Journal de Théorie des Nombres
de Bordeaux **12** (2000), 209–218

The cyclic subfield integer index

par Bart de SMIT

Résumé. Dans cet article, nous nous intéressons à l'indice dans l'anneau des entiers d'une extension abélienne d'un corps de nombres K du sous-groupe engendré par les entiers contenus dans des sous-corps cycliques sur K. Cet indice est fini et ne dépend que du groupe de Galois et du degré de K. Nous en donnons une expression combinatoire. Lorsqu'on considère plus généralement des anneaux de Dedekind, des termes correctifs apparaissent, s'il y a une extension inséparable du corps résiduel. Nous explicitons ces termes dans le cas d'une extension abélienne de type (p, p).

Abstract. In this note we consider the index in the ring of integers of an abelian extension of a number field K of the additive subgroup generated by integers which lie in subfields that are cyclic over K. This index is finite, it only depends on the Galois group and the degree of K, and we give an explicit combinatorial formula for it. When generalizing to more general Dedekind domains, a correction term can be needed if there is an inseparable extension of residue fields. We identify this correction term for abelian extensions of type (p, p).

1. Introduction

We first give the main result in some special cases. Let A be the ring of integers in an abelian extension of $\mathbb{Q}$ of type (p, p), where p is a prime number. Then the additive subgroup generated by all integers in A with degree p over $\mathbb{Q}$ has index $p^{p(p-1)/2}$ in A. For $p = 2$ this seems to be well-known, and for $p = 3$ this has been shown by Parry [11, Lemma 5]. It was proved by A. Fajardo Mirón [6] that for a Galois extension of $\mathbb{Q}$ with abelian Galois group of order 2^k and exponent 2, the index in the ring of integers of the subgroup generated by quadratic integers is $2^{(k-2)2^{k-1}+1}$. In this paper we give such an explicit formula for any abelian extension of number fields, and we consider generalizations to more general abelian extensions of quotient fields of Dedekind domains.

Manuscrit reçu le 9 septembre 1999.
The author was supported by a fellowship from the Koninklijke Nederlandse Akademie van Wetenschappen.

In order to state the full result, we first introduce some notation. Let G be a finite abelian group of order n and let $\mathbb{Z}[G]$ be the group ring of G with coefficients in $\mathbb{Z}$. For any $\mathbb{Z}[G]$-module M we let M_{cyc} be the additive subgroup $\sum_H M^H$ of M, where H ranges over all subgroups of G for which G/H is cyclic, and M^H denotes the set of H-invariants of M. We let $c(G)$ be the index

$$c(G) = [\mathbb{Z}[G] : \mathbb{Z}[G]_{\mathrm{cyc}}].$$

We will first compute this integer explicitly.

Theorem 1. *Let $n = \prod_p p^{a_p}$ be the prime factorization of n and for $d \geq 1$ let $O_d(G)$ be the number of elements of G of exact order d. Then the prime factorization of $c(G)$ is given by*

$$c(G) = \prod_{p|n} p^{c_p} \quad \textit{with} \quad c_p = \frac{np^{-a_p}}{2}\Big(a_p p^{a_p} - \frac{p^{a_p}-1}{p-1} - \sum_{m\geq 1} m O_{p^m}(G)\Big).$$

It is easy to see that $c_p = 0$ if and only if the p-Sylow subgroup of G is cyclic.

Let A be a Dedekind domain and let B be its integral closure in a finite abelian extension of the quotient field of A with Galois group G. Then B is a Dedekind domain as well [13, Ch. I, §4, Prop. 8, 9] and B_{cyc} is the sub-A-module of B generated by all integers in B that generate a cyclic extension of the quotient field of A.

The results and arguments will depend strongly on the following condition, which may or may not hold:

(∗) *for all maximal ideals $\mathfrak{q}$ of B the $\mathfrak{q}$-adic completion of B is generated by a single element as a ring extension of the completion of A.*

The condition (∗) seems to be the natural condition under which the traditional results of ramification theory [13, Ch. III, IV] hold. It is satisfied if all residue field extensions of B over A are separable [13, Ch. III, §6, Prop. 12]. In particular, (∗) holds for rings of integers in number fields. It also holds when G is cyclic of prime order. One can show in general that condition (∗) is equivalent to the condition that the module of differentials $\Omega_{B/A}$, which is a B-module of finite length, is *cyclic* as a B-module, i.e., it can be generated as a B-module by a single element; see [3].

For an inclusion $M \subset N$ of finitely generated modules over a Dedekind domain A we let the A-*index* $[N : M]_A$ be the Fitting ideal of the A-module N/M. If N/M has finite length as an A-module, then we can write $N/M \cong A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_t$ for non-zero ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ of A, and $[N : M]_A$ is equal the A-ideal $\mathfrak{a}_1 \cdots \mathfrak{a}_t$. If N/M does not have finite length then $[N : M]_A = 0$. Note that the usual index of M in N is given by $[N : M] = [A : [N : M]_A]$.

Theorem 2. *Let A be a Dedekind domain and let B be its integral closure in a finite Galois extension of the quotient field of A with an abelian Galois group G. If condition $(*)$ holds, then we have*

$$[B : B_{\mathrm{cyc}}]_A = c(G) \cdot A.$$

In the number field case one can deduce Theorem 2 from the theorem of Fröhlich [7] that says that B is "factor equivalent" to the group ring $A[G]$, and a characterization of factor equivalence by Burns [1, Prop. (1)]. Conversely, the proof of Theorem 2 given below gives rise to an alternative approach to Fröhlich's result; see [4]. See [5] for applications in a slightly different context.

The situation is much more cumbersome if condition $(*)$ does not hold. It was shown in [3] that in the case that G is of type (p, p) there is a single B-ideal $\mathfrak{d}$ which can be used to extend some ramification theoretic results, notably [13, Ch. IV, §1, Prop. 3, 4], to the case where $(*)$ does not hold. This ideal $\mathfrak{d}$ measures the degree to which $\Omega_{B/A}$ is non-cyclic. It is given by $\mathfrak{d} = \mathrm{Fit}_B(\Omega^2_{B/A})$ and it is the smallest B-ideal for which there exists a B-module epimorphism $\Omega_{B/A} \to B/\mathfrak{d} \times B/\mathfrak{d}$.

Theorem 3. *Let A be a Dedekind domain and let B be its integral closure in a Galois extension of the quotient field of A with an abelian Galois group G of type (p, p) for some prime number p. Then we have*

$$[B : B_{\mathrm{cyc}}]_A \cdot B = c(G) \cdot \mathfrak{d}^{p(1-p)/2} = (pB/\mathfrak{d})^{p(p-1)/2}.$$

The proofs of the Theorems are given in Section 3. They use some general properties of modules over abelian groups which are given in the next section.

2. Modules over abelian groups and the lemma of De Bruijn-Rédei

For a positive integer m we let $\Phi_m \in \mathbb{Z}[X]$ be the mth cyclotomic polynomial. We will need a basic lemma about these polynomials, which was first stated by Rédei [12] and proved by De Bruijn [2]. Gillard [8] and Gras [9] attribute it to Martinet. We include a different proof for completeness.

We first introduce some notation from [10, §2] that will be used throughout the paper. If C is a cyclic group of order m, then the $\mathbb{Q}$-algebra $\mathbb{Q}(C)$ will be the quotient of the group ring $\mathbb{Q}[C]$ by the ideal generated by $\Phi_m(g)$ with g a generator of C. Note that this ideal does not depend on the choice of g and that $\mathbb{Q}(C)$ is isomorphic to the field of mth roots of unity.

Lemma 4 (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 $\Phi_n(X)$.*

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 every $m \geq 1$ 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 the cyclotomic field $\mathbb{Q}(C_n)$. It suffices to show that $\mathbb{Z}[C_n]/I_n$ is a torsion free abelian group because it then follows that I_n is the kernel of the map $\mathbb{Z}[C_n] \to \mathbb{Q}(C_n)$.

If n is a prime power then this is trivial. We proceed by induction on the number of prime factors of n. Suppose $n = mk$ with m and k coprime and smaller than n. 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 $\mathbb{Z}[C_n]/I_n \cong (\mathbb{Z}[C_m]/I_m) \otimes (\mathbb{Z}[C_k]/I_k)$, which is torsion free, because by the induction hypothesis it is a tensor product of torsion free abelian groups. □

Let G be a finite abelian group, and let $\mathcal{C}$ be the set of cyclic quotients of G. The canonical maps $\mathbb{Q}[G] \to \mathbb{Q}(\rho)$ for $\rho \in \mathcal{C}$ give rise to a canonical isomorphism of $\mathbb{Q}$-algebras:

$$\mathbb{Q}[G] \xrightarrow{\sim} \prod_{\rho \in \mathcal{C}} \mathbb{Q}(\rho).$$

See [10, §2] for a short proof. It follows that every $\mathbb{Q}[G]$-module V decomposes as a product $V = \prod_\rho V^{(\rho)}$, where $V^{(\rho)} = V \otimes_{\mathbb{Q}[G]} \mathbb{Q}(\rho)$.

For any $\mathbb{Z}[G]$-module M and $\rho = G/H \in \mathcal{C}$ we let $M_\rho = M^H$ be the submodule of H-invariants of M. For a $\mathbb{Q}[G]$-module V we have $V_\rho = \prod_{\sigma \leq \rho} V^{(\sigma)}$, where the partial order on $\mathcal{C}$ is defined by $G/H' \leq G/H \iff H \subset H'$. Note that for $v \in V$ we have $v \in V^{(\rho)}$ if and only if $v \in V_\rho$ and $\Phi_{\#\rho}(g)m = 0$ for some generator g of ρ.

Now let M be a $\mathbb{Z}[G]$-module which is torsion free as an abelian group. Viewing M as a subgroup of the $\mathbb{Q}[G]$-module $M \otimes \mathbb{Q} = \prod_{\rho \in \mathcal{C}} (M \otimes \mathbb{Q})^{(\rho)}$, we let $M^{(\rho)}$ be the image of M_ρ under the projection on the factor $(M \otimes \mathbb{Q})^{(\rho)}$.

Lemma 5. *The kernel of the projection map $M_\rho \xrightarrow{\pi} M^{(\rho)}$ is $\sum_{\sigma < \rho} M_\sigma$.*

Proof. Note that $\mathrm{Ker}(\pi) = M_\rho \cap \prod_{\sigma < \rho} (M \otimes \mathbb{Q})^{(\sigma)}$. The inclusion $\sum_{\sigma < \rho} M_\sigma \subset \mathrm{Ker}(\pi)$ is clear. Suppose g is a generator of ρ and let $m = \#\rho$. Put $\Psi_m = (X^m - 1)/\Phi_m = \prod_{\sigma < \rho} \Phi_{\#\sigma}$. Since $(M \otimes_{\mathbb{Z}} \mathbb{Q})^{(\sigma)}$ is annihilated by $\Phi_{\#\sigma}(g)$ for every $\sigma < \rho$, we have $\Psi_m(g)x = 0$ for all $x \in \mathrm{Ker}(\pi)$.

By the previous lemma, the polynomials $P_p = \Psi_m/(X^{m/p} - 1)$, with p a prime divisor of m, generate the unit ideal in $\mathbb{Z}[X]$. By writing $1 = \sum_{p|m} Q_p$ in $\mathbb{Z}[X]$ with $Q_p \in P_p\mathbb{Z}[X]$, we see that every $x \in \operatorname{Ker}(\pi)$ can be written as $x = \sum_{p|m} x_p$ with $x_p = Q_p(g) \cdot x \in M_\rho$. Using that $\Psi_m(g)x = 0$ one sees that $g^{m/p}$ fixes x_p, so that $x \in \sum_{\sigma<\rho} M_\sigma$. □

In the next lemma we follow an argument that Gillard [8, §4] gives in the context of cyclotomic units.

Lemma 6. *Let A be a Dedekind domain of characteristic 0, and let $N \subset M$ be an inclusion of finitely generated $A[G]$-modules, which are torsion free as A-modules. If $[M : N]_A \neq 0$ then*

$$[M_{\mathrm{cyc}} : N_{\mathrm{cyc}}]_A = \prod_{\rho\in\mathcal{C}} [M^{(\rho)} : N^{(\rho)}]_A.$$

Proof. For a subset $\mathcal{D}$ of $\mathcal{C}$, denote $\sum_{\sigma\in\mathcal{D}} M_\sigma$ by $M_{\mathcal{D}}$. We claim that for every subset $\mathcal{D}$ of $\mathcal{C}$, for which $\sigma \in \mathcal{D}$ whenever $\sigma < \rho$ and $\rho \in \mathcal{D}$, we have

$$[M_{\mathcal{D}} : N_{\mathcal{D}}]_A = \prod_{\rho\in\mathcal{D}} [M^{(\rho)} : N^{(\rho)}]_A.$$

Taking $\mathcal{D} = \mathcal{C}$ the Lemma will follow. We prove this claim by induction to $\#\mathcal{D}$. If $\mathcal{D}$ is empty, then there is nothing to prove. Assume $\mathcal{D}$ is non-empty, choose a maximal element $\rho \in \mathcal{D}$, and put $\mathcal{E} = \mathcal{D}\backslash\{\rho\}$. It is clear that $M_{\mathcal{E}}$ is contained in $M_{\mathcal{D}} \cap (M\otimes\mathbb{Q})_{\mathcal{E}}$, which in turn lies in the kernel of the projection map $M_{\mathcal{D}} \xrightarrow{\pi} (M\otimes\mathbb{Q})^{(\rho)}$. This implies that $\pi(M_{\mathcal{D}}) = \pi(M_\rho) = M^{(\rho)}$. By Lemma 5 one sees that the kernel of π is equal to $M_{\mathcal{E}}$. By applying the same argument to N one gets a diagram with exact rows in which the vertical maps are injective:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N_{\mathcal{E}} & \longrightarrow & N_{\mathcal{D}} & \longrightarrow & N^{(\rho)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_{\mathcal{E}} & \longrightarrow & M_{\mathcal{D}} & \longrightarrow & M^{(\rho)} & \longrightarrow & 0.
\end{array}$$

By the snake lemma we get a short exact sequence of the cokernels of the vertical maps. Over a Dedekind domain, taking the Fitting ideal of a module of finite length is multiplicative over short exact sequences, so it follows that

$$[M_{\mathcal{D}} : N_{\mathcal{D}}]_A = [M_{\mathcal{E}} : N_{\mathcal{E}}]_A [M^{(\rho)} : N^{(\rho)}]_A.$$

This completes the induction step. □

3. Discriminants and conductors

Let A be a Dedekind domain and let B be a commutative A-algebra which is finitely generated and free as an A-module, with basis $\omega_1, \dots, \omega_n$. The discriminant $\Delta_{B/A}$ is the A-ideal generated by $\det(\mathrm{Tr}_{B/A}(\omega_i\omega_j)_{i,j})$, where $\mathrm{Tr}_{B/A}(x)$ is the trace of the matrix (a_{ij}) with coefficients in A defined by $x\omega_i = \sum_j a_{ij}\omega_j$. If B' is a sub-A-algebra which is also free as an A-module of rank n, then $\Delta_{B'/A} = [B : B']_A^2 \Delta_{B/A}$. When $A = \mathbb{Z}$ we often identify a $\mathbb{Z}$-ideal such as a discriminant or an A-index with its unique positive generator. By the discriminant $\Delta(K)$ of a number field K one means the discriminant of its ring of integers as a $\mathbb{Z}$-algebra, and the absolute discriminant of K is the real number $\Delta(K)^{1/d}$, where d is the degree of K.

Proof of Theorem 1. We identify $\mathbb{Q}[G]$ with $\prod_\rho \mathbb{Q}(\rho)$, so that the ring $N = \mathbb{Z}[G]$ becomes a subring of the product $M = \prod_\rho \mathbb{Z}(\rho)$ of the rings of integers in $\mathbb{Q}(\rho)$. We have $c(G) = [N : N_{\mathrm{cyc}}]$ and $M = M_{\mathrm{cyc}}$, so with Lemma 6 we get

$$c(G) = \frac{1}{[M : N]} \cdot [M_{\mathrm{cyc}} : N_{\mathrm{cyc}}] = \frac{\Delta_{M/\mathbb{Z}}^{1/2}}{\Delta_{N/\mathbb{Z}}^{1/2}} \cdot \prod_{\rho \in \mathcal{C}} [M^{(\rho)} : N^{(\rho)}].$$

We have $\Delta_{N/\mathbb{Z}} = n^n$ and $\Delta_{M/\mathbb{Z}} = \prod_\rho \Delta_{\mathbb{Z}(\rho)/\mathbb{Z}}$. If $\rho = G/H$ then $N_\rho = \mathbb{Z}[G]^H$ is generated as an abelian group by $\{S_x\colon\ x \in G/H\}$, where S_x is the formal sum of all elements in the coset x of G mod H. Under the projection map, such a sum S_x is mapped to the element $(\#H)x$ of $M^{(\rho)} = \mathbb{Z}(\rho)$, so $N^{(\rho)} = (\#H)M^{(\rho)}$. The $\mathbb{Z}$-rank of $M^{(\rho)}$ is $\varphi(\#\rho)$, where φ is the Euler phi-function. One deduces that $[M^{(\rho)} : N^{(\rho)}] = (n/\#\rho)^{\varphi(\#\rho)}$, so that

$$c(G) = n^{-n/2} \prod_{\rho \in \mathcal{C}} (n/\#\rho)^{\varphi(\#\rho)} \Delta_{\mathbb{Z}(\rho)/\mathbb{Z}}^{1/2}.$$

By duality of finite abelian groups, G has the same number of cyclic subgroups as cyclic quotients of each order. Using the fact that the mth cyclotomic field has degree $\varphi(m)$ and that a cyclic subgroup of order m is generated by exactly $\varphi(m)$ of its elements, we get

$$c(G) = n^{n/2} \prod_{g \in G} \frac{d(\mathrm{ord}(g))^{1/2}}{\mathrm{ord}(g)},$$

where $\mathrm{ord}(g)$ is the order of the cyclic group generated by g, and $d(m)$ denotes the absolute discriminant of the mth cyclotomic field.

Next, one remarks that for two abelian groups G_1 and G_2 of *coprime* order n_1 and n_2 one has $c(G_1 \times G_2) = c(G_1)^{n_2} c(G_2)^{n_1}$, and that one has the corresponding identity for the other side of the equality in Theorem 1. We may therefore assume that n is a power of a prime number p. With the formula $d(p^m) = p^{m-\frac{1}{p-1}}$ for $m \geq 1$ (see e.g. [14, Prop. 2.1]) the formula in Theorem 1 now follows easily. $\square$

Proof of Theorem 2. Let A and B be as in Theorem 2. Note first that $A[G]_{\mathrm{cyc}} = A \cdot \mathbb{Z}[G]_{\mathrm{cyc}}$, which in turn implies that $[A[G] : A[G]_{\mathrm{cyc}}]_A = c(G) \cdot A$.

Let us start with the easy case that A has positive characteristic p. If $p \nmid c(G)$ then $A[G] = A[G]_{\mathrm{cyc}}$ and $B = A[G]_{\mathrm{cyc}} \cdot B \subset B_{\mathrm{cyc}}$, so $B = B_{\mathrm{cyc}}$ and we are done. Now suppose that $p \mid c(G)$. By the normal basis theorem we can choose an $A[G]$-module injection $\varphi\colon\ A[G] \to B$. Let us also choose a non-zero element $x \in A$ so that xB is contained in the image of φ. Then we have inclusions

$$xB_{\mathrm{cyc}} = (xB)_{\mathrm{cyc}} \subset \varphi(A[G]_{\mathrm{cyc}}) \subset \varphi(A[G]) \subset B$$

and since $[A[G] : A[G]_{\mathrm{cyc}}]_A = 0$ it follows that $[B : xB_{\mathrm{cyc}}]_A = 0$. But we have $[B_{\mathrm{cyc}} : xB_{\mathrm{cyc}}]_A \neq 0$, and therefore $[B : B_{\mathrm{cyc}}]_A = 0 = c(G) \cdot A$.

Now assume that A has characteristic zero and let n be the A-rank of B. Let K and L be the quotient fields of A and B. The relative discriminant $\Delta_{B/A}$ can be defined as the A-ideal generated by all determinants $\det(\mathrm{Tr}_{L/K}(\omega_i\omega_j)_{i,j=1}^n)$ where $(\omega_i)_{i=1}^n$ ranges over all sequences of length n in B. It is a non-zero ideal of A. By induction to the cardinality of ρ we can define for each $\rho \in \mathcal{C}$ an A-ideal $\mathfrak{f}(\rho)$, called the *conductor* of ρ, such that

$$(**) \qquad \Delta_{B_\rho/A} = \prod_{\sigma \leq \rho} \mathfrak{f}(\sigma).$$

We can write down this definition in one stroke by Möbius inversion:

$$\mathfrak{f}(\rho) = \prod_{\sigma \leq \rho} \Delta_{B_\sigma/A}^{\mu(\#\rho/\#\sigma)},$$

where μ is the Möbius function. The *conductor discriminant product formula* now says the following.

Lemma 7. *If condition* $(*)$ *holds, then* $\Delta_{B/A} = \prod_{\rho \in \mathcal{C}} \mathfrak{f}(\rho)$.

Proof. For $g \in G$ let $\mathfrak{a}_g$ be the A-ideal which is the norm of the B-ideal generated by all $x - gx$ with x in B. For any subgroup H of G Hilbert's formula and transitivity of the different imply that

$$\Delta_{B^H/A}^{\#G} = \prod_{\substack{g \in G \\ g \notin H}} \mathfrak{a}_g^{[G:H]} = \prod_{g \in G} \mathfrak{a}_g^{\mathrm{Tr}(1-g|\mathbb{Q}[G/H])},$$

where $\mathrm{Tr}(x|V)$ denotes the trace of the action of an element x on a $\mathbb{Q}$-vector space V. For each $\rho \in \mathcal{C}$ we deduce that

$$\mathfrak{f}(\rho)^{\#G} = \prod_{g\in G} \mathfrak{a}_g^{\mathrm{Tr}(1-g|\mathbb{Q}(\rho))}.$$

The lemma now follows from the $\mathbb{Q}[G]$-module isomorphism $\mathbb{Q}[G] \cong \prod \mathbb{Q}(\rho)$. □

We continue the proof of Theorem 2. Consider the tensor product $N = B\otimes_A B$ as a module over the commutative ring $M = B[G]$ by letting B act on the left factor and G on the right factor. For every subgroup H of G we have $N^H = B\otimes_A(B^H)$ and $M^H = B\otimes_A(A[G]^H)$. This implies that $N_{\mathrm{cyc}} = B\otimes_A(B_{\mathrm{cyc}})$ and $M_{\mathrm{cyc}} = B\otimes_A(A[G]_{\mathrm{cyc}})$, so that $[N : N_{\mathrm{cyc}}]_B = [B : B_{\mathrm{cyc}}]_A \cdot B$ and $[M : M_{\mathrm{cyc}}]_B = c(G)\cdot B$. Since the canonical map from the ideal group of A to the ideal group of B is injective, it suffices to show that $[N : N_{\mathrm{cyc}}]_B = [M : M_{\mathrm{cyc}}]_B$.

The advantage of this base change to B-coefficients is that we now have a canonical $B[G]$-linear map

$$\varphi\colon\ N \to M, \qquad x\otimes y \mapsto \sum_{\sigma\in G} x\sigma(y)\cdot\sigma^{-1}.$$

For every subgroup H of G we claim that $[M^H : \varphi(N^H)]_B^2 = \Delta_{B^H/A}\cdot B$. To see this, let $\mathfrak{p}$ be a prime of A, let $A_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of A, put $B_\mathfrak{p} = A_\mathfrak{p}\otimes_A B$, and choose a basis $\omega_1,\dots,\omega_n$ of $A_\mathfrak{p}\otimes_A B^H$ over $A_\mathfrak{p}$. The $B_\mathfrak{p}$-linear map $B_\mathfrak{p}\otimes_B N^H \longrightarrow B_\mathfrak{p}\otimes_B M^H$ induced by φ is then given by the matrix $U = (\sigma_i(\omega_j))_{ij}$, where $\{\sigma_1,\dots,\sigma_n\} = G/H$. On the one hand, it follows that $\det(U)$ is the $\mathfrak{p}$-part of $[M^H : \varphi(N^H)]_B$. But on the other hand, it is well known that $\det(U)^2$ is the $\mathfrak{p}$-part of the discriminant of B^H over A; see [13, Ch. III, §3, 4]. This proves the claim.

For each $\rho\in\mathcal{C}$ we now get two product expansions of $[M_\rho : \varphi(N_\rho)]_B^2$: one from our definition $(**)$ of the conductor and one from Lemma 6 applied to the ρ-action on M_ρ. By induction to the size of ρ (or Möbius inversion) it follows that $[M^{(\rho)} : \varphi(N^{(\rho)})]_B^2 = \mathfrak{f}(\rho)\cdot B$ for all $\rho\in\mathcal{C}$. By Lemma 6, applied now to the G-action on M, we therefore have $[M_{\mathrm{cyc}} : \varphi(N_{\mathrm{cyc}})]_B^2 = \prod_{\rho\in\mathcal{C}}\mathfrak{f}(\rho)$. One can summarize this with the following commutative diagram of injections of B-modules, where the labels of the arrows indicate the square of the B-index of the image

$$\begin{array}{ccc} N & \xrightarrow{\Delta_{B/A}} & M \\ \uparrow & & \uparrow{\scriptstyle c(G)^2} \\ N_{\mathrm{cyc}} & \xrightarrow{\prod \mathfrak{f}(\rho)} & M_{\mathrm{cyc}}. \end{array}$$

Now we use condition $(*)$ in order to invoke Lemma 7. We obtain

$$[M_{\mathrm{cyc}} : \varphi(N_{\mathrm{cyc}})]_B^2 = \prod_{\rho\in\mathcal{C}} \mathfrak{f}(\rho)\cdot B = \Delta_{B/A}\cdot B = [M : \varphi(N)]_B^2.$$

Since $\Delta_{B/A} \neq 0$ this implies that $[M : M_{\mathrm{cyc}}]_B = [N : N_{\mathrm{cyc}}]_B$. □

Proof of Theorem 3. Note first that indeed $c(G) = p^{p(p-1)/2}$ by Theorem 1, so that the second equality holds.

The case that A has positive characteristic is again easy: either $p = 0$ in A, in which case we saw already that $[B : B_{\mathrm{cyc}}]_A$ vanishes, or $p \neq 0$ in A, in which case B is tamely ramified over A so that condition $(*)$ holds and we have $\mathfrak{d} = B$.

Thus, we assume that A is of characteristic zero. For each maximal ideal $\mathfrak{q}$ of B we need to check that the $\mathfrak{q}$-parts of the two B-ideals are the same. Let $\mathfrak{p}$ be a maximal ideal of A. Suppose that condition $(*)$ holds for the primes $\mathfrak{q}$ of B extending $\mathfrak{p}$. Then the $\mathfrak{q}$-part of $\mathfrak{d}$ is trivial for these $\mathfrak{q}$, and by localization and Theorem 2 we are done. The case that $(*)$ fails for some $\mathfrak{q}$ extending $\mathfrak{p}$ remains. Since $(*)$ holds for extensions of degree 1 and p, this can only happen when the completion $B_{\mathfrak{q}}$ has rank p^2 over $A_{\mathfrak{p}}$, and p is the residue characteristic. For the remainder of the proof we may therefore assume that A and B are complete discrete valuation rings of residue characteristic p. For this case the results in [13, Ch. IV, §1] have been extended: by Theorem 2.2 of [3] and transitivity of the different we have

$$\mathfrak{r}\mathfrak{D}_{B/A} = \prod_{\substack{g\in G\\ g\neq 1}} ((1-g)(B)\cdot B) = \prod_{\substack{\rho\in\mathcal{C}\\ \rho\neq 1}} \mathfrak{D}_{B/B_\rho} = \mathfrak{D}_{B/A}^{p+1}\prod_{\rho\in\mathcal{C}} \mathfrak{D}_{B_\rho/A}^{-1}.$$

Here $\mathfrak{D}_{B/A}$ denotes the different of B over A, and the ideal $\mathfrak{r}$, according to Theorem 5.1 of [3], is given by $\mathfrak{r} = \mathfrak{d}^{p-1}$. Dividing by $\mathfrak{D}_{B/A}$ and raising both sides to the power p, we deduce with definition $(**)$ that

$$\mathfrak{d}^{p(p-1)} = \mathfrak{r}^p = \Delta_{B/A}\prod_{\rho\in\mathcal{C}} \mathfrak{f}(\rho)^{-1}\cdot B.$$

We now use the same diagram as in the previous proof and find

$$[B : B_{\mathrm{cyc}}]_A^2\cdot B = [N : N_{\mathrm{cyc}}]_B^2 = \frac{[M : N_{\mathrm{cyc}}]_B}{[M : N]_B} = \frac{c(G)^2\prod_\rho \mathfrak{f}(\rho)}{\Delta_{B/A}\cdot B} = \frac{c(G)^2\cdot B}{\mathfrak{d}^{p(p-1)}}.$$

This proves Theorem 3. □

Example. Let us take $p = 2$ and let A be a complete discrete valuation ring of characteristic zero, whose residue field is the field $\mathbb{F}_2(x, y)$ with x and y algebraically independent over $\mathbb{F}_2$. Lifting x and y to elements $\tilde{x}$ and $\tilde{y}$ of A, we now consider $B = A[\sqrt{\tilde{x}}, \sqrt{\tilde{y}}]$. Then B is Dekekind with an action of an abelian Galois group G of type $(2,2)$. We now have $B = B_{\mathrm{cyc}}$ and $c(G) \cdot B = 2B = \mathfrak{d} \neq B$.

References

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

[2] N. G. de Bruijn, *On the factorization of cyclic groups.* Indag. Math. (N.S.) **15** (1953), 370–377.

[3] B. de Smit, *The different and differentials for local fields with imperfect residue fields.* Proc. Edinburgh Math. Soc. (2) **40** (1997), 353–365.

[4] B. de Smit, *Factor equivalence results for integers and units.* Enseign. Math. (2) **42** (1996), 383–394.

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

[6] A. Fajardo Mirón, private communication, May 1991.

[7] 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.

[8] R. Gillard, *Remarques sur les unités cyclotomiques et les unités elliptiques.* J. Number Theory **11** (1979), 21–48.

[9] G. Gras, *Étude d'invariants relatifs aux groupes des classes des corps abéliens.* Astérisque **41**–**42** (1977), 35–53.

[10] H.W. Lenstra, Jr., *Grothendieck groups of abelian group rings.* J. Pure Appl. Algebra **20** (1981), 173–193.

[11] C. Parry, *Bicyclic bicubic fields.* Canad. J. Math. **42** (1990) no. 3, 491–507.

[12] L. Rédei, *Über das Kreisteilungspolynom.* Acta Math. Hungar. **5** (1954), 27–28.

[13] J.-P. Serre, *Local fields.* Springer-Verlag, New York, 1979.

[14] L. C. Washington, *Introduction to cyclotomic fields.* Springer-Verlag, New York, 1982.

Bart De Smit
Mathematisch Instituut
Universiteit Leiden
P.O. Box 9512, 2300 RA Leiden
The Netherlands
E-mail : desmit@math.leidenuniv.nl