To appear in: **Acta Arithmetica** 1994

Primitive elements in integral bases

Bart de Smit

Abstract. On the basis of numerical observations H. Cohen and H. W. Lenstra, Jr. have posed the following question: does a $\mathbb{Z}$-basis of a ring of integers in a number field necessarily contain a field generator of the number field? In this note it is shown that the answer is yes for all normal fields of prime power degree and for all fields whose degree is less than 12. For dihedral fields of degree 12 the answer is no. More generally, we consider the index in the ring of integers of the additive subgroup generated by integers from subfields. This index depends on subtle ramification phenomena, but one can give explicit formulas in certain cases by applying Fröhlich's theory of factor equivalence.

Key words: rings of integers, Galois module structure, factor equivalence.

1991 Mathematics subject classification: 11R04, 11R33.

1. Introduction

Main questions. Let L be a number field with ring of integers B. Recall that a primitive element of L is an element $x \in L$ with $L = \mathbb{Q}(x)$. In this paper we are concerned with the truth of the following statements.

(1.1) Every set of additive generators of B contains a primitive element of L.

(1.2) Every $\mathbb{Z}$-basis of B contains a primitive element of L.

Clearly, (1.1) implies (1.2). The question whether (1.1) is true was first raised by A. Fajardo Mirón and H. W. Lenstra, Jr. [5, sec. 8] when they were looking for ways to find equation orders of small index in a given ring of integers. Independently, H. Cohen observed in 1989 from numerical examples that (1.2) always seems to hold for fields of small degree. Cohen was looking for integral bases that are small in some sense, and one may wonder if these small basis elements can all lie in small number fields.

In section 2 we will show that (1.1) is true for Galois extensions of prime power degree, and for certain other classes of extensions as well. We will deduce (1.1) for all fields of degree less than 12.

It is not hard to see that (1.1) is false for any normal field whose Galois group is dihedral of order 12. In section 3 we prove the stronger result that (1.2) is false for such a field too.

Notation. Throughout this paper, $K \subset L$ denotes an extension of number fields with rings of integers $A \subset B$. We let $S_K(B)$ be the A-module generated by integers that are not primitive, i.e., generated by all $x \in B$ with $K(x) \neq L$. The *subfield integer*

index $s(L/K) \in \mathbb{Z}_{>0} \cup \{\infty\}$ is defined to be the index $[B : S_K(B)]$. Note that (1.1) is equivalent to $s(L/\mathbb{Q}) \neq 1$.

For a finite group G and $\mathbb{Z}[G]$-module M we let $S_G(M)$ be the additive subgroup of M generated by elements of M that are fixed by some non-trivial element of G. We put $s(G) = [\mathbb{Z}[G] : S_G(\mathbb{Z}[G])]$. If L/K is a Galois extension with Galois group G, then $S_K(B) = S_G(B)$. The exponent rather than the order of the quotient group $\mathbb{Z}[G]/S_G(\mathbb{Z}[G])$ is the invariant $\epsilon(G)$ that was introduced by W. Scharlau [11] and investigated further by J. S. Hsia, R. D. Peterson [8; 9], and S. Böge [1].

Index computations. Suppose L/K is a Galois extension with Galois group G. For tamely ramified extensions L/K we will show in section 4 that

$$s(L/K) = s(G)^{[K:\mathbb{Q}]}. \tag{1.3}$$

If G is abelian of type (p, p) then Fröhlich's theory of "factor equivalence" [7; 2] implies that (1.3) holds without conditions on ramification. For base field $K = \mathbb{Q}$ and abelian G of type $(p, p, \ldots, p)$, we also show that (1.3) holds and we compute $s(G)$. In general however, ramification does play a role. To show this we will construct an extension L/K of type $(2, 2, 2)$ for which (1.3) is false. The argument uses some easily computed Galois cohomology groups of rings of integers in quadratic extensions.

Acknowledgement. The author is grateful to S. Böge, H. W. Lenstra, Jr., and the referee for helpful comments.

2. Affirmative results

In this section we prove that $s(L/K) \neq 1$ for certain extensions L/K, including all extensions of degree less than 12. This implies that for these extensions any set of A-module generators of B contains a primitive element, which confirms (1.1) and (1.2).

(2.1) Proposition.

(i) *If there is a prime* $\mathfrak{q}$ *of* L *that is ramified over all intermediate fields* $L' \neq L$ *of* L/K *then* $s(L/K) \neq 1$.

(ii) *If* $[L : K]$ *is a power of a prime number* p *and there is a prime* $\mathfrak{q}$ *of* L *lying over* p *that is tamely ramified in the extension* L/K, *then* $s(L/K) \neq 1$.

Proof. We first show (i). Denote by $B_\mathfrak{q}$ and $\mathfrak{q}_\mathfrak{q}$ the valuation ring and the prime ideal of the completion $L_\mathfrak{q}$ of L at $\mathfrak{q}$. Let $B_\mathfrak{q}^{\mathrm{unr}}$ be the valuation ring of the maximal subfield of $L_\mathfrak{q}$ which is unramified over $K_\mathfrak{p}$, where $\mathfrak{p} = \mathfrak{q}|_K$. Then $S_K(B)$ lies in $B_\mathfrak{q}^{\mathrm{unr}} + \mathfrak{q}_\mathfrak{q}^2$, which does not contain B if $L \neq K$.

Now assume the conditions of (ii). According to Noether's theorem [3, p. 21; 6, p. 26] the local trace map $B_{\mathfrak{q}} \to A_{\mathfrak{p}}$ is surjective. We deduce that $\mathrm{Tr}_{L/K}(B) \not\subset \mathfrak{p}$. For $x \in B$ we have $\mathrm{Tr}_{L/K}(x) = d\,\mathrm{Tr}_{K(x)/K}(x)$, where $d = [L : K(x)]$. If $K(x) \neq L$ then $p \mid d$ and $\mathrm{Tr}_{L/K}(x) \in \mathfrak{p}$. This shows that $\mathrm{Tr}_{L/K}(S_K(B)) \subset \mathfrak{p}$, so that $S_K(B) \neq B$. $\square$

The proofs above suggests two distinct techniques to deal with the tamely ramified case and with the totally ramified case. In the next theorem a combination of the two arguments is used for extensions of prime power degree. We seem to need an additional condition which is satisfied in the case of a Galois extension.

(2.2) Theorem. *Suppose that $[L : K]$ is a power of a prime number p, and that there is a prime $\mathfrak{p}$ of K lying over p for which the maximal ramification index*

$$e = \sup\{e(\mathfrak{q}/\mathfrak{p}) : \mathfrak{q} \text{ prime of } L \text{ with } \mathfrak{q} \mid \mathfrak{p}\}$$

is a power of p as well. Then $s(L/K) \neq 1$.

Proof. Let F be an unramified extension of the local field $K_{\mathfrak{p}}$ such that $[F : K_{\mathfrak{p}}]$ is divisible by the residue degree $f(\mathfrak{q}/\mathfrak{p})$ of every extension $\mathfrak{q}$ of $\mathfrak{p}$ to L. We denote the valuation ring of F by R, and its maximal ideal by $\mathfrak{r}$. Since R is unramified over $A_{\mathfrak{p}}$, the ring $C = B \otimes_A R$ is a product of discrete valuation rings $C_{\mathfrak{m}}$, where $\mathfrak{m}$ ranges over the maximal ideals of C, and the quotient field of each $C_{\mathfrak{m}}$ is a totally ramified extension of F. The maximal occuring ramification index $e(\mathfrak{m}/\mathfrak{r})$ is e, and we let $\mathcal{P}$ be the set of those maximal ideals $\mathfrak{m}$ of C for which $e(\mathfrak{m}/\mathfrak{r}) = e$.

By case (ii) of (2.1) we may assume that $e > 1$. For $\mathfrak{m} \in \mathcal{P}$ we define $\varphi_{\mathfrak{m}}$ to be the composite map $C \to C/(R + \mathfrak{m}^2) = \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{r}/\mathfrak{r}^2$, where the last map sends $x \in \mathfrak{m}/\mathfrak{m}^2$ to $x^e \in \mathfrak{m}^e/\mathfrak{m}^{e+1} = \mathfrak{r}/\mathfrak{r}^2$. Since e is a power of p, the map $\varphi_{\mathfrak{m}}$ is a homomorphism. Define $\varphi : C \to \mathfrak{r}/\mathfrak{r}^2$ by $x \mapsto \sum_{\mathfrak{m}\in\mathcal{P}} \varphi_{\mathfrak{m}}(x)$. For $x \in B$ and $r \in R$ we have $\varphi(x \otimes r) = r^e\varphi(x)$, so if $\varphi(B)$ were zero, then $\varphi(C) = 0$, which is clearly absurd. It follows that $\varphi(B) \neq 0$. To prove the theorem it suffices to show that $\varphi(S_K(B)) = 0$.

Suppose that L' is an intermediate field of L/K with $L' \neq L$. Let B' be the ring of integers of L', and put $C' = B' \otimes_A R$. Then C' is a product of discrete valuation rings $C'_{\mathfrak{n}}$, with $\mathfrak{n}$ ranging over the set of maximal ideals of C'. Let $x \in B'$ and fix one such factor $C'_{\mathfrak{n}}$ of C'. We claim that $\sum_{\mathfrak{m}} \varphi_{\mathfrak{m}}(x) = 0$ if we sum over all $\mathfrak{m} \in \mathcal{P}$ with $\mathfrak{m} \mid \mathfrak{n}$, i.e., $\mathfrak{m} \cap C' = \mathfrak{n}$. By summing over $\mathfrak{n}$ one then deduces that $\varphi(x) = 0$. It remains to prove the claim.

First suppose that there is a prime $\mathfrak{m}_0 \in \mathcal{P}$ with $\mathfrak{m}_0 \mid \mathfrak{n}$ and $e(\mathfrak{m}_0/\mathfrak{n}) = 1$. Since $e(\mathfrak{n}/\mathfrak{r}) = e$ and $e \geq e(\mathfrak{m}/\mathfrak{r})$ for all maximal ideals $\mathfrak{m}$ of C, it follows that *every* $\mathfrak{m} \mid \mathfrak{n}$ satisfies $e(\mathfrak{m}/\mathfrak{n}) = 1$ and $\mathfrak{m} \in \mathcal{P}$. If we write $x = r + x_0$ with $r \in R$ and $x_0 \in \mathfrak{n}$, then all $\varphi_{\mathfrak{m}}(x)$ with $\mathfrak{m} \mid \mathfrak{n}$ are equal to $x_0^e \in \mathfrak{n}^e/\mathfrak{n}^{e+1} = \mathfrak{r}/\mathfrak{r}^2$. There are exactly $[L : L']$

extensions $\mathfrak{m}$ of $\mathfrak{n}$ to C, because C is a free C'-module of rank $[L : L']$ and all local degrees are 1. Since $[L : L']$ is a non-trivial power of p and p annihilates $\mathfrak{r}/\mathfrak{r}^2$, it follows that $\sum_{\mathfrak{m}|\mathfrak{n}} \varphi_{\mathfrak{m}}(x) = [L : L']\varphi_{\mathfrak{m}_0}(x) = 0$.

Now suppose that there is no such $\mathfrak{m}_0$. For every $\mathfrak{m} \in \mathcal{P}$ with $\mathfrak{m} \mid \mathfrak{n}$ of C we then have $e(\mathfrak{m}/\mathfrak{n}) > 1$, so that $C'_{\mathfrak{n}} \subset R + \mathfrak{m}^2$ and $\varphi_{\mathfrak{m}}(x) = 0$. This proves the claim. □

(2.3) Corollary. *If the Galois closure of L over K has prime power degree, then $s(L/K) \neq 1$.*

Proof. If $[L : K]$ is a power of a prime p, and $\mathfrak{p}$ is a prime of K lying over p, then the hypothesis implies that $e(\mathfrak{q}/\mathfrak{p})$ is a power of p for all primes $\mathfrak{q}$ of L with $\mathfrak{q} \mid \mathfrak{p}$. □

In the case that the Galois group is abelian of type (p, p) this corollary can also be deduced from Fröhlich's theory of factor equivalence; see (4.3).

(2.4) Corollary. *If $[L : K] = p^2$ for some prime number p, or $[L : K] = 8$, then $s(L/K) \neq 1$.*

Proof. First suppose $[L : K] = p^2$. Let $\mathfrak{p}$ be any prime of K lying over p and let e be as in (2.2). If $e > p$ then we are in case (i) of (2.1), and if $e < p$ then case (ii) of (2.1) applies. If $e = p$ then (2.2) finishes the argument.

Now suppose that $[L : K] = 8$. If e is odd or $e > 4$ then (2.1) gives the result. This only leaves the cases $e = 2$ and $e = 4$, which are instances of (2.2). □

(2.5) Proposition. *If the degree of L/K is $2p$ with p prime, then $s(L/K) \neq 1$.*

Proof. We can assume that p is odd and that $K \otimes_A S_K(B) = L$. We first show that L/K is Galois with dihedral Galois group. There is at most one intermediate field of degree 2 over K, because otherwise L would contain a biquadratic extension of K, so that $4 \mid [L : K]$. Since $K \otimes_A S_K(B) = L$ this implies that there are at least two intermediate fields L_1 and L_2 of degree p over K. Now L is Galois over L_1 and L_2, so it is Galois over $L_1 \cap L_2 = K$, and we denote the Galois group by G. Note that $L \neq S_G(L)$ if G is cyclic, so G must be dihedral. We first compute $s(G)$.

(2.6) Lemma. *If G is dihedral of order $2p$, with p prime, then $s(G) = p$.*

Proof. The group G can be presented as $G = \langle \sigma, \rho \mid \sigma^2 = \rho^p = 1; \sigma\rho = \rho^{-1}\sigma \rangle$. We claim that $S = S_G(\mathbb{Z}[G])$ is the kernel of the ring homomorphism $f\colon \mathbb{Z}[G] \to \mathbb{F}_p$ that maps ρ to 1 and σ to -1. Clearly, $S \subset \operatorname{Ker} f$. Note that $\sigma\rho^i \equiv -1 \bmod S$ and $\rho^i \equiv -\sigma\rho^i \equiv 1 \bmod S$. Since $1 + \rho + \cdots + \rho^{p-1} \in S$ this shows that $p \in S$, and the other inclusion follows. □

We continue the proof of (2.5). Let $\mathfrak{p}$ be a prime of K lying over p and let e be the ramification index of $\mathfrak{p}$ in L/K. Suppose e is coprime to p so that L/K is tamely

ramified at $\mathfrak{p}$. By Noether's theorem [6, pp. 26–28] there is a G-module isomorphism $B \otimes_A A_{\mathfrak{p}} \cong A_{\mathfrak{p}}[G]$, where $A_{\mathfrak{p}}$ is the completion of A at $\mathfrak{p}$. Since $p \mid \mathfrak{p}$ and $p \mid s(G)$ we have $A_{\mathfrak{p}}[G] \neq S_G(A_{\mathfrak{p}}[G])$, which implies that $B \neq S_G(B)$.

If $e = 2p$ we are done by (2.1), so the only case that remains is $e = p$. Then $\mathfrak{p}B = \mathfrak{a}^p$, where $\mathfrak{a}$ is a G-stable B-ideal, which is either a prime of degree 2 over $\mathfrak{p}$ or the product of two primes of degree 1. If we let $B' = B^{\langle\rho\rangle}$ then $B = B' + \mathfrak{a}$. Consider the canonical G-equivariant map $\varphi\colon B \to B/(B' + \mathfrak{a}^2) = \mathfrak{a}/\mathfrak{a}^2$. The image of G in $\mathrm{Aut}(\mathfrak{a}/\mathfrak{a}^2)$ is of order 2, so elements of B that are fixed by some element of G of order 2 are mapped to the G-invariant part of $\mathfrak{a}/\mathfrak{a}^2$. Together with the fact that $\varphi(B') = 0$, this implies that $\varphi(S_G(B)) \subset (\mathfrak{a}/\mathfrak{a}^2)^G$, which is strictly contained in $\mathfrak{a}/\mathfrak{a}^2$. It follows that $B \neq S_G(B)$ because φ is surjective. □

(2.7) Corollary. *If the degree of L over K is less than 12, then $s(L/K) \neq 1$.*

Proof. The statement is trivial if $[L : K]$ is prime, and (2.4) and (2.5) cover all other possibilities. □

3. Counterexamples

In this section we show that (1.1) and (1.2) are false for Galois extensions of $\mathbb{Q}$ with dihedral Galois group of order 12.

Assume that L/K is a Galois extension with Galois group G. First note that $s(L/K) < \infty$ if and only if $S_G(L) = L$. The normal basis theorem implies that L is isomorphic to $K[G]$ as a $K[G]$-module, so that $s(L/K) < \infty$ is equivalent to $S_G(K[G]) = K[G]$, which in turn is equivalent to $s(G) < \infty$. We mention two observations of Scharlau [11] in this context, which will not be needed in the sequel:

(i) $s(G)$ is finite if and only if G has no fixpoint-free complex representations;
(ii) if $s(G) < \infty$ then all primes dividing $s(G)$ divide the order of G.

Here we say that an action of G on a vector space V is fixpoint-free if $gv = v$ implies that $g = 1$ or $v = 0$.

We will use the fact that $s(G)$ is a finite power of p if G contains an abelian subgroup H of type (p, p). To see this, one notes the following identity between the elements $N_{H'} = \sum_{\sigma \in H'} \sigma \in \mathbb{Z}[G]$ for subgroups H' of H

$$p = -N_H + \sum_{H' \subset H} N_{H'}, \tag{3.1}$$

where H' runs over the $p + 1$ subgroups of H of order p.

(3.2) Proposition. *If $s(G) < \infty$ then $s(L/K) < \infty$ and all prime divisors of $s(L/K)$ divide $s(G)$. We have $s(L/K) = 1$ if $s(G) = 1$.*

Proof. Clearly the second statement is implied by the first. It is obvious that $S_G(\mathbb{Z}[G]) \cdot B \subset S_G(B)$. Since $s(G) \cdot 1 \in S_G(\mathbb{Z}[G])$ this shows that $s(G)B \subset S_G(B)$. The index $[B : s(G)B]$ is a power of $s(G)$, and this implies our statement. □

We can now make counterexamples to (1.1) by finding groups G with $s(G) = 1$. If G is abelian of type (6,6), then G contains both a subgroup of type (2,2) and a subgroup of type (3,3). This implies that $s(G)$ is both a power of 2 and of 3, so that $s(G) = 1$. It follows that (1.1) is false for abelian extensions of $\mathbb{Q}$ of type (6,6). The reader is invited to show that for abelian G we have $s(G) = 1$ if and only if G contains subgroups of type (p, p) and (q, q) for two distinct primes p and q.

An example of smaller degree is the dihedral group G of order 12. In this case G contains an abelian subgroup V_4 of type $(2, 2)$, and a subgroup isomorphic to S_3, the symmetric group of order 6. We already showed in (2.6) that $s(S_3) = 3$, and since $s(V_4) = 2$ we deduce again that $s(G) = 1$. We have thus shown that any dihedral extension of $\mathbb{Q}$ of degree 12 is a counterexample to (1.1).

It is not clear immediately whether (1.2) fails to hold for Galois extensions of $\mathbb{Q}$ for which the Galois group G satisfies $s(G) = 1$, because for that we would need to produce an integral basis, rather than a set of generators, consisting of elements of subfields. In the rest of this section we will show how to make such a basis in the dihedral case of degree 12.

(3.3) Lemma. *Let $F \subset E$ be an extension of number fields with rings of integers A_E and A_F. Then the quotient A_E/A_F is torsion free. If E is the composite of two extensions E_1 and E_2 of F of coprime degrees, then $A_E/(A_{E_1} + A_{E_2})$ is torsion free.*

Proof. If $x \in A_E$ satisfies $kx \in A_F$ for some $k \in \mathbb{Z}_{>0}$ then $x \in F \cap A_E = A_F$, which shows the first statement.

Let p be a prime number. To show that $A_E/(A_{E_1} + A_{E_2})$ has no p-torsion we suppose that $x \in A_E$ with $px \in A_{E_1} + A_{E_2}$ and we will show that $x \in A_{E_1} + A_{E_2}$. Assume that p does not divide $n = [E_1 : F] = [E : E_2]$ by switching E_1 and E_2 if necessary. Write $px = a_1 + a_2$ with $a_i \in A_{E_i}$, so that $\mathrm{Tr}_{E/E_2}(px) = \mathrm{Tr}_{E_1/F}(a_1) + na_2$. We have

$$na_2 = p\,\mathrm{Tr}_{E/E_2}(x) - \mathrm{Tr}_{E_1/F}(a_1) \in pA_{E_2} + A_F$$

and $p \nmid n$, so $a_2 \in pA_{E_2} + A_F$. Let $a_2 = a_2' + r$ with $a_2' \in pA_{E_2}$ and $r \in A_F$. Putting $a_1' = a_1 - r \in A_{E_1}$ we have $px = a_1' + a_2'$ and $a_1' \in A_{E_1} \cap pA_E$. We already know that A_E/A_{E_1} is torsion free, so $A_{E_1} \cap pA_E = pA_{E_1}$. This shows that both a_1' and a_2' are divisible by p, so that $x \in A_{E_1} + A_{E_2}$. □

(3.4) Proposition. *If L/K is a Galois extension whose Galois group is isomorphic to the dihedral group of order 12, then $s(L/K) = 1$. Furthermore, if the class number of K is one, then there is an integral basis not containing a field generator for L/K.*

Proof. We already showed the first statement. Suppose that the class number of K is 1, so that every finitely generated torsion free A-module is free. The Galois group can be presented as $\langle \sigma, \rho \mid \sigma^2 = \rho^6 = 1; \sigma\rho = \rho^{-1}\sigma \rangle$.

We now make an A-basis for B as follows. First take a basis of $B^{\langle \rho^2 \rangle}$, which consists of 4 elements. Since $B^{\langle \rho^3 \rangle}/B^{\langle \rho \rangle}$ is torsion free, we can find 4 elements of $B^{\langle \rho^3 \rangle}$ that give a basis for the quotient group, and we get a set of A-generators for $B^{\langle \rho^2 \rangle} + B^{\langle \rho^3 \rangle}$ of 8 elements. By (3.3), there are 2 elements of $B^{\langle \sigma \rangle}$ that generate $B^{\langle \sigma \rangle}/(B^{\langle \sigma, \rho^2 \rangle} + B^{\langle \sigma, \rho^3 \rangle})$ as an A-module, and 2 elements of $B^{\langle \sigma\rho \rangle}$ generating $B^{\langle \sigma\rho \rangle}/(B^{\langle \sigma\rho, \rho^2 \rangle} + B^{\langle \sigma\rho, \rho^3 \rangle})$. Adding these 4 elements to our set of generators we get 12 elements generating the A-module $B^{\langle \rho^2 \rangle} + B^{\langle \rho^3 \rangle} + B^{\langle \sigma \rangle} + B^{\langle \sigma\rho \rangle}$. This sum is equal to B, as one can infer from the identity $1 = (1 + \rho^2 + \rho^4) - (1 + \rho^3) - (1 + \sigma)(\rho^2 + \rho^4 + \sigma\rho) + (1 + \sigma\rho)(1 + \rho^3 + \sigma\rho^2)$. □

4. The subfield integer index

So far we were only interested in whether or not the subfield integer index $s(L/K)$ is equal to 1. In this section we examine it more precisely for Galois extensions L/K. The following proposition reduces the tamely ramified case to the computation of the group theoretic invariant $s(G)$, where $G = \mathrm{Gal}(L/K)$.

(4.1) Proposition. *Suppose that L/K is tamely ramified at all primes of K that divide $s(G)$. Then we have*

$$s(L/K) = s(G)^{[K:\mathbb{Q}]}. \tag{4.2}$$

Proof. Let p be a prime number that divides $s(G)$. By Noether's theorem [6, pp. 26-28] there exists a $\mathbb{Z}_p[G]$-module isomorphism $B \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong A_p[G]$, where $A_p = A \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Since A_p is free over $\mathbb{Z}_p$ of rank $n = [K : \mathbb{Q}]$, the G-module $A_p[G]$ is a direct sum of n copies of $\mathbb{Z}_p[G]$. This shows that the p-parts of $s(L/K)$ and of $s(G)^n$ are equal. By (3.2) all primes dividing $s(L/K)$ also divide $s(G)$, so the proof is complete. □

Our main theme for the rest of this note will be the question whether (4.2) also holds for wildly ramified extensions. In certain situations, for instance when G is abelian of type (p, p) or dihedral of order $2p$ for some prime p, one can prove that (4.2) holds without hypothesis on ramification by using "factor equivalence." We will not address the dihedral case here, but we will sketch the argument for the bicyclic case.

Suppose that the Galois group G is abelian. For any G-module M let $C_G(M) \subset M$ be the submodule generated by those $m \in M$ that are fixed by a cocyclic subgroup, i.e., a subgroup H of G with G/H cyclic. In [4] a formula is given for the index $c(G) = [\mathbb{Z}[G] : C_G(\mathbb{Z}[G])]$. The next theorem asserts that the index $[B : C_G(B)]$, which could be called the "cyclic subfield integer index," does not depend on ramification.

(4.3) Theorem. *If L/K is abelian then $[B : C_G(B)] = c(G)^{[K:\mathbb{Q}]}$. If G is abelian of type (p, p) for a prime number p, then $s(L/K) = s(G)^{[K:\mathbb{Q}]}$.*

The second statement is a special case of the first. By an argument of Burns [2, §1] the index $[M : C_G(M)]$ only depends on the G-module structure of M up to a relation called "factor equivalence." Using the conductor discriminant product formula, Nelson and Fröhlich [7] have shown that B is factor equivalent a direct sum of $[K : \mathbb{Q}]$ copies of $\mathbb{Z}[G]$. Thus (4.3) follows. A full account of the proof is given in [4].

Let G be an abelian group of type $(p, p, \ldots, p)$, with p a prime number, and assume that G has order p^n with $n \geq 2$. The group ring $\mathbb{F}_p[G]$ is a local ring because the ideal $\mathfrak{m}$ generated by the elements $\sigma - 1$ with $\sigma \in G$ is maximal and it is nilpotent.

(4.4) Proposition. *The ideal $S_G(\mathbb{Z}[G])$ of $\mathbb{Z}[G]$ is the kernel of the canonical homomorphism $\mathbb{Z}[G] \to \mathbb{F}_p[G]/\mathfrak{m}^{p-1}$, and $s(G) = p^{\binom{n+p-2}{n}}$.*

Proof. Choose generators $\sigma_1, \ldots, \sigma_n$ of G and let $x_i = \sigma_i - 1 \in \mathbb{F}_p[G]$. We have $\mathfrak{m} = (x_1, \ldots, x_n)$. The ring homomorphism $\mathbb{F}_p[X_1, \ldots, X_n] \twoheadrightarrow \mathbb{F}_p[G]$ sending X_i to x_i has kernel $(X_1^p, \ldots, X_n^p)$. It follows that the monomials in $x_1, \ldots, x_n$ of degree at most $p - 2$ form an $\mathbb{F}_p$-basis of $\mathbb{F}_p[G]/\mathfrak{m}^{p-1}$. There are exactly $\binom{n+p-2}{n}$ such monomials, so it remains to prove the first statement.

Let $f\colon \mathbb{Z}[G] \to \mathbb{F}_p[G]$ be the canonical map. Since $n \geq 2$ the relation (3.1) implies that $\operatorname{Ker} f \subset S_G(\mathbb{Z}[G])$. We need to show that $f(S_G(\mathbb{Z}[G])) = \mathfrak{m}^{p-1}$. Note that $S_G(\mathbb{Z}[G])$ is generated as a $\mathbb{Z}[G]$-ideal by the elements $N_\sigma = 1 + \sigma + \ldots + \sigma^{p-1}$ with $\sigma \in G$. In the field $\mathbb{F}_p(X)$ we have the identity

$$1 + X + \cdots + X^{p-1} = \frac{X^p - 1}{X - 1} = \frac{(X-1)^p}{X-1} = (X-1)^{p-1}.$$

This shows that $f(N_\sigma) = (f(\sigma) - 1)^{p-1} \in \mathfrak{m}^{p-1}$. For $a_1, \ldots, a_n \in \mathbb{Z}$ we have

$$f(\sigma_1^{a_1} \cdots \sigma_n^{a_n}) - 1 \equiv a_1 x_1 + \cdots + a_n x_n \bmod \mathfrak{m}^2$$

and it follows that $\mathfrak{m}/\mathfrak{m}^2 = \{(f(\sigma) - 1) \bmod \mathfrak{m}^2 : \sigma \in G\}$. We now claim:

(4.5) the $\mathbb{F}_p[x_1, \ldots, x_n]$-ideal $\mathfrak{m}^k$ is generated by $\{x^k : x \in \mathfrak{m}\}$ if $0 \leq k < p$.

This claim implies that the elements $f(N_\sigma) = (f(\sigma) - 1)^{p-1}$ generate $\mathfrak{m}^{p-1}$ modulo $\mathfrak{m}^p$, and by Nakayama's lemma they then generate $\mathfrak{m}^{p-1}$ as an $\mathbb{F}_p[G]$-ideal. Thus (4.4) follows. It remains to prove (4.5).

First assume that $n = 2$. The elements $\beta_j = x_1^j x_2^{k-j}$ with $j = 0, 1, \ldots, k$ form an $\mathbb{F}_p$-basis of $\mathfrak{m}^k/\mathfrak{m}^{k+1}$. For $i = 0, 1, \ldots, k$ we have

$$(ix_1 + x_2)^k = \sum_j a_{ij}\beta_j \text{ with } a_{ij} = \binom{k}{j} i^j \in \mathbb{F}_p.$$

Here we take $0^0 = 1$. The determinant of (a_{ij}) is a product of binomial coefficients and a Vandermonde determinant

$$\det(a_{ij}) = \prod_{j=0}^{k} \binom{k}{j} \times \prod_{0 \le j < i \le k} (i - j).$$

All factors are units modulo p because $k < p$, so the elements $(ix_1 + x_2)^k$ generate $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ as an $\mathbb{F}_p$-vector space. By Nakayama's lemma, we deduce that this set generates $\mathfrak{m}^k$ as an R-ideal, and this finishes the case $n = 2$.

To prove (4.5) for $n > 2$, we proceed by induction. Suppose we know (4.5) for the subring $R' = \mathbb{F}_p[x_1, \ldots, x_{n-1}]$, with maximal ideal $\mathfrak{m}'$. For non-negative integers $a_1, \ldots, a_n$ with sum k we want to express $x_1^{a_1} \cdots x_n^{a_n}$ as an R-linear combination of elements x^k with $x \in \mathfrak{m}$. First, use the induction hypothesis to express $x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}$ as an R'-linear combination of powers y^{k-a_n} of elements y in $\mathfrak{m}'$. By the case $n = 2$, we can express each element $y^{k-a_n} x_n^{a_n}$ as an $\mathbb{F}_p[y, x_n]$-linear combination of elements of the form $(ay + bx_n)^k$, with $a, b \in \mathbb{F}_p$. Since $ay + bx_n$ lies in $\mathfrak{m}$ this completes the induction step. □

(4.6) Proposition. *Let L be an abelian extension of $K = \mathbb{Q}$ whose Galois group G is of prime exponent p and rank $n > 1$. Then $s(L/\mathbb{Q}) = s(G) = p^{\binom{p+n-2}{n}}$.*

Proof. We know that $s(G) = p^{\binom{p+n-2}{n}}$ and by (3.2) the index $s(L/K)$ is a power of p. For an abelian group M put $M_p = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We need to show that $[B_p : S_G(B_p)] = s(G)$.

All primes of L lying over p have the same inertia group I. Let H be a subgroup of G such that $G = I \times H$. Put $B_p^{\mathrm{ram}} = B_p^H$ and $B_p^{\mathrm{unr}} = B_p^I$, so that B_p^{ram} is totally ramified and B_p^{unr} is unramified. Denote $\mathbb{Z}_p[G]$ by Λ. Note that $S_G(\Lambda)$ is the Λ-ideal generated by the elements $N_{H'} = \sum_{\sigma \in H'} \sigma$, with H' ranging over the minimal subgroups of G. It follows that

$$S_G(\Lambda) B_p = \sum_{H'} \mathrm{Tr}_{L/L^{H'}}(B_p).$$

If H' is a minimal subgroup of G which is not contained in I, then L is unramified over $L^{H'}$ above p and $\mathrm{Tr}_{L/L^{H'}}(B_p) = B_p^{H'}$. The multiplication map from the tensor product $B_p^{\mathrm{ram}} \otimes B_p^{\mathrm{unr}}$ over $\mathbb{Z}_p$ to B_p is an isomorphism of Λ-modules. We deduce that $S_G(B_p)$ is the image of

$$S_I(B_p^{\mathrm{ram}}) \otimes B_p^{\mathrm{unr}} + S_G(\Lambda)(B_p^{\mathrm{ram}} \otimes B_p^{\mathrm{unr}}).$$

Putting $M_0 = B_p^{\mathrm{ram}}/S_I(B_p^{\mathrm{ram}})$ and $M = M_0 \otimes B_p^{\mathrm{unr}}$, we see that

$$B_p/S_G(B_p) \cong M/S_G(\Lambda)M.$$

Now apply the same argument to the Λ-module $\Lambda \cong \mathbb{Z}_p[I] \otimes \mathbb{Z}_p[H]$ instead of the module $B_p \cong B_p^{\mathrm{ram}} \otimes B_p^{\mathrm{unr}}$. It follows that

$$\Lambda/S_G(\Lambda) \cong M'/S_G(\Lambda)M',$$

where $M' = M_0' \otimes \mathbb{Z}_p[H]$ with $M_0' = \mathbb{Z}_p[I]/S_I(\mathbb{Z}_p[I])$. The proposition follows if we show that M and M' are isomorphic Λ-modules. Since B_p^{unr} is isomorphic to $\mathbb{Z}_p[H]$ as a $\mathbb{Z}_p[G]$-module and H acts trivially on M_0 and M_0', it suffices to show that M_0 and M_0' are isomorphic as $\mathbb{Z}_p[I]$-modules.

We can bound I with local class field theory: the local Artin map gives a surjective group homomorphism $\mathbb{Z}_p^* \to I$ (see [10, p. 221]). The index $[\mathbb{Z}_p^* : (\mathbb{Z}_p^*)^p]$ is equal to p if p is odd, and it is equal to 4 if $p = 2$. Since I is annihilated by p, it follows that $\#I \leq p$ if p is odd and that $\#I \leq 4$ if $p = 2$.

If I is trivial then $M_0 = \mathbb{Z}_p = M_0'$. If I is of rank 1 then M_0 and M_0' are isomorphic over $\mathbb{Z}_p[I]$ because they are torsion free modules over the discrete valuation ring $\mathbb{Z}_p[I]/\mathbb{Z}_p N_I \cong \mathbb{Z}_p[\zeta_p]$ of the same $\mathbb{Z}_p$-rank. Finally, suppose that the rank of I is 2, so that $p = 2$. Both M_0 and M_0' have cardinality 2 by (4.3) and they can only have trivial I-action. In all cases this shows that M_0 and M_0' are $\mathbb{Z}_p[I]$-isomorphic. □

In the rest of this section it is shown that (4.6) does not hold without the assumption that $K = \mathbb{Q}$. We will construct a counterexample to (4.2) of type (2,2,2) with a base field K that can be chosen to have degree 6 over $\mathbb{Q}$. We use a computation of some easy instances of the 1-cohomology of the ring of integers.

(4.7) Proposition. *There is a Galois extension L/K of number fields with abelian Galois group G of type $(2,2,2)$ for which $s(L/K) \neq s(G)^{[K:\mathbb{Q}]}$.*

Proof. It suffices to construct L/K over the field $\mathbb{Q}_2$ of 2-adic numbers. One can then construct dense number fields as in [10, p. 44] to show the proposition. Let K be a finite extension of $\mathbb{Q}_2$ satisfying the following conditions:

(i) the absolute ramification index a is even;

(ii) the residue degree of K is at least 3.

Put $n = [K : \mathbb{Q}_2]$, and let $\mathfrak{p}$ be the maximal ideal of the ring of integers A of K. For $i \geq 1$ put $U_i = 1 + \mathfrak{p}^i$. Note that $U_1^2 \subset U_2$ and that $U_1/U_2 \cong \mathfrak{p}/\mathfrak{p}^2$ is a finite abelian group of exponent 2 and rank at least 3. Pick a subgroup X of order 8 of U_1/U_1^2 such that the composite map $X \subset U_1/U_1^2 \to U_1/U_2$ is injective. Now let $L = K(\sqrt{X})$. It follows that all cyclic intermediate fields are of the form $K(\sqrt{1+\pi})$, where π is a prime element of K. Note that $K(\sqrt{1+\pi})$ is an extension of K with ramification index 2, prime element $1 - \sqrt{1+\pi}$ and discriminant $4A$. Put $G = \mathrm{Gal}(L/K)$ and recall that $s(G) = 2$.

Let G_0 be a subgroup of order 4 in G. Put $B_0 = B^{G_0}$, and let B_1, B_2, B_3 be the intermediate rings of integers of $B_0 \subset B$. Consider the following exact sequence of $A[G]$-modules:

$$0 \longrightarrow (B_0)^2 \xrightarrow{f} B_1 \oplus B_2 \oplus B_3 \xrightarrow{g} B_1 + B_2 + B_3 \longrightarrow 0,$$

where f is given by $f(x, y) = (x, y - x, -y)$ and g by $g(x, y, z) = x + y + z$. By (4.3) we know that $B_1 + B_2 + B_3$ is of index 2^{2n} in B. Now let H be any subgroup of G of order 2 that does not lie in G_0. We will show that $B^H \subset B_1 + B_2 + B_3$. It then follows that $S_G(B) = B_1 + B_2 + B_3$, so that $[B : S_G(B)]$ equals 2^{2n} rather than $2^n = s(G)^{[K:\mathbb{Q}_2]}$.

Take H-invariants of the short exact sequence above. This gives a long exact sequence of A-modules

$$\begin{aligned} 0 &\longrightarrow (B_0^H)^2 \longrightarrow B_1^H \oplus B_2^H \oplus B_3^H \longrightarrow (B_1 + B_2 + B_3)^H \\ &\longrightarrow H^1(H, B_0)^2 \xrightarrow{\varphi} H^1(H, B_1) \oplus H^1(H, B_2) \oplus H^1(H, B_3) \longrightarrow \cdots. \end{aligned}$$

We know by (4.3) that $[B^H : B_1^H + B_2^H + B_3^H] = 2^n$. Since $(B_1 + B_2 + B_3)^H \subset B^H$ we are done if we can show that the index of $B_1^H + B_2^H + B_3^H$ in $(B_1 + B_2 + B_3)^H$ is at least 2^n. We therefore need to show that $\#\operatorname{Ker}\varphi \geq 2^n$. The following lemma, which is a special case of a result of Sen [12], enables us to determine the cohomology groups with their A-module structure.

(4.8) Lemma. *Let $F \subset E$ be a quadratic extension of 2-adic fields with Galois group G and rings of integers $A_F \subset A_E$. Assume that the different $\mathcal{D}$ of A_E over A_F divides the ideal $2A_E$. Then $\mathcal{D} = \mathfrak{d} \cdot A_E$ for a unique A_F-ideal $\mathfrak{d}$, and $H^1(G, A_E)$ is isomorphic to $A_F/\mathfrak{d}$ as an A_F-module.*

Proof. We may assume that E is ramified over F. Let π be a prime element of E and let $G = \{1, \sigma\}$. One checks that $\mathcal{D} = tA_E$ where $t = \mathrm{Tr}_{E/F}(\pi) \in A_F$. Recall that

$H^1(G,M) = M^-/(\sigma-1)M$, where $M^- = \{m \in M : \sigma m = -m\}$. In this case we have $(\sigma-1)A_E = (t-2\pi)A_F$ and $(A_E)^- = (1-(2/t)\pi)A_F$, so $H^1(G,A_E) \cong A_F/tA_F$. $\square$

We return to the proof of (4.7). All intermediate fields of L/K that are quadratic over K have discriminant $4A$, and those that are quartic over K have discriminant $64A$ by the conductor discriminant product formula. This implies that $\mathcal{D}_{B_0/A} = 2B_0$, and that $\mathcal{D}_{B_i/B_i^H} = \mathfrak{a}B_i^H$ if $i = 1,2,3$, where $\mathfrak{a}$ is the unique ideal of A with $\mathfrak{a}^2 = 2A$.

The lemma implies that $H^1(H,B_0)$ is A-isomorphic to $A/2A$, and that $H^1(H,B_i)$ is B_i^H-isomorphic to $B_i^H/\mathfrak{a}B_i^H$. In particular the image of φ is annihilated by $\mathfrak{a}$. This means that $\mathfrak{a}H^1(H,B_0)^2$ lies in the kernel of φ. Since $\#(\mathfrak{a}/2A) = 2^{n/2}$ this implies that the kernel has at least 2^n elements, as required. This proves (4.7). $\square$

References

1. S. Böge, *Die ϵ-invariante von $SL(2,p)$*, Arch. Math. **46** (1986), 299–303.
2. D. Burns, *Factorisability, group lattices, and Galois module structure*, J. Algebra **134** (1990), 257–270.
3. J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Academic Press, London, 1967.
4. B. de Smit, *Class group relations and Galois module structure*, dissertation, University of California at Berkeley, 1993.
5. A. Fajardo Mirón, *The calculation of algebraic integers β with small index $[A{:}\mathbb{Z}[\beta]]$ using the basis reduction algorithm LLL*, doctoraal scriptie (MA thesis), Universiteit van Amsterdam, 1987.
6. A. Fröhlich, *Galois module structure of algebraic integers*, Ergeb. Math. Grenzgeb. (3) **1**, Springer-Verlag, 1983.
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. J. S. Hsia and R. D. Peterson, *An invariant ideal of a group ring of a finite group and applications*, J. Algebra **32** (1974), no. 3, 576–599.
9. J. S. Hsia and R. D. Peterson, *An invariant ideal of a group ring of a finite group II*, Proc. Amer. Math. Soc. **51** (1975), no. 2, 275–281.
10. S. Lang, *Algebraic number theory*, Graduate Texts in Math. **110**, Springer, New York, 1986.
11. W. Scharlau, *Eine Invariante endlicher Gruppen*, Math. Z. **130** (1973), 291–296.
12. S. Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90** (1969), 33–46.

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

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