Weak homological equivalence, canonical factorisability and chinburg's invariants

Holland, David

WEAK HOMOLOGICAL EQUIVALENCE, CANONICAL FACTORISABILITY AND CHINBURG'S INVARIANTS

David Holland

thesis for the degree of
Doctor of Philosophy, 1990

Abstract: Let N/K be a Galois extension of number fields with Galois group Γ. T. Chinburg has constructed invariants of the extension N/K lying in the locally free class group $Cl(\mathbf{Z}\Gamma)$.

In the first chapter we generalise this construction by defining weak homological equivalences and their projective invariants over any Noetherian ring Λ.

In the case where Λ is an order in a semisimple algebra, we obtain for each Λ-lattice M an effectively computable subgroup $\Delta(M)$ of the kernel group $D(\Lambda)$. Specialising to the case $\Lambda = \mathbf{Z}\Gamma$ we relate Δ subgroups to generalised Swan subgroups and we describe a representative of the coset of the Swan subgroup $T(\mathbf{Z}\Gamma)$ containing Chinburg's invariant $\Omega(N/K, 1)$ in terms of the projective invariant of a homomorphism.

In the second chapter we generalise A. Fröhlich's canonical factorisability from abelian to arbitrary finite groups. We obtain a canonical factorisation function — related to the ring of integers $\mathcal{O}_N$ — which determines a unique coset of $Cl(\mathbf{Z}\Gamma)/D(\mathbf{Z}\Gamma)$ equal to the coset generated by Chinburg's invariant $\Omega(N/K, 2)$. Thus we establish "modulo $D(\mathbf{Z}\Gamma)$" a conjecture of Chinburg.

WEAK HOMOLOGICAL EQUIVALENCE, CANONICAL FACTORISABILITY AND CHINBURG'S INVARIANTS

by

David Holland

A thesis presented for
the degree of Doctor of Philosophy
at the University of Durham

October 1990

CONTENTS.

General Introduction.

This thesis is divided into two chapters which can be read independently — a separate and detailed introduction is included for each chapter.

In the first chapter, we examine the possibility of obtaining projective invariants over an arbitrary Noetherian ring Λ. In other words we aim to produce elements of the group $\mathcal{K}_0(\Lambda)$ which classifies the finitely generated projective Λ-modules. Instead of producing projective modules directly, we use a more indirect approach (which in fact generalises previous methods of obtaining projective invariants from Mayer-Vietoris sequences). The raw data needed is a pair U and V of *non-projective* modules connected by a *weak homological equivalence*. This equivalence then gives rise to a projective invariant, which in some sense measures the "difference" between U and V.

Our main interest is concentrated in the case where Λ is an order in a finite dimensional semisimple algebra over a number field. We show that in this case one can often obtain invariants of locally free modules, in other words elements of the locally free classgroup $Cl(\Lambda)$. Further we show that each Λ-lattice U gives rise to an effectively computable subgroup $\Delta(U)$ of the kernel group $D(\Lambda) \subseteq Cl(\Lambda)$.

Let G be a finite group and R a Dedekind domain with field of quotients a number field. Many simplifications in the theory developed for orders occur when Λ is the integral group ring RG. We apply this theory in the case $R = \mathbf{Z}$ and give a connection between R. Oliver's generalised Swan subgroups and Δ-subgroups of permutation lattices. Both these sets of subgroups generate $D(\mathbf{Z}G)$.

Our final specialisation in this chapter is to let $G = \Gamma$ be the Galois group of a Galois extension N/K of number fields. T. Chinburg obtained in this case invariants $\Omega(N/K, i) \in Cl(\mathbf{Z}\Gamma)$ for $i = 1$ to 3 from four-term exact sequences of $\mathbf{Z}\Gamma$-modules. These sequences each induce an equivalence of Tate cohomology with dimension shift 2 of a Galois module U depending on N/K and a standard $\mathbf{Z}\Gamma$-lattice V. Thus the Chinburg invariants are examples of projective invariants of weak homological equivalences. These are the examples which motivated the work of this chapter.

As an application of the theory developed for integral group rings we show that the coset of the Swan subgroup $T(\mathbf{Z}\Gamma)$ — in this case the subgroup H is Γ — containing $\Omega(N/K, 1)$ is represented by the projective invariant of a homomorphism $T \to C_f$ where

T is a standard syzygy of the Γ-trivial lattice $\mathbf{Z}$ and C_f is a finitely generated module introduced by Chinburg which has the Tate cohomology of the idele class group of N.

In the second chapter we concentrate throughout on the Chinburg invariant $\Omega(N/K, 2)$. Again we use a method of obtaining projective invariants from pairs of $\mathbf{Z}G$-modules — the finite group G in the applications is either Γ or a decomposition subgroup of Γ. The method we use is a generalisation of that initiated by A. Fröhlich in the context of abelian groups G (for more details see II §2). This method has its origins in the elegant notion of factorisability introduced by A. Nelson.

Factorisability is essentially a condition imposed on $\mathbf{Z}\Gamma$-lattices U and V which is weaker than local isomorphism. It can be decided by elementary computation. Fröhlich's canonical factorisability is a refinement allowing one to salvage a projective invariant in the class group of a maximal order, or equivalently a coset of $D(\mathbf{Z}\Gamma)$ in $Cl(\mathbf{Z}\Gamma)$, in the case where U is not locally isomorphic to V.

An example of this is where $U = \mathcal{O}_N$ is the ring of integers in N, V is a free $\mathbf{Z}\Gamma$-module of finite index in $\mathcal{O}_N$ and N/K is wildly ramified. We compute in this case an invariant via canonical factorisability and show that the resulting coset of $D(\mathbf{Z}\Gamma)$ is that generated by $\Omega(N/K, 2)$. In the process we establish "modulo $D(\mathbf{Z}\Gamma)$" the conjecture of Chinburg that

$$\Omega(N/K, 2) = t_{N/K}$$

where $t_{N/K}$ is the generalised root number class; sometimes $t_{N/K} \notin D(\mathbf{Z}\Gamma)$. This equality is the conjectural generalisation to wild N/K of M. Taylor's deep result for tame N/K where the stable isomorphism class of $\mathcal{O}_N$ is computed in terms of the Artin root numbers.

This is my PhD thesis at Durham University. I would like to record here my deep indebtedness to Steve Wilson for his impeccable supervision, his unfailing input of ideas and his inexhaustible patience.

To my brother Martin, Jacqueline Gough and Ewan Squires I am profoundly grateful for encouragement when it was most needed.

I would like to thank David Burns and Ted Chinburg for useful comments on an early version of chapter II.

Finally, my thanks also to Graham Robertson for lunchtime discussions of the mysteries of quantum theory...

CHAPTER I. Weak homological equivalences and their projective invariants.

1. Introduction.

Let Λ be a Noetherian ring and let $\mathcal{K}_0(\Lambda)$ denote the Grothendieck group of the category of finitely generated projective Λ-modules. Let M and N be finitely generated Λ-modules and let n be a positive integer. An element f of either of the groups $\mathrm{Hom}_\Lambda(M, N)$ or $\mathrm{Ext}^n_\Lambda(M, N)$, satisfying certain conditions related to the homology of M and N, determines a projective invariant $\partial(f) \in \mathcal{K}_0(\Lambda)$.

This gives a method of obtaining projective invariants from non-projective modules, indeed ones of infinite projective dimension, over a very wide class of rings.

We develop the most general properties of ∂-invariants (the operator ∂ is additive on compositions of maps, the ∂-invariants of Ext are expressible in terms of those of Hom, and ∂ factors through the quotient of of Hom by projective maps) in §§2-3.

In §4 we restrict Λ to be an order in a finite dimensional semisimple $\mathbf{Q}$-algebra, the case we are really interested in. We show that in many cases ∂-invariants can be obtained in the locally free class group $Cl(\Lambda)$ of the order Λ. Indeed, we show that each finitely generated Λ-module M determines a subgroup $\Delta(M)$ (of ∂-invariants of endomorphisms) of the kernel group $D(\Lambda)$ of Λ. The main result of §4 is that $\Delta(M)$ can be determined in terms of reduced norms of local automorphisms of M if M is a Λ-lattice, using the idelic description of $D(\Lambda)$. At opposite extremes, $\Delta(\mathbf{Z}) = T(\mathbf{Z}G)$, the Swan subgroup of $\Lambda = \mathbf{Z}G$ an integral group ring, and $\Delta(M) = D(\Lambda)$ if M is a maximal order containing Λ.

Let R be a Dedekind domain with field of quotients a number field and let G be a finite group. In §5 we examine the case $\Lambda = RG$. Significant simplifications arise in the theory developed for orders. If U is an RG-lattice then a weak homological equivalence $f \in \mathrm{Hom}_{RG}(U, V)$ induces an equivalence of Tate cohomology of U and the RG-module V. Further, the projective invariants of all such weak homological equivalences lie in the coset of $\Delta(U)$ generated by $\partial(f)$. If W is a syzygy of the RG-lattice U then $\Delta(U) = \Delta(W)$.

This theory is applied in §6 in the case $R = \mathbf{Z}$. If H is a subgroup of G — giving rise to the permutation $\mathbf{Z}G$-lattice $\mathbf{Z}[G/H]$ — R. Oliver introduced the generalised Swan subgroup $T_H(\mathbf{Z}G)$ of $D(\mathbf{Z}G)$ and showed in **[Ol]** that all such subgroups generated $D(\mathbf{Z}G)$. We show that

$$T_H(\mathbf{Z}G) \subseteq \Delta(\mathbf{Z}[G/H])$$

and so the $\Delta(\mathbf{Z}[G/H])$ also generate $D(\mathbf{Z}G)$. If H is normal (so $\mathbf{Z}[G/H]$ is a quotient group ring) this inclusion is equality. On the other hand in §7 we give an example of strict inclusion when H is not normal and G is a dihedral group.

The final specialisation (in §6) is to take $G = \Gamma$ the Galois group of a Galois extension N/K of number fields. T. Chinburg (see **[Ch1]**, **[Ch2]**) derived in this case invariants $\Omega(N/K, i)$ for $i = 1$ to 3 from four-term exact sequences of finitely generated $\mathbf{Z}\Gamma$-modules. These we express as ∂-invariants of $\mathrm{Ext}^2_{\mathbf{Z}\Gamma}$ (which have been adjusted to make them rankless). Indeed this situation motivated the work of this chapter. Applying the results of §5 we show that the coset of $T(\mathbf{Z}\Gamma)$ containing $\Omega(N/K, 1)$ is represented by the ∂-invariant of *any* map in $\mathrm{Hom}_{\mathbf{Z}\Gamma}(T, C_f)$ which induces an equivalence of Tate cohomology. Here T is a certain $\mathbf{Z}\Gamma$-lattice and C_f a finitely generated $\mathbf{Z}\Gamma$-module (introduced by Chinburg) with the Tate cohomology of the idele class group of N. Indeed, if Γ is a cyclic group then $T(\mathbf{Z}\Gamma) = 0$ and $T = \mathbf{Z}$, so that $\Omega(N/K, 1)$ equals this ∂-invariant and only depends upon C_f.

We shall return to Chinburg's invariants in the next chapter; this requires new techniques we shall develop there.

§2. Weak equivalence and the ∂-map.

In this section we define weak homological equivalences and the ∂-map and give their basic properties.

Let Λ be any Noetherian ring and let $pd(M)$ denote the projective dimension (whether finite or infinite) of the Λ-module M. Let $\mathcal{K}_0(\Lambda)$ denote the Grothendieck group of the category of finitely generated Λ-modules of finite projective dimension. If L is such a module and $pd(L) = k$ then there is an exact sequence

$$0 \to P_k \to \cdots \to P_0 \to L \to 0$$

where each P_i is a finitely generated projective Λ-module. If we resolve the sequence into short exact sequences, and use the relations in $\mathcal{K}_0(\Lambda)$ (with respect to short exact sequences) then we obtain

$$[L] = \sum_{i=0}^{k}(-1)^i[P_i] \in \mathcal{K}_0(\Lambda),$$

where square brackets are used to denote classes in $\mathcal{K}_0(\Lambda)$. As is well known, this induces a well-defined isomorphism between $\mathcal{K}_0(\Lambda)$ and the Grothendieck group of the category of finitely generated projective Λ-modules. We shall use the symbol $\mathcal{K}_0(\Lambda)$ for both of these groups and identify them under this isomorphism. This will lead to no confusion, as if L is projective then the class $[L]$ in either group is the same under this identification.

If a and b are Λ-maps whose composition ba is defined then there is an exact sequence of Λ-modules

$$0 \to \ker a \to \ker ba \to \ker b \to \operatorname{coker} a \to \operatorname{coker} ba \to \operatorname{coker} b \to 0$$

with maps induced by a and b (see e.g. **[Ba]** I 4.5). We shall refer to this result as "the composition lemma for a and b" in the sequel.

We shall need some notation concerning extensions of Λ-modules; we adopt the viewpoint of MacLane in [Ma].

Suppose that M, N and T are Λ-modules and $n \geq 0$. We regard $\mathrm{Ext}^n_\Lambda(M, N)$ as the set of equivalence classes of n-fold extensions of M by N if $n \geq 1$, and identify $\mathrm{Ext}^0_\Lambda(M, N)$

and $\mathrm{Hom}_\Lambda(M, N)$. Let $f \in \mathrm{Ext}^n_\Lambda(M, N)$. Then f induces maps

$$f^*_k : \mathrm{Ext}^k_\Lambda(N, T) \to \mathrm{Ext}^{n+k}_\Lambda(M, T)$$

for each $k \geq 1$. For the definition of f^*_k see [Ma] Ch. III; refer to §5 p83 if $n = 0$ (the definition of "the composite of the congruence class of a long exact sequence with a matching homomorphism") and §9 p97 if $n \geq 1$ (the definition of "iterated connecting homomorphism").

2.1 Definition: Let k be a positive integer. A class $f \in \mathrm{Ext}^n_\Lambda(M, N)$ is a *weak homological equivalence of level k and grade n* (abbreviated (k,n)-*w.h.e.*) if, for each Λ-module T,

(i) $f^*_k : \mathrm{Ext}^k_\Lambda(N, T) \to \mathrm{Ext}^{k+n}_\Lambda(M, T)$ is surjective, and

(ii) $f^*_{k+1} : \mathrm{Ext}^{k+1}_\Lambda(N, T) \to \mathrm{Ext}^{k+n+1}_\Lambda(M, T)$ is injective.

Write w.h.e. for a (1,0)-w.h.e. in $\mathrm{Hom}_\Lambda(M, N)$, and write $\mathrm{Whe}_\Lambda(M, N)$ for the set of all such w.h.e.s.

2.2 Theorem. *Let k be a positive integer and $f \in \mathrm{Ext}^n_\Lambda(M, N)$. The following are equivalent:*

(i) f is a (k,n)-w.h.e.

(ii) f^*_k is surjective and f^*_l is bijective for each $l > k$

(iii) If n=0, there is an exact sequence of Λ-modules

$$0 \to L \to M \oplus F \overset{(f,g)}{\to} N \to 0,$$

where $pd(L) \leq k-1$, g is some Λ-map and F is a free Λ-module.

If $n > 0$, there is an exact sequence of Λ-modules

$$0 \to N \to L \to F_{n-2} \to \cdots \to F_0 \to M \to 0 \qquad \in f$$

with each F_j free and $pd(L) \leq k$.

Proof : (ii)$\Rightarrow$(i) is trivial.

(i)⇒(iii) If $n = 0$, choose a surjective map $g: F \to N$ where F is a free module. Let $L = \ker(f, g)$. We then have a short exact sequence as in (iii), and have to prove that $\mathrm{pd}(L) \leq k-1$. Apply $\mathrm{Hom}_\Lambda(-, T)$ to obtain a long exact sequence of Ext. The hypotheses on f_k^* and f_{k+1}^* ensure that $\mathrm{Ext}_\Lambda^k(L, T) = 0$, thus (iii) follows.

If $n > 0$, choose a resolution $\mathbf{F} \to M \to 0$ of M by free modules. By the Comparison Theorem ([Ma] Ch. 3 6.1) there is a commutative diagram

$$\begin{array}{ccccccccccc} 0 & \to & Q & \xrightarrow{i} & F_{n-1} & \to \cdots \to & F_0 & \to & M & \to & 0 \\ & & \downarrow h & & \downarrow & & \downarrow & & \| & & \\ 0 & \to & N & \to & T_{n-1} & \to \cdots \to & T_0 & \to & M & \to & 0 \ \in f \end{array}$$

where $Q = \mathrm{im}(F_n \to F_{n-1})$. Thus $\mathrm{Ext}_\Lambda^n(M, N) \cong \mathrm{Hom}_\Lambda(Q, N)/\mathrm{Hom}_\Lambda(F_{n-1}, N) \circ i$. Then let L be the pushout of the maps (i, h), so that we obtain an extension in f as in (iii); this time we have to prove that $\mathrm{pd}(L) \leq k$. Resolving the sequence into short exact sequences, by induction on n the hypotheses on f_k^* and f_{k+1}^* ensure that $\mathrm{Ext}_\Lambda^{k+1}(L, T) = 0$ as required.

(iii)⇒(ii) If $n = 0$, apply $\mathrm{Hom}_\Lambda(-, T)$ to the given short exact sequence; the hypothesis on $\mathrm{pd}(L)$ ensures that (i) holds. Similarly, an easy induction gives the required result for $n > 0$. ∎

2.3 Definition: Let M and N be finitely generated Λ-modules. Let $f \in \mathrm{Hom}_\Lambda(M, N)$ be a $(k, 0)$-w.h.e., then there is a short exact sequence

$$0 \to L \to M \oplus F \xrightarrow{(f,g)} N \to 0 \qquad (f, L, F)$$

with $pd(L) \leq k - 1$, by 2.2 (iii). Since N is finitely generated we can assume the same for the free module F. We say that (f, L, F) is a *sequence for* f.

L is finitely generated, since Λ is Noetherian, so determines a class $[L]$ in $\mathcal{K}_0(\Lambda)$. Define

$$\partial(f) = [F] - [L] \in \mathcal{K}_0(\Lambda).$$

If $f \in \mathrm{Ext}_\Lambda^n(M, N)$ is a (k, n)-w.h.e. for $n > 0$, we call the sequence of 2.2(iii), lying in f, a *sequence for* f, and define

$$\partial(f) = [L] - [F_{n-2}] + \cdots + (-1)^{n-1}[F_0] \in \mathcal{K}_0(\Lambda).$$

We will prove that $\partial(f)$ is well-defined for $(k, 0)$-w.h.e.s next, and for (k, n)-w.h.e.s $(n > 0)$ in 3.5.

2.4 Theorem. *Let M and N be finitely generated Λ-modules. If $f \in \mathrm{Hom}_\Lambda(M, N)$ is a $(k, 0)$-w.h.e. then $\partial(f)$ is independent of the choice of sequence for f.*

Proof : For the moment let us write $\partial(f, g) = [F] - [L]$ to emphasise the chosen g. By symmetry, the lemma follows if we can prove that

$$\partial(f, g) = \partial(f, g \oplus g'),$$

where $g' : F' \to N$ is surjective and F' is finitely generated free.

Let i denote the natural inclusion $M \oplus F \to M \oplus F \oplus F'$. Then $(f, g) = (f, g \oplus g') \circ i$. By the composition lemma for i and $(f, g \oplus g')$ there is an exact sequence

$$0 \to \ker(f, g) \to \ker(f, g \oplus g') \to F' \to 0$$

since i is injective and (f, g) is surjective. Hence

$$\partial(f, g) = [F] - [\ker(f, g)] = [F] + [F'] - [\ker(f, g \oplus g')] = \partial(f, g \oplus g'). \quad \blacksquare$$

2.5 Theorem. *Let k and l be positive integers and let L, M and N be finitely generated Λ-modules. Suppose that $f \in \mathrm{Whe}_\Lambda(L, M)$ is a $(k, 0)$-w.h.e. and $g \in \mathrm{Whe}_\Lambda(M, N)$ is a $(l, 0)$-w.h.e.. Then gf is a $(\max(k, l), 0)$-w.h.e. and*

$$\partial(gf) = \partial(f) + \partial(g).$$

Proof : For each $r \geq 1$, $(gf)^*_r = f^*_r g^*_r$. Compositions of surjective maps are surjective, and similarly for injective maps. The first statement follows by 2.2(ii).

Choose finitely generated free Λ-modules F_1 and F_2 so that there are surjective maps

$$L \oplus F_1 \xrightarrow{a} M \oplus F_2 \xrightarrow{b} N$$

where the component $L \to M$ of a is f and that $M \to N$ of b is g. By the composition lemma for a and b we obtain an exact sequence

$$0 \to \ker a \to \ker ba \to \ker b \to 0 \qquad (*)$$

Let c be the natural surjection $M \oplus F_2 \to M$. By the composition lemma for a and c we obtain an exact sequence

$$0 \to \ker a \to \ker ca \to F_2 \to 0 \qquad (**)$$

Since the F_i are free, $a_r^* = f_r^*$, $b_r^* = g_r^*$ and c_r^* is the identity map for $r \geq 1$. Thus a, b and c are $(m, 0)$-w.h.e.s for various m, and by 2.2(iii) the kernels of these maps have finite projective dimension. Hence the same applies to each module in $(*)$ and $(**)$. Therefore

$$\partial(gf) - \partial(f) - \partial(g) \stackrel{2.3}{=} [F_1] - [\ker ba] - [F_1] + [\ker ca] - [F_2] + [\ker b] \stackrel{(*),\,(**)}{=} 0. \quad \blacksquare$$

§3. Projective Homomorphisms

Let Λ be any ring, and M and N be finitely generated Λ-modules. First we must define projective homomorphisms, as in [CR] Vol. II around 78.10. We also define some related objects, and introduce notation to be used throughout this chapter.

3.1 Definition: A map $f \in \mathrm{Hom}_\Lambda(M, N)$ is a *projective homomorphism* if the map

$$f_1^* : \mathrm{Ext}^1_\Lambda(N, -) \to \mathrm{Ext}^1_\Lambda(M, -)$$

is the zero map for every 2nd variable.

Let $P_\Lambda(M, N)$ denote the subgroup of all projective homomorphisms in $\mathrm{Hom}_\Lambda(M, N)$, and denote the quotient group $\mathrm{Hom}_\Lambda(M, N)/P_\Lambda(M, N)$ by $\mathbf{Hom}_\Lambda(M, N)$.

If D is any left Λ-module we shall write D^* for the right Λ-module $\mathrm{Hom}_\Lambda(D, \Lambda)$.

Define

$$\tau = \tau_{M,N} : M^* \otimes_\Lambda N \to \mathrm{Hom}_\Lambda(M, N)$$

by

$$\tau(f \otimes n) : m \mapsto f(m)n$$

extended by linearity.

Define

$$\mathbf{Ext}^0_\Lambda(M,\, N) = \mathbf{Hom}_\Lambda(M,\, N);$$

$$\mathbf{Ext}^{-1}_\Lambda(M,\, N) = \ker(\tau);$$

$$\mathbf{Ext}^n_\Lambda(M,\, N) = \mathrm{Ext}^n_\Lambda(M,\, N) \text{ for each } n \geq 1;$$

$$\mathbf{Ext}^{-n}_\Lambda(M,\, N) = \mathrm{Tor}^\Lambda_{n-1}(M^*,\, N) \text{ for each } n \geq 2.$$

If $f \in \mathrm{Hom}_\Lambda(M, N)$ denote by $[f]$ the image of f in $\mathbf{Hom}_\Lambda(M,\, N)$.

Denote by $\mathbf{Whe}_\Lambda(M,\, N)$ the image of $\mathrm{Whe}_\Lambda(M,\, N)$ in $\mathbf{Hom}_\Lambda(M,\, N)$.

Remark: In [CR] Vol. I 29.15, it is shown that $\mathrm{im}(\tau) = P_\Lambda(M,\, M)$ in the case $M = N$. The proof given there holds for general N. The **Ext** groups occur in a long exact sequence:

3.2 Theorem. *Suppose we have a short exact sequence of Λ-modules*

$$0 \to A \to B \to C \to 0$$

and that D is a Λ-module. Then there is an exact sequence

$$\cdots \to \mathbf{Ext}^n_\Lambda(D,B) \to \mathbf{Ext}^n_\Lambda(D,C) \to \mathbf{Ext}^{n+1}_\Lambda(D,A) \to \cdots$$

for all integers n. If also $\mathrm{Ext}^1_\Lambda(C,\, \Lambda) = 0$, then there is an exact sequence

$$\cdots \to \mathbf{Ext}^n_\Lambda(B,D) \to \mathbf{Ext}^n_\Lambda(A,D) \to \mathbf{Ext}^{n+1}_\Lambda(C,D) \to \cdots$$

for all integers n.

Proof : By naturality of τ (in the 2nd variable) we have a commutative diagram:

$$\begin{array}{ccccccccc}
\cdots \to & D^* \otimes_\Lambda A & \to & D^* \otimes_\Lambda B & \to & D^* \otimes_\Lambda C & \to & 0 \\
 & \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau} & & \\
0 \to & \mathrm{Hom}_\Lambda(D,\, A) & \to & \mathrm{Hom}_\Lambda(D,\, B) & \to & \mathrm{Hom}_\Lambda(D,\, C) & \to & \cdots
\end{array}$$

By diagram-chasing the first part follows. If $\mathrm{Ext}^1_\Lambda(C,\, \Lambda) = 0$ then the sequence

$$0 \to C^* \to B^* \to A^* \to 0$$

is exact. A similar argument now completes the proof. ∎

The following useful characterisation of projective homomorphisms is adapted from [CR]. We need the finite generation property to obtain classes in $\mathcal{K}_0(\Lambda)$.

3.3 Theorem. *Let $f \in \mathrm{Hom}_\Lambda(M, N)$. Then f is a projective homomorphism if and only if f factors through a finitely generated projective module.*

Proof : It is shown in [CR] Vol. II 78.10 that f is a projective homomorphism if and only if f factors through some projective Q. Since we are assuming that N is finitely generated, we may choose a finitely generated projective P which projects onto N. The universal property of projectives now shows that f factors through P. ∎

Here is the main result in this section, which shows that ∂ factors through the quotient of $\mathrm{Hom}_\Lambda(M, N)$ by projective homomorphisms.

3.4 Theorem. *Let $f \in \mathrm{Hom}_\Lambda(M, N)$ be a $(k, 0)$-w.h.e. and suppose that $f' \in \mathrm{Hom}_\Lambda(M, N)$ is such that*

$$[f] = [f'] \in \mathbf{Hom}_\Lambda(M, N).$$

Then f' is a $(k, 0)$-w.h.e. and $\partial(f) = \partial(f')$.

Proof : Let $f' = f + g$ where $g \in P_\Lambda(M, N)$. Since g factors through some projective P, the induced map g_r^* factors through $\mathrm{Ext}_\Lambda^r(P, -) = 0$ for each $r \geq 1$ and each 2nd variable. Hence $(f')_r^* = f_r^*$ and f' is a $(k, 0)$-w.h.e.. Now choose a finitely generated free module F mapping onto N—as in the proof of 3.3, we find that g factors through F. Say $g = g_2 g_1$, where $g_1 : M \to F$. By 2.4 we can assume that f and f' are surjective. For, if we choose a surjective map $h: F \to N$ then $(f', h) = (f, h) + (g, 0)$ and $(g, 0) \in P_\Lambda(M \oplus F, N)$. Further $\partial(f', h) - \partial(f, h) = \partial(f') - \partial(f)$.

Let t denote transpose. We have $f' = (f, g_2) \circ (1, g_1)^t$. Since the sequence

$$0 \to M \xrightarrow{(1,g_1)^t} M \oplus F \xrightarrow{(-g_1,1)} F \to 0$$

is exact, by the composition lemma for $(1, g_1)^t$ and (f, g_2) we have an exact sequence

$$0 \to \ker f' \to \ker(f, g_2) \to F \to 0.$$

Hence

$$\partial(f) = [F] - [\ker(f, g_2)] = -[\ker f'] = \partial(f'). \quad \blacksquare$$

Using this result, we can now show that $\partial(f)$ does not depend on the choice of sequence for f for $n \geq 1$. Since the 2-extension we will consider in §6 (whose class is a (1,2)-w.h.e.) is not presented as in 2.2, we will prove a stronger result.

3.5 Theorem. *Let $f \in \mathrm{Ext}^n_\Lambda(M, N)$. Then f is a (t, n)-w.h.e. for some t if and only if there is an extension*

$$0 \to N \to T_{n-1} \to \cdots \to T_0 \to M \to 0 \qquad \in f$$

where each T_j is finitely generated, and of finite projective dimension. Moreover $\partial(f)$ does not depend on the choice of sequence for f, and

$$\begin{aligned}\partial(f) &= [\mathbf{T}] \stackrel{def}{=} [T_{n-1}] - [T_{n-2}] + \cdots + (-1)^{n-1}[T_0] \\ &= \partial(h) + [\mathbf{F}],\end{aligned}$$

where $0 \to Q \to \mathbf{F} \to M \to 0$ is a truncated resolution of M as in the proof of 2.2, and h maps to f under the surjection

$$\mathrm{Hom}_\Lambda(Q, N) \to \mathrm{Ext}^n_\Lambda(M, N).$$

Proof : If we take t to be the maximum of the $\mathrm{pd}(T_j)$, it is plain that f is a (t,n)-w.h.e.; the converse holds a fortiori by 2.2(iii).

Choose a surjective map $g: F \to N$ with F a finitely generated free module. We obtain a commutative diagram

$$\begin{array}{ccccccccccccc} 0 & \to & Q \oplus F & \to & F_{n-1} \oplus F & \to & F_{n-2} & \to \cdots \to & F_0 & \to & M & \to & 0 \\ & & \downarrow{\scriptstyle (h,g)} & & \downarrow & & \| & & \| & & \| & & \\ 0 & \to & N & \to & L & \to & F_{n-2} & \to \cdots \to & F_0 & \to & M & \to & 0 \end{array} \qquad (*)$$

in which all the vertical arrows are surjective. It follows immediately that $\ker(h, g)$ has finite projective dimension, h is a $(k, 0)$-w.h.e. where $k = pd(L)$, and $\partial(f) = \partial(h) + [\mathbf{F}]$. A more laborious argument, in which we add free modules to each F_j, establishes the same result with [T] replacing $\partial(f)$. Thus $[\mathrm{T}] = \partial(f)$. Since

$$\mathrm{Ext}^n_\Lambda(M, N) \cong \mathrm{Hom}_\Lambda(Q, N)/\mathrm{Hom}_\Lambda(F_{n-1}, N) \circ i,$$

where i is the map $Q \to F_{n-1}$, and the denominator consists of projective homomorphisms, by 3.4 it follows that $\partial(h)$ does not depend on the choice of h in the diagram. ∎

§4. Application to orders in semi-simple algebras.

In this section we assume throughout that R is a Dedekind ring with field of quotients the algebraic number field K ($\neq R$), and that Λ is an R-order in the finite dimensional semisimple K-algebra A. Write 'Λ-lattice' for 'finitely generated R-torsion-free Λ-module'. Note that if M is a Λ-lattice then the map $M \to K \otimes_R M$ is injective and we write KM for $K \otimes_R M$. Denote by $\Delta_\Lambda(M) = \Delta(M)$ the set of invariants $\partial(\mathrm{Whe}_\Lambda(M, M))$ for any finitely generated Λ-module M.

4.1 Theorem. *Let M and N be finitely generated Λ-modules. Then*

(i) $\mathbf{Hom}_\Lambda(M, N)$ *is finite;*

(ii) Localisation (or completion) gives a natural isomorphism

$$l_{M,N}: \mathbf{Hom}_\Lambda(M, N) \cong \bigoplus_P \mathbf{Hom}_{\Lambda_P}(M_P, N_P),$$

where the direct sum is taken over the maximal ideals P of R;

(iii) $\mathbf{Whe}_\Lambda(M, M) = \mathbf{End}_\Lambda(M)^\times$;

(iv) If M and N are locally isomorphic, then $\mathrm{Whe}_\Lambda(M, N)$ *and* $\mathrm{Whe}_\Lambda(N, M)$ *are non-empty. Choose $f \in \mathrm{Whe}_\Lambda(M, N)$. Then $l_{M,N}[f]$ is represented by a local isomorphism. Further*

$$\mathbf{Whe}_\Lambda(M, N) = [f] \circ \mathbf{End}_\Lambda(M)^\times$$

and

$$\partial(\mathrm{Whe}_\Lambda(M, N)) = \partial(f) + \Delta(M)$$

Given f as above, there exists some $f' \in \mathrm{Whe}_\Lambda(N, M)$ such that $[f \circ f'] = [1_N]$ and $[f' \circ f] = [1_M]$, and then $\partial(f) = -\partial(f')$.

Proof of (i): Choose an exact sequence

$$0 \to L \to F \to N \to 0$$

where F is a finitely generated free Λ-module. By 3.2 there is an exact sequence

$$\mathbf{Hom}_\Lambda(M, F) \to \mathbf{Hom}_\Lambda(M, N) \to \mathrm{Ext}^1_\Lambda(M, L) \to \mathrm{Ext}^1_\Lambda(M, F) \qquad (*)$$

and the first term vanishes since F is projective. So $\mathbf{Hom}_\Lambda(M, N)$ injects into the R-module $\mathrm{Ext}^1_\Lambda(M, L)$, which is R-torsion since A is semisimple. Since all our modules are finitely generated, (i) follows.

Proof of (ii): Naturality of localisation gives a commutative diagram (stemming from $(*)$):

$$\begin{array}{ccccccc} 0 & \to & \mathbf{Hom}_\Lambda(M, N)_P & \to & \mathrm{Ext}^1_\Lambda(M, L)_P & \to & \mathrm{Ext}^1_\Lambda(M, F)_P \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & \mathbf{Hom}_{\Lambda_P}(M_P, N_P) & \to & \mathrm{Ext}^1_{\Lambda_P}(M_P, L_P) & \to & \mathrm{Ext}^1_{\Lambda_P}(M_P, F_P) \end{array},$$

in which the rows are exact and the middle and right-hand vertical arrows are isomorphisms. Hence so is the left-hand vertical arrow. Since we are dealing with finite quotients, we could complete instead of localise at this point. The Chinese remainder theorem now completes the proof of (ii).

Proof of (iii): An element of a finite ring whose right annihilator is zero is a unit. Then suppose that $[h] \in \mathbf{Whe}_\Lambda(M, M)$ and that $[hg] = [0]$ for some $g \in \mathrm{End}_\Lambda(M)$, i.e. $hg \in P_\Lambda(M, M)$. Then $g^*h^* = (hg)^*: \mathrm{Ext}^1_\Lambda(M, -) \to \mathrm{Ext}^1_\Lambda(M, -)$ is the zero map for each 2nd variable. But h^* is surjective hence $g^* = 0$. Thus $g \in P_\Lambda(M, M)$ and $[g] = [0]$ which gives (iii).

Proof of (iv): Choose a local isomorphism i from M to N. Clearly $l_{M,N}^{-1}[i]$ and $l_{N,M}^{-1}[i^{-1}]$ are w.h.e.'s. Then $l[f] = [i] \circ [i^{-1}] \circ l[f]$, and the P-component of $[i^{-1}] \circ l[f]$ lies in $\mathbf{End}_{\Lambda_P}(M_P)^{\times}$ by (iii). But $\mathrm{End}_{\Lambda_P}(M_P)$ is semi-local, so a unit of $\mathbf{End}_{\Lambda_P}(M_P)$ lifts to a unit of $\mathrm{End}_{\Lambda_P}(M_P)$, by [Ba] III 2.9. Thus $[i^{-1}] \circ l[f] = [h]$ where h is a local automorphism of M. Consequently f is represented by a local isomorphism, j say. It follows that $[f]$ is invertible with $[f'] = l_{N,M}^{-1}[j^{-1}]$. The remaining properties are now obvious. ∎

It is well-known that any maximal order Λ' of A is hereditary. Thus, $pd(L) \leq 1$ for any finitely generated Λ'-module L, hence L gives a class $[L]$ in $\mathcal{K}_0(\Lambda')$. The following result shows that the image of $\partial(f)$ in $\mathcal{K}_0(\Lambda')$ for any $f \in \mathrm{Whe}_\Lambda(M, N)$ is a constant, only depending on M and N.

4.2 Theorem. *Let M and N be finitely generated Λ-modules. Let Λ' be a maximal order of A containing Λ. Write G for the functor $\Lambda' \otimes_\Lambda -$. Then, if $f \in \mathrm{Whe}_\Lambda(M, N)$,*

$$\mathcal{K}_0 G(\partial(f)) = [\Lambda' \otimes_\Lambda N] - [\Lambda' \otimes_\Lambda M] \in \mathcal{K}_0(\Lambda').$$

Proof : Choose a sequence (f, L, F) for f. Applying G, we obtain an exact sequence

$$\mathrm{Tor}_1^\Lambda(\Lambda', N) \to \Lambda' \otimes_\Lambda L \to \Lambda' \otimes_\Lambda M \oplus \Lambda' \otimes_\Lambda F \to \Lambda' \otimes_\Lambda N \to 0$$

But $\Lambda' \otimes_\Lambda L$ is Λ'-projective, (since L is Λ-projective) hence R-torsion-free, and $\mathrm{Tor}_1^\Lambda(\Lambda', N)$ is R-torsion since A is semisimple. Hence we can replace the left hand term by zero, and then

$$\mathcal{K}_0 G(\partial(f)) = [\Lambda' \otimes_\Lambda F] - [\Lambda' \otimes_\Lambda L] = [\Lambda' \otimes_\Lambda N] - [\Lambda' \otimes_\Lambda M]$$

as required. ∎

Now we introduce $\mathcal{K}_0^{lf}(\Lambda)$, $Cl(\Lambda)$ and $D(\Lambda)$. Let Q be a finitely generated projective Λ-module. Q is *locally free of rank* k if $Q_P \cong \Lambda_P^k$ for every non-zero prime ideal P of R. Define $\mathcal{K}_0^{lf}(\Lambda)$ to be the subgroup of $\mathcal{K}_0(\Lambda)$ generated by each $[Q]$, where Q is a locally free Λ-module of finite rank.

There is a map $rk\colon \mathcal{K}_0^{lf}(\Lambda) \to \mathbf{Z}$ induced by the rank of a locally free module. We define $Cl(\Lambda) = \ker(rk)$, the *class group* of Λ. It consists of elements $[M] - [N]$ with M and N locally free of equal rank. The map $[Q] \to [\Lambda' \otimes_\Lambda Q]$ induces a surjection $Cl(\Lambda) \to Cl(\Lambda')$

where Λ' is any maximal order of A containing Λ. Let $D(\Lambda)$—the kernel group of Λ—denote the kernel of this surjection. Regardless of the choice of Λ', we find that $D(\Lambda)$ is uniquely determined. These results are easily proved using the idelic description of the class group, due to Fröhlich, which we outline below.

Write $C = Z(A)$, the centre of A, throughout the remainder of this section. There is a well-known isomorphism

$$Cl(\Lambda) \cong \frac{J(C)}{C^{\times}\nu(U(\Lambda))}.$$

(See [Ta] Chapter 1; here we write $J(C)$ for the ideles of C, $U(\Lambda)$ for the unit ideles of Λ, and ν for reduced norm from A into C, extended continuously to all idelic constructions.)

Following Wilson (c.f. [Wil] §2) denote by cls the canonical map $J(C) \to Cl(\Lambda)$. We will use the following notation from now on: let M be a Λ-lattice and let $h \in \mathrm{Whe}_{\Lambda}(M, M)$. Write $V = KM$, $\Theta = \mathrm{End}_{\Lambda}(M)$ and $B = \mathrm{End}_{A}(V)$. We will devote the remainder of this section to proving that $\partial(h) = \mathrm{cls}(\nu\beta) \in D(\Lambda)$ for some $\beta \in U(\Theta)$. Note that $Z(B)$ is naturally embedded in C. For, C maps onto $Z(B)$ by multiplication maps $V \to V$. This surjection, restricted to simple components corresponding to simple A-modules occuring in V, is an isomorphism. The inverse of this isomorphism embeds $Z(B)$ in C.

4.3 Lemma. *There exists $\beta \in U(\Theta)$ such that $[\beta_P] = [h_P]$ for every place P of K.*

Proof : The lemma follows directly from 4.1(iv) after observing that a local automorphism β of M is just an element of $U(\Theta)$, if we adopt the convention that the infinite components are equal to 1. Note that $\Lambda_P = A_P$ at infinite places P, so by semisimplicity every Λ_P-map is projective. Hence the statement of the lemma places no restrictions on the infinite components of β. ∎

We find it convenient to prove the results first when M is a full lattice in a free A-module. So let W be an A-module such that there is an isomorphism $f: V \oplus W \xrightarrow{\sim} A^k$.

For each place P, if β is as in 4.3, then β_P extends uniquely to an element of $(B_P)^{\times}$. Write $\beta \oplus 1$ for the idele of $J(\mathrm{End}_A(V \oplus W))$ such that $(\beta \oplus 1)_P = \beta_P \oplus 1: V_P \oplus W_P \xrightarrow{\sim} V_P \oplus W_P$.

4.4 Lemma. *Choose β as in 4.3, and let $\alpha = f(\beta \oplus 1)f^{-1} \in J(\mathrm{Mat}_k(A))$. Then $\nu\beta = \nu\alpha \in J(C)$.*

Proof : It suffices to show that $(\nu\beta)_P = (\nu\alpha)_P$ at each P. So we change notation for the local case. Now $\alpha \in GL_k(A)$ and $\beta \in B^\times$. The diagram

$$\begin{array}{ccc} B^\times & \xrightarrow{\nu} & Z(B)^\times \\ \downarrow & & \downarrow \\ \mathcal{K}_1(A) & \xrightarrow{\nu} & C^\times \end{array}$$

commutes, where the left hand vertical arrow is the map $c \mapsto [V, c]$ for $c \in \mathrm{Aut}_A V = B^\times$, and the right hand vertical arrow is the embedding on unit groups induced by the embedding $Z(B) \to C$ described above. However, the diagram

$$\begin{array}{ccc} V \oplus W & \xrightarrow{f} & A^k \\ \downarrow{\scriptstyle \beta\oplus 1} & & \downarrow{\scriptstyle f(\beta\oplus 1)f^{-1}} \\ V \oplus W & \xrightarrow{f} & A^k \end{array}$$

also commutes, hence $[V, \beta] = [V \oplus W, \beta \oplus 1] = [A^k, f(\beta \oplus 1)f^{-1}]$, using the relations in $\mathcal{K}_1(A)$. By commutativity, identifying $\mathbf{Z}(B)^\times$ with its image in $C^\times$, it follows that $\nu\beta = \nu\alpha$. ∎

Choose a full Λ-lattice N in W, and set $L = f(M \oplus N)$, a full lattice in A^k. Then $f(h \oplus 1)f^{-1} \in \mathrm{End}_\Lambda(L)$.

4.5 Lemma. *$f(h \oplus 1)f^{-1}$ is a w.h.e. and $\partial(h) = \partial(f(h \oplus 1)f^{-1})$.*

Proof : Choose a surjective map $g: F \to M$ where F is finitely generated free. The diagram

$$\begin{array}{ccccccccc} 0 & \to & M \oplus F & \to & M \oplus N \oplus F & \to & N & \to & 0 \\ & & \downarrow{\scriptstyle (h,g)} & & \downarrow{\scriptstyle (h\oplus 1,g)} & & \| & & \\ 0 & \to & M & \to & M \oplus N & \to & N & \to & 0 \end{array}$$

commutes, where the rows are the natural split exact sequences. By the Snake lemma $\ker(h, g) \cong \ker(h \oplus 1, g)$, hence $\partial(h) = \partial(h \oplus 1)$. Changing notation, we may assume that $N = 0$, and it suffices to prove that $\partial(h) = \partial(fhf^{-1})$. The diagram

$$\begin{array}{ccc} M \oplus F & \overset{f\oplus 1}{\xrightarrow{\cong}} & L \oplus F \\ \downarrow{\scriptstyle (h,g)} & & \downarrow{\scriptstyle (fhf^{-1},fg)} \\ M & \overset{f}{\xrightarrow{\cong}} & L \end{array}$$

commutes. Thus $\ker(h, g) \cong \ker(fhf^{-1}, fg)$ and the result follows. ∎

We need a further lemma concerning injective w.h.e.s. This lemma will also be used in §5. We temporarily relax our assumptions on M and N in the statement of the lemma.

4.6 Lemma. *Let M and N be finitely generated Λ-modules and suppose that there exists some injective map $h \in \mathrm{Hom}_\Lambda(M, N)$. Then*

(i) h is a w.h.e. if and only if $pd(\mathrm{coker}\, h) \leq 1$. If h is a w.h.e. then $\partial(h) = [\mathrm{coker}\, h]$.

(ii) If M is a Λ-lattice and $f \in \mathrm{Hom}_\Lambda(M, N)$ then there exists an injective map $g \in \mathrm{Hom}_\Lambda(M, N)$ such that $[f] = [g]$.

Proof : For (i), choose a surjective map $k: F \to N$ where F is finitely generated free. Then $h = (h, k) \circ i$ where i is the natural inclusion $M \to M \oplus F$. By the composition lemma for i and (h, k) there is an exact sequence

$$0 \to \ker(h, k) \to F \to \mathrm{coker}\, h \to 0$$

Thus h is a w.h.e. if and only if $\ker(h, k)$ is projective, which occurs if and only if $pd(\mathrm{coker}\, h) \leq 1$. If h is a w.h.e. then

$$\partial(h) = [F] - [\ker(h, k)] = [\mathrm{coker}\, h]$$

and (i) holds.

For (ii), let t be the order of the finite group $\mathbf{Hom}_\Lambda(M, N)$. Let $f_a = f + ath$ for each positive integer a. If $a \neq a'$ then $\ker(f_a) \cap \ker(f_{a'}) = 0$ since th is injective. But there are infinitely many lattices $\ker(f_a)$ and M is finitely generated. Hence almost all of the f_a are injective. But $[f] = [f_a]$ and so (ii) follows. ∎

4.7 Theorem. *Let M be a Λ-lattice, and $\Theta = \mathrm{End}_\Lambda(M)$. The following diagram commutes:*

$$\begin{array}{ccc} U(\Theta) & \xrightarrow{\mathrm{cls} \circ \nu} & Cl(\Lambda) \\ & \searrow \quad\quad \nearrow \partial & \\ & \mathbf{Whe}_\Lambda(M, M) & \end{array}$$

where the unlabelled diagonal arrow is the natural one induced by the surjection $U(\Theta) \to \oplus_P \mathbf{End}_{\Lambda_P}(M_P)^\times$ and the isomorphism in 4.1 with $M = N$.

Proof: We have to show that $\partial(h) = \mathrm{cls}(\nu\beta)$ where β is chosen as in 4.3. Since $[\beta_P] = [h_P]$ at every P, it is immediate that $[\alpha_P] = [h'_P]$ where $h' = f(h \oplus 1)f^{-1}$ (note that α_P is a local isomorphism $L_P \to L_P$). By 4.5 $\partial(h) = \partial(h')$. Hence we may assume that $L = M$ and $\beta = \alpha$, i.e. that M is a full lattice in A^k. We now complete the proof using similar ideas to **[Wi2]** §5. Let S be a non-empty finite set of prime numbers, containing all primes p where Λ_p is not a maximal order. Choose any locally free sub-lattice X of M (with finite index in M) such that $X_p = M_p$ whenever $p \notin S$. This is possible, because for $p \notin S$ Λ_p is a maximal order. Hence the isomorphism class of M_p is determined by $\mathbb{Q}_p M_p = A_p^k$. Thus $M_p \cong \Lambda_p^k$.

Then let $Y = \alpha X$. Let c be a positive integer divisible by $|M/Y|$ and all primes in S. By weak approximation, choose $g \in \mathrm{End}_\Lambda(M)$ such that $g_p \equiv \alpha_p \pmod{c\mathrm{End}_{\Lambda_p}(M_p)}$ for every p in S. If $p \in S$ then α_p is an automorphism, hence g_p is an automorphism mod p, and hence an automorphism by [B] III 2.7 (since $p\mathrm{End}_{\Lambda_p}(M_p) \subseteq \mathrm{rad}\,\mathrm{End}_{\Lambda_p}(M_p)$). Thus $(\ker g)_p = \ker(g_p) = 0$ and $\ker g$ is finite (since S is non-empty). But M is a lattice, hence g is injective. Suppose that F is a finitely generated free Λ-module and there is an exact sequence

$$0 \to G \to F \to \operatorname{coker} g \to 0.$$

If $p \in S$ then $(\operatorname{coker} g)_p = \operatorname{coker}(g_p) = 0$ and so $G_p \cong F_p$ is free. If $p \notin S$ then Λ_p is hereditary and so G_p is projective. Hence G is projective. Thus $pd(\operatorname{coker} g) \leq 1$ and by 4.6(i) g is a w.h.e. and

$$(i) \qquad \partial(g) = [\operatorname{coker} g].$$

We claim that

(ii) $g^{-1}(Y) = X$;

(iii) $g(M) + Y = M$.

For (ii), it suffices to prove that $g_p^{-1}(Y_p) = X_p$ for each p. If $p \notin S$ then $Y_p = X_p = M_p$ so the result is clear. If $p \in S$ then

$$g_p(X_p) \subseteq \alpha_p(X_p) + cM_p \qquad \text{by choice of } g$$

$$= Y_p + cM_p \subseteq Y_p \qquad \text{by choice of c.}$$

But both g_p and α_p are isomorphisms so

$$\left|\frac{M_p}{g_p(X_p)}\right| = \left|\frac{M_p}{X_p}\right| = \left|\frac{M_p}{\alpha_p(X_p)}\right| = \left|\frac{M_p}{Y_p}\right|$$

therefore $g_p(X_p) = Y_p$ as required.

For (iii), it suffices to show that $g_p(M_p) + Y_p = M_p$ for each p. This is obvious since in each case either $g_p(M_p) = M_p$ or $Y_p = M_p$. Thus

$$\partial(g) \overset{(i)}{=} [M/g(M)] \overset{(iii)}{=} [Y/Y \cap g(M)] \overset{(ii)}{=} [Y/g(X)]$$

(iv)

$$= [Y] - [X] \qquad \text{since } g \text{ is injective.}$$

Now $[h_p] = [\alpha_p] = [g_p]$ for each $p \in S$. Further, if $p \notin S$ then h_p and g_p are projective homomorphisms (since M_p is projective). Thus by 4.1(ii) $[h] = [g]$. Thus by 3.4

$$\partial(h) = \partial(g) \overset{(iv)}{=} [\alpha X] - [X] = \operatorname{cls} \nu\alpha. \quad \blacksquare$$

Remark: By 4.1(iv) a similar result holds when M and N are full lattices in V which are in the same genus, rather than taking $M = N$ as in 4.7. However with $M = N$ we have the following refinement.

4.8 Theorem. *Let M be a Λ-lattice. Then $\Delta(M)$ is a subgroup of $D(\Lambda)$.*

Proof : By 2.5 $\Delta(M)$ is closed under addition. Clearly $\partial(1) = 0$ and by 4.1(iii) we have inverses. So $\Delta(M)$ is a subgroup of $Cl(\Lambda)$, by 4.7. The result now follows from 4.2. $\blacksquare$

More generally we have

4.9 Theorem. *Let M and N be finitely generated Λ-modules in the same genus and let $f \in \mathrm{Whe}_\Lambda(M, N)$. Then $\partial(f) \in Cl(\Lambda)$. If $M = N$ then $\Delta(M)$ is a subgroup of $D(\Lambda)$.*

Proof : By 2.5 and 4.2 the second statement follows from the first. For the first statement, choose a sequence

$$0 \to L \to M \oplus F \overset{(f,g)}{\to} N \to 0$$

for f. It suffices to show that L is locally free. Changing notation for the local case, we have to show that L is free. Let $J = \operatorname{rad} \Lambda$ and let $\overline{\Lambda} = \Lambda/J$. For brevity write $\overline{X}$ for

$\overline{\Lambda} \otimes_{\Lambda} X$. By right exactness of tensor there is an exact sequence of $\overline{\Lambda}$-modules

$$(4.10) \qquad \overline{L} \rightarrow \overline{M} \oplus \overline{F} \overset{(\overline{f}, \overline{g})}{\rightarrow} \overline{N} \rightarrow 0.$$

Let $T = \ker(\overline{f}, \overline{g})$. Since $\overline{\Lambda}$ is semisimple, the surjection $(\overline{f}, \overline{g})$ in 4.10 is split, hence

$$(4.11) \qquad T \oplus \overline{N} \cong \overline{M} \oplus \overline{F}.$$

$\overline{\Lambda}$ is also Artinian, and $M \cong N$ by hypothesis. Hence $T \cong \overline{F}$ by the Krull-Schmidt theorem (in other words we can cancel $\overline{M}$ and $\overline{N}$ in 4.11). Thus the surjection $\overline{L} \rightarrow T$ coming from 4.10 induces a surjection $\overline{L} \rightarrow \overline{F}$. By Nakayama's lemma this lifts to a surjection $L \rightarrow F$ (see e.g. **[Ba]** III proof of 2.12). Because F is free, this surjection is split. Comparing ranks, $F \cong L$ as required. ∎

§5. Applications to Group Rings.

In this section we let R be a Dedekind ring with field of quotients K ($\neq R$) an algebraic number field. Also let G be a finite group and $\Lambda = RG$ be the integral group ring. We write $\widehat{H}^*(G, M)$ for Tate cohomology with coefficients in a Λ-module M. We call M *cohomologically trivial* if $\widehat{H}^n(G, M) = 0$ for all integers n.

5.1 Theorem. *The following conditions on an RG-module M are equivalent.*

(i) M is cohomologically trivial;

(ii) $pd(M) \leq 1$;

(iii) $pd(M) < \infty$.

Proof : **[Br]** VI 8.12 for the case $R = \mathbf{Z}$. The general case is similar. ∎

We shall now give a number of results which are specific to orders which are group rings.

5.2 Theorem. *Let M be a Λ-lattice and N a finitely generated Λ-module. Let τ be the map of 3.1, and write* $X = \mathrm{Hom}_R(M, N)$. *Then* $\widehat{H}^n(G, X) \cong \mathbf{Ext}^n_{\Lambda}(M, N)$ *for each* $n \in \mathbf{Z}$. *In particular* $\widehat{H}^0(G, X) = \mathbf{Hom}_{\Lambda}(M, N)$ *and* $\widehat{H}^{-1}(G, X) \cong \ker(\tau)$.

Proof : The special cases can be extracted from the proof of (29.18) in **[CR]** Vol. I — once again the proof for $M = N$ generalises. The remainder is well-known (see for example **[Br]** Ch. III 2.2). ∎

5.3 Theorem. *Let M and N be as in 5.2 and let $f \in \mathrm{Hom}_\Lambda(M, N)$. The following are equivalent:*

(i) f is a w.h.e.;

(ii) f is a $(k,0)$-w.h.e. for some positive integer k;

(iii) $f_*: \widehat{H}^n(\Delta, M) \to \widehat{H}^n(\Delta, N)$ is an isomorphism for each $n \in \mathbf{Z}$ and for all subgroups Δ of G.

Proof : (i)⇒(ii) is trivial by 2.2. For f as in (ii), choose a sequence (f, L, F) for f; by 2.2 $pd(L)$ is finite. By 5.1 L is cohomologically trivial, which implies (iii) by taking the Tate cohomology of (f, L, F). Conversely, if (iii) holds, choose a finitely generated free module F mapping onto N, so we obtain a short exact sequence (f, L, F), where we do not yet know that L is projective. Taking the Tate cohomology of (f, L, F), we find that L is a cohomologically trivial Λ-lattice, hence is projective by [CF] IV Theorem 8. ∎

Remark: If we drop the condition that M is a Λ-lattice, we find that the theorem follows if (i) and (ii) are modified as follows:

(i) f is a $(2,0)$-w.h.e., (ii) f is a $(k,0)$-w.h.e. for some integer $k \geq 2$.

This follows by 5.1. If we further suppose that f is a (k,n)-w.h.e. (where $n > 0$) it follows that f is a $(1,n)$-w.h.e., by 2.2(iii) and 5.1.

The following property of group rings will be used repeatedly (see [CR] Vol. I §37 example(i) after 37.8 or [Br] VI §8 Ex. 3(a))

5.4 $\mathrm{Ext}^1_\Lambda(M, P) = 0$ if M and P are Λ-lattices, and P is projective.

Next we show that the coset properties of w.h.e.'s in 4.1(iv) hold more generally for group rings.

5.5 Theorem. *Let M and N be as in 5.2 and let $f \in \mathrm{Whe}_\Lambda(M, N)$. Then*

$$\mathbf{Whe}_\Lambda(M, N) = [f] \circ \mathbf{End}_\Lambda(M)^\times$$

and

$$\partial(\mathrm{Whe}_\Lambda(M, N)) = \partial(f) + \Delta(M).$$

Proof : The second property follows from the first. Choose a sequence (f, L, F) for f. By 3.2 we obtain an exact sequence

$$0 \to \mathbf{End}_\Lambda(M) \to \mathbf{Hom}_\Lambda(M, N) \to \mathrm{Ext}^1_\Lambda(M, L)$$

since L and F are projective. By 5.4 the right hand group vanishes and the first property follows. ∎

There is a strong connection between Λ-lattices connected by a w.h.e., which provides a partial converse to 4.1(iv), since projectives are locally free over group rings, by a theorem of R. G. Swan.

Definition: Let M and N be Λ-modules. Then M and N are *projectively equivalent* if

$$M \oplus P \cong N \oplus Q$$

where P and Q are projective Λ-modules.

5.6 Theorem. *Suppose that both M and N are Λ-lattices. Then* $\mathrm{Whe}_\Lambda(M, N)$ *is non-empty if and only if M and N are projectively equivalent.*

Proof : "if" is clear, for an isomorphism $M \oplus P \cong N \oplus P'$, where P and P' are projective, induces a w.h.e. $M \to N$ since the other component-wise maps are all projective.

For the converse, given $f \in \mathrm{Whe}_\Lambda(M, N)$, any sequence (f, L, F) for f splits by 5.4, giving the required equivalence $M \oplus F \cong N \oplus L$. ∎

The following result will be used in §6. First we introduce some notation for connecting homomorphisms (taken from [Ma] III Lemmas 1.2 and 1.4). For this we allow M, N, L and T to be any Λ-modules. Choose $\psi \in \mathrm{Ext}^1_\Lambda(M, N)$ and $f \in \mathrm{Hom}_\Lambda(L, M)$. Define $\psi f \in \mathrm{Ext}^1_\Lambda(L, N)$ as follows. Choose an extension

$$0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} M \to 0 \qquad \in \psi$$

Let P be the pullback of (f, β). There is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & N & \to & P & \to & L & \to & 0 \\ & & \| & & \downarrow & & \downarrow f & & \\ 0 & \to & N & \xrightarrow{\alpha} & E & \xrightarrow{\beta} & M & \to & 0 \end{array}$$

and the class of the top row is ψf, depending only on ψ and f. Similarly define $h\psi \in \mathrm{Ext}^1_\Lambda(M, T)$ for each $h \in \mathrm{Hom}_\Lambda(N, T)$ using the pushout of (α, h). We have $(\psi f_1)f_2 = \psi(f_1 f_2)$ and $g_1(g_2\psi) = (g_1 g_2)\psi$, and also ([Ma] III Lemma 1.6) $(g\psi)f = g(\psi f)$. Accordingly we write $\psi f_1 f_2$, etc. unambiguously.

5.7 Theorem. *Let N be an n-syzygy of the Λ-lattice M. Then there is a ring isomorphism $r\colon \mathbf{End}_\Lambda(M) \cong \mathbf{End}_\Lambda(N)$ such that $\partial[f] = (-1)^n \partial(r[f])$ for each $f \in \mathrm{Whe}_\Lambda(M, M)$ (where we extend the ∂-map to $\mathbf{Whe}_\Lambda(M, M)$ unambiguously by 3.4). In particular $\Delta(N) = \Delta(M)$.*

Proof : Breaking up an n-fold extension of M by N with projective middle modules into short exact sequences, it suffices by induction to prove the result for a 1-syzygy N. Then let

$$0 \to N \xrightarrow{\gamma} P \xrightarrow{\delta} M \to 0 \qquad \in \psi$$

be an extension with P projective. Since M is a Λ-lattice, using 5.4 we can apply 3.2 to obtain long exact sequences

(5.8) $$\cdots \to \mathbf{Ext}^n_\Lambda(-, P) \to \mathbf{Ext}^n_\Lambda(-, M) \to \mathbf{Ext}^{n+1}_\Lambda(-, N) \to \cdots$$

and

(5.9) $$\cdots \to \mathbf{Ext}^n_\Lambda(P, -) \to \mathbf{Ext}^n_\Lambda(N, -) \to \mathbf{Ext}^{n+1}_\Lambda(M, -) \to \cdots$$

Since P is projective, $\mathbf{Hom}_\Lambda(M, P) = 0 = \mathrm{Ext}^1_\Lambda(M, P)$, the last equality by 5.4. Then by 5.8 with $n = 0$ and variable M there is an isomorphism

(5.10)
$$\alpha\colon \mathbf{End}_\Lambda(M) \xrightarrow{\simeq} \mathrm{Ext}^1_\Lambda(M, N)$$
by
$$[f] \mapsto \psi f,$$

by the definition of the connecting homomorphism. Similarly by 5.9 with $n = 0$ and variable N we obtain an isomorphism

(5.11)
$$\beta\colon \mathbf{End}_\Lambda(N) \simeq \mathbf{Ext}^1_\Lambda(M, N)$$
by
$$[g] \mapsto g\psi.$$

Put $r = \beta^{-1}\alpha$. It suffices to show that r is a ring map, and that if f is as given then $\partial[f] = -\partial(r[f])$.

Let $f_1, f_2 \in \mathrm{End}_\Lambda(M)$. Choose $h \in \mathrm{End}_\Lambda(N)$ such that $h\psi = \psi f_1 f_2$, using 5.10 and 5.11. Similarly choose $h_i \in \mathrm{End}_\Lambda(N)$ such that $h_i\psi = \psi f_i$ for $i = 1, 2$. Then

$$h\psi = \psi f_1 f_2 = h_1\psi f_2 = h_1 h_2 \psi.$$

Applying β^{-1}, we see that $r[f_1 f_2] = [h] = [h_1 h_2] = r[f_1]r[f_2]$.

For the last part, we may assume by 4.6 that f is injective, and $\partial(f) = [\mathrm{coker}\, f]$. Let E be the pullback of (f, δ). Since f is injective, so is the induced map $E \to P$ and there is an exact sequence

$$0 \to E \to P \to \mathrm{coker}\, f \to 0.$$

Thus $pd(E) < \infty$. By 4.6 and 5.11 we can choose an injective map $g \in \mathrm{End}_\Lambda(N)$ such that $g\psi = \psi f$. Thus E is isomorphic to the pushout of (g, γ) and there is an exact sequence

$$0 \to P \to E \to \mathrm{coker}\, g \to 0.$$

Thus $pd(\mathrm{coker}\, g) < \infty$ and g is a w.h.e. (this is also a consequence of 4.1(iii)). But $[g] = r[f]$. Thus

$$\partial(r[f]) = [\mathrm{coker}\, g] = [E] - [P] = -[\mathrm{coker}\, f] = -\partial(f) \quad \blacksquare$$

§6. Swan Modules.

Let $\Lambda = \mathbf{Z}G$ be the integral group ring of a finite group G and let H be a normal subgroup of G. There is a Cartesian square

$$\begin{array}{ccc} \mathbf{Z}G & \stackrel{\epsilon_H}{\to} & \mathbf{Z}[G/H] \\ \downarrow & & \downarrow{\scriptstyle \pi_H} \\ \mathbf{Z}[G/(\sigma_H)] & \to & J_n[G/H] \end{array}$$

where $n = |H|$, $J_n = \mathbf{Z}/n\mathbf{Z}$ and $\sigma_H = \sum_{h\in H} h \in \mathbf{Z}H$. The corresponding Mayer-Vietoris sequence (see **[RU]**) is

$$J_n[G/H]^\times \stackrel{\delta_H}{\to} D(\mathbf{Z}G) \to D(\mathbf{Z}[G/H]) \oplus D(\mathbf{Z}[G/(\sigma_H)]) \to 0 \qquad (MV)$$

6.1 Definition: (see [CR] Vol. II §53 or [Ol]) $T_H(\mathbf{Z}G) = \mathrm{im}(\delta_H)$ is the Swan subgroup of $\mathbf{Z}G$ relative to H. When $H = G$ we write simply $T(\mathbf{Z}G)$, and this group is known as the Swan subgroup.

Let $\Lambda' = \mathbf{Z}[G/H]$, $\Lambda'' = \mathbf{Z}[G/(\sigma_H)]$ and $\overline{\Lambda} = J_n[G/H]$.

6.2 Lemma. *There is a ring anti-isomorphism* $\mathbf{End}_\Lambda(\Lambda') \cong \overline{\Lambda}$ *given by* $[f] \mapsto \pi_H f(H)$.

Proof : Since $\mathbf{Z}G$ acts as $\mathbf{Z}[G/H]$ on Λ', there is an anti-isomorphism $\mathrm{End}_\Lambda(\Lambda') = \mathrm{End}_{\Lambda'}(\Lambda') \cong \Lambda'$ by $f \mapsto f(H)$. But

$$P_\Lambda(\Lambda', \Lambda') \stackrel{5.2}{=} \sigma_G.\mathrm{End}_{\mathbf{Z}}(\Lambda') = n\sigma_{G/H}.\mathrm{End}_{\mathbf{Z}}(\Lambda') \stackrel{5.2}{=} nP_{\Lambda'}(\Lambda', \Lambda') = n\mathrm{End}_{\Lambda'}(\Lambda'),$$

the last equality because Λ' is free (over Λ'!). Evaluating the last group at H, we obtain $\ker \pi_H = n\Lambda'$, and the result follows. ∎

Let τ denote the composite map $\mathrm{Whe}_\Lambda(\Lambda', \Lambda') \to \mathbf{Whe}_\Lambda(\Lambda', \Lambda') = \mathbf{End}_\Lambda(\Lambda')^\times \simeq \overline{\Lambda}^\times$, where the first map is the natural projection and the last is the restriction to unit groups of the anti-isomorphism in the lemma.

6.3 Theorem. *There is a commutative diagram*

$$\begin{array}{ccc} \mathrm{Whe}_\Lambda(\Lambda', \Lambda') & \xrightarrow{\partial} & D(\Lambda) \\ & {}^{\tau}\searrow \quad \nearrow{}^{\delta_H} & . \\ & \overline{\Lambda}^\times & \end{array}$$

Proof : Write ϵ, π for ϵ_H, π_H. Let $h \in \mathrm{Whe}_\Lambda(\Lambda', \Lambda')$. By 4.7 we can choose some $\alpha \in U(\mathrm{End}_\Lambda(\Lambda'))$ such that $\partial(h) = \mathrm{cls}\,\nu\alpha$. If α_p is right multiplication by $v_p \in (\Lambda'_p)^\times$ for each p, and if $\tau(h) = w \in \overline{\Lambda}^\times$, from the proof of 4.7 it follows that $\pi_p v_p = w_p$ for each p. Since $\overline{\Lambda}_p$=0 if $p \not| n$, we may take $v_p = 1$ in this case. We may identify Λ with

$$\{ (\epsilon(\lambda), \pi(\lambda)) : \lambda \in \Lambda \} \subset \Lambda' \oplus \Lambda'';$$

this identification is compatible with the identification of $\mathbf{Q}G$ with $Q\Lambda' \oplus \mathbf{Q}\Lambda''$. Then the pullback Λw (such that $\delta_H(w) = [\Lambda w] - [\Lambda]$ —see **[RU]**) is identified with

$$\{ (a, b) \in \Lambda' \oplus \Lambda'' : \pi a = (\delta b) w \}.$$

Moreover $\Lambda w = \Lambda\beta$ where $\beta \in J(\mathbf{Q}G)$ is given by

$$\beta_p = \begin{cases} (1,1) & \text{if } p \not| n; \\ (v_p, 1) & \text{if } p | n. \end{cases}$$

with components in $\mathbf{Q}\Lambda'_p \oplus \mathbf{Q}\Lambda''_p$ for each p. (see **[CR]** Vol. II ex. 53.1). It is obvious that $\mathrm{cls}\,\nu\alpha = \mathrm{cls}\,\nu\beta$ which proves the theorem. ∎

Remark:

(i) One can define a generalised Swan module $\langle u, \sigma_H \rangle = \mathbf{Z}Gu + \mathbf{Z}G\sigma_H$, where the element $u \in \mathbf{Z}G \cap \mathbf{Q}G^\times$ is such that $u \in \mathbf{Z}_pG^\times$ for $p|n$. Then $(u, \sigma_H) = \partial(f) = \delta_H(w)$ where (u, σ_H) denotes $[\langle u, \sigma_H \rangle] - [\mathbf{Z}G] \in D(\Lambda)$, and $f \in \mathrm{Whe}_\Lambda(\Lambda', \Lambda')$ has image $w \in \overline{\Lambda}^\times$ under the isomorphism of 6.2, and $\pi_H\epsilon_H(u) = w$. For any unit w, such a u exists.

(ii) Similar results hold for more general Mayer-Vietoris sequences. For example, if Λ' is any order containing Λ and $(\Lambda' : \Lambda)$ is the two-sided conductor

$$(\Lambda' : \Lambda) = \{\, x \in K\Lambda : \Lambda' x \Lambda' \subset \Lambda \,\},$$

then there is a commutative diagram, the analogue of 6.3, with δ_H replaced by the connecting map ϵ in the Mayer-Vietoris sequence corresponding to the Cartesian square

$$\begin{array}{ccc} \Lambda & \to & \Lambda' \\ \downarrow & & \downarrow \\ \dfrac{\Lambda}{(\Lambda' : \Lambda)} & \to & \dfrac{\Lambda'}{(\Lambda' : \Lambda)} \end{array}$$

Here Λ can be any order as in §4.

(iii) If Λ' as in (ii) is chosen to be a maximal order, we find that $\partial\colon \mathrm{Whe}_\Lambda(\Lambda', \Lambda') \to D(\Lambda)$ is surjective, since ϵ is surjective because $D(\Lambda') = 0$. This also follows directly from the idelic description in §4.

6.4 Corollary. *Let H be any normal subgroup of G. Then*

$$T_H(\mathbf{Z}G) = \Delta\big(\mathbf{Z}[G/H]\big). \quad \blacksquare$$

The last result connects Chinburg's invariant $\Omega(N/K, 1)$ of a finite Galois extension N/K of number fields with Galois group Γ, with the Swan subgroup of the class group, as we will soon show. We take the following definition from **[Ch2]**.

There is an exact sequence

$$0 \to C_f \to A \to B \to \mathbf{Z} \to 0,$$

of finitely generated $\mathbf{Z}\Gamma$-modules, where A and B are cohomologically trivial. The module C_f is chosen to be a finitely generated $\mathbf{Z}\Gamma$-module with the same Tate cohomology as the infinitely generated module $C(N)$, the idele class group of N. In other words,

$$\widehat{H}^n(\Gamma, C_f) \cong \widehat{H}^n(\Gamma, C(N)) \quad \text{for all integers } n.$$

Define $\Omega = \Omega(N/K, 1) = [A] - [B] - r[\Lambda]$, where $r = rk([A]) - rk([B])$.

We can improve slightly on 3.5:

6.5 Theorem. *Let*

$$0 \to T \to P_{n-1} \to \cdots \to P_0 \to M \to 0$$

be an n-fold extension of the Λ-lattice M where each P_j is a projective Λ-lattice. Then there is a natural isomorphism $\mu\colon \mathrm{Ext}^n_\Lambda(M, N) \cong \mathbf{Hom}_\Lambda(T, N)$ for any Λ-module N. Further, if $f \in \mathrm{Ext}^n_\Lambda(M, N)$ is a $(1,n)$-w.h.e., such that $\mu(f) = [h]$, then h is a w.h.e. and $\partial(f) = \partial(h) + [\mathbf{P}]$.

Proof : Let Q be $\mathrm{im}(P_{n-1} \to P_{n-2})$. A standard result says that there is a natural isomorphism $\mathrm{Ext}^n_\Lambda(M, N) \cong \mathrm{Ext}^1_\Lambda(Q, N)$. Since Q is a lattice, by 5.4 and 3.2 the short exact sequence $T \to P_{n-1} \to Q$ yields a contravariant **Ext** sequence. Letting the variable be N, the connecting homomorphism gives an isomorphism $\mathbf{Hom}_\Lambda(T, N) \cong \mathrm{Ext}^1_\Lambda(Q, N)$. Putting these isomorphisms together yields the map μ. The result about $\partial(f)$ is a consequence of 3.4 and 3.5, and by 5.3 h is a w.h.e. (i.e. of level 1). ∎

Applying 6.5 with $M = \mathbf{Z}$, $N = C_f$, $n = 2$ and T the 2-syzygy in the bar resolution of $\mathbf{Z}$ (so $[\mathbf{P}] = [\mathbf{Z}\Gamma]$), we find:

6.6 Theorem. *Ω lies in the coset of $T(\mathbf{Z}\Gamma)$ determined by $\partial(h) + (1 - r)[\mathbf{Z}\Gamma]$ for any $h \in \mathrm{Whe}_\Lambda(T, C_f)$. Since T is uniquely determined (as a submodule of $\mathbf{Z}\Gamma^{(2)}$), this coset depends only on the module C_f.*

Proof : By 5.5 and 6.5, Ω lies in the coset of $\Delta(T)$ determined by the given representative. By 5.7, $\Delta(T) = \Delta(\mathbf{Z})$, and the latter group is $T(\mathbf{Z}\Gamma)$ by 6.4. ∎

6.7 Remark: A similar result holds when T is any 2-syzygy of a *free* resolution of $\mathbf{Z}$; the bar resolution simply makes this choice explicit.

In the case of a cyclic group Γ, two simplifications occur to make the above result more concrete. As in **[Ta]** Ch. 3 1.5, the Swan subgroup of a cyclic group is the trivial group. Also, we may choose the module T to be $\mathbf{Z}$ since there is an exact sequence $\mathbf{Z} \to \mathbf{Z}\Gamma \to \mathbf{Z}\Gamma \to \mathbf{Z}$, for a cyclic group Γ. Thus $\Omega = \partial(h) - r[\mathbf{Z}\Gamma]$ for any $h \in \mathrm{Whe}_{\mathbf{Z}\Gamma}(\mathbf{Z}, C_f)$, and only depends on the module C_f.

§7. Hecke algebras of subgroups of a finite group.

Let G be a finite group and H a subgroup of G. Define

$$\sigma_H = \sum_{h\in H} h, \qquad d_g = \sum_{x\in HgH} x \in \mathbf{Z}G,$$

for $g \in G$, and $e_H = \sigma_H/|H| \in \mathbf{Q}G$.

Note that e_H is an idempotent, and the d_g are the $H - H$ double-coset sums. Let $H^g = g^{-1}Hg$.

7.1 Lemma. *Let $g, g' \in G$. Then*

(i) $gH = g'H \iff g\sigma_H = g'\sigma_H$;

(ii) $|H \cap H^g| d_g = \sigma_H g \sigma_H$;

(iii) $d_g \in \{ (\sum_{x\in G} a_x x)\sigma_H : a_x = 0$ *or 1 for all* $x \}$.

Proof :

(i) $gH = g'H \iff g' = gh$ some $h \in H \iff g\sigma_H = g'\sigma_H$.

(ii) Let $h_i, h_i' \in H$, for $i = 1, 2$. Then $h_1 g h_2 = h_1' g h_2' \iff g^{-1}(h_1')^{-1}h_1 g h_2 = h_2'$. Fixing h_1 and h_2, the latter equation requires that $g^{-1}(h_1')^{-1}h_1 g \in H$, which allows $|H \cap H^g|$ choices of h_1', each of which fixes h_2'.

(iii) Let $h_1, h_2 \in H$. By (i), $h_1 g\sigma_H = h_2 g \sigma_H \iff h_1 gH = h_2 gH$. Fixing h_1, the second equation requires that $g^{-1}h_2^{-1}h_1 g \in H$, which gives $|H \cap H^g|$ choices of h_2. So (iii) now follows from (ii). ∎

7.2 Theorem.

(i) There is an isomorphism $R[G/H] \cong_{RG} RGe_H$, induced by R-linearity from the map $gH \mapsto ge_H$ for $g \in G$, where R is a domain of characteristic 0;

(ii) There is a ring anti-isomorphism

$$\mathrm{End}_{\mathbf{Q}G}(\mathbf{Q}Ge_H) \cong e_H\mathbf{Q}Ge_H = \langle d_g \rangle_{\mathbf{Q}}$$

by right multiplications. (The r.h.s. is the Hecke algebra corresponding to H.);

(iii) $\mathrm{End}_{\mathbf{Z}G}(\mathbf{Z}Ge_H) \cong \langle d_g/|H|\rangle_{\mathbf{Z}}$, *under the map of (ii).*

Proof :

(i) follows from 7.1(i).

(ii) The anti-isomorphism is clear, and the equality follows by 7.1(ii).

(iii) We identify the image of $\mathrm{End}_{\mathbf{Z}G}(\mathbf{Z}Ge_H)$ with $\{ \lambda \in \langle d_g\rangle_{\mathbf{Q}} : \mathbf{Z}Ge_H\lambda \subset \mathbf{Z}Ge_H \}$. 7.1(ii) shows that $e_H\lambda = \lambda$ for $\lambda \in \langle d_g\rangle_{\mathbf{Q}}$. If follows that the image is

$$\langle d_g\rangle_{\mathbf{Q}} \cap \mathbf{Z}Ge_H = \langle d_g/|H|\rangle$$

by 7.1(iii). ∎

7.3 Corollary. *Let* $X = \langle |H \cap H^g| d_g/|H|\rangle_{\mathbf{Z}}$. *Then the image of* $P_{\mathbf{Z}G}(\mathbf{Z}Ge_H, \mathbf{Z}Ge_H)$ *under the map of 7.2(iii) is* X, *hence*

$$\mathbf{End}_{\mathbf{Z}G}(\mathbf{Z}[G/H]) \cong \frac{\langle d_g/|H|\rangle_{\mathbf{Z}}}{X}.$$

Proof : Let $g, g' \in G$. There is a unique map $f(g, g') \in \mathrm{End}_{\mathbf{Z}}(\mathbf{Z}Ge_H)$ such that $f(g, g')(ge_H) = g'e_H$, and $f(g, g')(g''e_H) = 0$ if $g''e_H \neq g'e_H$ for $g'' \in G$. Then

$$\{\sigma_G . f(g, g')\}(e_H) = \sum_{g''e_H = ge_H} (g'')^{-1}g'e_H = \sum_{h\in H} hg^{-1}g'e_H = \sigma_H g^{-1}g'e_H.$$

Since the $f(g, g')$ generate $\mathrm{End}_{\mathbf{Z}}(\mathbf{Z}Ge_H)$ as abelian group, the result follows by 7.1 and 5.4. ∎

We will use the above results on Hecke algebras to show that Theorem 6.4 (*i.e.* $T_H(\mathbf{Z}G) = \Delta(\mathbf{Z}[G/H])$ if H is normal) fails for non-normal subgroups H, in general.

Since $\mathbf{Z}G \otimes_{\mathbf{Z}N}$ is flat, for any subgroup N of G, it follows by inducing a sequence for a w.h.e. of $\mathrm{End}_{\mathbf{Z}N}(\mathbf{Z}[N/H])$ that (following Oliver in [Ol])

$$T_H(\mathbf{Z}G) \stackrel{def}{=} \mathrm{ind}_N^G T_H(\mathbf{Z}N) \subseteq \Delta(\mathbf{Z}[G/H])$$

where $N = N_G(H)$ is the normaliser of H in G. For our example, we will choose G to be a dihedral group D_{pq}, where p and q are odd distinct primes and

$$D_n = \langle\, \sigma_n, \tau : \sigma_n^n = \tau^2 = 1,\ \tau\sigma_n = \sigma_n^{-1}\tau \,\rangle$$

is dihedral of order $2n$. Abusing notation, we can write $\sigma_{pq}^q = \sigma_p$, and let $H_p = \langle \sigma_p, \tau\rangle \cong D_p$. Similarly the dihedral subgroup H_q of G is defined. We have

7.4 Theorem. $\Delta(\mathbf{Z}[G/H_p]) + \Delta(Z[G/H_q]) = D(\mathbf{Z}G)$.

Before proving the theorem, we will show how it provides the required example, i.e. $T_H(\mathbf{Z}G) \neq \Delta(\mathbf{Z}[G/H])$ for some H which is not normal.

Note that H_p and H_q are their own normalisers in G. Thus $T_{H_p}(\mathbf{Z}G) = \mathrm{ind}_{H_p}^G T(\mathbf{Z}H_p)$. But $H_p \cong D_p$, and $D(\mathbf{Z}D_p) = 0$ ([CR] Vol. II 50.25), hence

$$T_{H_p}(\mathbf{Z}G) = T_{H_q}(\mathbf{Z}G) = 0.$$

Thus, whenever $D(\mathbf{Z}G) \neq 0$, the theorem gives the required example with H either H_p or H_q. But $D(\mathbf{Z}G) \neq 0$ when $p \equiv q \equiv 1 \pmod 4$ ([EM] Theorem 2.3), providing an infinite class of examples.

Proof of 7.4: Let $\mathcal{O}$ be the (unique) maximal order in the commutative semisimple algebra $C = Z(\mathbf{Q}G)$. The idelic description of the kernel group is

$$D(\mathbf{Z}G) \cong \frac{\mathcal{U}(\mathcal{O})}{\mathcal{O}^\times \nu(\mathcal{U}(\mathbf{Z}G))}. \tag{7.5}$$

Note that we may ignore the infinite primes in the idele groups since $\mathbf{Q}G$ is a sum of matrix rings over *fields* (see below).

Let $\Theta^p = \mathrm{End}_{\mathbf{Z}G}(\mathbf{Z}[G/H_p])$ and similarly for Θ^q. By the naturality of the isomorphism 7.5 and 4.7 it suffices to show

$$\nu(\mathcal{U}(\Theta^p))\nu(\mathcal{U}(\Theta^q))\nu(\mathcal{U}(\mathbf{Z}G)) = \mathcal{U}(\mathcal{O}) \tag{7.6}$$

We will prove 7.6 prime-by-prime. If r is a prime number, not dividing $2pq$, then $\mathbf{Z}_rG$ is a maximal order. Hence $\nu(\mathbf{Z}_rG^\times) = \mathcal{O}_r^\times$. Thus it suffices to prove the local version of 7.6 at the primes 2, p and q.

We will use the following notation. $C_n = \langle\sigma_n\rangle$ is the cyclic group of order n, D_n is the semi-direct product of C_n and the group $C_2 = \langle\tau\rangle$ (we put $\sigma_2 = \tau$), with τ acting by inversion, $\sigma_n \mapsto \sigma_n^{-1}$. Let ζ_n be a primitive n^{th} root of unity, and let

$$L^n = \mathbf{Q}(\zeta_n) \qquad K^n = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$$

$$S^n = \mathbf{Z}[\zeta_n] \qquad R^n = \mathbf{Z}[\zeta_n + \zeta_n^{-1}].$$

We fix the isomorphism (c.f. [CR] Vol. I example 7.39)

$$\mathbf{Q}G \cong \mathbf{Q}C_2 \oplus L^p \circ C_2 \oplus L^q \circ C_2 \oplus L^{pq} \circ C_2$$

where the "$\circ$" denotes twisted group algebras, τ acting by complex conjugation. e.g. the projection $\mathbf{Q}G \to L^p \circ C_2$ is induced by $\sigma_{pq} \mapsto \zeta_p$ (and $\tau \mapsto \tau$). Further (ibid.) we have $L^n \circ C_2 \cong M_2(K^n)$ for $n > 2$ (though $S^n \circ C_2 \not\cong M_2(R^n)$). Also we have $\mathbf{Q}C_2 = \mathbf{Q}^{(+)} \oplus \mathbf{Q}^{(-)}$, with τ acting trivially on the $(+)$- and by negation on the $(-)$-component. Thus this identification is $a + b\tau \mapsto ((a+b)/2, (a-b)/2)$. We then have an identification

$$\mathcal{O} = \mathbf{Z}^{(+)} \oplus \mathbf{Z}^{(-)} \oplus R^p \oplus R^q \oplus R^{pq}$$

and correspondingly

$$\mathbf{Z}_2 G = \mathbf{Z}_2 C_2 \oplus S_2^p \circ C_2 \oplus S_2^q \circ C_2 \oplus S_2^{pq} \circ C_2.$$

Now $\mathbf{Z}_2 C_2^\times = \mathbf{Z}_2^{(+)\times} \times \mathbf{Z}_2^{(-)\times}$, as is easily seen by computing radicals (units of $\mathbf{Z}_2$ are $\equiv 1 \pmod 2$). We need a lemma (extracted from the proof of Theorem 3.4 in [**Wi3**])

7.7 Lemma. *For each positive integer n and each prime number r*

$$\nu((S_r^n \circ C_2)^\times) = R_r^{n\times}. \quad \blacksquare$$

Applying 7.7 with $r = 2$ we have $\nu(\mathbf{Z}_2 G^\times) = \mathcal{O}_2^\times$. By symmetry in p and q 7.6 follows if we can show

$$\nu(\Theta_p^{p\times})\nu(\Theta_p^{q\times})\nu(\mathbf{Z}_p G^\times) = \mathcal{O}_p^\times \tag{7.8}$$

Write d_g for the double coset sums of H_q in G, and write σ for σ_{pq}. Observe that

$$H_q \sigma^{x+mp} \tau H_q = H_q \sigma^x H_q = H_q \sigma^{-x} H_q,$$

the first equality because $\sigma^p = \sigma_q$ and τ lie in H_q, the second because $\tau\sigma^x\tau = \sigma^{-x}$. Thus there are $(p-1)/2+1$ double cosets:

$$\{\, H_q\sigma^x H_q : 0 \le x \le (p-1)/2 \,\}.$$

By 7.2(iii) we can identify Θ^q with

$$\langle\, d_g/2q \,\rangle_{\mathbf{Z}} \overset{7.1(ii)}{=} \langle\, e_{H_q},\, 2e_{H_q}\sigma^x e_{H_q} \mid 1 \le x \le (p-1)/2 \,\rangle_{\mathbf{Z}}$$

since $H_q \cap H_q^{\sigma^x} = C_q$ if $x \not\equiv 0 \pmod p$. There is an isomorphism of (commutative) rings

$$\Theta^q \simeq \mathbf{Z}C_p{}^{C_2} \tag{7.9}$$

induced by $e_{H_q} \mapsto 1$ and $2e_{H_q}\sigma^x e_{H_q} \mapsto \sigma_p^x + \sigma_p^{-x}$. This clearly gives a group isomorphism, and that it is a ring map follows from the identity

$$\sigma^x \sigma_{H_q} \sigma^y = \sigma^{x+y}\sigma_{C_q} + \sigma^{x-y}\sigma_{C_q}\tau.$$

Thus we can omit the first two ν signs in 7.8.

Let $B = B_1 \oplus B_2$ be a direct sum of Wedderburn simple components of a semisimple algebra and let Γ be an order in B such that the restriction maps $\Gamma \to B_i$ have image the orders Γ_i for $i = 1, 2$. There is a fibre product diagram

$$\begin{array}{ccc} \Gamma & \to & \Gamma_1 \\ \downarrow & & \downarrow \\ \Gamma_2 & \to & \overline{\Gamma} \end{array} \tag{7.10}$$

in which $\overline{\Gamma}$ is finite and all the maps are surjective. This identifies Γ with a submodule of $\Gamma_1 \oplus \Gamma_2$. The analogous result still holds if we complete at an integer prime r and pass to unit groups, by semilocality and surjectivity. Suppose further that $\nu((\Gamma_i)_r^\times) = \Lambda_i$ for $i = 1, 2$. Then

$$\Lambda_1\nu(\Gamma_r^\times) = \Lambda_1 \times \Lambda_2 = \Lambda_2\nu(\Gamma_r^\times), \tag{7.11}$$

once more using surjectivity. We shall apply 7.11 thrice below. First observe that

$$\mathbf{Z}_pG = \mathbf{Z}_pD_p \oplus (S_p^qC_p) \circ C_2. \tag{7.12}$$

Observe that the conditions on 7.10 are satisfied when

(i) $\Gamma = \mathbf{Z}C_p^{C_2}$, $\Gamma_1 = R^p$, $\Gamma_2 = \mathbf{Z}$ and $\overline{\Gamma} = \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. (The surjection $\Gamma \to \Gamma_1$ is induced by $\sigma_p + \sigma_p^{-1} \mapsto \zeta_p + \zeta_p^{-1}$, that $\Gamma \to \Gamma_2$ by $\sigma_p \mapsto 1$, that $\Gamma_1 \to \overline{\Gamma}$ by $\zeta_p + \zeta_p^{-1} \mapsto 2 \pmod 2$ and that $\Gamma_2 \to \overline{\Gamma}$ is reduction mod p.)

(ii) $\Gamma = \mathbf{Z}D_p$, $\Gamma_1 = S^p \circ C_2$, $\Gamma_2 = \mathbf{Z}C_2$ and $\overline{\Gamma} = \mathbf{F}_pC_2$. The maps are analogous to (i), with $\sigma_p + \sigma_p^{-1}$ replaced by σ_p. τ is unaffected by each map. e.g. the surjection $\Gamma \to \Gamma_1$ is induced by $\sigma_p \mapsto \zeta_p$ and $\tau \mapsto \tau$.

(iii) $\Gamma = (S^qC_p) \circ C_2$, $\Gamma_1 = S^{pq} \circ C_2$, $\Gamma_2 = S^q \circ C_2$ and $\overline{\Gamma} = \overline{S}^q \circ C_2$, where $\overline{S}^q = S^q/pS^q$. The maps are analogous to those in (ii) but with $\mathbf{Z}$ replaced by S^q. e.g. we think of S^{pq} as $S^q[\zeta_p]$ where of course $\zeta_{pq} = \zeta_p\zeta_q$.

Now apply 7.11 with $r = p$ and

(i) $\Lambda_i = (\Gamma_i)_p^\times$;

(ii) $\Lambda_1 = R_p^{p\times}$ (by 7.7) and $\Lambda_2 = \mathbf{Z}_pC_2^\times$;

(iii) $\Lambda_1 = R_p^{pq\times}$ and $\Lambda_2 = R_p^{q\times}$ (by 7.7).

Now $\Theta_p^q \cong \mathbf{Z}_pC_p^{C_2}$ and $\Theta_p^p = R_p^q \oplus \mathbf{Z}_p$ (by the definition of $\overline{\Gamma}$ in (i)). We may regard $\Gamma_2 = \mathbf{Z}$ in (i) as $\mathbf{Z}^{(+)}$, since $e_{H_q}e_G = e_G$. Then we have

$$\begin{aligned}\Theta_p^{p\times}\Theta_p^{q\times}\nu(\mathbf{Z}_pG^\times) &\overset{7.12}{=} (\mathbf{Z}_p^{(+)^\times} \times R_p^{q\times})\mathbf{Z}_pC_p^{C_2\times}\nu(\mathbf{Z}_pD_p^\times)\nu\big((S_p^qC_p) \circ C_2^\times\big) \\ &\overset{7.11}{=} (\mathbf{Z}_p^{(+)^\times} \times R_p^{p\times} \times R_p^{q\times})\nu(\mathbf{Z}_pD_p^\times)\nu\big((S_p^qC_p) \circ C_2^\times\big) \\ &\overset{7.11}{=} (\mathbf{Z}_p^{(+)^\times} \times R_p^{p\times} \times R_p^{q\times})(\mathbf{Z}_pC_2^\times)(R_p^{pq\times}) \\ &= \mathcal{O}_p^\times\end{aligned}$$

since $\mathbf{Z}_pC_2 = \mathbf{Z}_p^{(+)} \oplus \mathbf{Z}_p^{(-)}$, as $2 \in \mathbf{Z}_p^\times$. This concludes the proof of 7.4. ∎

CHAPTER II. Canonical Factorisability and Chinburg's second invariant.

§1. Introduction.

Let N/K be a Galois extension of number fields with Galois group Γ. In **[Ch2]** T. Chinburg defined a class $\Omega(N/K, 2) \in Cl(\mathbf{Z}\Gamma)$ which measures the Galois structure of $\mathcal{J}(N)$ (the idele group of N). The ring of integers $\mathcal{O}_N$ in N is a locally free $\mathbf{Z}\Gamma$-module if (and only if) N/K is at most tamely ramified. We refer to this as the *tame* case. In the tame case $\mathcal{O}_N$ determines a class $(\mathcal{O}_N) \in Cl(\mathbf{Z}\Gamma)$ (this would have been written $[\mathcal{O}_N] - |K : \mathbf{Q}|[\mathbf{Z}\Gamma]$ in chapter I), and Chinburg showed that

$$\Omega(N/K, 2) = (\mathcal{O}_N).$$

Also in the tame case, M. Taylor proved the following beautiful and far-reaching result:

$$(1.1) \qquad (\mathcal{O}_N) = tW_{N/K} \in D(\mathbf{Z}\Gamma)$$

where $W_{N/K}$ (defined by Ph. Cassou-Noguès) is a function depending only on the root numbers $W(\chi) = \pm 1$ of the irreducible symplectic characters χ of Γ, and $tW_{N/K}$ is the class in the kernel group $D(\mathbf{Z}\Gamma)$ it determines. Thus (in multiplicative notation) $(\mathcal{O}_N)^2 = 1$ and in many cases (Γ abelian, odd order, dihedral) $(\mathcal{O}_N) = 1$ and indeed $\mathcal{O}_N$ is then a free $\mathbf{Z}\Gamma$-module.

A. Fröhlich generalised the definition of $tW_{N/K}$ to wildly ramified extensions (the *wild* case). The resulting class in $Cl(\mathbf{Z}\Gamma)$ was called the Cassou-Noguès Fröhlich class in **[Ch2]**, and also goes by the name of the (generalised) root number class. We shall denote it by $t_{N/K}$ (a definition appears in §4). This motivated the following conjectural generalisation of 1.1.

1.2 Conjecture. *(Chinburg)* $\Omega(N/K, 2) = t_{N/K}$ *for all* N/K.

We will prove in §4 that

$$(1.3)\qquad \Omega(N/K,\, 2) \equiv t_{N/K} \pmod{D(\mathbf{Z}\Gamma)}$$

thus giving evidence supporting 1.2, which has already been verified for a large class of quaternion extensions by S. Kim. Chinburg has shown that $t_{N/K} \notin D(\mathbf{Z}\Gamma)$ for certain wildly ramified extensions, hence the same applies for $\Omega(N/K,\, 2)$.

However, the arithmetic object $\mathcal{O}_N$ has "disappeared" from the statement of 1.2. We reinstate it in the proof of 1.3 by the method of *canonical factorisability* (for the genesis of this method see §2). Since $\mathcal{O}_N$ is not projective in the wild case, we cannot obtain from it a class in $Cl(\mathbf{Z}\Gamma)$. Instead, let $b \in \mathcal{O}_N$ be a normal generator of N/K and consider the finite module $\mathcal{O}_N/b\mathcal{O}_K\Gamma$. We show in §3 that this module has a canonical factorisation g_b. This function g_b (which depends on the norm resolvents $\mathcal{N}_{N/K}(b|\chi)$ of b and the Galois Gauss sums $\tau(N/K,\, \chi)$ of characters χ) gives rise to an invariant (which does not depend upon b) in $Cl(\mathcal{M}_\Gamma)$ where $\mathcal{M}_\Gamma$ is a maximal order of $\mathbf{Q}\Gamma$ containing $\mathbf{Z}\Gamma$. We show in §§3-4 that this invariant equals the images of $\Omega(N/K,\, 2)$ and $t_{N/K}$ under the surjection

$$Cl(\mathbf{Z}\Gamma) \to Cl(\mathcal{M}_\Gamma)$$

(which has kernel $D(\mathbf{Z}\Gamma)$) thus establishing 1.3.

A word about notation. We shall be using **[Fr1]** extensively as a reference for the tame theory, and shall adopt similar notations. In particular, in this chapter modules are ***right*** modules unless otherwise stated. Direction of composition of maps is inferred from the context (no endomorphisms appear in this chapter).

§2. Canonical Factorisability for finite groups.

Let r be a prime number. Let k be either of $\mathbf{Q}$ (global case) or $\mathbf{Q}_r$ (local case), and fix an algebraic closure $\overline{k}$ of k, in which lies each finite extension K of k. Let $\mathcal{O}_K$ be the ring of integers (maximal order) in K. Write Ω_K for $\mathrm{Gal}(\overline{k}/K)$. Write $\mathcal{I}_K$ for the fractional ideal group of K. In the global case, fix $\overline{\mathbf{Q}}$ to be the unique algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and write $\mathcal{J}(K)$ for the idele group and $\mathcal{U}(K)$ for the unit ideles of the number field K.

Let G be a finite group and let $\mathcal{S}(G)$ be the set of subgroups of G. Let R_G the ring of virtual characters of G, $\mathrm{Irr}(G)$ the absolutely irreducible characters and S_G the subset of $\mathrm{Irr}(G)$ consisting of symplectic characters, all characters over $\overline{k}$. If we need to indicate the dependence on $\overline{k}$ in the notation, we shall write $R_G(\overline{k})$, $\mathrm{Irr}(G, \overline{k})$, etc. If in doubt take $k = \mathbf{Q}$.

Let U be a finite Galois extension of $\mathbf{Q}$ which realises the $\overline{\mathbf{Q}}$-characters of G. Then the group $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G, \mathcal{J}(U))$ is defined, and there is a natural surjection

$$\mathrm{cls}_\Lambda\colon \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G, \mathcal{J}(U)) \to Cl(\Lambda), \tag{2.1}$$

for any order Λ in $\mathbf{Q}G$, induced by Fröhlich's Hom-description (see the proof of 2.6 below). There is a similar result for the group $\mathcal{K}_0T(\Lambda)$, which is the Grothendieck group of the category of locally freely presented finite Λ-modules, taken with respect to exact sequences. By I.5.1 if $\Lambda = \mathbf{Z}G$ the category is that of finite cohomologically trivial $\mathbf{Z}G$-modules. Whereas if Λ is a maximal order then the category is simply that of the finite Λ-modules, and there is an ideal-theoretic description of $\mathcal{K}_0T(\Lambda)$ (going back to Jacobinski) which we give a modern flavour via the Hom-description in 2.6.

When $\Lambda = \mathbf{Z}G$ there are useful formulae for change of group which we shall use extensively in this chapter. Let H be a subgroup and N a normal subgroup of G. Restriction, induction and inflation of characters induce maps $\mathrm{res}^G_H\colon R_G \to R_H$, $\mathrm{ind}^G_H\colon R_H \to R_G$ and $\mathrm{inf}^G_{G/N}\colon R_{G/N} \to R_G$ on the character rings. Further, fixing under N on $\overline{\mathbf{Q}}G$-modules gives a map $\mathrm{cut}^G_{G/N}\colon R_G \to R_{G/N}$. Let G_1 and G_2 be arbitrary groups. Let M be an abelian group. Any group homomorphism $R_{G_1} \to R_{G_2}$ induces a contravariant homomorphism

$$\mathrm{Hom}(R_{G_2}, M) \to \mathrm{Hom}(R_{G_1}, M). \tag{2.2}$$

In the case of the maps above, the contravariant, induced maps are denoted by ind^G_H, res^G_H, $\mathrm{coinf}^G_{G/N}$ and $\mathrm{cocut}^G_{G/N}$ respectively. The first three of these give maps in the Hom-description for the groups $\mathcal{K}_0T(\mathbf{Z}G)$, $\mathcal{K}_0T(\mathbf{Z}H)$, etc. (but the analogue of cocut does not preserve local freeness of modules). These are induced by the module-theoretic maps (again denoted by ind, res and coinf) as follows. The tensor product $\otimes_{\mathbf{Z}H}\mathbf{Z}G$ induces $\mathrm{ind}_H^G\colon \mathcal{K}_0T(\mathbf{Z}H) \to \mathcal{K}_0T(\mathbf{Z}G)$. Restriction of scalars from $\mathbf{Z}G$-modules to $\mathbf{Z}H$-modules induces $\mathrm{res}_H^G\colon \mathcal{K}_0T(\mathbf{Z}G) \to \mathcal{K}_0T(\mathbf{Z}H)$. Fixing under N (c.f. cutting of characters) from $\mathbf{Z}G$-modules to $\mathbf{Z}[G/N]$-modules induces $\mathrm{coinf}_{G/N}^G\colon \mathcal{K}_0T(\mathbf{Z}G) \to \mathcal{K}_0T(\mathbf{Z}[G/N])$.

Let $\mathcal{M}_G(\mathbf{Q}) = \mathcal{M}_G$ be any maximal order in $\mathbf{Q}G$ containing $\mathbf{Z}G$. There is an exact sequence

$$(2.3) \qquad 1 \to \mathcal{U}(U) \to \mathcal{J}(U) \xrightarrow{\mathrm{AI}} \mathcal{I}_U \to 1$$

in which AI is the associated ideal map. This induces a map (also denoted AI)

$$(2.4) \qquad \mathrm{AI}\colon \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G, \mathcal{J}(U)) \to \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G, \mathcal{I}_U).$$

We define $I(G, \overline{\mathbf{Q}})$ to be the subgroup of $g \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G, \mathcal{I}_U)$ such that

$$(2.5) \qquad g(\chi) \in \mathcal{I}_{\mathbf{Q}(\chi)}, \text{ for each } \chi \in R_G(\overline{\mathbf{Q}}).$$

Note that the symbol $\mathbf{Q}(\chi)$ indicates the number field generated by the values of the character χ. This is not the same as the smallest field over which a representation of the character is realised. e.g. If χ is an irreducible symplectic character, then in particular χ is real-valued so $\mathbf{Q}(\chi)$ is a subfield of $\mathbf{R}$. But no representation of χ is real (one could take this as the definition of irreducible symplectic character).

In 2.5—and throughout this paper—we are using the following convention. If L/K is a finite extension of number fields then there is a natural embedding of $\mathcal{I}_K$ in $\mathcal{I}_L$, which we shall regard as an inclusion. A similar convention holds in the local case. Indeed, if we replace U by a completion $U_{\mathcal{R}}$ of U at a finite prime $\mathcal{R}|r$ and $\mathbf{Q}$ by $\mathbf{Q}_r$ then we get the corresponding definition of $I(G, \overline{\mathbf{Q}_r})$. Note that the symbol $\overline{\mathbf{Q}_r}$ means the algebraic closure of the r-adic numbers, *not* the r-adic completion of $\overline{\mathbf{Q}}$!

In the global case, define $P^+(G, \overline{\mathbf{Q}})$ to be the subgroup of $g \in I(G, \overline{\mathbf{Q}})$ such that

P(i) $g(\chi)$ is principal for each $\chi \in R_G(\overline{\mathbf{Q}})$;

P(ii) $g(\chi)$ has a real, totally positive generator for each $\chi \in S_{G,\mathbf{Q}}$.

2.6 Theorem. *There are isomorphisms*

$$\mathcal{K}_0T(\mathcal{M}_G) \xrightarrow{\sim} I(G, \overline{\mathbf{Q}})$$

$$\ker(\mathcal{K}_0T(M_G) \to Cl(\mathcal{M}_G)) \xrightarrow{\sim} P^+(G, \overline{\mathbf{Q}})$$

induced by the Hom-description and the map AI.

Proof (sketch): The Hom-description isomorphisms are

$$\mathcal{K}_0T(\mathcal{M}_G) \cong \frac{\mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, \mathcal{J}(U))}{\mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, \mathcal{U}(U))}$$

and

$$Cl(\mathcal{M}_G) \cong \frac{\mathrm{Hom}_{\Omega_\mathbf{Q}}(R_G, \mathcal{J}(U))}{\mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, \mathcal{U}(U))\mathrm{Hom}_{\Omega_\mathbf{Q}}(R_G, U^\times)}$$

The surjection $\mathcal{K}_0T(\mathcal{M}_G) \to Cl(\mathcal{M}_G)$ is then extension of coset. To establish the theorem it suffices to show the equalities

$$\mathrm{AI} \circ \mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, \mathcal{J}(U)) = I(G, \overline{\mathbf{Q}})$$

and

$$\mathrm{AI} \circ \mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, U^\times) = P^+(G, \overline{\mathbf{Q}}).$$

For the second equality, note that one can place a + sign on each group in the Hom-description of $Cl(\mathcal{M}_G)$. The inclusions $\subseteq$ are clear from the fact that

$$\mathcal{J}(U)^{\Omega_{\mathbf{Q}(\chi)}} = \mathcal{J}(\mathbf{Q}(\chi))$$

for each $\chi \in R_G(\overline{\mathbf{Q}})$. We shall show how to pull back an element $g \in I(G, \overline{\mathbf{Q}})$ to one $\tilde{g} \in \mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, \mathcal{J}(U))$. Let χ run over a full set of representatives of the $\Omega_\mathbf{Q}$-orbits in $\mathrm{Irr}(G)$. Since AI: $\mathcal{J}(\mathbf{Q}(\chi)) \to \mathcal{I}_{\mathbf{Q}(\chi)}$ is surjective (and the infinite prime does not contribute) choose $\tilde{g}(\chi) \in \mathcal{J}(\mathbf{Q}(\chi))$ such that $\mathrm{AI}\tilde{g}(\chi) = g(\chi)$ and $\tilde{g}(\chi)_\infty = 1$. Choose $\tilde{g}$ on the remaining elements of $\mathrm{Irr}(G)$ so that $\tilde{g}$ respects $\Omega_\mathbf{Q}$-action. Since $\mathrm{Irr}(G)$ is a basis of R_G we find that $\mathrm{AI} \circ \tilde{g} = g$ and $\tilde{g} \in \mathrm{Hom}^+_{\Omega_\mathbf{Q}}(R_G, \mathcal{J}(U))$ as required. ∎

In future we shall identify the groups in 2.6 under these isomorphisms. From the proof given, it suffices to specify an element of $I(G, \overline{\mathbf{Q}})$ by its values on irreducible characters, which we shall do henceforth. It is easy to see that restriction, induction, inflation and cutting of characters induce corresponding maps on $I(G, \overline{k})$ (**Warning:** These do not have a natural interpretation at the level of $\mathcal{M}_G$-modules). For, these maps are well-defined if we take $M = \mathcal{I}_{\overline{k}}$ in 2.2, and if $\chi \in \mathrm{Irr}(G, k)$ then $k(\mathrm{res}^G_K \chi) \subseteq k(\chi)$, and similarly for induction, inflation and cutting of characters.

As motivation for the method of canonical factorisability, we give the elegant notion of *factorisability* (due to A. Nelson [**Ne**]).

Definition: Let $f: \mathcal{S}(G) \to \mathcal{I}_{\mathbf{Q}}$ be any map. Then f is *factorisable* if there exists a function $g \in I(G, \overline{\mathbf{Q}})$ (a *factorisation* of f) such that

$$\mathrm{res}^G_H\, g(1_H) = f(H)$$

for each $H \in \mathcal{S}(G)$.

Associating H with the G-set $H\backslash G$ one can consider f as a function on the Burnside ring of G, which is factorisable if it extends to the ring R_G. This idea has applications to integral representation theory of finite groups as follows. Let $| : |_{\mathbf{Z}}$ denote the $\mathbf{Z}$-module index. If X and Y are $\mathbf{Z}G$-lattices spanning the same $\mathbf{Q}G$-module, we can put

$$f(H) = |X^H : Y^H|_{\mathbf{Z}}$$

and if f is factorisable we may say that X and Y are *factor equivalent*, written $X_\vee Y$. This gives an equivalence relation on such lattices, which is weaker than the relation of local isomorphism. In the context of Galois module structure, the lattice X is taken to be an arithmetic one whose structure is an object of study and Y a "standard" lattice of transparent structure. Thus, factor equivalence places strong restrictions on the module structure of X. In addition (see [**Fr4**]) a factorisation function g may be expressed in terms of arithmetic functions (values of L-functions or Galois Gauss sums, say) and the invariant of $\mathcal{K}_0T(M_G)$ it represents is then parametrised, giving a source of "structure theorems" (see [**Fr4**] and [**Bu**] regarding the Martinet conjecture and its generalisations). As examples, if N/K is a finite abelian extension of number fields with Galois group Γ (in place of the group G) then (see [**Fr4**] or [**Ne**])

$$\mathcal{O}_N \cong \mathcal{O}_K\Gamma$$

as $\mathbf{Z}\Gamma$-modules. On the other hand, if Γ is abelian but not cyclic we have (see [**Fr2**] or [**Ne**])

$$\mathcal{O}_K\Gamma \not\cong \mathcal{M}_{\Gamma,K}$$

where $\mathcal{M}_{\Gamma,K}$ is the unique maximal order in $K\Gamma$. Fröhlich introduced the notion of canonical factorisability (an exposition of which appears in [**Bu**]) in the context of abelian groups G, to get around the problem that a function f may have several different factorisations (if it has any) and so the choice of an invariant in $\mathcal{K}_0T(\mathcal{M}_G)$ is not unique. Yet the arithmetic parametrisation of factorisations suggests that unique (and important) factorisations exist.

Fröhlich's canonical factorisations are uniquely determined, but of course this requires extra conditions on the function f. As in [**Bu**] one treats first the local case (completing at a prime number p) and then puts together all the local canonical factorisations into a global one. The extra information in the local case is encoded by extending the domain of f by introducing certain local idempotents.

In his second talk at the Durham Symposium on Algebraic Number Theory (1989) Fröhlich sketched a generalisation to non-abelian groups G, with the local f defined on pairs (H, e) where H is any subgroup of G and e is an idempotent of an *abelian* character of some subgroup of G of order prime to p, and further e commutes with the idempotent e_H of the subgroup H. We have adopted a simpler definition, based on an idea of Steve Wilson, in which the subgroup H is restricted to be cyclic. The definition in [**Bu**] is equivalent to ours in the cyclic case, and if a canonical factorisation (for arbitrary finite groups G) exists in Fröhlich's sense, then so does one in our sense, and they coincide.

Before proceeding to the definitions, note that just as we use the symbol G for a generic finite group and switch to Γ when the group is the Galois group of an extension N/K of number fields, we let r denote a generic prime number and reserve the symbol p (in later sections) for the fixed prime below a prime $\wp$ of K which is wildly ramified in N/K. This is to avoid confusion when using double-localisation methods (as in the tame additive theory), that is localising both arguments and values of functions, perhaps with respect to different primes.

2.7 Definition: Let r be a prime number. Let $\mathcal{S}^r(G)$ be the set of all pairs (C, e) as follows. C is any cyclic subgroup of G. We can write

$$C = C_r \times C_\times \tag{2.8}$$

where C_r is the Sylow r-subgroup of C. Then e is any indecomposable idempotent of the maximal $\mathbf{Z}_r$-order $\mathbf{Z}_r C_\times$.

Let $f: \mathcal{S}^r(G) \to \mathcal{I}_{\mathbf{Q}_r}$ be any map. Let $g \in I(G, \overline{\mathbf{Q}_r})$. Then g is the *canonical factorisation* (C. F.) of f if

$$\operatorname{res}^G_C g(\operatorname{inf}^C_{C_\times} \chi) = f(C, e) \tag{2.9}$$

for each $(C, e) \in \mathcal{S}^r(G)$, where χ is the $\mathbf{Q}_r$-valued character of $\mathbf{Q}_r C_\times e$.

Before we prove uniqueness of (local) canonical factorisations, we shall need some terminology for cyclic groups (these concepts also make sense for abelian groups). If C is a finite cyclic group, write $C^\dagger$ for $\operatorname{Irr}(C)$ (the character group of C). If $H \in \mathcal{S}(C)$, define H^* to be the subgroup of $C^\dagger$ consisting of those characters ψ such that $\psi(H) = 1$. Define a *division* D of $C^\dagger$ to be the set of generators of a subgroup (denoted $\overline{D}$) of $C^\dagger$.

2.10 Theorem. *The canonical factorisation of $f: \mathcal{S}^r(G) \to \mathcal{I}_{\mathbf{Q}_r}$ is unique if it exists.*

Proof : Let h and h' be canonical factorisations of f. Then $h'h^{-1}$ is a canonical factorisation for the constant map equal to $\mathbf{Z}_r$. For uniqueness, it suffices to show that any canonical factorisation for this constant map is also a constant map equal to $\mathbf{Z}_r$. Let $(C, e) \in \mathcal{S}^r(G)$. Let χ be as in 2.9. There is an $\Omega_{\mathbf{Q}_r}$-orbit Φ in ${C_\times}^\dagger$ such that

$$\chi = \sum_{\phi \in \Phi} \phi.$$

Choose $\phi \in \Phi$. Galois operation on ideals is trivial in the local case, so $\Omega_{\mathbf{Q}_r}$-equivariance of g actually means $g(\theta) = g(\theta^\omega)$ for $\omega \in \Omega_{\mathbf{Q}_r}$ and $\theta \in R_G^{\cdot}(\overline{\mathbf{Q}_r})$. Then by 2.9

$$\operatorname{res}^G_C g(\operatorname{inf}^C_{C_\times} \chi) = \operatorname{res}^G_C g(\operatorname{inf}^C_{C_\times} \phi)^{|\Phi|} = \mathbf{Z}_r.$$

Thus $\operatorname{res}^G_C g(\operatorname{inf}^C_{C_\times} \phi) = \mathbf{Z}_r$. Let $H \in \mathcal{S}(C_r)$. Then $\operatorname{ind}^{C_r}_H 1_H = \sum_{\psi \in H^*} \psi$. Let D run over the divisions of H^*. Then

$$(2.11) \qquad \prod_D \prod_{\psi \in D} \mathrm{res}_C^G\, g(\psi,\, \phi) = \mathrm{res}_C^G\, g(\mathrm{ind}_H^{C_r}\, 1_H,\, \phi) = \mathrm{res}_{H \times C_\times}^G\, g(\mathrm{inf}_{C_\times}^{H \times C_\times}\, \phi) = \mathbf{Z}_r.$$

By induction on the order of H it follows that for each division D of C_r †

$$\prod_{\psi \in D} \mathrm{res}_C^G\, g(\psi,\, \phi) = \mathbf{Z}_r.$$

Now

$$(2.12) \qquad |D| = |\mathrm{Gal}(\mathbf{Q}_r(\psi)/\mathbf{Q}_r)| = |\mathrm{Gal}(\mathbf{Q}_r(\psi,\, \phi)/\mathbf{Q}_r(\phi))|$$

by standard properties of cyclotomic fields. Since g is *a fortiori* $\Omega_{\mathbf{Q}_r(\phi)}$-invariant, it follows that

$$(2.13) \qquad \mathrm{res}_C^G\, g \text{ is the constant map equal to } \mathbf{Z}_r.$$

Let C run over the cyclic subgroups of G. By the Artin induction theorem, the map

$$\mathrm{ind}\colon \bigoplus_C R_C \to R_G$$

induced by the ind_C^G has image of finite index. Since $\mathcal{I}_{\overline{\mathbf{Q}_r}}$ is torsion-free, the induced contravariant map

$$\mathrm{res}\colon \mathrm{Hom}(R_G,\, \mathcal{I}_{\overline{\mathbf{Q}_r}}) \to \bigoplus_C \mathrm{Hom}(R_C,\, \mathcal{I}_{\overline{\mathbf{Q}_r}})$$

is injective. Hence by 2.13 g is the constant map equal to $\mathbf{Z}_r$. ∎

Before defining the global version of canonical factorisation, we shall need a localisation procedure.

2.14 Definition: Let $g \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_G(\overline{\mathbf{Q}}),\, \mathcal{I}_U)$ and let r be a prime number. Let $\mathcal{R}$ be any prime of U over r. Let $j\colon U \hookrightarrow U_{\mathcal{R}}$ be ~~the canonical embedding~~. For each $\psi \in R_G(\overline{\mathbf{Q}_r})$

any embedding inducing the $\mathcal{R}$-adic valuation.

there is a unique $\psi_g \in R_G(\overline{\mathbf{Q}})$ such that $\psi_g^j = \psi$. Define

$$g_r \in \mathrm{Hom}(R_G(\overline{\mathbf{Q}_r}), \mathcal{I}_{U_\mathcal{R}})$$

by

$$g_r(\psi) = g(\psi_g)_\mathcal{R}.$$

2.15 Lemma. *$g_r \in \mathrm{Hom}_{\Omega_{\mathbf{Q}_r}}(R_G(\overline{\mathbf{Q}_r}), \mathcal{I}_{U_\mathcal{R}})$ is independent of the choice of $\mathcal{R}|r$.* and of j.

Proof : Note that $U_\mathcal{R} = U_{\mathcal{R}'}$ for any other prime $\mathcal{R}'$ of U over r, since $U/\mathbf{Q}$ is Galois.

The ~~natural~~ * embedding $j': U \hookrightarrow U_{\mathcal{R}'}$ is equal to σj for some $\sigma \in \mathrm{Gal}(U/\mathbf{Q})$.

Consequently $\mathcal{R}' = \mathcal{R}^{\sigma^{-1}}$ and $\psi_g^{\sigma^{-1}}$ is the unique global character $\psi_{g'}$ such that $\psi_{g'}^{j'} = \psi$.

It follows (since g preserves $\Omega_\mathbf{Q}$-action) that

$$g(\psi_g^{\sigma^{-1}})_{\mathcal{R}^{\sigma^{-1}}} = g(\psi_g)^{\sigma^{-1}}_{\mathcal{R}^{\sigma^{-1}}} = g(\psi_g)_\mathcal{R}.$$

Thus g_r is independent of $\mathcal{R}$. and of j.

The embedding j induces an embedding

$$j^*: \mathrm{Gal}(U_\mathcal{R}/\mathbf{Q}_r) \hookrightarrow \mathrm{Gal}(U/\mathbf{Q}).$$

If $x \in U$ and $\omega \in \mathrm{Gal}(U_\mathcal{R}/\mathbf{Q}_r)$ then the maps j and j^* are connected by

$$\left(x^j\right)^\omega = \left(x^{j^*(\omega)}\right)^j.$$

Then

$$\psi^\omega = \left(\psi_g^j\right)^\omega = \left(\psi_g^{j^*(\omega)}\right)^j.$$

It follows (since g preserves $\Omega_\mathbf{Q}$-action) that

$$g_r\left(\psi^\omega\right) = g\left(\psi_g^{j^*(\omega)}\right)_\mathcal{R} = g\left(\psi_g\right)_\mathcal{R}^{j^*(\omega)} = g\left(\psi_g\right)_\mathcal{R},$$

the last equality because the image of j^* is the decomposition group of $\mathcal{R}$. The right hand side is $g_r(\psi)$. Thus g_r preserves $\Omega_{\mathbf{Q}_r}$-action. ∎

* j is any embedding inducing the $\mathcal{R}'$-adic valuation

2.16 Definition: Let

$$f^* = \{\, f^r | r \text{ is a prime number} \}$$

be any collection of maps $f^r: \mathcal{S}^r(G) \to \mathcal{I}_{\mathbf{Q}_r}$. Let $g \in I(G, \overline{\mathbf{Q}})$. Then g is the *canonical factorisation* (C. F.) of f^* if g_r is the canonical factorisation of f^r for each prime number r.

Now we shall introduce functions f^* which depend on $\mathbf{Z}G$-modules. Our treatment is formally different, but equivalent to that of Burns ([**Bu**]) in the case in which G is cyclic and M and N (below) are lattices.

2.17 Definition: Let M and N be—not necessarily finitely generated—$\mathbf{Z}G$-modules. Let $i: M \to N$ be an injective $\mathbf{Z}G$-map with finite cokernel. Let $\mathrm{ord}_{\mathbf{Z}_r}$ be the order ideal map on finite $\mathbf{Z}_r$-modules. Define $f_i^* = \{\, f_i^r \}$ by

$$f_i^r(C, e) = \mathrm{ord}_{\mathbf{Z}_r}(\mathrm{coker}(i^{C_r})_r e) = \mathrm{ord}_{\mathbf{Z}_r}(N_r^{C_r} e / i(M)_r^{C_r} e)$$

for each $(C, e) \in \mathcal{S}^r(G)$. When i is the inclusion map define $f_{M,N}^* = f_i^*$. When $M = 0$ (so N is finite) define $f_N^* = f_i^*$. If it is necessary to indicate the dependence on G we shall write $f_i^* = f_{G,i}^*$, etc.

Let $H \in \mathcal{S}(G)$. Denote by $N(H)$ the normaliser of H in G. If $(C, e) \in \mathcal{S}^r(G)$ then $N(C_r) \supseteq C$ and hence $e \in \mathbf{Z}_r N(C_r)$. The functor $(- \otimes_{\mathbf{Z}} \mathbf{Z}_r)e$ is exact. Thus the following rules for the f_i^* hold

(2.18)

(i) $f^*_{ij} = f^*_i f^*_j$;

(ii) if there is a $\mathbf{Z}N(H)$-isomorphism $\operatorname{coker}(i^H) \cong \operatorname{coker}(j^H)$

for each $H \in \mathcal{S}(G)$, then $f^*_i = f^*_j$;

(iii) if there is a $\mathbf{Z}N(H)$-isomorphism $\operatorname{coker}(i^H) \cong (\operatorname{coker} i)^H$

for each $H \in \mathcal{S}(G)$, then $f^*_i = f^*_{\operatorname{coker} i}$;

$(iiia)$ if $H \in \mathcal{S}(G)$, $i: M \to N$ is injective and $H^1(H, M) = 0$

then there is a $\mathbf{Z}N(H)$ isomorphism $\operatorname{coker}(i^H) \cong (\operatorname{coker} i)^H$;

(iv) if there is a short exact sequence of $\mathbf{Z}N(H)$-modules

$$0 \to \operatorname{coker}(i^H) \to \operatorname{coker}(k^H) \to \operatorname{coker}(j^H) \to 0$$

for each $H \in \mathcal{S}(G)$, then $f^*_k = f^*_i f^*_j$.

These are obvious except perhaps for (iv), which follows by the multiplicativity of the order ideal map on short exact sequences (this is a generalisation of Lagrange's Theorem).

Let us show that canonical factorisations exist.

2.19 Theorem. *Let T be a finite, cohomologically trivial $\mathbf{Z}G$-module. Suppose that (T) in $\mathcal{K}_0T(\mathbf{Z}G)$ is represented in the Hom-description by $h \in \operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_G, \mathcal{J}(U))$. Then $g = \mathrm{AI} \circ h$ is the canonical factorisation of f^*_T.*

Proof : $f^*_{(-)}$ factors through the relations in $\mathcal{K}_0T(\mathbf{Z}G)$ (because a short exact sequence of cohomologically trivial $\mathbf{Z}G$-modules necessarily remains exact over $\mathbf{Z}N(H)$ upon fixing under the subgroup H—then apply 2.18(iv)). Since $\mathcal{K}_0T(\mathbf{Z}G)$ is generated by classes $(\mathbf{Z}G/I)$ where I is a locally-free ideal of $\mathbf{Z}G$, we can assume that $T = \mathbf{Z}G/I$. Now $I = \alpha\mathbf{Z}G$ for some $\alpha \in \mathcal{J}(\mathbf{Q}G)$, and $h = \operatorname{Det}\alpha$ represents (T). By 2.6 $g = \mathrm{AI}\circ h \in I(G, \overline{\mathbf{Q}})$. Further, $g_r = \mathrm{AI} \circ \operatorname{Det}\alpha_r$ (where AI is defined on the subgroup $U^\times_{\mathcal{R}}$ of $\mathcal{J}(U)$) by **[Fr1]** II Lemma 2.1. Since $g_r \in \operatorname{Hom}_{\Omega_{\mathbf{Q}_r}}(R_G(\overline{\mathbf{Q}_r}), \mathcal{I}_{\overline{\mathbf{Q}_r}})$ by 2.14, we only have to show (changing notation for the local case) that for each $(C, e) \in \mathcal{S}^r(G)$

$$(2.20) \qquad (\mathrm{coinf}_{C_\times}^{C} \mathrm{res}_C^G \circ \mathrm{Det}\, \alpha(\chi)) = \mathrm{ord}_{\mathbf{Z}_r}(T^{C_r} e).$$

But $\mathrm{res}_C^G \mathrm{Det}\, \alpha$ represents $\mathrm{res}_C^G(T)$ in $\mathcal{K}_0T(\mathbf{Z}_r C)$. So we may assume that $G = C$. Further, $\mathrm{coinf}_{C_\times}^{C} \mathrm{Det}\, \alpha$ represents $\mathrm{coinf}_{C_\times}^{C}(T) = (T^{C_r})$ in $\mathcal{K}_0T(\mathbf{Z}_r C_\times)$. So we may assume that $r \nmid |C|$ and 2.20 becomes

$$(2.21) \qquad (\mathrm{Det}_\chi\, \alpha) = \mathrm{ord}_{\mathbf{Z}_r}(Te) = \mathrm{ord}_{\mathbf{Z}_r}(\mathbf{Z}_r Ce/\alpha \mathbf{Z}_r Ce).$$

Now $V = \mathbf{Q}_r Ce$ is a *left* $\mathbf{Q}_r C$-module with character χ. Let $\widehat{\alpha}: V \to V$ be the $\mathbf{Q}_r$-linear map given by left multiplication by α. Then both sides of 2.21 are $(\det_{\mathbf{Q}_r} \widehat{\alpha})$. ∎

Note that the canonical factorisation g in the above theorem is the image of (T) under the natural surjection $\mathcal{K}_0T(\mathbf{Z}G) \to \mathcal{K}_0T(\mathcal{M}_G)$ (recalling the identification 2.6 and the Hom-description of $\mathcal{K}_0T(\mathbf{Z}G)$).

It is not difficult to show that g is also a factorisation. As our principal interest is in computing invariants, we shall not pursue this.

We shall need in §3 two functorial properties of canonical factorisations under change of group. For those induced by cohomologically trivial modules as in 2.19, the results are obvious because of the functorial properties of $\mathcal{K}_0T(\mathbf{Z}G)$ and its Hom-description, and the fact that π'_G is surjective. However more generally we have (to simplify notation we assume that the usual injective map i is the inclusion, but the result holds generally)

2.22 Theorem. *Let N be a normal subgroup of G and let $\overline{G} = G/N$. Let $V \subseteq W$ be $\mathbf{Z}\overline{G}$-modules such that W/V is finite. Assume that $f^*_{\overline{G},V,W}$ has the canonical factorisation g. Then $\mathrm{cocut}_{\overline{G}}^{G}\, g$ is the canonical factorisation of $f^*_{G,V,W}$.*

Proof : Let $(C, e) \in \mathcal{S}^r(G)$. It suffices to show that

$$(2.23) \qquad \mathrm{res}_C^G\, \mathrm{cocut}_{\overline{G}}^{G}\, g_r(1_{C_r}, \chi) = f^r_{G,V,W}(C, e),$$

where χ is as in 2.9 and $\mathrm{inf}_{C_\times}^{C} \chi = (1_{C_r}, \chi)$, in the obvious notation. Let $\overline{C_\times}$ be $C_\times / C_\times \cap N$. Let $\mathrm{cut}_{\overline{C_\times}}^{C_\times} \chi = \overline{\chi}$, the character of $\mathbf{Z}_r \overline{C_\times}\, \overline{e}$ where $\overline{e}$ is the image of e in $\mathbf{Z}_r \overline{C_\times}$.

Let $\theta \in C^\dagger$. Then

$$\text{(2.24)} \qquad \operatorname{cut}^G_{\overline{G}} \operatorname{ind}^G_C \theta = \operatorname{ind}^{\overline{G}}_{\overline{C}} \operatorname{cut}^C_{\overline{C}} \theta,$$

where $\overline{C}$ denotes CN/N or $C/C \cap N$, as appropriate. Thus the left hand side of 2.23 is

$$\begin{aligned} g_r(\operatorname{cut}^G_{\overline{G}} \operatorname{ind}^G_C(1_{C_r}, \chi)) &= g_r(\operatorname{ind}^{\overline{G}}_{\overline{C}} \operatorname{cut}^C_{\overline{C}}(1_{C_r}, \chi)) \\ &= g_r(\operatorname{ind}^{\overline{G}}_{\overline{C}}(1_{\overline{C_r}}, \overline{\chi})) \\ &= \begin{cases} 1, & \text{if } \ker\chi \not\subseteq C_\times \cap N; \\ f^r_{\overline{G},V,W}(\overline{C}, \overline{e}), & \text{otherwise.} \end{cases} \\ &= f^r_{G,V,W}(C, e). \quad \blacksquare \end{aligned}$$

2.25 Theorem. *Let $K \in \mathcal{S}(G)$ and let $V \subseteq W$ be $\mathbf{Z}K$-modules such that W/V is finite. Assume that $f^*_{K,V,W}$ has the canonical factorisation g. Then $\operatorname{ind}^G_K g$ is the canonical factorisation of $f^*_{G,\operatorname{ind}^G_K V,\operatorname{ind}^G_K W}$, where $\operatorname{ind}^G_K V$ denotes $\mathbf{Z}G \otimes_{\mathbf{Z}K} V$.*

Proof : Let $(C, e) \in \mathcal{S}^r(G)$. It suffices to show that

$$\text{(2.26)} \qquad \operatorname{res}^G_C \operatorname{ind}^G_K g_r(1_{C_r}, \chi) = f^r_{G,\operatorname{ind}^G_K V,\operatorname{ind}^G_K W}(C, e).$$

where χ is as in 2.9. Let a run over representatives for the double cosets $C\backslash G/K$. Let $\theta \in C^\dagger$. By the Mackey subgroup theorem

$$\text{(2.27)} \qquad \operatorname{res}^G_K \operatorname{ind}^G_C \theta = \bigoplus_a \operatorname{ind}^K_{K\cap C^a} \operatorname{res}^{C^a}_{K\cap C^a} \theta^a.$$

Let $e^a = a^{-1}ea$. Let e_a be the unique indecomposable idempotent of $\mathbf{Q}_r[(K \cap C^a)_\times]$ such that $e_a e^a = e^a$. Let χ_a be the character of $\mathbf{Q}_r[(K \cap C^a)_\times]e_a$. Let m_a be the degree of the "abstract" field extension $\mathbf{Q}_r C^a_\times e^a / \mathbf{Q}_r[(K \cap C^a)_\times]e_a$. Let $\theta = (1_{C_r}, \chi)$. It follows that

$$\text{(2.28)} \qquad \operatorname{res}^{C^a}_{K\cap C^a} \theta^a = m_a(1_{(K\cap C^a)_r}, \chi_a).$$

Then by 2.27 the left hand side of 2.26 is

$$
\begin{aligned}
g_r(\operatorname{res}^G_K \operatorname{ind}^G_C \theta) &= \prod_a g_r\left(\operatorname{ind}^K_{K\cap C^a} \operatorname{res}^{C^a}_{K\cap C^a} \theta^a\right) \\
&= \prod_a \operatorname{res}^K_{K\cap C^a} g_r\left\{\left(1_{(K\cap C^a)_r}, \operatorname{res}^{C^a_\times}_{(K\cap C^a)_\times} \chi^a\right)\right\} \\
&= \prod_a \operatorname{res}^K_{K\cap C^a} g_r\left\{\left(1_{(K\cap C^a)_r}, \chi_a\right)\right\}^{m_a} \\
&= \prod_a f^r_{K,V,W}(K\cap C^a, \chi_a)^{m_a}.
\end{aligned}
\tag{2.29}
$$

Now a^{-1} runs over representatives of the double cosets $K\backslash G/C$. There is an analogous formula to 2.27 for $\operatorname{res}^G_C \operatorname{ind}^G_K V$. Thus

$$
\begin{aligned}
(\operatorname{ind}^G_K V)^{C_r} &= (\operatorname{res}^G_C \operatorname{ind}^G_K V)^{C_r} \\
&\cong \bigoplus_a \left(\operatorname{ind}^C_{C\cap K^{a^{-1}}} \operatorname{res}^{K^{a^{-1}}}_{C\cap K^{a^{-1}}} V^{a^{-1}}\right)^{C_r} \\
&\cong \bigoplus_a \operatorname{ind}^{C_\times}_{(C\cap K^{a^{-1}})_\times} \left\{\left(\operatorname{res}^{K^{a^{-1}}}_{C\cap K^{a^{-1}}} V^{a^{-1}}\right)^{(C\cap K^{a^{-1}})_r}\right\}.
\end{aligned}
\tag{2.30}
$$

The last isomorphism is by the analogue of 2.24 for modules. By orthogonality of the idempotents, and conjugating by a in the ath factor, there is an isomorphism of $\mathbf{Z}_r$-modules

$$
(\operatorname{ind}^G_K V_r)^{C_r} e \cong \bigoplus_a \mathbf{Z}_r C_\times e^a \otimes_{\mathbf{Z}_r[(K\cap C^a)_\times]e_a} (V_r)^{(K\cap C^a)_r} e_a.
$$

By the definition of m_a it follows immediately that the right hand side of 2.26 is 2.29. ∎

§3. Chinburg's second invariant and a canonical factorisation related to the ring of integers.

In this section we will define $\Omega(N/K, 2)$ and prove that its coset mod $D(\mathbf{Z}\Gamma)$ is determined by the canonical factorisation of

$$f^*_{b\mathcal{O}_K\Gamma, \mathcal{O}_N}$$

in a sense we shall make precise (at the same time we shall show that this canonical factorisation does exist).

Let N/K be a finite normal extension of number fields with Galois group Γ. For each finite prime $\wp$ of K choose a prime $\tilde{\wp}$ of N lying over $\wp$. Let $\Gamma(\tilde{\wp})$ be the decomposition group at $\tilde{\wp}$. Let $\exp_{\tilde{\wp}}$ be the $\tilde{\wp}$-adic exponential function, defined for elements of $N_{\tilde{\wp}}$ sufficiently close to 0.

We shall call $\wp$ *tame* if $N_{\tilde{\wp}}/K_\wp$ is at most tamely ramified; otherwise we shall call $\wp$ *wild*. We shall also call $\wp$ ramified or unramified in an analogous way. If $\wp$ is tame then $\mathcal{O}_{N,\tilde{\wp}}$ is free as $\mathcal{O}_{K,\wp}\Gamma(\tilde{\wp})$-module, by E. Noether's theorem. Thus we can choose $a \in \prod_\wp \mathcal{O}^\times_{N,\wp}$ ($\wp$ running over finite primes of K) such that

(3.1)
$$(i)\ a_\wp \in \mathcal{O}_{N,\tilde{\wp}} \text{ and } a_\wp K_\wp \Gamma(\tilde{\wp}) = N_{\tilde{\wp}} \text{ for each } \wp.$$
$$(ii)\ a_\wp \mathcal{O}_{K,\wp}\Gamma(\tilde{\wp}) = \mathcal{O}_{N,\tilde{\wp}} \text{ for each tame } \wp.$$

Since $N_\wp$ is isomorphic to the induced Γ-Galois algebra $\mathrm{Map}_{\Gamma(\tilde{\wp})}(\Gamma, N_{\tilde{\wp}})$ the conditions 3.1 imply the corresponding "semilocal" conditions obtained by replacing $\Gamma(\tilde{\wp})$ by Γ and $\tilde{\wp}$ by $\wp$.

We shall abbreviate $a_\wp \mathcal{O}_{K,\wp}\Gamma(\tilde{\wp})$ by $X_{\tilde{\wp}}$. Then $X = a\mathcal{O}_K\Gamma$ is the locally-free $\mathcal{O}_K\Gamma$-submodule of N whose $\wp$-adic completion is

$$X_\wp = a_\wp \mathcal{O}_{K,\wp}\Gamma \cong \mathrm{Map}_{\Gamma(\tilde{\wp})}(\Gamma, X_{\tilde{\wp}}),$$

the right hand side being the induced Γ-module of $X_{\tilde{\wp}}$ (the above is all taken from **[Wi2]** §3).

For the purposes of computation we shall require in addition

$$\text{(iii)}\begin{cases}\text{for each wild } \wp,\ a_\wp \in \breve{\wp}\mathcal{O}_{N,\breve{\wp}} \text{ and} \\ \qquad \exp_{\breve{\wp}}\colon X_{\breve{\wp}} \to 1 + X_{\breve{\wp}} \\ \text{is a well-defined isomorphism.}\end{cases}$$

For each wild $\wp$, let $\alpha_{\breve{\wp}} \in \mathrm{Ext}^2_{\mathbf{Z}\Gamma(\breve{\wp})}(\mathbf{Z}, N^\times_{\breve{\wp}})$ (*i.e.* $H^2(\Gamma(\breve{\wp}), N^\times_{\breve{\wp}})$) be the canonical class of $N_{\breve{\wp}}/K_\wp$. Let $q_{\breve{\wp}}$ be the natural projection

$$N^\times_{\breve{\wp}} \to N^\times_{\breve{\wp}}/(1 + X_{\breve{\wp}}).$$

As in [**Wi2**] §6, $q_{\breve{\wp}}\alpha_{\breve{\wp}} \in \mathrm{Ext}^2_{\mathbf{Z}\Gamma(\breve{\wp})}(\mathbf{Z}, N^\times_{\breve{\wp}}/(1 + X_{\breve{\wp}}))$ is a w.h.e. of $\mathbf{Z}\Gamma(\breve{\wp})$-modules (c.f. Ch. I, §§2,5) giving rise to an element

$$\partial(q_{\breve{\wp}}\alpha_{\breve{\wp}}) \in Cl(\mathbf{Z}\Gamma(\breve{\wp})).$$

Then we define

$$\Omega(N/K, 2) = \sum_{\wp \text{ wild}} \mathrm{ind}^{\Gamma}_{\Gamma(\breve{\wp})}\, \partial(q_{\breve{\wp}}\alpha_{\breve{\wp}}) + (X) \in Cl(\mathbf{Z}\Gamma). \tag{3.2}$$

(c.f. [**Wi2**], where it is proved that 3.2 is the same as Chinburg's original definition of $\Omega(N/K, 2)$ in [**Ch2**])

We shall concentrate on the local factor $\partial(q_{\breve{\wp}}\alpha_{\breve{\wp}})$. Then let $\breve{\wp}|\wp|p$ with $\wp$ wild. For brevity write $G = \Gamma(\breve{\wp})$, $L = N_{\breve{\wp}}$ and $F = K_\wp$. We can find a 2-extension

$$1 \to L^\times/(1 + X_{\breve{\wp}}) \xrightarrow{\epsilon} A \xrightarrow{\mu} \mathbf{Z}G \to \mathbf{Z} \to 0 \tag{3.3}$$

whose class is $q_{\breve{\wp}}\alpha_{\breve{\wp}}$, where the map $\mathbf{Z}G \to \mathbf{Z}$ is the augmentation, with kernel the augmentation ideal $\mathrm{Aug}(\mathbf{Z}G)$. Thus A is cohomologically trivial and

$$\partial(q_{\breve{\wp}}\alpha_{\breve{\wp}}) = (A) - (\mathbf{Z}G) \tag{3.4}$$

where A determines a class (A) by resolution by locally free modules. Let $\sigma_G = \sum_{g \in G} g$ be the trace element of $\mathbf{Z}G$ and let $n = |G|$. Because $\mathbf{Z}G$ is free, there exists a map δ making the right hand square of the following diagram commute (the lower row is taken from 3.3)

$$\text{(3.5)} \qquad \begin{array}{ccccccccc} 0 & \to & \mathbf{Z} & \xrightarrow{\phi} & \mathbf{Z}G & \to & (n-\sigma_G)\mathbf{Z}G & \to & 0 \\ & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle i} & & \\ 1 & \to & L^\times/(1+X_{\tilde{\wp}}) & \xrightarrow{\epsilon} & A & \xrightarrow{\mu} & \mathrm{Aug}(\mathbf{Z}G) & \to & 0 \end{array}$$

where i is the inclusion map and the maps $\mathbf{Z} \to \mathbf{Z}G$ and $\mathbf{Z}G \to (n - \sigma_G)\mathbf{Z}G$ are multiplication by the central elements σ_G and $n - \sigma_G$ respectively. By diagram chasing some map γ exists making the diagram commute.

3.6 Lemma. *All the vertical arrows in 3.5 may be chosen to be injective.*

Proof : If γ is injective there is nothing to prove. Otherwise, let π_F be a uniformiser for F, let $M = L^\times/(1+X_{\tilde{\wp}})$ and let $\alpha: \mathbf{Z} \to M$ and $\beta: \mathbf{Z}G \to M$ be the unique $\mathbf{Z}G$-maps which send 1 to the coset of π_F. If I and J are subgroups of $\mathbf{Z}$ such that $I \cap J = 0$, it follows that $I = 0$ or $J = 0$. Now α is injective, because $1 + X_{\tilde{\wp}} \subseteq \mathcal{O}_L^\times$. If we take $I = \ker\gamma \neq 0$ and $J = \ker(\gamma + |G|\alpha)$ it follows that $J = 0$. But $|G|\alpha = \beta\phi$. Since $\mu\epsilon = 0$ it follows that the diagram commutes with γ replaced by the injective map $\gamma + |G|\alpha$ and δ replaced by $\delta + \epsilon\beta$. ∎

Then by considering $\mathbf{Z}$-ranks in 3.5 it follows that

$$\text{(3.7)} \qquad \mathrm{coker}\,\delta \stackrel{def}{=} T = T_{\tilde{\wp}}$$

is a *finite*, cohomologically trivial $\mathbf{Z}G$-module.

There is a commutative diagram

$$\text{(3.8)} \qquad \begin{array}{ccc} \mathcal{K}_0T(\mathbf{Z}G) & \xrightarrow{\pi'_G} & \mathcal{K}_0T(\mathcal{M}_G) \\ \downarrow{\scriptstyle c_{\mathbf{Z}G}} & & \downarrow{\scriptstyle c_{\mathcal{M}_G}} \\ Cl(\mathbf{Z}G) & \xrightarrow{\pi_G} & Cl(\mathcal{M}_G) \end{array}$$

in which all the maps are surjective. The horizontal maps are induced by $- \otimes_{\mathbf{Z}G} \mathcal{M}_G$. If

$$0 \to U \to V \to T \to 0$$

is an exact sequence of $\mathbf{Z}G$-modules in which U and V are locally free of the same rank (so T is finite), then

$$c_{\mathbf{Z}G}(T) = (V) - (U),$$

and analogously for $c_{\mathcal{M}_G}$. Thus

$$\pi_G \partial(q_{\tilde{\wp}} \alpha_{\tilde{\wp}}) = \pi_G c_{\mathbf{Z}G}(T) = c_{\mathcal{M}_G}(\text{ C. F. of } f_T^*) \in Cl(\mathcal{M}_G), \tag{3.9}$$

by 3.4, 3.7 and 2.19. We shall eventually replace T by the finite module $\mathcal{O}_L/X_{\tilde{\wp}}$ in 3.9. We shall then use this "local" result, for each $\wp$, to establish the analogous global result which is the aim of this section (we now have the notation to state this precisely—see 3.37).

Let

$$M = \mathcal{O}_L^{\times}/(1 + X_{\tilde{\wp}}). \tag{3.10}$$

Let c be the positive rational

$$c = \left| \frac{F^{\times}/(1 + X_{\tilde{\wp}})^G}{\gamma(\mathbf{Z})} \right| /n|M^G|. \tag{3.11}$$

c is a quotient of integers $c1/c2$. Let f_c^* be the product $f_{c1\mathbf{Z},\mathbf{Z}}^*(f_{c2\mathbf{Z},\mathbf{Z}}^*)^{-1}$.

Let $\overline{G} = G/G_0$ where G_0 is the inertia subgroup of G.

Let k_L be the residue class field of L.

For each $H \in \mathcal{S}(G)$ write $e(L^H/F)$ and $f(L^H/F)$ for the ramification index and residue class degree of L^H/F.

From **[Fr2]** §2 (up to Theorem 1) there is an exact sequence

$$0 \rightarrow \mathrm{Aug}(\mathbf{Z}\overline{G}) \xrightarrow{j} \mathbf{Z}\overline{G}/\sigma_{\overline{G}}\mathbf{Z}\overline{G} \rightarrow \mathbf{Z}/|\overline{G}|\mathbf{Z} \rightarrow 0 \tag{3.12}$$

3.13 Theorem. *Let T be as in 3.7. Let M be as 3.10. Then*

$$f_T^* = f_M^* f_c^* f_{n\mathbf{Z}G,\mathbf{Z}G}^* (f_j^*)^{-1}$$

Remark: The first part of the proof consists of computing values $|\mathrm{coker}(\alpha^H)|$ where α is a $\mathbf{Z}G$-injection of finite cokernel and H is a subgroup of G, and of the behaviour of 3.5 after fixing under H (c.f. the discussion of factorisability).

Let $(C, e) \in \mathcal{S}^r(G)$. There are two cases. If e is the idempotent of $1_{C_\times}$ then

$$f^r_\alpha(C, e) = |\operatorname{coker}(\alpha^C)|\mathbf{Z}_r,$$

so the next part of the proof applies the first part with $H = C$.

In the second case (e is *not* the idempotent of $1_{C_\times}$) we make use of the first part with $H = C_r$. After fixing 3.5 under C_r, it only remains (in order to calculate the $f^r_\alpha(C, e)$) to complete at r and multiply by e. In the last process we use the result $e\sigma_G = 0$ to simplify the results.

Proof : Let $H \in \mathcal{S}(G)$. The diagram 3.5 remains exact on fixing under H, because $H^1(H, \mathbf{Z}) = 0 = H^1(H, L^\times) = H^1(H, L^\times/(1+X_{\check{\wp}}))$, the last equality because $1+X_{\check{\wp}} \cong X_{\check{\wp}}$ is cohomologically trivial. Thus by 2.18(iv)

$$f^*_\gamma f^*_i = f^*_\delta = f^*_T, \tag{3.14}$$

the last equation by 2.18(iiia) and 2.18(iii). We can write γ as a composition

$$\gamma: \mathbf{Z} \stackrel{\gamma_1}{\to} \left(\frac{L^\times}{1+X_{\check{\wp}}}\right)^G \stackrel{\gamma_2}{\to} \frac{L^\times}{1+X_{\check{\wp}}}$$

where γ_2 is the inclusion map. By 2.18(i)

$$f^*_\gamma = f^*_{\gamma_1} f^*_{\gamma_2}. \tag{3.15}$$

Let $v_H: (L^H)^\times \to \mathbf{Z}$ be the additive valuation which maps a uniformiser of L^H to 1. Let $i_1: \mathcal{O}^\times_F \to \mathcal{O}^\times_L$ and $i_2: F^\times \to L^\times$ be the inclusions. Since $(1 + X_{\check{\wp}})^H \subseteq (\mathcal{O}^\times_L)^H = (\mathcal{O}_{L^H})^\times = \ker v_H$, there is an induced exact diagram

$$\begin{array}{ccccccccc} 1 & \to & \mathcal{O}^\times_F/(1+X_{\check{\wp}})^G & \subsetneq & F^\times/(1+X_{\check{\wp}})^G & \stackrel{\widetilde{v_G}}{\to} & \mathbf{Z} & \to & 0 \\ & & \downarrow \tilde{i}_1^H & & \downarrow \tilde{i}_2^H & & \downarrow & & \\ 1 & \to & (\mathcal{O}_{L^H})^\times/(1+X_{\check{\wp}})^H & \subsetneq & (L^H)^\times/(1+X_{\check{\wp}})^H & \stackrel{\widetilde{v_H}}{\to} & \mathbf{Z} & \to & 0 \end{array} \tag{3.16}$$

where the vertical maps are injective, and the map $\mathbf{Z} \to \mathbf{Z}$ is multiplication by $e(L^H/F)$.

By the Snake lemma

$$|\operatorname{coker}(\tilde{i_2}^H)| = |\operatorname{coker}(\tilde{i_1}^H)| e(L^H/F). \tag{3.17}$$

Since $1 + X_{\breve{\wp}}$ is cohomologically trivial

$$\begin{cases} \text{there are } \mathbf{Z}N(H)\text{-isomorphisms} \\ \operatorname{coker}(\tilde{i_2}^H) \cong \operatorname{coker}(\gamma_2^H) \text{ and } (\mathcal{O}_{L^H})^\times/(1 + X_{\breve{\wp}})^H \cong M^H. \end{cases} \tag{3.18}$$

Since

$$\widehat{H}^0(H, \operatorname{Aug}\mathbf{Z}G) = \widehat{H}^{-1}(H, \mathbf{Z}) = 0 = H^1(H, \mathbf{Z}) = \widehat{H}^0(H, (n - \sigma_G)\mathbf{Z}G),$$

we have

$$\frac{\operatorname{Aug}\mathbf{Z}G^H}{((n - \sigma_G)\mathbf{Z}G)^H} = \frac{\operatorname{Aug}\mathbf{Z}G\sigma_H}{(n - \sigma_G)\mathbf{Z}G\sigma_H} = A, \text{ say.}$$

Let $\mathcal{R}$ be a left transversal of H in G, containing 1. Then the generators

$$\{ (g - 1)\sigma_H : g \in \mathcal{R} \setminus 1 \}$$

of $\operatorname{Aug}\mathbf{Z}G\sigma_H$ are free, since the left cosets of H in G are disjoint. Clearly the set $\{ (ng - \sigma_G)\sigma_H : g \in \mathcal{R} \}$ generates $(n - \sigma_G)\mathbf{Z}G\sigma_H$. The equation

$$(ng - \sigma_G)\sigma_H = n(g - 1)\sigma_H + (n - \sigma_G)\sigma_H$$

(valid for $g \in \mathcal{R}$) shows that

$$\{ (n - \sigma_G)\sigma_H, n(g - 1)\sigma_H : g \in \mathcal{R} \setminus 1 \}$$

also generates $(n - \sigma_G)\mathbf{Z}G\sigma_H$. Thus A is the abelian group with generators $\{ \lambda_g : g \in \mathcal{R} \setminus 1 \}$

By 3.21 to prove the formula for $f_T^r(C, e_{C_\times})$ it suffices to show

$$\left|T^C\right| = \left|M^C\right| c \left|\mathbf{Z}G^C : n\mathbf{Z}G^C\right| \left|\operatorname{coker}(j^C)\right|^{-1}.$$

By 3.22 the right hand side is

$$\left|M^C\right| cn^{|G:C|} f(L^C/F)^{-1} \overset{3.11}{=} \left|M^C\right| \left|M^G\right|^{-1} \left|\operatorname{coker}(\gamma_1^C)\right| n^{|G:C|-1} f(L^C/F)^{-1}$$

$$\overset{3.15}{=} \left|M^C\right| \left|M^G\right|^{-1} \left|\operatorname{coker}(\gamma^C)\right| \left|\operatorname{coker}(\gamma_2^C)\right|^{-1} n^{|G:C|-1} f(L^C/F)^{-1}$$

$$\overset{3.18,\, 3.16}{=} \left|\operatorname{coker}(\tilde{i_1}^C)\right| \left|\operatorname{coker}(\gamma^C)\right| \left|\operatorname{coker}(\tilde{i_2}^C)\right|^{-1} n^{|G:C|-1} f(L^C/F)^{-1}$$

$$\overset{3.17}{=} \left|\operatorname{coker}(\gamma^C)\right| n^{|G:C|-1} e(L^C/F)^{-1} f(L^C/F)^{-1}$$

$$\overset{3.20}{=} \left|\operatorname{coker}(\gamma^C)\right| n^{|G:C|-2} |C|$$

$$\overset{3.19}{=} \left|\operatorname{coker}(\gamma^C)\right| \left|\operatorname{coker}(i^C)\right|$$

$$\overset{3.14}{=} \left|T^C\right|$$

If $e \neq e_{C_\times}$ then

$$f_T^r(C, e) \overset{3.14}{=} f_\gamma^r(C, e) f_i^r(C, e)$$

$$\overset{3.15}{=} f_{\gamma_1}^r(C, e) f_{\gamma_2}^r(C, e) f_i^r(C, e)$$

$$\overset{3.25}{=} f_c^r(C, e) f_j^r(C, e)^{-1} f_{\gamma_2}^r(C, e) f_i^r(C, e)$$

$$\overset{3.24}{=} f_c^r(C, e) f_j^r(C, e)^{-1} f_M^r(C, e) f_i^r(C, e)$$

$$\overset{3.23}{=} f_c^r(C, e) f_j^r(C, e)^{-1} f_M^r(C, e) f_{n\mathbf{Z}G, \mathbf{Z}G}^r(C, e)$$

as required.

and relations

$$n\lambda_g = 0 \text{ for each } g \in \mathcal{R} \setminus 1, \text{ and } |H| \sum_{g \in \mathcal{R}\setminus 1} \lambda_g = 0$$

(since $(n - \sigma_G)\sigma_H = -|H| \sum_{g\in\mathcal{R}\setminus 1}(g-1)\sigma_H$). Calculation of a determinant gives

$$|A| = |\operatorname{coker}(i^H)| = |H| n^{|G:H|-2}. \tag{3.19}$$

Now

$$e(L^H/F) f(L^H/F)|H| = n. \tag{3.20}$$

Let $(C, e) \in \mathcal{S}^r(G)$. If $e = e_{C_\times}$ (the idempotent of $1_{C_\times}$) then

$$f_T^r(C, e) = \operatorname{ord}_{\mathbf{Z}_r}(T_r^C) = r\text{-part of } |T^C|, \tag{3.21}$$

identifying principal ideals and their generators. Also we have

$$f(L^H/F) = |\operatorname{coker}(j^H)| \text{ and } |\mathbf{Z}G^H/(n\mathbf{Z}G)^H| = n^{|G:H|}, \tag{3.22}$$

the first equality by [**Fr2**] Theorem 1. If we put $H = C$ then 3.14-3.22 give the formula for $f_T^r(C, e_{C_\times})$ by successive substitution.* If $e \neq e_{C_\times}$ then e annihilates σ_G, and hence G-trivial modules. Thus

$$(n - \sigma_G)\mathbf{Z}_r Ge = n\mathbf{Z}_r Ge \quad \text{and} \quad \operatorname{Aug}(\mathbf{Z}_r G)e = \mathbf{Z}_r Ge.$$

Hence

$$f_i^r(C, e) = f_{n\mathbf{Z}G,\mathbf{Z}G}^r(C, e). \tag{3.23}$$

From now on we put $H = C_r$. By the first part of 3.18 and 2.18(ii) we have the first equality below.

$$f_{\gamma_2}^r(C, e) = \operatorname{ord}_{\mathbf{Z}_r}(\operatorname{coker}(\tilde{i}_2^{C_r})_r e) = f_M^r(C, e). \tag{3.24}$$

The second equality follows after we apply $(-\otimes_{\mathbf{Z}} \mathbf{Z}_r)e$ and the Snake lemma to 3.16 (observe that $(\mathbf{Z}/e(L^H/F)\mathbf{Z})_r e = 0$) and use the second part of 3.18. Now

$$f_{\gamma_1}^r(C, e) = f_c^r(C, e) = 1 = f_j^r(C, e), \tag{3.25}$$

the final equality by applying $((-)_*^{C_r} \otimes_{\mathbf{Z}} \mathbf{Z}_r)e$ to 3.12, again observing that e annihilates G-trivial modules. By substitution the formula for $f_T^r(C, e)$ follows from 3.14, 3.15 and 3.23-3.25. ∎

* see extra sheet

We let the reader verify that

$$\chi \mapsto \begin{cases} c, & \text{if } \chi = 1_G; \\ 1, & \text{otherwise.} \end{cases}$$

is the canonical factorisation of f_c^*, and that

$$\chi \mapsto \left(n^{\deg \chi}\right)$$

is the canonical factorisation of $f^*_{n\mathbf{Z}G,\mathbf{Z}G}$, where χ runs over $\mathrm{Irr}(G)$.

From **[Fr2]** the function $f^*_{\overline{G},j}$ has the canonical factorisation

$$\theta \mapsto \mathbf{s}(\theta) \text{ for each } \theta \in \overline{G}^{\dagger}.$$

where

$$\mathbf{s}(\theta) = \begin{cases} 1, & \text{if } \theta = 1_{\overline{G}}; \\ \text{the ideal of } \mathbf{Q}(\theta) \text{ generated by} & \text{otherwise,} \\ \quad \text{the } \theta(g) - 1 \text{ for each } g \in \overline{G}, & \end{cases}$$

and θ runs over $\mathrm{Irr}(\overline{G})$. Fröhlich only proves that this is a factorisation, which is generally a weaker result. However, if $(C, e) \in \mathcal{S}^r(\overline{G})$ and $e \neq e_{C_\times}$, then $f^r_{\overline{G},j}(C, e) = 1$ (as in the proof above) and this gives the result we need. Then by 2.22 $f^*_{G,j}$ also has a canonical factorisation. It now follows by 3.13 that f^*_M has a canonical factorisation, namely the product of the canonical factorisations of f^*_T, $(f^*_c)^{-1}$, $(f^*_{n\mathbf{Z}G,\mathbf{Z}G})^{-1}$ and f^*_j. Except for those of f^*_T and f^*_M, all these canonical factorisations lie in $P^+(G, \overline{\mathbf{Q}})$. This is obvious for all but that of f^*_j; but by 2.22 this is obtained from a canonical factorisation (with principal values) over the cyclic group G/G_0, which has no irreducible symplectic characters. Hence the process of cutting characters from G to $\overline{G}$ eliminates such characters. So the canonical factorisation of f^*_j also lies in $P^+(G, \overline{\mathbf{Q}})$.

The final reduction involves a switch from multiplicative to additive Galois modules. Here the choice of $X_{\tilde{\wp}}$ (see condition (iii) after 3.1) becomes important.

Let

$$A = \mathcal{O}_L / X_{\tilde{\wp}}. \tag{3.26}$$

3.27 Theorem. *Let M be as in 3.10 and A be as in 3.26. Then*

$$f_M^* = f_A^* f_{k_L^\times}^* (f_{k_L}^*)^{-1}.$$

Remark: Let $\wp_L = \operatorname{rad} \mathcal{O}_L$. The proof works by using filtrations by powers of $\wp_L$ (the additive case) and of $1 + \wp_L$ (the multiplicative case). As is well known, the successive quotients in these filtrations are isomorphic. Condition (iii) on $X_{\tilde{\wp}}$ allows a similar result (at a sufficient depth in the filtrations) when the terms are factored by $X_{\tilde{\wp}}$ (additive case) or $1 + X_{\tilde{\wp}}$ (multiplicative case). The information is passed through the filtrations by use of 2.18.

Proof : Let $m: 1 + X_{\tilde{\wp}} \to \mathcal{O}_L^\times$ and $a: X_{\tilde{\wp}} \to \mathcal{O}_L$ be the inclusions. Suppose that $X_{\tilde{\wp}} \subseteq \wp_L^t$. By assumption (iii) on $X_{\tilde{\wp}}$ we may assume that $\exp_{\tilde{\wp}}$ induces an isomorphism

$$\wp_L^t / X_{\tilde{\wp}} \cong (1 + \wp_L^t)/(1 + X_{\tilde{\wp}}). \tag{3.28}$$

Now let a_l for $l = 0, \ldots, t+1$ be the inclusions as follows.

$$a_0: \wp_L \to \mathcal{O}_L, \qquad a_{t+1}: X_{\tilde{\wp}} \to \wp_L^t$$

$$a_l: \wp_L^{l+1} \to \wp_L^l, \qquad \text{for each } l = 1, \ldots, t.$$

Similarly define the inclusions m_l ($m_{t+1}: 1 + X_{\tilde{\wp}} \to 1 + \wp_L^t$, etc). By 2.18(i)

$$f_a^* = \prod_{l=0}^{t+1} f_{a_l}^* \quad \text{and} \quad f_m^* = \prod_{l=0}^{t+1} f_{m_l}^*. \tag{3.29}$$

By 2.18(iiia) and 2.18(iii)

$$f_a^* = f_A^*, \quad f_m^* = f_M^*, \quad f_{a_{t+1}}^* = f_{\operatorname{cok} a_{t+1}}^* \quad \text{and} \quad f_{m_{t+1}}^* = f_{\operatorname{cok} m_{t+1}}^*. \tag{3.30}$$

Let $H \in \mathcal{S}(G)$. Then $\mathcal{O}_L^H = \mathcal{O}_{L^H}$, $\wp_L^H = \wp_{L^H}$ and $k_L^H = k_{L^H}$. Similarly for $(\mathcal{O}_L^\times)^H$, etc.

Thus by 2.18(iii)

$$f^*_{a_0} = f^*_{k_L} \quad \text{and} \quad f^*_{m_0} = f^*_{k_L^\times} \tag{3.31}$$

By 3.29-3.31 it suffices to show that

$$f^*_{a_l} = f^*_{m_l} \quad \text{for } l = 1, \ldots, t+1.$$

For $l = t+1$ this follows by 3.28, 3.30 and 2.18(ii).

For the other l this follows because the well-known isomorphism

$$\wp_L^l/\wp_L^{l+1} \cong (1+\wp_L^l)/(1+\wp_L^{l+1})$$

restricts to an isomorphism of $\mathbf{Z}N(H)$-submodules

$$(\wp_L^l)^H/(\wp_L^{l+1})^H \cong (1+\wp_L^l)^H/(1+\wp_L^{l+1})^H,$$

since $(1+\wp_L^l)^H = 1 + (\wp_L^l)^H$. Then apply 2.18(ii). ∎

In order to prove that $f^*_{X_{\hat{\wp}}, \mathcal{O}_L}$ has a canonical factorisation and

$$(\text{C. F. of } f^*_T)\,.\,(\text{C. F. of } f^*_{X_{\hat{\wp}}, \mathcal{O}_L})^{-1} \in P^+(G, \overline{\mathbf{Q}}) \tag{3.32}$$

we only need—in view of 2.22, 3.13 and 3.27—to show that $f^*_{k_L}$ and $f^*_{k_L^\times}$ have canonical factorisations which lie in $P^+(G, \overline{\mathbf{Q}})$ in the case where L/F is unramified. In this case we can identify G with $\mathrm{Gal}(k_L/k_F)$.

3.33 Lemma. *([Ch2] Lemma 4.3)*

Let l/k be a finite extension of finite fields and let $\mathcal{F}$ be the Frobenius element of $G = \mathrm{Gal}(l/k)$. Then there are exact sequences of $\mathbf{Z}G$-modules

$$0 \to p\mathbf{Z}G^{(f)} \xrightarrow{i} \mathbf{Z}G^{(f)} \to l \to 0 \tag{3.34}$$

$$0 \to (q-\mathcal{F})\mathbf{Z}G \xrightarrow{i} \mathbf{Z}G \to l^\times \to 1 \tag{3.35}$$

in which p is the characteristic of l, $q = p^f$ is the order of k and i denotes inclusion. The modules $p\mathbf{Z}G^{(f)}$ and $(q-\mathcal{F})\mathbf{Z}G$ are free of ranks f and 1, respectively. ∎

3.36 Remark: In the unramified case, it is well known that both k_L and $k_L^\times$ are cohomologically trivial. However, 3.34 and 3.35 show the stronger result that they have class 0 in $Cl(\mathbf{Z}G)$ under $c_{\mathbf{Z}G}$. Hence the canonical factorisations of $f^*_{k_L}$ and $f^*_{k_L^\times}$ lie in $P^+(G, \overline{\mathbf{Q}})$ and 3.32 follows.

We now have the main result of this section.

3.37 Theorem. *Let Γ, a and X be as in the beginning of this section. Let $b \in X$ be a free generator of N over $K\Gamma$. Then $f^*_{\Gamma, b\mathcal{O}_K\Gamma, \mathcal{O}_N}$ has a canonical factorisation and*

$$\pi_\Gamma \Omega(N/K, 2) = c_{\mathcal{M}_\Gamma}(\textit{the C. F. of } f^*_{b\mathcal{O}_K\Gamma, \mathcal{O}_N}).$$

Proof : If $i: V \to W$ is an injective $\mathcal{O}_K\Gamma$-map with finite cokernel then there are isomorphisms

$$\mathrm{coker}(i^H)_p \cong \mathrm{coker}(i_p^H) \cong \sum_{\wp | p} \mathrm{coker}(i_\wp^H)$$

of $\mathbf{Z}_p N(H)$-modules for each $H \in \mathcal{S}(\Gamma)$. Since

$$\mathrm{coker}(i_\wp^H)_r = \begin{cases} \mathrm{coker}(i_\wp^H), & \text{if } r = p; \\ 0, & \text{otherwise.} \end{cases}$$

it follows (c.f. 2.18(ii),(iv)) that

$$f_i^* = \prod_p f_{i_p}^* = \prod_\wp f_{i_\wp}^*, \tag{3.38}$$

where the products make sense because $f_{i_p}^* = f_{i_\wp}^* = 1$ for almost all $\wp$ and p, as coker i is finite. Let i be the inclusion $X \hookrightarrow \mathcal{O}_N$. If $\wp$ is tame then $i_\wp$ is the identity map. Hence

$$f^*_{X, \mathcal{O}_N} = \prod_{\wp \text{ wild}} f^*_{X_\wp, \mathcal{O}_{N,\wp}}. \tag{3.39}$$

By 3.1 and the remarks following it

$$f^*_{\Gamma, \mathrm{ind}^\Gamma_{\Gamma(\tilde\wp)} X_{\tilde\wp}, \mathrm{ind}^\Gamma_{\Gamma(\tilde\wp)} \mathcal{O}_{N,\tilde\wp}} = f^*_{\Gamma, X_\wp, \mathcal{O}_{N,\wp}}. \tag{3.40}$$

By 3.2

$$\pi_\Gamma \Omega(N/K, 2) = \sum_{\wp \text{ wild}} \pi_\Gamma \operatorname{ind}_{\Gamma(\tilde\wp)}^{\Gamma} \partial(q_{\tilde\wp}\alpha_{\tilde\wp}) + \pi_\Gamma(X)$$

$$\overset{3.9}{=} \sum_{\wp \text{ wild}} \operatorname{ind}_{\Gamma(\tilde\wp)}^{\Gamma} c_{\mathcal{M}_{\Gamma(\tilde\wp)}}(\text{C. F. of } f^*_{T_{\tilde\wp}}) + \pi_\Gamma c_{\mathbf{Z}G}(X/b\mathcal{O}_K\Gamma)$$

$$\overset{3.32}{=} \sum_{\wp \text{ wild}} \operatorname{ind}_{\Gamma(\tilde\wp)}^{\Gamma} c_{\mathcal{M}_{\Gamma(\tilde\wp)}}(\text{C. F. of } f^*_{X_{\tilde\wp},\mathcal{O}_{N,\tilde\wp}}) + c_{\mathcal{M}_\Gamma}\pi'_\Gamma(X/b\mathcal{O}_K\Gamma)$$

$$\overset{3.40,\,2.25}{=} \sum_{\wp \text{ wild}} c_{\mathcal{M}_\Gamma}(\text{C. F. of } f^*_{X_\wp,\mathcal{O}_{N,\wp}}) + c_{\mathcal{M}_\Gamma}\pi'_\Gamma(X/b\mathcal{O}_K\Gamma)$$

$$\overset{3.39}{=} c_{\mathcal{M}_\Gamma}(\text{C. F. of } f^*_{X,\mathcal{O}_N}) + c_{\mathcal{M}_\Gamma}(\text{C. F. of } f^*_{b\mathcal{O}_K\Gamma,X})$$

(the first statement follows)

$$= c_{\mathcal{M}_\Gamma}(\text{C. F. of } f^*_{b\mathcal{O}_K\Gamma,\mathcal{O}_N}). \quad \blacksquare$$

§4. Norm resolvents, Galois Gauss sums and symplectic root numbers.

In this section we shall compute the canonical factorisation which is the subject of 3.37. This function is parametrised by norm resolvents and Galois Gauss sums. All properties of the Gauss sums we shall use are already known. However, we shall do some computations with resolvents, hence for the reader's convenience we give their basic properties here.

Let p be a prime number. Let $k = \mathbf{Q}$ or $\mathbf{Q}_p$. Let F be a finite extension of k in $\overline{k} = \overline{F}$. Let E/F be a finite Galois extension with Galois group G. Let B be a commutative F-algebra. Then $E \otimes_F B$ is free on one generator over BG, where G acts via E. Define the *resolvent mapping* (a BG-homomorphism)

$$\zeta\colon E \otimes_F B \to (E \otimes_F B)G$$

by

$$a \mapsto \sum_{g \in G} a^g g^{-1}.$$

Let $\chi \in R_G(\overline{k})$. Let $a \in E \otimes_F B$. Define

$$(a|\chi) = \operatorname{Det}_\chi \zeta(a),$$

the *resolvent* of a with respect to χ. The properties of resolvents are summarised as follows.

4.1 Theorem. *([Fr1] I §4) Let a be a free generator of $E \otimes_F B$ over BG. Then $\zeta(a) \in (E \otimes_F B)G^\times$ and $(a|\chi) \in (\overline{F} \otimes_F B)^\times$. The map*

$$\chi \mapsto (a|\chi)$$

lies in $\mathrm{Hom}_{\Omega_E}(R_G, (\overline{F} \otimes_F B)^\times)$. ∎

In the case where E/F is abelian and χ is an abelian character, $(a|\chi)$ is the Lagrange resolvent. In the semilocal, unramified case the resolvent generates the trivial ideal:

4.2 Theorem. *([Fr1] I §4) Suppose that $\wp$ is a prime ideal of $\mathcal{O}_F$, unramified in E/F and that a is a free generator of $\mathcal{O}_{E,\wp}$ over $\mathcal{O}_{F,\wp}G$. Then*

$$\zeta(a) \in \mathcal{O}_{E,\wp}G^\times. \quad ∎$$

Next we need a formula for restriction of scalars on class groups in the Hom-description. Let M be a multiplicative Ω_k-module. Let $\{\sigma\}$ be a right transversal of Ω_F in Ω_k. Let $f \in \mathrm{Hom}_{\Omega_F}(R_G, M)$. Then define the *norm* map

$$\mathcal{N}_{F/k}\colon \mathrm{Hom}_{\Omega_F}(R_G, M) \to \mathrm{Hom}_{\Omega_k}(R_G, M)$$

by

$$\left(\mathcal{N}_{F/k} f\right)(\chi) = \prod_{\sigma} f(\chi^{\sigma^{-1}})^{\sigma}.$$

This definition is independent of the choice of $\{\sigma\}$. Return to the global case $k = \mathbf{Q}$, $E/F = N/K$ and $G = \Gamma$.

Theorem. *([Fr1] I Theorem 2) There is a commutative diagram*

$$\begin{array}{ccc} Cl(\mathcal{O}_K\Gamma) & \simeq & \dfrac{\mathrm{Hom}_{\Omega_K}(R_\Gamma, \mathcal{J}(U))}{\mathrm{Hom}_{\Omega_K}(R_\Gamma, U^\times)\,\mathrm{Det}\,\mathcal{U}(\mathcal{O}_K\Gamma)} \\ \downarrow & & \downarrow \mathcal{N}_{K/\mathbf{Q}} \\ Cl(\mathbf{Z}\Gamma) & \simeq & \dfrac{\mathrm{Hom}_{\Omega_\mathbf{Q}}(R_\Gamma, \mathcal{J}(U))}{\mathrm{Hom}_{\Omega_\mathbf{Q}}(R_\Gamma, U^\times)\,\mathrm{Det}\,\mathcal{U}(\mathbf{Z}\Gamma)} \end{array}$$

where the left hand vertical map is induced by restriction of scalars. ∎

Let a be as in 3.1 and let b be as in 3.37. Following Fröhlich ([**Fr1**] I Theorem 4), assuming that U contains N, we define resolvents $(a|\chi) \in \mathcal{J}(U)$ (resp. $(b|\chi) \in U^{\times}$), where $B = \mathrm{Ad}(K)$, the adele ring of K (resp. $B = K$). Then define

$$\mathcal{N}_{K/\mathbf{Q}}(a|\chi) = \prod_{\sigma}(a|\chi^{\sigma^{-1}})^{\sigma}$$

and the same with b replacing a.

Warning. These definitions *do* depend on the choice of $\{\sigma\}$. However ([**Fr1**] I Prop. 4.4(ii))

$$\text{(4.3)} \qquad \begin{cases} \mathrm{AI} \circ \mathcal{N}_{K/\mathbf{Q}}(a|\chi) \quad \text{and} \quad \left(\mathcal{N}_{K/\mathbf{Q}}(b|\chi)\right) \\ \qquad \text{are independent of } \{\sigma\}. \end{cases}$$

By the inclusion $U^{\times} \hookrightarrow \mathcal{J}(U)$ we may regard $(b|\chi)$ as lying in $\mathcal{J}(U)$. A slight modification to Theorem 4 in [**Fr1**] I (replacing $\mathcal{O}_N$ by the locally free module $X = a\mathcal{O}_K\Gamma$) gives

4.4 Theorem. *Let X, a and b be as in 3.37. Then $(X) \in Cl(\mathbf{Z}\Gamma)$ is represented in the Hom-description by the map*

$$\chi \mapsto \mathcal{N}_{K/\mathbf{Q}}(b|\chi)\mathcal{N}_{K/\mathbf{Q}}(a|\chi)^{-1}$$

in $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_{\Gamma}, \mathcal{J}(U))$. ∎

This substitution of the locally free module X (in the wild case) for the locally free module $\mathcal{O}_N$ (in the tame case) will occur repeatedly.

Warning. In [**Fr1**] one has the multiplicative inverse map to that of 4.4, for Fröhlich's map $\mathcal{K}_0T(\mathbf{Z}\Gamma) \to Cl(\mathbf{Z}\Gamma)$ is $-c_{\mathbf{Z}\Gamma}$.

By 4.3 and 2.19 we have

4.5 Theorem. *Let X, a and b be as in 3.37. Then the canonical factorisation of $f^*_{\mathfrak{b}\mathcal{O}_K\Gamma, X}$ is*

$$\chi \mapsto \mathrm{AI} \circ \left(\frac{\mathcal{N}_{K/\mathbf{Q}}(b|\chi)}{\mathcal{N}_{K/\mathbf{Q}}(a|\chi)}\right). \quad \blacksquare$$

Let $\chi \in R_\Gamma(\overline{\mathbf{Q}})$. Let $\tau(N/K, \chi) \in U^\times$ (again enlarging U as required) be the Galois Gauss sum of χ (for the definitions see **[Fr1]** I §5). Now we can state our first main result of this section.

4.6 Theorem. *The canonical factorisation of $f^*_{\mathfrak{b}\mathcal{O}_K\Gamma, \mathcal{O}_N}$ (which exists by 3.37 and 4.5) is given by*

$$g_b \colon \chi \mapsto \left(\frac{\mathcal{N}_{K/\mathbf{Q}}(b|\chi)}{\tau(N/K, \chi)}\right). \quad \blacksquare$$

The proof of 4.6 will take up most of this section. First we deduce our second main result.

Let $W_\infty(N/K, \chi)$ be the root number at infinity of $\chi \in R_\Gamma(\overline{\mathbf{Q}})$ (see **[Fr1]** I §5). Following Wilson (**[Wi2]** §3) define $T^s \in \mathrm{Hom}(R_\Gamma, U^\times)$ by its restriction to irreducible characters as follows.

$$T^s(\chi) = \begin{cases} \tau(N/K, \chi) W_\infty(N/K, \chi), & \text{if } \chi \text{ is symplectic;} \\ 1, & \text{otherwise.} \end{cases} \tag{4.7}$$

In fact $T^s \in \mathrm{Hom}_{\Omega_\mathbf{Q}}(R_\Gamma, U^\times)$ (**[Wi2]** 3.9(i)). Let $i_p \colon U^\times \to \mathcal{J}(U)$ be inclusion in $U_p^\times$, where p runs over the finite and infinite places of $\mathbf{Q}$. By **[Wi2]**, before 3.11

$$\mathrm{cls}_{\mathbf{Z}\Gamma}(i_\infty T^s) \quad \text{is the Cassou-Noguès-Fröhlich class } t_{N/K}. \tag{4.8}$$

4.9 Theorem. $\Omega(N/K, 2) \equiv t_{N/K} \pmod{D(\mathbf{Z}\Gamma)}$.

Proof : By 4.8 we have to show that

$$\pi_\Gamma \Omega(N/K, 2) = \mathrm{cls}_{\mathcal{M}_\Gamma}(i_\infty T^s). \tag{4.10}$$

We shall do this by comparing character functions in $\mathrm{Hom}_{\Omega_\mathbf{Q}}(R_\Gamma, \mathcal{J}(U))$ which represent invariants in $Cl(\mathcal{M}_\Gamma)$ under the Hom-description isomorphism:

$$Cl(\mathcal{M}_\Gamma) \cong \frac{\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, \mathcal{J}(U))}{\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U^\times)\mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, \mathcal{U}(U))}$$

Throughout this proof let χ run over $\mathrm{Irr}(\Gamma)$. The map

$$(4.11) \qquad \left\{ \begin{array}{c} c\colon \chi \mapsto \dfrac{\mathcal{N}_{K/\mathbf{Q}}(b|\chi)}{\tau(N/K, \chi)} \\ \text{lies in } \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U^\times) \end{array} \right\}$$

by Theorem 20 in [Fr1]. By 3.37 and 4.6

$$(4.12) \qquad \pi_\Gamma \Omega(N/K, 2) = \mathrm{cls}_{\mathcal{M}_\Gamma}\, g_f,$$

where g_f is defined by

$$(4.13) \qquad g_f(\chi)_p = \begin{cases} i_p c(\chi), & \text{if } p < \infty; \\ 1, & \text{otherwise.} \end{cases}$$

Now

$$(4.14) \qquad g_f g_\infty = c$$

where

$$(4.15) \qquad g_\infty(\chi)_p = \begin{cases} i_\infty c(\chi), & \text{if } p = \infty; \\ 1, & \text{otherwise.} \end{cases}$$

Further

$$(4.16) \qquad g_\infty = g^s g^+$$

where

$$(4.17) \qquad g^+(\chi)_p = \begin{cases} 1, & \text{if } \chi \text{ is symplectic or } p < \infty; \\ i_\infty c(\chi), & \text{otherwise.} \end{cases}$$

We define g^s analogously, with "not symplectic" in place of "symplectic".

Clearly

$$(4.18) \qquad g^+ \in \mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, \mathcal{U}(U)).$$

Checking all cases, we have

$$(4.19) \quad (g^s i_\infty T^s)(\chi)_p = \begin{cases} i_\infty\left(\mathcal{N}_{K/\mathbf{Q}}(b|\chi) W_\infty(N/K,\chi)\right), & \text{if } p=\infty \text{ and } \chi \text{ is symplectic;} \\ 1, & \text{otherwise.} \end{cases}$$

Let $\mathcal{P}$ be any infinite prime of U. Let $\chi \in S_\Gamma$. By **[Fr1]** III 4.9 p126

$$\mathrm{sign}_{\mathcal{P}}\left(\mathcal{N}_{K/\mathbf{Q}}(b|\chi)\right) = W_\infty(N/K,\chi).$$

Hence by 4.19

$$(4.20) \qquad g^s i_\infty T^s \in \mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, \mathcal{U}(U)).$$

Successive substitution in 4.11, 4.14, 4.16, 4.18 and 4.20 gives

$$g_f(i_\infty T^s)^{-1} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U^\times)\mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, \mathcal{U}(U))$$

and 4.10 follows by 4.12. ∎

By 4.5 and 2.18(i), 4.6 follows from

4.21 Theorem. *The canonical factorisation of $f^*_{X,\mathcal{O}_N}$ (which exists by 3.37 and 4.5) is given by*

$$g_a\colon \chi \mapsto \mathrm{AI} \circ \left(\frac{\mathcal{N}_{K/\mathbf{Q}}(a|\chi)}{\tau(N/K,\chi)}\right). \quad ∎$$

We shall devote the rest of this section to the proof of 4.21. Let $\chi \in R_\Gamma(\overline{\mathbf{Q}})$ and let $\wp$ be a finite prime of K. For the next result we shall need the local Galois Gauss sum $\tau(N_{\tilde{\wp}}/K_\wp, \mathrm{res}^\Gamma_{\Gamma(\tilde{\wp})}\chi) \in U^\times$ (once again enlarging U as necessary). See **[Fr1]** I §5* for the definitions.

*and III Theorem 18

Define $g_{a,\wp} \in \mathrm{Hom}(R_\Gamma, \mathcal{I}_U)$ by

$$(4.22) \qquad g_{a,\wp}(\chi) = \mathrm{AI} \circ \left(\frac{\mathcal{N}_{K/\mathbf{Q}}(a_\wp|\chi)}{\tau(N_{\breve{\wp}}/K_\wp, \mathrm{res}^{\Gamma}_{\Gamma(\breve{\wp})} \chi)} \right).$$

4.23 Theorem. *Let $\wp|p$ be a finite prime of K. Let g_a be as in 4.21 and $g_{a,\wp}$ be as in 4.22. Then $g_a \in I(G, \overline{\mathbf{Q}})$ and $g_{a,\wp} \in \mathrm{Hom}_{\Omega_\mathbf{Q}}(R_\Gamma, \mathcal{I}_U)$. The values of $g_{a,\wp}$ are ideals lying over p.*

Proof : Let $\omega \in \Omega_\mathbf{Q}$ and let $\chi \in R_\Gamma(\overline{\mathbf{Q}})$. By Theorem 20 in **[Fr1]**

$$(4.24) \qquad \frac{\mathcal{N}_{K/\mathbf{Q}}(a|\chi)^\omega}{\tau(N/K, \chi)^\omega} = \frac{\mathcal{N}_{K/\mathbf{Q}}(a|\chi^\omega)}{\tau(N/K, \chi^\omega)}$$

and

$$(4.25) \qquad \frac{\mathcal{N}_{K/\mathbf{Q}}(a_\wp|\chi)^\omega}{\mathcal{N}_{K/\mathbf{Q}}(a_\wp|\chi^\omega)} \quad \text{and} \quad \frac{\tau(N_{\breve{\wp}}/K_\wp, \mathrm{res}^{\Gamma}_{\Gamma(\breve{\wp})} \chi)^\omega}{\tau(N_{\breve{\wp}}/K_\wp, \mathrm{res}^{\Gamma}_{\Gamma(\breve{\wp})} \chi^\omega)} \quad \text{are roots of unity.}$$

It follows immediately that g_a and $g_{a,\wp}$ lie in $\mathrm{Hom}_{\Omega_\mathbf{Q}}(R_\Gamma, \mathcal{I}_U)$. Now let $\omega \in \Omega_{\mathbf{Q}(\chi)}$. By 4.24 again $g_a \in I(\Gamma, \overline{\mathbf{Q}})$. The final statement follows from the definition of the semilocal norm resolvent, and the fact that the square of the modulus of the local Galois Gauss sum is a power of p (c.f. **[Fr1]** I 5.7). ∎

4.26 Theorem. *Let $\wp|p$ be a finite prime of K. Let $\mathcal{P}$ be a prime of U lying over p. Let $j: U \hookrightarrow U_\mathcal{P}$ be the canonical embedding. Let $\chi \in R_{\Gamma(\breve{\wp})}(\overline{\mathbf{Q}_p})$ and let $\chi_g \in R_{\Gamma(\breve{\wp})}(\overline{\mathbf{Q}})$ be such that $\chi_g^j = \chi$. Define*

$$g_{a,\breve{\wp}}(\chi) = \left(\frac{\mathcal{N}_{K_\wp/\mathbf{Q}_p}(a_\wp|\chi)}{\tau(N_{\breve{\wp}}/K_\wp, \chi_g)^j} \right).$$

Then $g_{a,\breve{\wp}} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}_p}}(R_{\Gamma(\breve{\wp})}(\overline{\mathbf{Q}_p}), \mathcal{I}_{U_\mathcal{P}})$ and

$$\mathrm{ind}^{\Gamma}_{\Gamma(\breve{\wp})}\, g_{a,\breve{\wp}} = (g_{a,\wp})_p\,.$$

If $\wp$ is tame, then $g_{a,\breve{\wp}} = 1 = g_{a,\wp}$.

Remark: By 4.25 and a similar argument to the proof of 2.15, $g_{a,\tilde{\wp}}$ does not depend on the choice of $\mathcal{P}|p$.

See facing page

Proof : ~~Since $g_{a,\wp} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma(\overline{\mathbf{Q}}), \mathcal{I}_U)$ the first statement is a consequence of the second. Alternatively, adapt Theorem 20 of [Fr1] for local characters.~~ The last statement follows from the second and Theorem 23 in [**Fr1**] (recall 3.1(ii)). Let $\theta \in R_\Gamma(\overline{\mathbf{Q}_p})$. Then (in the obvious notation)

$$(g_{a,\wp})_p(\theta) = g_{a,\wp}(\theta_g)_{\mathcal{P}}$$

$$(4.27) \qquad = \left\{ \mathrm{AI} \circ \left(\frac{\mathcal{N}_{K/\mathbf{Q}}(a_\wp|\theta_g)}{\tau(N_{\tilde{\wp}}/K_\wp, \operatorname{res}^\Gamma_{\Gamma(\tilde{\wp})} \theta_g)} \right) \right\}_{\mathcal{P}}$$

$$= \left(\frac{\mathcal{N}_{K_\wp/\mathbf{Q}_p}(a_\wp| \operatorname{res}^\Gamma_{\Gamma(\tilde{\wp})} \theta)}{\tau(N_{\tilde{\wp}}/K_\wp, \operatorname{res}^\Gamma_{\Gamma(\tilde{\wp})} \theta_g)^j} \right).$$

The last equality, in the tame case, is Theorem 19 in [**Fr1**]. As usual, we can replace $\mathcal{O}_N$ by X to obtain a generalisation of Theorem 19 to the "wild" case. Thus 4.27 also holds for $\wp$ wild. But 4.27 is $\operatorname{ind}^\Gamma_{\Gamma(\tilde{\wp})} g_{a,\tilde{\wp}}(\theta)$. ∎

4.28 Theorem. *$g_{a,\tilde{\wp}}$ is the canonical factorisation of $f^{\mathcal{P}}_{X_{\tilde{\wp}},\mathcal{O}_{N,\tilde{\wp}}}$.* ∎

Before proving 4.28, we shall use it to establish 4.21. We need

4.29 Lemma.

$$g_a = \prod_{\wp \text{ wild}} g_{a,\wp}.$$

Proof : Since $(a_\wp|\chi) = (a|\chi)_\wp$, by 4.2

$$(4.30) \qquad \mathrm{AI} \circ \mathcal{N}_{K/\mathbf{Q}}(a|\chi) = \prod_{\wp \text{ ramified}} \mathrm{AI} \circ \mathcal{N}_{K/\mathbf{Q}}(a_\wp|\chi).$$

If $\theta \in R_{\Gamma(\tilde{\wp})}(\overline{\mathbf{Q}})$ then $\tau(N_{\tilde{\wp}}/K_\wp, \theta)$ is ~~1~~ a root of unity for $\wp$ unramified, and

$$(4.31) \qquad \left(\tau(N/K, \chi)\right) = \left(\prod_{\wp \text{ ramified}} \tau(N_{\tilde{\wp}}/K_\wp, \operatorname{res}^\Gamma_{\Gamma(\tilde{\wp})} \chi),\right)$$

by [**Fr1**] Theorem 18. By 4.30, 4.31 and the last part of 4.26 the lemma follows. ∎

Recall from 3.40 that

$$f^{*}_{\Gamma,\mathrm{ind}^{\Gamma}_{\Gamma(\tilde{\wp})} X_{\tilde{\wp}},\mathrm{ind}^{\Gamma}_{\Gamma(\tilde{\wp})} \mathcal{O}_{N,\tilde{\wp}}} = f^{*}_{\Gamma,X_{\wp},\mathcal{O}_{N,\wp}}. \tag{4.32}$$

Then by 2.25, the first part of 4.26, 4.28 and the last part of 4.23

$$g_{a,\wp} \quad \text{is the C. F. of} \quad f^{*}_{\Gamma,X_{\wp},\mathcal{O}_{N,\wp}}. \tag{4.33}$$

Finally, by 4.29 and 3.39, 4.21 holds.

It remains to prove 4.28, which will take up the rest of this section. Change notation for the local case. Let G and L/F be as usual. Write a in place of $a_{\wp}$, X in place of $X_{\tilde{\wp}}$ and g in place of $g_{a,\tilde{\wp}}$. By the first statement of 4.26 it suffices to prove that, for each $(C, e) \in \mathcal{S}^p(G)$

$$\mathrm{res}^{G}_{C}\, g(\mathrm{inf}^{C}_{C_\times}\, \chi) = f^{p}_{X,\mathcal{O}_L}(C, e), \tag{4.34}$$

where χ is as in 2.9. Let Φ be as in the proof of 2.10, and let $\phi \in \Phi$. Let $\theta = \mathrm{inf}^{C}_{C_\times}\, \phi$. We shall re-express 4.34 by the use of induction and inflation formulae for norm resolvents and Galois Gauss sums. Let $M = L^C$ and let d be a free generator of L over MC. By the induction formulae in **[Fr1]** III Notes [4] (generalised to the "wild" case—a is a free generator for L over FG, rather than for $\mathcal{O}_L$ over $\mathcal{O}_F G$ as in the tame case, so the element λ below lies in $FC^\times$ rather than $\mathcal{O}_F C^\times$ as in the tame case)

$$\mathrm{res}^{G}_{C}\, g(\theta) = \left(\frac{\mathcal{N}_{F/\mathbf{Q}_p}(a|\,\mathrm{ind}^{G}_{C}\,\theta)}{\tau(L/F,\, \mathrm{ind}^{G}_{C}\,\theta_g)^j}\right) = \left(\frac{\mathcal{N}_{M/\mathbf{Q}_p}(d|\theta)}{\tau(L/M,\, \theta_g)^j \mathcal{N}_{F/\mathbf{Q}_p}\, \mathrm{Det}_\theta(\lambda)}\right), \tag{4.35}$$

for some $\lambda \in FC^\times$. To be more precise, we must introduce some notation. Let $\{\omega\}$ be a right transversal of Ω_M in Ω_F and let $\{c_j\}$ be a free basis of $\mathcal{O}_M$ over $\mathcal{O}_F$. Let $\{a_i\}$ be any free basis of L over FC. Define

$$\mathrm{Det}_\theta\{a_i\} = \det\left(\sum_c a_i^{c\omega}\theta(c)^{-1}\right)_{\omega,i}, \tag{4.36}$$

where c runs over C. With λ as in 4.35 we have

$$\mathrm{Det}_\theta(\lambda) = \frac{\mathrm{Det}_\theta\{a^{\omega^{-1}}\}_\omega}{\mathrm{Det}_\theta\{c_j d\}_j}, \tag{4.37}$$

with the left hand side having the usual meaning and the right hand side that of 4.36 with $\{a_i\}_i$ taken to be $\{a^{\omega^{-1}}\}_\omega$ and $\{c_j d\}_j$ (4.36 and 4.37 are taken from **[Fr3]** pp166-167).

Let h run over $H \stackrel{def}{=} C_p$. So $\theta = (1_H, \phi)$. Let x run over $C_\times$. From 4.36

$$\text{(4.38)} \qquad \begin{aligned} \mathrm{Det}_\theta\{a_i\} &= \det\left(\sum_{x,h} a_i^{xh\omega}\phi(x)^{-1}\right)_{\omega,i} \\ &= \det\left(\sum_x \left(\mathrm{tr}_{L/L^H} a_i\right)^{x\omega}\phi(x)^{-1}\right)_{\omega,i}. \end{aligned}$$

Let $t = \mathrm{tr}_{L/L^H} d$. By the inflation formula for resolvents (**[Fr3]** Theorem 10 p162), again extended to the wild case, and the inflation invariance of Galois Gauss sums (c.f. **[Fr1]** III ex. 6 p105) we have

$$\text{(4.39)} \qquad \left(\frac{\mathcal{N}_{M/\mathbf{Q}_p}(d|\theta)}{\tau(L/M,\,\theta_g)^j}\right) = \left(\frac{\mathcal{N}_{M/\mathbf{Q}_p}(t|\phi)}{\tau(L^H/M,\,\phi_g)^j}\right).$$

Now L^H/M is tame (since $H = C_p$).

This reduction to the tame case appears in **[Fr4]** (where the case of abelian groups is treated) and our proof proceeds along similar lines. Indeed Fröhlich's work motivated our computation of the canonical factorisation g.

Returning to the proof, we can find a free generator z of $\mathcal{O}_{L^H}$ over $\mathcal{O}_M C_\times$. By **[Fr1]** Theorem 23

$$\text{(4.40)} \qquad \left(\mathcal{N}_{M/\mathbf{Q}_p}(z|\phi)\right) = \left(\tau(L^H/M,\,\phi_g)^j\right).$$

By 4.39 and 4.40, 4.35 is

$$\text{(4.41)} \qquad \left(\frac{\mathcal{N}_{M/\mathbf{Q}_p}(t|\phi)}{\mathcal{N}_{M/\mathbf{Q}_p}(z|\phi)}\cdot\frac{1}{\mathcal{N}_{F/\mathbf{Q}_p}\mathrm{Det}_\theta(\lambda)}\right).$$

Now ϕ induces an isomorphism

$$\text{(4.42)} \qquad \mathbf{Z}_p C_\times e \cong \mathbf{Z}_p[\phi].$$

We shall identify the rings in 4.42 under this isomorphism. Let $|\,:\,|_{\mathbf{Z}_p[\phi]}$ denote the module index. If we can show that 4.41 equals

$$\text{(4.43)} \qquad |\mathcal{O}_{L^H} e : (a\mathcal{O}_F G)^H e|_{\mathbf{Z}_p[\phi]}$$

then 4.34 follows by $\Omega_{\mathbf{Q}_p}$-invariance of g, since the norm into $\mathcal{I}_{\mathbf{Q}_p}$ of 4.43 is $f^p_{X,\mathcal{O}_L}(C,\,e)$.

Note that $\mathcal{O}_{L^H} e = \mathcal{O}_M C_\times ez$. If we now introduce the intermediate lattice $\mathcal{O}_M C_\times et$, the equality between 4.41 and 4.43 follows from

4.44 Theorem. *Let ω and ω_1 run over the same right transversal of Ω_M in Ω_F. Let τ run over a right transversal of Ω_F in $\Omega_{\mathbf{Q}_p}$. For brevity (with the notation preceding this theorem) write*

$$x_j = c_j t \quad \text{and} \quad y_\omega = \mathrm{tr}_{L/L^H}(a^{\omega^{-1}}).$$

Then

$$(i) \qquad \left(\frac{\mathcal{N}_{M/\mathbf{Q}_p}(t|\phi)}{\mathcal{N}_{M/\mathbf{Q}_p}(z|\phi)}\right) = |\mathcal{O}_M C_\times ez : \mathcal{O}_M C_\times et|_{\mathbf{Z}_p[\phi]}$$

$$(ii) \qquad \left(\mathcal{N}_{F/\mathbf{Q}_p} \mathrm{Det}_\theta(\lambda)\right)^{\# H} = \prod_\tau \left(\frac{\det(\sum_x y_{\omega_1}^{x\omega\tau}\, \phi(x)^{-1})_{\omega,\omega_1}}{\det(\sum_x x_j^{x\omega\tau}\, \phi(x)^{-1})_{\omega,j}}\right)$$

$$= |\mathcal{O}_M C_\times et : (a\mathcal{O}_F G)^H e|_{\mathbf{Z}_p[\phi]}.$$

Remark: The method of proof is to replace the modules appearing in the module indices by their isomorphic images under the resolvent mapping, and compute these indices as follows. A non-degenerate bilinear form (induced by the trace form $M \to \mathbf{Q}_p$) is introduced. Because we are in the local, tame case, all the modules are free, and can be computed via discriminants with respect to this form. As with the trace form, each discriminant can be re-written as the determinant of the conjugates of a basis. Computing determinants of specific bases we obtain the required equalities.

Proof : The resolvent map $\zeta: L^H \to \zeta(L^H) \subseteq L^H C_\times$ is an $MC_\times$-isomorphism. Thus we can replace the lattices $\mathcal{O}_M C_\times ez$, etc., appearing in the module indices of (i) and (ii) by their isomorphic images $\mathcal{O}_M C_\times e\zeta(z)$, etc.

t and z are free generators of L^H over $MC_\times$. By 4.1 $\zeta(t)$ and $\zeta(z)$ lie in $(L^H C_\times)^\times$. Multiplication by $\zeta(z)^{-1}e$ (or $\zeta(t)^{-1}e$) is a $\mathbf{Q}_p C_\times e$-linear automorphism of $L^H C_\times e$, so we can replace the indices in (i) and (ii) by

$$(ia) \qquad |\mathcal{O}_M C_\times e : \mathcal{O}_M C_\times e\zeta(t)\zeta(z)^{-1}|_{\mathbf{Z}_p[\phi]}$$

and

$$(iia) \qquad |\mathcal{O}_M C_\times e : \sum_{\omega_1} \mathcal{O}_F C_\times e\zeta(y_{\omega_1})\zeta(t)^{-1}|_{\mathbf{Z}_p[\phi]}$$

since $(a\mathcal{O}_F G)^H = \sum_{\omega_1} \mathcal{O}_F C_\times y_{\omega_1}$. Let $\{\sigma\}$ be a right transversal of Ω_M in $\Omega_{\mathbf{Q}_p}$. Define

$$B_e \colon MC_\times e \times MC_\times e \to \mathbf{Q}_p C_\times e$$

by

$$(\lambda, \mu) \mapsto \sum_\sigma (\lambda\mu)^\sigma$$

where $\Omega_{\mathbf{Q}_p}$ acts coefficient-wise on $MC_\times$. Then B_e is $\mathbf{Q}_p C_\times e$-bilinear. If $\{b_l\}$ is a $\mathbf{Z}_p$-basis of $\mathcal{O}_M$ then $\{b_l e\}$ is a $\mathbf{Z}_p C_\times e$-basis of $\mathcal{O}_M C_\times e$, and

$$\det B_e(b_l e,\, b_{l_1} e)_{l, l_1} = (\det(b_l^\sigma)_{\sigma, l}\, e) \neq 0$$

by a standard trick, since $\{b_l\}$ is a $\mathbf{Q}_p$-basis of M. Thus B_e is non-degenerate. So we can compute (ia) and (iia) via B_e-discriminants. Now $\{b_l e \zeta(t)\zeta(z)^{-1}\}$ is a $\mathbf{Z}_p C_\times e$-basis of $\mathcal{O}_M C_\times e\zeta(t)\zeta(z)^{-1}$. By the same determinant trick, (ia) is

$$(ib) \qquad \left(\frac{\det(b_l^\sigma e(\zeta(t)\zeta(z)^{-1})^\sigma)_{\sigma, l}}{\det(b_l^\sigma e)_{\sigma, l}}\right) = \prod_\sigma ((\zeta(t)\zeta(z)^{-1})^\sigma e).$$

Extend ϕ to $L^H C_\times$ by trivial action on the coefficients. If we apply ϕ to (ib) then we obtain (i).

Now

$$\mathcal{N}_{F/\mathbf{Q}_p} \operatorname{Det}_{(1_H, \phi)}(\lambda)^{-1} = \prod_\tau (\operatorname{Det}_{\tau^{-1}(1_H, \phi)}(\lambda))^{\tau\, -1}$$

$$\overset{4.37, 4.38}{=} \prod_\tau \left(\frac{\det(\sum_x x_j^{x\omega}(\tau^{-1}\phi)(x)^{-1})_{\omega, j}}{\det(\sum_x y_{\omega_1}^{x\omega}(\tau^{-1}\phi)(x)^{-1})_{\omega, \omega_1}}\right)^\tau$$

and the first equality in (ii) holds. Take $\{\sigma\}$ to be $\{\tau\omega\}$ and $\{b_l\}$ to be $\{c_j d_k\}$ where $\{d_k\}$ is some $\mathbf{Z}_p$-basis of $\mathcal{O}_F$. Thus $\{d_k \zeta(y_{\omega_1})\zeta(t)^{-1} e\}$ is a $\mathbf{Z}_p C_\times e$-basis of the lattice $\sum_{\omega_1} \mathcal{O}_F C_\times e \zeta(y_{\omega_1})\zeta(t)^{-1}$ (because $\{d_k y_{\omega_1}\}$ is a $\mathbf{Z}_p$-basis of $\oplus_{\omega_1} \mathcal{O}_F C_\times y_{\omega_1}$). Then (iia) is

(iib)

$$\left(\frac{\det((c_j d_k)^{\omega\tau}\, e)_{(\tau, \omega), (j, k)}}{\det(d_k^{\omega\tau}(\zeta(y_{\omega_1})\zeta(t)^{-1})^{\omega\tau}\, e)_{(\tau, \omega), (\omega_1, k)}}\right) = \left(\frac{\det(d_k^\tau)_{\tau, k} \prod_\tau \det(c_j^{\omega\tau}\, e)_{\omega, j}}{\det(d_k^\tau)_{\tau, k} \prod_\tau \det((\zeta(y_{\omega_1})\zeta(t)^{-1})^{\omega\tau}\, e)_{\omega, \omega_1}}\right)$$

$$= \prod_\tau \left(\frac{\det(\zeta(x_j)^{\omega\tau}\, e)_{\omega, j}}{\det(\zeta(y_{\omega_1})^{\omega\tau}\, e)_{\omega, \omega_1}}\right)$$

If we apply ϕ once more we get (ii). ∎

References.

[Ba] H. Bass, Algebraic K-Theory, W. A. Benjamin, Inc., 1968

[Br] K. S. Brown, Cohomology of groups, Graduate Texts in Maths., Springer-verlag, 1982

[BS] Z. Borevich and I. Shafarevich, Number Theory, Academic Press, New York, 1966

[Bu] D. J. Burns, Canonical Factorisability and a variant of Martinet's conjecture, to appear

[CF] Algebraic Number Theory, Ed. J. W. S. Cassels and A. Fröhlich, Academic Press, (1967)

[Ch1] T. Chinburg, On the Galois structure of algebraic integers and S-units, Inv. Math. **74** (1983), 321-349

[Ch2] ———, Exact sequences and Galois module structure, Annals of Math. **121** (1985), 351-376

[CR] C. W. Curtis and I. Reiner, Methods of Representation Theory with applications to finite groups and orders (in 2 volumes), Wiley (New York), 1983

[EM] S. Endo and T. Miyata, On the Class Groups of Dihedral groups, J. of Algebra **63** (1980), 548-573

[Fr1] A. Fröhlich, Galois module structure of algebraic integers, Springer-Verlag, Berlin, 1983

[Fr2] ———, Module Defect and Factorisability, Ill. J. of Math., 32 (1988), 407-421

[Fr3] ———, "Galois module structure" in "Algebraic Number Theory", Proc. Durham Symp. 1975 (ed. A. Fröhlich), Academic Press, London, 1977, 133-191

[Fr4] ———, L-values at zero and multiplicative Galois modules structure (also Galois Gauss sums and additive Galois module structure), J. Reine angew. Math. **397** (1989), 42-99

[Ma] S. MacLane, Homology, Springer–Verlag, 1963

[Ne] A. Nelson, London, PhD thesis 1979

[Ol] R. Oliver, Subgroups generating $D(\mathbf{Z}G)$, J. of Algebra **55** (1978), 43-57

[RU] I. Reiner and S. Ullom, A Mayer-Vietoris sequence for Class Groups, J. of Algebra **31** (1974), 305-347

[Ro] J. J. Rotman, An Introduction to Homological Algebra, Academic Press, 1979

[Ta] M. Taylor, Classgroups of Group Rings, LMS lecture note series: **91** (1984), CUP

[Wi1] S. M. J. Wilson, Galois module structure of rings of integers in wildly ramified extensions, Ann. Inst. Fourier, Grenoble **39**, 3 (1989), 529-551

[Wi2] ———, A projective invariant comparing wild Galois module structure, to appear in Crelle

[Wi3] ———, Twisted group rings and ramification, Proc. London Math. Soc. (**3**) 31 (1975), 311-330