Factorizability and Galois module structure

Bart de Smit

Abstract. We generalize theorems 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. The arguments work for any base field and Galois group without using "admissibility." For abelian extensions $K \subset L$ of number fields we deduce a formula for the index in the ring of integers of L of the additive subgroup generated by integers from subfields that are cyclic over K.

Key words: Factorizability, Galois module structure of rings of integers, class number relations.

1991 Mathematics subject classification: 11R33, 11R04.

1. Introduction.

This note focuses on two theorems of Fröhlich on the Galois module structure of rings of integers and of groups of units in number fields. Fröhlich [12] published these theorems for the case of abelian Galois groups in 1989, and they are given in [5, §3] for "admissible" Galois groups. It was proved by Ritter and Weiss [23] (1992) that all finite groups are admissible. In this paper we show how more general versions of the two theorems can be derived without using any subtle properties of integral representations like admissibility. Basically, the theorems are reformulations of Hasse's conductor discriminant product formula and of Brauer's class number relations.

The results are formulated in terms of "factorizability." More subtle modifications such as "canonical factorizability" have been considered in the past few years [3; 26], but in this note we only deal with the original notion. We give the definitions in the next section and we will point out existing factorizability results in number theory and algebraic geometry, which occur in Brauer's 1951 paper [1], and in work of Kani and Rosen [16; 17] (1989, 1994).

The notion of factorizability gives rise to an equivalence relation on lattices over finite group rings called "factor equivalence." The additive theorem says that the ring of integers in a Galois extension is factor equivalent to the group ring of the Galois group. We give a short algebraic proof of this fact in section 3, that works over any Dedekind domain of characteristic 0 with a perfect residue field.

For the abelian case a more explicit characterization of factor equivalence is given in section 4. This approach enables us to apply the additive theorem to do certain index computations in rings of integers. For any abelian extension of number fields $K \subset L$, a formula is given for the index in the ring of integers of L of the subgroup generated additively by the integers from intermediate fields that are cyclic over K. The

remarkable point here is that this index is determined by the Galois module structure of the ring of integers *up to factor equivalence* so that our computation only needs to consider the group ring. This will allow us to answer some particular cases of a problem raised by Cohen and Lenstra; see (4.8).

In section 5 the multiplicative theorem is given, which essentially expresses the factor equivalence class of the Galois module of S-units in terms of S-class numbers. We use ideas that can be found in Tate's formulation of the Stark conjectures [27].

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 $\mathbb{Q}$. Denote the additive group of rational characters of G by $R(G)$. One can view $R(G)$ as the Grothendieck group of finitely generated $\mathbb{Q}[G]$-modules. It is the free abelian group generated by the set $X(G)$ of isomorphism classes of irreducible $\mathbb{Q}[G]$-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 $\mathbb{Q}[G/H]$.

(2.1) Definition. *A Brauer relation is an equality $\sum_H a_H 1_H^G = 0$ in $R(G)$, where H ranges over the subgroups of G and $a_H \in \mathbb{Z}$.*

The permutation character 1_H^G depends only on H up to conjugacy, so we have a Brauer relation $1_H^G = 1_{H'}^G$ for every pair H, H' of conjugate subgroups of G.

(2.2) Examples. If $G = V_4$ is the Klein group of order 4, i.e. abelian of type $(2,2)$, then G has 3 subgroups H_1, H_2, H_3 of order 2, and the trivial subgroup 1. We have the Brauer relation $2 \cdot 1_G + 1_1^G = 1_{H_1}^G + 1_{H_2}^G + 1_{H_3}^G$.

For the symmetric group $G = S_3$, which has a normal subgroup A_3 of order 3 and a subgroup H of order 2, we have the relation $2 \cdot 1_G + 1_1^G = 1_{A_3}^G + 2 \cdot 1_H^G$.

Let T be any abelian group, with multiplicative notation of the group operation.

(2.3) Definition. *A function f on the set of subgroups of G with values in T is factorizable if $\prod_H f(H)^{a_H} = 1$ for every Brauer relation $\sum a_H 1_H^G = 0$.*

(2.4) Remark. A function f as in (2.3) is clearly factorizable if there are $g(\chi) \in T$ for $\chi \in X(G)$ such that

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

where $n_{H,\chi}$ is the multiplicity of χ in 1_H^G, i.e., $1_H^G = \sum_\chi n_{H,\chi}\chi$. In many cases, for instance if G is abelian or T is divisible (see (2.8) below), the converse holds, that is, there are such values $g(\chi)$ whenever f is factorizable. This is the factorization that the

word "factorizable" refers to. Often, the product can be broken down further to the irreducible complex characters.

(2.5) Examples from group theory. Take $T = \mathbb{Z}$ and let $f(H) = [G : H]$ for any subgroup H of G. With $g(\chi) = \deg \chi$ the above factorization holds, so f is factorizable. The function $H \mapsto 1 \in \mathbb{Z}$ is also factorizable. This follows by taking $g(\chi) = 1$ for the trivial character, and $g(\chi) = 0$ for other $\chi \in X(G)$. The function $H \mapsto \#H \in \mathbb{Z}$ is not in general factorizable. A more subtle factorizable function in a purely group theoretic setting is given in (5.7).

(2.6) Examples from number theory. If L/K is a Galois extension of number fields with Galois group G, then each subgroup H of G has a field of invariants L^H. Many well-known parameters of the number field L^H turn out to depend factorizably on H. The most important examples are the discriminant over the base field (see (3.1)) and the parameter hR/w. The latter result is known as "Brauer's class number relations." In fact the zeta-function of L^H depends factorizably on H, and $-hR/w$ is its leading coefficient at $s = 0$ (see (5.1)).

Brauer showed that the odd part of the number of roots of unity in L^H is a $\mathbb{Q}^*$-valued factorizable function of H. We elaborate on his proof (5.9) and we also deduce that the number of primes of L^H over a fixed prime $\mathfrak{p}$ of K with given residue degree, is a factorizable $\mathbb{Z}$-valued function. Walter [28] has shown that for primes p not dividing the order of G the p^k-rank of the class group is factorizable. I. Kersten has pointed out to the author that this was already known to E. Witt [29] in 1961.

See Perlis [21] for constructions of Brauer relations of the form $1^G_{H_1} = 1^G_{H_2}$ for non-conjugate subgroups of G. Thus, one can obtain non-isomorphic number fields with the same zeta-function. Such fields need not have the same class number [10].

(2.7) Examples from algebraic geometry. Let C be a smooth curve over a field k, and let G be a subgroup of $\mathrm{Aut}_k(C)$. Kani and Rosen [16] have shown that the Jacobians of the curves C/H satisfy Brauer relations up to isogeny (i.e., the map sending H to the k-isogeny class of $\mathrm{Jac}(C/H)$ is a factorizable map with values in the free abelian group on simple abelian varieties up to k-isogeny). In particular, the genus of C/H, which is the dimension of its Jacobian, is a factorizable $\mathbb{Z}$-valued function of H. For a quasi-projective variety X over a finite field k and a finite group $G \subset \mathrm{Aut}_k(X)$, the zeta function of X/H depends factorizably on H and the number of k-rational points on X/H is a $\mathbb{Z}$-valued factorizable function of H (cf. [17, 19]).

(2.8) Factorizable homomorphisms. Let $B(G)$ be the free abelian group generated by the subgroups of G. A function f from the set of subgroups of G to T induces a group homomorphism from $B(G)$ to T, which will be called factorizable if f is factorizable.

The map $H \mapsto 1_H^G$ gives a canonical homomorphism $r : B(G) \to R(G)$, which is by definition factorizable. A homomorphism $f : B(G) \to T$ is factorizable if and only if it vanishes on the kernel of r. In particular, if f factors through $R(G)$, that is, $f = gr$ for some homomorphism $g : R(G) \to T$, then f is factorizable. With this g one can write down the factorization in (2.4). Clearly, the converse holds if T is divisible.

For abelian groups G the map r is surjective (see (4.2)), so factorizable functions factor through $R(G)$. For arbitrary groups G, the image of $B(G)$ in $R(G)$ is of finite index by Artin's induction theorem (see [6, §39] or [25, chap. 13, thm. 30]). For instance, if G is the quaternion group of order 8, then the image of $B(G)$ in $R(G)$ is of index 2.

(2.9) Other coefficient fields. Let K be a field whose characteristic does not divide the order of G. The group ring $K[G]$ is semisimple, so the Grothendieck group $R_K(G)$ of finitely generated $K[G]$-modules is the free abelian group generated by the irreducible representations of G over K. The homomorphism $B(G) \to R_K(G)$ that sends a subgroup H of G to the class of the module $K[G/H]$, is factorizable. In fact, it factors through the map $R(G) \to R_K(G)$ that sends a $\mathbb{Q}[G]$-module V to $\Lambda \otimes_{\mathbb{Z}} K$, where Λ is a G-stable lattice of V; see Serre [25, §15.2] for details.

Let M be a finitely generated $K[G]$-module and let φ be a $K[G]$-endomorphism of M. Then φ maps V^H to V^H for any subgroup H of G, and the characteristic polynomial $f(H) \in K[t]$ of the restriction $\varphi|_{V^H}$ is a $K(t)^*$-valued factorizable function. To see this, define $g(V)$ for any $K[G]$-module V as the characteristic polynomial of the K-linear endomorphism of $\mathrm{Hom}_{K[G]}(V, M)$ induced by φ. Indeed, $g : R_K(G) \to T$ is a homomorphism and we have $f(H) = g(K[G/H])$. This result is also given by Kani and Rosen [17, prop. 4.6]. It implies the following lemma.

(2.10) Lemma. *The functions* $\dim_K(M^H) \in \mathbb{Z}$ *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.* □

If $\mathrm{char}\, K \mid \#G$, then the lemma is not necessarily true. For example, let G be the additive group of the field $\mathbb{F}_4$ of four elements and let $a \in G$ act on $M = \mathbb{F}_4 \times \mathbb{F}_4$ as the matrix $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. It is easy to check that the function $H \mapsto \dim_{\mathbb{F}_4} M^H$ does not satisfy the Brauer relation given in (2.2).

We now give the definition of factor equivalence. Let K be the quotient field of a Dedekind domain A and still assume that $\mathrm{char}\, K \nmid \#G$. An A-lattice is 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. Denoting the Jordan-Hölder factors of X/Y by $A/\mathfrak{p}_1, \ldots, A/\mathfrak{p}_m$, we define the A-index $[Y : X]_A$ to

be the A-ideal $\mathfrak{p}_1 \cdots \mathfrak{p}_m$ (cf. [24, chap. I, §5]).

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

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

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

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

Proof. We have $j = \varphi i$, where i is the embedding from (2.11) and φ is a $K[G]$-linear automorphism of $N \otimes_A K$. Using [24, chap. III, §1, prop. 2] and the notation of (2.10) we have $d_\varphi(H) = [i(M^H) : j(M^H)]_A$. It follows that

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

which is a product of two factorizable functions by (2.10) and our choice of i. □

The fact that "factor equivalence" is an equivalence relation is an easy consequence of (2.12). For the abelian case the same definition of factor equivalence can be found in [2; 12; 13].

The next proposition says that the only primes of A that play a role in (2.11) are those that divide the order of G. In particular, if $p = \operatorname{char} K > 0$ and $p \nmid \#G$ then the theory of factor equivalence is vacuous in the sense that (1) implies (2) in (2.11).

(2.13) Proposition. *If $\mathfrak{p}$ is a prime of K not dividing $\#G$ then condition* (1) *of* (2.11) *implies that the $\mathfrak{p}$-part of $[N^H : i(M)^H]_A$ is factorizable.*

Proof. Denote the localization of A at $\mathfrak{p}$ by $A_\mathfrak{p}$. By (2.12) we are done if $M \otimes_A A_\mathfrak{p}$ and $N \otimes_A A_\mathfrak{p}$ are isomorphic as $A_\mathfrak{p}[G]$-modules. Let k be the residue field $A/\mathfrak{p}$. Since $M \otimes_A K$ and $N \otimes_A K$ are isomorphic $K[G]$-modules, the $k[G]$-modules $M \otimes_A k$ and $N \otimes_A k$ are Jordan-Hölder-isomorphic [25, §15.2] and since $k[G]$ is semisimple this implies that they are isomorphic. We now deduce by [25, §14.4, lemma 21] that $M \otimes_A A_\mathfrak{p}$ and $N \otimes_A A_\mathfrak{p}$ are projective as $A_\mathfrak{p}[G]$-modules and that they are isomorphic. □

(2.14) Remark. The definitions of factorizability given by Fröhlich [12; 13] and Burns [2] for abelian groups G are special cases of our definitions. We now show that the definition in [5, §3] for arbitrary finite groups is a special case of our definition as well. Here a factorizable function f has to take values in the ideal group $I(\mathbb{Q})$ of $\mathbb{Q}$, and it has to satisfy the following additional condition: there is a map g from the group of complex characters $R_\mathbb{C}(G)$ to $I(E)$, where E is some normal number field containing all character values of G, such that g is $\mathrm{Gal}(E/\mathbb{Q})$-equivariant, and such that $g(1_H^G)$

is the E-ideal generated by $f(H)$. If f is factorizable in the sense of (2.3), then this condition is satisfied as follows. First note that for some positive integer n, the map nf factors through $h : R(G) \to I(\mathbb{Q})$. For each irreducible rational character χ of G, suppose χ is a sum of k_χ complex irreducible characters. Let k be a positive integer such that $k_\chi \mid k$ for all such χ. Let E be a normal splitting field of G in which the ramification index of each prime p occurring in $f(H)$ for some H, is divisible by nk. It is easy to check that the fractional ideal in E generated by any such p is a nkth power of a Galois invariant ideal in E. The fractional E-ideal generated by $h(\chi)$ is therefore equal to $\mathfrak{a}^{nk_\chi}$ for some Galois invariant ideal $\mathfrak{a}$. For each irreducible complex constituent χ_i of χ, we can now define $g(\chi_i)$ to be $\mathfrak{a}$.

3. Rings of integers.

Let A be a Dedekind domain with quotient field K and let L a Galois extension of K with Galois group G. The group of fractional A-ideals is denoted by $I(A)$. The integral closure B of A in L is again a Dedekind domain. Assume that at all primes of L the extension of residue class fields is separable.

(3.1) Proposition. *The map from the set of subgroups of G to $I(A)$ sending H to the discriminant $\Delta(B^H/A)$ over A of the H-invariants of B, is factorizable.* □

The proof is immediate from the discriminant conductor product formula of Hasse [24, chap. VI, §3]. In fact, f factors through a map $R_{\mathbb{C}}(G) \to I(A)$ that sends a complex character χ of G to its Artin-conductor $\mathfrak{f}(\chi, L/K) \in I(A)$. The proposition does not hold without the assumption that the residue field extensions are separable.

The following theorem is a generalization of theorem 1 in [5, §3]. In view of (4.5), theorem 7 (additive) in [12] is the same statement for abelian G. The first statement of this sort is due to Nelson [18].

(3.2) Theorem. *If the characteristic of K does not divide the order of G, then the $A[G]$-lattices B and $A[G]$ are factor equivalent.*

Proof. By the normal basis theorem there is an $A[G]$-linear injection $i : A[G] \to B$ satisfying the first condition of (2.11). Define a $B[G]$-module structure on $B \otimes_A B$ by letting G act on the left factor and B on the right. The map i induces a $B[G]$-linear map $i_* : B[G] \rightarrowtail B \otimes_A B$ given by $i_*(b\sigma) = i(\sigma) \otimes b$ for $\sigma \in G$ and $b \in B$. Furthermore, taking H-invariants commutes with tensoring with B, so

$$[(B \otimes B)^H : i_*(B[G]^H)]_B = [B^H : i(A[G]^H)]_A \cdot B.$$

It remains to show that $B \otimes B$ and $B[G]$ are factor equivalent $B[G]$-lattices, because (2.12) then implies that the left hand side is a factorizable function of H.

The base change from $A[G]$-lattices to $B[G]$-lattices has the advantage that we now have a canonical $B[G]$-linear map $\varphi : B \otimes B \rightarrowtail B[G]$ defined by

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

We claim that for any subgroup H of G we have

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

It is clear from (3.1) that this implies our theorem.

It suffices to prove the claim in the case that A is local, so that A-lattices are free A-modules. We will write down a matrix for the restriction of φ to H-invariants. Define the B-basis $\{b_i\}_i$ of $B[G]^H$ by letting $\{\sigma_i\}_i$ be the set of K-algebra homomorphisms of $L^H \to L$ and letting b_i be the sum of all the $\sigma \in G$ with $\sigma^{-1}|_H = \sigma_i$. If $\{\omega_j\}_j$ denotes a basis for B^H over A, then $\{\omega_j \otimes 1\}_j$ is a basis of $(B \otimes B)^H = B^H \otimes B$ over B. The matrix of the restricted B-linear map $\varphi : (B \otimes B)^H \to B[G]^H$ on the given bases is $(\sigma_i(\omega_j))_{ij}$. We know that the square of its determinant generates the A-ideal $\Delta(B^H/A)$, which proves our claim. □

4. Factor equivalence in the abelian case.

We now give a description of a criterion for factor equivalence in the abelian case, and then proceed with the index computation announced in the introduction.

The main argument was given by Gillard [14], and Burns [2] indicated the relevance to factor equivalence. A key ingredient is the following lemma, which was first stated by Rédei and proved by De Bruijn [7; 22]. Gillard and Gras [15] attribute it to Martinet.

(4.1) Lemma (De Bruijn-Rédei). *Let $n > 1$ be an integer. The ideal of $\mathbb{Z}[X]$ generated by the polynomials $(X^n - 1)/(X^{n/p} - 1)$, where p ranges over the prime factors of n, is the principal ideal generated by the n-th cyclotomic polynomial $\Phi_n(X)$.*

Proof. Note that $\mathbb{Z}[X]/(X^n - 1)$ is the group ring $\mathbb{Z}[C_n]$ of the cyclic group C_n of order n generated by the image of X. Let I_n be the image in $\mathbb{Z}[C_n]$ of the ideal generated by the polynomials $(X^n - 1)/(X^{n/p} - 1)$ where p ranges over the prime factors of n.

For any $m \geq 0$ we have $\prod_{d|m} \Phi_d(X) = X^m - 1$, and since $\mathbb{Q}[X]$ is a unique factorization domain this implies that $(\mathbb{Z}[C_n]/I_n) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathbb{Q}(\zeta_n)$. We still have to show that $\mathbb{Z}[C_n]/I_n$ is a torsion free abelian group or, equivalently, that we have a ring isomorphism $\mathbb{Z}[C_n]/I_n \cong \mathbb{Z}[\zeta_n]$.

If n is a prime power, the lemma is clear. Otherwise write $n = mk$ with $m > 1$ and $k > 1$ coprime. We have $\mathbb{Z}[C_n] \cong \mathbb{Z}[C_m] \otimes \mathbb{Z}[C_k]$, and under this isomorphism I_n

maps to $I_m \otimes \mathbb{Z}[C_k] + \mathbb{Z}[C_m] \otimes I_k$. It follows that $\mathbb{Z}[C_n]/I_n = (\mathbb{Z}[C_m]/I_m) \otimes (\mathbb{Z}[C_k]/I_k)$, and by induction this is $\mathbb{Z}[\zeta_m] \otimes \mathbb{Z}[\zeta_k] \cong \mathbb{Z}[\zeta_n]$. □

Let G be an abelian group. The group ring $\mathbb{Q}[G]$ is a product of cyclotomic fields F_χ, where χ ranges over the set $X(G)$ of irreducible rational characters of G. If $\chi_0 : G \to \mathbb{C}^*$ is an irreducible complex constituent of χ of order n_χ, then $F_\chi \cong \mathbb{Q}(\chi_0(G)) = \mathbb{Q}(\zeta_{n_\chi})$. The kernel of χ_0, which depends only on χ, is denoted by H_χ. Clearly, H_χ is cocyclic, i.e., G/H_χ is cyclic.

If $\psi \in X(G)$ has non-zero multiplicity in the $\mathbb{Q}[G]$-module $\mathbb{Q}[G/H_\chi]$, then the multiplicity is 1 and we write $\psi \mid \chi$. In other words, we have $1_{H_\chi}^G = \sum_{\psi \mid \chi} \psi$, and the following lemma follows from Möbius inversion.

(4.2) Lemma. *The permutation characters 1_H^G of cocyclic subgroups H of G form a $\mathbb{Z}$-basis of $R(G)$.* □

A $\mathbb{Q}[G]$-module V is just a product of vector spaces V_χ over F_χ. For a $\mathbb{Z}[G]$-lattice M, we let $M(\chi)$ be the projection of M^{H_χ} in $(M \otimes_{\mathbb{Z}} \mathbb{Q})_\chi$.

(4.3) Lemma. *The kernel of the epimorphism $M^{H_\chi} \to M(\chi)$ is $\sum_{H'} M^{H'}$, where H' runs over all subgroups of G that strictly contain H_χ.*

Proof. One inclusion is clear: $\sum_{H'} M^{H'}$ lies in the stated kernel, because the character χ does not occur in $M^{H'} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Let g be a generator of G/H_χ. Note that $(M \otimes_{\mathbb{Z}} \mathbb{Q})_\psi$ is killed by $\Phi_{n_\psi}(g)$ for any $\psi \mid \chi$. Put $n = n_\chi$ and let $\Psi_n = (X^n - 1)/\Phi_n \in \mathbb{Z}[X]$. If $x \in M_\chi^H$ maps to zero in $M(\chi)$, then the characters $\psi \in X(G)$ for which the image of x in $(M \otimes_{\mathbb{Z}} \mathbb{Q})_\psi$ is non-zero satisfy $\psi \mid \chi$ and $\psi \neq \chi$. It follows that $\Psi_n(g)x = 0$ because Ψ_n is the product of all Φ_m where m strictly divides n.

It follows from (4.1) that the polynomials $\Psi_n/(X^{n/p} - 1)$ generate the unit ideal in $\mathbb{Z}[X]$. By writing 1 as a $\mathbb{Z}[X]$-linear combination of these polynomials, and substituting g for X, we see that the element x is a sum of elements of M^H each annihilated by $g^{n/p} - 1$ for some $p \mid n$, in other words $x \in \sum_{H'} M^{H'}$. □

Let A be the ring of integers in a number field K. For an $A[G]$-lattice M, we define M_{cyc} as $\sum_H M^H$, where H ranges over all subgroups of G with G/H cyclic. The following generalizes the argument of [14, §4.1].

(4.4) Lemma (Gillard). *If $N \subset M$ are $A[G]$-lattices with $M \otimes_A K = N \otimes_A K$, then*

$$[M_{\mathrm{cyc}} : N_{\mathrm{cyc}}]_A = \prod_{\chi \in X(G)} [M(\chi) : N(\chi)]_A.$$

Proof. In this proof we will write M^χ for M^{H_χ}. For a subset S of $X(G)$ we denote $\sum_{\chi\in S} M^\chi$ by M^S. We claim that for every subset S of $X(G)$ for which $\chi \in S$ whenever $\chi \mid \psi$ and $\psi \in S$, we have

$$[M^S : N^S]_A = \prod_{\chi\in S} [M(\chi) : N(\chi)]_A.$$

Taking $S = X(G)$ the proposition then follows.

We prove this claim by induction to $\#S$. If S is empty there is nothing to prove. Assume S is non-empty and choose a maximal element $\chi \in S$, so that there is no $\psi \in S$ with $\chi \mid \psi$ and $\chi \neq \psi$. Then $S' = S - \{\chi\}$ satisfies the condition of our claim, and

$$[M^S : N^S]_A = [M^{S'} + M^\chi : N^\chi + M^{S'}]_A [N^\chi + M^{S'} : N^\chi + N^{S'}]_A =$$

$$[M^\chi : N^\chi + (M^\chi \cap M^{S'})]_A [M^{S'} : N^{S'} + (N^\chi \cap M^{S'})]_A$$

By (4.3) the intersection $M^\chi \cap M^{S'}$ is the kernel of the map $M^\chi \to M(\chi)$. Furthermore, $N^\chi \cap M^{S'}$ maps to zero in $N(\chi)$, so by (4.3) it is contained in the sum of all N^ψ with $\psi \mid \chi$ and $\psi \neq \chi$, which in turn lies in $N^{S'}$ by maximality of χ. It follows that

$$[M^S : N^S]_A = [M(\chi) : N(\chi)]_A [M^{S'} : N^{S'}]_A.$$

Applying the induction hypothesis for S', we get the desired formula for S. □

(4.5) Remark. It follows from (4.4) that for two factor equivalent $\mathbb{Z}[G]$-lattices $N \subset M$ the map $g : R(G) \to I(\mathbb{Q})$ defined by $g(1_H^G) = [M^H : N^H]$ sends an irreducible rational character χ to $[M(\chi) : N(\chi)]$. As $M(\chi)/N(\chi)$ is a finite $\mathbb{Z}[\zeta_{n_\chi}]$-module, it follows that $g(\chi)$ is a norm of an ideal of $\mathbb{Q}(\zeta_{n_\chi})$. This implies that the notion of "$\mathbb{Q}$-factor equivalence" in [2; 12; 13] is in fact the same as factor equivalence.

(4.6) Corollary (Burns [2, §1]). *The lattices M and N are factor equivalent if and only if for all subgroups H of G one has*

$$[M^H : (M^H)_{\mathrm{cyc}}]_A = [N^H : (N^H)_{\mathrm{cyc}}]_A.$$

Proof. We know from (4.4) that $[(M^H)_{\mathrm{cyc}} : (N^H)_{\mathrm{cyc}}]_A$ is a factorizable function of H, so M and N are factor equivalent if and only if

$$H \mapsto \frac{[M^H : (M^H)_{\mathrm{cyc}}]_A}{[N^H : (N^H)_{\mathrm{cyc}}]_A}$$

is factorizable. Since $M^H = (M^H)_{\mathrm{cyc}}$ if H is cocyclic, (4.2) implies that the latter function is factorizable if and only if it is identically 1. □

(4.7) Theorem. *If $K \subset L$ is a Galois extension of number fields with abelian Galois group G and rings of integers $A \subset B$, then $[B : B_{\mathrm{cyc}}]_A = [\mathbb{Z}[G] : \mathbb{Z}[G]_{\mathrm{cyc}}] \cdot A$.*

For $\chi \in X(G)$, let D_χ be the absolute value of the discriminant of $F_\chi = \mathbb{Q}(\zeta_{n_\chi})$ over $\mathbb{Q}$, and let φ be the Euler phi-function. Then one has:

$$[\mathbb{Z}[G] : \mathbb{Z}[G]_{\mathrm{cyc}}] = n^{-n/2} \prod_{\chi \in X(G)} (n/n_\chi)^{\varphi(n_\chi)} D_\chi^{1/2}.$$

Proof. The first statement follows from (3.2) and (4.6).

Under the isomorphism $\mathbb{Q}[G] \cong \prod F_\chi$, the ring $N = \mathbb{Z}[G]$ maps into the product M of the rings of integers $\mathcal{O}_\chi \cong \mathbb{Z}[\zeta_{n_\chi}]$ of F_χ. We first compute $[M : N_{\mathrm{cyc}}]$ with (4.4), using that $M = M_{\mathrm{cyc}}$. If $\chi \in X(G)$, then $[M(\chi) : N(\chi)]$ is the index of the image of N^{H_χ} in $\mathcal{O}_\chi$. Note that N^{H_χ} is generated as an abelian group by the sums of elements in a fixed coset of G mod H_χ. Such a sum maps to $\#H_\chi \zeta$, for some root of unity ζ in $\mathcal{O}_\chi$, and as $\mathcal{O}_\chi$ is a free abelian group on $\varphi(n_\chi)$ of these roots of unity, it follows that $[M(\chi) : N(\chi)] = (n/n_\chi)^{\varphi(n_\chi)}$ and $[M : N_{\mathrm{cyc}}] = \prod_\chi (n/n_\chi)^{\varphi(n_\chi)}$.

In order to compute $[M : N]$, note that both $M = \prod \mathcal{O}_\chi$ and $N = \mathbb{Z}[G]$ are algebras over $\mathbb{Z}$, so that their index can be computed by calculating their discriminants. It is easy to see that $|\Delta(N/\mathbb{Z})| = n^n$, and we have $|\Delta(M/\mathbb{Z})| = \prod_\chi D_\chi$. The theorem now follows from $[M : N]^2 = |\Delta(N/\mathbb{Z})|/|\Delta(M/\mathbb{Z})|$, and $[N : N_{\mathrm{cyc}}] = [M : N_{\mathrm{cyc}}][M : N]^{-1}$. □

(4.8) Examples. If G is of exponent 2 and rank m, then the only occurring cyclotomic field is $\mathbb{Q}$. The theorem gives

$$[B : B_{\mathrm{cyc}}]_A = (2^m)^{-2^{m-1}} 2^m (2^{m-1})^{2^m - 1} \cdot A = 2^{(m-2)2^{m-1}+1} \cdot A.$$

This formula was first established by A. Fajardo [11].

If G is of type (p, p), for some prime number p, then there are $p+1$ cyclic quotients of order p, and one of order 1. Using that $|\Delta(\mathbb{Z}[\zeta_p]/\mathbb{Z})| = p^{p-2}$, we get

$$[B : B_{\mathrm{cyc}}]_A = p^{-p^2} \cdot p^2 \cdot (p^{p-1} p^{\frac{p-2}{2}})^{p+1} \cdot A = p^{\frac{p(p-1)}{2}} \cdot A.$$

The case $p = 3$ has been computed by Parry [20, lemma 5].

If G is an abelian p-group generated by two elements, then one can deduce from the formula for type (p, p), that there is no set of generators of B as an A-module, whose elements lie in extensions of K that are strictly contained in L. This confirms at least a special case of a numerical observation of H. Cohen and of H. W. Lenstra, Jr., that a $\mathbb{Z}$-basis of a ring of integers always seems to contains a field generator over $\mathbb{Q}$ of the number field. See [8] for a more thorough discussion of this topic.

5. Class number relations and S-units.

Let $K \subset L$ be a Galois extension of number fields with Galois group G. Let μ_L be the group of roots of unity in L, and denote its order by $w(L)$. Let S be a finite G-stable set of primes of L, containing the infinite primes.

The S-class number $h_S(L)$ is defined as the class number of the ring consisting of all elements of L that are integral outside S. The S-units $U_S(L)$ of L are the elements of L that are units outside S. We now recall the definition of the S-regulator $R_S(L)$ as in Tate [27, chap. I]. By Dirichlet's unit theorem the logarithm map $U_S(L) \to \mathbb{R}^S$ given by $u \mapsto (\log ||u||_{\mathfrak{q}})_{\mathfrak{q}} \in \mathbb{R}^S$ embeds $U_S(L)/\mu_L$ as a cocompact lattice in the hyperplane of $\mathbb{R}^S$ with coordinate sum zero. If we choose a basis $\{u_i\}_i$ of $U_S(L)/\mu_L$ as a $\mathbb{Z}$-module, then the S-regulator $R_S(L)$ is defined as $|\det(\log ||u_i||_{\mathfrak{q}_j})_{ij}|$, where the $\mathfrak{q}_j$ are the primes of S, with one prime omitted. Here the normalization of the valuation at a prime $\mathfrak{q}$ of L lying over a prime $\mathfrak{p}$ of $\mathbb{Q}$, is given by $||u||_{\mathfrak{q}} = |\mathrm{N}_{L_{\mathfrak{q}}/\mathbb{Q}_p}(u)|_{\mathfrak{p}}$, where $|\cdot|_p$ is the usual valuation on the completion $\mathbb{Q}_p$ of $\mathbb{Q}$. Note that we also consider the infinite prime $p = \infty$ and $\mathbb{Q}_\infty = \mathbb{R}$.

For a subfield F of L, we denote the restriction of S to F by $S(F)$, but we will write $h_S(F)$ for $h_{S(F)}(F)$ and $R_S(F)$ for $R_{S(F)}(F)$.

(5.1) Theorem (Brauer). *The map $H \mapsto \frac{h_S(L^H)R_S(L^H)}{w(L^H)}$ is a factorizable function with values in $\mathbb{R}_{>0}$.*

Applying this theorem to the relations given in (2.2), we obtain the well-known class number formulas for biquadratic fields and for fields with Galois group S_3 over $\mathbb{Q}$.

Using zeta functions of number fields one can prove (5.1) as follows. Denote the S-zeta function of the number field L^H by $\zeta_{L^H,S}(s)$. The map $H \mapsto \zeta_{L^H,S}$ is factorizable, because $\zeta_{L^H,S}$ is equal to the Artin L-series $L(1_H^G, s)$, and we have $L_S(\chi_1 + \chi_2, s) = L_S(\chi_1, s)L_S(\chi_2, s)$ for any characters χ_1, χ_2 of G. Brauer [1] now looks at the residue of zeta functions at $s = 1$. Alternatively, one can use that the quotient in the theorem is the absolute value of the leading coefficient in the Taylor series expansion at $s = 0$ of $\zeta_{L^H,S}(s)$ (see Tate [27]). Since the leading coefficient of a product of Taylor series is the product of their leading coefficients, this implies (5.1).

In this section we show how (5.1) implies statements about the Galois module structure of $U_S(L)$. The group G acts on the set S, so it acts on the free abelian group $\mathbb{Z}[S]$ generated by S. Define the $\mathbb{Z}[G]$-lattice X_S by the short exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to X_S \to \mathbb{Z}[S] \to \mathbb{Z} \to 0,$$

where every $\mathfrak{q} \in S$ maps to $1 \in \mathbb{Z}$. The logarithm map $U_S(L) \to \mathbb{R}[S]$ in the definition

of the regulator is the composite map

$$U_S(L) \xrightarrow{\log_L} X_S \otimes_{\mathbb{Z}} \mathbb{R} \subset \mathbb{R}[S].$$

The map $\log_L$ provides an isomorphism of $\mathbb{R}[G]$-modules $U_S(L) \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} X_S \otimes_{\mathbb{Z}} \mathbb{R}$. It follows that $U_S(L) \otimes \mathbb{Q}$ and $X_S \otimes \mathbb{Q}$ are isomorphic $\mathbb{Q}[G]$-modules (see e.g. [4, p. 110]). In particular, there exists a $\mathbb{Z}[G]$-linear embedding $i : X_S \to U_S(L)$.

Let H be a subgroup of G. For $\mathfrak{p} \in S(L^H)$ let $n_{\mathfrak{p}}$ denote the local degree of $\mathfrak{p}$ in the extension $L^H \subset L$ by $n_{\mathfrak{p}}$. Let $n(H)$ be the product of all $n_{\mathfrak{p}}$ with $\mathfrak{p} \in S(L^H)$, and let $l(H)$ be the least common multiple of the same collection of $n_{\mathfrak{p}}$.

(5.2) Theorem. *For any $\mathbb{Z}[G]$-linear embedding $i : X_S \rightarrowtail U_S(L)$, the function*

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

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

Proof. For $\mathbb{Z}$-lattices L_1, L_2 spanning the same real vector space V we define $[L_2 : L_1] \in \mathbb{R}_{>0}$ 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 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 $\mathbb{R}$-linear automorphism φ of V we have $[L_1 : \varphi(L_1)] = |\det \varphi|$.

The composite map

$$X_S \xrightarrow{i} U_S(L) \xrightarrow{\log_L} X_S \otimes_{\mathbb{Z}} \mathbb{R}$$

induces an $\mathbb{R}[G]$-automorphism φ of $X_S \otimes_{\mathbb{Z}} \mathbb{R}$. We have $R_S(L) = [X_S : \log_L U_S(L)]$ and therefore $|\det \varphi| = R_S(L)[\log_L U_S(L) : \log_L i(X_S)]$ so that

$$\frac{[U_S(L) : i(X_S)]}{h_S(L)} = |\det \varphi| \frac{w(L)}{h_S(L) R_S(L)}. \tag{5.3}$$

It is the idea to obtain a formula similar to (5.3) for the H-invariants of X rather than X itself, and that the right-hand side should then be factorizable by (2.10) and (5.1).

We have an injective map $\mathbb{Z}[S(L^H)] \to \mathbb{Z}[S]$ sending $\mathfrak{p}$ to $\sum_{\mathfrak{q}|\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$. Thus $X_{S(L^H)}$ is identified with a subgroup of X_S^H, and the logarithm map is respected in the sense that we have a commutative diagram

$$\begin{array}{ccc} U_S(L^H) & \xrightarrow{\log_{L^H}} & X_{S(L^H)} \otimes_{\mathbb{Z}} \mathbb{R} \\ \downarrow & & \downarrow \\ U_S(L)^H & \xrightarrow{\log_L} & X_S^H \otimes_{\mathbb{Z}} \mathbb{R}. \end{array}$$

We therefore have

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

For any subgroup H of G we have

$$|d_\varphi(H)| = [X_S^H : \varphi(X_S^H)] = [X_S^H : \log_L U_S(L)^H][U_S(L)^H : i(X_S^H)]/w(L^H).$$

Combining these two, and dividing by $h_S(L^H)$ we get our version of (5.3) for H-invariants:

$$\frac{[U_S(L)^H : i(X_S)^H]}{h_S(L^H)}\ [X_S^H : X_{S(L^H)}] = |d_\varphi(H)|\ \frac{w(L^H)}{h_S(L^H)R_S(L^H)}. \tag{5.4}$$

The right hand side is factorizable by (2.10) and (5.1). To obtain the first statement of the theorem it remains to show that $n(H)/l(H) = [X_S^H : X_{S(L^H)}]$. First note that we have a commutative diagram with exact rows

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

The vertical maps are injective, and the cokernel C of the middle vertical map is the group $\bigoplus_{\mathfrak{p}\in S(L^H)} \mathbb{Z}/n_\mathfrak{p}\mathbb{Z}$, which has order $n(H)$. It is not hard to see that the image of C in the cokernel $\mathbb{Z}/n\mathbb{Z}$ of the rightmost vertical map has order $l(H)$. This shows the theorem. □

(5.5) Remark. One can shorten this proof somewhat by using results in Tate's book on the Stark-conjectures. Tate shows in [27, chap. II, 1.1] that the quantity on the left in (5.3) is the quotient $A(1, i)$ from the Stark-conjectures, where 1 is the trivial character of the trivial Galois group of L over L. Properties of $A(\chi, i)$, such as compatibility with inflation and additivity in χ, imply that the number on the left in (5.4) equals $A(1_H^G, i)$, and that it is a factorizable function of H.

(5.6) Remark. We only developed the notion of factor equivalence for torsion free G-modules. In order to say that (5.2) determines the factor equivalence class of $U_S(L)$ we should develop factor equivalence for modules with finite torsion. This can be done by replacing condition (ii) in (2.11) by the condition that the quotient of the order of cokernel and kernel of the map $M^H \to N^H$ should be factorizable. The reader may check that (2.12) can then be generalized for any j giving an isomorphism over K.

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

$$H \mapsto [\overline{U}(L)^H : i(X_S)^H] \, \frac{w(L^H)n(H)}{h_S(L^H)c(H)l(H)} \tag{5.7}$$

is factorizable. Thus we recover Fröhlich's statement [5, §3, theorem 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 $w(L^H) = 2$.

In the rest of this paper we seek to identify factors of the function in (5.2) which are factorizable themselves.

If S is totally split, then of course $n(H) = l(H) = 1$. In the case that S is the set of infinite primes then $l(H) = 1$ if no infinite primes ramify in L/L^H, and $l(H) = 2$ otherwise. For a complex V_4-extension of $\mathbb{Q}$ this already fails to be factorizable.

Our main tool is the following lemma, which is inspired on Brauer's proof [1, §2] that the odd part of $w(L^H)$ is factorizable. Kani and Rosen have formulated a result [17, prop. 4.7] which is easily seen to be equivalent.

(5.8) Lemma. *Let G be a group, D a subgroup of G and N a normal subgroup of D such that D/N is cyclic. For every integer $d \mid [D : N]$ and subgroup H of G, let $m_d(H) \in \mathbb{Z}$ 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 $\mathbb{Z}$-valued function of H.*

Proof. Let χ be a complex linear character of D that vanishes on N. Let n be the order of χ, 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 $n \mid d$. See [25, §7.2] for the notation $\langle \cdot, \cdot \rangle_G$. Clearly, $\langle \chi^G, 1_H^G \rangle_G$ is factorizable, and letting χ vary, we deduce our lemma by Möbius inversion.

By Frobenius reciprocity we have $\langle \chi^G, 1_H^G \rangle_G = \langle \chi, 1_H^G|_D \rangle_D$, which is equal to the $\mathbb{C}$-dimension of $\mathrm{Hom}_{\mathbb{C}[D]}(\mathbb{C}[G/H], \mathbb{C}_\chi)$, where $\mathbb{C}_\chi$ is $\mathbb{C}$ with the χ-action of D. Now $\mathbb{C}[G/H]$ is D-isomorphic to $\bigoplus_x \mathbb{C}[D/D_x]$, where x runs over the D-orbits of G/H, and D_x is a subgroup of D which is determined by x up to conjugation. It follows that $\langle \chi^G, 1_H^G \rangle_G$ is equal to the number of D-orbits x of G/H for which $\chi(D_x) = 1$. Now $\chi(D_x) = 1$ is equivalent to $\chi(ND_x) = 1$, which is the case if and only if the number of N-orbits of D/D_x is divisible by n. This proves the claim. □

(5.9) Roots of unity. Let p be a prime number, denote the p-part of w by w_p, and let K' be the field generated over K by the p-power roots of unity in L. Let $D = G$

and $N = \mathrm{Gal}(L/K')$ and suppose that G/N is cyclic. Then $w_p(L^H)$ is factorizable, because $w_p(L^H) = \prod_d w_p(K_d)^{m_d(H)}$, where d ranges over the divisors on $[D : N]$ and $K_d \subset K'$ is determined by $[K_d : K] = d$.

Note that D/N is a subgroup of $(\mathbb{Z}/w_p(L)\mathbb{Z})^*$, which is indeed cyclic if p is odd. Therefore, we may replace $w(L^H)$ by $w_2(L^H)$ in (5.2) and (5.7), and we may omit it altogether if the 2-power roots of unity in L generate a cyclic extension of K. An example where $w(L^H)$ is not factorizable is the extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$.

(5.10) Local degrees and residue degrees. Let $\mathfrak{p}$ be a prime of K and let D be the decomposition group of some extension $\mathfrak{q}$ of $\mathfrak{p}$ to L. If we take N to be the inertia group of $\mathfrak{q}$, then $m_d(H)$ is the number of primes of L^H lying over $\mathfrak{p}$ for which the residue degree in the extension L/L^H is d. It follows that the number of primes of L^H lying over $\mathfrak{p}$ with given residue degree, is factorizable. Kani and Rosen have shown a similar result in scheme theoretic context [17, cor. 4.8].

If D is cyclic then we can also take $N = 1$, so that $m_d(H)$ is the number of primes of L^H with local degree d in the extension L/L^H. For primes $\mathfrak{p}$ with cyclic decomposition group it follows that the number of primes of L^H lying over $\mathfrak{p}$ of given local degree, is factorizable.

One deduces that the factor $n(H)$ in (5.2) and (5.7) can be replaced by the factor $e(H)$, which is defined as follows: $e(H)$ is the product of the ramification indices in the extension L/L^H of those primes $\mathfrak{q} \in S(H)$ which 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.

References

1. R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. **4** (1951), 158–174.
2. D. Burns, *Factorisability, group lattices, and Galois module structure*, J. Algebra **134** (1990), 257–270.
3. D. Burns, *Canonical factorisability and a variant of Martinet's conjecture*, J. London. Math. Soc. (2) **44** (1991), 24–46.
4. J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Academic Press, London, 1967.
5. Ph. Cassou-Noguès, 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.
6. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York 1962.
7. N. G. de Bruijn, *On the factorization of cyclic groups*, Indag. Math. **15** (1953), 370–377.
8. B. de Smit, *Primitive elements in integral bases*, to appear.

10 B. de Smit and R. Perlis, *Zeta functions do not determine class numbers,* to appear in: Bull. Amer. Math. Soc. (NS) 1994.

11. A. Fajardo, private communication, May 1991.
12. A. Fröhlich, *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.

13. A. Fröhlich, *Module defect and factorisability*, Illinois J. Math. **32** (1988), 407–421.
14. R. Gillard, *Remarques sur les unités cyclotomiques et les unités elliptiques*, J. Number Theory **11** (1979), 21–48.
15. G. Gras, *Étude d'invariants relatifs aux groupes des classes des corps abéliens*, Astérisque **41**–**42** (1977), 35–53.
16. E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), 307–327.
17. E. Kani and M. Rosen, *Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties*, J. Number Theory **46** (1994), 230–254.
18. A. M. Nelson, *Monomial representations and Galois module structure*, Ph.D. thesis, King's College, University of London, 1979.
19. A. Pacheco, *A note on relations between the zeta-functions of Galois coverings over finite fields*, Canad. Math. Bull. **33** No. 3 (1990), 282–285.
20. C. Parry, *Bicyclic bicubic fields*, Canad. J. Math. **42** (1990) no. 3, 491–507.
21. R. Perlis, *On the class numbers of arithmetically equivalent fields*, J. Number Theory **10** (1978), 489–509.
22. L. Rédei, *Über das Kreisteilungspolynom*, Acta Math. Hungar. **5** (1954), 27–28.
23. J. Ritter and A. Weiss, *Galois action on integral representations*, J. London Math. Soc. (2) **46** (1992), 411–431.
24. J-P. Serre, *Local fields*, Graduate Texts in Math. **67**, Springer, New York, 1979.
25. J-P. Serre, *Linear representations of finite groups*, Graduate Texts in Math. **42**, Springer, New York, 1977.
26. D. Solomon, *Canonical factorisations in multiplicative Galois module structure*, J. Reine Angew. Math. **424** (1992), 181–217.
27. J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s=0*, Progr. Math. **47**, Birkhäuser, Boston, 1984.
28. C. D. Walter, *Brauer's class number relation*, Acta Arith. **35** (1979), 33–40; *Kuroda's class number relation*, Acta Arith. **35** (1979), 41–51.
29. E. Witt, *Collected papers*, Springer, to appear.

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

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