FACTOR EQUIVALENCE RESULTS FOR INTEGERS AND UNITS

Autor(en): **De Smit, Bart**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **42 (1996)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-87884

L'Enseignement Mathématique, t. 42 (1996), p. 383–394

FACTOR EQUIVALENCE RESULTS FOR INTEGERS AND UNITS

by Bart DE SMIT

ABSTRACT. We give alternative proofs of two results of Fröhlich on the Galois module structure of the ring of integers and of the group of S-units in a Galois extension of number fields. We also point out applications to index computations in rings of integers and to class number relations.

1. INTRODUCTION

The purpose of this note is to give a brief presentation of basic factor equivalence results about the Galois module structure of the ring of integers and of the group of units in a Galois extension of number fields. Such results were first given by Nelson [12] and by Fröhlich [8, 9]. In [8] and [4, § 3] these results are proved for abelian and for "admissible" Galois groups. It was shown later by Ritter and Weiss that all finite groups are "admissible" [14]. The proofs given below do not use any subtle representation-theoretic properties such as admissibility.

We set up the terminology in the next section. In Section 3 we show that the ring of integers in a Galois extension of number fields is "factor equivalent" to the group ring of the Galois group over the ring of integers of the base field. The proof uses the conductor discriminant formula, and it holds in the more general context of extensions of Dedekind domains of characteristic zero with separable residue field extensions.

In Section 4 the factor equivalence class of the lattice of units is expressed in terms of class numbers of intermediate fields. The proof uses zeta-functions and it holds for arbitrary Galois extensions of number fields.

1991 Mathematics subject classification : 11R33.

Finally, we give two applications in Section 5 that show how these results are related to more concrete questions in algebraic number theory. First we indicate how to do certain index computations for rings of integers in abelian extensions of number fields. For a bicyclic quartic field this implies that the lattice generated by its quadratic integers has index 2 in the ring of integers. Then we explain that the result for units gives a method to obtain class number inequalities between so-called "arithmetically equivalent" number fields.

2. Factorizability and factor equivalence

Let G be a finite group. A character of G is said to be rational if it is the character of a representation of G defined over $\mathbf{Q}$. Denote the additive group of rational characters of G by $R(G)$. One can view $R(G)$ as the Grothendieck group of finitely generated $\mathbf{Q}[G]$-modules. It is the free abelian group generated by the set $X(G)$ of isomorphism classes of irreducible $\mathbf{Q}[G]$-modules.

The trivial character 1_H on a subgroup H of G induces the permutation character $1_H^G \in R(G)$, corresponding to the G-module $\mathbf{Q}[G/H]$. Let $\mathcal{S}$ denote the set of subgroups of G and let T be an abelian group. We will use multiplicative notation for the group operation on T.

(2.1) Definition. *A function $f\colon \mathcal{S} \to T$ is said to be factorizable if for every collection of integers $(a_H)_{H\in\mathcal{S}}$ with $\sum_{H\in\mathcal{S}} a_H 1_H^G = 0$ we have $\prod_{H\in\mathcal{S}} f(H)^{a_H} = 1$.*

(2.2) Examples. If G is the Galois group of an extension of number fields L/K then Galois theory gives a bijection between $\mathcal{S}$ and the set of intermediate fields of L/K. For any parameter associated to number fields one thus obtains a function on $\mathcal{S}$, and one may wonder if it is factorizable. The discriminant, zeta-function, and the odd part of the number of roots of unity in a number field, are all factorizable. The p-part of the class number for $p \nmid [L : K]$ is also factorizable; cf. [18]. The fact that the parameter hR/w is factorizable is known as "Brauer's class number relations" (see Section 4). See Kani and Rosen [10, 11] for factorizability results for curves and Jacobians.

A function $f\colon \mathcal{S} \to T$ induces a group homomorphism $f_*\colon \mathbf{Z}[\mathcal{S}] \to T$, where $\mathbf{Z}[\mathcal{S}]$ is the free abelian group generated by $\mathcal{S}$. By definition f is factorizable if and only if f_* vanishes on the kernel of the homomorphism $r\colon \mathbf{Z}[\mathcal{S}] \to R(G)$ given by $H \mapsto 1_H^G$. For abelian groups G the map r is surjective. For every group G the image of r has finite index by Artin's

induction theorem [16, Ch. 13, Th. 30]. If G is abelian or T is divisible, then it follows that f is factorizable if and only if $f_* = gr$ for some homomorphism $g\colon R(G) \to T$. We then have

$$f(H) = \prod_{\chi \in X(G)} g(\chi)^{n_{H,\chi}}$$

where $n_{H,\chi}$ is the multiplicity of χ in 1_H^G, i.e., $1_H^G = \sum_\chi n_{H,\chi}\chi$. This is the factorization that the word factorizable refers to. One way to show that a function f is factorizable is by exhibiting such a map g. For instance, to show that the discriminant function in (2.2) is factorizable one lets $g(\chi)$ be the Artin conductor of χ (see [15, Ch. VI, § 3]).

Let us give another example from linear algebra. Suppose that K is a field of characteristic zero and that M is a finitely generated $K[G]$-module. Let φ be a $K[G]$-endomorphism of M. Then φ maps M^H to M^H for any subgroup H of G, and the characteristic polynomial $f(H) \in K[t]$ of the restriction $\varphi|_{M^H}$ is a factorizable function with values in $T = K(t)^*$. To see this, define $g(V)$ for any $\mathbf{Q}[G]$-module V as the characteristic polynomial of the K-linear endomorphism of $\mathrm{Hom}_{K[G]}(K \otimes_{\mathbf{Q}} V, M)$ induced by φ. Then $g\colon R(G) \to T$ is a homomorphism such that $g(1_H^G) = f(H)$. This result is also given by Kani and Rosen [11, Prop. 4.6]. It implies the following lemma.

(2.3) LEMMA. *The functions* $\dim_K(M^H) \in \mathbf{Z}$ *and* $\mathrm{Tr}(\varphi|_{M^H}) \in K$ *are factorizable. If* φ *is an automorphism then* $d_\varphi(H) = \det(\varphi|_{M^H}) \in K^*$ *is factorizable.* □

Now suppose that K is the quotient field of a Dedekind domain A and still assume that $\mathrm{char}\, K = 0$. By an A-lattice we mean a finitely generated A-module without A-torsion, or equivalently, a finitely generated projective A-module. An $A[G]$-lattice is an $A[G]$-module that as an A-module is an A-lattice. Denote the group of fractional A-ideals by $I(A)$. For two A-lattices $X \subset Y$ with $X \otimes K = Y \otimes K$ the quotient X/Y is an A-module of finite length. If the Jordan-Hölder factors of X/Y are $A/\mathfrak{p}_1, \ldots, A/\mathfrak{p}_m$ then the A-index $[Y : X]_A$ is defined to be the A-ideal $\mathfrak{p}_1 \cdots \mathfrak{p}_m$ (cf. [15, Ch. I, § 5]).

(2.4) DEFINITION. *We say that two* $A[G]$*-lattices* M *and* N *are factor equivalent if there is an* $A[G]$*-linear map* $i\colon M \to N$ *for which the following hold:*

(1) *the induced map* $M \otimes_A K \to N \otimes_A K$ *is an isomorphism;*

(2) *the index* $\left[N^H : (M)^H\right]_A \in I(A)$ *is a factorizable function of* H.

(2.5) PROPOSITION. *If N and M are factor equivalent then for any $A[G]$-linear embedding $j\colon M \rightarrowtail N$ the function $H \mapsto \left[N^H : j(M^H)\right]_A$ is factorizable.*

Proof. We have $j = \varphi i$, where i is an embedding as in (2.4) and φ is a $K[G]$-linear automorphism of $N \otimes_A K$. Using [15, Ch. III, § 1, Prop. 2] and the notation of (2.3) we see that

$$\left[N^H : j(M^H)\right]_A = d_\varphi(H) \cdot \left[N^H : i(M^H)\right]_A \ .$$

This is a product of two factorizable functions by (2.3) and by our choice of i. □

The fact that "factor equivalence" is an equivalence relation is an easy consequence of (2.5). If $\mathfrak{p}$ is a prime of K not dividing $\#G$ then condition (1) of (2.4) implies that the $\mathfrak{p}$-part of $\left[N^H : i(M)^H\right]_A$ is factorizable. One can prove this with [16, § 15.2] and [16, § 14.4, Lemma 21].

(2.6) REMARK. The definitions of factorizability given by Fröhlich [8; 9] and Burns [2] for abelian groups G are in agreement with our definitions. They also define the notion called $\mathbf{Q}$-factorizability in the abelian case, which is a stronger condition than factorizability. However, the function that one wants to be factorizable in the definition of factor equivalence automatically satisfies this stronger condition if it is factorizable. Thus, $\mathbf{Q}$-factor equivalence is the same as factor equivalence.

In [4, § 3] a factorizable function f with values in $I(\mathbf{Q})$ must also satisfy an additional condition: there should be a map g from the group of complex characters $R_{\mathbf{C}}(G)$ to $I(E)$, where E is some normal number field containing all character values of G, such that g is $\mathrm{Gal}(E/\mathbf{Q})$-equivariant, and such that $g(1_H^G)$ is the E-ideal generated by $f(H)$. It is not hard to see that this condition is satisfied by all functions that are factorizable in our sense.

3. RINGS OF INTEGERS

Let A be a Dedekind domain with quotient field K of characteristic zero and let L a Galois extension of K with Galois group G. The integral closure B of A in L is again a Dedekind domain. Assume that for all primes of L the residue class field extension is separable.

(3.1) THEOREM. *The $A[G]$-lattices B and $A[G]$ are factor equivalent.*

Proof. Define a $B[G]$-module structure on $B \otimes_A B$ by letting B act on the left factor and G on the right. We will show first that $B \otimes_A B$ and $B[G]$ are factor equivalent as $B[G]$-lattices. Define the canonical $B[G]$-linear map $\varphi\colon B \otimes_A B \to B[G]$ by

$$x \otimes y \mapsto \sum_{\sigma \in G} x\sigma(y) \cdot \sigma^{-1} .$$

Let H be a subgroup of G. If $\sigma_1, \ldots, \sigma_n$ are the K-embeddings of L^H in L, and if there is an A-basis $\omega_1, \ldots, \omega_n$ of B^H, then the restriction $(B \otimes_A B)^H \to B[G]^H$ of φ is a B-linear map with matrix $\big(\sigma_i(\omega_j)\big)_{ij}$ on the bases $\{1 \otimes \omega_j\}$ and $\{b_i\}$, where b_i is the formal sum of those $\sigma \in G$ for which σ^{-1} restricts to σ_i. The square of the determinant of this matrix generates the discriminant $\Delta(B^H/A)$ as an A-ideal. By localization it follows that even if B is not free over A, we have

$$\big[B[G]^H : \varphi(B \otimes_A B)^H\big]_B^2 = \Delta(B^H/A) \cdot B .$$

By Hasse's conductor discriminant product formula [15, Ch. VI, § 3] the ideal $\Delta(B^H/A)$ is a factorizable function of H, so $B \otimes_A B$ and $B[G]$ are factor equivalent $B[G]$-lattices.

In order to descend to $A[G]$-lattices, note that there exists an $A[G]$-linear injection $i\colon A[G] \to B$ by the normal basis theorem, and consider the induced $B[G]$-linear map $i_*\colon B[G] \to B \otimes_A B$ that sends $b\sigma$ to $b \otimes i(\sigma)$ for $b \in B$ and $\sigma \in G$. We have

$$\big[(B \otimes_A B)^H : i_*\big(B[G]\big)^H\big]_B = \big[B^H : i\big(A[G]\big)^H\big]_A \cdot B ,$$

and by (2.5) we know that the left hand side is a factorizable function of H. But then the A-index $\big[B^H : i\big(A[G]\big)^H\big]_A$ is also factorizable. □

4. S-UNITS

Let L/K be a Galois extension of number fields with Galois group G, and let S be a finite G-stable set of primes of L containing the infinite primes. The ring of S-integers of L consists of all elements of L that are integral outside S. Its class number is written as $h_S(L)$ and its unit group, the group of S-units of L, is denoted by $U_S(L)$. The group of roots of unity in L is denoted by μ_L and its order is written as $w(L)$.

Define the $\mathbf{Z}[G]$-lattice X_S to be the kernel of the map $\mathbf{Z}[S] \to \mathbf{Z}$ that sends each $\mathfrak{p} \in S$ to 1. We have a canonical map $\log_L : U_S(L) \to \mathbf{R} \otimes_{\mathbf{Z}} X_S$ sending x to the formal sum $\sum_{\mathfrak{p} \in S} (\log |x|_{\mathfrak{p}}) \otimes \mathfrak{p}$ in $\mathbf{R}[S]$. Here the normalization of the valuation at a prime $\mathfrak{p}$ of L, lying over a prime p of $\mathbf{Q}$, is given by $|u|_{\mathfrak{p}} = |N_{L_{\mathfrak{p}}/\mathbf{Q}_p}(u)|_p$, where $|\cdot|_p$ is the usual valuation on the completion $\mathbf{Q}_p$ of $\mathbf{Q}$ (with $\mathbf{Q}_p = \mathbf{R}$ if $p = \infty$). Dirichlet's unit theorem says that $\log_L$ embeds $U_S(L)/\mu_L$ as a discrete cocompact lattice in $\mathbf{R} \otimes_{\mathbf{Z}} X_S$. The S-regulator $R_S(L) \in \mathbf{R}_{>0}$ is defined to be the covolume of this lattice when the measure on $\mathbf{R} \otimes_{\mathbf{Z}} X_S$ is normalized to give $1 \otimes X_S$ covolume 1.

For a subgroup H of G we let $S(H)$ be the set of primes of L^H that extend to a prime in S. We will write $h_S(L^H)$ for $h_{S(H)}(L^H)$ and $R_S(L^H)$ for $R_{S(H)}(L^H)$. Brauer [1] has shown that the function $H \mapsto h_S(L^H)R_S(L^H)/w(L^H)$ is a factorizable function with values in $\mathbf{R}_{>0}$. The easiest way to see this is by noting that this quotient is the absolute value of the leading coefficient in the Taylor series expansion at $s = 0$ of the zeta-function $\zeta_{L^H,S}(s)$ of L^H; see Tate [17, Ch. I, 2.2]. Since $\zeta_{L^H,S}(s)$ is equal to the Artin L-series $L_S(1_H^G, s)$, the factorizability result then follows from the fact that $L_S(\chi_1 + \chi_2, s) = L_S(\chi_1, s)\, L_S(\chi_2, s)$.

The group G acts on S, so it acts on $\mathbf{Z}[S]$ and on X_S. The map $\log_L$ induces an $\mathbf{R}[G]$-linear isomorphism $\mathbf{R} \otimes_{\mathbf{Z}} U_S(L) \xrightarrow{\sim} \mathbf{R} \otimes_{\mathbf{Z}} X_S$. It follows that the $\mathbf{Q}[G]$-modules $\mathbf{Q} \otimes_{\mathbf{Z}} U_S(L)$ and $\mathbf{Q} \otimes_{\mathbf{Z}} X_S$ are isomorphic; see [3, p. 110]. In particular, there exists a $\mathbf{Z}[G]$-linear embedding $i : X_S \to U_S(L)$.

For a prime $\mathfrak{p}$ of L^H all primes $\mathfrak{q}$ of L lying over $\mathfrak{p}$ have the same local degree, which we denote by $n_{\mathfrak{p}}(L/L^H)$. Let $n(H)$ be the product of all $n_{\mathfrak{p}}(L/L^H)$ with $\mathfrak{p} \in S(H)$, and let $l(H)$ be their least common multiple.

(4.1) THEOREM. *For any $\mathbf{Z}[G]$-linear embedding $i : X_S \hookrightarrow U_S(L)$, the function*

$$H \mapsto \left[U_S(L)^H : i(X_S)^H\right] \frac{n(H)}{l(H)\, h_S(L^H)}$$

with values in $\mathbf{Q}_{>0}$ is factorizable.

Proof. For $\mathbf{Z}$-lattices L_1, L_2 spanning the same real vector space V we define the "index" $[L_2 : L_1] \in \mathbf{R}_{>0}$ as follows: choose a Haar measure on V such that L_2 has covolume 1 and let $[L_2 : L_1]$ be the covolume of L_1. Note that this notion coincides with the usual index in the case that $L_1 \subset L_2$, and that $[L_1 : L_2][L_2 : L_3] = [L_1 : L_3]$. Moreover, for any $\mathbf{R}$-linear automorphism φ of V we have $\left[L_1 : \varphi(L_1)\right] = |\det \varphi|$.

For each subgroup H of G we have an injective map $j_H\colon \mathbf{Z}[S(H)] \to \mathbf{Z}[S]$ sending $\mathfrak{p}$ to $\sum_{\mathfrak{q}|\mathfrak{p}} n_{\mathfrak{p}}(L/L^H)\cdot\mathfrak{q}$. This map respects the logarithm map in the sense that we have a commutative diagram

$$\begin{array}{ccc} U_S(L^H) & \xrightarrow{\log_{L^H}} & \mathbf{R}\otimes X_{S(H)} \\ \| & & \downarrow 1\otimes j_H \\ U_S(L)^H & \xrightarrow{\log_L} & \mathbf{R}\otimes X_S^H\,, \end{array}$$

where the vertical map on the left is inclusion. We therefore have

$$R_S(L^H) = \left[X_{S(H)} : \log_{L^H} U_S(L^H)\right] = \frac{\left[X_S^H : \log_L U_S(L)^H\right]}{\left[X_S^H : j_H(X_{S(H)})\right]}\,.$$

The composite map $X_S \xrightarrow{i} U_S(L) \xrightarrow{\log_L} \mathbf{R}\otimes X_S$ induces an $\mathbf{R}[G]$-linear automorphism φ of $\mathbf{R}\otimes X_S$. With the notation of (2.3) one has

$$|d_\varphi(H)| = \left[X_S^H : \varphi(X_S^H)\right] = \left[X_S^H : \log_L U_S(L)^H\right]\frac{\left[U_S(L)^H : i(X_S^H)\right]}{w(L^H)}\,.$$

Combining these two formulas, and dividing by $h_S(L^H)$, we get

$$\left[U_S(L)^H : i(X_S)^H\right]\frac{\left[X_S^H : j_H(X_{S(H)})\right]}{h_S(L^H)} = |d_\varphi(H)|\frac{w(L^H)}{h_S(L^H)R_S(L^H)}\,. \tag{4.2}$$

The right hand side is factorizable by (2.3) and Brauer's theorem. It remains to show that $\left[X_S^H : j_H(X_{S(H)})\right] = n(H)/l(H)$. In order to do this we compare the sequence defining $X_{S(H)}$ with the H-invariants of the sequence defining X_S :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_{S(H)} & \longrightarrow & \mathbf{Z}[S(H)] & \longrightarrow & \mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow j_H & & \downarrow \#H & & \\ 0 & \longrightarrow & X_S^H & \longrightarrow & \mathbf{Z}[S]^H & \longrightarrow & \mathbf{Z}\,. & & \end{array}$$

The rows in this commutative diagram are exact and the vertical maps are injective. The cokernel C of the map j_H is the group $\bigoplus_{\mathfrak{p}\in S(H)} \mathbf{Z}/n_{\mathfrak{p}}(L/L^H)\mathbf{Z}$, which has order $n(H)$. It is not hard to see that the image of C in the cokernel of the rightmost vertical map has order $l(H)$. With the snake lemma our claim follows. □

(4.3) REMARK. One can shorten this proof somewhat by using results in Tate's book on the Stark conjectures. Tate shows in [17, Ch. II, 1.1] that $\big[U_S(L) : i(X_S)\big]/h_S(L)$ is equal to the Stark-quotient $A(1, i)$, where 1 denotes the trivial character of the trivial Galois group of L over L. Compatibility of the Stark-quotient with respect to inflation and addition of characters implies that the number on the left in (4.2) equals $A(1_H^G, i)$, and that it is a factorizable function of H.

(4.4) REMARK. In order to say that (4.1) determines the factor equivalence class of $U_S(L)$ we should define factor equivalence for $\mathbf{Z}[G]$-modules with $\mathbf{Z}$-torsion. This can be done by replacing condition (2) in (2.4) by the condition that the quotient of the order of cokernel and kernel of the map $M^H \to N^H$ should be factorizable.

Alternatively, one can look at $\overline{U}(L) = U_S(L)/\mu_L$ instead of $U_S(L)$. This approach does introduce new factors into the formula because $\overline{U}(L)^H$ is not necessarily equal to $\overline{U}(L^H)$. More precisely, $c(H) = \big[\overline{U}(L)^H : \overline{U}(L^H)\big]$ is the order of the kernel of the map $H^1(H, \mu_L) \to H^1\big(H, U_S(L)\big)$, so we know that it is built up from primes dividing both $w(L)$ and $\#G$. For $\mathbf{Z}[G]$-embeddings $i\colon X_S \rightarrowtail \overline{U}(L)$ it turns out that the map

$$H \mapsto \big[\overline{U}(L)^H : i(X_S)^H\big] \frac{w(L^H)\, n(H)}{h_S(L^H)\, c(H)\, l(H)} \tag{4.5}$$

is factorizable. Thus one recovers [4, § 3, Th. 3], where it is assumed that L has odd degree over K and K is totally real, so that $c(H) = n(H) = l(H) = 1$ and $w(L^H) = 2$. Brauer [1] showed that the odd part of $w(L^H)$ is a factorizable $\mathbf{Q}^*$-valued function of H, and his argument inspired the following lemma (cf. [11, Prop. 4.7]).

(4.6) LEMMA. *Let G be a group, let D be a subgroup of G and let N be a normal subgroup of D of index n such that D/N is cyclic. For every divisor d of n and subgroup H of G, let $m_d(H) \in \mathbf{Z}$ be the number of D-orbits of G/H that split up into exactly d orbits under the action of N. Then $m_d(H)$ is a factorizable $\mathbf{Z}$-valued function of H.*

Proof. Let $\chi\colon D \to \mathbf{C}^*$ be a complex linear character such that $\chi(N) = 1$, and let χ^G be the induced character of G. We claim that $\langle \chi^G, 1_H^G \rangle_G$ is the sum of those $m_d(H)$ for which d is a multiple of the order of χ. Since $\langle \cdot\,, \cdot \rangle_G$ is a bilinear operation on characters of G (see [16, § 7.2]) the integer $\langle \chi^G, 1_H^G \rangle_G$ is a factorizable function of H. We deduce the lemma from the claim by

taking χ of order d and using induction: we start with $n = d$ and then successively remove prime factors from d. It remains to show the claim.

By Frobenius reciprocity one has $\langle \chi^G, 1_H^G \rangle_G = \langle \chi, 1_H^G |_D \rangle_D$, which is equal to the multiplicity of χ in the complex representation $\mathbf{C}[G/H]$ of D. The D-set G/H is D-isomorphic to a disjoint union $\coprod_X D/D_X$, where X runs over the D-orbits of G/H, and each D_X is a subgroup of D. The multiplicity of χ in $\mathbf{C}[D/D_X]$ is either 0 or 1, and it is 1 if and only if $D_X \subset \operatorname{Ker} \chi$. Since $N \subset \operatorname{Ker} \chi$, and D/N is cyclic, it follows that $\langle \chi^G, 1_H^G \rangle_G$ is equal to the number of X for which the order of χ divides $[D : ND_X]$. This index is the number of N-orbits of D/D_X, so the claim follows. □

If for a prime number p the roots of unity in L of p-power order generate a cyclic extension of K, then one can show with the lemma (with $D = G$) that the p-part of $w(L^H)$ is a factorizable $\mathbf{Q}^*$-valued function of H. The condition holds for all $p > 2$, so the odd part of $w(L^H)$ is factorizable.

For any prime $\mathfrak{p}$ of K and $d \in \mathbf{Z}$ the number of primes in L^H extending $\mathfrak{p}$ with residue degree d is a $\mathbf{Z}$-valued factorizable function of H. This follows from the lemma if we take D and N to be the decomposition group and the inertia group of $\mathfrak{p}$. If $\mathfrak{p}$ has a cyclic decomposition group D then one can also take $N = 1$, and deduce the same statement with "residue degree" replaced by "local degree".

It follows that the factor $n(H)$ in (4.1) can be replaced by the product of the ramification indices in the extension L/L^H of those primes $\mathfrak{p} \in S(H)$ that extend to a prime of L with non-cyclic decomposition group in L/K. In particular, $n(H)$ is factorizable if S contains no finite ramified primes.

5. Applications

Without giving proofs we indicate some concrete applications of the factor equivalence results given in the last two sections.

(5.1) Cyclic subfield integer index. Let K be a Galois extension of $\mathbf{Q}$ with abelian Galois group G and ring of integers $\mathcal{O}_K$. For a $\mathbf{Z}[G]$-module M let $c_G(M)$ be the index in M of $\sum M^H$, where the sum is taken over those subgroups H of G for which G/H is cyclic. In particular,

$c_G(\mathcal{O}_K)$ is the index in $\mathcal{O}_K$ of the lattice generated by integers in the cyclic subfields of K. An argument of Gillard (see [2, Prop. 1]) implies that $c_G(M)$ only depends on the $\mathbf{Z}[G]$-module structure of M up to factor equivalence. With (3.1) it follows that $c_G(\mathcal{O}_K) = c_G(\mathbf{Z}[G])$. Therefore, one only needs to consider the group ring for the computation of this "cyclic subfield integer index". An explicit formula for $c_G(\mathbf{Z}[G])$ is given in [6]. For instance, if G has type (p,p) for some prime number p then one obtains $c_G(\mathcal{O}_K) = p^{p(p-1)/2}$. In this case one can deduce in particular that every integral basis of $\mathcal{O}_K$ contains a primitive element of K (cf. [5]).

(5.2) CLASS NUMBER INEQUALITIES. Theorem (4.1) gives a relation between the relative position of the groups of units of fields, and their class numbers. Let us consider the fields of degree 8 of Perlis [13]: we take $a \in \mathbf{Z}$ with $|a|$ not a square or twice a square. The fields $K = \mathbf{Q}(\sqrt[8]{a})$ and $K' = \mathbf{Q}(\sqrt[8]{16a})$ are the invariant fields under subgroups H and H' of $G = \mathrm{Gal}(L/\mathbf{Q})$ with $L = \mathbf{Q}(\zeta_8, \sqrt[8]{a})$. The fields K and K' are "arithmetically equivalent", i.e., they have the same zeta-function. One way to see this is by checking that $1_H^G = 1_{H'}^G$. Since $w(K) = w(K')$, Brauer's theorem implies that $hR = h'R'$, where h, h' and R, R' are the class number and regulator of K and K'. There exist integers a for which $h \neq h'$, such as $a = -15$; see [7].

Choose any $\mathbf{Z}[G]$-linear embedding $\varphi\colon X_S \to U_S(L)$, where S is the set of infinite primes of L. Suppose that we also have an injective $\mathbf{Z}[G]$-linear homomorphism $f\colon \mathbf{Z}[G/H'] \to \mathbf{Z}[G/H]$. Applying the functors $\mathrm{Hom}_G(-, X_S)$ and $\mathrm{Hom}_G\big(-, U_S(L)\big)$ to f we get a commutative diagram

$$\begin{array}{ccc} X_S^H & \xrightarrow{f_X} & X_S^{H'} \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} \\ U_S(K) & \xrightarrow{f_U} & U_S(K')\ . \end{array}$$

With (4.1) and this diagram one sees that the quotient h/h' is given by

$$\frac{h}{h'} = \frac{\#\,\mathrm{Cok}\,\varphi_1}{\#\,\mathrm{Cok}\,\varphi_2} = \frac{\#\,\mathrm{Ker}\,f_U \cdot \#\,\mathrm{Cok}\,f_X}{\#\,\mathrm{Cok}\,f_U} = \frac{\big[X_S^{H'} : f_X(X_S^H)\big]}{\big[U_S(K') : \mu_{K'} f_U(U_S(K))\big]}\ .$$

Thus, h/h' is equal to the index $i_f = \big[X_S^{H'} : f_X(X_S^H)\big]$ divided by some positive integer. One obtains a bound in the other direction by switching the role of K

and K'. The index i_f is an entirely combinatorial object; it only depends on f and the signature of K. With a judicious choice of the map f as in [13, p. 507] one can get $i_f = 16$ if $a > 0$, and $i_f = 4$ if $a < 0$. One now recovers [13, Th. 8]: we have $h/h' = 2^k$ with $|k| \leq 4$ if $a > 0$ and $|k| \leq 2$ if $a < 0$.

REFERENCES

[1] BRAUER, R. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math. Nachr. 4* (1951), 158–174.

[2] BURNS, D. Factorisability, group lattices, and Galois module structure. *J. Algebra 134* (1990), 257–270.

[3] CASSELS, J. W. S. and A. FRÖHLICH (eds.). *Algebraic number theory*. Academic Press, London, 1967.

[4] CASSOU-NOGUÈS, Ph., T. CHINBURG, A. FRÖHLICH and M. J. TAYLOR. L-functions and Galois-modules, pp. 75–139 in: J. Coates and M. J. Taylor (eds.), *L-functions and arithmetic*, Proc. 1989 Durham Symp. London Math. Soc. Lecture Note Ser. 153, Cambridge 1991.

[5] DE SMIT, B. Primitive elements in integral bases. *Acta Arith. 71* (1995), 159–170.

[6] —— On the integers from cyclic subfields in an abelian number field. *Technical Report 96-16*, Universiteit van Amsterdam, 1996.

[7] DE SMIT, B. and R. PERLIS. Zeta functions do not determine class numbers. *Bull. Amer. Math. Soc. (N.S.) 31* (1994), 213–216.

[8] FRÖHLICH, A. L-values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure). *J. Reine Angew. Math. 397* (1989), 42–99.

[9] —— Module defect and factorizability. *Illinois J. Math. 32* (1988), 407–421.

[10] KANI, E. and M. ROSEN. Idempotent relations and factors of Jacobians. *Math. Ann. 284* (1989), 307–327.

[11] KANI, E. and M. ROSEN. Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties. *J. Number Theory 46* (1994), 230–254.

[12] NELSON, A. M. Monomial representations and Galois module structure. Ph. D. thesis, King's College, University of London, 1979.

[13] PERLIS, R. On the class numbers of arithmetically equivalent fields. *J. Number Theory 10* (1978), 489–509.

[14] RITTER, J. and A. WEISS. Galois action on integral representations. *J. London Math. Soc. (2) 46* (1992), 411–431.

[15] SERRE, J.-P. *Local fields*. Springer-Verlag, New York, 1979.

[16] SERRE, J.-P. *Linear representations of finite groups*. Springer-Verlag, New York, 1977.

[17] TATE, J. *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*. Birkhäuser, Boston, 1984.

[18] WALTER, C. D. Brauer's class number relation. *Acta Arith. 35* (1979), 33–40.

(Reçu le 3 avril 1995; version révisée reçue le 18 décembre 1995)

Bart de Smit

Econometrisch Instituut
Erasmus Universiteit Rotterdam
Postbus 1738, 3000 DR Rotterdam
Netherlands

E-mail : dsmit@wis.few.eur.nl