Ramification Invariants and Torsion Galois Module Structure in Number Fields

STEPHEN U. CHASE*

Department of Mathematics, Cornell University, Ithaca, New York 14853

Communicated by A. Fröhlich

Received August 1, 1983

Let $k$ be a number field with ring of integers $\mathfrak{O}$, and $K$ be a normal extension of $k$ with Galois group $\Gamma$. The integer ring $\mathfrak{O}$ of $K$ is then a Galois module, i.e., a module over the group ring $\mathfrak{O}[\Gamma]$. During the last few years a great deal of information has been obtained regarding the structure of such Galois modules. In particular, Fröhlich's conjecture—recently proved by Taylor [14]—asserts that if $K/k$ is tame then $\mathfrak{O}$ is determined up to stable $\mathfrak{O}[\Gamma]$-module isomorphism by the Artin root numbers of the symplectic characters of $\Gamma$, with $\mathfrak{O}$ the ring of rational integers. The theory, as developed by Fröhlich [5], Taylor [14], and others, encompasses three distinct but apparently related topics in algebraic number theory: (1) Galois module structure of rings of algebraic integers, (2) Galois module structure of ideal class groups of number fields and Grothendieck and class groups of group rings, and (3) the study of arithmetically or analytically defined functions on complex characters of the Galois group such as the Artin root number, the Artin conductor, and the Galois Gauss sum.

In this paper we investigate two other Galois modules which intervene in a natural way in the consideration of the above topics. These modules arise as elementary ramification invariants of the extension $K/k$. Their distinctive feature is that they are torsion $\mathfrak{O}$-modules. Although they are completely determined by local data, their projective resolutions, together with standard applications of Schanuel's Lemma [1, Proposition 6.3, p. 36], yield information on global Galois module structure.

The simplest of these modules is defined by the equality

$$T(K/k) = \mathcal{C}(K/k) / \mathfrak{D}$$

with $\mathcal{C}(K/k)$ the codifferent (i.e., inverse different) of $K/k$. In Section 1, Theorems 1.7 and 1.8, we give an explicit structure theorem for the $\mathfrak{O}[\Gamma]$-
module $T(K/k)$ under the hypothesis that $K/k$ is tame, in which case $\mathcal{O}$ and $\mathcal{C}(K/k)$ are locally free $\mathcal{O}I$-modules. Our theorem permits the conclusion that $T(K/k)$ has a free resolution as a $\mathbb{Z}I$-module. Comparing with (0.1) and using Schanuel's Lemma, one sees that $\mathcal{O}$ and $\mathcal{C}(K/k)$ are stably isomorphic $\mathbb{Z}I$-modules. Since $\mathcal{C}(K/k)$ is the dual Galois module of $\mathcal{O}$, it follows that $\mathcal{O}$ is "stably self-dual" over $\mathbb{Z}I$, a result proved by Taylor [13] under the stronger assumption that the primes of $\mathfrak{o}$ which ramify in $k$ do not divide the order of $I$.

In Sections 2–4 we study the second torsion Galois module, which we denote by $R(K/k)$. It is defined as follows. Writing $(X, Y)$ for the set of all mappings from a set $X$ to a set $Y$, we have the familiar bijection

$$
\psi: K \otimes_k \mathbb{K} \rightarrow (I, K) \quad (0.1a)
$$

where

$$
\psi(x \otimes y)(\sigma) = x\sigma(y)
$$

for $x, y$ in $K$ and $\sigma$ in $I$. $K \otimes_k \mathbb{K}$ is a $KI$-module with $K$ acting on the left factor, $I$ on the right, and we then have a unique $KI$-module structure on $(I, K)$ such that $\psi$ is an isomorphism of such modules. Restricting $\psi$ to the subring $\mathcal{O} \otimes_k \mathcal{O}$ of $K \otimes_k K$ yields an $\mathcal{O}I$-module injection

$$
\psi: \mathcal{O} \otimes_k \mathcal{O} \rightarrow (I, \mathcal{O}). \quad (0.1b)
$$

It is well known that the homomorphism $\psi$ of (0.1b) is an isomorphism if and only if $K/k$ is non-ramified; this is, for example, a standard application of the Galois theory of rings [3, Proposition 1.2, pp. 80–81]. Hence the torsion $\mathcal{O}I$-module

$$
R(K/k) = \text{Coker}\{\psi: \mathcal{O} \otimes_k \mathcal{O} \rightarrow (I, \mathcal{O})\} \quad (0.1c)
$$

is an invariant of ramification. Moreover, since $(I, \mathcal{O})$ is a free $\mathcal{O}I$-module, (0.1c) and Schanuel's Lemma imply that $R(K/k)$ determines the Galois module $\mathcal{O} \otimes_k \mathcal{O}$ up to stable isomorphism, and hence should yield at least weak information on the Galois module structure of $\mathcal{O}$. For example, we show in Theorem 2.10 that $R(K/k)$ determines completely the local Galois module structure of $\mathcal{O}$. The general expectation is that $T(K/k)$ and $R(K/k)$ should be useful in treating questions regarding the Galois module structure of rings of algebraic integers which are trivial for non-ramified extensions $K/k$, and this paper provides substantial evidence for the accuracy of that point of view. These torsion Galois modules are linked by a short exact sequence which is a module-theoretic generalization of the elementary fact that the discriminant ideal $d(K/k)$ is the square of an ideal of $\mathcal{O}$; see Theorem 2.4 and the remark following (4.3).
Our main result on $R(K/k)$ is Theorem 2.15 which, together with Addendum 2.30, determines completely its primary components for primes at which the extension is tame. From this theorem one sees, in a natural and conceptual way, how the various “Stickelberger elements” enter into the theory of Galois module structure. As corollaries we derive Stickelberger-like formulae for the composition series of certain primary components of $R(K/k)$ for $K/k$ cyclic and elementary abelian, respectively. The first of these is reminiscent of the classical Stickelberger relations satisfied by the ideal class group of a cyclotomic field [7, p. 8; 6]; the second uses explicitly the Stickelberger element introduced by McCulloh [8] to study the Galois module structure of integer rings in elementary abelian extensions. The proof of the main theorem rests in part on certain base-change and local-global formulae for $R(K/k)$ explicated in Section 3.

Section 4 contains a more detailed study of $R(K/k)$ for cyclic extensions of degree $n$. Our point of view is the following. From $R(K/k)$ we obtain torsion modules over the integer ring $\mathcal{O}_L$ of the field $L = k(\mu_n)$, with $\mu_n$ the group of $n$th roots of 1 in an algebraic closure of $k$. These modules arise essentially by change-of-rings via an isomorphism of the Galois group $\Gamma$ of $K/k$ with $\mu_n$. In Theorems 4.10 and 4.15 we describe the composition series of certain of their primary components in terms of routine generalizations of the classical Stickelberger elements. These formulae provide similar descriptions of the order ideals [10, pp. 49–50] of these modules which can in turn be applied to yield global results. For example, we show in Corollary 4.20 that, if there is a single prime $p$ of $\mathcal{O}$ which ramifies in $K$, $p$ splits completely in $L$, and $\mathcal{O} \otimes \mathcal{O}$ is a free $\mathcal{O}\Gamma$-module, then

$$q^n\Theta_p(r)$$

is a principal ideal of $\mathcal{O}_L$ for any prime $q$ of $\mathcal{O}$ above $p$, with $\Theta_p(r)$ an appropriate Stickelberger element. In Corollary 4.24 we establish, by a similar but somewhat more delicate argument, a weak form of the classical Stickelberger theorem for cyclotomic extensions of the rational field $\mathbb{Q}$. Our approach here is somewhat similar to that of Fröhlich [6], although it has perhaps a more module-theoretic flavor. Throughout this section the principal tool in our analysis is the above-mentioned “cyclic” corollary of the main theorem of Section 2, together with the elementary fact (4.1d) that, if $M$ is the cokernel of a one-to-one endomorphism of a finitely generated projective module over a Dedekind domain, then the order ideal of $M$ is principal.

The preceding discussion elucidates some of the connections between the contents of this paper and topics (1)–(2) listed in the first paragraph. The relation with (3) arises as follows. If $\mathcal{O}$ is as above and $\Gamma$ is any finite group, then the $\mathcal{O}\Gamma$-modules of finite homological dimension which are finitely
generated torsion \( \mathcal{O} \)-modules give rise to functions, defined on the complex characters of \( \Gamma \), with values in the ideal group of a sufficiently large number field. In the theory of such modules these "character functions" assume a role somewhat analogous to that played by the characters themselves in classical representation theory. Their construction is implicit in [5, Appendix A.1, pp.426–429]; for a direct treatment see Desrochers [4, Sect. 8], where they are introduced as a routine generalization of the order ideal of a finite \( \mathcal{O} \)-module.

If \( K/k \) is tame with Galois group \( \Gamma \), then it follows from the results of Section 1 that the character function associated to the \( \mathcal{O}\Gamma \)-module \( T(K/k) \) is the Artin conductor of \( K/k \) [4, Theorem 8.1]. In a similar fashion, an elementary algebraic argument shows that the character of \( R(K/k) \) is closely related to Fröhlich’s generalization of the Lagrange resolvent [5, Sect. 1, pp. 384–390], and hence also to the Galois Gauss sum via his fundamental theorem [5, Theorem 2, p. 391].

Queyrut [9] has extended Fröhlich’s general theory of Galois module structure to obtain results for arbitrary (i.e., not necessarily tame) extensions, and in particular he and Cassou-Nogues have proved a self-duality theorem [16, Corollaire 6.3, p. 23] which includes that of Section 1 mentioned earlier. More recently Desrochers [4, Sects. 4–6] has generalized the methods of Section 1 to obtain an explicit description of the class of the module \( T(K/k) \) (for arbitrary \( K/k \)) in an appropriate Grothendieck group of torsion \( \mathcal{O}\Gamma \)-modules, and has deduced from this a more elementary proof of their theorem, as well as further information regarding the self-duality of \( \mathcal{O} \) as an \( \mathcal{O}\Gamma \)-module.

0. Preliminaries

Throughout this paper all rings will have identity elements which act as the identity transformation on all modules. All modules will be left modules unless explicitly stated otherwise. If \( R \) is a ring, \( M \) is an \( R \)-module, and \( n \) is a non-negative integer, then the direct sum (or coproduct) of \( n \) copies of \( M \) will be written as \( nM \). If \( I \) is a group, we shall denote by \( RI \) the group ring of \( I \) with coefficients in \( R \).

Now let \( \mathcal{O} \) be a Dedekind domain with quotient field \( k \). The phrase "prime of \( \mathcal{O} \)" will always mean a non-zero prime ideal of \( \mathcal{O} \). If \( \mathfrak{p} \) is such, we denote by \( k(\mathfrak{p}) = \mathcal{O}/\mathfrak{p} \) the residue field of \( \mathfrak{p} \), and by \( \mathcal{O}_\mathfrak{p} \) and \( k_\mathfrak{p} \) the completions of \( \mathcal{O} \) and \( k \) at \( \mathfrak{p} \), respectively. If \( M \) is an \( \mathcal{O} \)-module, then we set \( M_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M \), an \( \mathcal{O}_\mathfrak{p} \)-module. Of course, if \( M \) is a finitely generated torsion \( \mathcal{O} \)-module, then \( M_\mathfrak{p} \) is simply the \( \mathfrak{p} \)-primary component of \( M \). This notation will also be applied to the slightly more general situation in which \( \mathcal{O} \) is a finite product of Dedekind domains and \( k \) is the corresponding product of the quotient fields;
in this case, too, \( \mathfrak{O}_p \) is always a complete discrete valuation ring and \( k_p \) is its quotient field.

In various parts of this paper we shall have use for separable algebras over a commutative ring and for Galois extensions of such rings, and we refer to [3, Chap. II, Sects. 1–2, and Chap. III] for the basic theory of these objects. In particular, if \( \mathfrak{O} \) is a Dedekind domain with quotient field \( k \), we shall often consider a Galois (not necessarily field) extension \( K \) of \( k \) with Galois group \( \Gamma \). \( K \) is then a commutative separable \( k \)-algebra, and hence a finite product

\[
K = \prod_{i=1}^{r} K_i
\]

with each \( K_i \) a finite separable field extension of \( k \) [3, Theorem 2.5, p. 50].

There is then a unique maximal \( \mathfrak{O} \)-order in \( K \) [10, Theorem 10.5, p. 128], namely,

\[
\mathcal{O} = \prod_{i=1}^{r} \mathcal{O}_i
\]

with \( \mathcal{O}_i \) the integral closure of \( \mathfrak{O} \) in \( K_i \). If \( p \) is a prime of \( \mathfrak{O} \) and \( \mathfrak{P} \) is a prime of \( \mathcal{O} \) above \( p \) (i.e., \( \mathfrak{P} \cap \mathfrak{O} = p \)), then we define the decomposition group \( \Gamma_{\mathfrak{P}} \leq \Gamma \) in the usual way, i.e.,

\[
\Gamma = \{ \sigma \in \Gamma \mid \sigma(\mathfrak{P}) = \mathfrak{P} \}.
\]

Since, as noted above, \( \mathcal{O}_{\mathfrak{P}} \) is a complete discrete valuation ring with quotient field \( K_{\mathfrak{P}} \), a standard argument shows that \( K_{\mathfrak{P}}/k_p \) is a Galois extension with Galois group naturally isomorphic to \( \Gamma_{\mathfrak{P}} \), and the usual theory of the decomposition and inertial groups [2, Chap. I, Sects. 8–9, pp. 29–39] is valid in this setting.

1. The Torsion Galois Module \( T(K/k) \)

Throughout this section \( \mathfrak{O} \) will denote a Dedekind domain with quotient field \( k \), and \( K \) will be a finite normal separable extension of \( k \) with Galois group \( \Gamma \). We shall view \( K \) as a left \( k\Gamma \)-module; the integral closure \( \mathcal{O} \) of \( \mathfrak{O} \) in \( K \) is then a left \( \mathfrak{O}\Gamma \)-submodule of \( K \).

Let \( t_{K/k} : K \rightarrow k \) denote the trace map of the extension \( K/k \), i.e.,

\[
t_{K/k}(x) = \sum_{\sigma \in \Gamma} \sigma(x) \quad (x \in K).
\]

If we set

\[
\mathcal{O}(K/k) = \{ x \in K \mid t_{K/k}(xy) \text{ is in } \mathcal{O} \text{ for all } y \in \mathcal{O} \}
\]
the so-called codifferent or complementary ideal of $K/k$, then $\mathfrak{O}(K/k)$ is an $\sigma \Gamma$-submodule of $K$ and $\mathfrak{O} \subseteq \mathfrak{O}(K/k)$. We define

$$T(K/k) = \mathfrak{O}(K/k)/\mathfrak{O}$$

(1.1)

a finitely generated $\sigma \Gamma$-module which is torsion as an $\sigma$-module (since $\mathfrak{O}$ contains a $k$-basis of $K$). Note that, by [2, (4), p. 16, and Theorem 1, p. 211], $T(K/k) = 0$ if and only if $K$ is a non-ramified extension of $k$.

Recall now that $\mathfrak{O}(K/k)$ admits the following module-theoretic interpretation. $t_{K/k}$ yields a non-degenerate $k$-bilinear form on $K$, and hence a bijection $j: K \overset{\sim}{\longrightarrow} \text{Hom}_k(K, k)$, where $j(x)(y) = t_{K/k}(xy)$ for $x, y$ in $K$. $j$ is a $k\Gamma$-module isomorphism if we define the $k\Gamma$-module structure on $\text{Hom}_k(K, k)$ by the formula

$$(c\sigma)f^*(x) = cf(\sigma^{-1}(x))$$

for $c$ in $k$, $\sigma$ in $\Gamma$, $x$ in $K$, and $f$ in $\text{Hom}_k(K, k)$. If we view $\text{Hom}_k(\mathfrak{O}, k)$ in the usual way as an $\sigma \Gamma$-submodule of $\text{Hom}_k(K, k)$, then $j$ induces an $\sigma \Gamma$-module isomorphism

$$\mathfrak{O}(K/k) \overset{\sim}{\longrightarrow} \text{Hom}_k(\mathfrak{O}, k).$$

(1.2)

It is then clear that $T(K/k)$ measures, in some sense, the deviation of $\mathfrak{O}$ from being a "self-dual" $\sigma \Gamma$-module (i.e., being isomorphic to its dual $\text{Hom}_k(\mathfrak{O}, k)$), and later we shall investigate this situation for tame extensions of number fields.

Note, incidentally, that $j$ is also an isomorphism of $K$-spaces if we define the $K$-space structure on $\text{Hom}_k(K, k)$ in the usual manner:

$$(af^*)(x) = f(ax)$$

for $a, x$ in $K$ and $f$ in $\text{Hom}_k(K, k)$. Then $\text{Hom}_k(\mathfrak{O}, k)$ is an $\mathfrak{O}$-submodule of $\text{Hom}_k(K, k)$, and (1.2) is an isomorphism of $\mathfrak{O}$-modules as well as $\sigma \Gamma$-modules.

It will also be useful to observe that the definitions and remarks made so far apply without the assumption that $K$ be a field. That is to say, they apply to the case in which $K$ is a Galois (ring) extension of the field $k$ with Galois group $\Gamma$ (see [3, Chap. III, particularly p. 84]). In that case $K$ is a finite direct product of finite separable field extensions of $k$ [3, p. 84 and Corollary 2.4, p. 49]; we then take $\mathfrak{O}$ to be the maximal $\sigma$-order in $K$.

We devote the remainder of this section to the computation of $T(K/k)$ for the case in which $K/k$ is tamely ramified (or tame), i.e., there exists $x$ in $\mathfrak{O}$ such that $t_{K/k}(x) = 1$ [2, Theorem 2, p. 21]. We assume first that $\mathfrak{O}$ is a complete discrete valuation ring with maximal ideal $p$. We shall then denote
the maximal ideal of $\mathcal{O}$ by $\Psi$, the residue fields of $\mathfrak{o}$ and $\mathcal{O}$ by $k(\mathfrak{p})$ and $K(\Psi)$, respectively, and the characteristics of these fields by $p$. Moreover, we set

$$t_\Gamma = \sum_{\sigma \in \Gamma} \sigma \quad \text{in } \mathbb{Z}\Gamma,$$

(1.3a)

and

$$I(p, \Gamma) = \mathbb{Z}\Gamma/\langle p, t_\Gamma \rangle$$

(1.3b)

with $\langle p, t_\Gamma \rangle$ the left ideal of $\mathbb{Z}\Gamma$ generated by $p$ and $t_\Gamma$. $T(p, \Gamma)$ is then a $\mathbb{Z}\Gamma$-module annihilated by $p$, and hence can be viewed, when convenient, as an $\mathbb{F}_p\Gamma$-module with $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

**Lemma 1.4.** Assume that $K$ is a tame and totally ramified (field) extension of $k$. Then $T(K/k) \simeq k(\mathfrak{p}) \otimes_{\mathcal{O}} T(p, \Gamma)$ as $\mathcal{O}\Gamma$-modules.

**Proof:** Let $n = [K : k]$. Then, by [2, Proposition 1, p. 32], $n$ is prime to $p$, and $K = k(\alpha)$, with $\alpha^n = a$, $p = \alpha a$, and $\Psi = \mathcal{O}a$. Moreover, if $\sigma$ is in $\Gamma$, then $\sigma(a) = \chi(\sigma) a$, with $\chi: \Gamma \simeq \mu_n$ an isomorphism of $\Gamma$ onto the group $\mu_n$ of $n$th roots of 1 in $k$ (in particular, $\Gamma$ is cyclic). Finally, $\mathcal{O}(K/k) = \Psi^{-n+1}$ [2, Theorem 2, p. 21], and thus

$$T(K/k) = \Psi^{-n+1}/\mathcal{O}.$$

Of course, since $\Psi^n = \mathcal{O}p$, $p$ annihilates $T(K/k)$, which can therefore be regarded as a $k(\mathfrak{p})\Gamma$-module.

Now, $T(K/k)$ possesses the descending chain $\{\Psi^i/\mathcal{O}\}$ of $k(\mathfrak{p})\Gamma$-submodules, with $-n + 1 \leq i \leq 0$. Since $k(\mathfrak{p})$ has characteristic prime to the order $n$ of $\Gamma$, it follows that

$$T(K/k) \simeq \bigcup_{i=-1}^{-n+1} \Psi^i/\Psi^{i+1}$$

as $\mathcal{O}\Gamma$-modules (or $k(\mathfrak{p})\Gamma$-modules). However, for any integer $i$, multiplication by $\alpha^i$ yields a $k(\mathfrak{p})$-space isomorphism

$$k(\mathfrak{p}) \simeq K(\Psi) = \mathcal{O}/\Psi \simeq \Psi^i/\Psi^{i+1}$$

and the induced $\Gamma$-module structure on $k(\mathfrak{p})$ is such that $\sigma$ in $\Gamma$ acts via multiplication by $\chi^i(\sigma) (= \chi(\sigma)^i)$. Thus, replacing the character $\chi$ by $\chi^{-1}$, we have that

$$T(K/k) \simeq \bigcup_{i=1}^{n-1} k(\mathfrak{p})$$
with $\Gamma$ acting on the $i$th summand via the character $\chi^i$. That is to say, $T(K/k)$ is isomorphic, as a $k(p)$ $\Gamma$-module, to the direct sum of all irreducible non-principal representations of $\Gamma$ in the field $k(p)$. But we have easily from the definition of $t_r$ that $k(p) \otimes \mathcal{X} T(p, \Gamma)$ is isomorphic as $k(p)$ $\Gamma$-module to the same direct sum, and the lemma follows.

The observations below will be useful in our computation of $T(K/k)$ in a more general case. Let, for the moment, $k \subseteq F \subseteq K$ be fields with $K/k$ finite, normal, and separable with Galois group $\Gamma$. Let

$$(\Gamma, K) = \{ u: \Gamma \to K \}$$

the set of all functions from $\Gamma$ to $K$. We may view $(\Gamma, K)$, on the one hand, as a $K$-algebra with the pointwise operations, and, on the other, as a $k(\Gamma \times \Gamma)$-module, where

$$\{(\sigma, \tau) u(\rho) = \sigma(u(\rho \delta)) \}$$

for $\sigma, \tau, \rho$ in $\Gamma$ and $u$ in $(\Gamma, K)$. We then have the well-known bijection

$$\psi: K \otimes_k K \cong (\Gamma, K)$$

where $\psi(x \otimes y)(\sigma) = x\sigma(y)$ for $x, y$ in $K$ and $\sigma$ in $\Gamma$ (see, e.g., [3, Proposition 1.2 (4), p. 81]). $\psi$ is an isomorphism both of $K$-algebras (if we let $K$ act on $K \otimes_k K$ via the left factor) and of $k(\Gamma \times \Gamma)$-modules (if we let $\Gamma \times \Gamma$ act on $K \otimes_k K$ via the formula $(\sigma, \tau)(x \otimes y) = \sigma(x) \otimes \tau(y)$).

Now let $\Delta$ be a subgroup of $\Gamma$, and $F = K^\Delta$ be the corresponding subfield of $K$. $\psi$ then induces a bijection

$$(\Gamma, K) = (K \otimes_k K)^{\Delta \times 1} \cong (\Gamma, K)^{\Delta \times 1} = (\Gamma, K)^\Delta$$

the right-most term denoting (with some ambiguity of notation) the subset of $(\Gamma, K)$ consisting of all functions $u: \Gamma \to K$ such that $u(\delta \gamma) = \delta(u(\gamma))$ for all $\gamma$ in $\Gamma$, $\delta$ in $\Delta$. This bijection is an isomorphism both of $F$-algebras and of $F\Gamma$-modules (with $\Gamma$ acting on both domain and range as $1 \times \Gamma \subseteq \Gamma \times \Gamma$).

Suppose now that $\mathfrak{o}$ is a Dedekind domain with quotient field $k$, and $\mathfrak{o}_F$ and $\mathfrak{D}$ are the integral closures of $\mathfrak{o}$ in $F$ and $K$, respectively (with $k \subseteq F \subseteq K$ as above). Assume, moreover, that $F/k$ is non-ramified. Then, by the general theory of separable algebras [3, Proposition 2.3, p. 48], $\mathfrak{o}_F \otimes_\mathfrak{o} \mathfrak{D}$ is a hereditary ring and hence the maximal order in $F \otimes_k K$, and therefore the isomorphism of (1.6b) induces an isomorphism

$$\mathfrak{o}_F \otimes_\mathfrak{o} \mathfrak{D} \cong (\Gamma, \mathfrak{D})^\Delta$$

(1.6c)

(the latter being the maximal order in $(\Gamma, K)^\Delta$). Also, $\mathfrak{o}_F \otimes_\mathfrak{o} \mathfrak{D} \subseteq$


\( T(K/k) \subseteq F \otimes_k K \) and \((\Gamma, \mathcal{D})^\Delta \subseteq (\Gamma, \mathcal{E}(K/F))^\Delta \subseteq (\Gamma, K)^\Delta \) and a routine computation then establishes that (1.6b) likewise induces an isomorphism

\[
\mathcal{O}_F \otimes_{\mathcal{O}} \mathcal{E}(K/k) \xrightarrow{\sim} (\Gamma, \mathcal{E}(K/F))^\Delta.
\]  

(1.6d)

Of course, what is behind this fact is simply that the trace map can be defined for arbitrary commutative algebras of finite dimension over a field, and is preserved by base extension and direct product. The same is then true for the codifferent, and so \( \mathcal{E}(F \otimes_k K) = \mathcal{O}_F \otimes_{\mathcal{O}} \mathcal{E}(K/k) \) and \( (\Gamma, \mathcal{E}(K/F))^\Delta = (\Gamma, \mathcal{E}(K/F))^\Delta \); then (1.6b), an isomorphism of Galois extensions of \( F \) with Galois group \( \Gamma \), preserves this data. We note that (1.6c) and (1.6d) are isomorphisms of \( \mathcal{O}_F \Gamma \)-modules.

Putting together (1.6c) and (1.6d), we obtain finally that, if \( F/k \) is non-ramified, then

\[
\mathcal{O}_F \otimes_{\mathcal{O}_k} T(K/k) \xrightarrow{\sim} (\Gamma, T(K/F))^\Delta \xrightarrow{\sim} \mathbb{Z} \Gamma \otimes_{\mathbb{Z}_{\Delta}} T(K/F)
\]

(1.6e)

as \( \mathcal{O}_F \Gamma \)-modules, the latter isomorphism following from the well-known and easily verified fact that \((\Gamma, M)^\Delta \approx \mathbb{Z} \Gamma \otimes_{\mathbb{Z}_{\Delta}} M\) as \( R \Gamma \)-modules for any \( R \Delta \)-module \( M \), \( R \) any ring.

**Theorem 1.7.** Let \( \mathcal{O} \) be a complete discrete valuation ring with quotient field \( k \), and \( K \) be a finite normal separable tame extension of \( k \) with Galois group \( \Gamma \). Then

\[
T(K/k) \approx k(p) \otimes_{\mathbb{Z}} (\mathbb{Z} \Gamma \otimes_{\mathbb{Z}_{\Delta}} T(p, \Delta))
\]

as \( \mathcal{O} \Gamma \)-modules, with \( \Delta \) the inertial group of \( K/k \).

**Proof:** Let \( F = K^\Delta \) denote the maximal non-ramified extension of \( k \) in \( K \). Let \( \mathcal{O}_r \) and \( \mathcal{O} \) be as in the preceding discussion, and denote the residue fields of \( k \) and \( F \) by \( k(p) \) and \( F(p) \), respectively, with \( p \) the maximal ideal of \( \mathcal{O} \). \( K/F \) is then tame and totally ramified [2, Theorem 2, p. 27], and hence we can apply Lemma 1.4 to it, obtaining, via (1.6e), the \( \mathcal{O}_F \Gamma \)-module isomorphism

\[
\mathcal{O}_F \otimes_{\mathcal{O}_k} T(K/k) \xrightarrow{\sim} F(p) \otimes_{\mathbb{Z}} (\mathbb{Z} \Gamma \otimes_{\mathbb{Z}_{\Delta}} T(p, \Delta))
\]

It is then clear that \( p \) annihilates \( T(K/k) \) (since it annihilates \( F(p) \)), and thus, regarding it as a \( k(p) \Gamma \)-module, we may replace the left term above by \( F(p) \otimes_{k(p)} T(K/k) \). Writing \( F(p) \) as \( F(p) \otimes_{k(p)} k(p) \), we then obtain the \( \mathcal{O}_F \Gamma \)-module (or \( F(p) \Gamma \)-module) isomorphisms

\[
F(p) \otimes_{k(p)} T(K/k) \approx F(p) \otimes_{k(p)} [k(p) \otimes_{\mathbb{Z}} (\mathbb{Z} \Gamma \otimes_{\mathbb{Z}_{\Delta}} T(p, \Delta))].
\]
Finally, since all terms are $F(p)\Gamma$-modules of finite length, we may apply the Krull–Schmidt theorem to conclude that
\[ T(K/k) \simeq k(p) \otimes \mathbb{Z} \{\mathbb{Z} \otimes \mathbb{Z}_A T(p, \Delta)\} \]
as $k(p)\Gamma$-modules, hence as $\mathfrak{o}\Gamma$-modules. This completes the proof of the theorem.

We turn finally to the tame global case.

**Theorem 1.8.** Let $\mathfrak{o}$ be a Dedekind domain with quotient field $k$, $K$ be a finite normal separable tame extension of $k$ with Galois group $\Gamma$, and $\mathfrak{O}$ be the integral closure of $\mathfrak{o}$ in $K$.

(a) If $p$ is a non-zero prime of $\mathfrak{o}$, then
\[ T(K/k)_p \simeq k(p) \otimes \mathbb{Z} \{\mathbb{Z} \otimes \mathbb{Z}_A T(p, \Delta)\} \]
as $\mathfrak{o}\Gamma$-modules, with $k(p) = \mathfrak{o}/p$, $\Delta$ the inertial group of a prime of $\mathfrak{O}$ above $p$, and $p$ the characteristic of $k(p)$.

(b) Let $p_1, \ldots, p_r$ be all primes of $\mathfrak{o}$ which ramify in $K$, and for each $i$ let $\Delta_i$ be the inertial group of a prime of $\mathfrak{O}$ above $p_i$. Then
\[ T(K/k) \simeq \bigsqcup_{i=1}^r k(p_i) \otimes \mathbb{Z} \{\mathbb{Z} \otimes \mathbb{Z}_{\Delta_i} T(p_i, \Delta_i)\} \]
as $\mathfrak{o}\Gamma$-modules, with $p_i$ the characteristic of $k(p_i)$.

**Proof:** Since $T(K/k)$ is a torsion $\mathfrak{o}$-module
\[ T(K/k) = \bigsqcup_p T(K/k)_p \]
with $p$ tracing all non-zero primes of $\mathfrak{o}$. Moreover, it follows from the definition of $T(K/k)$ that $T(K/k)_p = 0$ if and only if $p$ does not ramify in $K$. Hence
\[ T(K/k) = \bigsqcup_{i=1}^r T(K/k)_{p_i} \]
with $p_i$ ($i \leq r$) as in (b), and so (b) is a consequence of (a).

We now prove (a). Let $p$ be a non-zero prime of $\mathfrak{o}$, $\mathfrak{P}$ be a prime of $\mathfrak{O}$ above $p$, and $\Gamma_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$. Then [2, (2), p. 15] can be interpreted as asserting the existence of an isomorphism
\[ k_p \otimes_k K \xrightarrow{\sim} (\Gamma, K_{\mathfrak{P}})^{\Gamma_{\mathfrak{P}}} \] (1.9a)
of $k_p$-algebras and $k_p\Gamma$-modules (the isomorphism sending $x \otimes y$ in $k_p \otimes_k K$ to the function $u: \Gamma \to K_p$, where $u(y) = x\gamma(y)$ for $y$ in $\Gamma$). Moreover, this bijection induces an $o_p$-algebra and $o_p\Gamma$-module isomorphism

$$o_p \otimes o_\mathcal{O} \cong (\Gamma, \mathcal{O}_\Psi)^{\Gamma \Psi} \quad (1.9b)$$

[2, Lemma 2, p. 15]. In particular, $o_p \otimes o_\mathcal{O}$ is the maximal order in $k_p \otimes_k K$.

An argument entirely similar to that of the proof of (1.6d) and Theorem 1.7 then yields an isomorphism

$$T(K/k)_p = o_p \otimes o_\mathcal{O} T(K/k) \cong (\Gamma, T(K_\Psi/k_\Psi))^{\Gamma \Psi} \quad (1.9c)$$

of $o_p\Gamma$-modules. Hence, if $\Delta_\Psi$ is the inertial group of $\Psi$, we may apply Theorem 1.7 to obtain the following isomorphisms of $o\Gamma$-modules:

$$T(K/k)_p \cong (\Gamma, T(K_\Psi/k_\Psi))^{\Gamma \Psi}$$

$$\cong \mathbb{Z} \Gamma \otimes \mathbb{Z}_\Psi T(K_\Psi/k_\Psi)$$

$$\cong \mathbb{Z} \Gamma \otimes \mathbb{Z}_\Psi \{k(p) \otimes \mathbb{Z} (\mathbb{Z} \Gamma \otimes \mathbb{Z}_\Psi T(p, A_\Psi))\}$$

$$\cong k(p) \otimes \mathbb{Z} (\mathbb{Z} \Gamma \otimes \mathbb{Z}_\Psi T(p, A_\Psi)).$$

This establishes (a) and completes the proof of the theorem.

In the remainder of this section we apply Theorem 1.8 to obtain information on the Galois module structure of $\mathcal{O}$. If $M$ is an $o\Gamma$-module (e a Dedekind domain, $\Gamma$ a finite group), we say that $M$ is stably self-dual if there is a finitely generated projective $o\Gamma$-module $P$ such that

$$\text{Hom}_o(M, o) \oplus P \cong M \oplus P \quad (1.10)$$

as $o\Gamma$-modules, the $o\Gamma$-module structure on $\text{Hom}_o(M, o)$ being defined by the formula $\sigma(f)(x) = f(\sigma^{-1}x)$ for $\sigma$ in $\Gamma$, $f$ in $\text{Hom}_o(M, o)$, and $x$ in $M$. Of course, in that case $P$ can be chosen to be a free $o\Gamma$-module. Recall, moreover, that $M$ is called stably free if there exists a finitely generated free $o\Gamma$-module $F$ such that $M \oplus F$ is likewise free. If $M$ is stably free, then it is necessarily stably self-dual.

The results below generalize theorems of A. Sze [12, Proposition 3.1] and M. Taylor [13], respectively.

**Theorem 1.11.** Let $K/k, \Gamma, \text{etc.}$, be as in Theorem 1.8 (in particular, $K/k$ is tame), and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\Delta_1, \ldots, \Delta_n$ be as in Theorem 1.8(b). Assume that $k$ is a finite separable extension of a field $k'$, and $o'$ is a Dedekind
domain with quotient field \( k' \). Then \( \mathfrak{D} \) is a stably self-dual \( o'T \)-module if and only if

\[
N = \bigoplus_{i=1}^{r} s_i o'T \otimes_{o'A_i} \langle p'_i, t_{\Delta_i} \rangle
\]

is a stably free \( o'T \)-module, where \( \langle p'_i, t_{\Delta_i} \rangle \) is the left ideal of \( o'A_i \) generated by \( p'_i = p_i \cap o' \) and \( t_{\Delta_i} \), respectively, and \( s_i = [k(p_i): k'(p'_i)] \).

**Proof:** (1.1) and (1.2) yield an exact sequence

\[
0 \to \mathfrak{D} \to \text{Hom}_o(\mathfrak{D}, o) \to T(K/k) \to 0
\]
of \( oT \)-modules. Moreover, by Theorem 1.8 (b),

\[
T(K/k) \cong \bigoplus_{i=1}^{r} k(p_i) \otimes_{k(p'_i)} \langle p'_i, t_{\Delta_i} \rangle T(p_i, A_i)
\]

as \( oT \)-modules. Now, the obvious \( F_{p_i} A_i \)-module exact sequence

\[
0 \to \bigoplus_{i=1}^{r} k(p_i) \otimes_{k(p'_i)} \langle p'_i, t_{\Delta_i} \rangle T(p_i, A_i) \to 0
\]
gives rise to the \( k(p'_i) A_i \)-module exact sequence

\[
0 \to \bigoplus_{i=1}^{r} k(p_i) \otimes_{k(p'_i)} \langle p'_i, t_{\Delta_i} \rangle T(p_i, A_i) \to 0
\]

and hence also to the \( o'A_i \)-module exact sequence

\[
0 \to \bigoplus_{i=1}^{r} k(p_i) \otimes_{k(p'_i)} \langle p'_i, t_{\Delta_i} \rangle T(p_i, A_i) \to 0
\]

since the inverse image of \( \{k(p'_i) A_i\} t_{\Delta_i} \), under the canonical homomorphism \( o'A_i \to k(p'_i) A_i \), is simply \( \langle p'_i, A_i \rangle \). It then follows easily that we have a short exact sequence

\[
0 \to N \to F \to T(K/k) \to 0
\]
of \( o'T \)-modules with \( F \) a free \( o'T \)-module of rank \( s = \sum_{i=1}^{r} s_i \). Finally, since \( K/k \) is tame, \( \mathfrak{D} \) and \( \text{Hom}_o(\mathfrak{D}, o) \) are \( oT \)-projective [2, p. 22], and hence,

\[
\text{Hom}_o(\mathfrak{D}, o) \oplus N \cong \mathfrak{D} \oplus F
\]
by Schanuel's Lemma [1, Proposition 6.3, p. 36]. A routine rank argument then yields the theorem.

**Corollary 1.12.** Let \( K/k \) be a normal separable tame extension of algebraic number fields with Galois group \( \Gamma \), and \( \mathcal{O} \) be the ring of integers in \( K \). Then \( \mathcal{O} \) is a stably self-dual \( \mathbb{Z}\Gamma \)-module.

**Proof:** We apply Theorem 1.11 with \( k' = \mathbb{Q} \) and \( \sigma' = \mathcal{O} \). In this case

\[
N = \bigoplus_{i=1}^{r} s_i \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\mathcal{A}_i} \langle p_i, t_{\mathcal{A}_i} \rangle
\]

where \( p_1, \ldots, p_r \) are ordinary prime numbers. Since the inertial group \( \mathcal{A}_i \) is cyclic of order prime to \( p_i \) [2, Theorem 1, p. 29], it follows from a well-known result of Swan [11, Corollary 6.1, p. 280] that \( \langle p_i, t_{\mathcal{A}_i} \rangle \) is a free \( \mathbb{Z}\mathcal{A}_i \)-module, and hence \( N \) is a free \( \mathbb{Z}\Gamma \)-module. This completes the proof.

**Remarks 1.13.** Using arithmetic methods, Cassou-Nogues and Queyrut [16, Corollaire 6.3, p. 23] have proved a self-duality theorem for arbitrary (i.e., not necessarily tame) extensions of algebraic number fields which generalizes Corollary 1.12. More recently, M. Desrochers has used the torsion Galois module \( T(K/k) \) and the techniques of this section to obtain an algebraic proof of their result [4, Theorem 5.1].

2. **The Torsion Galois Module \( R(K/k) \)**

Let \( \mathfrak{o} \) be a Dedekind domain with quotient field \( k \), \( K \) be a finite Galois extension of \( k \) with Galois group \( \Gamma \), and \( \mathcal{O} \) be the maximal \( \mathfrak{o} \) order in \( K \). The remarks following (1.6a) imply that the bijection \( \psi: K \otimes_k \mathfrak{o} \overset{\sim}{\rightarrow} (\Gamma, K) \) introduced there is an isomorphism of \( K\Gamma \)-modules, with \( K, \Gamma \) acting on the left and right factors of \( K \otimes_k K \), respectively, and the \( K\Gamma \)-module structure of \( (\Gamma, K) \) given by the formula \( (a\sigma) u(\tau) = au(\sigma\tau) \) for \( a \in K; \sigma, \tau \in \Gamma; \) and \( u \) in \( (\Gamma, K) \). Restricting \( \psi \) to \( \mathcal{O} \otimes_\mathfrak{o} \mathcal{O} \subseteq K \otimes_k K \) then yields an injection

\[
\psi: \mathcal{O} \otimes_\mathfrak{o} \mathcal{O} \rightarrow (\Gamma, \mathcal{O})
\]

of left \( \mathcal{O}\Gamma \)-modules. We define

\[
R(K/k) = \operatorname{Coker}\{\psi: \mathcal{O} \otimes_\mathfrak{o} \mathcal{O} \rightarrow (\Gamma, \mathcal{O})\}
\]

(2.1)

a left \( \mathcal{O}\Gamma \)-module. Since \( (\Gamma, \mathcal{O}) \) is a finitely generated \( \mathcal{O} \)-module and \( \mathcal{O} \otimes_\mathfrak{o} \mathcal{O} \) contains a \( K \)-basis of \( K \otimes_k K \), \( R(K/k) \) is then a finitely generated torsion \( \mathcal{O} \)-module.
In this section and the next we shall elaborate some of the elementary properties of $R(K/k)$, discuss its connection with the Galois module structure of $\mathcal{O}$, compute it in important special cases, and prove some of the fundamental "change-of-base" formulae used in these computations. For $K/k$ tame, $R(K/k)$ is closely related to the "resolvent" character functions of [5, Sect. 1, pp. 384–390]. Its connection with the Galois module $T(K/k)$ introduced in Section 1 arises through Theorem 2.4 below, which is a module-theoretic counterpart of the "conductor-resolvent formula" [5, Theorem 18, p. 423].

For this theorem we shall need the concept of the transpose $M'$ of a finitely generated torsion $\mathfrak{o}$-module $M$, which is defined by the condition

$$M' = \text{Hom}_\mathfrak{o}(M, k/\mathfrak{o}).$$

Just as with ordinary duality of finite abelian groups, one sees that $M' \cong M$ as $\mathfrak{o}$-modules (although not in a natural way); in particular, $M'$ is likewise finitely generated and torsion. Moreover, the assertions below follow quickly from standard homological algebra:

$$M' \cong \text{Ext}^1_\mathfrak{o}(M, \mathfrak{o})$$

the isomorphism being the appropriate connecting homomorphism in the long exact sequence for $\text{Ext}^\bullet_{\mathfrak{o}}(M, -)$ which arises from the short exact sequence $0 \to \mathfrak{o} \to k \to k/\mathfrak{o} \to 0$.

If $M = \text{Coker}(f)$, with $f : Q \to P$

an injection of finitely generated projective $\mathfrak{o}$-modules, then there is a short exact sequence

$$0 \to \text{Hom}_\mathfrak{o}(P, \mathfrak{o}) \xrightarrow{\text{Hom}_\mathfrak{o}(f, \mathfrak{o})} \text{Hom}_\mathfrak{o}(Q, \mathfrak{o}) \to M' \to 0$$

the unlabeled arrow denoting the composition of the connecting homomorphism $\text{Hom}_\mathfrak{o}(Q, \mathfrak{o}) \to \text{Ext}^1_\mathfrak{o}(M, \mathfrak{o})$ and the inverse of the isomorphism (2.3a).

**Theorem 2.4.** Let $\mathfrak{o}$ be a Dedekind domain with quotient field $k$, $K$ be a Galois extension of $k$ with Galois group $\Gamma$, and $\mathcal{O}$ be the maximal $\mathfrak{o}$-order in $K$. Then there is an exact sequence of $\mathcal{O}\Gamma$-modules

$$0 \to R(K/k) \to \mathcal{O} \otimes_{\mathfrak{o}} T(K/k) \to R(K/k)' \to 0$$

where $R(K/k)' = \text{Hom}_\mathfrak{o}(R(K/k), K/\mathcal{O})$ is the transpose of the $\mathcal{O}$-module $R(K/k)$. 
Proof. Let $t_{B/\mathcal{O}}$ be the trace map of the $\mathcal{O}$-algebra $B = (\Gamma, \mathcal{O})$; $t_{B/\mathcal{O}}$ satisfies the formula

$$t_{B/\mathcal{O}}(u) = \sum_{\sigma \in \Gamma} u(\sigma) \quad (u \in (\Gamma, \mathcal{O}))$$

and gives rise to an isomorphism of $\mathcal{O}\Gamma$-modules

$$j_{B/\mathcal{O}}: B \xrightarrow{\sim} \text{Hom}_\mathcal{O}(B, \mathcal{O}) \quad (2.5a)$$

where

$$j_{B/\mathcal{O}}(u)(v) = t_{B/\mathcal{O}}(uv) = \sum_{\sigma \in \Gamma} u(\sigma) v(\sigma)$$

for $u, v$ in $B$. These assertions can be verified easily by direct computation, or by using the fact that $B$ is a Galois extension of $\mathcal{O}$ with Galois group $\Gamma$ (see [3], especially Proposition 1.2, pp. 80–81, and Definition, pp. 84–85]).

This isomorphism then fits into the commutative diagram of $\mathcal{O}\Gamma$-module homomorphisms

$$\begin{array}{ccc}
\mathcal{O} \otimes_\mathcal{O} \mathcal{O} & \xrightarrow{\psi} & B & \xrightarrow{j_{B/\mathcal{O}}} & \text{Hom}_\mathcal{O}(B, \mathcal{O}) & \xrightarrow{\psi'} & \text{Hom}_\mathcal{O}(\mathcal{O} \otimes_\mathcal{O} \mathcal{O}, \mathcal{O}) \\
\downarrow & & & \downarrow \approx & & \downarrow \approx & \\
\mathcal{O} \otimes_\mathcal{O} \mathcal{O} & \xrightarrow{\text{id} \otimes j} & \mathcal{O} \otimes_\mathcal{O} \text{Hom}_\mathcal{O}(\mathcal{O}, \mathcal{O})
\end{array} \quad (2.5b)$$

where the right-most vertical isomorphism is the canonical one, $\psi' = \text{Hom}_\mathcal{O}(\psi, \mathcal{O})$, and the injection $j: \mathcal{O} \to \text{Hom}_\mathcal{O}(\mathcal{O}, \mathcal{O})$ is induced by the isomorphism $j: K \xrightarrow{\sim} \text{Hom}_\mathcal{O}(K, K)$ discussed before (1.2). Of course, $\psi$, $1_\mathcal{O} \otimes j$, and $\psi'$ are injections, $\psi'$ being so because $R(K/k) = \text{Coker}(\psi)$ is a torsion $\mathcal{O}$-module. That the diagram commutes follows immediately from naturality properties of the trace map; it can also be verified easily by direct computation.

Now, since $\mathcal{O}$ is a projective $\mathcal{O}$-module, $\text{Coker}(1_\mathcal{O} \otimes j) \approx \mathcal{O} \otimes_\mathcal{O} T(K/k)$ as $\mathcal{O}\Gamma$-modules. Moreover, (2.3b) yields an $\mathcal{O}\Gamma$-module isomorphism $\text{Coker} (\psi') \approx R(K/k)'$. The desired exact sequence follows immediately, completing the proof.

Next we examine $R(K/k)$ for the case in which $k$ is the quotient field of a complete discrete valuation ring $\mathfrak{o}$ with prime $p$, and $K$ is a tame and totally ramified Galois (field) extension of $k$ of degree $n$ with Galois group $\Gamma$. Let $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in $K$, and $\mathfrak{p}$ be the prime of $\mathcal{O}$. Recall that then, as noted in the proof of Lemma 1.4, $n$ is prime to the characteristic $p$ of $k(p)$,
and \( K = k(a) \), where \( a^n = a \) in \( k \), \( \mathfrak{P} = \mathfrak{D}a \), and \( p = \mathfrak{p}a \). Moreover, there is an isomorphism

\[
\chi: \Gamma \xrightarrow{\sim} \mu_n
\]  

(2.6)

(with \( \mu_n \) the group of \( n \)th roots of 1 in \( k \)) such that \( \sigma(a) = \chi(\sigma)a \) for all \( \sigma \) in \( \Gamma \). Sometimes it will be convenient for us to identify \( \mu_n \) with the group of \( n \)th roots of 1 in \( k(p) \) under the bijection induced by the residue map \( \sigma \to k(p) \). Note that the character \( \chi \) is unique; e.g., it is uniquely specified by the condition that \( \sigma(x) \equiv \chi(\sigma)x \mod \mathfrak{P}^2 \) for all \( x \) in \( \mathfrak{P} \). Finally, if \( M \) is an \( \mathfrak{D} \)-module and \( i \) is an integer, we shall denote by \( M_i \) the \( \mathfrak{D}\Gamma \)-module defined by the conditions that

\[
M_i = M \quad \text{as } \mathfrak{D}\text{-modules} \quad (2.7a)
\]

\[
\sigma(m) = \chi^i(\sigma)m \quad \text{for } \sigma \text{ in } \Gamma \text{ and } m \text{ in } M \quad (2.7b)
\]

**Theorem 2.8.** Let \( K/k \), etc., be as in the preceding paragraph. Then

\[
R(K/k) \simeq \bigoplus_{i=1}^{n-1} (\mathfrak{D}/\mathfrak{P}^i)_i
\]

as \( \mathfrak{D}\Gamma \)-modules.

**Proof.** Since \( \mathfrak{D} = \mathfrak{o}[a] \) by [2, Theorem 1(ii), p. 23], \( \{1, a, \ldots, a^{n-1}\} \) is a basis of the free \( \mathfrak{o} \)-module \( \mathfrak{D} \), and thus \( \{1 \otimes 1, 1 \otimes a, \ldots, 1 \otimes a^{n-1}\} \) is a basis of the free \( \mathfrak{D} \)-module \( \mathfrak{D} \otimes \mathfrak{D} \). Moreover, if \( \psi: K \otimes_{\mathfrak{D}} K \xrightarrow{\sim} (\Gamma, K) \) is as in (1.6a), then an easy computation shows that \( \psi(1 \otimes a^i) = a^i u_i \), where \( u_i \) in \( (\Gamma, \mathfrak{D}) \) satisfies the condition \( u_i(\sigma) = \chi^i(\sigma) \) for \( \sigma \) in \( \Gamma \). Since \( \chi: \Gamma \xrightarrow{\sim} \mu_n \) is an isomorphism, it is well known that the matrix \( (\chi^i(\sigma)) \) (where \( 0 \leq i < n \) and \( \sigma \) is in \( \Gamma \)) is invertible over \( \mathfrak{o} \), and thus \( \{u_0, u_1, \ldots, u_{n-1}\} \) is a basis of the free \( \mathfrak{D} \)-module \( (\Gamma, \mathfrak{D}) \). Since \( \mathfrak{D}a^i = \mathfrak{P}^i \) and the definition of the \( \mathfrak{K}\Gamma \)-module structure on \( (\Gamma, \mathfrak{D}) \) yields easily that \( \gamma(u_i) = \chi^i(\gamma) u_i \) for \( \gamma \) in \( \Gamma \), the theorem then follows from (2.1).

**Remarks 2.9.** Here is an alternate approach to avoid the computation that the matrix \( (\chi^i(\sigma)) \) is invertible. Since \( \psi \) is injective, \( \{u_0, \ldots, u_{n-1}\} \) is a basis of a free \( \mathfrak{D} \)-submodule \( F \) of \( (\Gamma, \mathfrak{D}) \). Now use Lemma 1.4 and Theorem 2.4 to show that the finitely generated torsion \( \mathfrak{D} \)-modules \( R(K/k) \) and \( F/\text{Im}(\psi) \) have the same length and hence \( F = (\Gamma, \mathfrak{D}) \).

Before turning to more involved computations in further special cases, we show that the \( \mathfrak{o}\Gamma \)-module \( R(K/k) \) completely determines the "local" Galois module structure of \( \mathfrak{D} \), and provides much information regarding the "global" Galois module structure of \( n\mathfrak{D} \), with \( n = [K:k] \).
THEOREM 2.10. Let \( D \) be a Dedekind domain with quotient field \( k \), \( \Gamma \) be a finite group of order \( n \), \( K \) and \( K' \) be Galois extensions of \( k \) with Galois group \( \Gamma \), and \( \mathfrak{O} \) and \( \mathfrak{O}' \) be the maximal \( \mathfrak{o} \)-orders in \( K \) and \( K' \), respectively. Assume that \( R(K/k) \approx R(K'/k) \) as \( \mathfrak{o}\Gamma \)-modules. Then:

(a) \( \mathfrak{o}_p \otimes \mathfrak{O} \approx \mathfrak{o}_p \otimes \mathfrak{O}' \) as \( \mathfrak{o}\Gamma \)-modules for all primes \( p \) of \( \mathfrak{o} \). Hence \( \mathfrak{O} \) and \( \mathfrak{O}' \) are in the same "genus" of \( \mathfrak{o}\Gamma \)-lattices (see [10, p. 232]).

(b) If \( \mathfrak{O} \) and \( \mathfrak{O}' \) are free \( \mathfrak{o} \)-modules, then there is a finitely generated free \( \mathfrak{o}\Gamma \)-module \( F \) such that

\[
(n\mathfrak{O}) \oplus F \approx (n\mathfrak{O}') \oplus F
\]

as \( \mathfrak{o}\Gamma \)-modules, i.e., \( n\mathfrak{O} \) and \( n\mathfrak{O}' \) are "stably isomorphic."

Proof: We look at the short exact sequences of \( \mathfrak{o}\Gamma \)-modules arising from the definition (2.1) of \( R(K/k) \), namely,

\[
0 \rightarrow \mathfrak{O} \otimes \mathfrak{o} \rightarrow (I, \mathfrak{O}) \rightarrow R(K/k) \rightarrow 0
\]

\[
0 \rightarrow \mathfrak{O}' \otimes \mathfrak{o} \rightarrow (I, \mathfrak{O}') \rightarrow R(K'/k) \rightarrow 0.
\]

By the remark following (1.6e), \( (I, \mathfrak{O}) \approx \mathfrak{O}\Gamma \), etc., as \( \mathfrak{o}\Gamma \)-modules; thus the middle terms of the above sequences are \( \mathfrak{o}\Gamma \)-projective, and Schanuel’s Lemma [1, Proposition 6.3, p. 36] then implies that

\[
(\mathfrak{O} \otimes \mathfrak{o}) \otimes (\mathfrak{O}\Gamma) \approx (\mathfrak{O}' \otimes \mathfrak{o}) \otimes (\mathfrak{O}'\Gamma)
\]

as \( \mathfrak{o}\Gamma \)-modules. If \( \mathfrak{O} \) and \( \mathfrak{O}' \) are free \( \mathfrak{o} \)-modules, then \( \mathfrak{O} \otimes \mathfrak{o} \approx n\mathfrak{O} \) and \( \mathfrak{O}' \otimes \mathfrak{o} \approx n\mathfrak{O}' \) as \( \mathfrak{o}\Gamma \)-modules, \( \mathfrak{O}\Gamma \approx \mathfrak{O}'\Gamma \approx F \) is a free \( \mathfrak{o}\Gamma \)-module of rank \( n \), and (b) then follows easily from (2.11).

On the other hand, if \( p \) is as in (a) \( \mathfrak{o}_p \otimes \mathfrak{O} \) and \( \mathfrak{o}_p \otimes \mathfrak{O}' \) are free \( \mathfrak{o}_p \)-modules, and so we may apply the functor \( \mathfrak{o}_p \otimes (-) \) to both sides of (2.11) to obtain an \( \mathfrak{o}_p\Gamma \)-module isomorphism

\[
n((\mathfrak{o}_p \otimes \mathfrak{O}) \oplus \mathfrak{o}_p \Gamma) \approx n((\mathfrak{o}_p \otimes \mathfrak{O}') \oplus \mathfrak{o}_p \Gamma).
\]

The Krull–Schmidt Theorem for \( \mathfrak{o}_p\Gamma \)-modules [10, Exercise 6, pp. 88–89] then implies that

\[
\mathfrak{o}_p \otimes \mathfrak{O} \approx \mathfrak{o}_p \otimes \mathfrak{O}'
\]

as \( \mathfrak{o}_p\Gamma \)-modules, completing the proof of (a) and the theorem.

We devote the remainder of this section to descriptions of composition series of \( R(K/k) \) for certain abelian extensions \( K/k \). In order to discuss these composition series in a systematic way, we shall use the "semi-simplification" of a module with finite length, which we introduce forthwith
(the appropriate Grothendieck groups would provide a slicker treatment, but at the price of more space and greater abstraction).

**Definition and Remarks 2.12.** Let $R$ be any ring, $M$ be an $R$-module of finite length, and

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_r = 0$$

be a composition series of $M$, i.e., $M_i/M_{i-1}$ is a simple $R$-module for all $i < r$. We define the **semi-simplification of $M$** to be the semi-simple $R$-module

$$\mathfrak{s}_R(M) = \bigoplus_{i=0}^{r-1} M_i/M_{i+1}.$$

Of course, the Jordan–Hölder Theorem implies that the isomorphism class of $\mathfrak{s}_R(M)$ is independent of the choice of composition series of $M$.

**Example 2.13.** Let $K/k$, etc., be as in Theorem 2.8. Then, for $i > 0$, the $\mathcal{O}I$-module $(\mathcal{O}/\mathfrak{p}^i)_i$ has the composition series

$$(\mathcal{O}/\mathfrak{p}^i)_i \supseteq (\mathfrak{p}/\mathfrak{p}^i)_i \supseteq \cdots \supseteq (\mathfrak{p}^{i-1}/\mathfrak{p}^i)_i \supseteq 0$$

with simple factor modules isomorphic to $K(\mathfrak{p})_i$, where $K(\mathfrak{p})$ is the residue field of $K$ (recall that the $\mathcal{O}I$-modules $K(\mathfrak{p})_i$, etc., are defined in (2.7)). Hence, by the theorem

$$\mathfrak{e}_{\mathfrak{o}I}(R(K/k)) \cong \bigoplus_{i=1}^{n-1} iK(\mathfrak{p})_i$$

as $\mathfrak{o}I$-modules. Since $K/k$ is totally ramified, $K(\mathfrak{p}) = k(\mathfrak{p})$, the residue field of $k$, and so

$$\mathfrak{e}_{\mathfrak{o}I}(R(K/k)) \cong \bigoplus_{i=1}^{n-1} ik(\mathfrak{p})_i$$

as $\mathfrak{o}I$-modules.

The following change-of-base formulae for $R(K/k)$ will play an important role in our computations; they will be proved in Section 3, Corollaries 3.8 and 3.11. Let $\mathfrak{o}$ be a Dedekind domain with quotient field $k$, $K$ be a Galois extension of $k$ with Galois group $\Gamma$, and $\mathcal{O}$ be the maximal $\mathfrak{o}$-order in $K$.

(2.14a) Assume that $K$ is a field, and let $\Delta$ be a subgroup of $\Gamma$ such that $F = K^\Delta$ is non ramified over $k$. Then

$$R(K/k) \cong \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} R(K/F)$$

as $\mathfrak{o}I$-modules.
(2.14b) Let \( p \) be a prime of \( \mathfrak{o} \), \( \mathfrak{P} \) be a prime of \( \mathfrak{O} \) above \( p \), and \( \Gamma_{\mathfrak{P}} \subseteq \Gamma \) be the decomposition group of \( \mathfrak{P} \). Then

\[
R(K/k)_p \simeq \left[ \Gamma; \Gamma_{\mathfrak{P}} \right] \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\mathfrak{P}} R(K_{\mathfrak{P}}/k_p)
\]

as \( \mathfrak{o}\Gamma \)-modules.

(2.13) and (2.14) yield a concise formula for the semi-simplification of certain primary components of \( R(K/k) \).

**Theorem 2.15.** Let \( \mathfrak{o} \) be a Dedekind domain with quotient field \( k \), \( K \) be a Galois extension of \( k \) with Galois group \( \Gamma \) of order \( n \), and \( \mathfrak{O} \) be the maximal \( \mathfrak{o} \)-order in \( K \). Let \( p \) be a prime of \( \mathfrak{o} \) which is ramified in \( K \), \( \Delta \subseteq \Gamma \) be the inertial group of a prime \( \mathfrak{P} \) of \( \mathfrak{O} \) above \( p \), and \( F = K_{\mathfrak{P}}^\Delta \). Assume finally that the characteristic of \( k(p) \) is prime to \( n \). Then there is an isomorphism \( \chi: \Delta \xrightarrow{\sim} \mu_d(F(p)) \), with \( d = [\Delta: 1] \), such that

(a) \[
\sigma\mathfrak{a}^\mathfrak{r}(R(K/k)_p) \simeq \frac{n}{sd} \prod_{i=1}^{d-1} i\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} F(p)_i
\]

as \( \mathfrak{o}\Gamma \)-modules, where \( s = [F:k_p] \) and the \( \mathfrak{o}\Delta \)-module \( F(p)_i \) is defined as in (2.7) relative to the character \( \chi \). If \( k(p) \) contains all \( d \)th roots of 1, then

(b) \[
\sigma\mathfrak{a}^\mathfrak{r}(R(K/k)_p) \simeq \frac{n}{d} \prod_{i=1}^{d-1} i\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} k(p)_i.
\]

**Proof.** Note first that (b) is meaningful, since if \( k(p) \) contains all \( d \)th roots of 1, then \( \chi \) takes values in \( \mu_d(k(p)) \). Observe also that, since the characteristic of \( k(p) \) is prime to \( n \), all terms in the above formulac are semi-simple \( \mathfrak{o}\Gamma \)-modules; moreover, \( K_{\mathfrak{P}}/k_p \) is tame \cite[Theorem 1, p. 29]{2}. \( K_{\mathfrak{P}}/F \) is then tame and totally ramified, and so we have the “canonical character”

\[
\chi: \Delta \xrightarrow{\sim} \mu_d(F(p))
\]

of (2.6) which (given \( \mathfrak{P} \)) is uniquely determined by the condition

\[
\sigma(x) \equiv \chi(\sigma) x \pmod{\mathfrak{P}^2}.
\]

(2.16)

(2.13) and (2.14) then yield that

(2.17)

\[
\sigma\mathfrak{a}^\mathfrak{r}(R(K/k)_p) \simeq \left[ \Gamma; \Gamma_{\mathfrak{P}} \right] \prod_{i=1}^{d-1} i\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} F(p)_i
\]

as \( \mathfrak{o}\Gamma \)-modules, with \( \Gamma_{\mathfrak{P}} \subseteq \Gamma \) the decomposition group of \( \mathfrak{P} \) (note that we are using the fact that the functors \( \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\mathfrak{P}} (-) \) and \( \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\mathfrak{P}} (-) \), being exact,
preserve semi-simplifications). Equation (2.17), together with the equation $n = sd[G: F_p]$, yields (a). Part (b) then follows from (a) and the observation that if $\chi$ takes values in $\mu_d(k(p))$ then $F(p)_i \approx sk(p)_i$ as $oI$-modules. This completes the proof of the theorem.

We now specialize to the case in which $K/k$ is cyclic. If $x$ is a rational number we shall denote the fractional part of $x$ by $\langle x \rangle$, i.e., $\langle x \rangle$ is the unique rational number satisfying the conditions

$$0 \leq \langle x \rangle < 1 \quad (2.18a)$$

$$\langle x \rangle \equiv x \pmod{\mathbb{Z}}. \quad (2.18b)$$

In particular, if $m, n$ are natural numbers and $m = nq + r$ with $0 \leq r < n$, then

$$\left\lfloor \frac{m}{n} \right\rfloor = \frac{r}{n} \quad \text{and} \quad r = n \left\lfloor \frac{m}{n} \right\rfloor. \quad (2.18c)$$

**Corollary 2.19.** Let $K/k$, $\mathfrak{o} \subseteq \mathcal{O}, p$, etc., satisfy the hypotheses of Theorem 2.15. Assume in addition that the Galois group $\Gamma$ of $K/k$ is cyclic of order $n$ and $k(p)$ contains all $n$th roots of 1. Then there exists an isomorphism

$$\chi: \Gamma \rightarrow \mu_n(k(p))$$

such that

$$\phi_a(R(K/k)_p) \cong \bigoplus_{i=1}^{n-1} n \left\lfloor \frac{ri}{n} \right\rfloor k(p)_{\sigma_i}$$

with $r = [\Gamma: A]$ and $k(p)_i$ as in (2.7) relative to the character $\chi$.

**Proof.** If $\Gamma'$ is a subgroup of $\Gamma$ and $\chi': \Gamma' \rightarrow \mu_n(k(p))$ is a homomorphism, we denote by $k(p)(\chi')$ the $k(p)\Gamma'$-module (hence $oI'$-module) defined by the conditions that $k(p)(\chi') = k(p)$ as a $k(p)$-space and $\sigma(x) = \chi'(\sigma) x$ for $\sigma$ in $\Gamma'$ and $x$ in $k(p)(\chi')$. In particular, $k(p)(\chi')$ is the $o\Gamma'$-module $k(p)$, appearing in the formula we wish to prove. Since the inertial group $A$ (of a prime over $p$) has order $d = n/r$, we obtain from Theorem 2.15(b) an isomorphism

$$\psi: A \rightarrow \mu_d(k(p))$$

such that

$$\phi_a(R(K/k)_p) \cong r \bigoplus_{i=1}^{d-1} i\mathbb{Z} \otimes A k(p)(\psi^i). \quad (2.20)$$
Now, our hypotheses on \( n \) and \( p \) imply that the basic definitions and theorems of the theory of representations of finite groups apply to representations and characters of subgroups of \( \Gamma \) in the field \( k(p) \); see, e.g., [15, Chaps. I-II]. In particular, we obtain from the Frobenius Reciprocity Law [15, Theorem 13, p. 73] that

\[
\mathbb{Z} \Gamma \otimes_{\mathbb{Z} \Delta} k(p)\psi_1 \approx \bigoplus_{\chi'} k(p)(\chi')
\]

with \( \chi' \) tracing all homomorphisms \( \chi' : \Gamma \to \mu_n(k(p)) \) such that \( \text{Res}_x^\Delta \chi' = \psi_i \), where "\( \text{Res}_x^\Gamma \)" denotes the restriction of characters of \( \Gamma \) to the subgroup \( \Delta \). Since \( \Gamma \) is cyclic of order \( n \), we may select an isomorphism \( \chi : \Gamma \cong \mu_n(k(p)) \) such that \( \text{Res}_x^\Delta \chi = \psi \). For the same reason, \( \Delta = \langle \gamma' \mid \gamma \in \Gamma \rangle \), and it is then an easy exercise to show that, if \( \chi' : \Gamma \to \mu_n(k(p)) \) is a character of \( \Gamma \), then \( \text{Res}_x^\Delta \chi' = \psi_1 \) if and only if

\[
\chi' = \chi^{i + dj}
\]

for some \( j = 0,\ldots, r - 1 \). Substituting in (2.20) yields

\[
\sigma_{af}(R(K/k)_p) \approx \bigoplus_{i=1}^{d-1} \bigoplus_{j=0}^{r-1} \mathbb{Z} k(p)_{i + dj}.
\]

We wish to index the terms in this coproduct by the natural numbers less than \( n \). To do this, note that, if \( 0 \leq i < d \) and \( 0 \leq j < r \), then

\[
ri = nj + ri
\]

since \( rd = n \), and since \( ri < n \) it follows from (2.18c) that

\[
ri = n \left\langle \frac{r(i + dj)}{n} \right\rangle = n \left\langle \frac{rk}{n} \right\rangle
\]

with \( k = i + dj \). But, as \( i \) traces the set \( \{0,\ldots, d - 1\} \) and \( j \) traces the set \( \{0,\ldots, r - 1\} \), \( k = i + dj \) traces the set \( \{0,\ldots, n - 1\} \), and so (2.21) becomes

\[
\sigma_{af}(R(K/k)_p) \approx \bigoplus_{k=1}^{n-1} n \left\langle \frac{rk}{n} \right\rangle k(p)_k.
\]

Replacing \( k \) by \( i \) yields the desired formula, and the proof of the corollary is complete.

Finally, we consider \( R(K/k) \) for an elementary abelian extension \( K/k \). We shall deduce, from the general formula of Theorem 2.15, an expression for the semi-simplification of certain primary components of \( R(K/k) \) in terms of
the "Stickelberger element" of an elementary abelian extension introduced by McCulloh [8].

The expression we shall derive utilizes the following general construction. Let \( \omega: R \rightarrow S \) be a homomorphism of rings and \( M \) be an \( R \)-module. We denote by \( \omega \cdot M \) the \( S \)-module obtained from \( M \) by "change of rings," i.e.,

\[
\omega \cdot M = S \otimes_R M
\]  
(2.22a)

with \( S \) viewed as an \( S \)-\( R \)-bimodule according to the formula

\[
bya = by\omega(a) \quad (a \text{ in } R; \ b, y \text{ in } S).
\]

It is well known and easily verified that, if also \( \omega': S \rightarrow T \) is a ring homomorphism, then

\[
\omega' \cdot (\omega \cdot M) \cong (\omega' \omega) \cdot M
\]  
(2.22b)

as \( T \)-modules.

We shall be interested in \( \omega \cdot M \) primarily for the special case in which \( S = R \) and \( \omega \) is an automorphism of \( R \); note that then the mapping \( x \mapsto 1 \otimes x \) yields an isomorphism

\[
M \cong \omega \cdot M
\]  
(2.22c)

of abelian groups. Moreover, the action of \( R \) on \( \omega \cdot M \) satisfies the formula

\[
a(1 \otimes x) = 1 \otimes \omega^{-1}(a)x
\]  
(2.22d)

for \( a \) in \( R \), \( x \) in \( M \). Now let \( \Omega \) be the automorphism group of the ring \( R \) and \( \omega_1, \ldots, \omega_r \) be elements of \( \Omega \). If \( n_1, \ldots, n_r \) are nonnegative integers, then

\[
\theta = n_1 \omega_1 + \cdots + n_r \omega_r
\]

is an element of the integral group ring \( \mathbb{Z}\Omega \), and we define the \( R \)-module \( \theta \cdot M \) by

\[
\theta \cdot M = \bigoplus_{i=1}^r n_i (\omega_i \cdot M). \quad (2.22e)
\]

In particular, let \( R = \mathcal{O}_I \), with \( I \) a group and \( \mathcal{O} \) a commutative ring. Then any automorphism \( \omega \) of \( I \) extends uniquely to an \( \mathcal{O} \)-algebra automorphism of \( R \); thus \( \omega \cdot M \) is meaningful in this case and, moreover, (2.22b) is an isomorphism of \( \mathcal{O} \)-modules. Equation (2.22d) is similarly meaningful for an automorphism \( \omega_1, \ldots, \omega_r \) of \( I \).

Now let \( p \) be a prime and \( I \) be an elementary abelian group of order \( n = q^t \). Following McCulloh [8, Summary and Sect. 3], we invoke a charac-
characterization of $\Gamma$ which allows the introduction of a counterpart of the classical Stickelberger element. Namely, the additive group $\mathbb{F}_n^+$ of the field $\mathbb{F}_n$ with $n$ elements is isomorphic to $\Gamma$. If $\phi: \mathbb{F}_n^+ \overset{\sim}{\longrightarrow} \Gamma$ is such an isomorphism and $\alpha$ is an element of the multiplicative group $\mathbb{F}_n^*$ of $\mathbb{F}_n$, we shall denote by $[\alpha]_\phi$ the automorphism of $\Gamma$ corresponding via $\phi$ to the automorphism of $\mathbb{F}_n^+$ obtained by multiplication by $\alpha$, i.e.,

$$[\alpha]_\phi(y) = \phi(\alpha \phi^{-1}(y))$$  \hspace{1cm} (2.23)

for $y$ in $\Gamma$. Let $\mathbb{F}_q$ be the (prime) subfield of $\mathbb{F}_n$ with $q$ elements. If $\alpha$ is in $\mathbb{F}_n$, we denote by $t(\alpha)$ the non-negative integer uniquely determined by the conditions

$$0 \leq t(\alpha) < q$$  \hspace{1cm} (2.24a)

$$t(\alpha) = Tr_{\mathbb{F}_q/\mathbb{F}_q}(\alpha) \quad \text{in} \quad \mathbb{F}_q$$  \hspace{1cm} (2.24b)

where "$Tr_{\mathbb{F}_q/\mathbb{F}_q}$" denotes the trace of the field extension $\mathbb{F}_n/\mathbb{F}_q$.

**Lemma 2.25.** Given the following data:

(a) a prime $q$, an elementary abelian $q$-group $\Gamma$ of order $n = q^t$, and a subgroup $\Lambda$ of $\Gamma$ of order $q$;

(b) an isomorphism $\phi: \mathbb{F}_n^+ \overset{\sim}{\longrightarrow} \Gamma$ of groups;

(c) a field $k$ of characteristic prime to $q$ which contains all $q$th roots of 1, and a homomorphism $\chi: \Gamma \rightarrow \mu_q(k)$ which is nontrivial on $\Lambda$;

(d) a $k$-space $M$;

denote by $M(\chi)$ the $k\Gamma$-module defined by the conditions that $M(\chi) = M$ as a $k$-space and $\sigma x = \chi(\sigma)x$ for $\sigma$ in $\Gamma$, $x$ in $M$. Then there exists $\beta$ in $\mathbb{F}_n^*$ such that, for any $i = 0, \ldots, q - 1$,

$$\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Lambda} M(\chi^t) \simeq \bigsqcup_{\alpha \in \Lambda} [\alpha]_\phi^{-1} \cdot M(\chi)$$

as $k\Gamma$-modules, with

$$A_i = \{ \alpha \text{ in } \mathbb{F}_n^* \mid t(\alpha \beta) = i \}.$$  

**Proof.** Let $\lambda: \mathbb{F}_q^* \overset{\sim}{\longrightarrow} \mu_q(k)$ be any isomorphism; then there is a unique $\mathbb{F}_q$-space homomorphism $f: \mathbb{F}_n \rightarrow \mathbb{F}_q$ rendering the diagram below commutative:

$$\begin{array}{ccc}
\mathbb{F}_n^+ & \xrightarrow{f} & \mathbb{F}_q^+ \\
\downarrow & & \downarrow \lambda \\
\Gamma & \xrightarrow{x} & \mu_q(k)
\end{array}$$
Since $\chi$ is non-trivial on $A$, there exists $\beta_1$ in $\phi^{-1}(A)$ with $f(\beta_1) = 1$, in which case $\phi^{-1}(A) = \mathbb{F}_q \beta_1$ and $f(x\beta_1) = x$ for $x$ in $\mathbb{F}_q$. Moreover, since $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_q}: \mathbb{F}_q \to \mathbb{F}_q$ is surjective and $\text{Hom}_{\mathbb{F}_q}(\mathbb{F}_n, \mathbb{F}_q)$ is an $\mathbb{F}_n$-space of dimension 1 via the formula following (1.2), there is a unique $\beta_2$ in $\mathbb{F}_n^*$ such that

$$f(x) = \text{Tr}_{\mathbb{F}_n/\mathbb{F}_q}(\beta_2 x)$$

for all $x$ in $\mathbb{F}_n$. Setting $\beta = \beta_1 \beta_2$ in $\mathbb{F}_n^*$, we then have that, for all $\alpha$ in $\mathbb{F}_n^*$ and $x$ in $\mathbb{F}_q$,

$$f(\alpha(\beta_1 x)) = f(\alpha(\beta_2)) x = \text{Tr}_{\mathbb{F}_n/\mathbb{F}_q}(\alpha \beta) f(\beta_1 x).$$

(2.26a)

Now, if $\chi': \Gamma \to \mu_n(k)$ is any homomorphism, then there is a unique $f'$ in $\text{Hom}_{\mathbb{F}_q}(\mathbb{F}_n^*, \mathbb{F}_q)$ such that $\chi' = \lambda \circ f' \circ \phi^{-1}$, and then a unique $\alpha$ in $\mathbb{F}_n^*$ such that $f'(x) = f(\alpha x)$ for all $x$ in $\mathbb{F}_n$. Equations (2.23), (2.26a), and the equation $\Delta = \phi^{-1}(\mathbb{F}_q \beta_1)$ then imply that

$$\text{Res}_i^\Gamma(\chi') = \text{Res}_i^\Gamma(\chi') \quad \text{with} \quad i = t(\alpha \beta).$$

(2.26b)

In other words:

If $0 < i < q$, then $\text{Res}_i^\Gamma(\chi') = \text{Res}_i^\Gamma(\chi')$ if and only if $\alpha$ (defined as above) is in $A_i$. (2.26c)

Note, in addition, that if $\gamma$ is in $\Gamma$ then we have from (2.23) that

$$\chi([\alpha]_\phi(\gamma)) = \chi(\phi(\alpha \phi^{-1}(\gamma))) = \lambda \{ f(\alpha \phi^{-1}(\gamma)) \} = \lambda \{ f'(\phi^{-1}(\gamma)) \} = \chi'(\gamma).$$

Hence, if $M$ is as in (d), (2.22c, d) yield that

$$[\alpha]_{\phi^{-1}} \cdot M(\chi) \approx M(\chi')$$

(2.26d)

as $k\Gamma$-modules.

Finally, just as in the argument following (2.20), we have from the Frobenius Reciprocity Law that

$$\mathbb{Z} \cap \mathbb{Z}_A M(\chi') \approx \bigoplus_{\chi'} M(\chi')$$

for any $i$, where $\chi'$ traces all homomorphisms $\chi': \Gamma \to \mu_q(k)$ such that $\text{Res}_i^\Gamma \chi' = \text{Res}_i^\Gamma \chi'$. This, together with (2.26c), yields the desired formula, completing the proof of the lemma.

We now introduce the Stickelberger element arising in the context of Lemma 2.25. Given $q, n, \Gamma$, etc., as in the lemma, we set

$$\mathcal{O}_n = \frac{1}{q} \sum_{\alpha \in \mathbb{F}_n^*} t(\alpha)[\alpha]_{\phi^{-1}}$$

(2.27)
\( \Theta_n \) is an element of the rational group ring \( \mathbb{Q}[\Omega] \), with \( \Omega \) the automorphism group of \( \Gamma \), and

\[
n \Theta_n = q^{s-1} \sum_{\alpha \in \mathbb{F}_q^*} t(\alpha)[\alpha]_{\mathbb{F}_q}^{-1}
\]

is in \( \mathbb{Z}[\Omega] \). We assume the isomorphism \( \varphi : \mathbb{F}_q^* \xrightarrow{\sim} \Gamma \) chosen once and for all.

**Corollary 2.28.** Let \( \mathcal{O} \) be a Dedekind domain with quotient field \( k \), \( K \) be a normal separable extension of \( k \) with Galois group \( \Gamma \), and \( \mathcal{O} \) be the integral closure of \( \mathcal{O} \) in \( K \). Assume that \( \Gamma \) is an elementary abelian \( q \)-group of order \( n = q^s \), with \( q \) a prime. Let \( p \) be a prime of \( \mathcal{O} \), ramified in \( K \), such that the characteristic of the residue field \( k(p) \) is prime to \( q \). Then there is a simple \( \mathcal{O}\Gamma \)-module \( M \) with the property that

\[
\sigma_{\mathcal{O}}(R(K/k)_p) \approx n \Theta_n \cdot M
\]

with the semi-simple \( \mathcal{O}\Gamma \)-module \( n \Theta_n \cdot M \) as in (2.22e).

**Proof.** Let \( \Delta \subseteq \Gamma \) be the inertial group of a prime \( \mathfrak{P} \) of \( \mathcal{O} \) above \( p \). Our assumption on \( p \) implies that \( p \) is tamely ramified in \( K \) [2, Theorem 1, p. 29], and hence \( \Delta \) is cyclic [2, Proposition 1, p. 32]. Since \( \Gamma \) is elementary abelian, it follows that \( \Delta \) has order \( q \); moreover, if \( \Gamma_{\mathfrak{P}} \) is the decomposition group of \( \mathfrak{P} \), there is a subgroup \( \Sigma \) of \( \Gamma_{\mathfrak{P}} \) with \( \Gamma_{\mathfrak{P}} = \Delta \times \Sigma \). \( E = K_{\mathfrak{P}}^\mathbb{F}_q \) is then a tame extension of \( k_p \) with Galois group isomorphic to \( \Delta \). Also, since \( K_{\mathfrak{P}}^\mathbb{F}_q \) is the unique maximal subfield of \( K_{\mathfrak{P}} \) non-ramified over \( k_p \), it follows that \( E/k_p \) is totally ramified. Therefore \( k_p \) (and hence \( k(p) \)) contain all \( q \)-th roots of 1, by [2, Proposition 1, p. 32]. We may now apply Theorem 2.15 to obtain an isomorphism \( \psi : \Delta \xrightarrow{\sim} \mu_q(k(p)) \) with the property that (in the notation of that theorem)

\[
\psi_{\mathcal{O}}(R(K/k)_p) \approx q^{s-1} \prod_{i=1}^{q-1} \mathbb{Z} \Gamma \otimes_{\mathbb{Z}\Delta} k(p)_i
\]

as \( \mathcal{O}\Gamma \)-modules.

Since \( \Gamma \) is elementary abelian, \( \psi = \text{Res}_{\Delta}'(\chi) \) for some homomorphism \( \chi : \Gamma \rightarrow \mu_q(k(p)) \); then, by Lemma 2.25, there exists \( \beta \) in \( \mathbb{F}_q^* \) such that, for all \( i = 0, \ldots, q - 1 \),

\[
\mathbb{Z} \Gamma \otimes_{\mathbb{Z}\Delta} k(p)_i - \mathbb{Z} \Gamma \otimes_{\mathbb{Z}\Delta} k(p)(\chi') \approx \prod_{\alpha \in \mathbb{F}_q^*} \mathbb{Z} \Gamma \otimes_{\mathbb{Z}\Delta} k(p)(\chi)
\]
as \( k(p) \Gamma \text{-modules (hence as } o \Gamma \text{-modules), with } A_i \text{ as in the lemma. Thus}

\[
\sigma_d(R(K/k)_p) \simeq q^{s-1} \prod_{l=1}^{q-1} \prod_{\alpha \in A_l} i[\alpha]_{\phi}^{-1} \cdot k(p)(\chi)
\]

\[
= q^{s-1} \prod_{\alpha \in F_n^s} t(\alpha\beta)[\alpha]_{\phi}^{-1} \cdot k(p)(\chi)
\]

the latter equation because \( F_n^s \) is the disjoint union of \( A_0, \ldots, A_{q-1} \). Since the mapping \( F_n^s \to \Omega = \text{Aut}(\Gamma) \), where \( \alpha \to [\alpha]_{\phi} \), is a homomorphism of groups, we may replace \( \alpha \) by \( \alpha\beta \) in the above coproduct and use (2.22b) to conclude that

\[
\sigma_d(R(K/k)_p) \simeq q^{s-1} \prod_{\alpha \in F_n^s} t(\alpha)[\alpha]_{\phi}^{-1} \cdot M = n\theta_n \cdot M
\]

with \( M = [\beta]_{\phi} \cdot k(p)(\chi) \). This completes the proof of the corollary.

**Addendum 2.30.** In Theorem 2.15 we exhibited a formula only for the semi-simplification of certain primary components of \( R(K/k) \), since that was what was desired for our applications. It is easy, however, to obtain a similar formula for these components themselves; we need only make minor adjustments in the proof of the theorem, the most important of which is to use (2.8) rather than (2.13). This yields, with notation as in the statement of the theorem,

\[
R(K/k)_p \simeq [\Gamma: \Gamma_p] \prod_{i=1}^{d-1} \Z \Gamma \otimes_{\Z \Delta_o} (O/\Psi)_i
\]

as \( o \Gamma \text{-modules for any prime } p \text{ of } o \text{ which is tamely ramified in } K \).

**3. Base-Change Formulae**

The purpose of this section is to discuss the behavior of the Galois module \( R(K/k) \) under change of field and Galois group, base extension, and completion at a prime. We begin with the following situation:

\[
\sigma \text{ is a Dedekind domain with quotient field } k,
\]

\( k \subseteq F \subseteq K \) are fields, with \( K \) normal separable over \( k \), and \( \Delta = \text{Gal}(K/F) \subseteq \Gamma = \text{Gal}(K/k) \). \( O \) and \( o_\Gamma \) are the integral closures of \( o \) in \( K \) and \( F \), respectively. Finally, we write \( \Gamma = \langle \gamma_1, \ldots, \gamma_r \rangle \Delta \), with \( r = [\Gamma: \Delta] \) and \( \{\gamma_i \mid i \leq r\} \) a fixed transversal of \( \Gamma/\Delta \).
The following construction will be useful. If $M$ is a $\mathcal{D}$-module, we define another $\mathcal{D}$-module $\{\Gamma/\Delta, M\}$ by the conditions that:

As a $k\mathcal{D}$-module, $\{\Gamma/\Delta, M\} = (\Gamma/\Delta, M)$ the set of all functions $u: \Gamma/\Delta \to M$, a $k\mathcal{D}$-module under the pointwise operations.

$$\{\Gamma/\Delta, M\}$$ is a $K$-module according to the formula

$$(au)(\gamma_i \Delta) = \gamma_i^{-1}(a) u(\gamma_i \Delta) \quad (i \leq r).$$

If $M$ is an $\mathcal{O}_m$-module we define, in entirely similar fashion, another $\mathcal{O}_m$-module $\{\Gamma/\Delta, M\}$. It is easy to see that the mapping $\{\Gamma/\Delta, M\} \to \gamma_i \cdot M$, where $\gamma_i \cdot M$ is as in (2.22a) and $u \mapsto 1 \otimes \mathcal{O} u(\gamma_i \Delta)$, is a surjection of $\mathcal{O}_m$-modules, and these for $i \leq r$ give rise to an $\mathcal{O}_m$-module isomorphism

$$\{\Gamma/\Delta, M\} \xrightarrow{\sim} \prod_{i=1}^{r} \gamma_i \cdot M.$$  

Note that a homomorphism $f: M \to N$ of $\mathcal{D}$-modules (or $\mathcal{O}_m$-modules) yields another such homomorphism $\{\Gamma/\Delta, f\}: \{\Gamma/\Delta, M\} \to \{\Gamma/\Delta, N\}$; in fact, in either case we obtain an exact endo-functor $\{\Gamma/\Delta, -\}$. Finally, it is not difficult to show that the module $\{\Gamma/\Delta, M\}$ depends on the choice of transversal of $\Gamma/\Delta$ only up to isomorphism; however, we shall not need that fact.

**Lemma 3.5.** Let $K/F/k$, etc., be as in (3.1). Then the diagrams below commute. In the first, each mapping is an isomorphism of $\mathcal{D}$-modules; in the second, each is an isomorphism of $K\mathcal{I}$-modules.

$$
\begin{array}{cccccc}
K \otimes_k K & \xrightarrow{\phi_{K/k}} & (\Gamma, K) \\
\downarrow & & \downarrow \approx \\
(K \otimes_F F) \otimes_K K & \xrightarrow{\phi_{K/F} \otimes F} & (\Gamma/\Delta, K) \otimes_F K & \xrightarrow{f_1} & \{\Gamma/\Delta, K \otimes_F K\} & \xrightarrow{f_1} & \{\Gamma/\Delta, (\Delta, K)\} \\
\approx & & \approx & & \approx \\
K \otimes_k K & \xrightarrow{\phi_{K/k}} & (\Gamma, K) \\
\downarrow & & \downarrow \approx \\
K \otimes_F (F \otimes_K K) & \xrightarrow{f_1 \otimes F} & K \otimes_K (\Gamma, K) & \xrightarrow{f_1} & (\Gamma, K \otimes_F K) & \xrightarrow{f_1} & (\Gamma, (\Delta, K))(\Delta)
\end{array}
$$
The mappings are defined as follows:

(a) \( \psi_{K/k} \) and \( \psi_{K/F} \) are as in (1.6a).

(b) \( \psi_{K/F/k} : K \otimes_k F \to (\Gamma/\Delta, K) \) is the K-space isomorphism given by the formula

\[
\psi_{K/F/k}(x \otimes y)(\gamma \Delta) = x \gamma(y)
\]

(it is an obvious variant of the isomorphisms of (1.6)).

(c) \( \psi_{F/k} \) is the isomorphism of (1.6b).

(d) \( i_1 \) and \( j_1 \) are defined by the formulae

\[
i_1(u \otimes_F y)(\gamma \Delta) = \gamma_1^{-1}(u(\gamma \Delta)) \otimes_F y
\]
\[
j_1(x \otimes_F v)(\gamma) = x \otimes_F v(\gamma)
\]

for \( x, y \in K, \gamma \in \Gamma, u \in (\Gamma/\Delta, K), \) and \( v \in (\Gamma, K)^\Delta \).

(e) \( i_2 \) and \( j_2 \) are defined by the formulae

\[
i_2(u)(\gamma \delta) = \gamma_1^{-1}(u(\gamma \Delta)(\delta))
\]
\[
j_2(v)(\gamma)(\delta) = v(\delta \gamma)
\]

for \( u \in \{\Gamma/\Delta, (\Delta, K)\}, v \in (\Gamma, K), \gamma \in \Gamma, \) and \( \delta \in \Delta \).

(f) \( g_1 = \{\Gamma/\Delta, \psi_{K/F} \} \) and \( g_2 = (\Gamma, \psi_{K/F})^\Delta \).

The lemma is proved by routine (although somewhat tedious) computations which we omit. We remark only that \( K \otimes_F K \) is always viewed as a \( K\Delta \)-module with \( K, \Delta \) acting on the left and right factors, respectively; the formulae for the inverses of \( i_2 \) and \( j_2 \) are

\[
i_2^{-1}(u')(\gamma \Delta)(\delta) = \gamma \Delta \gamma_1^{-1}(u'(\gamma \delta))
\]
\[
j_2^{-1}(v')(\gamma)(1) = v'(\gamma)(1).
\]

The next lemma is an easy consequence of Lemma 3.5.

**Lemma 3.6.** The isomorphisms of Lemma 3.5 yield, upon restriction to the appropriate submodules, the commutative diagrams below. In the first, all mappings are injections of \( \Delta \)-modules, with \( i_1 \) and \( i_2 \) isomorphisms. In the second, all mappings are injections of \( \Gamma \)-modules, with \( j_1 \) and \( j_\Delta \) isomorphisms.
Theorem 3.7. Let $K/F/k$, etc., be as in (3.1). Then the homomorphisms of Lemma 3.6 yield the short exact sequence

$$(a) \ 0 \to R(K/F/k) \otimes_{\mathcal{O}} \mathcal{O} \to R(K/k) \to \{\Gamma/\Delta, R(K/F)\} \to 0$$

of $\mathcal{O}\Delta$-modules, and the short exact sequence

$$(b) \ 0 \to \mathcal{O} \otimes_{\mathcal{O}} R'(K/F/k) \to R(K/k) \to (\Gamma, R(K/F))^\Delta \to 0$$

of $\mathcal{O}\Gamma$-modules. The unfamiliar terms in (a) and (b) are as follows:

(c) $R(K/F/k)$ is defined by the short exact sequence of $\mathcal{O}$-$\mathcal{O}_F$-bimodules

$$0 \to \mathcal{O} \otimes_{\mathcal{O}} o_F \otimes_{\mathcal{O}} (\Gamma/\Delta, \mathcal{O}) \to R(K/F/k) \to 0$$

the bimodule structure of $(\Gamma/\Delta, \mathcal{O})$ being given by the formula

$$(aub)(\gamma_i \Delta) = au(\gamma_i \Delta) \gamma_i(b)$$

for $a$ in $\mathcal{O}$, $b$ in $o_F$, and $u$ in $(\Gamma/\Delta, \mathcal{O})$. $R(K/F/k) \otimes_{\mathcal{O}} \mathcal{O}$ is viewed as an $\mathcal{O}\Delta$-module with $\mathcal{O}$ acting on the left factor, $\Lambda$ on the right.

(d) $R'(K/F/k)$ is defined by the short exact sequence of $o_F\Gamma$-modules

$$0 \to o_F \otimes_{\mathcal{O}} \mathcal{O} \otimes_{\mathcal{O}} \mathcal{O} \to R'(K/F/k) \to 0.$$
COROLLARY 3.8. Let $K/F/k$, etc., be as in Theorem 3.7, with $F/k$ non-ramified. Then $R(K/k) \approx \{\Gamma/\Delta, R(K/F)\}$ as $\Delta$-modules, and

$$R(K/k) \approx (\Gamma, R(K/F))^{\Delta} \approx \mathbb{Z} \Gamma \otimes_{\mathbb{Z} \Delta} R(K/F)$$

as $\Omega \Gamma$-modules.

Proof. If $F/k$ is non-ramified, then we obtain from Theorem 3.7(d) and (1.6c) that $R'(K/F/k) = 0$, and an entirely similar argument shows that then $R(K/F/k) = 0$, too. The desired isomorphisms then follow from (a) and (b) of Theorem 3.7, together with the remarks following (1.6e).

Remarks 3.9. There exist analogues for $T(K/k)$ of Theorem 3.7 and Corollary 3.8. For example, the counterpart of the second isomorphism of (3.8) is simply (1.6e). The counterpart of (3.7a) is the short exact sequence of $\mathfrak{o}\Delta$-modules

$$0 \to T(F/k) \otimes_{\mathfrak{o} F} \mathfrak{D} \to T(K/k) \to \mathfrak{F}(F/k) \otimes_{\mathfrak{o} F} T(K/F) \to 0$$

which is an easy consequence of the product formula for the codifferent [4, (4.7), p. 27].

In the remainder of this section we discuss the behavior of $R(K/k)$ under base extension and completion. With regard to the former, $R(K/k)$ is, in an obvious sense, preserved whenever $\mathfrak{D}$ is, as is apparent from the definitions. We discuss the latter in Proposition 3.10 below. Recall first that the bijection $\psi: K \otimes_k E \sim (\Gamma, K)$ of (1.6) is an isomorphism of $k(\Gamma \times \Gamma)$-modules if $K \otimes_k K$ and $(\Gamma, K)$ are given the module structures described in (1.5b). The injection $\psi: \mathfrak{D} \otimes_{\mathfrak{D}} \mathfrak{D} \to (\Gamma, \mathfrak{D})$ of (2.1) is then clearly an $\mathfrak{o}(\Gamma \times \Gamma)$-module homomorphism, and hence gives rise to an $\mathfrak{o}(\Gamma \times \Gamma)$-module structure on $R(K/k)$.

PROPOSITION 3.10. Let $\Delta$ be a subgroup of a finite group $\Gamma$. Let $\mathfrak{o}$ be a Dedekind domain with quotient field $k$, $E$ be a Galois extension of $k$ with Galois group $\Delta$, and $K = (\Gamma, E)^{\Delta}$, a Galois extension of $k$ with Galois group $\Gamma$. Let $\mathfrak{o}_E$ and $\mathfrak{D} = (\Gamma, \mathfrak{o}_E)^\Delta$ be the maximal $\mathfrak{o}$-orders in $E$ and $K$, respectively, and view $R(E/k)$ as an $\mathfrak{o}(\Delta \times \Delta)$-module as described in (3.9). Then

$$R(K/k) \approx (\Gamma \times \Gamma, R(E/k)^\Delta \times \Delta)$$

as $\Omega \Gamma$-modules, the $\Omega \Gamma$-module structure on the right-hand side being given by the formula

$$((w_\gamma) w)(\sigma, \tau) = u(\sigma) w(\sigma, \gamma \tau)$$

for $\gamma, \sigma, \tau$ in $\Gamma$, $u$ in $\mathfrak{D}$, and $w$ in $(\Gamma \times \Gamma, R(E/k)^\Delta \times \Delta)$. 

as $\mathfrak{o}_E, R(K/k) \approx Z \Gamma \otimes_{\mathbb{Z}_\Delta} R(E/k)$

as $\mathfrak{o}_E, R(K/k) \approx Z \Gamma \otimes_{\mathbb{Z}_\Delta} R(E/k)$ as $\mathfrak{o}_E$-modules.

**Proof.** The proposition follows from arguments quite similar to those applied in the proofs of (1.6d), Theorem 1.7, Theorem 3.7(b) and Corollary 3.8, and hence they will be only briefly sketched. One uses the commutative diagram of $K\Gamma$-module isomorphisms

$$
\begin{array}{ccc}
K \otimes_k K & \overset{\phi_{K/k}}{\approx} & (\Gamma, K) \\
\downarrow h_1 & & \approx \downarrow h_1 \\
(\Gamma \times \Gamma, E \otimes_k E)^{\Delta \times \Delta} & \overset{h_1}{\approx} & (\Gamma \times \Gamma, (\Delta, E))^{\Delta \times \Delta}
\end{array}
$$

with $\psi_{K/k}, \psi_{E/k}$ as in (1.6a) and $h_i (i = 1, 2)$ given by the formulae

$$
\begin{align*}
&h_1(u \otimes v)(\sigma, \tau) = u(\sigma) \otimes v(\tau) \\
&\{h_2(w)(\sigma, \tau)\}(\delta) = w(\sigma^{-1} \delta \tau)(\sigma)
\end{align*}
$$

for $\sigma, \tau$ in $\Gamma$, $\delta$ in $\Delta$, $u, v$ in $K$, and $w$ in $(\Gamma \times \Gamma, (\Delta, E))^{\Delta \times \Delta}$. The $K\Gamma$-module structures on the lower terms of the diagram are defined by obvious analogues of the formula of (a). As in Lemma 3.6, we obtain a commutative diagram of $\Omega\Gamma$-injections, with $h_1$ and $h_2$ isomorphisms. Equation (2.1) and the exactness of the functor $(\Gamma \times \Gamma, -)^{\Delta \times \Delta}$ then establish (a).

In order to prove (b) and (c), we select a function

$$
\Delta \backslash \Gamma \to \Gamma
$$

$$
\Delta \gamma \to \tilde{\gamma}
$$

such that $\Delta \gamma = \Delta \tilde{\gamma}$ for all $\gamma$ in $\Gamma$ and $\bar{1} = 1$. With $M = R(E/k)$, consider the mappings

$$
\begin{align*}
f: (\Gamma \times \Gamma, M)^{\Delta \times \Delta} & \to (\Delta \Gamma, (\Gamma, M)^{\Delta}) \\
p: \mathfrak{o}_E \otimes \mathfrak{o} (\Gamma \times \Gamma, M)^{\Delta \times \Delta} & \to (\Gamma, M)^{\Delta} \\
q: (\Gamma, M)^{\Delta} & \to \mathfrak{o}_E \otimes \mathfrak{o} (\Gamma \times \Gamma, M)^{\Delta \times \Delta}
\end{align*}
$$
given by the formulae

\[ f(w)(\Delta y)(\sigma) = w(\gamma, \sigma) \]

\[ p(a \otimes_{\mathcal{E}} w)(\sigma) = aw(1, \sigma) \]

\[ q(v) = 1 \otimes_{\mathcal{E}} v' \]

for \( \gamma, \sigma \) in \( \Gamma \) and \( a, w, v \) in \( \mathcal{E}, (\Gamma \times \Gamma, M)^{\Delta \times \Delta} \), and \( (\Gamma, M)^{\Delta} \), respectively, where \( v' \) in \((\Gamma \times \Gamma, M)^{\Delta \times \Delta} \) is defined by

\[ v'(\gamma, \sigma) = \begin{cases} (\gamma, 1)(v(\sigma)) & \text{if } \gamma \text{ is in } \Delta \\ 0 & \text{if } \gamma \text{ is not in } \Delta. \end{cases} \]

We omit the tedious but routine verifications that these mappings are well defined, \( f \) and \( q \) are homomorphisms of \( \mathcal{E}\Gamma \)-modules (the module structure on \( (\Delta \setminus \Gamma, (\Gamma, M)^{\Delta}) \) arising from that on \( (\Gamma, M)^{\Delta} \), and \( p \) is an \( \mathcal{E}\Gamma \)-module homomorphism. \( f \) is, in fact, an isomorphism, its inverse being given by the formula

\[ f^{-1}(w')(\gamma, \sigma) = (\delta, 1) w'(\Delta y)(\sigma) \]

for \( \gamma, \sigma \) as above, \( w' \) in \((\Delta \setminus \Gamma, (\Gamma, M)^{\Delta}) \), and \( \gamma = \delta \gamma \) with \( \delta \) in \( \Delta \). Part (a) and the remark following (1.6e) then yield the \( \mathcal{E}\Gamma \)-module isomorphisms

\[ R(K/k) \cong (\Gamma \times \Gamma, M)^{\Delta \times \Delta} \cong (\Delta \setminus \Gamma, (\Gamma, M)^{\Delta}) \cong [\Gamma : \Delta](\Gamma, M)^{\Delta} \]

\[ \cong [\Gamma : \Delta] \mathbb{Z} \Gamma \otimes_{\mathbb{Z} \Delta} R(E/k) \]

establishing (c).

Turning now to (b), one sees easily that \( pq \) is the identity map of \((\Gamma, M)^{\Delta}\). Our task is to show that \( qp \) is the identity map of \( \mathcal{E}\Gamma \otimes_{\mathcal{E}} (\Gamma \times \Gamma, M)^{\Delta \times \Delta} \), and in that case \( p \) is an isomorphism of \( \mathcal{E}\Gamma \)-modules and we have, again from (a) and the remark following (1.6c), that

\[ \mathcal{E}\Gamma \otimes_{\mathcal{E}} R(K/k) \cong \mathcal{E}\Gamma \otimes_{\mathcal{E}} (\Gamma \times \Gamma, M)^{\Delta \times \Delta} \cong (\Gamma, M)^{\Delta} \cong \mathbb{Z} \Gamma \otimes_{\mathbb{Z} \Delta} R(E/k) \]

as \( \mathcal{E}\Gamma \)-modules, as desired.

So let \( p(a \otimes_{\mathcal{E}} w) = v \) in \((\Gamma, M)^{\Delta}\), with \( a, w \) in \( \mathcal{E} \) and \((\Gamma \times \Gamma, M)^{\Delta \times \Delta}, \) respectively; then

\[ qp(a \otimes_{\mathcal{E}} w) = q(v) = 1 \otimes_{\mathcal{E}} v' \]

with \( v' \) in \((\Gamma \times \Gamma, M)^{\Delta \times \Delta} \) defined by the conditions that \( v'(\gamma, \sigma) = 0 \) if \( \gamma \) is not in \( \Delta \), and if \( \gamma \) is in \( \Delta \) then

\[ v'(\gamma, \sigma) = (\gamma, 1)(v(\sigma)) = (\gamma, 1)(aw(1, \sigma)) = \gamma(a) w(\gamma, \sigma). \]
Now define $u$ in $\mathcal{O} = (\Gamma, o_E)^{\Delta}$ as follows:

$$u(\gamma) = \begin{cases} \gamma(a) & \text{for } \gamma \text{ in } \Delta \\ 0 & \text{for } \gamma \text{ not in } \Delta. \end{cases}$$

The definition of the $\mathcal{O}$-module structure on $(\Gamma \times \Gamma, M)^{\Delta \times \Delta}$, as given in (a), yields easily that $uw = v'$, and then

$$qp(a \otimes \mathcal{O} w) = 1 \otimes \mathcal{O} v' = 1 \otimes \mathcal{O} uw = u(1) \otimes \mathcal{O} w = a \otimes \mathcal{O} w.$$

Thus $qp$ is the identity map of $(\Gamma \times \Gamma, M)^{\Delta \times \Delta}$, establishing (b) and completing the proof of the proposition.

**Corollary 3.11.** Let $\mathfrak{o}$ be a Dedekind domain with quotient field $k$, and $\mathfrak{p}$ be a prime of $\mathfrak{o}$. Let $K$ be a Galois extension of $k$ with Galois group $\Gamma$, and $\mathcal{O}$ be the maximal $\mathfrak{o}$-order in $K$. If $\mathfrak{P}$ is a prime of $\mathcal{O}$ above $\mathfrak{p}$, then

(a) $R(K/k) \approx \mathcal{O} \otimes_{\mathcal{O}_\mathfrak{P}} R(K_\mathfrak{P}/k_\mathfrak{P})$ as $\mathcal{O}\Gamma$- or $\mathcal{O}_\mathfrak{P}\Gamma$-modules, and

(b) $R(K/k) \approx [\Gamma : \Gamma_\mathfrak{P}] \mathcal{O} \otimes_{\mathcal{O}_\mathfrak{P}} R(K_\mathfrak{P}/k_\mathfrak{P})$ as $\mathfrak{o}\Gamma$- or $\mathfrak{o}_\mathfrak{p}\Gamma$-modules, with $\Gamma_\mathfrak{P} \subseteq \Gamma$ the decomposition group of $\mathfrak{P}$.

**Proof.** Since the maximal order in $k_\mathfrak{P} \otimes_k K$ is $\mathfrak{p}_\mathfrak{e} \otimes_k \mathcal{O}$, it follows easily from (2.1) that

$$R(K/k_\mathfrak{P}) = \mathfrak{p}_\mathfrak{e} \otimes_k R(K/k) \approx R(k_\mathfrak{P} \otimes_k K/k_\mathfrak{P})$$

as $\mathcal{O}\Gamma$-modules.

In view of the isomorphisms of (1.9), (b) then follows from Proposition 3.10(c) with $K_\mathfrak{P}, \Gamma_\mathfrak{P}$, and $k_\mathfrak{P} \otimes_k K$ playing the roles of $E, \Delta$, and $K$, respectively. Part (a) follows in similar fashion from Proposition 3.10(b) via the $\mathcal{O}_\mathfrak{P}\Gamma$-module isomorphisms

$$R(K/k) \approx \mathcal{O}_\mathfrak{P} \otimes \mathcal{O} R(K/k) \approx \mathcal{O}_\mathfrak{P} \otimes_{\mathfrak{p}_\mathfrak{e} \otimes_k \mathcal{O}} (\mathfrak{p}_\mathfrak{e} \otimes_k R(K/k))$$

$$\approx \mathcal{O}_\mathfrak{P} \otimes_{\mathfrak{p}_\mathfrak{e} \otimes_k \mathcal{O}} R(k_\mathfrak{P} \otimes_k K/k_\mathfrak{P}) \approx \mathcal{O}_\mathfrak{P} \otimes_{\Gamma_\mathfrak{P}} R(K_\mathfrak{P}/k_\mathfrak{P}),$$

completing the proof.

4. **Order Ideals and Stickelberger Elements**

We begin with a brief review of the properties of the order ideal [10, pp. 49–50] of a finitely generated torsion module over a Dedekind domain $\mathfrak{o}$. We shall also compute these ideals for some of the Galois modules so far introduced.

If $M$ is a finitely generated torsion $\mathfrak{o}$-module, then the order ideal of $M$ is
an ideal \(\text{ord}(M)\) of \(\mathfrak{o}\) which is uniquely determined by the following conditions:

\[(4.1a)\] If \(M = \mathfrak{o}/a\), with \(a\) an ideal of \(\mathfrak{o}\), then \(\text{ord}(M) = a\).

\[(4.1b)\] If

\[0 \to M' \to M \to M'' \to 0\]

is a short exact sequence of finitely generated torsion \(\mathfrak{o}\)-modules, then \(\text{ord}(M) = \text{ord}(M') \cdot \text{ord}(M'')\).

We list some additional important properties.

\[(4.1c)\] \(\text{ord}(M) = \mathfrak{o}\) if and only if \(M = 0\).

\[(4.1d)\] If \(P\) is a finitely generated projective \(\mathfrak{o}\)-module of rank \(n\), \(f: P \hookrightarrow P\) is an injective endomorphism of \(P\), and \(M = \text{Coker}(f)\), then \(\text{ord}(M)\) is the principal ideal of \(\mathfrak{o}\) generated by \(\det(f)\), the determinant of \(f\).

Finally, we review the properties of the order ideal with respect to "change of rings." We shall sometimes write \(\text{ord}(M) = \text{ord}_k(M)\), with \(M\) as above and \(k\) the quotient field of \(\mathfrak{o}\).

\[(4.1e)\] Let \(\omega: \mathfrak{o} \hookrightarrow \mathfrak{o}'\) be an injection of Dedekind domains, \(M\) be a finitely generated torsion \(\mathfrak{o}\)-module, and \(\omega \cdot M = M' \otimes_\mathfrak{o} M\) be the finitely generated torsion \(\mathfrak{o}'\)-module constructed as in (2.22a). If \(k'\) is the quotient field of \(\mathfrak{o}'\), then

\[\text{ord}_{k'}(\omega \cdot M) = \omega(\text{ord}(M)) \mathfrak{o}'.\]

In particular, if \(\omega: \mathfrak{o} \xrightarrow{\simeq} \mathfrak{o}'\) is an isomorphism, then

\[\text{ord}_{k'}(\omega \cdot M) = \omega(\text{ord}_k(M)).\]

\[(4.1f)\] Let \(K\) be a finite separable extension field of \(k\), \(\mathfrak{O}\) be the integral closure of \(\mathfrak{o}\) in \(K\), and \(M, N\) be finitely generated torsion modules over \(\mathfrak{o}\) and \(\mathfrak{O}\), respectively. Then

\[\text{ord}_K(\mathfrak{O} \otimes_\mathfrak{o} M) = \text{ord}_k(M) \mathfrak{O}\]

\[\text{ord}_k(N) = N_{K/k}(\text{ord}_k(N))\]

with "\(N_{K/k}\)" the ideal norm.

Of course, the first equation of (4.1f) is a special case of (4.1e).

Now, with \(\mathfrak{o} \subseteq k\) as above, let \(K\) be a Galois extension of \(k\) with Galois group \(\Gamma\) and \(\mathfrak{O}\) be as in (4.1f). To evaluate the order ideals of \(T(K/k)\) and \(R(K/k)\), let us assume for the moment that \(\mathfrak{O}\) is a free \(\mathfrak{o}\)-module with basis \(\{x_1, \ldots, x_n\}\), say. Let \(\{y_1, \ldots, y_n\}\) be the \(k\)-basis of \(K\) which is dual to
\{x_1, \ldots, x_n\} \text{ with respect to the non-degenerate } k\text{-bilinear form on } K \text{ arising from the trace map } t_{K/k}, \text{i.e.,}

\[ t_{K/k}(x_i, y_j) = \delta_{ij}, \]

If } x \text{ is in } K, \text{ then}

\[ x = \sum_{j=1}^{n} t_{K/k}(xx_j) y_j \]

and from this it follows quickly that } \{y_1, \ldots, y_n\} \text{ is an } \sigma\text{-basis of the codifferential } \mathcal{D}(K/k). \text{ Hence, by (1.1), generators may be chosen for } T(K/k) \text{ so that the corresponding matrix of relations is } B = (t_{K/k}(x_ix_j)), \text{ and (4.1d) then yields that } \text{ord}_k(T(K/k)) = \det(B) \sigma. \text{ Since the latter is simply the discriminant (ideal) } b(K/k) \text{ of } K/k, \text{ we conclude that}

\[ \text{ord}_k(T(K/k)) = b(K/k). \quad (4.2) \]

A routine localization argument using (4.1e) then establishes that (4.2) is true in general, i.e., even without the assumption that } \sigma \text{ be a free } \sigma\text{-module.}

As for } \text{ord}_k(R(K/k)), \text{ note that, if } \mathfrak{O} \text{ is } \sigma\text{-free as before, then } \{1 \otimes x_1, \ldots, 1 \otimes x_n\} \text{ and } \{u_1, \ldots, u_n\} \text{ are bases of the free } \mathfrak{O}\text{-modules } \mathfrak{O} \otimes_{\sigma} \mathfrak{O} \text{ and } (I, \mathfrak{O}), \text{ respectively, where } I = \{\sigma_1, \ldots, \sigma_n\} \text{ and } u_i(\sigma_j) = \delta_{ij}. \text{ Then clearly}

\[ \psi(1 \otimes x_i) = \sum_{j=1}^{n} \sigma_j(x_i) u_j \]

with } \psi \text{ as in (2.1), and so generators may be chosen for the } \mathfrak{O}\text{-module } R(K/k) \text{ so that the corresponding matrix of relations is } A = (\sigma_j(x_i)); \text{ then (4.1d) applies again to yield that}

\[ \text{ord}_k(R(K/k)) = \det(A) \mathfrak{O} = \det(\sigma_j(x_i)) \mathfrak{O} \quad (4.3) \]

for the case in which } \mathfrak{O} \text{ is a free } \sigma\text{-module with basis } \{x_1, \ldots, x_n\}.

Of course, a well-known and trivial computation shows that } A^tA = B, \text{ and Theorem 2.4 can be viewed as a module-theoretic generalization of this identity.}

We shall be especially interested in order ideals which arise in the following situation. Let } k \text{ be an algebraic number field with integer ring } \sigma, \text{ and } K \text{ be a Galois extension of } k \text{ with Galois group } \Gamma \text{ of order } n. \text{ If } L \text{ is a finite extension of } k \text{ with integer ring } \sigma_L, \text{ then a homomorphism } \chi: \Gamma \rightarrow \mu_n(L) \text{ of groups extends uniquely to an } \sigma\text{-algebra homomorphism } \sigma\Gamma \rightarrow \sigma_L \text{ which we shall also denote by } \chi. \text{ The construction (2.22a), applied to the } \sigma\Gamma\text{-module } R(K/k), \text{ then yields the finitely generated torsion } \sigma_L\text{-module}

\[ \chi \cdot R(K/k) = \sigma_L \otimes_{\sigma_L} R(K/k) \]
and our aim is to describe, for a cyclic extension $K/k$, the ideals $\text{ord}_L(\chi \cdot R(K/k))$ by means of appropriate generalizations of the classical Stickelberger elements of cyclotomic fields. Note that, in view of (4.1a, b), these ideals are closely related to composition series of $R(K/k)$, and hence the formulae of Section 2 will be relevant in this investigation.

We introduce, then, the following data:

(4.4a) If $n$ is a natural number, we denote by $\mu_n = \mu_n(\overline{Q})$ the cyclic group of order $n$ consisting of all $n$th roots of 1 in a fixed algebraic closure $\overline{Q}$ of $Q$.

(4.4b) If $\Gamma$ is a cyclic group of order $n$ and $i$ is a rational integer, we shall denote by $[i]_\Gamma$ the endomorphism of $\Gamma$ defined by the condition

$$[i]_\Gamma(\gamma) = \gamma^i$$

for $\gamma$ in $\Gamma$ (we write simply $[i]$ if the group $\Gamma$ is understood from the context). Of course, the mapping

$$(\mathbb{Z}/n\mathbb{Z})^* \to \text{Aut}(\Gamma)$$

$$i + n\mathbb{Z} \to [i]_\Gamma$$

is an isomorphism of groups.

(4.4c) We shall write $\Omega_n = \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$, the Galois group of the cyclotomic extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$. By the elementary theory of cyclotomic fields, the restriction map

$$\Omega_n \overset{\sim}{\longrightarrow} \text{Aut}(\mu_n)$$

is an isomorphism, and we shall use it to identify the two groups. Thus, in view of (4.4b), the symbol $[i] = [i]_{\mu_n}$ for $i$ in $\mathbb{Z}$ denotes a well-defined automorphism of the field $\mathbb{Q}(\mu_n)$; namely, that which is uniquely determined by the conditions

$$[i](\zeta) = \zeta^i$$

for $\zeta$ in $\mu_n$.

(4.4d) More generally, if $k$ is a subfield of $\mathbb{Q}$, we set $\Omega_{n,k} = \text{Gal}(k(\mu_n)/k)$. The restriction map $\Omega_{n,k} \hookrightarrow \Omega_n$ is then injective, and we shall identify $\Omega_{n,k}$ with its image in $\Omega_n$ under this map. As noted in (4.4c), $\Omega_{n,q} = \Omega_n$.

(4.4e) We set

$$\overline{\Omega}_n = \{i \text{ in } \mathbb{Z} \mid 0 < i < n \text{ and } (i, n) = 1\}.$$
In view of the last remark of (4.4b), the mapping

$$\bar{\Omega}_n \xrightarrow{\sim} \Omega_n$$

$$i \mapsto [i]_{\mu_n}$$

is bijective. If $X$ is a subset of $\Omega_n$, we denote by $\bar{X}$ its inverse image in $\bar{\Omega}_n$ under this map. Note that, if $k$ is a subfield of $\bar{Q}$, then

$$\{i + n\mathbb{Z} \mid i \text{ is in } \bar{\Omega}_{n,k}\}$$

constitutes the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ corresponding to $\Omega_{n,k} \subseteq \Omega_n$ under the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{\sim} \text{Aut}(\mu_n) = \Omega_n$$

of (4.4b).

We now introduce the desired Stickelberger elements and, after a crucial lemma, use them to obtain further information on the Galois module structure of $R(K/k)$ for suitable extensions $K/k$.

**Definition 4.5.** Given $n, r$ in $\mathbb{Z}$ with $n > 1$. If $k$ is a subfield of $\bar{Q}$, we set

$$\Theta_{n,k}(r) = \sum_{i \in \bar{\Omega}_{n,k}} \left< \frac{ri}{n} \right> [i]_{\mu_n}^{-1}$$

an element of $\mathbb{Q}\Omega_{n,k}$, with $\left< \quad \right>$ as in (2.18). We shall write

$$\Theta_n(r) = \Theta_{n,\mathbb{Q}}(r) = \sum_{i \in \bar{\Omega}_n} \left< \frac{ri}{n} \right> [i]_{\mu_n}^{-1}$$

in $\mathbb{Q}\Omega_n$. Note that $n\Theta_{n,k}(r)(n\Theta_n(r))$ is in $\mathbb{Z}\Omega_{n,k}(\mathbb{Z}\Omega_n)$.

Our results in the remainder of this section will arise from the data outlined below. Let:

(4.6a) $k$ be an algebraic number field contained in $\bar{Q}$, and $\mathfrak{o}$ be the ring of integers in $k$.

(4.6b) $\Gamma$ be a cyclic group of order $n$.

(4.6c) $\mathfrak{o}_L$ be the ring of integers in the cyclotomic field $L = k(\mu_n)$.

(4.6d) $\psi: \Gamma \xrightarrow{\sim} \mu_n$ be an isomorphism of groups. We shall denote by the same letter the induced $k$-algebra ($\mathfrak{o}$-algebra) homomorphism $\psi: k\Gamma \to L$ ($\psi: \mathfrak{o}\Gamma \to \mathfrak{o}_L$).
(4.6e) \( p \) be a prime of \( \mathfrak{o} \) such that the characteristic of the residue field \( k(p) \) is prime to \( n \) and \( k(p) \) contains \( n \) distinct \( n \)th roots of 1.

(4.6f) \( \chi: \Gamma \to \mu_n(k(p)) \) be a homomorphism of groups and \( k(p)(\chi) \) be, as in Lemma 2.25, the \( \mathfrak{o}_L \)-module defined by the conditions that \( k(p)(\chi) = k(p) \) as an \( \mathfrak{o} \)-module and \( \sigma(x) = \chi(\sigma) x \) for \( \sigma \) in \( \Gamma \) and \( x \) in \( k(p) \).

(4.6g) \( \psi \cdot k(p)(\chi) \) denote the \( \mathfrak{o}_L \)-module defined as in (2.22).

(4.6h) \( q \) be a prime of \( \mathfrak{o}_L \) above \( p \). Note that, in view of (e), \( p \) splits completely in \( L \), and so the canonical injection \( k(p) \isom L(q) \) is an isomorphism.

(4.6i) \( \psi_q: \Gamma \isom \mu_n(k(p)) \) denote the isomorphism defined by the commutative diagram

\[
\begin{array}{ccc}
\Gamma & \xrightarrow{\phi} & \mu_n(k(p)) \\
\downarrow{\phi} & & \downarrow{\cong} \\
\mu_n(k(p)) & \xrightarrow{\mu_n} & \mu_n(L(q))
\end{array}
\]

with the vertical and horizontal arrows denoting the canonical isomorphism of (h) and the isomorphism induced by the residue map \( \mathfrak{o}_L \to L(q) \), respectively.

The lemma below describes, under the hypotheses of (4.6), the \( \mathfrak{o}_L \)-module \( \psi \cdot k(p)(\chi) \).

**Lemma 4.7.** Given the data of (4.6).

(a) Assume that \( \chi = \psi^i \) for some \( i \) in \( \Omega_{n,k} \). Then

\[
\psi \cdot k(p)(\chi) \cong [i]^{-1} \cdot L(q)
\]

as \( \mathfrak{o}_L \)-modules, with \( [i] = [i]_n \) in \( \Omega_{n,k} \).

(b) If \( \chi \neq \psi^i \) for all \( i \) in \( \Omega_{n,k} \) (in particular, if \( \chi: \Gamma \to \mu_n(k(p)) \) is not an isomorphism), then

\[
\psi \cdot k(p)(\chi) = 0.
\]

**Proof.** Set \( M = \psi \cdot k(p)(\chi) \). The definition of \( M \) yields quickly that, if \( x, \sigma \) are in \( M \) and \( \Gamma \), respectively, then

\[
\psi(\sigma)x = \chi(\sigma)x.
\]  

(4.8a)
Note that $\chi(\sigma)x$ is a well-defined element of $M$ because $\chi(\sigma)$ is in $k(p)$ and $M$, being an $o$-module annihilated by $p$, can be viewed as a $k(p)$-space.

Assume now that $M \neq 0$; then, since $M$ has finite length, there is a simple (non-zero) factor $o_L$-module $N$ of $M$. Of course, the formula (4.8a) holds also for all $\sigma$ in $\Gamma$ and $x$ in $N$. Moreover, since $N$ is a simple $o_L$-module annihilated by $p$, the annihilator of $N$ is a prime $q'$ of $o$ above $p$. This means that $N \cong L(q')$ as $o_L$-modules, and thus the formula (4.8a) holds in $L(q')$.

Now, since $L/k$ is Galois and, by (4.6e), $p$ splits completely in $L$, we have that $q' = [i]^{-1}(q)$ for unique $i$ in $\mathcal{O}_{n,k}$. The diagram below then commutes:

\[
\begin{array}{ccc}
\mu_n & \xrightarrow{[i]^{-1}} & \mu_n \\
\alpha_1 & \downarrow & \phi \\
\Gamma & \rightarrow & \Gamma \\
\phi_i & \downarrow & \phi_i \\
\mu_n(L(q)) & \rightarrow & \mu_n(k(p)) & \rightarrow & \mu_n(L(q'))
\end{array}
\]

the unlabeled arrows denoting isomorphisms induced by obvious (and aforementioned) canonical maps. Of course, all mappings in the diagram are isomorphisms. It follows that

\[\psi(\sigma)x = \psi_q^i(\sigma)x\quad (4.8b)\]

for all $\sigma$ in $\Gamma$ and $x$ in $L(q')$. Comparison with (4.8a) yields that

\[\chi(\sigma) = \psi_q^i(\sigma)\]

in $k(p)$ for all $\sigma$ in $\Gamma$, i.e., $\chi = \psi_q^i$. This establishes (b).

Turning now to (a), let $\chi = \psi_q^i$ for some $i$ in $\mathcal{O}_{n,k}$. Then, with $[i]_\Gamma$ in $\text{Aut}(\Gamma)$ as in (4.4b),

\[k(p)(\chi) = k(p)(\psi_q^i) \cong [i]_\Gamma^{-1} \cdot k(p)(\psi_q)\]

as $o\Gamma$-modules, by (2.22d) and the fact that $\psi_q^i(\sigma) = \psi_q(\sigma^i)$ for all $\sigma$ in $\Gamma$. Since $\psi[i]_\Gamma^{-1} = [i]^{-1}\psi: o\Gamma \rightarrow o_L$, it follows from (2.22b) that

\[\psi \cdot k(p)(\chi) \cong \psi \cdot [i]_\Gamma^{-1} \cdot k(p)(\psi_q) \cong [i]^{-1} \cdot \{\psi \cdot k(p)(\psi_q)\}\]

as $o_L$-modules. Part (a) is then an immediate consequence of the $o_L$-module isomorphism

\[\psi \cdot k(p)(\psi_q) \cong L(q)\quad (4.9)\]
which we establish below (of course, (4.9) is simply the special case of (a) with \( i = 1 \)).

The desired \( \mathfrak{o}_L \)-module isomorphism

\[
f : \psi \cdot k(p)(\psi_q) = \mathfrak{o}_L \otimes_{\mathfrak{a}_q} k(p)(\psi_q) \to L(q)
\]

is given by the formula

\[
f(a \otimes_{\mathfrak{a}_q} x) = ax
\]

for \( a \) in \( \mathfrak{o}_L \) and \( x \) in \( k(p)(\psi_q) = k(p) \), where we identify \( x \) with its image in \( L(q) \) under the canonical isomorphism (4.6h). That \( f \) is a well-defined \( \mathfrak{o}_L \)-module homomorphism follows via routine computations from the commutative diagram of (4.6i); moreover, \( f \) is onto because \( f(1 \otimes_{\mathfrak{a}_q} x) = x \). Hence, to show that \( f \) is an isomorphism, it suffices to show that \( \psi \cdot k(p)(\psi_q) \) is a simple \( \mathfrak{o}_L \)-module.

Let \( \psi : I \to \mathfrak{o}_L/\mathfrak{p}_L \) be the composition \( \mathfrak{o} \)-algebra homomorphism

\[
\mathfrak{o} \xrightarrow{\psi} \mathfrak{o}_L \xrightarrow{\psi} \mathfrak{o}_L / \mathfrak{p}_L
\]

the unlabeled arrow denoting the canonical surjection. Since \( p \cdot k(p)(\psi_q) = 0 \),

\[
\psi \cdot k(p)(\psi_q) \cong \tilde{\psi} \cdot k(p)(\psi_q)
\]

as \( \mathfrak{o}_L \)-modules. Now, since \( p \) splits completely in \( L \),

\[
\mathfrak{p}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r
\]

where \( \mathfrak{q}_j \) for \( j \leq r \) are all primes of \( \mathfrak{o}_L \) above \( p \). Moreover, by (4.6i) the diagram below commutes:

\[
\begin{array}{ccc}
\mathfrak{o} & \xrightarrow{\psi} & \mathfrak{o}_L \\
\downarrow & & \downarrow \\
k(p) & \xrightarrow{\cong} & L(q_j)
\end{array}
\]

and thus the composite

\[
\mathfrak{o} \xrightarrow{\psi} \mathfrak{o}_L \to L(q_j)
\]

is surjective for each \( j \leq r \) (the unlabeled arrow denoting the residue map). The Chinese Remainder Theorem then implies that \( \tilde{\psi} \) is surjective; therefore, since \( k(p)(\psi_q) \) is a simple \( \mathfrak{o} \)-module, \( \psi \cdot k(p)(\psi_q) \) (and hence also \( \psi \cdot k(p)(\psi_q) \)) is a simple \( \mathfrak{o}_L \)-module. It follows that \( f \) is an isomorphism, completing the proof of (4.9) and the lemma.
We are now ready to obtain further information on \( R(K/k) \) for a cyclic extension \( K/k \) of number fields.

**Theorem 4.10.** Let \( \mathfrak{o} \subseteq k, n, L \) and \( v \) be as in (4.6), \( K \) be a Galois extension of \( k \) with cyclic Galois group \( \Gamma \) of order \( n \), and \( \mathfrak{O} \) be the maximal \( \mathfrak{o} \)-order in \( K \). Assume that \( v \) is ramified in \( K \), and let \( A \) be the inertial group of a prime \( \mathfrak{B} \) of \( \mathfrak{O} \) above \( v \) and \( r = [\Gamma : A] \). Then there is an isomorphism \( \chi: \Gamma \cong \mu_n(k(p)) \) such that the conditions below are satisfied for any prime \( q \) of \( \mathfrak{o}_L \) above \( v \):

(a) If \( \psi: \Gamma \cong \mu_n \) is any isomorphism, then

\[
\mathfrak{o}_L(\psi \cdot R(K/k)_v) \cong \bigoplus_{i \in \chi} n \left\langle \frac{r_i}{n} \right\rangle [i]^{-1} \cdot L(q)
\]

as \( \mathfrak{o}_L \)-modules, where \( \left\langle \cdot \right\rangle \) is as in (2.18), \( j \) is the unique element of \( \Omega_n \) such that \( \chi = \psi_q \) with \( \psi_q: \Gamma \cong \mu_n(k(p)) \) as in (4.6), and

\[
X_j = [j]^{-1} \Omega_{n,k} = \{ i \in \Omega_n \mid [i] \text{ is in } [j]^{-1} \Omega_{n,k} \}.
\]

(b) In particular, if \( \psi: \Gamma \cong \mu_n \) is the unique isomorphism rendering the diagram below commutative:

\[
\begin{array}{ccc}
\Gamma & \xrightarrow{\chi} & \mu_n(k(p)) \\
\downarrow{\psi} & & \downarrow{\cong} \\
\mu_n & \cong & \mu_n(L(q))
\end{array}
\]

then

\[
\mathfrak{o}_L(\psi \cdot R(K/k)_v) \cong n\Theta_{n,k}(r) \cdot L(q)
\]

and

\[
\ord_L(\psi \cdot R(K/k)_v) = q^{n\Theta_{n,k}(r)}
\]

(where we write the action of the group ring \( \mathbb{Z}\Omega_{n,k} \) on ideals and ideal classes exponentially).

**Proof.** Note first that the \( \mathfrak{o}_L \)-modules \( [i]^{-1} \cdot L(q) \) in the formula of (a) are meaningful, since \( [i] = [i] [j] \) is in \( \Omega_{n,k} \subseteq \Omega_n \) for \( i \) in \( X_j \). Moreover, if \( \psi \) is as in (b), then \( \chi = \psi_q \) and so, in view of (4.5), the first assertion of (b)
follows from (a) upon setting \( j = 1 \). The second assertion of (b) is then a consequence of the first, together with (a), (b), and (e) of (4.1).

Turning now to (a), recall first that, by Corollary 2.19,

\[
\phi_{af}(R(K/k)_{p}) \simeq \bigoplus_{i=1}^{n} n \left( \frac{r_i}{n} \right) k(p)(\chi^i)
\]

for a suitable group isomorphism \( \chi: \Gamma \cong \mu_n(k(p)) \). Since \( p \) is prime to \( n \), it follows from Maschke's Theorem and a routine localization argument that \( k(p)(\chi^i) \) is an \( \sigma \Gamma \)-module of homological dimension one. Since the functor

\[
\psi \cdot (-) = \sigma_{\Gamma} \otimes_{\sigma_{af}} (-)
\]

preserves short exact sequences of such modules, we obtain that

\[
\phi_{af}(\psi \cdot R(K/k)_{p}) \simeq \bigoplus_{i=1}^{n} n \left( \frac{r_i}{n} \right) \psi \cdot k(p)(\chi^i)
\]

as \( \sigma_{\Gamma} \)-modules. But, if \( \chi = \psi_q^i \), then \( \chi^i = \psi_q^{ij} \), and thus, by (4.4d) and Lemma 4.7,

\[
\psi \cdot k(p)(\chi^i) \simeq \begin{cases} [ij]^{-1} \cdot L(q) & \text{if } [ij] \text{ is in } \Omega_{n,k} \\ 0 & \text{if } [ij] \text{ is not in } \Omega_{n,k}. \end{cases}
\]

Since \([ij]\) is in \( \Omega_{n,k} \) if and only if \( i \) is in \( X_j \), (a) follows immediately, completing the proof of the theorem.

We now pursue the considerations of Theorem 4.10 a bit further but in a somewhat different direction. Assume given the data of (4.6); in particular, an isomorphism \( \psi: \Gamma \cong \mu_n \) of groups. As in (4.6d), we also denote by \( \psi \) the induced \( k \)-algebra surjection \( \psi: k\Gamma \rightarrow L = k(\mu_n) \). However, we have in addition the induced \( \mathbb{Q} \)-algebra surjection

\[
\psi_0: \mathbb{Q} \Gamma \rightarrow \mathbb{Q}(\mu_n)
\]

which yields, upon tensoring with \( k \), a \( k \)-algebra surjection

\[
\psi_0: k\Gamma \rightarrow A = k \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_n).
\]  

(4.11a)

\( A \) is a commutative semi-simple \( k \)-algebra, and thus possesses a unique maximal \( \sigma \)-order \( \mathfrak{A} \). We then have, finally, the induced \( \sigma \)-algebra homomorphism

\[
\psi_0: \sigma \Gamma \rightarrow \mathfrak{A}.
\]  

(4.11b)

Given the cyclic extension \( K/k \) as in Theorem 4.10, we shall obtain a partial
description of the \( \mathfrak{M} \)-module \( \psi_0 \cdot R(K/k) \) in terms of the Stickelberger elements of (4.5a); this description will follow easily from our preceding discussion.

Let us examine the algebras \( \mathfrak{M} \subseteq A \) a bit more closely. It follows easily from Galois theory that there is a \( k \)-algebra isomorphism

\[
\phi: A \xrightarrow{\cong} (\Omega_n, L)^{\Omega_{n,k}}
\]

with the property that

\[
\phi(x \otimes y)(\omega) = x\omega(y)
\]

for \( x, y, \omega \in k, \mathcal{O}(\mu_n), \) and \( \Omega_n, \) respectively, where we regard \( \Omega_n \) as a left \( \Omega_{n,k} \)-set. Note that the formula is meaningful since, if \( y, \omega \) are as above, then \( \omega(y) \) is in \( \mathcal{O}(\mu_n) \subseteq L \). \( \phi \) is a routine variant of the isomorphisms of (1.6). Restriction to \( \mathfrak{M} \) yields the corresponding \( \mathfrak{m} \)-algebra isomorphism

\[
\phi: \mathfrak{M} \xrightarrow{\cong} (\Omega_n, \mathfrak{m})^{\Omega_{n,k}}.
\]

Note finally that the action of \( \Omega_n \) on the right factor of \( A = k \otimes \mathcal{O}(\mu_n) \) renders \( A \) a Galois extension of \( k \) with Galois group \( \Omega_n \), since such extensions are preserved by change of base.

We shall, when convenient, identify the relevant algebras via the isomorphisms of (4.12). Then \( A \) is isomorphic to a product of copies of \( L \), one for each right coset of \( \Omega_n \) modulo \( \Omega_{n,k} \). If \( \omega \) is in \( \Omega_n \), then the corresponding projection map

\[
\phi_\omega: A \to L
\]

is, in view of (4.12a), given by the formula

\[
\phi_\omega(x \otimes y) = x\omega(y)
\]

for \( x, y \) as in (4.12a). This quickly yields the useful identities below:

\[
\begin{align*}
\phi_{\omega\omega'} &= \phi_\omega \omega' \quad (\omega, \omega' \in \Omega_n) \\
\phi_{\omega\omega'} &= \omega \phi_\omega \quad (\omega \in \Omega_{n,k}, \omega' \in \Omega_n) \\
\phi_{[i]} \psi_0 &= \psi^i : k\Gamma \to L
\end{align*}
\]

with \( i \) in \( \Omega_n \) and \([i] = [i]_{\mu_n} \) in \( \Omega_n \). The right-hand side of (4.13b) is meaningful in view of the above-noted action of \( \Omega_n \) on \( A \) by \( k \)-algebra automorphisms, and we interpret the \( k \)-algebra homomorphism \( \psi^i : k\Gamma \to L \) by means of the convention of (4.6d). Assertions analogous to (4.12)–(4.13) apply also to \( \mathfrak{M} \) with \( L, k\Gamma \) replaced by \( \mathfrak{m} \) and \( \mathfrak{m}\Gamma \), respectively. The trivial
structure theory of modules over a direct product of rings, together with (4.12b), (4.13c), and (2.22b), then yields the following facts:

(4.14) Assume given, for each $\omega$ in $\Omega_n$, an $o_L$-module $M(\omega)$ with the property that $M(\omega \omega') \approx \omega \cdot M(\omega')$ for all $\omega$ in $\Omega_{n,k}$ and $\omega'$ in $\Omega_n$. Then there is an $\mathfrak{U}$ module $M$, unique up to isomorphism, such that $\phi_\omega \cdot M \approx M(\omega)$ as $o_L$-modules for all $\omega$ in $\Omega_n$. In particular, if $M$ and $N$ are $\mathfrak{U}$-modules, then $M \approx N$ if and only if $\phi_\omega \cdot M \approx \phi_\omega \cdot N$ as $o_L$-modules for all $\omega$ in $\Omega_n$.

The theorem below follows from the general formulae of Theorem 4.10 via a fairly routine computation. However, it is perhaps clearer to apply a direct argument utilizing Lemma 4.7.

**THEOREM 4.15.** Let $n, \Gamma, K/k, p, \text{etc.},$ be as in Theorem 4.10, and $\psi: \Gamma \cong \mu_n$ be an isomorphism. Then there is a simple $\mathfrak{U}$-module $M$, depending on $\psi$, such that $pM = 0$ and

$$\delta_{\mathfrak{U}}(\psi_0 \cdot R(K/k)_p) \approx n\Theta_n(r) \cdot M$$

as $\mathfrak{U}$-modules, with the $o$-algebra homomorphism $\psi_0: o\Gamma \to \mathfrak{U}$ as in (4.11b).

**Proof.** An argument entirely similar to that of the proof of Theorem 4.10(a) shows that, for a suitable group isomorphism $\chi: \Gamma \cong \mu_n(k(p)),$

$$\delta_{\mathfrak{U}}(\psi_0 \cdot R(K/k)_p) \approx \prod_{i=1}^{n} \left( \frac{ri}{n} \right) \psi_0 \cdot k(p)(\chi^i)$$

as $\mathfrak{U}$-modules. Now, letting $q$ be a prime of $o_L$ above $p$, we shall first consider the case in which $\psi$ is as in Theorem 4.10(b), i.e., the unique isomorphism $\psi: \Gamma \cong \mu_n$ such that $\psi_q = \chi$, with $\psi_q$ as in (4.6i).

By (4.14), (4.13c), and (2.22b), there is an $\mathfrak{U}$-module $M$ which is uniquely determined up to $\mathfrak{U}$-module isomorphism by the conditions below for $\omega$ in $\Omega_n$:

$$\phi_\omega \cdot M = \begin{cases} \omega \cdot L(q) & \text{if } \omega \text{ is in } \Omega_{n,k} \\ 0 & \text{if } \omega \text{ is not in } \Omega_{n,k}. \end{cases}$$

Since $L(q)$ is a simple $o_L$ module and $pL(q) = 0$, (4.12b) and the remarks following it imply that $M$ is a simple $\mathfrak{U}$-module and $pM = 0$. Moreover, if $i, j$ are rational integers prime to $n$, then

$$\phi_{[i-1]} \cdot ([i]^{-1} \cdot M) \approx \phi_{[i-1]} \cdot M$$

$$\approx \begin{cases} [i]^{-1} \cdot L(q) & \text{if } [ij] \text{ is in } \Omega_{n,k} \\ 0 & \text{if } [ij] \text{ is not in } \Omega_{n,k} \end{cases}$$

(4.17b)
the first isomorphism from (4.13b). Now, if \( \tilde{\psi}: \Gamma \xrightarrow{\sim} \mu_n \) is the unique isomorphism with the property that \( \tilde{\psi}^j = \psi \), then
\[
\chi^j = \psi^j_0 = \tilde{\psi}^j
\]
and then, by (2.22b), (4.13d), and Lemma 4.7.
\[
\phi_{|j|} \cdot (\psi_0 \cdot k(p)(\chi^j)) \approx \tilde{\psi} \cdot k(p)(\chi^j) \approx \begin{cases} 
|j|^{-1} \cdot L(a) & \text{if } |j| \text{ is in } \Omega_{n,k} \\
0 & \text{if } |j| \text{ is not in } \Omega_{n,k}.
\end{cases}
\quad (4.18)
\]
Since this is true for all \( j \) prime to \( n \), we may compare (4.17b) and (4.18) and apply (4.14) to conclude that
\[
\psi_0 \cdot k(p)(\chi^i) \approx |i|^{-1} \cdot M
\]
(4.19a) as \( \sigma \cdot \text{modules} \) for all \( i \) prime to \( n \). On the other hand, if \( i \) is not prime to \( n \) then, by (4.13d) and Lemma 4.7,
\[
\phi_{|j|} \cdot (\psi_0 \cdot k(p)(\chi^j)) \approx \psi^j \cdot k(p)(\chi^j) = 0
\]
for all \( j \) as above, and thus
\[
\psi_0 \cdot k(p)(\chi^i) = 0
\]
(4.19b) again by (4.14). The formulæ (4.16) and (4.19) immediately yield the desired \( \mathfrak{U} \)-module isomorphism
\[
\varphi_{\mathfrak{U}}(\psi_0 \cdot R(K/k)_p) \approx n\Theta_n(r) \cdot M
\]
for the special case in which \( \psi_0 = \chi \).

In the general case, \( \psi = \tilde{\psi}^j \) for some \( j \) prime to \( n \), with \( \tilde{\psi}: \Gamma \xrightarrow{\sim} \mu_n \) the unique isomorphism such that \( \tilde{\psi}_0 = \chi \). Then \( \psi_0 = |j| \tilde{\psi}_0: \sigma \Gamma \to \mathfrak{U} \). Moreover, by the special case proved above, there is a simple \( \mathfrak{U} \)-module \( \tilde{M} \) such that \( p\tilde{M} = 0 \) and
\[
\varphi_{\mathfrak{U}}(\psi_0 \cdot R(K/k)_p) \approx n\Theta_n(r) \cdot \tilde{M}.
\]
But then
\[
\varphi_{\mathfrak{U}}(\psi_0 \cdot R(K/k)_p) \approx \varphi_{\mathfrak{U}}(|j| \cdot (\tilde{\psi}_0 \cdot R(K/k)_p)) \approx |j| \cdot \varphi_{\mathfrak{U}}(\tilde{\psi}_0 \cdot R(K/k)_p) \approx |j| \cdot n\Theta_n(r \cdot \tilde{M}) \approx n\Theta_n(r) \cdot M
\]
with \( M = |j| \cdot \tilde{M} \), the third isomorphism because the functor \( |j| \cdot (-) \) is exact and preserves simple modules. This completes the proof of the theorem.
Corollary 4.20. Let $\mathfrak{o} \subseteq k, n, \Gamma, \mathfrak{o}_L \subseteq L,$ and $\mathfrak{A} \subseteq A$ be as in Theorem 4.15, $K$ be a Galois extension of $k$ with Galois group $\Gamma,$ and $\mathfrak{O}$ be the maximal $\mathfrak{o}$-order in $K.$ Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be all primes of $\mathfrak{o}$ which ramify in $K,$ and for each $i \leq s$ let $\Delta_i$ be the inertial group of a prime of $\mathfrak{O}$ above $\mathfrak{p}_i.$ Assume that the following conditions hold:

(a) Each $\mathfrak{p}_i$ is prime to $n$ and the residue field $k(\mathfrak{p}_i)$ contains $n$ distinct $n$th roots of 1.

(b) $r = [\Gamma: \Delta_i]$ is independent of $i \leq s.$

Then, if $\psi: \Gamma \cong \mu_n$ is an isomorphism of groups, there is an $\mathfrak{o}$-torsion $\mathfrak{A}$-module $M$ (depending upon $\psi$) such that $M_{\mathfrak{p}_i}$ is a simple $\mathfrak{A}$-module for $i \leq s,$ $M_\mathfrak{p} = 0$ for $\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and

$$\phi_{\mathfrak{A}}(\psi_0 \cdot R(K/k)) \approx n\Theta_n(r) \cdot M$$

as $\mathfrak{A}$-modules, with $\psi_0: \mathfrak{o}\Gamma \to \mathfrak{A}$ as in (4.11b).

Proof. By Theorem 4.15 there is, for each $i,$ a simple $\mathfrak{A}$-module $M_i,$ $\mathfrak{p}_i$-primary as an $\mathfrak{o}$-module, such that

$$\phi_{\mathfrak{A}}(\psi_0 \cdot R(K/k)_{\mathfrak{p}_i}) \approx n\Theta_n(r) \cdot M_i.$$ 

Since $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are all primes of $\mathfrak{o}$ which ramify in $K$

$$R(K/k) \cong \prod_{i=1}^{s} R(K/k)_{\mathfrak{p}_i}$$

and so the corollary follows immediately with

$$M = \prod_{i=1}^{s} M_i.$$ 

Theorems 4.10 and 4.15 quickly yield two global results, the second of which is a weak form of the classical theorem that the ideal class group of a cyclotomic extension of $\mathbb{Q}$ is annihilated by the "Stickelberger ideal"; see, e.g., [7, Theorem 2.4, p. 131] or [6, Sect. 4, pp. 604–605]. Our proof is based on the Hilbert–Speiser theorem that a tame abelian extension of $\mathbb{Q}$ possesses a normal integral basis, and in that respect is similar in spirit to the argument given in [6].

Corollary 4.21. Given the data of Corollary 4.20. Assume, in addition to conditions (a)–(b) of Corollary 4.20, that $\mathfrak{O} \otimes_\mathfrak{o} \mathfrak{O} \cong \mathfrak{O}\Gamma$ as $\mathfrak{o}\Gamma$-modules (with $\Gamma$ acting on the right-most factor of $\mathfrak{O} \otimes_\mathfrak{o} \mathfrak{O}$).
(a) If $s = 1$, then

$$q^{n\Theta_{n,k}(r)}$$

is a principal ideal of $\mathcal{O}_L$ for any prime $q$ of $\mathcal{O}_L$ above $p = p_1$.

(b) Assume, on the other hand, that $k$ and $L$ are linearly disjoint. Then there is an ideal $b$ of $\mathcal{O}_L$ such that $b \cap \mathcal{O} = p_1 \cdots p_s$ and

$$b^{n\Theta_{n,k}(r)}$$

is a principal ideal of $\mathcal{O}_L$.

Proof. The definition of $R(K/k)$ yields the $\mathcal{O}_L$-module short exact sequence

$$0 \rightarrow \mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O} \rightarrow (\Gamma, \mathcal{O}) \rightarrow R(K/k) \rightarrow 0. \quad (4.22a)$$

Now, Corollary 4.20(a) and Maschke's Theorem imply, via an argument entirely similar to that of the proof of Theorem 4.10(a), that $R(K/k)$ is an $\mathcal{O}_L$-module of homological dimension one. Hence, if $\psi: \Gamma \overset{\sim}{\rightarrow} \mu_n$ is an isomorphism of groups, $(4.22a)$ and routine homological algebra yield the exact sequence

$$0 \rightarrow \psi \cdot (\mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O}) \rightarrow \psi \cdot (\Gamma, \mathcal{O}) \rightarrow \psi \cdot R(K/k) \rightarrow 0 \quad (4.22b)$$

of $\mathcal{O}_L$-modules, with the $\mathcal{O}$-algebra homomorphism $\psi: \Gamma \rightarrow \mathcal{O}_L$ as in $(4.6d)$. In addition, since $(\Gamma, \mathcal{O}) \cong \mathcal{O}\Gamma \cong \mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O}$ as $\mathcal{O}_L$-modules, we obtain that

$$\psi \cdot (\mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O}) \cong \psi \cdot (\Gamma, \mathcal{O}) \quad (4.23)$$

as $\mathcal{O}_L$-modules.

Note first that, if $s = 1$, then Corollary 4.20(b) is vacuous and $R(K/k) = R(K/k)_p$ with $p = p_1$ the unique prime of $\mathcal{O}$ ramified in $K$. Then, if $q$ is a prime of $\mathcal{O}_L$ above $p$, we have from Theorem 4.10(b) that

$$\text{ord}_L(\psi \cdot R(K/k)) = q^{n\Theta_{n,k}(r)}$$

for a suitable group isomorphism $\psi: \Gamma \overset{\sim}{\rightarrow} \mu_n$. Equations $(4.22b)$, $(4.23)$, and $(4.1d)$ then yield that this ideal of $\mathcal{O}_L$ is principal, establishing (a).

On the other hand, if $k$ and $L$ are linearly disjoint, then $L = A$, $\mathcal{O}_f = \mathfrak{A}$, $\Omega_{n,k} = \Omega_n$, and $\psi = \psi_0: \mathcal{O}_f \rightarrow \mathcal{O}_L = \mathfrak{A}$, with $\mathfrak{A} \subseteq A$ as in Corollary 4.20 and $\psi: \Gamma \overset{\sim}{\rightarrow} \mu_n$, any isomorphism. Therefore, by that corollary

$$\sigma_{\mathcal{O}_f}(\psi \cdot R(K/k)) \cong n\Theta_{n,k}(r) \cdot M$$
with $M$ an $\mathcal{A}$-module satisfying the conditions of the corollary. The same argument as above, together with (4.1b) and (4.1e), then shows that

$$\text{ord}_{\mathfrak{L}}(\psi \cdot R(K/k)) = b^{\Theta_{n,k}(r)}$$

is a principal ideal of $\mathcal{L}$, with $b = \text{ord}_{\mathfrak{L}}(M)$.

Now, by Corollary 4.20, $M_{p_i}$ is a simple $p_i$-primary $\mathcal{O}_L$-module for all $i < s$, and thus $M_{p_i} \cong L(q_i)$ for some prime $q_i$ of $\mathcal{O}_L$ above $p_i$. Since

$$M = \prod_{i=1}^{s} M_{p_i} = \prod_{i=1}^{s} L(q_i)$$

it follows from (4.1a,b) that $b = q_1 \cdots q_s$. Thus $b \cap \mathfrak{p} = p_1 \cdots p_s$, establishing (b) and completing the proof.

Finally, we apply the preceding considerations to the case $k = \mathbb{Q}$. Of course, in that case $L = \mathbb{Q}(\mu_n)$ and $\mathcal{O}_{n,k} = \mathcal{O}_{n,l} = \mathcal{O}_n$. We shall denote by $\text{Pic}(\mathcal{O}_L)$ the ideal class group of $\mathcal{O}_L$, a $\mathbb{Z}_{\mathcal{O}_n}$-module.

**Corollary 4.24.** Let $n$ be a natural number greater than one, $L = \mathbb{Q}(\mu_n)$, and $r$ be a divisor of $n$. Then the element

$$\left(\frac{n}{r}\right) \Theta_{n}(r)$$

of $\mathbb{Z}_{\mathcal{O}_n}$ annihilates $\text{Pic}(\mathcal{O}_L)$.

**Proof.** Note first that, by (2.18),

$$\frac{n}{r} \left(\frac{r^i}{n}\right)$$

is in $\mathbb{Z}$ for any $i$ in $\mathbb{Z}$, and thus the above multiple of $\Theta_{n}(r)$ is in $\mathbb{Z}_{\mathcal{O}_n}$.

Given $C$ in $\text{Pic}(\mathcal{O}_L)$, a classical theorem on primes in an arithmetic progression provides a prime $q$ of $\mathcal{O}_L$ in the ideal class $C$ with the property that, if $q \cap \mathbb{Z} = p\mathbb{Z}$ with $p$ a rational prime, then $p \equiv 1 \pmod{n}$. Then, by [2, Lemmas 1–4, p. 87], $\mathbb{Q}(\mu_p)$ is a cyclic extension of $\mathbb{Q}$ of degree $p - 1$ which is totally ramified at $p$ and non-ramified at all other primes. Let $d = n/r$; then $d \mid p - 1$, and so there is a unique subfield $E$ of $\mathbb{Q}(\mu_p)$ which is a cyclic extension of $\mathbb{Q}$ of degree $d$ and satisfies the same ramification conditions.

Let $G$ be cyclic of order $n$; then the Galois group of $E/\mathbb{Q}$ can be identified with the subgroup $\Delta$ of $G$ of order $d$. By [3, Proposition 1.2(5), p. 81] the $\mathbb{Q}$-algebra

$$K = (G, E)^\Delta$$
is then a Galois extension of $\mathbb{Q}$ with Galois group $\Gamma$ which acts on $K$ according the formula

$$\gamma(u)(\sigma) = u(\gamma)$$

for $\sigma, \gamma$ in $\Gamma$ and $u: \Gamma \to E$ in $K$. Let $\mathfrak{O}$ be the maximal order in $K$. The above-mentioned ramification conditions on $E$ then imply that $p$ is the only rational prime which ramifies in $K$, and $\Delta$ is the inertial group of a prime of $\mathfrak{O}$ above $p$. Since $p$ is prime to $n$, $E/\mathbb{Q}$ is tame, and thus the integer ring $\mathfrak{o}_E$ of $E$ is a free $\mathbb{Z}\Delta$-module by the above-mentioned theorem of Hilbert–Speiser [6, p. 591]; then

$$\mathfrak{O} = (\Gamma, \mathfrak{o}_E)^{\Delta} \approx \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathfrak{o}_E$$

is a free $\mathbb{Z}\Gamma$-module. Finally, since $p \equiv 1 \pmod{n}$, the residue field $F_p$ contains all $n$th roots of 1, and so we may apply Corollary 4.21 (a) to obtain that

$$\mathfrak{o}_E^{n\Theta_\alpha(r)}$$

is a principal ideal of $\mathfrak{o}_E$.

However, we want a stronger result; namely, that

$$\mathfrak{o}_E^{(n/r)\Theta_\alpha(r)}$$

is a principal ideal, and to this end we must argue a bit more carefully. By (4.25), $\mathfrak{O}$ is isomorphic as a $\mathbb{Z}$ algebra to a direct product of $r$ copies of $\mathfrak{o}_E$, one for each coset of $\Gamma$ modulo $\Delta$. Since the mappings in the exact sequence (4.22a) are $\mathfrak{O}\Gamma$-module homomorphisms, we may pass to components to obtain a $\mathbb{Z}\Gamma$-module exact sequence

$$0 \to \mathfrak{o}_E \otimes \mathbb{Z} \mathfrak{O} \to (\Gamma, \mathfrak{o}_E) \to S(K/\mathbb{Q}) \to 0$$

where $\mathfrak{o}_E \otimes \mathbb{Z} \mathfrak{O}$ and $(\Gamma, \mathfrak{o}_E) \approx \mathbb{Z}\Gamma \otimes \mathbb{Z} \mathfrak{o}_E$ are free $\mathbb{Z}\Gamma$-modules and

$$rS(K/\mathbb{Q}) \approx R(K/\mathbb{Q})$$

as $\mathbb{Z}\Gamma$-modules. If $\psi: \Gamma \cong \mu_p$ is an isomorphism of groups, we then obtain, as in the proof of Corollary 4.21, the $\mathfrak{o}_E$-module exact sequence

$$0 \to \psi \cdot (\mathfrak{o}_E \otimes \mathbb{Z} \mathfrak{O}) \to \psi \cdot (\Gamma, \mathfrak{o}_E) \to \psi \cdot S(K/\mathbb{Q}) \to 0$$
with the two left terms free $\mathcal{O}$-modules. Also, by (4.26b) and Theorem 4.10 (b),
\[ \text{ord}_L(\psi \cdot S(K/Q))^r = \text{ord}_L(\psi \cdot R(K/Q)) = q^{n \theta_n(r)} \]
for suitable $\psi$ (since, in this case, $R(K/Q) = R(K/Q)_p$), and thus
\[ \text{ord}_L(\psi \cdot S(K/Q)) = q^{(n/r) \theta_n(r)}. \]
We then conclude from (4.26c) and (4.1d) that this is a principal ideal of $\mathcal{O}_L$.

Therefore
\[ C^{(n/r) \theta_n(r)} = 1 \]
in $\text{Pic}(\mathcal{O}_L)$, completing the proof.

Remark 4.27. Note that the hypothesis of Corollary 4.21 that $\mathcal{O} \otimes_{\mathcal{O}} \mathcal{O}$
and $\mathcal{O}^r$ be isomorphic $\mathcal{O}^r$-modules is satisfied if, for example, $\mathcal{O}$ is a free $\mathcal{O}$-
module and $\mathcal{O} \otimes_{\mathcal{O}} \mathcal{O}$ is free $\mathcal{O}^r$-module.

ACKNOWLEDGMENTS

Although the research for this paper spans the years 1977–1982, much of the work was
done in early 1979 when the author was on sabbatical leave from Cornell University and
visiting King's College, London. The author is indebted to King's College for its generous
hospitality, to the National Science Foundation and British Science Research Council for
their support, and to his colleagues in London and Ithaca for stimulating conversations and
timely suggestions, particularly T. Chinburg, A. Fröhlich, L. McCulloh, A. Nelson, and
M. Taylor.

REFERENCES

   1967.
3. F. De Meyer and E. Ingraham, Separable algebras over commutative rings, in "Lecture
5. A. Fröhlich, Arithmetic and Galois module structure for tame extensions, J. Reine
6. A. Fröhlich, Stickelberger without Gauss sums, in "Algebraic Number Fields (L-