ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 1988

MODULE DEFECT AND FACTORISABILITY

BY

A. FRÖHLICH

To the memory of Irv Reiner, friend and colleague

Introduction

This paper deals with two concepts relating to modules over Abelian group rings. One is *factorisability*, introduced in Nelson's thesis (cf. [9], see also [5]), the other is the *module defect*, first investigated in [3] in the more general setting of orders in commutative algebras. Both now come into prominence in work on Galois module structure, multiplicative as well as additive. The background on the multiplicative side is the connection between the Galois module structure of units or S-units on the one hand, and the quotients of "L-values at zero" and generalised regulators on the other. Analogously we relate the additive Galois module of algebraic integers with the quotients of Galois Gauss sums and generalised resolvents. All this lies outside the "tame" theory, as presented in [6].

Factorisability leads to an equivalence relation between lattices over integral group rings, weaker than local isomorphism, and turning up naturally and significantly when one sets out to compare multiplicative modules of units or additive modules of algebraic integers with certain "standard" modules. The module defect is then the natural channel for information on the structure of our Galois modules. But beyond that the properties of module defects are actually reflected in integral properties of certain L-value-regulator quotients (or Gauss sum-resolvent quotients). We are then led to integral formulations of problems and of theorems in the direction of the Stark conjectures (cf. [10], [11]). For all this see [7], [8].

These number theoretic applications provide the motivation for the separate treatment of some purely algebraic aspects, to be given in the present paper. It is striking how our algebraic ideas and methods, which will be seen to be absolutely elementary, although quite novel, lead to highly significant results when applied to Galois module structure. We shall attempt to give some indication of this at various places.

Received September 8, 1987.

Notations. As usual $\mathbf{Z}$ is the ring of integers, $\mathbf{Q}$ the field of rational numbers, $\mathbf{Q}_p$ that of p-adic rationals. For any finite extension F of $\mathbf{Q}$ or $\mathbf{Q}_p$, the ring of integers in F will be denoted by o_F. "Ideals" in F are non zero fractional ideals of o_F. The module index over o_F is denoted by $[\ :\ ]_{o_F}$ (cf. [1]). The algebraic closure of a field k is k^c. The multiplicative group of a field F is F^*, the group ring of a group Γ over over a commutative ring R is $R\Gamma$.

This paper was written while the author was partly supported by a Leverhulm Emeritus Fellowship.

1. Formal aspects

Throughout Γ is a finite Abelian group, $\Gamma^\dagger$ its character group. More precisely we work over a basefield $k = \mathbf{Q}$ (global case) or $k = \mathbf{Q}_p$ (local case) and accordingly we take $\Gamma^\dagger = \mathrm{Hom}(\Gamma, k^{c*})$. A *division* D of $\Gamma^\dagger$ is an equivalence class in $\Gamma^\dagger$, with θ, θ' belonging to the same division if $\langle\theta'\rangle = \langle\theta\rangle$ (cyclic group generated by θ). $\mathscr{S}(\Gamma^\dagger)$ is the set of subgroups of $\Gamma^\dagger$, A is an Abelian group which we write multiplicatively. We then consider the group $\mathrm{Map}(\mathscr{S}(\Gamma^\dagger), A)$ of maps $f\colon \mathscr{S}(\Gamma^\dagger) \to A$. We extend each f to a function on the set of divisions by the Möbius rule

$$f(D) = \prod_{C<\overline{D}} f(C)^{\mu(\overline{D}:C)}. \tag{1.1}$$

The product runs over the subgroups C of the cyclic group $\overline{D}$ generated by any element θ of D and μ is the Möbius function. The use of the same symbol f for the original function on subgroups of $\Gamma^\dagger$ and for the extended function on divisions D should not create confusion: The only division which is also a subgroup is that consisting of the identity of $\Gamma^\dagger$ and in this case the two definitions coincide. Note that in general $f(\overline{D}) \neq f(D)$, the symbol D here and in the sequel always denoting divisions. Of course (1.1) for all D is equivalent to

$$f(G) = \prod_{D<G} f(D) \tag{1.2}$$

for all cyclic subgroups G of $\Gamma^\dagger$. If (1.2) holds for all subgroups G of $\Gamma^\dagger$ then we call f *factorisable*. To restate this we introduce for any f its factorisable form f', given by

$$f'(G) = \prod_{D<G} f(D), \tag{1.3}$$

for all subgroups G of $\Gamma^\dagger$. f' is factorisable. Now define $\tilde{f}$ by

$$\tilde{f}(G) = f'(G)f(G)^{-1} \quad \text{for all } G. \tag{1.4}$$

Then f is factorisable precisely when $\tilde{f}(G) = 1$ for all G.

We actually make no use of the group structure of $\Gamma^\dagger$, except to define $\mathscr{S}(\Gamma^\dagger)$. Given G, the representation of Γ over k^c which is the sum $\Sigma_{\theta \in G}\, \theta$ is induced from the trivial representation of a unique subgroup Δ of Γ—and of course

$$G = G_\Delta = \text{annihilator of } \Delta \text{ in } \Gamma^\dagger. \tag{1.5}$$

The symbol G_Δ will always be used in this sense. Viewing f as a function on the set of such induced representations, it will be factorisable precisely when it extends to a homomorphism on the (additive group of the) rational representation ring of Γ (case $k = \mathbf{Q}$). Or again the original function f defines a homomorphism from the additive group of the Burnside ring of Γ, and it is factorisable precisely when it factorises through the rational representation ring.

In the sequel let F be an extension of finite degree of k, inside k^c. Write $F(\theta)$ for the field of values of the character θ over F. Then

$$F(\theta) = F(D) \tag{1.6}$$

only depends on the division D of θ. Let $\mathscr{I}_F$ denote the ideal group of F and $N_{F(D)/F}$ the norm map $\mathscr{I}_{F(D)} \to \mathscr{I}_F$.

A map $f \in \mathrm{Map}(\mathscr{S}(\Gamma^\dagger), \mathscr{I}_F)$ is said to have the *norm property at* D if

$$f(D) \in N_{F(D)/F}\big(\mathscr{I}_{F(D)}\big). \tag{1.7}$$

Next, for given F and D, let $I_{F,D}$ be the group of maps

$$g\colon D \to \mathscr{I}_{F(D)} \tag{1.8a}$$

with

$$g(\theta^\omega) = g(\theta)^\omega \quad \text{for all } \omega \in \mathrm{Gal}\big(F(D)/F\big). \tag{1.8b}$$

We now call a map $f \in \mathrm{Map}(\mathscr{S}(\Gamma^\dagger), \mathscr{I}_F)$ *F-factorisable* if, for all subgroups G of $\Gamma^\dagger$, we have

$$f(G) = \prod_{\theta \in G} g(\theta), \tag{1.9}$$

where g is a map of $\Gamma^\dagger$ whose restriction to D lies in $I_{F,D}$, for each D. The

right hand side of (1.9) bracketed by divisions indeed makes sense in the group $\mathscr{I}_F$. Moreover f is F-factorisable if and only if it is factorisable and, for each D, $f(D)$ has the norm property. It is clear that F-factorisability also has an interpretation in terms of representations of Γ.

It is clear that we could have considered more generally any suitable functor of fields F, but $\mathscr{I}_F$ is the one which we shall need here. The motivation comes from the structure problem for Galois modules such as rings of algebraic integers or groups of units, which are not given explicitly—even approximately—by generators and relations. The aim is then to gain information by criteria of comparison with known "standard" modules. We consider injective homomorphisms

$$i\colon L \to M \tag{1.10}$$

say of $o_F\Gamma$-lattices with finite cokernel—in the applications one of these will be an "arithmetic lattice" the other a known standard lattice. To each such map i we associate the function f_i with values

$$f_i(G_\Delta) = O\left(\operatorname{coker} i^\Delta\right) = \left[M^\Delta : L^\Delta\right]_{o_F} \tag{1.10a}$$

(notation as in (1.5)). Here O is the o_F-order ideal, $[\ ]_{o_F}$ the o_F-index, where we have assumed, as we may, that $M \otimes_{o_F} F = L \otimes_{o_F} F$ with M, L embedded in this $F\Gamma$-module. Clearly

$$\begin{aligned} f_{i\circ j} &= f_i f_j \quad (\circ = \text{composition}) \\ f_{i\oplus j} &= f_i f_j \quad (\oplus = \text{direct sum}). \end{aligned} \tag{1.11}$$

What is important is that $\tilde{f}_i$ (defined in (1.4)) only depends on the pair M, L to within isomorphism, so that we may write

$$\tilde{f}_i = \tilde{f}_{L,M}. \tag{1.12}$$

Indeed, if i' is a further such injective homomorphism $L \to M$ then $f_i f_{i'}^{-1}$ is actually F-factorisable, as we shall show below. (Note that $f \mapsto \tilde{f}$ is a group homomorphism). We thus obtain equivalence relations

$$\begin{aligned} &L \wedge M && \text{if } f_i \text{ is factorisable}, \\ &L \wedge_F M && \text{if } f_i \text{ is } F\text{-factorisable}. \end{aligned} \tag{1.13}$$

Next, let

$$\mathscr{M} = \mathscr{M}_{F,\Gamma}$$

be the maximal o_F-order of $F\Gamma$ and for any $o_F\Gamma$-lattice L write $L^{\mathscr{M}}$ for its

maximal $\mathscr{M}$-sublattice. If

$$L \otimes_{o_F} F \simeq M \otimes_{o_F} F \quad \text{as } F\Gamma\text{-modules} \tag{1.14}$$

we define the *module defect* by

$$\jmath^{\times}(o_F\Gamma, L, M) = \jmath^{\times}(L, M) = \left[L : L^{\mathscr{M}}\right]_{o_F} \Big/ \left[M : M^{\mathscr{M}}\right]_{o_F}. \tag{1.15}$$

(See [3]—there we would have spoken of a codefect however; also see [7].) We fabricate out of this a map $\mathscr{S}(\Gamma^{\dagger}) \to \mathscr{J}_F$ by setting

$$\jmath^{\times}_{L,M}(G_{\Delta}) = \jmath^{\times}\left(o_F(\Gamma/\Delta), L^{\Delta}, M^{\Delta}\right). \tag{1.16}$$

The earlier assertion on $f_i \cdot f_{i'}^{-1}$ is then a consequence of:

(1.17) *For i: $L \to M$ the map $\jmath^{\times}_{L,M} \cdot f_i$ is F-factorisable.*

This follows from the equation

$$\left[M : L\right]_{o_F} = \jmath^{\times}(L, M)^{-1}\left[M^{\mathscr{M}} : L^{\mathscr{M}}\right]_{o_F}.$$

For $\theta \in \Gamma^{\dagger}$ let

$$e_{\theta} = (\operatorname{ord}\Gamma)^{-1} \sum_{\gamma} \theta(\gamma)^{-1}\gamma \tag{1.18}$$

be the associated idempotent, and write, for any division D,

$$e_D = \sum_{\theta \in D} e_{\theta}.$$

This is an idempotent in $F\Gamma$. From the equation

$$\left[M^{\mathscr{M}} : L^{\mathscr{M}}\right]_{o_F} = \prod_{D \subset \Gamma^{\dagger}} \left[M^{\mathscr{M}} e_D : L^{\mathscr{M}} e_D\right]_{o_F}$$

and corresponding equations with M, L replaced by M^{Δ}, L^{Δ} and $\Gamma^{\dagger}$ by G_{Δ} ($\Delta < \Gamma$) we easily conclude that $\jmath^{\times}_{L,M} \cdot f_i$ is factorisable, and indeed

$$\left(\jmath^{\times}_{L,M} \cdot f_i\right)(D) = \left[M^{\mathscr{M}} e_D : L^{\mathscr{M}} e_D\right]_{o_F}. \tag{1.19}$$

We complete the proof by showing that $\jmath^{\times}_{L,M} \cdot f_i$ has the norm property at

each D, i.e., that for $\theta \in D$ we always have

$$\begin{aligned} \left[M^{\mathcal{M}} e_D : L^{\mathcal{M}} e_D\right]_{o_F} &= \prod_{\theta \in D} g(\theta), \\ g(\theta) &= \left[\left(M^{\mathcal{M}} o_{F(\theta)}\right) e_\theta : \left(L^{\mathcal{M}} o_{F(\theta)}\right) e_\theta\right]_{o_{F(\theta)}}. \end{aligned} \tag{1.20}$$

It is clear that g has the Galois property (1.8b). Moreover, denoting the maximal order of $(F(D)\Gamma)e_D$ by $\mathcal{N}$, we have

$$\prod_{\theta \in D} g(\theta) = \left[\left(M^{\mathcal{M}} o_{F(\theta)} e_D\right)\mathcal{N} : \left(L^{\mathcal{M}} o_{F(\theta)} e_D\right)\mathcal{N}\right]_{o_{F(\theta)}}. \tag{1.21}$$

Next observe that $M^{\mathcal{M}} e_D$ and $L^{\mathcal{M}} e_D$ are lattices over the maximal order $\mathcal{M} e_D$ of $(F\Gamma)e_D$ spanning the same $(F\Gamma)e_D$-module, hence are locally isomorphic as $\mathcal{M} e_D$-modules at all primes of o. Therefore $M^{\mathcal{M}} o_{F(\theta)} e_D$ and $L^{\mathcal{M}} o_{F(\theta)} e_D$ are $\mathcal{M} o_{F(\theta)} e_D$-modules isomorphic locally everywhere. If follows that

$$\left[\left(M^{\mathcal{M}} o_{F(\theta)} e_D\right)\mathcal{N} : \left(M^{\mathcal{M}} o_{F(\theta)} e_D\right)\right]_{o_{F(\theta)}} = \left[\left(L^{\mathcal{M}} o_{F(\theta)} e_D\right)\mathcal{N} : \left(L^{\mathcal{M}} o_{F(\theta)} e_D\right)\right]_{o_{F(\theta)}}.$$

This however implies that

$$\begin{aligned} \left[\left(M^{\mathcal{M}} o_{F(\theta)} e_D\right)\mathcal{N} : \left(L^{\mathcal{M}} o_{F(\theta)} e_D\right)\mathcal{N}\right]_{o_{F(\theta)}} &= \left[\left(M^{\mathcal{M}} o_{F(\theta)} e_D\right) : \left(L^{\mathcal{M}} o_{F(\theta)} e_D\right)\right]_{o_{F(\theta)}} \\ &= \left[M^{\mathcal{M}} e_D : L^{\mathcal{M}} e_D\right]_{o_F} \cdot o_{F(\theta)}. \end{aligned}$$

This in conjunction with (1.21) now establishes (1.20).

For a list of properties of $j^{\times}$ see [3], [7, (4.5), (4.6)] or [2, 35.9]. We only mention one:

(1.22) *If $L \sim M$, i.e., L and M belong to the same genus of $o_F\Gamma$-lattices, then $j^{\times}_{L,M} = 1$, hence by* (1.17) $L \wedge_F M$.

This is immediately obvious as the global $j^{\times}$ will localise.

We can now indicate how these ideas occur in the arithmetic setting. Let N/K be a Galois extension of number fields, with

$$\mathrm{Gal}(N/K) = \Gamma, \quad [K : \mathbf{Q}] = n. \tag{1.23}$$

Thus

$$(\mathbf{Z}\Gamma)^n \otimes_{\mathbf{Z}} \mathbf{Q} = (\mathbf{Q}\Gamma)^n \simeq N = o_N \otimes_{\mathbf{Z}} \mathbf{Q}.$$

But $(\mathbf{Z}\Gamma)^n \sim o_N$ if, and only if, N/K is tame. However we still have

$$\mathbf{Z}\Gamma^n \wedge_{\mathbf{Q}} o_N \tag{1.24}$$

even in the wild case (cf. [9] or [7]). An analogous result, although more complicated, holds also for Galois modules of units (cf. [7]). Further details will follow in §2.

2. Computations

We shall actually compute $\tilde{f}_{L,M}$ in two cases where it will be seen to be highly divisible by primes p at which Γ is non-cyclic. We shall thus incidentally show that our new concept admits effective computations and also that factorisability equivalence is far from trivial. Both our theorems of this section lead to non-trivial results on Galois module structure, the first multiplicative, the second additive.

Let J_Γ be the augmentation ideal of $\mathbf{Z}\Gamma$, and $\mathscr{A}_\Gamma = \mathbf{Z}\Gamma/(\Sigma\gamma)$ the residue class ring of $\mathbf{Z}\Gamma$ mod the sum of the group elements. Then

$$J_\Gamma \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \mathscr{A}_\Gamma \otimes_{\mathbf{Z}} \mathbf{Q} \cong \mathscr{U}_N \otimes_{\mathbf{Z}} \mathbf{Q}$$

as $\mathbf{Q}\Gamma$-modules where $\mathscr{U}_N$ is the group of units mod ± 1 in a real number field N with $\mathrm{Gal}(N/\mathbf{Q}) = \Gamma$.

Following our general philosophy we should want to compare $\mathscr{U}_N$ with either $\mathscr{A}_\Gamma$ or with J_Γ and indeed $\mathscr{J}^\times(J_\Gamma, \mathscr{U}_N)$ turns up as part of a product of L-value-regulator quotients. It is thus important to note that

$$\tilde{f}_{J_\Gamma, \mathscr{A}_\Gamma} \neq 1, \tag{2.1}$$

i.e., $J_\Gamma \not\sim \mathscr{A}_\Gamma$, if Γ is non-cyclic.

The commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z} & \longrightarrow & \mathbf{Z}\Gamma & \longrightarrow & \mathscr{A}_\Gamma & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbf{Z} & \longrightarrow & \mathbf{Z} & \longrightarrow & \mathbf{Z}/\mathrm{ord}(\Gamma)\mathbf{Z} & \longrightarrow & 0 \end{array}$$

with $\mathbf{Z} \to \mathbf{Z}\Gamma$ given by $1 \mapsto \Sigma\gamma$ and $\mathbf{Z}\Gamma \to \mathbf{Z}$ the augmentation, gives rise to an exact sequence

$$0 \to J_\Gamma \xrightarrow{i} \mathscr{A}_\Gamma \to \mathbf{Z}/\mathrm{ord}(\Gamma)\mathbf{Z} \to 0. \tag{2.2}$$

We then have to show that

(2.1.a) *f_i is not factorisable.*

This is a corollary of the more precise Theorem 1 below, which gives exact numerical information on f_i', so on $\tilde{f}_i$.

We shall need some more notations. For $\theta \in \Gamma^\dagger$, $\theta \neq \varepsilon$ the identity character, we define

$$\mathfrak{o}(\theta) = \text{ideal in } \mathbf{Q}(\theta) \text{ generated by the } \theta(\gamma) - 1, \text{ all } \gamma \in \Gamma.$$

In addition we put

$$\mathfrak{o}(\varepsilon) = 1.$$

These ideals occur also in an integrality theorem on certain L-value-regulator quotients for unit groups $\mathscr{U}_N$ as above.

Next if G is an Abelian p-group of exponent p^t with invariants $(p^t, p^{t_2}, \ldots, p^{t_r})$ we write $G^{(0)}$ for that Abelian p-group with invariants $(p^{t-1}, p^{t_2}, \ldots, p^{t_r})$ (not necessarily in order of magnitude). Now identifying positive rationals with rational fractional ideals, and denoting their p-parts by subscripts, we have:

THEOREM 1. (i) $f_i(G) = \operatorname{ord}(G)$ *for any subgroup* G *of* $\Gamma^\dagger$.

(ii) *For any division* D *of* $\Gamma^\dagger$

$$f_i(D) = \prod_{\theta \in D} \mathfrak{o}(\theta) = \begin{cases} p & \text{if } \overline{D} \text{ is of order } p^r > 1,\ p \text{ a prime}, \\ 1 & \text{otherwise}. \end{cases}$$

For any subgroup G *of* $\Gamma^\dagger$,

$$f_i'(G) = \prod_p f_i'(G_p)$$

$f_i'(G)_p = f_i'(G_p)$ *for each prime* p, *where* G_p *is the* p*-Sylow group of* G,

$$f_i'(G) = \prod_{\theta \in G} \mathfrak{o}(\theta).$$

(iii) *If* G *is a* p*-group of order* p^n *and exponent* p^t *then*

$$f_i'(G)/f_i'(G^{(0)}) = p^{p^{n-t}}$$

and so

$$\tilde{f}_i(G)/\tilde{f}_i(G^{(0)}) = p^{p^{n-t}-1}.$$

In particular if G *is of exponent* p *then*

$$\tilde{f}_i(G) = p^{(p^n-1)/(p-1)-n}.$$

We thus see that $\tilde{f}_i = \tilde{f}_{\mathscr{T}_\Gamma, \mathscr{A}_\Gamma}$ is actually integral and highly divisible at the relevant primes.

Proof. Let $\Delta < \Gamma$. The cohomology sequence of the exact sequence (2.2) of Δ-modules gives (writing $g = \mathrm{ord}(\Gamma)$, $d = \mathrm{ord}(\Delta)$ for the moment)

$$0 \to J_\Gamma^\Delta \to \mathscr{A}_\Gamma^\Delta \to \mathbf{Z}/g\mathbf{Z} \to \hat{\mathbf{H}}^1(\Delta, J_\Gamma) \to \hat{\mathbf{H}}^1(\Delta, \mathscr{A}_\Gamma) \to \hat{\mathbf{H}}^1(\Delta, \mathbf{Z}/g\mathbf{Z}) \to 0.$$

As $d|g$, $\hat{\mathbf{H}}^1(\Delta, \mathbf{Z}/g\mathbf{Z})$ is of order d and so is $\hat{\mathbf{H}}^1(\Delta, \mathscr{A}_\Gamma) = \hat{\mathbf{H}}^2(\Delta, \mathbf{Z})$. As

$$\hat{H}^1(\Delta, J_\Gamma) = \hat{H}^0(\Delta, \mathbf{Z}) = \mathbf{Z}/d\mathbf{Z},$$

the above sequence reduces to

$$0 \to J_\Gamma^\Delta \to \mathscr{A}_\Gamma^\Delta \to \mathbf{Z}/g\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z} \to 0.$$

Therefore indeed $f_i(G_\Delta) = g/d = \mathrm{ord}(G_\Delta)$, i.e., we have established (i).

By (1.2) for cyclic G we verify that indeed $f_i(D) = p$ or $= 1$ as indicated. Also if the order of θ is not a prime power then $\mathfrak{o}(\theta) = (1)$, while if it is $p^r > 1$, p a prime then $\mathfrak{o}(\theta)^{\phi(p^r)} = p$, ϕ the Euler function. This yields the equation for $f_i(D)$. This implies that we always have

$$f_i'(G) = \prod_{\theta \in G} \mathfrak{o}(\theta)$$

and the rest of the theorem follows by elementary calculations. For instance

$$f_i'(G)/f_i'(G^{(0)}) = \prod_{\substack{\theta \in G \\ \theta \notin G^{(0)}}} \mathfrak{o}(\theta).$$

Out second theorem will be stated in global terms. If E/F is an extension of number fields then we have a natural embedding

$$\mathrm{Map}\big(\mathscr{S}(\Gamma^\dagger), \mathscr{I}_F\big) \subset \mathrm{Map}\big(\mathscr{S}(\Gamma^\dagger), \mathscr{I}_E\big).$$

We shall use this to compare maps f defined in the first place with respect to different fields. For orders $\mathscr{A}$, $\mathscr{B}$ in $F\Gamma$, the map $f_{\mathscr{B}, \mathscr{A}}$ is always understood to be defined in terms of σ_F-indices. We shall write

$$h(G) = \mathrm{ord}(G)^{\mathrm{ord}(G)}, \qquad h \in \mathrm{Map}\big(\mathscr{S}(\Gamma^\dagger), \mathscr{I}_\mathbf{Q}\big).$$

THEOREM 2. (i) *For any number field F,*

$$\tilde{f}^2_{\sigma_F\Gamma, \mathscr{M}_{F,\Gamma}} = \tilde{h}^{-1},$$

and more generally

$$\tilde{f}^2_{o_F\Gamma,\mathscr{A}} = \tilde{h}^{-1}$$

if $\mathscr{A}$ *is an order in* $F\Gamma$ *which contains* $\mathscr{M}_{\mathbf{Q},\Gamma} \otimes_{\mathbf{Z}} o_F$.

(ii) *Let* G_p *be the p-Sylow group of* $G < \Gamma^\dagger$, *and* $G = G_p \times G'$. *Then*

$$k(G)_p = k(G_p)^{\mathrm{ord}(G')}$$

for $k = h, h', \tilde{h}$.

(iii) *Let G be a p-group, p a prime, of order* p^n *and of exponent* p^t, *with* $G^{(0)}$ *as defined prior to Theorem* 1. *Then*

$$h'(G)/h'(G^{(0)}) = g^{t(p^n-p^{n-1})+p^{n-1}}$$

and so

$$\tilde{h}(G)^{-1}/\tilde{h}(G^{(0)})^{-1} = p^{(n-t)(p^n-p^{n-1})}.$$

In particular if G is of exponent p then

$$\tilde{h}(G)^{-1} = p^{np^n-(p+\cdots+p^n)}.$$

Thus we see again the phenomenon of an integral and highly divisible map $\tilde{f}_i$.

An immediate corollary is that for non cyclic Γ,

$$o_F\Gamma \not\simeq \mathscr{M}_{F,\Gamma}, \tag{2.3}$$

a result proved in [9]. Nelson's proof is much simpler, but does not give the detailed numerical properties of $\tilde{f}$.

We shall give an application to the situation described in (1.23), and assuming (1.24). Let F be a subfield of K, say $[K:F] = m$. Let $\mathscr{A}$ be an order in $F\Gamma$ containing $\mathscr{M}_{\mathbf{Q},\Gamma} \otimes_{\mathbf{Z}} o_F$. Then, viewing N as an $F\Gamma$-module, we have:

(2.4) *If* Γ *is non cyclic then* o_N *will not admit multiplication by* $\mathscr{A}$, *and in particular* $o_N \not\sim \mathscr{A}^m$.

For $\mathscr{A} = \mathscr{M}_{K,\Gamma}$ this is a theorem of Nelson (cf. [9]). In the particular case of Kummer extensions N/K this is already in [4].

Proof of (2.4). If o_N admits $\mathscr{A}$ then it admits $\mathscr{M}_{\mathbf{Q},\Gamma}$. Therefore $o_N \sim \mathscr{M}^n_{\mathbf{Q},\Gamma}$, so by (1.24) $\mathbf{Z}\Gamma^n \wedge \mathscr{M}^n_{\mathbf{Q},\Gamma}$, i.e., $\mathbf{Z}\Gamma \wedge \mathscr{M}_{\mathbf{Q},\Gamma}$ contradicting (2.3). Note that $L \wedge M$ if and only if $L^n \wedge M^n$.

Proof of Theorem 2. (i) Let E be a number field containing the given field F, and the values of all the characters θ of Γ. We shall prove that

$$\tilde{f}^2_{o_E\Gamma,\mathscr{M}_{E,\Gamma}} = \tilde{h}^{-1}. \tag{2.5}$$

If now $\mathscr{A}$ is an order in $F\Gamma$ containing $\mathscr{M}_{\mathbf{Q},\Gamma} \otimes_{\mathbf{Z}} o_F$ then $\bar{\mathscr{A}} = \mathscr{A} \otimes_{o_F} o_E$ is an order in $E\Gamma$ containing the primitive idempotents

$$e_D = \sum_{\theta \in D} e_\theta \quad \text{(see (1.18))} \tag{2.6}$$

of $\mathscr{M}_{\mathbf{Q},\Gamma}$. Thus

$$\left[\mathscr{M}^{\Delta}_{E,\Gamma} : \bar{\mathscr{A}}^{\Delta}\right]_{o_E} = \prod_{D < G_\Delta} \left[\mathscr{M}_{E,\Gamma} e_D : \bar{\mathscr{A}} e_D\right]_{o_E}$$

which shows that $\tilde{f}_{\bar{\mathscr{A}},\mathscr{M}_{E,\Gamma}} = 1$. In other words

$$\tilde{f}_{o_E\Gamma,\bar{\mathscr{A}}} = \tilde{f}_{o_E\Gamma,\mathscr{M}_{E,\Gamma}}$$

and of course

$$\tilde{f}_{o_F\Gamma,\mathscr{A}} = \tilde{f}_{o_E\Gamma,\bar{\mathscr{A}}}.$$

Thus (2.5) is indeed what we need to prove (i) of the theorem.

(ii) Define a scalar product in $E\Gamma$ with Γ as orthonormal basis. Denote by $\hat{M}$ the o_E-dual of a lattice M spanning $E\Gamma$, with respect to this product. Then

$$\left[\mathscr{M}_{E,\Gamma} : o_E\Gamma\right]_{o_E} = \left[\widehat{o_E\Gamma} : \widehat{\mathscr{M}_{E,\Gamma}}\right]_{o_E}.$$

But

$$\widehat{o_E\Gamma} = o_E\Gamma, \widehat{\mathscr{M}_{E,\Gamma}} = g\mathscr{M}_{E,\Gamma}$$

where for the moment we write $\mathrm{ord}(\Gamma) = g$. Therefore

$$\left[\mathscr{M}_{E,\Gamma} : o_E\Gamma\right]^2_{o_E} = g^g \tag{2.7}$$

Let $\Delta < \Gamma$. Put

$$e_\Delta = \mathrm{ord}(\Delta)^{-1} \sum_{\delta \in \Delta} \delta = \sum_{\theta \in G_\Delta} e_\theta.$$

Then

$$(\mathscr{M}_{E,\Gamma})^\Delta = (\mathscr{M}_{E,\Gamma}) e_\Delta, \quad (o_E\Gamma)^\Delta = \mathrm{ord}(\Delta)(o_E\Gamma) e_\Delta.$$

Therefore, writing $t = [\Gamma : \Delta] = \mathrm{ord}(G_\Delta)$,

$$\left[\mathscr{M}_{E,\Gamma}^\Delta : o_E\Gamma^\Delta\right]_{o_E} = \left[\mathscr{M}_{E,\Gamma} e_\Delta : o_E\Gamma e_\Delta\right]_{o_E} \cdot \left(\frac{g}{t}\right)^t. \tag{2.8}$$

The isomorphism

$$E\Gamma e_\Delta \simeq E(\Gamma/\Delta), \quad \gamma e_\Delta \mapsto \gamma \bmod \Delta$$

yields isomorphisms

$$\mathscr{M}_{E,\Gamma} e_\Delta \simeq \mathscr{M}_{E,\Gamma/\Delta}, \quad o_E\Gamma e_\Delta \simeq o_E(\Gamma/\Delta).$$

Hence by (2.7), (2.8),

$$\left[\mathscr{M}_{E,\Gamma}^\Delta : o_E\Gamma^\Delta\right]_{o_E}^2 = t^t\left(\frac{g}{t}\right)^{2t} = g^{2t} \cdot t^{-t}.$$

But the map $G \mapsto (g^2)^{\mathrm{ord}(G)}$ is clearly factorisable, and hence indeed we get (2.5).

(iii) We now look at h. Suppose the division D generates a group G of order $p^r m$ with $(p, m) = 1$. Write

$$h(D)_p = p^{l(D)}.$$

Thus $l(D) = 0$ if $r = 0$, and for $r \geq 1$ we have

$$\begin{aligned} l(D) &= \sum_{s|m} s\mu(m/s) \cdot \sum_{j=0}^{r} jp^j\mu(p^{r-j}) \\ &= \phi(p^r)\phi(m)\left(r + \frac{1}{p-1}\right) \quad (\phi \text{ the Euler function}) \\ &= \mathrm{ord}(D)\left(r + \frac{1}{p-1}\right). \end{aligned}$$

Then to every element θ of $\Gamma^\dagger$ attach a weight

$$\wr(\theta) = \begin{cases} 1 & \text{if } p \nmid \operatorname{ord}(\theta), \\ p^{r+1/(p-1)} & \text{if } \operatorname{ord}(\theta) = p^r m,\ (m, p) = 1,\ r > 0. \end{cases}$$

Then $h(D)_p = \prod_{\theta \in D} \wr(\theta)$, and so

$$h'(G)_p = \prod_{\theta \in G} \wr(\theta) \quad \text{for all } G < \Gamma^\dagger.$$

The assertions under (ii) and (iii) in Theorem 2 are an easy consequence of the last equation.

3. A norm theorem

This section displays another aspect of the techniques in this subject. Our aim is to prove a theorem relating to the norm property discussed in §1.

THEOREM 3. *Let the field F be of one of the following types*:

(i) *F is a number field and none of the prime divisors of* $\operatorname{ord}(\Gamma)$ *are ramified in $F/\mathbf{Q}$;*

(ii) *F is a non-ramified extension of $\mathbf{Q}_p$.*

Let M be an $o_F\Gamma$-lattice and for $G_\Delta < \Gamma^\dagger$, let

$$f(G_\Delta) = \left[M^\Delta : (M^\Delta)^{\mathscr{M}_{\Gamma/\Delta}} \right]_{o_F},$$

$\mathscr{M}_{\Gamma/\Delta}$ the maximal order of $F(\Gamma/\Delta)$. Then for any division D of $\Gamma^\dagger$, $f(D)$ is norm of an ideal in $F(D)$.

An immediate consequence of the theorem is that the value $\mathscr{J}^{\chi}_{L,M}(D)$, for $o_F\Gamma$-lattices L, M, is a norm from $F(D)$. For $F = \mathbf{Q}$ this leads to norm results on certain L-value-regulator quotients. Another consequence is the norm property of maps f_i for i: $L \to M$, as before.

Proof of Theorem 3. The hypothesis on F implies that $\mathscr{M}_{F,\Gamma}$ is generated over $o_F\Gamma$ by the idempotents. We fix a prime p, also in the global case, and denote by $[\ ]_\mathfrak{p}$ the $\mathfrak{p}$-part of the module index over o_F where $\mathfrak{p}$ lies above p. In the local case $[\ ]_\mathfrak{p}$ is just $[\ ]_{o_F}$.

Let D be the given division. Our aim is to prove that if $\overline{D} = G_\Delta$ then

$$f(D)_\mathfrak{p} = \left[(M^\Delta) e_D : M^{e_D} \right]_\mathfrak{p} = \left[(M^\Delta) e_D : (M^\Delta)^{e_D} \right]_\mathfrak{p} \tag{3.1}$$

where $M^{e_D} = [x \in M,\ xe_D = x]$. (3.1) for all $\not p$ implies that in fact

$$f(D) = \left[(M^\Delta)e_D : (M^\Delta)^{e_D}\right]_{o_F}$$

and this is clearly a norm from $F(D)$.

Let $\Gamma = \Gamma_p \oplus \Gamma_\times$, Γ_p the p-Sylow group. Then

$$\mathcal{M}_{F,\Gamma} = \mathcal{M}_{F,\Gamma_p} \otimes_{o_F} \mathcal{M}_{F,\Gamma_\times} \quad \text{and} \quad \Gamma^\dagger = \Gamma_p^\dagger \times \Gamma_\times^\dagger.$$

Let D generate the group G. Then $G = G_p \times G_\times$, $G_p < \Gamma_p^\dagger$, $G_\times < \Gamma_\times^\dagger$. Let $\operatorname{ord}(G) = p^r m$, $(m, p) = 1$. Let $\tilde{e}_j$ be the sum over all primitive idempotents e_ψ corresponding to characters $\psi \in G_p$ of order p^j. These lie in $E\Gamma_p$ for some splitting field E of Γ_p, but $\tilde{e}_j \in F\Gamma_p$ and in fact is primitive in $F\Gamma_p$ (recall (1.18) for the definition of e_ψ). Similarly let $\tilde{g}_d$ be the sum over all primitive idempotents g_λ corresponding to characters $\lambda \in G_\times$ of order d. Also put $e_j = \sum_{k=0}^{j} \tilde{e}_k$, $g_t = \sum_{d|t} \tilde{g}_d$.

Write $G_{j,t}$ for the subgroup of G of order $p^j t$. If $G_{j,t} = G_\Lambda$ then

$$M^\Lambda = M^{e_j \otimes g_t}.$$

If $g_t = \sum_i g_t^{(i)}$ (sum of primitive idempotents in $F\Gamma_\times$) then actually

$$\left[M^{(e_j \otimes g_t)} : \bigoplus_{d|t} M^{(e_j \otimes \tilde{g}_d)}\right]_{\not p} = \left[M^{(e_j \otimes g_t)} : \bigoplus_{i} M^{(e_j \otimes g_t^{(i)})}\right]_{\not p} = 1.$$

Therefore

$$f(G_{j,t})_{\not p} = \prod_{d|t} \left[M^{(e_j \otimes \tilde{g}_d)} : \bigoplus_{k \le j} M^{(\tilde{e}_k \otimes \tilde{g}_d)}\right]_{\not p}$$

Hence

$$f(D)_{\not p} = \prod_{j=0}^{r} \prod_{d|m} \left[M^{(e_j \otimes \tilde{g}_d)} : \bigoplus_{k \le j} M^{(\tilde{e}_k \otimes \tilde{g}_d)}\right]_{\not p}^{A_{j,d}}$$

where

$$A_{j,d} = \mu(p^{r-j}) \cdot \sum_{s|\frac{m}{d}} \mu(m/ds).$$

Thus $A_{j,d} = 0$ if $d < m$, $A_{j,m} = \mu(p^{r-j})$.

We now have

$$f(D)_{\mathfrak{p}} = \left[M^{(e_r \otimes \tilde{g}_m)} : \bigoplus_{k \le r} M^{(\tilde{e}_k \otimes \tilde{g}_m)}\right]_{\mathfrak{p}} \left[M^{(e_{r-1} \otimes \tilde{g}_m)} : \bigoplus_{k \le r-1} M^{(\tilde{e}_k \otimes \tilde{g}_m)}\right]_{\mathfrak{p}}^{-1}$$
$$= \left[M^{(e_r \otimes \tilde{g}_m)} : M^{(\tilde{e}_r \otimes \tilde{g}_m)} \oplus M^{(e_{r-1} \otimes \tilde{g}_m)}\right]_{\mathfrak{p}}.$$

We have quite generally the following rule for orthogonal idempotents f_1, f_2:

$$\left[M^{f_1+f_2} : M^{f_1} \oplus M^{f_2}\right] = \left[(M^{f_1+f_2})f_1 : M^{f_1}\right].$$

Thus

$$f(D)_{\mathfrak{p}} = \left[M^{(e_r \otimes \tilde{g}_m)}(\tilde{e}_r \otimes \tilde{g}_m) : M^{(\tilde{e}_r \otimes \tilde{g}_m)}\right]_{\mathfrak{p}}.$$

Let $g_m = \tilde{g}_m + g'$. As

$$\left[M^{(e_r \otimes g_m)} : M^{(e_r \otimes \tilde{g}_m)} \oplus M^{(e_r \otimes g')}\right]_{\mathfrak{p}} = 1$$

and as $g'\tilde{g}_m = 0$ we get

$$f(D)_{\mathfrak{p}} = \left[M^{(e_r \otimes g_m)}(\tilde{e}_r \otimes \tilde{g}_m) : M^{\tilde{e}_r \otimes \tilde{g}_m}\right]_{\mathfrak{p}}.$$

But $\tilde{e}_r \otimes \tilde{g}_m = e_D$, and $M^{(e_r \otimes g_m)} = M^{\Delta}$ for $G = G_{\Delta}$. This then is the required result.

References

1. A. Fröhlich, "Local fields" in *Algebraic number theory*, Brighton Proceedings (Ed. J.W.S. Cassels and A. Frohlich), Academic Press, Orlando, Florida, 1967.
2. C.W. Curtis and I. Reiner, *Methods of representation theory*, Vol. I, Wiley, New York, 1983.
3. A. Fröhlich, *Invariants for modules over commutative separable orders*, Quart. J. Math., vol. 16 (1965), pp. 193–232.
4. _____, *The module structure of Kummer extensions over Dedekind domains*, Crelle, vol. 209 (1962), pp. 39–53.
5. _____, *Gauss'sche Summen*, Notes by Kleinert, Denninger, Everest, Math. Inst. Univ. Köln, 1982/83.
6. _____, *Galois module structure of algebraic integers*, Springer, New York, 1983.
7. _____, *L-values at zero and multiplicative Galois module structure* (also *Galois Gauss sums and additive Galois module structure*) to appear.
8. _____, *L-functions at s = 0 and Galois modules*, Sem. de Théorie de Nombres de Bordeaux, to appear.
9. A. Nelson, London, Ph.D. thesis 1979.
10. H.M. Stark, *L-functions at s = 1*, Adv in Math., vol. 7 (1971), pp. 310–343; vol. 17 (1975), pp. 60–92; vol. 22 (1976), pp. 68–84.
11. J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*, Progr. Math., vol. 47 (1984).

Imperial College
London
Robinson College
Cambridge, England