$ is a cyclic group, one can easily compute with such extensions much as one does with ordinary group extensions with cyclic factor group [11, pp. 109–110]. In Section 3 we obtain two simple and computable invariants of an extension ξ as above, describe how they behave with respect to equivalence of extensions, and show that they determine the class of ξ in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)$. In Section 4 we use these invariants to obtain explicit formulae for $\{\mathrm{cl}(\xi), b\}_n$ and $(\mathrm{cl}(\xi), b)_n$ (b in k^*), expressing the latter in terms of the reciprocity map for the local field k. These formulae generalize well-known expressions for the usual norm residue symbols.

It is in certain equations satisfied by the above-mentioned invariants of the extension ξ that terms reminiscent of the Stickelberger relations appear. In Section 3 we briefly discuss these phenomena and the connection between our invariants and the 'Stickelberger cohomology' of Fröhlich [10, §5] and Childs [8].

Throughout this paper all rings will have identity elements which act as such on all modules. The multiplicative group of a ring R (i.e., the group of invertible elements of R under multiplication) will be denoted by R^*. If V is a vector space of finite dimension over a field k, then that dimension will be witten $[V:k]$. If G is a group and H is a subgroup of G of finite index, then that index will be written $[G:H]$; in particular, the order of a finite group G will be written $[G:1]$.

We shall have use for Galois theory not only of fields but also of commutative rings (our ground ring will always be a field, but some of the Galois extensions of it need not be). For the basic definitions and facts regarding the Galois theory of rings see DeMeyer–Ingraham [9, Ch. III] or Chase–Harrison–Rosenberg [3]. For information on local fields see Cassels–Fröhlich [2, Chs. I and VI] or Serre [16].

1. The canonical pairing

Let k be a field, and let

$$\Omega = \mathrm{Gal}(k^s/k)$$

be the Galois group of a given fixed separable closure of k.

We shall view Ω as a topological group in the usual (Krull) topology. If J is a finite abelian group, we denote by

$$\mathrm{Hom}_c(\Omega, J)$$

the abelian group of continuous homomorphisms of Ω into J, where J is given the discrete topology. Of course, a homomorphism $\chi : \Omega \to J$ is continuous if and only if the kernel of χ is an open subgroup of Ω.

Now let n be a natural number greater than one. The usual norm residue symbol arises from the 'canonical pairing':

$$\langle \cdot, \cdot \rangle_n : \mathrm{Hom}_c\left(\Omega, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right) \otimes_{\mathbb{Z}} k^* \to \mathrm{Br}(k)_n \tag{1.1}$$

with $\mathrm{Br}(k)_n$ the n-torsion subgroup of the Brauer group of k.

A cohomological definition of this pairing is provided in [16, p. 204]; we shall give a direct construction in terms of cyclic algebras, as in [20, Corollary 3, p. 223]. Given χ in $\mathrm{Hom}_c(\Omega, (1/n)\mathbb{Z}/\mathbb{Z})$, we set

$$K = (k^s)^{\mathrm{Ker}(\chi)} \subseteq k^s.$$

By the definition of the topology on Ω, K is a finite Galois extension of k, and we obtain a commutative diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\ \chi\ } & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\ & \searrow & \uparrow{\scriptstyle i} \\ & & \Gamma = \mathrm{Gal}(K/k) \end{array}$$

with i injective and the unlabeled arrow denoting the canonical surjection. Hence $\mathrm{Im}(\chi) = \mathrm{Im}(i) = (1/d)\mathbb{Z}/\mathbb{Z}$ for some d dividing n, and so Γ is cyclic of order d with distinguished generator σ, say, where $i(\sigma) = (1/d) + \mathbb{Z}$.

If a is in k^*, we now define $K\langle a \rangle$ to be the cyclic k-algebra constructed using the element a and the generator σ of Γ [15, pp. 259–262]. That is, as a left K-space $K\langle a \rangle$ has basis $\{1, u, u^2, \dots, u^{d-1}\}$, with the multiplication in $K\langle a \rangle$ defined by the formula

$$(xu^i)(yu^j)=x\sigma^i(y)a^q u^r \tag{1.2}$$

where x, y are in K and

$$i+j=dq+r, \quad 0\le r<d.$$

In particular, $u^d=a$ and $uxu^{-1}=\sigma(x)$ for all x in K. We then set

$$\langle\chi, a\rangle_n=\mathrm{cl}(K\langle a\rangle) \tag{1.3}$$

in $\mathrm{Br}(k)_n$, where 'cl' denotes the equivalence class of $K\langle a\rangle$ in the Brauer group of k. The mapping $\langle\cdot,\cdot\rangle_n$ is bimultiplicative, and hence yields a homomorphism (1.1) of abelian groups.

For the special case in which k is a local field, we obtain the classical canonical pairing for local fields

$$[\cdot,\cdot]_n:\mathrm{Hom_c}\left(\Omega, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)\otimes_{\mathbb{Z}} k^*\to\frac{1}{n}\mathbb{Z}/\mathbb{Z} \tag{1.4}$$

[20, Corollary 3, p. 223] by composing $\langle\cdot,\cdot\rangle_n$ with the 'Hasse invariant' isomorphism

$$\mathrm{Inv}_k:\mathrm{Br}(k)_n\xrightarrow{\approx}\frac{1}{n}\mathbb{Z}/\mathbb{Z} \tag{1.5}$$

[15, Theorem (31.8), p. 266]. That is, if χ and a are as above, then

$$[\chi, a]_n=\mathrm{Inv}_k(\langle\chi, a\rangle_n). \tag{1.6}$$

This pairing can be succinctly described in terms of the reciprocity (or Artin) map of k; see, e.g., [2, Proposition 1, p. 140] or [16, Proposition 3, p. 205].

Theorem 1.7. *Let*

$$k^*\to\Omega^{\mathrm{ab}} \quad \textit{where } a\mapsto(a,k)$$

denote the reciprocity map of the local field k. Then

$$[\chi, a]_n=\chi((a,k))$$

for χ in $\mathrm{Hom_c}(\Omega,(1/n)\mathbb{Z}/\mathbb{Z})$ and a in k^*.

2. Recycling Kummer theory

The version of the norm residue symbol introduced in this paper arises from the canonical pairing of Section 1 upon interpretation of one of the terms in that pairing in the light of the generalized Kummer theory of [5, particularly Corollary 17.19, p. 126]. In this section we review the latter and make some related remarks.

Given $k\subseteq k^s$ and Ω as in Section 1, let n be a natural number greater than one and relatively prime to the characteristic of k, and

$$\mu_n = \{\zeta \text{ in } k^s \mid \zeta^n = 1\}.$$

Then μ_n is a cylic subgroup of $(k^s)^*$ of order n, and

$$L = k(\mu_n) \subseteq k^s$$

is a finite Galois field extension of k. Setting

$$\Delta = \mathrm{Gal}(L/k)$$

we have a unique mapping

$$t : \Delta \to \mathbb{Z}$$

satisfying the conditions that

$$0 < t(\delta) < n \tag{2.1a}$$

and

$$\delta(\zeta) = \zeta^{t(\delta)} \tag{2.1b}$$

for all ζ in μ_n. The composition of t with the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ then has image in $(\mathbb{Z}/n\mathbb{Z})^*$ and yields an injection

$$\Delta \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

of groups which we also denote by t.

Restriction of elements of Ω to the subfield L of k^s yields a continuous surjection

$$\Omega \to \Delta. \tag{2.2}$$

The kernel Ω_L of this surjection is then an open subgroup of Ω of finite index, and in fact

$$\Omega_L = \mathrm{Gal}(k^s/L), \qquad L = (k^s)^{\Omega_L}.$$

The theorem below provides the formulation of Kummer theory that we shall use; it is simply [5, Corollary 17.19, p. 126] (see also [4, (2), p. 11].) For more general theorems involving finite k-group schemes see, e.g. [5, Theorem 16.14, p. 109], [4, (1), p. 10], [19, Theorem 2, p. 183], and [17, Theorem 4.3, pp. 1468–1469].

Theorem 2.3. *Let J be a finite abelian group of exponent n, and let $\hat{J}$ denote the $\mathbb{Z}\Delta$-module*

$$\hat{J} = \mathrm{Hom}_{\mathbb{Z}}(J, \mu_n).$$

Then there is an isomorphism

$$\mathrm{Hom}_c(\Omega, J) \xrightarrow{\cong} \mathrm{Ext}^1_{\mathbb{Z}\Delta}(\hat{J}, L^*)$$

of abelian groups.

We shall review the concepts necessary to define this isomorphism (for further discussion see [4], [5, §§16–17, pp. 103–126]). To this end it will be convenient to write J multiplicatively.

Given χ in $\mathrm{Hom}_c(\Omega, J)$, we first construct an Ω-J-set $J(\chi)$ as follows (an Ω-J-set being a set equipped with an operation of Ω from the left and an operation of J from the right such that the usual associative law holds). Namely, we set

$$J(\chi)=J \tag{2.4a}$$

as a right J-set, with Ω-action defined by

$$\omega\cdot\sigma=\chi(\omega)\sigma \tag{2.4b}$$

for ω in Ω, σ in J. $J(\chi)$ then gives rise to a commutative k-algebra

$$K(\chi)=(J(\chi),k^s)^\Omega \tag{2.5a}$$

where, if X and Y are Ω-sets, $(X,Y)^\Omega$ denotes the set of all Ω-equivariant mappings from X to Y. The k-algebra structure on $K(\chi)$ arises from that of k^s. Moreover, the right action of J on $J(\chi)$ yields an operation of J on $K(\chi)$ by k-algebra automorphisms; namely

$$\sigma(\alpha)(\tau)=\alpha(\tau\sigma) \tag{2.5b}$$

for α in $K(\chi)$ and σ,τ in J. The techniques of Galois theory show that $K(\chi)$ is a Galois (ring) extension of k with Galois group J (called a 'Galois Jk-object' in [4], [5]).

Suppose now that K is a Galois extension of k with Galois group J (e.g., $K=K(\chi)$ as above). The k-algebra $K\otimes_k L$ is then a Galois extension of k with Galois group $J\times\Delta$, where J operates on the left factor and Δ on the right. If we ignore the action of Δ, then the L-algebra $K\otimes_k L$ is a Galois extension of L with Galois group J, and we define

$$E(K/k)=\{x \text{ in } (K\otimes_k L)^* \mid x^{-1}\sigma(x) \text{ is in } L^* \text{ for all } \sigma \text{ in } J\}. \tag{2.6}$$

$E(K/k)$ is a $\mathbb{Z}\Delta$-submodule of $(K\otimes_k L)^*$. Moreover, if x is in $E(K/k)$, then

$$\psi_x : J\to L^* \tag{2.7a}$$

where

$$\psi_x(\sigma)=x^{-1}\sigma(x) \qquad (\sigma \text{ in } J) \tag{2.7b}$$

is a homomorphism of groups, and since J has exponent n it follows that $\mathrm{Im}(\psi_x)\subseteq \mu_n\subseteq L^*$ and ψ_x is in $\hat{J}$. We then obtain an extension of $\mathbb{Z}\Delta$-modules

$$\xi_{K/k}:\quad 1\to L^*\to E(K/k)\to\hat{J}\to 1 \tag{2.8}$$

with the two non-trivial homomorphisms in the extension the inclusion map and

$$x\to\psi_x \qquad (x \text{ in } E(K/k))$$

respectively. In fact, it is easy to see that the mapping

$$\psi\to(\alpha\mid\psi)$$

yields a Δ-equivariant (set-theoretic) section

$$\hat{J} \to E(K/k)$$

of $\xi_{K/k}$, where α is a normal basis element of K [3, Theorem 4.2, pp. 27–28] and $(\alpha \mid \psi)$ is the 'Lagrange resolvent'

$$(\alpha \mid \psi) = \sum_{\sigma \text{ in } J} \psi(\sigma)\sigma^{-1}(\alpha)$$

[10, (3.5), p. 600]. We then have

(2.9) The isomorphism of Theorem 2.3 maps χ in $\mathrm{Hom}_c(\Omega, J)$ to $\mathrm{cl}(\xi_{K/k})$ in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\hat{J}, L^*)$, where $K = K(\chi)$ is as in (2.5a) and 'cl' denotes the equivalence class of the extension $\xi_{K/k}$.

The definition of the isomorphism of (2.3) thus interposes two intermediate constructions. If χ in $\mathrm{Hom}_c(\Omega, J)$ corresponds under this isomorphism to $\mathrm{cl}(\xi)$ in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$, then one has the above described Galois extension $K = K(\chi)$ of k with Galois group J, as well as the Ω-J-set $X = J(\chi)$ of (2.4) which is isomorphic to J as a right J-set. It will be convenient to label K the 'Galois extension of k associated to $\mathrm{cl}(\xi)$ (or to χ)'; it is uniquely determined up to k-algebra isomorphism which preserves the action of J. Galois theory again provdes a direct description of the Ω-J-set X in terms of K; namely

$$X = \mathrm{Alg}_k(K, k^s). \tag{2.10}$$

That is, X is the set of all k-algebra homomorphisms of K into k^s, the action of Ω and J on X arising from that on k^s and K, respectively. Moreover, (2.4b) yields a similar formula for χ in terms of X. Hence, in order to describe the isomorphism which is inverse to that of (2.3), it is necessary only to construct, from a $\mathbb{Z}\Delta$-module extension

$$\xi: \quad 1 \to L^* \to E \to \hat{J} \to 1 \tag{2.11}$$

the associated Galois extension K of k. Such a construction is implicit in the Hopf algebraic computations of [5, §16, pp. 103–115], but for our purposes it will be useful to obtain a somewhat different and more direct description.

It should be noted that χ can be obtained directly from $\mathrm{cl}(\xi)$ without using K; see, e.g., [19] for a group scheme theoretic version of this (in the context considered here such a description is given in Corollary 2.16(a) below). However, the Galois extension K will play its own role in our discussion of the norm residue symbol. [19] also provides elegant geometric constructions of ξ and the affine k-scheme of K, each in terms of the other.

Recall first that an *autmorphism* of the module extension ξ of (2.11) is an automorphism of the $\mathbb{Z}\Delta$-module E such that the diagram below commutes:

$$\begin{array}{lccccccccc}
\xi: & 1 & \longrightarrow & L^* & \longrightarrow & E & \longrightarrow & \hat{J} & \longrightarrow & 1 \\
 & & & \| & & \approx\downarrow & & \| & & \\
\xi: & 1 & \longrightarrow & L^* & \longrightarrow & E & \longrightarrow & \hat{J} & \longrightarrow & 1
\end{array}$$

The automorphisms of ξ form a group $\mathrm{Aut}(\xi)$ and we have an isomorphism

$$J \xrightarrow{\approx} \mathrm{Aut}(\xi) \tag{2.12a}$$

which is defined to be the composite of the canonical isomorphisms

$$J \xrightarrow{\approx} \mathrm{Hom}_{\mathbb{Z}\Delta}(\hat{J}, \mu_n) = \mathrm{Hom}_{\mathbb{Z}\Delta}(\hat{J}, L^*) \xrightarrow{\approx} \mathrm{Aut}(\xi)$$

with the right-most arrow denoting the well-known isomorphism

$$h \mapsto \bar{h}.$$

That is, given h in $\mathrm{Hom}_{\mathbb{Z}\Delta}(\hat{J}, L^*)$, $\bar{h}: E \xrightarrow{\approx} E$ is defined by the formula

$$\bar{h}(x) = h(\psi)x$$

for x in E and ψ the image of x in $\hat{J}$. It is then easily checked that the isomorphism (2.12a) maps σ in J to the automorphism $\bar{\sigma}$ of ξ, where

$$\bar{\sigma}(x) = \psi(\sigma)x.$$

We shall identify J with $\mathrm{Aut}(\xi)$ via this isomorphism, and thus view E as a $\mathbb{Z}J$-module according to the formula

$$\sigma(x) = \psi(\sigma)x \tag{2.12b}$$

with, as above, σ in J, x in E, and ψ the image of x in $\hat{J}$.

Of course, since we are dealing with $\mathbb{Z}\Delta$-module extensions and automorphisms of such, the actions of Δ and J on E commute, and so E is a $\mathbb{Z}(\Delta \times J)$-module.

We now define I to be the L-subspace of the group algebra LE spanned by all elements of LE of the form

$$\langle xy \rangle - x\langle y \rangle \tag{2.13}$$

for x in L^*, y in E (to avoid ambiguity we denote by $\langle y \rangle$ the element of LE corresponding to y). Clearly I is an ideal of LE.

Proposition 2.14. *Let K be the Galois extension of k associated to the group extension ξ of* (2.11) (*hence we may assume $E = E(K/k)$ as in* (2.6)). *Then:*

(a) *The inclusion map $E \hookrightarrow (K \otimes_k L)^*$ extends to a* surjection

$$LE \to K \otimes_k L$$

of L-algebras and $\mathbb{Z}(J \times \Delta)$-modules (*the action of Δ on LE arising from that on* *both L and E). The kernel of this surjection is the ideal I of* (2.13), *and thus it yields an L-algebra and $\mathbb{Z}(J\times\Delta)$-module isomorphism*

$$LE/I \xrightarrow{\approx} K\otimes_k L.$$

(b) *Given any ψ in $\hat{J}$, there exists x_ψ in $(K\otimes_k L)^*$ such that*

$$\sigma(x_\psi)=\psi(\sigma)x_\psi$$

for all σ in J. If for each ψ in $\hat{J}$ we select such an x_ψ, then

$$\{x_\psi \mid \psi \text{ in } \hat{J}\}$$

is an L-basis of $K\otimes_k L$.

Proof. The mapping $LE\to K\otimes_k L$ of (a) is a homomorphism of L-algebras; that it is also a $\mathbb{Z}(J\times\Delta)$-module homomorphism follows easily from the definition of $E=E(K/k)$, the fact that E is a $\mathbb{Z}\Delta$-submodule of $(K\otimes_k L)^*$, and (2.12b). Moreover, if $\{x_\psi \mid \psi \text{ in } \hat{J})$ is a transversal of E modulo L^*, then the definition of I implies that the cosets modulo I of the elements $\langle x_\psi\rangle$ of LE span the L-space LE/I, and thus

$$[LE/I:L]\le[J:1]=[K\otimes_k L:L]. \tag{2.15}$$

Finally, given ψ in $\hat{J}$, we obtain from (2.6)–(2.8) that the elements of $(K\otimes_k L)^*$ which satisfy the equation of (b) are precisely the elements of $E=E(K/k)\subseteq(K\otimes_k L)^*$ which map to ψ under the canonical surjection $E\to\hat{J}$ of (2.8), and thus the first assertion of (b) holds.

Let us now assume for the moment that the elements of a subset $\{x_\psi \mid \psi \text{ in } \hat{J}\}$ as in (b) are linearly independent over L. Since $[K\otimes_k L:L]=[J:1]$, it follows that they form a basis of the L-space $K\otimes_k L$, thus completing the proof of (b). Moreover, since these elements are in E, we also obtain that the homomorphism of (a) is surjective, and the remainder of (a) then follows from the inequality (2.15).

That the elements x_ψ are L-linearly independent follows from routine Hopf algebraic arguments such as those outlined in [6, Example 1.6, pp. 156–157]. We avoid such techniques by the following artifice. Let F be the pure rational function field over L in the indeterminates $\{z_\sigma \mid \sigma \text{ in } J\}$; then we need only show that the elements $x_\psi\otimes_L 1$ in $(K\otimes_k L)\otimes_L F=K\otimes_k F$ are linearly independent over F. Now define an F-space endomorphism T of $K\otimes_k F$ by the formula

$$T(y)=\sum_{\sigma \text{ in } J} z_\sigma\sigma(y)$$

for y in $K\otimes_k F$ (the operation of J on $K\otimes_k L$ by L-algebra automorphisms being extended to an operation on $K\otimes_k F$ by F-algebra automorphisms). Then $x_\psi\otimes_L 1$ is an eigenvector for T corresponding to the eigenvalue

$$\lambda_\psi=\sum_{\sigma \text{ in } J} z_\sigma\psi(\sigma)$$

and, since the latter are all distinct for distinct ψ in $\hat{J}$, the linear independence of the elements x_ψ follows. This completes the proof of the proposition.

Corollary 2.16. *Let ξ, K, etc., be as in Proposition* 2.14, *and X be the Ω-J-set corresponding to K as in* (2.10).

(a) *There is a k-algebra and $\mathbb{Z}J$-module isomorphism*

$$(LE/I)^{\Delta} \xrightarrow{\approx} K$$

rendering the diagram below commutative:

$$\begin{array}{ccc} (LE/I)^{\Delta} & \xrightarrow{\approx} & K \\ \downarrow & & \downarrow \\ LE/I & \xrightarrow{\approx} & K\otimes_k L \end{array}$$

the lower horizontal arrow denoting the isomorphism of Proposition 2.14(a) *and the vertical arrows the inclusion maps.*

(b) *Let X' denote the set of all group homomorphisms*

$$E \to (k^s)^*$$

whose restrictions to L^* are the inclusion map $L^* \hookrightarrow (k^s)$. Then there is a bijection

$$X = \mathrm{Alg}_k(K, k^s) = \mathrm{Alg}_L(K\otimes_k L, k^s) \xrightarrow{\approx} X' \tag{2.17}$$

defined by $\phi \mapsto \phi'$ where ϕ' is the restriction of the L-algebra homomorphism

$$\phi : K\otimes_k L \to k^s$$

to the subset $E = E(K/k) \subseteq (K\otimes_k L)^*$. (2.17) *is an isomorphism of Ω-J-sets if we view ξ as an extension of $\mathbb{Z}\Omega$-modules via the surjection* (2.6) *and define the operation of Ω and J on X' by the formulae*

$$(\phi'\sigma)(u) = \phi'(\sigma(u)), \tag{2.18a}$$

$$(\omega\phi')(u) = \omega(\phi'(\omega^{-1}(u))) \tag{2.18b}$$

for ϕ', u, σ, ω in X', E, J, Ω, respectively.

Proof. (a) follows immediately from Proposition 2.14(a) and the fact that $(K\otimes_k L)^{\Delta} = K$. Moreover, Proposition 2.14(a) and the obvious bijection

$$\mathrm{Alg}_L(LE/I, k^s) \xrightarrow{\approx} X'$$

imply that the mapping (2.17) is similarly bijective, and it is thus an isomorphism of J-sets in view of the definition of the J-action on X (see the sentence following (2.10)). Thus we need only show that (2.17) is a mapping of Ω-sets.

At this point we confess that the identity

$$\text{"}\mathrm{Alg}_k(K, k^s) = \mathrm{Alg}_L(K \otimes_k L, k^s)\text{"}$$

appearing in (2.17) is a euphemism for the canonial bijection

$$\mathrm{Alg}_L(K \otimes_k L, k^s) \xrightarrow{\approx} \mathrm{Alg}_k(K, k^s)$$

arising from the restriction to K of L-algebra homomorphisms $K \otimes_k L \to k^s$. If ω is in Ω and ϕ is in X, define

$$\tilde{\phi} : K \otimes_k L \to k^s$$

by the formula

$$\tilde{\phi}(x) = \omega(\phi(\omega^{-1}(x)))$$

for x in $K \otimes_k L$. $\tilde{\phi}$ is in $\mathrm{Alg}_L(K \otimes_k L, k^s)$ and its restriction to K is $\omega\phi$ (keeping in mind that the Ω-action on $X = \mathrm{Alg}_k(K, k^s)$ arises from the action on k^s), and so $\omega\phi$ in X is identified with $\tilde{\phi}$ in $\mathrm{Alg}_L(K \otimes_k L, k^s)$. Comparing with (2.18b) then yields that the bijection (2.17) is an isomorphism of Ω-sets, completing the proof.

We shall identify X with X' via the isomorphism of (2.17), thus obtaining a description of X in terms of the corresponding $\mathbb{Z}\Delta$-module extension ξ of (2.11). There remains only to find a similar description of χ in $\mathrm{Hom}_c(\Omega, J)$ corresponding to $\mathrm{cl}(\xi)$ under the isomorphism of theorem 2.3. To this end it suffices to so describe the composition $\psi \cdot \chi : \Omega \to \mu_n$ for each ψ in $\hat{J}$.

Corollary 2.19. *Let*

$$\xi: \quad 1 \to L^* \to E \to \hat{J} \to 1$$

be a $\mathbb{Z}\Delta$-module extension, and let χ in $\mathrm{Hom}_c(\Omega, J)$ *map to* $\mathrm{cl}(\xi)$ *in* $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\hat{J}, L^*)$ *under the isomorphism of Theorem* 2.3. *Let*

$$\phi : E \to (k^s)^*$$

be any homomorphism of groups whose restriction to L^* is the inclusion map $L^* \hookrightarrow (k^s)^*$. Let u in E map to ψ in $\hat{J}$ under the surjection $E \to \hat{J}$ appearing in the definition of ξ. Then, for each ω in Ω

$$\psi(\chi(\omega)) = \phi(u)^{-1}\omega(\phi(\omega^{-1}(u)))$$

in $\mu_n \subseteq (k^s)^*$, with ξ viewed as an extension of $\mathbb{Z}\Omega$-modules via the surjection (2.2).

Proof. Let X be the Ω-J-set corresponding to χ and ξ; i.e., $X = J(\chi)$ as in (2.4). Then, by Corollary 2.16 and the identification introduced above, ϕ is an element of X; moreover, by (2.18b),

$$(\omega\phi)(u) = \omega(\phi(\omega^{-1}(u)))$$

for all ω in Ω and u in E. But also, by (2.4),

$$\omega\phi = \phi\chi(\omega)$$

in X. Hence, by (2.18a) and (2.12b),

$$\omega(\phi(\omega^{-1}(u))) = \phi(\chi(\omega)(u)) = \phi(\psi(\chi(\omega))u) = \psi(\chi(\omega))\phi(u)$$

in $(k^s)^*$ with ψ as above, the final equality holding because $\psi(\chi(\omega))$ is in $\mu_n \subseteq L^*$ and $\phi(z) = z$ for all z in L^*. The corollary follows.

Remarks 2.20. The approach outlined in this section yields, after a bit more work, a direct proof of Theorem 2.3 which avoids the group scheme methods of [5].

3. Extensions of cyclic modules

We wish to apply the observations of Section 2 to the special case in which the abelian group J is $\mathbb{Z}/n\mathbb{Z}$. Then $\hat{J} \approx \mu_n \subseteq L^*$, and so Theorem 2.3 provides an isomorphism

$$\mathrm{Hom}_c(\Omega, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\approx} \mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$$

which is crucial in our definition of the norm residue symbol.

It is then desirable to describe the $\mathbb{Z}\Delta$-module extensions of μ_n by L^* in terms of concrete data much as one does for ordinary group extensions with cyclic factor group. It will be convenient and no more difficult to work in a somewhat more general context.

Let Δ be a group, n be a natural number greater than one, and

$$t : \Delta \to \mathbb{Z}$$

be a mapping satisfying (2.1a) and such that the composition of t with the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ has image in $(\mathbb{Z}/n\mathbb{Z})^*$ and yields a *homomorphism* $\Delta \to (\mathbb{Z}/n\mathbb{Z})^*$. As in Section 2, we shall denote the homomorphism also by t. Let Γ be a cyclic group of order n. If we write Γ multiplicatively, then Γ is a $\mathbb{Z}\Delta$-module with Δ-action defined by the formula

$$\delta(\gamma) = \gamma^{t(\delta)} \tag{3.1}$$

for γ in Γ, δ in Δ. We shall describe the $\mathbb{Z}\Delta$-module extensions of Γ by a $\mathbb{Z}\Delta$-module C. Throughout this section we shall write all such modules multiplicatively.

So let

$$\xi: \quad 1 \to C \to E \to \Gamma \to 1 \tag{3.2}$$

be a $\mathbb{Z}\Delta$-module extension, and σ be a generator of Γ which shall be fixed throughout this discussion. We shall identify elements of C with their images in E. If u in E maps onto σ, then

$$u^n = a \tag{3.3a}$$

is in C. Moreover, by the familiar theory of group extensions with cyclic factor group [11, pp. 109–110],

$$E=\{cu^i \mid c \text{ in } C,\ 0\leq i<n\}.$$

If c, c' are in C and $0\leq i,\ j<n$, then

$$cu^i=c'u^j \quad \text{if and only if} \quad c=c' \text{ and } i=j. \tag{3.3b}$$

Finally

$$(cu^i)(c'u^j)=cc'a^q u^r \tag{3.3c}$$

with $i+j=nq+r$ and $0\leq r<n$.

Now, if δ is in Δ, then $\delta(u)$ and $u^{t(\delta)}$ have the same image in Γ by (3.1), and so

$$\delta(u)=f(\delta)u^{t(\delta)} \tag{3.4a}$$

with $f(\delta)$ in C. We thus obtain a mapping

$$f:\Delta\to C.$$

Routine calculations using (3.3) and (3.4a) then establish that

$$f(\delta)^n=a^{-t(\delta)}\delta(a) \tag{3.4b}$$

and

$$f(\delta\omega)=f(\delta)^{t(\omega)}\delta(f(\omega))a^{(t(\delta)t(\omega)-t(\delta\omega))/n} \tag{3.4c}$$

for all δ, ω in Δ.

Suppose now that υ is another element of E mapping onto σ; then, as in (3.3a),

$$\upsilon^n=b \text{ is in } C. \tag{3.5a}$$

But also $\upsilon=cu$ for some c in C, and so

$$b=ac^n. \tag{3.5b}$$

Finally, as in (3.4c),

$$\delta(\upsilon)=g(\delta)\upsilon^{t(\delta)} \tag{3.5c}$$

for all δ in Δ with $g:\Delta\to C$, and since $\upsilon=cu$, we then see that

$$g(\delta)=c^{-t(\delta)}\delta(c)f(\delta) \tag{3.5d}$$

for all δ in Δ.

Proposition 3.6. *Given $\mathbb{Z}\Delta$-module extensions*

$$\xi:\quad 1\to C\to E\to\Gamma\to 1$$

and

$$\xi':\quad 1\to C\to E'\to\Gamma\to 1$$

select u and υ in E and E', respectively, which map onto σ. Define a, b in C by (3.3a) *and* (3.35a), *and mappings $f, g:\Delta\to C$ by* (3.4a) *and* (3.5c), *respectively. Then*

$\mathrm{cl}(\xi)=\mathrm{cl}(\xi')$ *in* $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\Gamma, C)$ *if and only if the identities* (3.5b) and (3.5d) *hold for some* c *in* C.

Proof. It follows easily from the preceding discussion and the definition of equivalence of module extensions that, if $\mathrm{cl}(\xi)=\mathrm{cl}(\xi')$, then there exists c in C satisfying the asserted conditions. Conversely, assume that there exists such a c. Then, by [11, pp. 109–110], the mapping $\phi: E\to E'$, where

$$\phi(c'v^i)=c'c^iu^i \quad \text{for } c' \text{ in } C,$$

is an isomorphism of abelian groups and the diagram below commutes:

$$\begin{array}{cccccccccc}
\xi': & 1 & \longrightarrow & C & \longrightarrow & E' & \longrightarrow & \Gamma & \longrightarrow & 1 \\
 & & & \| & & \approx \big\downarrow \phi & & \| & & \\
\xi: & 1 & \longrightarrow & C & \longrightarrow & E & \longrightarrow & \Gamma & \longrightarrow & 1
\end{array}$$

But it follows quickly from (3.5d) that ϕ is also a homomorphism of $\mathbb{Z}\Delta$-modules. Thus ξ and ξ' are equivalent $\mathbb{Z}\Delta$-module extensions and $\mathrm{cl}(\xi)=\mathrm{cl}(\xi')$, as desired.

Remarks 3.7. Given a in C, we have from [11, pp. 109–110] that the set E of all symbols

$$cu^i \qquad (c \text{ in } C,\ 0\le i<n)$$

is an abelian group if equality and composition are defined as in (3.3b) and (3.3c), respectively. Moreover, the mappings $C\to E$ and $E\to\Gamma$, where $c\to cu^0$ and $cu^i\to\sigma^i$, respectively, are group homomorphisms, and

$$\xi:\quad 1\to C\to E\to \Gamma\to 1$$

is an extension of $\mathbb{Z}\Delta$-modules if the action of Δ on E is defined by the formula

$$\delta(cu^i)=\delta(c)f(\delta)^i a^q u^r$$

with $it(\delta)=nq+r$, $0\le r<n$. We shall not need this fact, and omit the proof.

Some of the formulae of this section, particularly (3.4) and (3.5b), are reminiscent of the 'Stickelberger relations' satisfied by the ideal class group of a cyclotomic field; see, e.g. [18, Theorem 6.10, p. 94], [10], [7]. We briefly digress for some related observations on this matter. Set $R=\mathbb{Z}/n\mathbb{Z}$; then, viewing the mapping t as a homomorphism $t:\Delta\to R^*$, we obtain a homomorphism

$$t': \Delta\to(R\Delta)^*$$

of groups if we define

$$t'(\delta)=t(\delta)^{-1}\delta \qquad (\delta \text{ in } \Delta).$$

t' extends uniquely to an endomorphism of the group ring $R\Delta$.

Now, if M is a $\mathbb{Z}\Delta$-module and $M^n = 1$, then M is an $R\Delta$-module, and we obtain from it a new $R\Delta$- (or $\mathbb{Z}\Delta$-) module M_t if we 'twist' the action of Δ on M by t'; i.e.,

$$M_t = M \quad \text{as an abelian group,} \tag{3.8a}$$

$$\delta[x] = t'(\delta)(x) = \delta(x)^{t(\delta)^{-1}} \tag{3.8b}$$

for x in $M_t = M$, δ in Δ [10, §5, pp. 605–607]. If Δ is finite, then the norm mapping $N_\Delta : M_t \to M_t$ corresponds to the endomorphism of M arising from $n\theta_n$, with θ_n the classical Stickelberger element of the rational group ring $\mathbb{Q}\Delta$; i.e.,

$$\theta_n = \frac{1}{n} \sum_{\delta \text{ in } \Delta} t(\delta)\delta^{-1}.$$

In other words, for x in $M_t = M$,

$$N_\Delta[x] \stackrel{\text{def}}{=} \prod_{\delta \text{ in } \Delta} \delta[x] = \prod_{\delta \text{ in } \Delta} \delta^{-1}(x)^{t(\delta)} = (n\theta_n)(x).$$

If Δ is cyclic, then the cohomology groups $\{H^i(\Delta, M_t)\}$ yield the 'cyclic Stickelberger cohomology' of M introduced in [8].

Now let C be a $\mathbb{Z}\Delta$-module as in Proposition 3.6 and the discussion preceding it, and $\Gamma = \langle\sigma\rangle$ be a cyclic group of order n regarded as a $\mathbb{Z}\Delta$-module as in (3.1). If we view $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, C)$ as a $\mathbb{Z}\Delta$-module via the usual diagonal action, it is then easy to see that the standard isomorphism

$$C_n \xrightarrow{\approx} \mathrm{Hom}_{\mathbb{Z}}(\Gamma, C)$$

of abelian groups, with C_n the n-torsion submodule of C, yields a $\mathbb{Z}\Delta$-module isomorphism

$$(C_n)_t \xrightarrow{\approx} \mathrm{Hom}_{\mathbb{Z}}(\Gamma, C), \tag{3.9a}$$

that is, $c \mapsto \phi_c$ for c in $(C_n)_t = C_n$, where

$$\phi_c(\sigma^i) = c^i.$$

In entirely similar fashion we obtain a $\mathbb{Z}\Delta$-module isomorphism

$$(C/C^n)_t \xrightarrow{\approx} \mathrm{Ext}^1_{\mathbb{Z}}(\Gamma, C) \tag{3.9b}$$

from the canonical isomorphism

$$C/C^n \xrightarrow{\approx} \mathrm{Ext}^1_{\mathbb{Z}}(\Gamma, C)$$

of abelian groups which arises upon applying the exact sequence for $\mathrm{Ext}^*_{\mathbb{Z}}(-, C)$ to the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

and identifying $\mathbb{Z}/n\mathbb{Z}$ with Γ via the isomorphism which maps $1 + n\mathbb{Z}$ to σ.

On the other hand, we have from [1, (5), p. 351] a spectral sequence

$$H^p(\Delta, \mathrm{Ext}^q_{\mathbb{Z}}(\Gamma, C)) \overset{m}{\Longrightarrow} \mathrm{Ext}^m_{\mathbb{Z}\Delta}(\Gamma, C).$$

Passing to the associated exact sequence of terms of low degree and using (3.9), we obtain an exact sequence

$$1 \to H^1(\Delta, (C_n)_t) \to \mathrm{Ext}^1_{\mathbb{Z}\Delta}(\Gamma, C) \to (C/C^n)^{\Delta}_t \to H^2(\Delta, (C_n)_t). \tag{3.9c}$$

If $\mathrm{cl}(\xi)$ is in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\Gamma, C)$ with ξ as in (3.2), then it is not difficult to show that the image in $(C/C^n)_t$ of $\mathrm{cl}(\xi)$ is aC^n, with a as in (3.3a). On the other hand, if

$$h: \Delta \to (C_n)_t$$

is a one-cocycle, then its cohomology class in $H^1(\Delta, (C_n)_t)$ maps to the class in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\Gamma, C)$ of the $\mathbb{Z}\Delta$-module extension ξ for which the corresponding element a of (3.3a) is equal to 1 (hence ξ is a split extension of abelian groups), and the associated mapping $f: \Delta \to C$ of (3.4a) is given by the formula

$$f(\delta) = h(\delta)^{t(\delta)} \qquad (\delta \text{ in } \Delta).$$

We return now to the situation of Section 2: k is a field of characteristic prime to a natural number $n > 1$, $L = k(\mu_n) \subseteq k^s$ with μ_n the group of n-th roots of 1 in k^s, $\Delta = \mathrm{Gal}(L/k)$, and $t: \Delta \to \mathbb{Z}$ is as in (2.1). We shall be interested in the special case for which $J = \mathbb{Z}/n\mathbb{Z}$. The mapping

$$\mu_n \xrightarrow{\approx} \hat{J}, \qquad \zeta \mapsto \hat{\zeta} \tag{3.10}$$

where $\hat{\zeta}(i + n\mathbb{Z}) = \zeta^i$, is then an isomorphism of $\mathbb{Z}\Delta$-modules, and we shall identify these modules via this isomorphism. The isomorphism of Theorem 2.3 then assumes the form

$$\mathrm{Hom}_c(\Omega, J) \xrightarrow{\approx} \mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*). \tag{3.11}$$

Given $\mathrm{cl}(\xi)$ in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$, we shall use the invariants of ξ discussed earlier in this section to describe the character $\chi: \Omega \to J$ corresponding to it under the isomorphism (3.11).

In the theorem below it will be convenient to sometimes write J multiplicatively; say

$$J = \{\eta^i \mid i \text{ in } \mathbb{Z}\} \quad \text{with } \eta = 1 + n\mathbb{Z}.$$

Theorem 3.12. *Let*

$$\xi: \quad 1 \to L^* \to E \to \mu_n \to 1$$

be a $\mathbb{Z}\Delta$-module extension, and let a in L^* and $f: \Delta \to L^*$ be as in (3.3a) *and* (3.4a), *respectively, relative to a given (fixed) generator ζ of μ_n and an element u of E mapping onto ζ.*

(a) *Let χ in* $\mathrm{Hom}_c(\Omega, \mathbb{Z}/n\mathbb{Z})$ *correspond to* $\mathrm{cl}(\xi)$ *in* $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$ *under the isomorphism* (3.11), *and let α be any element of k^s such that $\alpha^n = a$. Then, for all ω in Ω,*

$$\zeta^{\chi(\omega)} = \alpha^{-1}\omega(\alpha)^{t(\omega^{-1})}\omega(f(\omega^{-1}))$$

where we again view ξ as a $\mathbb{Z}\Omega$-module extension via the surjection $\Omega \to \Delta$ of (2.6).

(b) *Let K be the Galois extension of k associated to ξ, as in Proposition* 2.14. *Let $L[\bar{z}]$ be the polynomial ring in the indeterminate $\bar{z}$ with coefficients in L, and set*

$$L(z) = L[\bar{z}]/(\bar{z}^n - a)$$

with z the image of $\bar{z}$ in $L(z)$ (hence $L(z)$ is the L-algebra generated by z subject only to the relation $z^n = a$). Then $\Delta \times J$ operates on $L(z)$ by k-algebra automorphisms if we define

$$\delta(xz^i) = \delta(x)f(\delta)^i z^{it(\delta)}, \qquad \eta(xz^i) = x\zeta^i z^i$$

for x in L and δ in Δ. Moreover, there is an L-algebra and $\mathbb{Z}(J \times \Delta)$-module isomorphism

$$L(z) \xrightarrow{\approx} K \otimes_k L$$

and its restriction to $L(z)^\Delta$ yields a k-algebra and $\mathbb{Z}J$-module isomorphism

$$L(z)^\Delta \xrightarrow{\approx} K.$$

Proof. To review the connections among the various objects appearing in the theorem, recall that ξ is equivalent to the extension $\xi_{K/k}$ of (2.8), and $K \approx K(\chi)$ as k-algebras and $\mathbb{Z}J$-modules, with $K(\chi)$ as in (2.5a). Now, if α is as in (a), then it follows easily from the description of E given in (3.3) that there is a unique homomorphism

$$\phi : E \to (k^s)^*$$

of groups such that $\phi(u) = \alpha$ and $\phi(x) = x$ for all x in L^*. Then, by Corollary 2.19,

$$\hat{\zeta}(\chi(\omega)) = \phi(u)^{-1}\omega(\phi(\omega^{-1}(u)))$$

in $J = \mathbb{Z}/n\mathbb{Z}$ for all ω in Ω, with $\hat{\zeta} : J \to \mu_n$ the image in $\hat{J}$, under the isomorphism (3.10), of the given primitive root ζ. (a) then follows from (3.4a) and the fact that

$$\hat{\zeta}(i + n\mathbb{Z}) = \zeta^i.$$

Turning now to (b), we have again from (3.3) that there is a unique L-algebra homomorphism

$$LE \to L(z)$$

which maps u to z and the ideal $I \subseteq LE$ of (2.13) to 0. It is also a $\mathbb{Z}(J \times \Delta)$-module homomorphism, by (3.4a) and (2.12b). Finally, it surjective because z generates $L(z)$. Since $[L(z) : L] = n$ and $[LE/I : L] = [J : 1] = n$ by Proposition 2.14(a), we obtain an isomorphism

$$LE/I \xrightarrow{\approx} L(z)$$

of L-algebras and $\mathbb{Z}(J\times\Delta)$-modules. (b) now follows from Proposition 2.14(a) and Corollary 2.16(a), completing the proof of the theorem.

4. The norm residue symbol

In this section we discuss the promised generalization of the classical norm residue symbol. We shall continue with the notation introduced and used in the latter part of Section 3, especially (3.10)–(3.12) and the paragraph preceding (3.10). It will also be convenient to identify $(1/n)\mathbb{Z}/\mathbb{Z}$ with $\mathbb{Z}/n\mathbb{Z}$ by means of the isomorphism

$$\mathbb{Z}/n\mathbb{Z}\overset{\approx}{\to}\frac{1}{n}\mathbb{Z}/\mathbb{Z}\quad\text{where } i+n\mathbb{Z}\mapsto\frac{i}{n}+\mathbb{Z}. \tag{4.1}$$

First we have a homomorphism of abelian groups, defined as the composition

$$\begin{aligned}&\operatorname{Ext}^1_{\mathbb{Z}\Delta}(\mu_n,L^*)\otimes_{\mathbb{Z}}k^*\overset{\approx}{\to}\operatorname{Hom}_c(\Omega,\mathbb{Z}/n\mathbb{Z})\otimes_{\mathbb{Z}}k^*\\&=\operatorname{Hom}_c\left(\Omega,\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)\otimes_{\mathbb{Z}}k^*\xrightarrow{\langle\cdot,\cdot\rangle_n}\operatorname{Br}(k)_n\end{aligned} \tag{4.2}$$

where $\langle\cdot,\cdot\rangle_n$ is the canonical pairing of (1.1), the left-most isomorphism is the inverse of (3.11), and the equality is meaningful in view of (4.1). Observe now that

$$\operatorname{Hom}_{\mathbb{Z}}(\mu_n,\mathbb{Z}/n\mathbb{Z})=\operatorname{Hom}_{\mathbb{Z}\Delta}(\mu_n,(\mathbb{Z}/n\mathbb{Z})^t) \tag{4.3a}$$

with $(\mathbb{Z}/n\mathbb{Z})^t=\mathbb{Z}/n\mathbb{Z}$ viewed as a $\mathbb{Z}\Delta$-module via the homomorphism $t:\Delta\to(\mathbb{Z}/n\mathbb{Z})^*$ of (2.1). We then have the 'Yoneda pairing'

$$\begin{aligned}&\operatorname{Hom}_{\mathbb{Z}}(\mu_n,\mathbb{Z}/n\mathbb{Z})\otimes_{\mathbb{Z}}\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t,L^*)\\&=\operatorname{Hom}_{\mathbb{Z}\Delta}(\mu_n,(\mathbb{Z}/n\mathbb{Z})^t)\otimes_{\mathbb{Z}}\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t,L^*)\to\operatorname{Ext}^1_{\mathbb{Z}\Delta}(\mu_n,L^*).\end{aligned} \tag{4.3b}$$

This can be described explicitly as follows: Given θ in $\operatorname{Hom}_{\mathbb{Z}}(\mu_n,\mathbb{Z}/n\mathbb{Z})$ and a $\mathbb{Z}\Delta$-module extension ξ of $(\mathbb{Z}/n\mathbb{Z})^t$ by L^*, then

$$\theta\otimes\operatorname{cl}(\xi)\to\theta^*(\operatorname{cl}(\xi)) \tag{4.3c}$$

with

$$\theta^*=\operatorname{Ext}^1_{\mathbb{Z}\Delta}(\theta,L^*):\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t,L^*)\to\operatorname{Ext}^1_{\mathbb{Z}\Delta}(\mu_n,L^*) \tag{4.3d}$$

the homomorphism induced by $\theta:\mu_n\to\mathbb{Z}/n\mathbb{Z}$. Composing (4.3b) with (4.2) then yields a homomorphism

$$\operatorname{Hom}_{\mathbb{Z}}(\mu_n,\mathbb{Z}/n\mathbb{Z})\otimes_{\mathbb{Z}}\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t,L^*)\otimes_{\mathbb{Z}}k^*\to\operatorname{Br}(k)_n. \tag{4.4}$$

Finally, we may use the inverse ε of the evaluation isomorphism

$$\mu_n\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(\mu_n,\mathbb{Z}/n\mathbb{Z})\overset{\approx}{\to}\mathbb{Z}/n\mathbb{Z} \tag{4.5}$$

to construct from (4.4) our general norm residue symbol

$$\{\cdot,\cdot\}_n:\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t,L^*)\otimes_{\mathbb{Z}}k^*\to\operatorname{Br}(k)_n\otimes_{\mathbb{Z}}\mu_n. \tag{4.6a}$$

That is, $\{\cdot,\cdot\}_n$ is the composite homomorphism

$$\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)\otimes_{\mathbb{Z}} k^* = (\mathbb{Z}/n\mathbb{Z})\otimes_{\mathbb{Z}} \operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)\otimes_{\mathbb{Z}} k^*$$

$$\xrightarrow{\varepsilon\otimes 1\otimes 1} \mu_n \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}}(\mu_n, \mathbb{Z}/n\mathbb{Z})\otimes_{\mathbb{Z}} \operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)\otimes_{\mathbb{Z}} k^*$$

$$\xrightarrow{1\otimes G} \mu_n \otimes_{\mathbb{Z}} \operatorname{Br}(k)_n = \operatorname{Br}(k)_n \otimes_{\mathbb{Z}} \mu_n \tag{4.6b}$$

with G the homomorphism of (4.4) and the left equality holding because

$$n \operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*) = 0.$$

Given $\mathrm{cl}(\xi)$ and b in $\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)$ and k^*, respectively, we shall denote by $\{\mathrm{cl}(\xi), b\}_n$ the image in $\operatorname{Br}(k)_n \otimes_{\mathbb{Z}} \mu_n$ of $\mathrm{cl}(\xi)\otimes b$ under the homomorphism (4.6).

The construction of $\{\cdot,\cdot\}_n$ given above ensures that it is independent of all possible choices (e.g., of a primitive n-th root of 1); however, in obtaining explicit formulae such choices will be useful.

(4.7) Let $\mu_n = \langle\zeta\rangle$, and $\theta: \mu_n \xrightarrow{\approx} \mathbb{Z}/n\mathbb{Z}$ be the isomorphism defined by

$$\theta(\zeta^i) = i + n\mathbb{Z}.$$

If $\mathrm{cl}(\xi)$ and b are in $\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)$ and k^*, respectively, then

$$\{\mathrm{cl}(\xi), b\}_n = \left\langle \frac{1}{n}\chi, b\right\rangle_n \otimes \zeta$$

where χ in $\operatorname{Hom}_c(\Omega, \mathbb{Z}/n\mathbb{Z})$ corresponds to $\theta^*(\mathrm{cl}(\xi))$ in $\operatorname{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$ under the isomorphism (3.11), with $J = \mathbb{Z}/n\mathbb{Z}$.

The proof of (4.7) is simply a routine examination of the mappings defined in (4.2)–(4.6); one need only keep in mind the identification of (4.1) which introduces the factor $1/n$.

For the special case in which k is a local field we may compose, as in (1.4)–(1.6), the norm residue symbol (4.6a) with the Hasse invariant isomorphism to obtain a generalization of the classical norm residue symbol for such fields. First consider the homomorphism

$$\operatorname{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*)\otimes_{\mathbb{Z}} k^* \to \left(\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)\otimes_{\mathbb{Z}} \mu_n \tag{4.8a}$$

where

$$\mathrm{cl}(\xi)\otimes b \to (\operatorname{Inv}_k\otimes 1)(\{\mathrm{cl}(\xi), b\}_n),$$

and the isomorphism

$$\operatorname{Inv}_k: \operatorname{Br}(k)_n \xrightarrow{\approx} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is as in (1.5). Composing this with the isomorphism

$$\left(\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)\otimes_{\mathbb{Z}} \mu_n \xrightarrow{\approx} \mu_n \quad \text{where } (x+\mathbb{Z})\otimes\zeta \mapsto \zeta^{nx},$$

we obtain the desired homomorphism

$$(\cdot\,,\cdot)_n : \mathrm{Ext}^1_{\mathbb{Z}\Delta}((\mathbb{Z}/n\mathbb{Z})^t, L^*) \otimes_{\mathbb{Z}} k^* \to \mu_n. \tag{4.8b}$$

We shall now use the data discussed in Section 3 to give explicit formulae for the norm residue symbols introduced above. When describing $\mathbb{Z}\Delta$-module extensions of $((\mathbb{Z}/n\mathbb{Z})^t$ it will be convenient to write this group multiplicatively; hence, as in Theorem 3.12(b), we shall sometimes write

$$(\mathbb{Z}/n\mathbb{Z})^t = \Gamma = \{\sigma^i \mid i \text{ in } \mathbb{Z}\}$$

with $\sigma = 1 + n\mathbb{Z}$. Thus

$$\delta(\sigma^i) = \sigma^{it(\delta)} \qquad (\delta \text{ in } \Delta).$$

Theorem 4.9. *Let b be in k^*,*

$$\xi: \quad 1 \to L^* \to E \to \Gamma \to 1$$

be a $\mathbb{Z}\Delta$-module extension, and a in L^* and $f: \Delta \to L^*$ be as in (3.3a) *and* (3.4a) *relative to an element u of E mapping onto $\sigma = 1 + n\mathbb{Z}$ in $\Gamma = (\mathbb{Z}/n\mathbb{Z})^t$, i.e., $u^n = a$ and $\delta(u) = f(\delta)u^{t(\delta)}$ for δ in Δ. Finally, let ζ in μ_n be a primitive n-th root of* 1.

(a) *Define an L-algebra A with generators z, w subject only to the relations*

$$z^n = a, \qquad w^n = b, \qquad wz = \zeta z w$$

(i.e., if $L[[\bar{z}, \bar{w}]]$ denotes the free L-algebra in the two non-commuting indeterminates $\bar{z}, \bar{w}$, then the assignments $\bar{z} \to z$, $\bar{w} \to w$ yield an isomorphism onto A of $L[[\bar{z}, \bar{w}]]$ modulo the two-sided ideal generated by $\bar{z}^n - a$, $\bar{w}^n - b$, and $\bar{w}\bar{z} - (\zeta\bar{z}\bar{w})$. Δ then operates on A by k-algebra automorphisms according to the formulae

$$\delta(xz^i) = \delta(x)f(\delta)^i z^{it(\delta)}, \qquad \delta(xw^i) = \delta(x)w^i$$

(δ in Δ, x in L). Moreover, A^Δ is a central simple k-algebra, and

$$\{\mathrm{cl}(\xi), b\}_n = \mathrm{cl}(A^\Delta) \otimes \zeta$$

in $\mathrm{Br}(k)_n \otimes_{\mathbb{Z}} \mu_n$, where $\{\cdot\,,\cdot\}_n$ is the norm residue symbol of (4.6a) *and $\mathrm{cl}(A^\Delta)$ is the equivalence class of A^Δ in the Brauer group of k.*

(b) *Suppose now that k is a local field. Then*

$$(cl(\xi), b)_n = \alpha^{-1}\omega(\alpha)^{t(\omega^{-1})}\omega(f(\omega^{-1}))$$

in μ_n, where $(\cdot\,,\cdot)_n$ is the norm residue symbol of (4.8b), *α is any element of k^s such that $\alpha^n = a$, and $\omega = (b, k)$ in Ω^{ab}, with*

$$(-, k) : k^* \to \Omega^{\mathrm{ab}}$$

the local reciprocity map of Theorem 1.7.

Proof. Given ζ as above, let $\theta : \mu_n \xrightarrow{\approx} \mathbb{Z}/n\mathbb{Z}$ be as in (4.7), and define the $\mathbb{Z}\Delta$-module extension $\theta^*\xi$ of μ_n by L^* by the commutative diagram

$$\begin{array}{rccccccccc}
\theta^*\xi: & 1 & \longrightarrow & L^* & \longrightarrow & \bar{E} & \longrightarrow & \mu_n & \longrightarrow & 1 \\
& & & \Vert & & \approx\downarrow\phi & & \approx\downarrow\theta & & \\
\xi: & 1 & \longrightarrow & L^* & \longrightarrow & E & \longrightarrow & \Gamma & \longrightarrow & 1
\end{array}$$

with ϕ an isomorphism of $\mathbb{Z}\Delta$-modules (hence $\mathrm{cl}(\theta^*\xi)=\theta^*(\mathrm{cl}(\xi))$ in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$ with $\theta^*: \mathrm{Ext}^1_{\mathbb{Z}\Delta}(\Gamma, L^*)\to\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$ as in (4.3d)). Let $\bar{u}=\phi^{-1}(u)$ in $\bar{E}$; then, since $\theta(\xi)=1+n\mathbb{Z}=\sigma$ in J, $\bar{u}$ maps onto ζ in μ_n. Moreover, the definitions of a in L^* and $f:\Delta\to L^*$ imply that $\bar{u}^n=a$ and $\delta(\bar{u})=f(\delta)\bar{u}^{t(\delta)}$ for δ in Δ.

If k is a local field, we now have from (4.7), (4.8), and Theorem 1.7 that

$$(\mathrm{cl}(\xi), b)_n=\zeta^{\chi(\omega)}$$

where $\omega=(b,k)$ in Ω^{ab} is as above and χ in $\mathrm{Hom}_c(\Omega, \mathbb{Z}/n\mathbb{Z})$ corresponds to $\mathrm{cl}(\theta^*\xi)$ in $\mathrm{Ext}^1_{\mathbb{Z}\Delta}(\mu_n, L^*)$ under the isomorphism (3.11). (b) then follows upon applying Theorem 3.12(a) to the $\mathbb{Z}\Delta$-module extension $\theta^*\xi$.

Turning now to (a), let K be the Galois extension of k with Galois group J which is associated to the $\mathbb{Z}\Delta$-module extension $\theta^*\xi$ as in Proposition 2.14 and Theorem 3.12(b). Then (4.7) and Lemma 4.14 below (applied to the character $(1/n)\chi$ in $\mathrm{Hom}_c(\Omega, (1/n)\mathbb{Z}/\mathbb{Z})$ of (4.7)) yield that

$$\{\mathrm{cl}(\xi), b\}_n=\mathrm{cl}(K\langle b\rangle)\otimes\zeta \tag{4.10}$$

in $\mathrm{Br}(k)_n\otimes\zeta$, with $K\langle b\rangle$ the cyclic k-algebra constructed using K, b, and the generator η of J. That is, $K\langle b\rangle$ is the free left K-module with basis $\{1, v, v^2, \ldots, v^{n-1}\}$ and multiplication defined by the formula

$$(xv^i)(yv^j)=x\eta^i(y)b^q v^r \tag{4.11}$$

with x, y in K and $i+j=nq+r$, $0\le r<n$. Note that the operation of Δ on L extends uniquely to an operation of Δ on $K\langle b\rangle\otimes_k L$ by k-algebra automorphisms and $(K\langle b\rangle\otimes_k L)^\Delta=K\langle b\rangle$. Thus, in view of (4.10), we need only establish an L-algebra isomorphism

$$A\xrightarrow{\approx}K\langle b\rangle\otimes_k L \tag{4.12}$$

which preserves the operation of Δ.

Recall now that, by Theorem 3.12(b), there is a k-algebra and $\mathbb{Z}(\Delta\times J)$-module isomorphism

$$L(z)\xrightarrow{\approx}K\otimes_k L \tag{4.13}$$

where $L(z)$ is the L-algebra generated by an element z subject only to the relation $z^n=a$, and Δ and $J=\mathbb{Z}/n\mathbb{Z}$ operate on $L(z)$ according to the formulae provided in the statement of the theorem. We shall (with some ambiguity of notation) identify $L(z)$ with its image in $K\langle b\rangle\otimes_k L$ under the composite L-algebra and $\mathbb{Z}\Delta$-module injection

$$L(z) \xrightarrow{\approx} K \otimes_k L \hookrightarrow K\langle b \rangle \otimes_k L.$$

Note then that, by (4.11) and Theorem 3.12(b),

$$vz = \eta(z)v = \zeta zv.$$

It then follows easily from Theorem 3.12(b) and the definitions of A and $K\langle b \rangle$ that the assignments

$$z \mapsto z, \qquad w \mapsto v$$

yield a well-defined L-algebra isomorphism (4.12) which preserves the operation of Δ. This reduces the proof of the theorem to the promised Lemma 4.14, with which we have yet to deal.

First, however, let us consider the special case of Theorem 4.9 in which $\mu_n \subseteq k$; i.e., $L = k$ and $\Delta = 1$. The exact sequence (3.9c) (with $C = L^* = k^*$) then reduces to the familiar isomorphism

$$\mathrm{Ext}^1_{\mathbb{Z}}(\Gamma, k^*) \xrightarrow{\approx} k^*/(k^*)^n$$

which maps $\mathrm{cl}(\xi)$ to $a(k^*)^n$ (this isomorphism can also be derived by the well-known and elementary argument of [11, pp. 109–110]). The norm residue symbols (4.6a), (4.8b) then become essentially the classical ones:

$$\{\cdot,\cdot\}_n : k^* \otimes_{\mathbb{Z}} k^* \to \mathrm{Br}(k)_n \otimes_{\mathbb{Z}} \mu_n,$$

$$(\cdot,\cdot)_n : k^* \otimes_{\mathbb{Z}} k^* \to \mu_n,$$

the latter defined only for a local field. In this case Theorem 4.9(a) reduces to the well-known formula

$$\{a, b\}_n = \mathrm{cl}(A) \otimes \zeta$$

with ζ as in the theorem and A the k-algebra generated by the elements z, w subject only to the relations

$$z^n = a, \qquad w^n = b, \qquad wz = \zeta zw.$$

On the other hand, if k is a local field, Theorem 4.9(b) asserts that

$$(a, b)_n = \alpha^{-1}(b, k)(\alpha)$$

with α any element of k^s such that $\alpha^n = a$; this agrees with [16, Proposition 6, p. 208].

In the lemma below it will be convenient to write

$$\mathbb{Z}/n\mathbb{Z} = J = \{\eta^i \mid i \text{ in } \mathbb{Z}\}$$

as in Section 3 ($\eta = 1 + n\mathbb{Z}$) and identify J with $(1/n)\mathbb{Z}/\mathbb{Z}$ via the isomorphism

$$J = \mathbb{Z}/n\mathbb{Z} \xrightarrow{\approx} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \qquad \text{of (4.1).}$$

Lemma 4.14. *Let $k \subseteq k^s$, $n>1$, b in k^*, etc., be as in Theorem* 4.9; *χ be in* $\mathrm{Hom}_c(\Omega,(1/n)\mathbb{Z}/\mathbb{Z})$; *and $K=K(\chi)$ be the associated Galois extension of k with Galois group J as in* (2.10) *and the discussion preceding it. Then*

$$\langle \chi, b\rangle_n = \mathrm{cl}(K\langle b\rangle)$$

in $\mathrm{Br}(k)_n$, *with*

$$\langle\cdot,\cdot\rangle_n : \mathrm{Hom}_c\left(\Omega, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)\otimes_{\mathbb{Z}} k^* \to \mathrm{Br}(k)_n$$

as in (1.1) *and $K\langle b\rangle$ the cyclic k-algebra constructed using K, b, and the generator η of J.*

Proof. Recall that, by (1.3) and the remarks preceding it,

$$\langle \chi, b\rangle_n = \mathrm{cl}(\bar{K}\langle b\rangle)$$

where

$$\bar{K} = (k^s)^{\mathrm{Ker}(\chi)} \subseteq k^s$$

is a Galois field extension of k with Galois group $\Omega/\mathrm{Ker}(\chi)$, which we may identify with

$$\bar{J} = \mathrm{Im}(\chi) \subseteq J$$

via the isomorphism induced by χ (keep in mind that we have also identified J with $(1/n)\mathbb{Z}/\mathbb{Z}$ according to the warning issued before the statement of the lemma). The cyclic k-algebra $\bar{K}\langle b\rangle$ is defined using the generator $\bar{\eta}=\eta^m$ of $\bar{J}$, with $m=[J:\bar{J}]$. Thus we need only show that the central simple k-algebras $A=K\langle b\rangle$ and $\bar{A}=\bar{K}\langle b\rangle$ are Brauer equivalent. This fact is well-known and is true in greater generality, but since we haven't found a convenient reference for it we shall give a direct proof. Note that the Galois extension K need not be a field; nevertheless, the definition and basic properties of the cyclic k-algebra A can be carried through in this slight generalization of the classical context.

Let $J(\chi)$ be, as in (2.4), the Ω-J-set arising from the character χ; then as in (2.4) we may assume that

$$K = (J(\chi), k^s)^{\Omega}$$

the set of all Ω-equivariant mappings from $J(\chi)$ to k^s, with the operation of J on K arising from that on $J(\chi)$. Thus there is a k-algebra homomorphism $\phi: K\to k^s$, where $\phi(\alpha)=\alpha(1)$ is the value of α in K on 1 in $J=J(\chi)$. If ω is in $\mathrm{Ker}(\chi)$, then by (2.4b),

$$\omega\cdot 1 = 1\cdot\chi(\omega) = 1$$

in $J(\chi)$, and so

$$\omega(\phi(\alpha)) = \omega(\alpha(1)) = \alpha(\omega\cdot 1) = \alpha(1) = \phi(\alpha).$$

That is, $\phi(\alpha)$ is in $(k^s)^{\mathrm{Ker}(\chi)} = \bar{K}$ for all α in K, and so we may regard ϕ as a k-

algebra homomorphism $\phi : K \to \bar{K}$. Moreover, if $\sigma = \chi(\omega)$ is in $\bar{J} = \mathrm{Im}(\chi) \subseteq J$ with ω in Ω, then, by (2.4b) and (2.5b),

$$\phi(\sigma(\alpha)) = \sigma(\alpha)(1) = \alpha(\sigma) = \alpha(\omega \cdot 1) = \omega(\alpha(1)) = \omega(\phi(\alpha)) = \sigma(\phi(\alpha)).$$

Hence ϕ is a homomorphism of $\mathbb{Z}\bar{J}$-modules.

Let us now view $\bar{K}$ as a K-module via the homomorphism ϕ; then, since A may be regarded in the obvious way as a K-A-bimodule, we obtain a $\bar{K}$-A-bimodule

$$M = \bar{K} \otimes_K A.$$

In fact, it follows from routine but tedious computations that M is an $\bar{A}$-A-bimodule if we define the left $\bar{A}$-module structure of M by the formula

$$(\bar{x}\bar{v}^i)(\bar{y} \otimes_k x v^j) = \bar{x}\bar{\eta}^i(\bar{y}) \otimes_K \bar{\eta}^i(x) v^{mi+j}$$

for $\bar{x}, \bar{y}$ in $\bar{K}$; x, y in K; and $v, \bar{v}$ the distinguished elements of $A, \bar{A}$, respectively, as in (4.11). This $\bar{A}$-A-bimodule structure on M yields, in the usual manner, a k-algebra homomorphism

$$A \to \mathrm{End}_{\bar{A}}(M) \tag{4.15}$$

(writing, for the moment, endomorphisms of modules opposite scalars). This homomorphism is injective, since A is a simple k-algebra.

We now compute some dimensions. We may write $n = md$ with $d = [\bar{J} : 1]$. Since A is a left K-module of rank n, M is a left $\bar{K}$-module of rank n, and thus

$$[M : k] = n[\bar{K} : k] = nd = md^2.$$

Since $[\bar{A} : k] = d^2$, it follows from the structure theory for modules over simple k-algebras of finite dimension that M is a free $\bar{A}$-module of rank m. $\mathrm{End}_{\bar{A}}(M)$ is then isomorphic to the k-algebra of all $m \times m$ matrices over $\bar{A}$, and thus

$$[\mathrm{End}_{\bar{A}}(M) : k] = m^2[\bar{A} : k] = n^2 = [A : k].$$

We may conclude that the k-algebra injection (4.15) is an isomorphism and $\mathrm{cl}(A) = \mathrm{cl}(\bar{A})$ in $\mathrm{Br}(k)$. This completes the proof of the lemma.

References

[1] H. Cartan and S. Eilenberg, Homological Algebra (Princeton University Press, Princeton, NJ, 1956).

[2] J. Cassels and A. Fröhlich, Algebraic Number Theory (Thompson Book Co., Washington, DC, 1967).

[3] S. Chase, D. Harrison, and A. Rosenberg, Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. 52 (1965) 15–33.

[4] S. Chase, Galois objects and extensions of Hopf algebras, in: Category Theory, Homology Theory and their Applications II, Lecture Notes in Math. 92 (Springer, Berlin, 1969) 10–31.

[5] S. Chase, Galois objects and extensions of Hopf algebras, in: S. Chase and M. Sweedler, Hopf Algebras and Galois Theory, Lecture Notes in Math. 97 (Springer, Berlin, 1969) 84–130.

[6] S. Chase, On a variant of the Witt and Brauer group, in: Brauer Groups, Lecture Notes in Math. 549 (Springer, Berlin, 1975) 148–187.
[7] L. Childs, A Stickelberger condition on cylic Galois extensions, Canad. J. Math. 34 (1982) 686–690.
[8] L. Childs, Cyclic Stickelberger cohomology and descent of Kummer extensions, Proc. Amer. Math. Soc. 90 (1984) 505–510.
[9] F. DeMeyer and E. Ingraham, Separable Algebras over Commutative Rings, Lecture Notes in Math. 181 (Springer, Berlin, 1971).
[10] A. Fröhlich, Stickelberger without Gauss sums, in: A. Fröhlich, ed., Algebraic Number Fields – L-Functions and Galois Properties (Academic Press, London, 1977) 589–607.
[11] S. MacLane, Homology (Academic Press, New York, 1963).
[12] L. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra 82 (1983) 102–133.
[13] A. Merkur'ev, On the norm residue symbol of degree 2, Soviet Math. Dokl. 24 (1981) 546–551.
[14] A. Merkur'ev and A. Suslin, K-cohomology of Severi–Brauer varieties and norm residue homomorphism, Izvesti'a Akad. Nauk SSSR Ser. Mat. 46 (5) (1982) 1011–1046.
[15] I. Reiner, Maximal Orders (Academic Press, New York, 1975).
[16] J.-P. Serre, Local Fields (Springer, Berlin, 1979).
[17] M.Takeuchi, On extensions of formal groups by μ^A, Comm. in Algebra 5 (1977) 1439–1481.
[18] L. Washington, Introduction to Cyclotomic Fields (Springer, Berlin, 1980).
[19] W. Waterhouse, Principal homogeneous spaces and group scheme extensions, Trans. Amer. Math. Soc. 153 (1971) 181–189.
[20] A. Weil, Basic Number Theory (Springer, New York, 1967).