Galois Module Structure
of Elementary Abelian Extensions

LEON R. MCCULLOH*

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Communicated by A. Fröhlich

Received April 2, 1982

Let $K$ be an algebraic number field, $\mathcal{O} = \mathcal{O}_K$ its ring of integers, and $G$ an elementary abelian group of order $p^a$. In this article, we determine which classes in the locally free class group $Cl(\mathcal{O}G)$ of the group ring $\mathcal{O}G$ are realizable as Galois module classes of rings of integers $\mathcal{O}_L$ in tame Galois extensions $L/K$ with $\text{Gal}(L/K) \cong G$. The set $R(\mathcal{O}G)$ of such realizable classes is described in terms of the action on $Cl(\mathcal{O}G)$ of a Stickelberger ideal $\mathcal{F}$ in the integral group ring $\mathbb{Z}C$, where $C$ ($\cong \mathbb{F}_p^a$) is a (Cartan) subgroup of the automorphism group $\text{Aut} G (\cong \text{GL}_a(\mathbb{F}_p))$.


table

| $L/K$ is a Galois extension of algebraic number fields, the ring of integers $\mathcal{O}_L$ is a Galois module—that is, a representation module for the Galois group $G$. Much is known about the structure of $\mathcal{O}_L$ as a $\mathbb{Z}G$-module.

With Taylor’s proof [12] of Fröhlich’s conjecture, we know that for tame extensions $L/K$, $\mathcal{O}_L$ is determined up to stable $\mathbb{Z}G$-isomorphism by the Artin root numbers $W(\chi)$ of the symplectic characters of $G$, and in particular that $\mathcal{O}_L$ is stably free if all such $W(\chi) = 1$. (So, for example, if $G$ is abelian and $L/K$ is tame, then $\mathcal{O}_L$ is always free as a $\mathbb{Z}G$-module.)

In this article, we adopt a somewhat different viewpoint. We regard $\mathcal{O}_L$ as an $\mathcal{O}G$-module, where $\mathcal{O} = \mathcal{O}_K$, the ring of integers of $K$. Changing the coefficient ring from $\mathbb{Z}$ to $\mathcal{O}$ introduces complications. Typically $\mathcal{O}_L$ is not free as an $\mathcal{O}$-module, and all the less so as an $\mathcal{O}G$-module. For example, the unramified extension $\mathbb{Q}(\sqrt{-5}, \sqrt{5})/\mathbb{Q}(\sqrt{-5})$, has no relative normal integral basis (although it does have a relative integral basis).

* The main result of this article was obtained while the author was on sabbatical leave from the University of Illinois at Universität Regensburg and at King’s College, London. The author wishes to thank those institutions for their generous hospitality and the NSF for providing support while the results were being extended and the proofs simplified.

0021-8693/83 $3.00
Copyright © 1983 by Academic Press, Inc.
All rights of reproduction in any form reserved.
Our emphasis differs also in the following respect. We fix the ground field $K$ and a finite group $G$ and let $L$ range over all Galois extensions of $K$ with Galois group isomorphic to $G$, regarding all the rings of integers $\mathcal{O}_L$ as modules over the same group ring $\sigma G$ by choosing isomorphisms $\text{Gal}(L/K) \cong G$. Changing the isomorphism $\text{Gal}(L/K) \to G$ amounts to changing the representation by an automorphism of $G$, so it is natural in this context to consider the totality of $\sigma G$-representations under the action of the automorphism group $\text{Aut} G$.

The extension $L/K$ is tame if and only if $\mathcal{O}_L$ is a locally free $\sigma G$-module. It is then determined up to stable isomorphism by its “Galois module class” in the class group $\text{Cl}(\sigma G)$. We shall restrict our attention to tame extensions and denote by $R(\sigma G)$ the set of those classes in $\text{Cl}(\sigma G)$ which are realizable as Galois module classes of rings of integers $\mathcal{O}_L$ in tame Galois extensions $L/K$ with $\text{Gal}(L/K) \cong G$. Trivially, $R(\sigma G)$ is closed under the action of $\text{Aut} G$ on $\text{Cl}(\sigma G)$.

The main result of this article is the description of $R(\sigma G)$ for elementary abelian $G$ in terms of the action on $\text{Cl}(\sigma G)$ of a Stickelberger ideal. Specifically, let $G$ be the additive group of the finite field $\mathbb{F}_{p^k}$ and let $C = \mathbb{F}_{p^k}^\times$, the multiplicative group. Multiplication represents $C$ as a group of automorphisms of $G$ and hence as a group of automorphisms of $\sigma G$ fixing $\sigma$. The class group $\text{Cl}(\sigma G)$ is thus a $\mathbb{Z}C$-module. We define a Stickelberger ideal in $\mathbb{Z}C$ as follows.

For $\delta \in C$, let $t(\delta)$ denote the least non-negative residue (mod $l$) of $\text{Tr}(\delta)$, where $\text{Tr}: \mathbb{F}_{p^k} \to \mathbb{F}_l (=\mathbb{Z}/l\mathbb{Z})$ is the trace. Let

$$\theta = \sum_{\delta \in C} t(\delta) \delta^{-1} \in \mathbb{Z}C,$$

and

$$\mathcal{F} = \mathbb{Z}C \cdot (\theta/l) \cap \mathbb{Z}C.$$

The Stickelberger ideal $\mathcal{F}$ is a relative of one used by Kubert and Lang [7]. However, it is associated with values of L-functions at $s = 0$ rather than at $s = -1$.

The main result is

**Theorem.** If $G$ is elementary abelian,

$$R(\sigma G) = \text{Cl}'(\sigma G)^{\mathcal{F}},$$

where $\text{Cl}'(\sigma G)$ is the kernel of the map $\text{Cl}(\sigma G) \to \text{Cl}(\sigma)$ induced by the augmentation $\sigma G \to \sigma$. 
Putting \( K = \mathbb{Q} \), we immediately obtain the result announced in Theorem (1.2) of [91:

**COROLLARY.** If \( G \) is elementary abelian, \( \text{Cl}(\mathbb{Z}G)\mathcal{F} = 1 \).

**Proof.** \( \text{Cl}'(\mathbb{Z}G) = \text{Cl}(\mathbb{Z}G) \) since \( \text{Cl}(\mathbb{Z}) = 1 \), and \( R(\mathbb{Z}G) = 1 \) since every tame abelian extension of \( \mathbb{Q} \) has a normal integral basis.

Now specialize further to the case \( G \) cyclic of order 1. Choosing a non-trivial character \( \chi: G \to \mu \) induces an isomorphism (see [11])

\[
\text{Cl}(\mathbb{Z}G) \cong \text{Cl}(\mathbb{Z}|\mu_1|).
\]

If we interpret \( C (=\mathbb{F}^\chi \mathcal{F}) \) as the Galois group of \( \mathbb{Q}(\mu_1)/\mathbb{Q} \), \( \mathcal{F} \) becomes the classical Stickelberger ideal for \( \mathbb{Q}(\mu_1) \) and the corollary asserts the classical Stickelberger relations for the class group of \( \mathbb{Q}(\mu_1) \).

The connection between Galois module structure and Stickelberger ideals can be seen as a natural outgrowth of Hilbert’s proof [6, Satz 136] of the Stickelberger relations for \( \mathbb{Q}(\mu_1) \) which was based on the fact that tame cyclic extensions \( L/\mathbb{Q} \) of degree 1 have normal integral bases. Hilbert determines the prime factorization of resolvents of normal basis generators by utilizing their behavior under the action of \( \text{Gal}(L/\mathbb{Q}) \) and of \( \text{Gal}(\mathbb{Q}(\mu_1)/\mathbb{Q}) \). (The resolvents are not specifically required to be Gauss sums.)

Our approach is very close to that of Hilbert’s proof. The cyclotomic field \( \mathbb{Q}(\mu_1) \) is replaced by the group algebra \( KG \) with the group elements playing the role of the roots of unity. Abelian extensions of \( K \) with group isomorphic to \( G \) are described by a Kummer theory over \( KG \). The resolvents are replaced by “resolvends” which are elements of \( K^cG \) whose images under the characters of \( G \) are resolvents. (\( K^c \) is the algebraic closure of \( K \).) The Stickelberger condition arises from the shape of the prime factorization in \( \sigma G \) of the \( l \)th power of resolvends of elements generating local normal integral bases at the prime divisors of \( l \). The shape of this prime factorization is determined by the behavior of the resolvends under the Galois action of \( G \) and of \( C \). These ideas are developed in Sections 1, 2, and 4. Section 3 is devoted to describing the properties of the Stickelberger ideal. At the end of Section 4, we prove \( R(\sigma G) \subseteq \text{Cl}'(\sigma G)\mathcal{F} \). In Section 5 we prove \( R(\sigma G) \cong \text{Cl}'(\sigma G)\mathcal{F} \) (which is the essential inclusion for the corollary \( \text{Cl}(\mathbb{Z}G)\mathcal{F} = 1 \)). We choose a class in \( \text{Cl}'(\sigma G)\mathcal{F} \) and must construct an extension whose ring of integers realizes that class. At the analogous point in Hilbert’s proof, a prime \( p \) of degree one is chosen in an ideal class of \( \mathbb{Q}(\mu_1) \). Then \( N(p) = p \equiv 1 \) (mod \( l \)) and an extension \( L/\mathbb{Q} \) is produced inside the cyclotomic field \( \mathbb{Q}(\mu_p) \). In Section 5, the desired extension \( L/K \) is produced utilizing the Kummer theory developed in the earlier sections. A key tool is the fact that ray
classes contain infinitely many prime ideals of degree one, and this is the only "non-algebraic" fact which we use.

The theorem $R(\sigma G) = Cl'(\sigma G)^\alpha$ was obtained first in the special case where $G$ is cyclic of order $l$ and $K$ contains $\mu_l$, the $l$th roots of unity [8]. Childs [2] removed the hypothesis that $\mu_l \subseteq K$ and proved $R(\sigma G) \supseteq Cl'(\sigma G)^\alpha$, which sufficed to recover the classical $Cl(\mathbb{Z}[\mu_l])^\alpha = 1$.

My interest in the elementary abelian case was stimulated by reading a preliminary version of the thesis of Glass [5]. Glass considered elementary abelian $G$ of order $l^2$, $\mu_{l^2} \subseteq K$. She obtained a description of $R(\sigma G)$ based on Stickelberger-like elements in $\mathbb{Z}C_s$, where $C_s = \mathbb{F}_l^k \times \mathbb{F}_l^s$, a split Cartan subgroup of $GL_2(\mathbb{F}_l)$. That is, let $G = G_1 \times G_2$, where each $G_i$ is the additive group of $\mathbb{F}_l$. Then $C_s = C_1 \times C_2$, where $C_i = \mathbb{F}_l^k$. We denote, as before, the augmentation kernel of $Cl$ by $C_1$. The canonical map

$$Cl'(\sigma G) \to Cl'(\sigma G_1) \times Cl'(\sigma G_2)$$

is a split surjection preserving the action of $C_s$. Denote its kernel by $C_1''(\sigma G)$ so that

$$Cl'(\sigma G) = C_1''(\sigma G) \times R(\sigma G_1) \times R(\sigma G_2).$$

**Theorem (Glass).** Suppose $\mu_l \subseteq K$ and $G$ is as above. Then

$$R(\sigma G) = C_1''(\sigma G)^\alpha \times R(\sigma G_1) \times R(\sigma G_2),$$

where

$$\alpha = \sum_{\substack{i,j=1 \atop i+j \geq 1}}^{l-1} (\delta_i, \delta_j)^{-1} \in \mathbb{Z}C_s$$

(and $\delta_i \in \mathbb{F}_l^k$ is the residue class of $i$).

Note that under the canonical maps $\mathbb{Z}C_s \to \mathbb{Z}C_i$ (induced by the projections $C_s \to C_i$) the image of $\alpha$ is $\sum r\delta_r^{-1}$, the classical Stickelberger element. It would be of interest to find a unified approach to $R(\sigma G)$ which would simultaneously yield Glass's theorem and the main theorem of this article.

The results of this article have partial generalizations to the case where $G$ is abelian of homogeneous type $(l^n,...,l^n)$ with $k$ factors. The results of Sections 1, 2, and 3 are presented in this generality. The main theorem does not generalize as stated even in the case where $G$ is cyclic ($k = 1$). For cyclic $G$ of order $l^n$, $n > 1$, $Cl(\mathbb{Z}G)^\alpha \neq 1$, in general (see remarks at the end of [10]) whence $R(\sigma G) \not\subseteq Cl'(\sigma G)^\alpha$. Childs [3] has recently shown for cyclic $G$ that the opposite inclusion also fails in general. However, by extending the
methods of Sections 4 and 5 we can obtain the following: Let $G$ be of type $(I_1, \ldots, I_n)$ and let $\sigma A$ be the image of $\sigma G$ in the quotient algebra $A$ of $KG$ defined by the decomposition $KG = A \times K(G/H)$, where $H$ is the largest elementary abelian subgroup in $G$. (If $K = \mathbb{Q}$ and $G$ is cyclic, then $\sigma A = \mathbb{Z} \mid \mu_n \mid$.). Denote by $R(\sigma A)$ the image of $R(\sigma G)$ under the map $Cl(\sigma G) \to Cl(\sigma A)$. We can show that $R(\sigma A) \supseteq Cl(\sigma A)^\mathcal{F}$, where $\mathcal{F} = \mathcal{F}_{k,n}$ is an enlarged Stickelberger ideal defined in Section 3. In particular, of course, $Cl(\mathcal{F} A)^\mathcal{F} = 1$ and when $k = 1$ we can recover the classical $Cl(\mathcal{F} [\mu_n])^{\mathcal{F}} = 1$. These results will appear later, embedded, one hopes, in a more complete description of $R(\sigma G)$ for $n > 1$, $k > 1$.

It should be pointed out that Fröhlich [4] has shown that the Stickelberger relations for arbitrary cyclotomic extensions $\mathbb{Q}(\mu)/\mathbb{Q}$ can be derived from the fact that tame abelian extensions of $\mathbb{Q}$ have normal integral bases. His results have particularly influenced Section 4 of this article. In addition, he suggested an approach which has substantially simplified Section 5. Thanks are also due to many others, particularly to C. J. Bushnell for crucial and timely suggestions.

1. GALOIS $G$-EXTENSIONS AND RESOLVENDS

Let $G$ be a finite group and $K$ an algebraic number field. There is a natural correspondence between Galois extensions of $K$ with Galois group isomorphic to $G$ and (continuous) surjective homomorphisms $\text{Gal}(K^c/K) \to G$, where $K^c$ is the algebraic closure of $K$. Namely, to each such homomorphism, one associates the fixed field of its kernel. This correspondence is not biunique, however, since different homomorphisms may have the same kernel. We obtain a biunique correspondence through the notion of a Galois $G$-extension. To an arbitrary (continuous) homomorphism $\text{Gal}(K^c/K) \to G$ we associate a Galois $G$-extension of $K$, in the sense of [1], as follows: Let $\pi \in \text{Hom}(\Omega_K, G)$, where $\Omega_K = \text{Gal}(K^c/K)$. Let $K^\pi = (K^c)^{\text{ker } \pi}$, the subfield of $K^c$ fixed elementwise by the kernel of $\pi$. Then $K^\pi$ is a Galois extension of $K$ with Galois group $\Omega_K/\ker \pi$, isomorphic to a subgroup $\pi(\Omega_K)$ of $G$. To obtain a Galois $G$-extension, we (co)-induce (from $\Omega_K$) to $G$ by letting $K^\pi = \text{Map}_{\Omega_K}^\pi(G, K^c)$, the $K$-algebra of functions from $G$ to $K^c$ preserving the action of $\Omega_K$, where $G$ is regarded as an $\Omega_K$-set under left multiplication via $\pi$. Thus

$$v \in K^\pi \Leftrightarrow v(\pi(\sigma) \cdot s) = v(s)^\sigma, \quad \forall \sigma \in \Omega_K, s \in G.$$  

(1.1)

(Note that we will always regard Galois groups as acting on the left even though the action is written exponentially. Thus $\alpha^\sigma = (\alpha^\tau)^\sigma$ for $\alpha \in K^c$, $\sigma$, $\tau \in \Omega_K$.)

From (1.1), one sees immediately that

(a) the values of $v$ belong to $K^r$, so that $K_\pi = \text{Map}_{\Omega_K}(G, K^r)$, and
(b) $v$ is determined by its values on a set of coset representatives for $\pi(\Omega_K)G$.

The choice of such a set of coset representatives gives a representation of $K_\pi$ as a product of copies of $K^r$. If $\pi$ is surjective, $K_\pi \cong K^r$ under the map $v \mapsto v(1)$.

The elements of $G$ act as automorphisms of $K_\pi$ under the rule $v^G(t) = v(ts)$. (Again we have $(v^G)^t = v^G$.). One easily sees that the fixed points are the constant functions with values in $K$ (i.e., $K_\pi^c = K$) so $K_\pi$ is a Galois $G$-extension of $K$ in the sense of [1]. Moreover, one can show that the correspondence $\pi \mapsto K_\pi$ is biunique between $\text{Hom}(\Omega_K, G)$ and the set of isomorphism classes of Galois $G$-extension of $K$.

Notice that if $G$ is abelian, the set of Galois $G$-extensions of $K$ forms an abelian group through its natural identification with $\text{Hom}(\Omega_K, G)$. (This group was introduced by Harrison in a more general context.)

There is a natural correspondence $\text{Map}(G, K^c) \rightarrow K^cG$ given by

$$v \mapsto \tilde{v} = \sum_{s \in G} v(s) \cdot s^{-1}. \quad (1.2)$$

The image $\tilde{v}$ of $v$ will be called the resolvend of $v$. One easily checks that the resolvend map is a left $KG$-isomorphism:

$$v^s \mapsto v^G = s \cdot \tilde{v}, \quad \forall s \in G. \quad (1.3)$$

The map does not preserve the algebra structure—the multiplication in $K^cG$ would correspond to a convolution multiplication in the function algebra. The Galois group $\Omega_K$ acts (coefficientwise) as a group of $K$-algebra automorphisms of $K^cG$ which also preserve left or right multiplication by elements of $G$. Clearly

$$(K^cG)^{\Omega_K} = KG.$$

(If $G$ is abelian, $K^cG$ is an (infinite) Galois extension of $KG$ in an appropriate sense.)

If $\pi \in \text{Hom}(\Omega_K, G)$, then $K_\pi \subseteq \text{Map}(G, K^c)$ and its image $\tilde{K}_\pi$ under the resolvend map is easily seen to be characterized by

$$\alpha \in \tilde{K}_\pi \iff \alpha \in K^cG \quad \text{and} \quad \alpha^\tau = \alpha \cdot \pi(\tau), \quad \tau \in \Omega_K. \quad (1.4)$$

Moreover, if $v$ is a normal basis generator of $K_\pi$ over $K$, then $\tilde{K}_\pi$ is a rank-one free $KG$-module generated by $\tilde{v}$. Indeed,

$$K_\pi = KG \cdot v \iff \tilde{K}_\pi = KG \cdot \tilde{v}.$$
(1.5) **Proposition.** Let \( \pi \in \text{Hom}(\Omega_K, G) \) and \( v \in K_\pi \). Then \( K_\pi = KG \cdot v \iff \tilde{v} \in (K^c G)^{\times} \). (Here \( R^{\times} \) denotes the group of units of a ring \( R \).)

**Proof.** If \( \tilde{v} \in (K^c G)^{\times} \), then the map \( \alpha \mapsto \alpha \cdot \tilde{v} \) is injective \( KG \to \tilde{K}_\pi \). Hence it is surjective and \( \tilde{K}_\pi = KG \cdot \tilde{v} \), so \( K_\pi = KG \cdot v \).

The converse is a little harder. If \( v \) generates a normal basis \( \{ v^s \mid s \in G \} \) of \( K_\pi \) over \( K \), then the dual basis with respect to the trace is also a normal basis. For, if \( \text{Tr}(v^su) = \delta_{s,1} \), then \( \text{Tr}(v^st) = \text{Tr}((v^s)^{-1}u) = \delta_{s,t} \). We will show directly that

\[
\tilde{v}^{-1} = \sum_{t \in G} u(t) \cdot t.
\]

To verify this, it is useful to observe first that, as an element of \( K \),

\[
\text{Tr} v = \sum_{s \in G} v^s(1) = \sum_{s \in G} v(s)
\]

for \( v \in K_\pi \). Also notice that \( \sum_{t \in G} u(t)t \) is the image of \( \tilde{u} \) under the canonical involution of \( K^c G \) defined by sending each group element to its inverse, \( t \mapsto t^{-1} \). If we denote this involution by \([ -1]\), we have \( \tilde{u}^{-1} = \sum_{t \in G} u(t)t \) and the assertion to be proved is

\[
\tilde{v} \cdot \tilde{u}^{-1} = 1.
\]

(Since \( K^c G \) is a finite dimensional \( K^c \) algebra, it suffices to show that \( \tilde{v} \) has a right inverse.)

The above assertion follows from a more general result which we record for future use:

\[
\tilde{v} \tilde{u}^{-1} = \sum_{t \in G} \text{Tr}(vu') \cdot t, \quad \forall u, v \in K_\pi .
\]

(1.6)

To show this, we calculate

\[
\tilde{v} \tilde{u}^{-1} = \sum_{s, t} v(s) u(t) s^{-1} t = \sum_{s, t} v(s) u(ss^{-1} t) s^{-1} t
\]

\[
= \sum_{s, t} v(s) u(st)t = \sum_{s} \sum_{t} v(s) u'(s)t.
\]

**Remark.** \( K_\pi \) always has a normal basis over \( K \). For if \( a \in K_\pi^{\times} \) generates a normal basis of \( K_\pi^{\times}/K \), then \( v \in K_\pi \) defined by

\[
v(s) = a^s \quad \text{if} \quad s = \pi(\sigma)
\]

\[
= 0 \quad \text{if} \quad s \notin \pi(\Omega_K)
\]

generates a normal basis of \( K_\pi/K \).
Henceforth we will assume $G$ is abelian. Then the multiplicative group $(K^cG)^\times$ is a discrete $\Omega_K$-module. We shall characterize the invertible resolvends of elements of Galois $G$-extensions of $K$ in terms of the $\Omega_K$ action on $(K^cG)^\times$. Let

$$H(KG) = \{ a \in (K^cG)^\times \mid a^\sigma - 1 \in G, \forall \sigma \in \Omega_K \}. \quad (1.7)$$

Then $H(KG)$ is a subgroup of $(K^cG)^\times$ containing $(KG)^\times$.

\begin{enumerate}
\item[(1.8)] \textbf{Proposition.} (a) If $a \in H(KG)$, the map $\pi_a : \Omega_K \to G$ given by $\pi_a(\sigma) = a^\sigma - 1$ is a group homomorphism.
\item[(b)] The map $\alpha \mapsto \pi_\alpha$ gives rise to an exact sequence

$$1 \to (KG)^\times \to H(KG) \to \text{Hom}(\Omega_K, G) \to 1.$$

(c) $H(KG) = (K^cG)^\times \cap \bigcup_{\pi}(K_{\pi})$,

where the union is over all $\pi \in \text{Hom}(\Omega_K, G)$.
\end{enumerate}

\textbf{Proof}: Parts (a) and (b) follow from elementary cohomological considerations. Consider the exact sequence of $\Omega_K$-modules:

$$1 \to G \to (K^cG)^\times \to ((K^cG)^\times/G)^{\Omega_K} \to \text{Hom}(\Omega_K, G) \to 1.$$

The associated long exact sequence begins (since $\Omega_K$ acts trivially on $G$):

$$1 \to G \to (K^cG)^\times \to ((K^cG)^\times/G)^{\Omega_K} \to \text{Hom}(\Omega_K, G).$$

Clearly $((K^cG)^\times/G)^{\Omega_K} = H(KG)/G$ by (1.7), and the connecting homomorphism is, in effect, $a \mapsto \pi_a$. Hence we have exactness of

$$1 \to (KG)^\times/G \to H(KG)/G \to \text{Hom}(\Omega_K, G).$$

Exactness on the right could be shown by observing (in a variety of ways) that Hilbert's Theorem 90 applies to the Galois extension $K^cG$ of $KG$. Instead, we simultaneously prove (c) by observing that under the map $H(KG) \to \text{Hom}(\Omega_K, G)$, the pre-image of $\pi$ is $(K^cG)^\times \cap K_{\pi}$ (by (1.4)) and that $(K^cG)^\times \cap K_{\pi} \neq \emptyset$ (by Proposition (1.5)).

Proposition 1.8 can be interpreted as indicating a sort of Kummer theory for Galois $G$-extensions of $K$ in which the elements of $G$ in the group algebra $KG$ play the role of the roots of unity. It also gives a characterization of the (invertible) resolvends in terms of the action of $\Omega_K$ on $(K^cG)^\times$. We will now derive from this $\Omega_K$-characterization a more powerful characterization in terms of the action on $(K^cG)^\times$ of endomorphisms of $G$.

Let $E$ be a ring of endomorphisms of $G$ containing the identity. ($E$ may, but need not, be the full ring $\text{End}(G)$.) We write the action of $E$ exponen-
tially, continuing the convention that \((s^\eta)^n = s^{n\eta}\) for \(s \in G\), \(\eta, \rho \in E\). As usual, we denote by \(E^\times\) the group of units of \(E\). It will also be necessary to consider the full multiplicative monoid (including zero) of \(E\), which we will denote by \(E\).

If \(\rho \in E\), \(\rho\) extends by linearity to an algebra endomorphism of \(KcG\) (preserving the identity) and hence also to a group endomorphism of \((KcG)^\times\). In this way, \(E\) acts as a monoid (but not as a ring) of endomorphisms of \((KcG)^\times\). That is, \((a^\eta)^n = a^{n\eta}\) for \(a \in KcG\), \(\eta, \rho \in E\), but in general \(a^{\eta + \rho} \neq a^{\eta} a^\rho\). Since \(E\) acts on elements of \(G\) while \(\Omega_k\) acts on coefficients, the two actions commute:

\[
\text{For } \beta \in (KcG)^\times, \quad (\beta^\eta)^n = (\beta^n)^\eta \quad \text{if } \sigma \in \Omega_k, \rho \in E^\times. \tag{1.9}
\]

Now any abelian group on which \(E\) acts as a monoid of endomorphisms is, in a natural way, a module over the monoid ring \(\mathbb{Z}E^\times\). (Note that the “monoid ring” is left-adjoint to the forgetful functor from rings with identity to monoids, \(R \mapsto R^\times\).) When necessary to avoid confusion, we will enclose elements of \(E^\times\) in brackets when writing elements of \(\mathbb{Z}E^\times\), as in \(\sum_{\rho \in E} a_\rho [\rho]\).

In particular, \([0] \neq 0\) in \(\mathbb{Z}E^\times\) whereas, by definition, \([1] = 1\). In fact, \([0]\) is the augmentation map \(KcG \to Kc\). \(1 \in KcG\):

\[
\left(\sum_{s \in G} a_s \cdot s\right)^{[0]} = \sum_{s \in G} a_s \cdot s^{[0]} = \sum_{s \in G} a_s \cdot 1.
\]

Likewise, \([{-1}]\) is the canonical involution of \(KcG\) described previously. Now, \(E\) acts as a ring of endomorphisms of the dual group \(G^* = \text{Hom}(G, (Kc)^\times)\) by the rule \(\chi^\rho(s) = \chi(s^\rho)\) for \(\chi \in G^*, s \in G, \rho \in E\).

But, whereas \(G\) was a left \(E\)-module, \(G^*\) is a right \(E\)-module: \((\alpha^\eta)^a = \alpha^{a^\eta}\). The characterization of resolvends which we will obtain will be in terms of the kernel \(\mathcal{A}\) of the canonical (adjunction) homomorphism \(\mathbb{Z}E^\times \to E\). Since \(E\) acts (by definition) faithfully on \(G\), we clearly have \(\mathcal{A} = \text{Ann}_{\mathbb{Z}E^\times} G\), the annihilator of \(G\) as a \(\mathbb{Z}E^\times\)-module. Likewise, \(G^*\) is a faithful right \(E\)-module and so \(\mathcal{A} = \text{Ann}_{\mathbb{Z}E^\times} G^*\). Note that \(\mathcal{A}\) contains elements such as \([\rho] + [\eta] - [\rho + \eta]\) for \(\rho, \eta \in E\) and \(r - [r]\) for \(r \in \mathbb{Z}\).

(1.10) **Theorem.** Suppose \(G^*\) is a cyclic \(E\)-module. Let \(\beta \in (KcG)^\times\).

Then

(a) \(\beta \in G \iff \beta^\eta = 1, \forall \alpha \in \mathcal{A}\) and

(b) \(\beta \in H(KcG) \iff \beta^\eta \in (KcG)^\times, \forall \alpha \in \mathcal{A}\).

Remark. It is easy to see that \(G\) and \(G^*\) are cyclic over \(\text{End} G\). This is obvious if \(G\) is cyclic, and it is also clear that a product of cyclic groups is cyclic over the product of their endomorphism rings. So, in fact, one can
always find a commutative ring $E$ of endomorphisms of $G$ such that $G$ and $G^*$ are cyclic over $E$. One can find, however, cases where $G$ is cyclic over $E$ but $G^*$ is not (and vice versa).

Proof of (1.10). (a) Here, "⇒" is trivial. To show the converse, consider the map $G^* \rightarrow (K^e)^{\times}$ given by $\chi \mapsto \chi(\beta)$, where $\chi$ is extended by linearity from $G$ to $K^eG$. It suffices to show that this map is a homomorphism. For then, since $G^{**} = G$, there is an $s \in G$ such that this homomorphism is the same as $\chi \mapsto \chi(s)$. But $\chi(\beta) = \chi(s)$ for all $\chi \in G^*$ implies that $\beta = s \in G$. Now, let $\chi$ generate $G^*$ over $E$. It suffices to show, for any $\gamma, \rho \in E$ that $(\chi\gamma^\rho)(\beta) = \chi(\beta) \gamma^\rho(\beta)$. Contrary to appearances, this is not obvious, or we would have proved $(K^eG)^{\times} = G$. Here is the argument (note that $(K^eG)^{\times}$ is not an $E$-module, but only a $\mathbb{Z}E^*$-module):

$$(\chi\gamma^\rho)(\beta) = \chi(\gamma^\rho)(\beta) = \chi(\beta^{\gamma^\rho}).$$

Now in $\mathbb{Z}E^*$, $[\gamma + \rho] = [\gamma] + [\rho]$ (mod $\mathfrak{m}$), and $\beta^{\mathfrak{m}} = 1$ so

$$\chi(\beta^{\gamma^\rho}) = \chi(\beta^{[\gamma^{\rho}]} = \chi(\beta^{\gamma}) \chi(\beta^{\rho})$$

(b) Let $\beta \in (K^eG)^{\times}$ and recall that by (1.9) the actions of $\Omega_K$ and $\mathbb{Z}E^*$ commute on $\beta$. Starting from definition (1.7):

$$\beta \in H(KG) \iff \beta^{-1} \in G, \forall \sigma \in \Omega_K \iff (\beta^{-1})^\sigma = 1, \forall \sigma \in \Omega_K, \alpha \in A$$

$$\iff (\beta^\sigma) = \beta^\alpha, \forall \sigma \in \Omega_K, \alpha \in A \iff \beta^\alpha \in (KG)^{\times}, \forall \alpha \in A.$$

Throughout this section we have been considering the set of all Galois $G$-extensions of $K$. However, in the following sections, we shall consider only tame Galois $G$-extensions. If we replace $K^e$ by $K^t$, the maximal tame (at most tamely ramified) extension of $K$ in $K^e$ and $\Omega_K$ by $\Omega_K^t = \text{Gal}(K^t/K)$, the results of this section carry over with appropriate modifications. In particular, the set of tame Galois $G$-extensions is identified with $\text{Hom}(\Omega_K^t, G)$ and the exact sequence of (1.8)(b) becomes

$$1 \rightarrow (KG)^{\times} \rightarrow H^t(KG) \rightarrow \text{Hom}(\Omega_K^t, G) \rightarrow 1,$$

where

$$H^t(KG) = H(KG) \cap (K^tG)^{\times}$$

and is characterized as the set of invertible resolvends of elements in tame Galois $G$-extensions. The criteria of Theorem (1.10) carry over when the indicated substitutions are made, the only deviation from the rule being that $G^*$ must continue to be the full dual group $\text{Hom}(G, (K^e)^{\times})$. We shall use the
abbreviated expression “tame $G$-extension” instead of “tame Galois $G$-
extension.” We shall also regard $\text{Hom}(\Omega^t_K, G)$ as a subgroup of $\text{Hom}(\Omega^G_K, G)$
and say $\pi$ is tame if $\pi \in \text{Hom}(\Omega^t_K, G)$.

2. THE GALOIS MODULE CLASS OF A TAME $G$-EXTENSION

Henceforth we shall assume $G$ is an abelian group of exponent $l^n$, where $l$
is a prime.

The ring of integers $\mathcal{O}_m$ in a Galois $G$-extension $K_m/K$ can be identified
with $\text{Map}_{K_m}(G, \mathcal{O}^c) = \text{Map}_{\Omega_K}(G, \mathcal{O}^\pi)$, where $\mathcal{O}^c$
is the ring of integers in $K^c$
and $\mathcal{O}^\pi = \mathcal{O}^c \cap K^\pi$. The extension $K_m/K$ is tame, if and only if $\mathcal{O}_m$ is a rank
one locally free $\mathcal{O}G$ module, where $\mathcal{O} = \mathcal{O}_K$, the ring of integers in $K$ (see
(2.6) below). As such, its structure is determined up to $\mathcal{O}G$-isomorphism by
its class $\text{cl}(\mathcal{O}_m)$ in the class group $\text{Cl}(\mathcal{O}G)$. Since $G$ is abelian, we may
describe $\text{Cl}(\mathcal{O}G)$ simply as the quotient of the group $I(\mathcal{O}G)$ of invertible
(fractional) $\mathcal{O}G$-ideals in $KG$ by the subgroup of invertible principal
ideals—that is, ideals of form $(\beta) = \mathcal{O}G \cdot \beta$, where $\beta \in KG^\times$. We denote this
subgroup simply by $(KG^\times)$. The class of a rank one locally free $\mathcal{O}G$-module
$M$ is then defined as follows:

Choose $m \in KM$ with $KM = KGm$ (where $M \subseteq KM = K \otimes_{\mathcal{O}} M$). Then
$M = mm$, where $m \in I(\mathcal{O}G)$. Since the choice of $m$ is unique up to
multiplication by elements of $KG^\times$, $m$ is unique up to multiplication by
elements of $(KG^\times)$. We define the class $\text{cl}(M)$ of $M$ to be the ideal class of $m$
in $I(\mathcal{O}G)/(KG^\times)$.

For computational purposes, we find it more convenient to use a different
description of the class group which we will describe for an arbitrary $\mathcal{O}$-
order $\Lambda$ in a commutative semi-simple $K$-algebra $A$. Let $\mathcal{M}$ be the maximal
$\mathcal{O}$-order of $A$, and let $f \in \mathcal{O}$, $f \neq 0$, such that $f, \mathcal{M} \subseteq \Lambda$. For any prime ideal $p$
of $\mathcal{O}$ let $v_p$ denote the corresponding normalized additive valuation of $K$. Now $\mathcal{O}$ is the intersection of two overrings of $\mathcal{O}$ in $K$:

$$\mathcal{O} = \mathcal{O}_f \cap \mathcal{O}', \quad (2.1)$$

where

$$\mathcal{O}' = \mathcal{O}[f^{-1}]$$

$$= \{ a \in K \mid v_p(a) \geq 0 \text{ if } p \nmid f \}$$

and

$$\mathcal{O}_f = \text{(semi)-localization of } \mathcal{O} \text{ at the prime divisors of } f$$

$$= \{ a \in K \mid v_p(a) \geq 0 \text{ if } p \mid f \}. $$
The group \( I(\sigma') \) of fractional \( \sigma' \)-ideals can be identified with the group of \( \sigma \)-ideals relatively prime to \( f \). The units \( \sigma_f^\times \) generate the principal \( \sigma \)-ideals which are relatively prime to \( f \). It is standard number theory that

\[
\mathcal{C}l(\sigma) \cong I(\sigma')/(\sigma_f^\times).
\]

Jacobinski's ideal-theoretic definition of class groups of genera is analogous to this formula and in our special case it amounts to

\[
\mathcal{C}l(A) \cong I(A')/(A_f^\times),
\]

where

\[
A' = \sigma' A = \sigma' A_f^\times
\]

and

\[
A_f = \sigma_f A.
\]

We shall explain this expression in more detail. Since \( A' \) is the maximal \( \sigma' \)-order in \( A \), the group \( I(A') \) of invertible (fractional) \( A' \)-ideals in \( A \) is a product of ideal groups of Dedekind domains—specifically of the integral closures of \( \sigma' \) in the components of \( A \). The subgroup \( (A_f^\times) \) of \( I(A') \) consists of those principal \( A' \)-ideals \( (\beta) = \beta \cdot A' \) generated by elements \( \beta \in A_f^\times \). In this notation, the description of the class \( \mathcal{C}l(M) \) associated to a rank-one, locally free \( A \)-module \( M \) is slightly different. Since \( A_f \) is semi-local \( M_f = \sigma_f M \) is a rank-one free \( A_f \)-module. Choose a generator \( m \):

\[
M_f = A_f \cdot m.
\]

Now \( M' = \sigma' M \) is locally free rank one over \( \sigma' G \) so

\[
M' = m \cdot m \quad \text{for a unique } m \in I(A').
\]

Since \( m \) is unique up to multiplication by a unit in \( A_f^\times \), \( m \) is unique up multiplication by a principal \( A' \)-ideal in \( (A_f^\times) \). Thus the ideal class of \( m \) in \( I(A')/(A_f^\times) \) is uniquely determined by \( M \). It is the class \( \mathcal{C}l(M) \) in \( \mathcal{C}l(A) \). Conversely if \( m \in I(A') \) then it can be shown that \( m \cap A_f \subseteq I(A) \) and is a locally free, rank one \( A \)-module whose class is the ideal class of \( m \) in \( I(A')/(A_f^\times) \).

It is useful to observe also that \( A_f^\times \) contains the subgroup \( 1 + f \cdot A_f^\times \). (One easily sees that \( 1 + f \cdot A_f^\times \subseteq A_f^\times \) since \( f \cdot A_f^\times \) is contained in the radical of \( A_f^\times \). It is also a standard fact about orders that \( A_f^\times \cap A_f = A_f^\times \).) Now, \( 1 + f \cdot A_f \) is the subgroup of \( K^\times \) traditionally called the "numerical ray (mod \( f \)) of \( K' \)" and one sees easily that \( I(\sigma')/(1 + f \sigma_f) \) is the ray class group (mod \( f \)) of \( K \). Since \( A_f^\times \) is the maximal \( \sigma_f \)-order of \( A \), \( 1 + f \cdot A_f^\times \) is the product of the
numerical rays (mod f) of the components of A. Thus the class group \( \mathcal{O}(A) \) is a quotient of \( I(A')/(1 + fM) \) which in turn is the product of the ray class groups (mod f) of the components of A.

We return now to the case \( A = \mathfrak{D}G \) and \( M = \mathcal{O}_n \) for \( \pi \in \text{Hom}(\Omega^l \mathfrak{D}, G) \). In this case, we take \( f = |G| = a \) power of \( l \). Then \( \mathfrak{D}_j = \mathfrak{D}_j \), and

\[
\mathcal{O}_{\pi l} = \mathfrak{D}_j G v \quad \text{for some} \quad v \in \mathfrak{D}_{\pi l},
\]

and

\[
\mathcal{O}_{\pi} = \mathfrak{D}_j G v \quad \text{for some} \quad m \in I(\mathfrak{D}^G)
\]

and

\[
\mathcal{O}(\mathfrak{D}_{\pi}) = \text{ideal class of } m \text{ in } I(\mathfrak{D}^G)/(\mathfrak{D}_j G^x).
\]

If \( \mathfrak{D}_{\pi l} = \mathfrak{D}_j G \cdot v \) we shall say that \( v \) is an \( l \)-local normal basis generator of \( K/\mathbb{Q} \). In the next proposition we characterize such elements and show directly that \( K/\mathbb{Q} \) is tame if and only if such a generator \( v \) exists.

(2.6) **Proposition.** Let \( \pi \in \text{Hom}(\Omega_K \mathfrak{D}, G) \). Then \( \pi \) is tame if and only if there is a \( v \in K_\pi \) satisfying one of the following equivalent conditions:

1. \( \mathfrak{D}_{\pi l} = \mathfrak{D}_j G \cdot v \),
2. \( v \in \mathfrak{D}_{\pi l} \) and \( \text{Tr} v \in \mathfrak{D}_j \),
3. \( \tilde{v} \in \mathfrak{D}_j^G \).

**Proof.** Since \( G \) is an \( l \)-group, the only possible wild ramification is at prime divisors of \( l \). The traditional criterion for \( \mathfrak{D}_j \) to be tame over \( \mathfrak{D}_j \) becomes \( \text{Tr}(\mathfrak{D}_{\pi l}) = \mathfrak{D}_j \) which is clearly equivalent to the existence of a \( v \in K_\pi \) satisfying (b). (The transition from field extensions to Galois \( G \)-extensions presents no difficulties, since for \( K/\mathbb{Q} \) to be tame merely means \( K^G/\mathbb{Q} \) is tame.) Thus it suffices to show the equivalence of (a), (b), and (c):

(a) \( \Rightarrow \) (b) is trivial: \( 1 = \sum_{s \in G} a_s v^s = a \cdot \sum_{s \in G} v^s. \)

(b) \( \Rightarrow \) (c): Since \( v \in \mathfrak{D}_{\pi l}, \) \( \tilde{v} \in \mathfrak{D}_j^G \), where \( \mathfrak{D}_j^G = \mathfrak{D}_j \cap K_\pi. \) Since \( G \) is an \( l \)-group and \( l \in \text{Rad} \mathfrak{D}_j^G \), then \( s - 1 \in \text{Rad} \mathfrak{D}_j^G \) for all \( s \in G \). Hence

\[
\tilde{v} = \sum_{s \in G} v(s) \cdot s^{-1} = \text{Tr} v \quad (\text{mod } \text{Rad} \mathfrak{D}_j^G). \]

Since \( \text{Tr} v \in \mathfrak{D}_j \subseteq \mathfrak{D}_j^G \), \( \tilde{v} \in \mathfrak{D}_j^G \subseteq \mathfrak{D}_j^G \).

(c) \( \Rightarrow \) (a): \( v \in K^G \) implies \( K^G = KG \cdot v \) by (1.5). Moreover, as shown in the proof of (1.5), \( \tilde{u}^{-1} = u \tilde{u}^{-1} \), where \( u \) generates the normal basis of \( K/\mathbb{Q} \) dual to that generated by \( v \). Since \( \tilde{v} \in \mathfrak{D}_j^G \), we have \( v \in \mathfrak{D}_{\pi l} \) so

\[
\mathfrak{D}_j G \cdot v \subseteq \mathfrak{D}_{\pi l} \subseteq \mathfrak{D}_{\pi l} \subseteq (\mathfrak{D}_j G v)^* = \mathfrak{D}_j G \cdot u.
\]

But \( \tilde{v} \in \mathfrak{D}_j^G \) implies \( \tilde{u} \in \mathfrak{D}_j^G \) so \( u \in \mathfrak{D}_{\pi l} \). Hence, easily,

\[
\mathfrak{D}_j G \cdot v = \mathfrak{D}_{\pi l} = \mathfrak{D}_{\pi l} = \mathfrak{D}_j G \cdot u.
\]
(2.7) Corollary. Let

\[ H(\sigma, G) = \mathcal{O}_l^G \cap H(KG) \]

and

\[ H(\sigma', G) = \mathcal{O}_l^G \cap H(KG) \quad (\text{where } \mathcal{O}_l^G = \mathcal{O}_l^C \cap K^l). \]

Then \( H(\sigma, G) = H(\sigma', G) \) and consists of the resolvends of \( l \)-local normal basis generators of tame \( G \)-extensions of \( K \).

Proof. This is immediate from (1.8)(c) and (2.6).

Now returning to (2.5) we see, upon taking resolvends, that

\[ \tilde{\mathcal{E}}^l_n = m \tilde{v} \quad \text{and} \quad \tilde{v} \in H(\sigma, G). \quad (2.8) \]

In order to investigate the behavior of the ideal class of \( m \) under the action of endomorphisms of \( G \), we shall regard \( \mathcal{E} \) as an element of a group \( I'(\sigma', G) \) on which the multiplicative monoid of endomorphisms of \( G \) will act.

Let

\[ I'(\sigma', G) = \{ a \cdot \beta \mid a \in I(\sigma', G), \beta \in K^l \}. \quad (2.9) \]

Then \( I'(\sigma', G) \) is a multiplicative group whose elements are the rank one, locally free \( \sigma', G \) modules in \( K^lG \) which contain units of \( K^lG \). If \( \rho \in \text{End } G \), then \( \rho \) induces an endomorphism (denoted \( [\rho] \)) of each of \( K^lG \), \( I(\sigma', G) \) and \( I'(\sigma', G) \). (For example, if \( a \in I(\sigma', G) \), then \( a^{[\rho]} \) is the \( \sigma', G \) ideal generated by the image of \( a \) under the endomorphism of the \( K \)-algebra \( KG \) induced by \( \rho \).) Thus, as in Section 1, these groups are \( \mathbb{Z} [\text{(End } G') \} \)-modules. Moreover

(2.11) Proposition. Let \( E = \text{End } G \). Then \( \tilde{E}^l_\alpha \in I(\sigma', G) \) for all \( \alpha \in \text{Ann}_{\mathcal{E}} G \).

Proof. As in (2.8), \( \tilde{E}^l_\alpha = m \cdot \tilde{v} \in I'(\sigma', G) \) with \( m \in I(\sigma', G), \tilde{v} \in H(KG) \). Clearly \( \tilde{E}^l_\alpha = m^\alpha \cdot \tilde{v}^\alpha \) for \( \alpha \in \mathcal{E} \). But, \( \tilde{v}^\alpha \in K^lG \) by (1.10)(b) for \( \alpha \in \text{Ann}_{\mathcal{E}} G \), whence \( m^\alpha \cdot \tilde{v}^\alpha \in I(\sigma', G) \).

The main result of this section is the following. (Recall that \( G \) is abelian of exponent \( l^n \).)

(2.12) Theorem. Let \( E = \text{End } G \) and \( \mathcal{E}_{x,l} = \sigma_1 G \cdot v \). Then

(a) \( \tilde{v}^\alpha \in \sigma_1 G \) for all \( \alpha \in \text{Ann}_{\mathcal{E}} G \).

(b) Let \( w = \tilde{v}^\alpha \). Then \( w \in \sigma_1 G \) and \( \mathcal{E}(\sigma_\alpha) \) in \( \mathcal{E}(\sigma G) \) is represented by the (unique) ideal \( m \in I(\sigma G) \) such that \( m^\alpha(w) \) is integral and \( l^n \)-power free (in \( I(\sigma G) \)).
Note. Since \( \mathfrak{a}'G \) is a product of Dedekind domains, ideals in \( I(\mathfrak{a}'G) \) factor uniquely into products of (invertible) prime ideals in an obvious way and so the notion of "integral and \( l^n \)-power free" makes sense.

Proof. Observe that \( \mathfrak{d} \in H(\mathfrak{a},G) = \mathfrak{c}_n^i G^\times \cap H(KG) \) by (2.7). Hence, by (1.10)(b), \( \mathfrak{d} \subseteq \mathfrak{c}_n^i G^\times \cap KG^\times = \mathfrak{a}_i G^\times \) for all \( \alpha \subseteq \text{Ann}_{\mathcal{E}_E} G \), which shows (a). Now \( l^n \in \text{Ann}_{\mathcal{E}_E} G \), so \( v^n = w \in \mathfrak{a}_i G^\times \). From (2.8) we have

\[
m^{ln}(w) = (\mathfrak{c}_n^i)^{ln} \in I(\mathfrak{a}'G),
\]

where \( m \in I(\mathfrak{a}'G) \) represents \( cl(\mathfrak{a}_n^i) \) in \( \mathfrak{c}_n(\mathfrak{a}G) \). So, it suffices to show that \( (\mathfrak{c}_n^i)^{ln} \) is integral and \( l^n \)-power free (in \( I(\mathfrak{a}'G) \)). Clearly \( \mathfrak{c}_n^i \subseteq \mathfrak{c}_n^\times G \) so \( (\mathfrak{c}_n^i)^{ln} \subseteq \mathfrak{a}'G \) and is, thus, integral. If \( b^n \) divides \( (\mathfrak{c}_n^i)^{ln} \), where \( b \) is integral in \( I(\mathfrak{a}'G) \), then \( b^{-1}\mathfrak{c}_n^i \subseteq \mathfrak{a}'G \) (the integral closure of \( \mathfrak{a}'G \) in \( KG \)). But \( b^{-1}\mathfrak{c}_n^i \subseteq \mathfrak{K}_n \) so \( b^{-1}\mathfrak{c}_n^i \subseteq \mathfrak{c}_n^\times G \cap \mathfrak{K}_n = \mathfrak{c}_n^i \) (clearly). Thus \( b^{-1} \subseteq \mathfrak{a}'G \), the left order of \( \mathfrak{c}_n^i \). Hence \( b = b^{-1} \mathfrak{a}'G \) and the theorem follows.

Finally we point out the connection between resolvends and (tame) discriminants:

\[
(2.13) \text{PROPOSITION.} \quad \text{Let } b(\mathfrak{c}_n^i/\mathfrak{a}') \text{ denote the relative discriminant of } \mathfrak{c}_n^i/\mathfrak{a}'. \text{ Then}

\[
\mathfrak{c}_n^i, \mathfrak{c}_n^i[-1] \subseteq I(\mathfrak{a}'G)
\]

and

\[
[\mathfrak{a}'G : \mathfrak{c}_n^i, \mathfrak{c}_n^i[-1], \mathfrak{a}'] = b(\mathfrak{c}_n^i/\mathfrak{a}'),
\]

(where \( |A : B|_{\mathfrak{a}'} \in I(\mathfrak{a}') \) denotes the \( \mathfrak{a}' \)-module index of \( B \) in \( A \)).

Proof. Since \( 1 + [-1] \in \text{Ann}_{\mathcal{E}_E} G \), the first assertion follows from (2.11). The second assertion can be proved locally. Let \( p \) be a prime of \( \mathfrak{a} \), not dividing \( l \). Then \( \mathfrak{a}' \subseteq \mathfrak{a}_p \). Since \( \mathfrak{c}_n^i \) is locally free, we may choose \( v_p \in K_\pi \) with \( \mathfrak{a}_p G \cdot v_p = \mathfrak{c}_n^i, p \). Then

\[
\mathfrak{c}_n^i, \mathfrak{c}_n^i[-1] = \mathfrak{a}_p G \cdot \mathfrak{c}_n^i, p = \mathfrak{c}_n^i, p[-1].
\]

But, by (1.6),

\[
\bar{v}_p \mathfrak{c}_n^i[-1] = \sum_{i \in G} \text{Tr}(v_p v_p^i) \cdot t \in \mathfrak{a}_p G,
\]

so by a standard computation,

\[
[\mathfrak{a}_p G : \mathfrak{a}_p G \cdot \bar{v}_p \mathfrak{c}_n^i[-1], \mathfrak{a}_p] = b(\mathfrak{c}_n^i, \mathfrak{a}_p).
\]
Hence

\[ \left[ \mathcal{O}' : \mathcal{O} \mathcal{O}' / \mathcal{O}' \right] = \mathfrak{d}(\mathcal{O}' / \mathcal{O}) \]

In Section 4 we will obtain a decomposition of the integral $l$-power free part of $(\omega)$ in terms of a Stickelberger element for the special case that $G$ is elementary abelian. In Section 3, Stickelberger elements are described for a somewhat more general situation.

3. The Stickelberger Ideal

In this section, we specialize $G$ further to be an abelian group of type $(l^n, l^n, ..., l^n)$ with $k$ factors. We can regard $G$ as the additive group of a certain residue class ring. Specifically, let $R_k$ be the ring of integers in the (unique) unramified extension of degree $k$ of $\mathbb{Q}_l$, the field of $l$-adic numbers. Let

\[ E = E_{k,n} = R_k / l^n. \tag{3.1} \]

We let $G = G_{k,n}$ be a multiplicative group isomorphic to the additive group of $E$. We can regard $G$ as the additive group of a certain residue class ring. Specifically, let $R_k$ be the ring of integers in the (unique) unramified extension of degree $k$ of $\mathbb{Q}_l$, the field of $l$-adic numbers. Let

\[ E = E_{k,n} = R_k / l^n. \tag{3.1} \]

We let $G = G_{k,n}$ be a multiplicative group isomorphic to the additive group of $E$. We will write the elements of $G$ as $\{x^\rho \mid \rho \in E\}$ so that the isomorphism $E \rightarrow G$ is given by $\rho \mapsto x^\rho$. Thus $x^{\rho_1 + \rho_2} = x^{\rho_1}x^{\rho_2}$ for $\rho_1, \rho_2 \in E$. We also regard $E$ as a ring of endomorphisms of $G$ by putting

\[ (x^\rho x^\sigma) x^\rho = x^{\rho x^\sigma}. \]

Clearly $G$ is cyclic over $E$.

The unit group $E^\times$ is a group of automorphisms of $G$ and we put

\[ C = C_{k,n} = E_{k,n}^\times. \tag{3.2} \]

Then $G$ is a $\mathbb{Z}C$-module, generated by $x = x^1$. The Stickelberger ideals will be ideals in the group ring $\mathbb{Z}C$.

Let $\text{Tr} = \text{Tr}_k : R_k \rightarrow \mathbb{Z}_l$ denote the trace map. We use the same symbol to denote the trace map (mod $l^n$):

\[ \text{Tr} = \text{Tr}_k : R_{k,n} \rightarrow \mathbb{Z}_l / l^n. \tag{3.3} \]

Since $R_k$ is unramified over $\mathbb{Z}_l$, it is self-dual with respect to the trace. Likewise $E = E_{k,n}$ is self-dual with respect to the trace. From this, one easily sees that the dual group $G^*$ is cyclic over $E$. Fixing a $\mathbb{Z}/l^n$-basis $\delta_1 = 1, \delta_2, ..., \delta_k$, of $E$, we denote the associated dual basis by $\delta_1^*, \delta_2^*, ..., \delta_k^*$. Then $\text{Tr}(\delta_i \delta_j)$ is the Kronecker $\delta_{ij}$. Note that the $\delta_i$ and $\delta_i^*$ all have precise order $l^n$ in $E$ and hence belong to the unit group $C$. 

GALOIS MODULE STRUCTURE
To define the Stickelberger elements we shall need the canonical section map

\[ t_1 = t_{1,n} : \mathbb{Z}/l^n \to [0, l^n) \cap \mathbb{Z} \]  

(3.4)

lifting each residue class mod \( l^n \) to its least non-negative residue. Further, let

\[ t = t_k = t_{k,n} = t_{1,n} \circ \text{Tr}_k. \]  

(3.5)

Thus, the following commutes:

\[ \begin{array}{ccc}
E_{k,n} & \xrightarrow{t = t_k} & \mathbb{Z}/l^n \\
\xrightarrow{\text{Tr}_k} & & \xrightarrow{t_1} \\
\mathbb{Z}/l^n & \xrightarrow{t_1} & \mathbb{Z}
\end{array} \]

The following proposition describes the annihilator of \( G \) as a \( \mathbb{Z}C \)-module:

(3.6) PROPOSITION. Let \( \mathcal{A} = \text{Ann}_{\mathbb{Z}C} G. \) Then \( \mathcal{A} \) has \( \mathbb{Z} \)-basis

\[ \{l^n \delta_i \mid i = 1, \ldots, k\} \cup \{d(\gamma) \mid \gamma \in C, \gamma \neq \delta_i \text{ for } i = 1, \ldots, k\}, \]

where we define for all \( \rho \in E, \)

\[ d(\rho) = \rho - \sum_{i=1}^{k} t(\rho \delta_i') \delta_i. \]

Moreover, \( d(\rho) \in \text{Ann}_{\mathbb{Z}C} G \) for all \( \rho \in E. \)

Proof: \( \mathbb{Z}C \) acts on \( G \) through the ring homomorphism \( \mathbb{Z}C \to E \subseteq \text{End} G \) induced by the group isomorphism \( C \xrightarrow{\cong} E^\times. \) Thus \( \mathcal{A} \) is the kernel of the homomorphism and we have the exact sequence

\[ 0 \to \mathcal{A} \to \mathbb{Z}C \to E \to 0. \]

Evidently \( l^n \delta_i \in \mathcal{A}. \) The fact that \( d(\gamma) \in \mathcal{A} \) comes from the standard property of dual bases that

\[ \rho = \sum_{i=1}^{k} \text{Tr}(\rho \delta_i') \delta_i \quad \text{in } E. \]

(Thus, also \( d(\rho) \in \text{Ann}_{\mathbb{Z}C} G. \)) Now, let \( \mathcal{A}' \subseteq \mathcal{A} \) be the \( \mathbb{Z} \)-module generated by the \( l^n \delta_i \) and the \( d(\gamma) \) with \( \gamma \in C, \gamma \notin \{\delta_1, \ldots, \delta_k\}. \) Let \( \sum_{\gamma \in C} a_\gamma \gamma \in \mathcal{A} \), where the \( a_\gamma \in \mathbb{Z}. \) Then, modulo \( \mathcal{A}', \)

\[ \sum_{\gamma \in C} a_\gamma \gamma = \sum_{\gamma \in C} a_\gamma \gamma - \sum_{\gamma \neq \delta_i} a_\gamma d(\gamma) = \sum_{i=1}^{k} b_i \delta_i, \quad b_i \in \mathbb{Z}. \]
Then \( \sum_{i=1}^{k} b_i \delta_i \in \mathcal{A} = \ker(\mathbb{Z}C \to E) \), and since the \( \delta_i \) form a \( \mathbb{Z}/l^n \)-basis of \( E \), we must have \( l^n \mid b_i \) for \( i = 1, \ldots, k \). Thus \( \sum a_i \gamma \equiv \sum b_i \delta_i \equiv 0 \pmod{\mathcal{A}'} \) showing that \( \mathcal{A} = \mathcal{A}' \). Moreover since the number of generators of \( \mathcal{A} \) is equal to the \( \mathbb{Z} \)-rank of \( \mathbb{Z}C \), they must form a \( \mathbb{Z} \)-basis of \( \mathcal{A} \).

**Remark.** If \( \mathcal{A}_E = \text{Ann}_{\mathbb{Z}C} G \), one can show similarly that \( \{ l^n \delta_i \} \) and \( \{ d(\rho) \mid \rho \in E, \rho \neq \delta_1, \ldots, \delta_k \} \) is a \( \mathbb{Z} \)-basis of \( \mathcal{A}_E \).

(3.7) **Definition.** For each \( \rho \in E_{k,n} \), we define the Stickelberger element associated to \( \rho \) to be

\[
\theta(\rho) = \theta_{k,n}(\rho) = \sum_{\gamma \in C} t_{k,n}(\gamma \rho) \gamma^{-1} \in \mathbb{Z}C_{k,n},
\]

Let \( \theta = \theta(1) = \sum_{\gamma \in C} t(\gamma) \gamma^{-1} \).

**Note.** A simple calculation shows that for \( \gamma \in C \) and \( \rho \in E \),

\[ \gamma \theta(\rho) = \theta(\gamma \rho). \]

(Indeed, \( \sum_{\delta \in C} t(\delta \rho) \gamma \delta^{-1} = \sum_{\delta \in C} t(\delta \rho) \delta^{-1} \).)

(3.8) **Proposition.** The function \( \rho \mapsto l^{-n} \theta(\rho) + \mathbb{Z}C \) is a \( \mathbb{Z}C \)-monomorphism \( E \to \mathbb{Q}C/\mathbb{Z}C \).

**Proof.** The note after (3.7) shows that the action of \( C \) is preserved. It remains only to show the map is a \( \mathbb{Z} \)-monomorphism. But if \( \rho_1, \rho_2 \in E \) and \( \gamma \in C \), we have

\[ t(\gamma \rho_1) + t(\gamma \rho_2) \equiv t(\gamma(\rho_1 + \rho_2)) \pmod{l^n} \]

so

\[ \theta(\rho_1) + \theta(\rho_2) \equiv \theta(\rho_1 + \rho_2) \pmod{l^n \mathbb{Z}C}. \]

Moreover,

\[ l^{-n} \theta(\rho) \in \mathbb{Z}C \iff t(\gamma \rho) \equiv 0 \pmod{l^n} \]

\[ \iff \text{Tr}(\gamma \rho) = 0 \]

for all \( \gamma \in C \). (In particular, recall \( \rho = \sum_{i=1}^{k} \text{Tr}(\rho \delta_i) \delta_i \).)

(3.9) **Definition.** We define two \( \mathbb{Z}C \)-submodules of \( \mathbb{Q}C \):

\[ \mathcal{S} = \mathcal{S}_{k,n} = \sum_{\rho \in E} \mathbb{Z} \cdot l^{-n} \theta(\rho) \subseteq l^{-n} \mathbb{Z}C \]

and

\[ \mathcal{S}' = \mathcal{S}'_{k,n} = \mathbb{Z}C \cdot l^{-n} \theta \subseteq l^{-n} \mathbb{Z}C. \]
Also, we define two Stickelberger ideals:

\[ \mathcal{S} = \mathcal{S}_{k,n} = \mathcal{S}' \cap \mathbb{Z}C \]

and

\[ \mathfrak{I} = \mathcal{S}_{k,n} = \mathfrak{I}' \cap \mathbb{Z}C. \]

Note that \( \mathfrak{I}' \subset \mathcal{S}' \) and \( \mathfrak{I} \subset \mathcal{S} \). Also, when \( n = 1 \), \( E = \mathbb{C} \cup \{0\} \), whence easily \( \mathfrak{I}_{k,1}' = \mathcal{S}_{k,1}' \).

(3.10) **Proposition.** (a) \( \mathfrak{I}' + \mathbb{Z}C = \mathcal{S}' + \mathbb{Z}C \), and \( \mathfrak{I}'/\mathfrak{I} \cong \mathfrak{I}'/\mathcal{S} \cong \mathbb{E} \).

(b) \( \mathfrak{A} = \text{Ann}_{\mathbb{Z}C} G = \{ \alpha \in \mathbb{Z}C \mid \alpha \cdot l^{-n} \theta \in \mathbb{Z}C \} \) and \( \mathfrak{I} = \mathfrak{A} \cdot l^{-n} \theta. \)

**Proof.** Clearly the image of the \( \mathbb{Z}C \)-monomorphism \( E \to \mathbb{C}/\mathbb{Z}C \) of (3.8) is \( \mathfrak{I}' + \mathbb{Z}C/\mathbb{Z}C \). Since \( 1 \in E \) is a \( \mathbb{Z}C \)-generator of \( E \), its image \( l^{-n} \theta + \mathbb{Z}C \) generates \( \mathfrak{I}' + \mathbb{Z}C/\mathbb{Z}C \). Hence \( \mathfrak{I}' + \mathbb{Z}C = \mathfrak{I}' + \mathbb{Z}C/\mathbb{Z}C \) and part (a) follows from the first isomorphism theorem. Likewise the first statement of (b) is an immediate consequence of the fact that \( l^{-n} \theta + \mathbb{Z}C \) generates \( \mathfrak{I}' + \mathbb{Z}C/\mathbb{Z}C \cong E \cong G \). A moment of quiet reflection upon the definition of \( \mathfrak{I} \) yields the further conclusion that \( \mathfrak{A} \cdot l^{-n} \theta = \mathfrak{I} \).

Now we restrict attention to the case \( n = 1 \); that is, \( G \) is elementary abelian of order \( l^k \). Under our conventions, then \( G \) is isomorphic to the additive group of \( \mathbb{E}_{k,1} \), which we may identify with the finite field \( \mathbb{F}_{l^k} \), and \( C \) is identified with \( \mathbb{F}_{l^k}^* \). As remarked above, in this case

\[ \mathfrak{I}' = \mathcal{S}' \quad \text{and} \quad \mathfrak{I} = \mathcal{S}. \]

(3.11) **Proposition.** If \( n = 1 \), then \( \mathfrak{I} + \mathfrak{A} = \mathbb{Z}C. \)

**Proof.** Both \( \mathfrak{A} \) and \( \mathfrak{I} \) are ideals of \( \mathbb{Z}C \), so it suffices to find an element of \( \mathfrak{I} \) which is \( \equiv 1 \pmod{\mathfrak{A}} \), that is, which acts as identity on \( \mathbb{Z}C/\mathfrak{A} \cong E \cong \mathbb{F}_{l^k} \). Now \( C \) has order \( l^k - 1 \), and \( E \) is evidently an irreducible module over the semi-simple group algebra \( \mathbb{F}_l C \). The character of the representation of \( C \) afforded by \( E \) is \( \gamma \mapsto \text{Tr}(\gamma) \). The idempotent corresponding to this \( \mathbb{F}_l \)-irreducible character is

\[ e = (l^k - 1)^{-1} \sum_{\gamma \in C} \text{Tr}(\gamma) \gamma^{-1}. \]

Thus \( -\theta = e \pmod{l \cdot \mathbb{Z}C} \) and a fortiori \( \pmod{\mathfrak{A}} \). But \( -\theta \in \mathfrak{I} \) and since \( e \) acts as identity on \( E \), \( -\theta \equiv 1 \pmod{\mathfrak{A}} \), whence the result follows.

(3.12) **Corollary.** Let \( n = 1 \) and let \( \mathcal{C} \) be a \( \mathbb{Z}C \)-module (written multiplicatively). The following are equivalent for \( m \in \mathcal{C} \):


(a) \( m \in \mathcal{C}^\gamma \).
(b) \( m^a \in \mathcal{C}^\gamma \) for all \( a \in \mathcal{A} \).
(c) There is an \( a \in \mathcal{C} \) such that
\[
m^a = a^{\alpha \cdot l^{-1} \theta} \quad \text{for all} \quad \alpha \in \mathcal{A}.
\]

**Proof.** (c) \(\Rightarrow\) (b): This is clear since \( \alpha \cdot l^{-1} \theta \in \mathcal{I} \).

(b) \(\Rightarrow\) (a): From (b) it follows that \( m^\mathcal{A} \subseteq \mathcal{F}^\gamma \). Clearly \( m^\mathcal{F} \subseteq \mathcal{F}^\gamma \). Hence \( m^\mathcal{F} + \mathcal{F} \subseteq \mathcal{F}^\gamma \). But \( \mathcal{A} + \mathcal{I} = \mathbb{Z} \mathcal{C} \), so \( m \in \mathcal{C}^\gamma \).

(a) \(\Rightarrow\) (c): If \( m \in \mathcal{C}^\gamma \), then \( m = \prod b_i^{\beta_i} \cdot l^{-1} \theta \), with \( b_i \in \mathcal{C} \) and \( \beta_i \in \mathcal{A} \).

Hence, for any \( \alpha \in \mathcal{A} \), \( m^a = (\prod b_i^{\beta_i})^{a^{\alpha \cdot l^{-1} \theta}} \).

(3.13) **Corollary.** Let \( n = 1 \). If \( \mathcal{C} \) is a \( \mathbb{Z} \mathcal{C} \)-module with \( \mathcal{C}^\gamma = 1 \), then \( \mathcal{C} \) has no submodule (or subquotient) which is \( \mathbb{Z} \mathcal{C} \)-isomorphic to \( G \).

**Proof.** If \( \mathcal{C}_1 \) is a subquotient of \( \mathcal{C} \), then \( \mathcal{C}_1^\gamma = 1 \). But if \( \mathcal{C}_1 \cong G \cong E \), then \( \mathcal{C}_1^\mathcal{I} = 1 \), so \( \mathcal{C}_1^\mathcal{C} = 1 \), whence \( \mathcal{C}_1 = 1 \).

Remark. When \( k = 1 \), there are analogous results to (3.11), (3.12), and (3.13) for \( n > 1 \).

4. **The Stickelberger Condition on Realizable Classes**

We continue with the notation of Section 2 and suppose, in addition, that \( G \) is elementary abelian of order \( \ell^k \). As in Section 3 we choose a fixed isomorphism \( \rho \mapsto x^\rho \) from the additive group of \( E(= \mathbb{F}_\ell) \) to \( G \) and regard \( C(= \mathbb{F}_\ell) \) as a group of automorphisms of \( G \). We have the Stickelberger element \( \theta = \theta_{k,1} \in \mathbb{Z} \mathcal{C} \) and ideal \( \mathcal{F} = \mathcal{F}_{k,1} \subseteq \mathbb{Z} \mathcal{C} \).

Now, let \( \pi \in \text{Hom}(\Omega \mathbb{K}, G) \) and continue with the tame \( G \)-extension \( K_\pi/K \) as in Theorem (2.12). The exponent \( l^n \) of \( G \) has now become \( l \).

(4.1) **Theorem.** (a) There is a unique integral ideal \( a \in I(\sigma'G) \) such that
\[
a^\theta = m^l(w)(= (c_{\mathcal{C}^\gamma}')^l).
\]

(b) Moreover, \( a \) is square free and, for \( \gamma, \delta \in C \), \( a^\gamma \) and \( a^\delta \) are co-prime unless \( \gamma = \delta \).

**Proof.** As remarked after (2.12), \( I(\sigma'G) \) is a free abelian group generated by the (invertible) prime ideals of \( \sigma'G \). For any such prime \( p \) and any \( a \in I(\sigma'G) \) we denote by \( v_p(a) \) the exponent to which \( p \) occurs in the decomposition of \( a \). For \( a \in K \mathbb{C}^\times \), we put \( v_p(a) = v_p((a)) \), where \( (a) = \sigma'G - a \). With this notation we define the ideal \( a \) of the theorem to be
the product of the distinct primes \( p \) of \( \sigma'G \) such that \( v_p(w') \equiv t(y) \pmod{l} \) for all \( y \in C \). That is, \( a \) is integral, square free and

\[
p \mid a \Leftrightarrow v_p(w') \equiv t(y) \pmod{l} \quad \text{for all } y \in C.
\]

One sees easily that at most finitely many primes \( p \) can satisfy this condition, so it genuinely defines a square free integral ideal \( a \in I(\sigma'G) \).

Claim 1. For any \( p \) and any \( y \in C \),

\[
v_p(w') \equiv \sum_{i=1}^{k} t(y \delta_i) v_p(w^{\delta_i}) \pmod{l}.
\]

For recall that \( w = v' \), where \( \sigma_{n,l} = \sigma_l G \cdot v \). Now since \( d(y) \in I \) by (3.6), it follows from (2.12)(a) \( \) (or, indeed (1.10) \) that \( v^{d(y)} \in KG^{\times} \) so that \( (v^{d(y)})^l \) is an \( l \)th power in \( I(\sigma'G) \). Since \( d(y) = y - \sum_{i=1}^{k} t(y \delta_i) \delta_i \), this implies that \( (w') \) differs from \( \prod_{i=1}^{k} (w^{\delta_i})^{t(y \delta_i)} \) by an \( l \)th power. The claim follows immediately.

Claim 2. For any \( p \) and any \( \delta \in C \),

\[
p \mid a^{\delta-1} \Leftrightarrow v_p(w') \equiv t(y \delta) \pmod{l} \quad \text{for all } y \in C.
\]

Note, first, that \( v_{\rho \delta}(a) = v_{\delta}(a^{\delta-1}) \) since \( \delta \) is an automorphism of \( \sigma'G \). Hence,

\[
p \mid a^{\delta-1} \Leftrightarrow p \mid a \Leftrightarrow v_p(w^{\delta-1}) = v_p(w') \equiv t(y) \pmod{l} \quad \text{for all } y \in C
\]

\[
\Leftrightarrow v_p(w') \equiv t(y \delta) \pmod{l} \quad \text{for all } y \in C.
\]

Claim 3. The ideals \( a^\delta \) for \( \delta \in C \) are square free and coprime.

By definition, \( a \) is square free, and since \( \delta \in C \) is an automorphism of \( \sigma'G \), \( a^\delta \) is likewise square free. Now, suppose \( a^\delta \) and \( a^\gamma \) have common prime factor \( p \), where \( \delta, \gamma \in C \). Then, by Claim 2, for all \( p \in C \), \( t(p \delta^{\delta-1}) \equiv t(p \gamma^{\gamma-1}) \pmod{l} \), whence \( \text{Tr}(p \delta^{\delta-1}) = \text{Tr}(p \gamma^{\gamma-1}) \). By non-degeneracy of the trace, \( \text{Tr}: \mathbb{F}_p \to \mathbb{F}_l \), we conclude \( \delta^{-1} = \gamma^{-1} \), proving Claim 3.

Now, recall that \( \theta = \sum_{\gamma \in C} t(y) \gamma^{-1} \) so that

\[
a^\theta = \prod_{\gamma \in C} (a^{\gamma-1})^{t(y)}.
\]

Since the \( a^{\gamma-1} \) are square free and coprime and since \( t(y) < l \) for all \( y \in C \), it follows that \( a^\theta \) is integral and \( l \)th power free. Thus, by Theorem (2.12)(b), in order to prove \( a^\theta = m^l(w) \), it suffices to prove

Claim 4. If \( 0 < a < l \), then for any \( p \), \( v_p(w) \equiv a \pmod{l} \Leftrightarrow p \mid a^{\gamma-1} \) for some \( \gamma \in C \) with \( t(y) = a \).
The implication "=" follows from Claim 2 since \( p \mid a^{r-1} \Rightarrow v_p(w) \equiv t(y) \pmod{l} \). To show the converse implication, we show \( p \mid a^{r-1} \), where

\[
\gamma = \sum_{i=1}^{k} v_p(w^{d_i}) \cdot \delta_i' \quad \text{in } E.
\]

(Observe that \( \gamma \neq 0 \) since \( v_p(w^{d_i}) \equiv a \neq 0 \pmod{l} \).) Since the \( \delta_i \) and \( \delta_i' \) are dual bases of \( \mathbb{F}_{l^k} \) over \( \mathbb{F}_l \),

\[
v_p(w^{d_i}) \equiv t(y\delta_i) \pmod{l} \quad \text{for } i = 1, \ldots, k.
\]

Thus, for any \( \delta \in C \), it follows from Claim 1 that

\[
v_p(w^\delta) \equiv \sum_{i=1}^{k} t(\delta\delta_i') t(y\delta_i) \pmod{l}.
\]

But

\[
\text{Tr}(\delta y) = \sum_{i=1}^{k} \text{Tr}(\delta\delta_i') \text{Tr}(y\delta_i)
\]

by the duality of the \( \delta_i \) and \( \delta_i' \) so

\[
v_p(w^\delta) \equiv t(\delta y) \pmod{l}.
\]

The criterion of Claim 2 being satisfied, \( p \mid a^{r-1} \). Moreover, taking \( \delta = 1 \) gives \( t(y) = v_p(w) = a \pmod{l} \). Hence Claim 4 is proved, and we have shown that \( a \) has all the properties described in the theorem except for uniqueness.

To show uniqueness, suppose \( b \) is integral and \( b^\gamma = m'(w) \). Then

\textbf{Claim 5.} The \( b^\gamma \) for \( \gamma \in C \) are square free and coprime.

This will follow from the fact that \( b^\theta \) is \( l \)th power free (by (2.12)). For

\[
b^\theta = \prod_{\gamma \in C} (b^{\gamma-1})^{t(\gamma)}.
\]

Choosing \( \delta \in C \) with \( \text{Tr}(\delta) = -1 \) we get \( t(\delta) = l - 1 \) so \( b^\theta \) has the factor \( (b^{\delta-1})^{(l-1)} \). Thus \( b^{\delta-1} \) must be square free whence all \( b^\gamma \) are square free.

Now, for any \( \delta \in C \),

\[
b^{\delta \cdot \theta} = b^{\theta(\delta)} = \prod_{\gamma \in C} (b^{\gamma-1})^{t(\delta \gamma)}
\]

and \( b^{\delta \cdot \theta} \) is \( l \)th power free. Suppose \( b \) and \( b^{\gamma-1} \) have a common factor where \( \gamma \neq 1 \). Then

\[
t(\delta) + t(\delta \gamma) < l \quad \text{for all } \delta \in C.
\]
We show this is impossible. It suffices to show there is a $\delta \in C$ with $\text{Tr}(\delta) = -1$ and $\text{Tr}(\delta \gamma) \neq 0$, for then

$$t(\delta) + t(\delta \gamma) \geq (l - 1) + 1 = l.$$  

To show this, it suffices to show there is a $\delta \in C$ with $\text{Tr}(\delta) \neq 0$ and $\text{Tr}(\delta \gamma) \neq 0$, for then with $a = -(\text{Tr} \delta)^{-1} \in \mathbb{F}_l^\times$ we have

$$\text{Tr}(a \delta) = a \text{Tr}(\delta) = -1 \quad \text{and} \quad \text{Tr}(a \delta \gamma) = a \text{Tr}(\delta \gamma) \neq 0.$$  

Now, finally, observe that the conditions (on $\delta$) $\text{Tr}(\delta) = 0$ and $\text{Tr}(\delta \gamma) = 0$ determine two proper $\mathbb{F}_l$-subspaces of $\mathbb{F}_l$. Since $\mathbb{F}_l$ is not the union of two proper subspaces we can find the required $\delta \in C$ and the claim is proved.

**Claim 6.** $b = a$.

Applying $\delta \in C$ to $b^\theta = m'(w)$ we see $(m^\delta)'(w^\delta) = b^\delta \cdot \theta = \prod_{\gamma \in C}(b^{\gamma^{-1}})^{t(\delta \gamma)}$. Since the $b^{\gamma^{-1}}$ are square free and coprime, we see that (for all $\delta \in C$),

$$p \mid b \Rightarrow p \mid a \text{ so } b \mid a \text{ and } b^{\gamma^{-1}} \mid a^{\gamma^{-1}} \text{ for all } \gamma \in C.$$  

Hence $p \mid b \Rightarrow p \mid a$ and $b^{\gamma^{-1}} \mid a^{\gamma^{-1}}$ for all $\gamma \in C$. But $\prod_{\gamma \in C}(b^{\gamma^{-1}})^{t(\delta \gamma)} = \prod_{\gamma \in C}(a^{\gamma^{-1}})^{t(\delta \gamma)}$ so $b^{\delta \gamma} = a^{\delta \gamma}$ for all $\delta \in C$. Since there is a $\delta \in C$ with $t(\delta) \neq 0$, we see $b = a$. This completes the proof of (4.1).

**Corollary.** $\mathcal{C}(\sigma_a) \in \mathcal{C}(\sigma G)^\sigma$.

**Proof.** By (2.12), $\mathcal{C}(\sigma_a)$ is represented by $m$, and from (4.1),

$$m'(w) = a^\theta.$$  

Let $\bar{m}$ and $\bar{a}$ denote the classes of $m$ and $a$, respectively, in $\mathcal{C}(\sigma G) = I(\sigma^I G)/(\sigma_1 G^\times)$. We will show that for any $\alpha \in \mathcal{A} = \text{Ann}_{\mathbb{Z}G} G$,

$$\bar{m}^\alpha = \bar{a}^\alpha \cdot l^{-1} \theta$$  

from which it follows by (3.12) that $\bar{m} \in \mathcal{C}(\sigma G)^\sigma$ as required. Let $a \in \mathcal{A}$. Then $a \cdot l^{-1} \theta \in \mathcal{A}$ and we have

$$(ma)^l(w^\alpha) = (a^\alpha \cdot l^{-1} \theta)^l.$$  

But $w = \bar{v}^l$ so $w^\alpha = (\bar{v}^\alpha)^l$ and $\bar{v}^\alpha \in KG^\times$. Since $I(\sigma^I G)$ is a free abelian group, we can take $l$th roots and get

$$m^\alpha \cdot (\bar{v}^\alpha) = a^\alpha \cdot l^{-1} \theta.$$  

But, by (2.12)(a), $\bar{v}^\alpha \in \sigma_1 G^\times$ so modulo $(\sigma_1 G^\times)$ we get $\bar{m}^\alpha = \bar{a}^\alpha \cdot l^{-1} \theta$ as promised.
We shall refine this corollary slightly as follows. Consider the augmentation
\[ \varepsilon: \sigma G \to \sigma \] (sending \( s \to 1 \) for all \( s \in G \)).

This induces a homomorphism
\[ \varepsilon_\# : \ell(\sigma G) \to \ell(\sigma). \]

Let
\[ \ell'(\sigma G) = \ker(\varepsilon_\#) \] (4.3)

Then

(4.4) Corollary. \( \ell(\sigma) \in (\ell'(\sigma G))^\varepsilon. \)

Proof. First observe that \( \ell(\sigma) \in \ell'(\sigma G) \). This is a general fact which can be shown for arbitrary groups \( G \) (including non-abelian). We can see it most easily here by recalling (2.5):
\[ \sigma_\pi = m \cdot v, \quad \text{where } \sigma_\pi' = \sigma_i v. \]

Applying \( \text{Tr}: K_\pi \to K \) we get
\[ \sigma' = \text{Tr}(\sigma_\pi') = \text{Tr}(m \cdot v) = \varepsilon(m) \cdot \text{Tr}(v), \]

where \( \text{Tr}(v) \in \sigma_j^\vee \) (by (2.6), for example). Thus \( \varepsilon(m) \) is in the trivial class of \( \ell'(\sigma) = I(\sigma')/(\sigma_i^\vee') \).

To complete the argument observe that the augmentation \( \varepsilon: \sigma G \to \sigma \) is split by the inclusion \( i: \sigma \to \sigma G \). That is,
\[ \varepsilon \circ i = \text{identity on } \sigma \ (\text{and } i \circ \varepsilon = [0]). \]

This retraction of rings induces a splitting of ideal groups
\[ I(\sigma' G) \xrightarrow{\varepsilon_\#} I(\sigma') \]

and of class groups
\[ \ell(\sigma G) \xrightarrow{\varepsilon_\#} \ell(\sigma). \]

For \( \gamma \in G \), \( \varepsilon \circ \gamma = \varepsilon \) and \( \gamma \circ i = i \), so both \( \varepsilon_\# \) and \( i_\# \) are \( ZC \)-homomorphisms, where \( C \) acts trivially on \( \sigma \) and \( \ell(\sigma) \). From the \( ZC \)-decomposition
\[ \ell(\sigma G) = (\ker \varepsilon_\#) \times (\text{im } i_\#) \]
we easily see that
\[ \mathcal{E}l'(\sigma G)^\mathcal{F} = \mathcal{E}l(\sigma G)^\mathcal{F} \cap \mathcal{E}l'(\sigma G) \]
and the corollary follows immediately.

For future reference we note here also that if we let
\[ I'(\sigma'G) = \ker(\varepsilon : I(\sigma'G) \to I(\sigma')), \quad (4.5) \]
then an easy chase in the diagram

\[ \begin{array}{ccc} I(\sigma'G) & \xrightarrow{\varepsilon} & I(\sigma') \\ \downarrow & & \downarrow \\ \mathcal{E}l(\sigma G) & \xrightarrow{\varepsilon_{\pi}} & \mathcal{E}l(\sigma) \end{array} \]

shows that the surjection \( I(\sigma'G) \twoheadrightarrow \mathcal{E}l(\sigma G) \) restricts to a surjection of \( \mathbb{Z}C \)-modules:
\[ I'(\sigma'G) \twoheadrightarrow \mathcal{E}l'(\sigma G). \quad (4.6) \]

Finally we observe that the ideal \( \alpha \) is a fundamental (tame) ramification invariant of \( K_{\sigma'/K} \) in the following sense.

In (2.13) we obtained the discriminant formula
\[ b(\mathcal{O}_{\sigma'/\sigma'}) = [\sigma'G : \mathcal{O}_{\sigma'/\sigma'}^{1+1}]_{\sigma'}. \]
But now, we see easily
\[ \mathcal{O}_{\sigma'/\sigma'}^{1+1} = a^{1+1+1-1} \cdot \theta/l \quad \text{in } I(\sigma'G), \]
since both sides have the same \( l \)th power. Hence
\[ b(\mathcal{O}_{\sigma'/\sigma'}) = [\sigma'G : a^{1+1-1}]_{\sigma'}. \]
Since the module index can be computed component-wise in \( \sigma'G \), we see that a prime \( p \) of \( \sigma' \) divides the discriminant \( b(\mathcal{O}_{\sigma'/\sigma'}) \) if and only if some prime factor \( \mathfrak{p} \) of \( p \cdot \sigma'G \) in \( \sigma'G \) divides \( \alpha \). But \( \alpha \) is square free and relatively prime to all of its “conjugates” \( \alpha^n \). It can be shown from this that \( \alpha \) cannot be divisible by two distinct prime factors of \( p \cdot \sigma'G \) in \( \sigma'G \), and, indeed, if \( p \) is ramified in \( \mathcal{O}_{\sigma'/\sigma'}' \), then \( p \) is “split completely” in \( \sigma'G \). Finally note, however, that \( \alpha \) depends very much on the choice of the isomorphism \( E \cong G \) and the resulting action of \( C \) as a group of automorphisms of \( \sigma'G/\sigma' \).
5. Sufficiency of the Stickelberger Condition

We continue with the notation of the previous section. In particular, $G$ is elementary abelian ($n = 1$).

(5.1) Theorem. Let $m \in \mathcal{O}^1(\sigma G)^\sigma$. Then there is a (proper) tame $G$-extension $K_\pi/K$ with $cl(\sigma G)_\pi = m$. Moreover $K_\pi/K$ can be chosen to have discriminant $\neq (1)$ and relatively prime to any pre-assigned ideal of $K$.

Proof. As before, $G^* = \text{Hom}(G, (K^c)^\times)$, the character group of $G$. Through its action on $(K^c)^\times$, $\Omega_K$ acts as a group of automorphisms of $G^*$:

\[ \chi^\sigma(s) = (\chi(s))^\sigma, \quad \chi \in G^*, \sigma \in \Omega_K, \text{ and } s \in G. \]

We can describe elements of $K^cG$ as functions defined on $G^*$. That is, if $\alpha \in K^cG$, we denote also by $\alpha$ the function $\chi \mapsto \alpha_\chi$ from $G^* \to K^c$, where $\alpha_\chi = \chi(\alpha)$. With this notation, we identify $K^cG$ and $\text{Map}(G^*, K^c)$. This identification preserves the action of $\Omega_K$, where $\Omega_K$ acts on $\text{Map}(G^*, K^c)$ by

\[ f^\sigma(\chi) = (f(\chi^{-1}))^\sigma \quad \text{for } f \in \text{Map}(G^*, K^c), \]

$\chi \in G^*$ and $\sigma \in \Omega_K$. This follows by noting that $\chi^\sigma(\alpha^\sigma) = \chi(\alpha)^\sigma$ for $\alpha \in K^cG$, $\chi \in G^*$, and $\sigma \in \Omega_K$. Hence,

\[ KG \cong \text{Map}_{\Omega_K}(G^*, K^c), \]

and for $\alpha \in KG$, $\chi \in G^*$, $\sigma \in \Omega_K$, $\alpha_\chi = (\alpha_\chi)^\sigma$. The simple components of the group algebra $KG$ correspond to the $\Omega_K$-orbits in $G^*$, that is, to the elements of $G^*/\Omega_K$. This is reflected in the above identification by the observation that if $\Phi$ is a set of representatives of $G^*/\Omega_K$, then an $\Omega_K$-map $\alpha : G^* \to K^c$ is determined uniquely by its values $\alpha_\phi$ for $\phi \in \Phi$ and that $\alpha_\phi$ can be arbitrary in $K(\phi)$ ($= K(\phi(G))$). Thus

\[ KG \cong \prod_{\phi \in \Phi} K(\phi) \]

and likewise for $\sigma^tG$ and $I(\sigma^tG)$:

\[ \sigma^tG \cong \prod_{\phi \in \Phi} \sigma^t[\phi], \quad \text{where } \sigma^t[\phi] = \sigma^t[\phi(G)] \]

and

\[ I(\sigma^tG) = \prod_{\phi \in \Phi} I(\sigma^t[\phi]). \]
Clearly $\Phi$ contains the trivial character $\varepsilon$ which induces the augmentation $\varepsilon : \sigma G \to \sigma$ and, recalling (4.5), we may write

$$I'(\sigma' G) = \{ a \in I(\sigma' G) \mid a_\varepsilon = (1) \}.$$ 

Now, let $m \in \mathcal{G}^t(\sigma G)$. From (4.6) we have a surjection

$$I'(\sigma' G)^t \twoheadrightarrow \mathcal{G}^t(\sigma G),$$

so we may choose a representative $m \in I'(\sigma' G)^t$ of the class $m$. Then, by (3.12), there is an ideal $b \in I'(\sigma G)$ such that

$$m^a = b^{a \cdot l - 10} \quad \text{for all} \quad a \in \mathcal{A} = \text{Ann}_{\mathcal{I}} G,$$

and in particular $m^l = b^l$.

The strategy will be to replace $b$ by an integral ideal $a \in I'(\sigma' G)$ in the same class as $b$ such that $a^\theta$ is integral and $l$th power free. We will then have $(a)^b = a$ for some $y \in \sigma G^\times$. Since $K\sigma G^\times$ is divisible we can choose $v \in (K\sigma G)^\times$ such that $v^l = y$. Then $m^l(y^\theta) = a^\theta$, where $y^\theta = (v^\theta)^l$. It will suffice by (2.12) to show that $v^\theta = \tilde{b}$, where $v$ is an $l$-local normal basis generator for some tame $G$-extension $K_{\mathfrak{p}}/K$. To show that $v^\theta$ is a resolvable, it will suffice by (1.10) to show that $(v^\theta)^a \in K\sigma G^\times$ for all $a \in \mathcal{A} = \text{Ann}_{\mathcal{I}} G$. This will be seen to follow from (3.10) and the remark following (3.6) if $v$ is chosen so that $v_\varepsilon = 1$. Then $v^\theta = \tilde{v} \in \tilde{K}_{\pi} \cap (K\sigma G)^\times$ for a unique $\pi \in \text{Hom}(O_K, G)$, and $v \in K_{\pi}$. It will remain to show that $\pi$ is tame and that $\tilde{\sigma}_{\pi} = \sigma G \cdot \tilde{b}$. That will follow from criterion (b) of (2.6) by showing $\tilde{v} = v^\theta \in \tilde{\sigma}_{\pi}$ and $\text{Tr} v = (v^\theta)^l = 1$. Since $\tilde{\sigma}_{\pi} = \tilde{K}_{\pi} \cap \sigma G$, the crux of the matter will be to show $v^\theta \in \sigma G$, where $\sigma G$ is the integral closure of $\sigma G \cdot \tilde{b}$. This will be the case if $y$ is chosen properly. We begin now with the choice of $a$ and $y$.

For an integral ideal $a$ to be such that $a^\theta$ is $l$th power free, it suffices that $a$ should be square free and relatively prime to all of its $\mathcal{C}$-conjugates $a^\gamma$, $\gamma \in \mathcal{C}, \gamma \neq 1$. (Indeed, this is also necessary as we showed, in effect, in Claim 5 in the proof of Theorem (4.1).) To define a square free ideal $a \in I'(\sigma' G)$ it suffices to define a square free ideal $a_\phi \in I(\sigma' G)$ for each $\phi \in \Phi, \phi \neq \varepsilon$. For $a$ to be in the same class as $b$, it suffices for $a_\phi$ to be in the same ray class mod $l^k$ as $b_\phi$ in $I(\sigma' G)$. (Recall that, as remarked in Section 2, $l^k \mathcal{M} \subseteq \sigma G$, where $\mathcal{M}$ is the maximal $\sigma$-order of $K_{\mathfrak{p}}$, so

$$\sigma G^\times \ni 1 + l^k \mathcal{M} = \prod_\phi (1 + l^k \sigma_1 [\phi]),$$

and the ray class group mod $l^k$ of $K(\phi)$ is $I(\sigma' G)/(1 + l^k \sigma_1 [\phi])$.)
Now, each ray class contains infinitely many prime ideals of absolute degree one. We choose \( a_\phi = (1)(-b_\phi) \) and for \( \phi \in \Phi, \phi \neq \varepsilon \), we choose \( a_\phi \) to be a prime ideal of \( I(\sigma^i(\phi)) \) lying in the same ray class \( \pmod{I^n} \) as \( b_\phi \), where \( N = \max(2, k) \). Moreover, we choose the \( a_\phi \)

(i) to be split completely over \( K \) (indeed of absolute degree one if desired),

(ii) to lie over distinct primes of \( K \),

(iii) to be distinct from all primes occurring in the \( b_\chi \) for \( \chi \in G^* \), and

(iv) to be relatively prime to any preassigned ideal of \( K \).

This choice of the \( a_\phi \) determines a unique square free integral ideal \( a \in I'(\sigma^i G') \) which corresponds to \( \langle a_\phi \rangle_{\phi \in \Phi} \) under the previously described isomorphism \( I(\sigma^i G) \cong \prod_{\phi \in \Phi} I(\sigma^i(\phi)) \).

**Claim 1.** The \( a^\gamma, \gamma \in C, \) are square free and relatively prime.

The \( a^\gamma \) are square free since \( a \) is. Next, observe that the \( \chi(a), \chi \in G^*, \chi \neq \varepsilon \) are distinct primes of \( K(\chi) = K(\mu_i) \). For, any \( \chi \neq \varepsilon \) is of form \( \chi = \sigma^\alpha \) for a unique \( \phi \in \Phi \) and some \( \sigma \in \Omega_K \). If \( a_{\phi^\sigma} = a_{\phi^{\sigma'}} \) (in \( I(\sigma^i[\mu_i]) \)) then \( (a_\phi)^\sigma = (a_{\phi})^{\sigma'} \), so \( a_\phi \) and \( a_{\phi} \) are conjugate (over \( K \)). Hence, condition (ii) on the \( a_\phi \)'s implies \( \phi = \phi' \). But then (i) implies \( \sigma \) and \( \sigma' \) have the same restriction to \( K(\mu_i) \) so \( \phi^\sigma = \phi'^{\sigma'} \). Now, if \( a^\gamma \) and \( a^\gamma' \) for \( \gamma, \gamma' \in C \) have a common prime factor, it comes from some component \( K(\phi) \) of \( KG, \phi \neq \varepsilon \) (since \( (a^\gamma)^\varepsilon = (a^\gamma')^\varepsilon = a_\varepsilon = (1) \)). Hence \( \phi(a^\gamma) \) and \( \phi(a^\gamma') \) have a common prime factor in \( K(\mu_i) \). But \( \phi(a^\gamma) = a_{\sigma^\gamma} \) and \( \phi(a^\gamma') = a_{\sigma^\gamma'} \). Since the \( a_\chi, \chi \neq \varepsilon, \) are distinct primes, \( a^\gamma = a^\gamma' \). But \( G^* \) is cyclic and faithful over \( E \), generated by \( \phi \) (or any \( \chi \neq \varepsilon \)), so \( \gamma = \gamma' \).

**Claim 2.** \( a^\gamma \) is integral and \( l^h \)th power free.

This is immediate from Claim 1.

Now, for each \( \phi \in \Phi, \ b_\phi^{-1}a_\phi = (y_\phi), \) where \( y_\phi = 1 \) and if \( \phi \neq \varepsilon, \ y_\phi \in 1 + l^h_\phi [\phi] \). Together, the \( y_\phi \) determine a unique element \( y \in 1 + l^h \mathcal{M}_l \) corresponding to \( \langle y_\phi \rangle_{\phi \in \Phi} \) under the isomorphism \( KG \cong \prod_{\phi \in \Phi} K(\phi) \). Clearly,

\[
a = (y)b \quad \text{and} \quad m^l(y^\phi) = a^\phi \quad (5.2)
\]

since \( m^l = b^\phi \).

Now, choose \( \nu \in (K^cG)^* \cong \text{Map}(G^*, (K^c)^*) \) so that \( \nu^l = y \), by choosing \( \nu_{\varepsilon} = y_{\varepsilon} = 1 \) and for each \( \chi \neq \varepsilon, \nu_{\chi} \in K^c \) with \( \nu_{\chi}^l = y_{\chi} \). Notice that, even though \( y \in 1 + l^h \mathcal{M}_l \subset (\sigma_l G)^* \), there is no guarantee that \( \nu \in \sigma_l G \), and it may indeed be that no such \( \nu \in \sigma_l G \). However, we will later show that \( \nu^\phi \in \sigma_l G \).

**Claim 3.** \( \nu^\phi \in \tilde{K}_\pi \) for a unique \( \pi \in \text{Hom}(\Omega_K, G) \).
Since \( G^* \) is cyclic over \( E \), it suffices by (1.8) and (1.10) to show that
\[
\nu^a \in KG^* \quad \text{for all} \quad a \in \mathcal{A}_E = \text{Ann}_{E, G}.
\]
Now, by the remark following (3.6),
\[
\mathcal{A}_E = \mathcal{A} + \mathbb{Z}[0], \quad \text{where} \quad \mathcal{A} = \text{Ann}_{\mathbb{Z}, G},
\]
since \( d([0]) = [0] \).

From (3.10) for \( a \in \mathcal{A}, \ a \cdot l^{-1} \theta \in \mathbb{Z}C \) so \( \nu^{a \theta} = \nu^{a} \cdot l^{-1} \theta \in KG^* \). Also \( \nu^{\theta[0]} = 1 \) since \( \nu^{[0]} = \nu_e = 1 \), and the claim follows.

Hence \( \nu^{\theta} = \tilde{\nu} \) for a unique \( \nu \in K_\pi \).

**Claim 4.** \( K_{\mathcal{A}}/K \) is tame and \( \mathcal{O}_{\pi, 1} = \sigma_{1} G \cdot v \).

By criterion (b) of (2.6), it suffices to show that \( \text{Tr} \nu = 1 \) and \( \nu \in \mathcal{O}_{\pi, 1} \).

Now \( \text{Tr} \nu = \varepsilon(\tilde{\nu}) = (\nu^\theta)_e = 1 \) since \( \nu_e = 1 \). To show \( \nu \in \mathcal{O}_{\pi, 1} \) it suffices to show
\[
\nu^\theta = \tilde{\nu} \in \mathcal{O}_{\pi} G,
\]
where \( \mathcal{O}_{\pi} \) is the integral closure of \( \sigma_{1} \) in \( K_{\mathcal{A}} \), since
\[
\mathcal{O}_{\pi, 1} = \mathcal{O}_{\pi} G \cap K_{\pi}.
\]
Since \( \nu^\theta = \sum_{s \in G} v(s) \cdot s^{-1} \), it suffices to show \( v(s) \in \mathcal{O}_{\pi} \) for all \( s \in G \). Let \( \omega = \nu^{\theta s} \). Then orthogonality of the characters gives
\[

v(s) = l^{-k} \sum_{\chi \in G^*} \omega \chi.
\]
(Alternatively, since \( \tilde{\nu} \) regarded as a function on \( G^* \) is a Fourier transform of \( \nu \) regarded as a function on \( G \), one gets immediately
\[
v(s) = l^{-k} \sum_{\varepsilon \in \mathcal{O}_{\pi} G^*} \tilde{\nu} \chi(s) = l^{-k} \sum_{\chi \in G^*} \chi(\nu^\theta s).
\]
Let \( \psi \in G^*, \ \psi \neq e \). Then since \( G^* \) is cyclic over \( E \), the map \( \rho \mapsto \psi^\rho \) from \( E \to G^* \) is bijective. Hence
\[
v(s) = l^{-k} \sum_{\rho \in E} \psi^\rho(\omega) = l^{-k} \sum_{\rho \in E} \psi(\omega^\rho).
\]
Recalling the definition of the element \( d(\rho) \in \mathcal{A}_E = \text{Ann}_{\mathbb{Z}, G} \) from (3.6), we see that
\[
\omega^\rho = \omega^{d(\rho)} \cdot \prod_{i=1}^{k} (\omega^h)^{n(\rho \delta \rho^i)}.
\]
Now, for $\rho = \gamma \in \mathcal{C}$, $d(\gamma) l^{-1} \theta \in \mathbb{Z} \mathcal{C}$, by (3.10) so

$$\omega^{d(\gamma)} = (v^\theta s)^{d(\gamma)} = \gamma^{d(\gamma) l^{-1} \theta} \in 1 + l^n \mathcal{C}_1,$$

while for $\rho = [0]$, $d(\rho) = [0]$ and

$$\omega^{d([0])} = (v^\theta [0])^{[0]} = v^{[0] \theta} = 1.$$

In either case, we have, for $\rho \in \mathcal{E}$,

$$\psi(\omega^{d(\rho)}) \equiv 1 \pmod{l^n \mathcal{C}_1[\psi]}.$$

Since $N \geq k$, we get from (5.5) that

$$l^{-k} \psi(\omega^\rho) \equiv l^{-k} \prod_{i=1}^{k} \omega_i^{t(\rho \delta_i)} \pmod{\mathcal{C}_1^e},$$

where we have abbreviated $\psi(\omega^\delta_i)$ to $\omega_i$. Hence, from (5.4) we get

$$v(s) \equiv l^{-k} \sum_{\rho \in \mathcal{E}} \prod_{i=1}^{k} \omega_i^{t(\rho \delta_i)} \pmod{\mathcal{C}_1^e}. \quad (5.6)$$

Recalling now that in $\mathcal{E}$,

$$\rho = \sum_{i=1}^{k} \text{Tr}(\rho \delta_i) \delta_i,$$

we see that as $\rho$ runs over $\mathcal{E}$, the $k$-tuple $(t(\rho \delta_i), \ldots, t(\rho \delta_i))$ runs over all $k$-tuples of integers in $\{0, 1, \ldots, (l-1)\}$. Hence, from (5.6) we get

$$v(s) \equiv l^{-k} \prod_{i=1}^{k} \sum_{j=0}^{l-1} \omega_i^{j} = \prod_{i=1}^{k} \frac{w_i - 1}{l(\omega_i - 1)} \pmod{\mathcal{C}_1^e}, \quad (5.7)$$

where $w_i = \omega_i = \psi(\omega^{\delta_i}) = \psi(j^\delta_i) \in 1 + l^n \mathcal{C}_1[\psi]$ since $j^\delta_i \in 1 + l^n \mathcal{C}_1$. Now $N \geq 2$ so $w_i \equiv 1 \pmod{\lambda^i}$, where $\lambda = 1 - \zeta$, $\zeta^i = \mu_i$, and $(l) = (\lambda)^{-1}$. A time-honored argument (see, for example, [8, Remark (3.1.3)]) then shows that

$$\frac{w_i - 1}{\omega_i - 1} \equiv 0 \pmod{l}.$$ 

Hence, from (5.7), $v(s) \equiv 0 \pmod{\mathcal{C}_1^e}$. This completes the proof of Claim 4.

The argument is now essentially complete, by (2.12). For if $w = \delta^i = \gamma^\theta$, then by (5.2), $m^i(w) = a^\theta$, where $a^\theta$ is integral and $l$th power free (by Claim 2). Thus, since $\mathcal{C}_n = \mathcal{C}_1^e \cdot v$, $\ell_l(\mathcal{C}_n)$ in $G \ell(\mathcal{C}_1^e)$ is represented by $m$. 

Galois Module Structure
which by choice, also represents the original class \( m \in \mathcal{C}'(\sigma G)^{\mathfrak{t}} \). It only remains to show that the discriminant \( d(\mathcal{O}_n/\sigma) \) could have been (and in fact was) chosen relatively prime to any pre-assigned ideal of \( K \). This follows from the fact that since \( K_n/K \) is tame, \( d(\mathcal{O}_n/\sigma) \) is relatively prime to \( l \) and that, by the remarks at the end of Section 4, \( d(\mathcal{O}_n/\sigma^t) \) is divisible only by primes \( p \) of \( \sigma^t \) for which some factor \( \mathfrak{B} \) of \( p \cdot \sigma^t G \) divides \( n \). But, by (iv), the components of \( n \) and hence also \( n \) itself were chosen relatively prime to any preassigned ideal of \( K \).

(5.8) Remark. The \( G \)-extension \( K_n/K \) constructed in the proof of (5.1) is actually a field, and not merely a Galois algebra. To see this, it suffices to show that for any proper subgroup \( H < G \), the tame \( G/H \)-extension \( K_n^H \) is ramified—that is, \( d(\mathcal{O}_n^H/\sigma) \neq (1) \). (For it is easy to see that \( (K_n)^{\pi(\Omega_k)} \) is a product of \( [G : \pi(\Omega_k)] \) copies of \( K \) and is not ramified whence \( \pi(\Omega_k) = G \), so \( K_n = K_n^{\pi} \).)

To see that \( K_n^H \) must be ramified, observe first that \( K_n^H \) can be identified with \( K_n^\pi \), the Galois \( \bar{G} \)-extension corresponding to \( \pi \) where \( \pi \) is the composite of \( \pi \) with the canonical \( G \to \bar{G} = G/H \). Then one easily checks commutativity of the diagram

\[
\begin{array}{ccc}
K_n & \longrightarrow & K^G \\
\downarrow & & \downarrow \\
K_n^\pi & \longrightarrow & K^G
\end{array}
\]

where the horizontal maps are the respective resolvend maps, \( K_n \to K_n^\pi \) is the trace \( (\text{Tr} = \sum_{h \in H} h) \) and \( K^G \to K^G \) is induced by the canonical \( G \to \bar{G} \). Since \( K_n/K \) is tame, \( \text{Tr}(\mathcal{O}_n^\pi) = \mathcal{O}_n^H = \mathcal{O}_n^\pi \) and (by (2.13)), \( d(\mathcal{O}_n^H/\sigma') = [\sigma^t \bar{G} : \mathcal{O}_n^{\pi([1+1]-1)}]_{\sigma'} \). If \( d(\mathcal{O}_n^H/\sigma') = (1) \), then \( \mathcal{O}_n^\pi = \sigma^t \bar{G} \) since

\[
\sigma^t \bar{G} = (\sigma^t \bar{G})' = (\mathcal{O}_n^{\pi})' \cdot (\mathcal{O}_n^{\pi([-1]-1)})'.
\]

Regard \( \bar{G}^* \) as a subgroup of \( G^* \) and suppose \( \chi \in \bar{G}^* \), \( \chi \neq \varepsilon \). Then since \( \mathcal{O}_n^\pi = \text{Tr}(\mathcal{O}_n^\pi) \),

\[
\chi((\mathcal{O}_n^\pi)') = \chi((\mathcal{O}_n^{\pi})') = \chi(\sigma^t \bar{G}) = (1).
\]

But \( \chi(\mathcal{O}_n^\pi) = \chi(a^\theta) = \prod_{\gamma \in \mathfrak{C}} \chi'(\alpha^{(\theta)}) \). Since we showed that the \( \chi(a) \) for \( \chi \neq \varepsilon \) were distinct primes of \( \sigma^t [\mu_2] \) (when proving Claim 1 of the proof of (5.1)) it follows that \( \chi(a^\theta) \neq (1) \), a contradiction. Hence \( d(\mathcal{O}_n^H/\sigma') \neq (1) \).

In view of these remarks we can strengthen (5.1) as follows:

(5.9) Theorem. Let \( m \in \mathcal{C}'(\sigma G)^{\mathfrak{t}} \). Then there are infinitely many tame \( G \)-extensions \( K_m/K \) satisfying
(i) \(\text{cl}(\sigma_n) = mn\).

(ii) \(K_n/K\) is a tame field extension.

(iii) If \(K \subseteq L \subseteq K_n\) then \(L/K\) is ramified.

(iv) The discriminant of \(K_n/K\) can be chosen relatively prime to any pre-assigned ideal of \(K\).

Proof. This is immediate.

(5.10) Definition. We define the set of realizable classes \(R(\sigma G) \subseteq \mathcal{E}l(\sigma G)\) to be

\[\{ \text{cl}(\sigma_n) | \pi \in \text{Hom}(\Omega^I_k, G) \}.\]

(5.11) Corollary. If \(G\) is elementary abelian,

\[R(\sigma G) = \mathcal{E}l'(\sigma G)^\mathfrak{F}.\]

Proof. This is immediate from (4.4) and (5.1).

(5.12) Corollary. If \(G\) is elementary abelian,

\[\mathcal{E}l(\mathbb{Z}G)^\mathfrak{F} = 1.\]

Proof. Since \(\mathcal{E}l(\mathbb{Z}) = 1,

\[\mathcal{E}l'(\mathbb{Z}G) = \ker \varepsilon_* = \mathcal{E}l(\mathbb{Z}G).\]

Also, \(R(\mathbb{Z}G) = 1\), since every tame abelian extension of \(\mathbb{Q}\) has a normal integral basis. The corollary follows from (5.11).

References

3. L. N. Childs, Tame Kummer extensions and Stickelberger conditions, manuscript.


