ANNALES

DE

L'INSTITUT FOURIER

Cornelius GREITHER & Henri JOHNSTON

Non-existence and splitting theorems for normal integral bases

Tome 62, n° 1 (2012), p. 417-437.

<http://aif.cedram.org/item?id=AIF_2012__62_1_417_0>

Ann. Inst. Fourier, Grenoble
62, 1 (2012) 417-437

NON-EXISTENCE AND SPLITTING THEOREMS FOR NORMAL INTEGRAL BASES

by Cornelius GREITHER & Henri JOHNSTON (*)

Abstract. — We establish new conditions that prevent the existence of (weak) normal integral bases in tame Galois extensions of number fields. This leads to the following result: under appropriate technical hypotheses, the existence of a normal integral basis in the upper layer of an abelian tower $\mathbb{Q} \subset K \subset L$ forces the tower to be split in a very strong sense.

Résumé. — Nous établissons de nouvelles conditions sous lesquelles il ne peut exister de bases normales entières (faibles) dans les extensions galoisiennes modérées de corps de nombres. Ceci nous conduit au résultat suivant : sous quelques hypothèses techniques convenables, l'existence d'une base normale entière dans l'étage supérieur d'une tour abélienne $\mathbb{Q} \subset K \subset L$ force que la tour se décompose dans un sens très fort.

1. Introduction

Let L/K be a tame abelian extension of number fields with Galois group G. Then the ring of integers $\mathcal{O}_L$ is projective over the group ring $\mathcal{O}_K[G]$ and we say that L/K has a *normal integral basis* (NIB) if $\mathcal{O}_L$ is in fact free over $\mathcal{O}_K[G]$. In the case $K = \mathbb{Q}$, the Hilbert-Speiser Theorem says that L/K always has an NIB. However, the situation is rather more complex when $K \neq \mathbb{Q}$, as illustrated by the following two results of Brinkhuis.

We call a number field K a CM-field if it is a totally imaginary quadratic extension of a totally real field. Note that if $K/\mathbb{Q}$ is abelian then K is either CM or totally real.

Keywords: Normal integral basis.
Math. classification: 11R33, 11R18, 11R20.
(*) Johnston was partially supported by a grant from the Deutscher Akademischer Austausch Dienst.

THEOREM 1.1 ([1]). — *Let K be a number field that is either CM or totally real and let L be a finite abelian extension of K of odd order. Assume that for some subfield k of K, over which K and L are Galois, the short exact sequence of Galois groups*

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1$$

is non-split. Then L/K has no normal integral basis.

THEOREM 1.2 ([2]). — *Let L/K be an unramified abelian extension of number fields, each of which is either CM or totally real. If the Galois group of L/K is not 2-elementary, then L/K has no normal integral basis.*

A further obstruction rests on the factorization of resolvents and prevents the existence of so-called *weak normal integral bases* (WNIBs). We recall that L/K has a WNIB if $\mathfrak{M}\mathcal{O}_L$ is free over $\mathfrak{M}$, where $\mathfrak{M}$ is the maximal $\mathcal{O}_K$-order in the group algebra $K[G]$. In [2], Brinkhuis shows non-existence of a WNIB in certain cases when $L = \mathbb{Q}(\zeta_p)$, the pth cyclotomic field, and Cougnard generalises these results in [4].

In Section 4 of this paper, we exhibit further cases in which there is no WNIB. The main technical difference with the work of Brinkhuis and Cougnard is that we do not use comparison with absolute extensions when showing that certain resolvents have nontrivial class.

Recall that two number fields L and K are said to be *arithmetically disjoint* over a common subfield F if $\mathcal{O}_{LK} = \mathcal{O}_L \otimes_{\mathcal{O}_F} \mathcal{O}_K$, or equivalently, $(\mathrm{Disc}(\mathcal{O}_L/\mathcal{O}_F), \mathrm{Disc}(\mathcal{O}_K/\mathcal{O}_F)) = \mathcal{O}_F$ and L is linearly disjoint from K over F (see [6, III.2.13]). In his classic book [5], Fröhlich makes the observation that if L and K are arithmetically disjoint over F and L/F has an NIB, then so does LK/K. He goes on to say, "What one wants are of course somewhat less trivial conditions [for the existence of NIBs]". In Section 5, we show that in certain settings there are no such conditions! More precisely, we prove that under appropriate technical hypotheses, the existence of an NIB in the upper layer of an abelian tower $\mathbb{Q} \subset K \subset L$ forces the tower to be *arithmetically split*, that is, there exists a number field L' arithmetically disjoint from K over $\mathbb{Q}$ such that $L = L'K$.

2. Preliminaries

Let L/K be a tame abelian extension of number fields with Galois group G. (In this paper, we take "tame" to mean "at most tamely ramified".) The group algebra $K[G]$ contains a unique maximal $\mathcal{O}_K$-order $\mathfrak{M} = \mathfrak{M}_{K[G]} =$

$\mathfrak{M}_{L/K}$. We say that L/K has a *weak normal integral basis* (WNIB) if the projective $\mathfrak{M}$-module $\mathfrak{M} \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L$ is free. Note that we may identify $\mathfrak{M} \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L$ with $\mathfrak{M}\mathcal{O}_L \subset L$.

Let $D(G) = D(K, G)$ denote the set of K-irreducible characters of G. For each $\psi \in D(G)$, let $D(\psi)$ denote the set of absolutely irreducible characters χ such that $\psi = \sum_{\chi \in D(\psi)} \chi$. Let

$$e_\psi := \frac{1}{|G|} \sum_{g \in G} \psi(g^{-1}) g$$

be the corresponding primitive idempotent of $K[G]$. For $\psi \in D(G)$, fix an absolutely irreducible character $\chi_\psi \in D(\psi)$ and let $K_\psi = K(\chi_\psi)$ be the field extension of K generated by the values of χ_ψ. Then we have K-algebra isomorphisms $K[G]e_\psi \longrightarrow K_\psi$ induced by $g \mapsto \chi_\psi(g)$. (Note that these depend on the choices of $\chi_\psi \in D(\psi)$, but the fields K_ψ do not.) These restrict to isomorphisms $\mathfrak{M}_\psi := \mathfrak{M}e_\psi \longrightarrow \mathcal{O}_{K_\psi}$ and we have

$$K[G] = \bigoplus_{\psi \in D(G)} K[G]e_\psi \cong \bigoplus_{\psi \in D(G)} K_\psi$$

$$\text{and} \quad \mathfrak{M} = \bigoplus_{\psi \in D(G)} \mathfrak{M}e_\psi \cong \bigoplus_{\psi \in D(G)} \mathcal{O}_{K_\psi}.$$

For $\chi \in D(\mathbb{C}, G)$ and $\alpha \in L$, define

$$(\alpha \mid \chi) = (\alpha \mid \chi)_{L/K} := \sum_{g \in G} \chi(g^{-1}) g(\alpha) = |G| e_\chi \alpha \in L(\chi)$$

to be the *resolvent* attached to α and χ. Denote by $(\mathcal{O}_L : \chi)$ the $\mathcal{O}_{K(\chi)}$-module generated by the $(\alpha \mid \chi)$ with $\alpha \in \mathcal{O}_L$ where the action is given by multiplication in $L(\chi)$. Note that G acts on $\mathcal{O}_{K(\chi)}$ via χ and thereby acts on $(\mathcal{O}_L : \chi)$, giving $g(\alpha|\chi) = (g(\alpha)|\chi)$ for all $\alpha \in \mathcal{O}_L$ and $g \in G$.

PROPOSITION 2.1. — *L/K has a WNIB if and only if $(\mathcal{O}_L : \chi_\psi)$ is free over $\mathcal{O}_{K_\psi}$ for every $\psi \in D(G)$. (Note that this is true irrespective of the choices of $\chi_\psi \in D(\psi)$.)*

Proof. — We emulate the argument given for [7, Proposition 1.2]. Observe that

$$\begin{aligned} & \mathfrak{M} \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L \cong \mathfrak{M} \text{ as } \mathfrak{M}\text{-modules} \\ \iff \quad & \mathfrak{M}e_\psi \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L \cong \mathfrak{M}e_\psi \text{ as } \mathfrak{M}e_\psi\text{-modules for all } \psi \in D(G) \\ \iff \quad & \mathcal{O}_{K_\psi} \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L \cong \mathcal{O}_{K_\psi} \text{ as } \mathcal{O}_{K_\psi}\text{-modules for all } \psi \in D(G). \end{aligned}$$

Therefore it suffices to show that $\mathcal{O}_{K_\psi} \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L \cong (\mathcal{O}_L : \chi_\psi)$ for each $\psi \in D(G)$. Consider the map $\varphi : \mathcal{O}_L \to (\mathcal{O}_L : \chi_\psi)$, $\alpha \mapsto (\alpha \mid \chi_\psi)$. Recall G acts on $\mathcal{O}_{K_\psi}$ via χ_ψ, hence φ is $\mathcal{O}_K[G]$-linear, and we obtain an epimorphism

$$\varphi' : \mathcal{O}_{K_\psi} \otimes_{\mathcal{O}_K[G]} \mathcal{O}_L \longrightarrow (\mathcal{O}_L : \chi_\psi).$$

By a rank argument, φ' is also injective. □

Corollary 2.2. — *Let L' be any finite extension of L such that $L(\chi) \subseteq L'$ for all $\chi \in D(\mathbb{C}, G)$. If L/K has a WNIB, then for every $\psi \in D(G)$ the ideal $\mathcal{O}_{L'}(\mathcal{O}_L : \chi_\psi)$ is principal.*

Proof. — This follows trivially from Proposition 2.1 once one notes that the hypothesis ensures $(\mathcal{O}_L : \chi_\psi) \subseteq \mathcal{O}_{L'}$ for every $\psi \in D(G)$. □

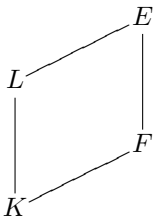
Lemma 2.3. — *Let $K \subset L \subset N$ be a tower of number fields such that N/K is tame abelian. If N/K has an NIB (resp. WNIB), then L/K also has an NIB (resp. WNIB).*

Proof. — Let $G = \mathrm{Gal}(N/K)$ and $H = \mathrm{Gal}(L/K)$. Since N/L is tame, $\mathrm{Tr}_{N/L}(\mathcal{O}_N) = \mathcal{O}_L$. Suppose that N/K has an NIB, i.e., there exists $\alpha \in \mathcal{O}_N$ such that $\mathcal{O}_N = \mathcal{O}_K[G] \cdot \alpha$. Adapting the proof of [3, Lemma 6], we have

$$\begin{aligned}\mathcal{O}_L &= \mathrm{Tr}_{N/L}(\mathcal{O}_N) = \mathrm{Tr}_{N/L}(\mathcal{O}_K[G] \cdot \alpha) = \mathcal{O}_K[G] \cdot \mathrm{Tr}_{N/L}(\alpha) \\ &= \mathcal{O}_K[H] \cdot \mathrm{Tr}_{N/L}(\alpha).\end{aligned}$$

A similar argument applies for WNIBs. □

Lemma 2.4. — *Let K be a number field with finite extensions L and F such that L/K is tame abelian. Let $E = LF$ and suppose that L and F are arithmetically disjoint over K.*



If L/K has an NIB (resp. WNIB), then E/F also has an NIB (resp. WNIB).

Proof. — Straightforward. □

3. Bounding a certain kernel

DEFINITION 3.1. — *Let L/K be Galois extension of number fields with Galois group G.*

(1) *Let* $\mathrm{Ram}(L/K)$ *be the set of finite primes of K that ramify in L.*
(2) *For* $\mathfrak{p} \in \mathrm{Ram}(L/K)$, *let* $e_\mathfrak{p} = e_{\mathfrak{p},L/K}$ *denote the ramification index of* $\mathfrak{p}$ *in* L/K.
(Note that $e_\mathfrak{p}$ is well-defined because L/K is Galois.)
(3) *Let* $\mathrm{M}(L/K)$ *be the abelian group* $\bigoplus_{\mathfrak{p}\in\mathrm{Ram}(L/K)} \mathbb{Z}/e_\mathfrak{p}\mathbb{Z}$.
(4) *Define a homomorphism of abelian groups*

$$\varepsilon_{L/K} : \mathrm{M}(L/K) \longrightarrow \frac{\mathrm{Cl}(\mathcal{O}_L)^G}{\mathrm{Img}(\mathrm{Cl}(\mathcal{O}_K))}$$

by sending $\bar{1}$ *(at position* $\mathfrak{p}$*) to the class of* $\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$ *($\mathfrak{P}$ prime of L) where* $\mathrm{Img}(\mathrm{Cl}(\mathcal{O}_K))$ *denotes the image of the natural map* $\mathrm{Cl}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}(\mathcal{O}_L)$.
(Note that $(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P})^{e_\mathfrak{p}} = \mathfrak{p}\mathcal{O}_L$, *and therefore* $\varepsilon_{L/K}$ *is well-defined.)*

Suppose that L is a CM-field and that K is either CM or totally real.

(5) *Let j denote complex multiplication.*
(6) *For a finite G-module X, let* X_{odd} *be the odd part of X. If j also acts on X, let* X^- *be the minus part of* X_{odd}, *i.e.,* $X^- = (X_{\mathrm{odd}})^{1-j}$.
(7) *Let* μ_L *be the group of roots of unity in L.*

We make no claim that the following result is new; for cyclic G it can be deduced from results in [9, Chapter 13, §4].

PROPOSITION 3.2. — *Suppose that j commutes with every element of G. Then j acts on* $\mathrm{Ram}(L/K)$ *and* $\mathrm{Ker}(\varepsilon_{L/K})^-$ *is isomorphic to a subquotient of* $\mathrm{H}^1(G, \mu_{L,\mathrm{odd}})$.

Proof. — The first claim is immediate.

Let I be any ambiguous (G-stable) ideal of $\mathcal{O}_L$ such that $[I] \in \mathrm{Cl}(\mathcal{O}_L)^- \cap \mathrm{Img}(\mathrm{Cl}(\mathcal{O}_K))$. Then $I = x\mathfrak{a}\mathcal{O}_L$ for some $x \in \mathcal{O}_L$ and some ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Thus, $J := I^{1-j} = y\mathfrak{a}^{1-j}\mathcal{O}_L$ with $y = x^{1-j}$, so y is an anti-unit, i.e., $y^{1+j} = 1$. For every $\sigma \in G$, $J^\sigma = J$, hence $y^{\sigma-1}$ must be a unit of L, and therefore a root of unity because it is an anti-unit as well. The map $\alpha_I : \sigma \mapsto y^{\sigma-1}$ is a 1-cocycle on G with values in μ_L.

For $z = (z_\mathfrak{p})_\mathfrak{p} \in \mathrm{M}(L/K)$, let $I(z)$ denote the ideal $\prod_\mathfrak{p}(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P})^{z_\mathfrak{p}}$, so that $\varepsilon_{L/K}(z)$ is the class of $I(z)$. Now assume $z \in \mathrm{Ker}(\varepsilon_{L/K})^-$. Then $J = I(z)^{1-j}$ can be written as above and one obtains a cocycle $\alpha_{I(z)}$. Let $\bar{\alpha}(z)$ denote the class of this cocycle in $\mathrm{H}^1(G, \mu_L)$. If $\bar{\alpha}(z)$ is trivial,

then there exists a root of unity ζ such that $\zeta^{1-\sigma} = \alpha_{I(z)}(\sigma) = y^{\sigma-1}$ for all $\sigma \in G$. Then setting $y' = \zeta y$ gives $J = y'\mathfrak{a}^{1-j}\mathcal{O}_L$, and y' is fixed under G, hence in K. Therefore J is induced from an ideal of $\mathcal{O}_K$. Now $J = I((1-j)z) = I(2z)$; from the definition one sees that $I(z')$ is only induced from a $\mathcal{O}_K$-ideal if z' is trivial in $\mathrm{M}(L/K)$. Hence we have $z = 0$.

It remains only to resolve the technical problem that $\bar{\alpha}$ is not necessarily a homomorphism. Let U be the group of all cocycles $w \mapsto w^{\sigma-1}$, where w is an anti-unit generating an ideal $\mathfrak{b}^{1-j}\mathcal{O}_L$ with $\mathfrak{b}$ an ideal of $\mathcal{O}_K$. Then changing the representation $I = x\mathfrak{a}\mathcal{O}_L$ to another $I = x_1\mathfrak{a}_1\mathcal{O}_L$ changes $\bar{\alpha}_I$ by a factor in U. Conversely, if $\bar{\alpha}_I \in U$, we can change the representation of I so as to make $\bar{\alpha}_I$ trivial. If we define β to be $\bar{\alpha}$ followed by the projection $\mathrm{H}^1(G,\mu_L) \to \mathrm{H}^1(G,\mu_L)/U$, we see that β is an injective homomorphism. Since the domain of definition of β has odd order, we may replace μ_L by its odd part. □

4. Non-existence of weak normal integral bases

Definition 4.1. — *Let $k \subset K \subset L$ be a tower of number fields. We adopt the following harmless abuse of language: we say that a prime $\mathfrak{p}$ of k ramifies in L/K if some prime above $\mathfrak{p}$ ramifies in L/K. We denote by $e_{\mathfrak{p},K/k}$ the ramification degree of $\mathfrak{p}$ in K/k and, if L/k is Galois, we let $e_{\mathfrak{p},L/K}$ denote the ramification degree in L/K of* any *prime above $\mathfrak{p}$ in K.*

Theorem 4.2. — *Let L/k be an abelian extension of number fields. Let K be an intermediate field such that L/K is tame and K is totally real. Suppose there exists a prime $\mathfrak{p}$ of k such that $e_{\mathfrak{p},K/k}$ has a nontrivial odd factor and $e_{\mathfrak{p},L/K}$ has an odd prime factor ℓ, for which the following two conditions are satisfied:*

1. *K is linearly disjoint from $\mathbb{Q}(\zeta_\ell)$ over $\mathbb{Q}$ (equivalently, $[K(\zeta_\ell) : K] = \ell - 1$); and*
2. *if $\ell = 3$, then $e_{\mathfrak{p},K/k}$ has an odd prime divisor q such that $\zeta_q \notin L(\zeta_{3^\infty})$.*

Then L/K has no WNIB.

Proof. —

(1) Looking at ramification groups, we see that there exists an intermediate extension $K \subset \tilde{L} \subset L$ such that $\tilde{L}$ is cyclic of ℓ-power degree over K and in which (a prime above) $\mathfrak{p}$ is ramified with precise exponent ℓ. By Lemma 2.3, we may therefore suppose without loss of generality that in fact $L = \tilde{L}$. (We have implicitly used the

hypothesis that L/k is abelian here; if we were only to assume L/k Galois and L/K abelian, then $\tilde{L}/k$ would not necessarily be Galois.) Note that L is totally real since $[L : K]$ is odd, L/K is Galois and K is totally real. Furthermore, since $[L : K]$ is a power of ℓ, $[K(\zeta_\ell) : K] = \ell - 1$ implies that $[L(\zeta_\ell) : L] = \ell - 1$. In other words, L is linearly disjoint from $\mathbb{Q}(\zeta_\ell)$ over $\mathbb{Q}$.

(2) There exists an intermediate extension $k \subset \tilde{k} \subset K$ such that (a prime above) $\mathfrak{p}$ is still ramified in $K/\tilde{k}$ and $K/\tilde{k}$ is cyclic of odd prime order. (In the case $\ell = 3$, we choose $\tilde{k}$ such that $[K : \tilde{k}] = q$.) We may therefore suppose without loss of generality that in fact $k = \tilde{k}$.

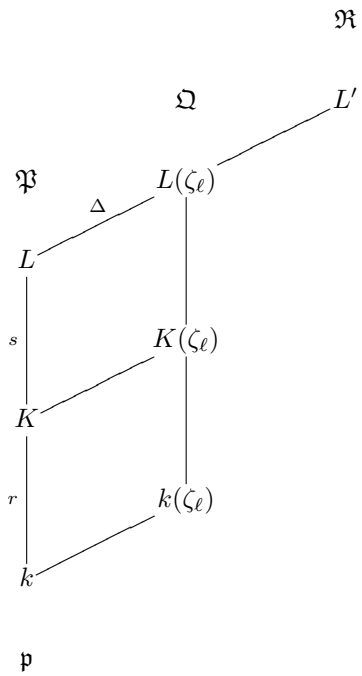
(3) Let $r = [K : k]$ (an odd prime), $s = [L : K]$ (a power of ℓ) and $L' = L(\zeta_s)$. By Corollary 2.2, it is enough to show for some faithful character $\chi : \mathrm{Gal}(L/K) \to L'^{\times}$ that the ideal $I := \mathcal{O}_{L'}(\mathcal{O}_L : \chi)$ is not principal. From the fact that ℓ divides $e_{\mathfrak{p},L/k}$, we know that ℓ also divides $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) - 1 = |(\mathcal{O}_k/\mathfrak{p})^{\times}|$ (use the local Artin map) and so $\mathfrak{p}$ is totally split in $k(\zeta_\ell)/k$. Let $\Delta = \mathrm{Gal}(L(\zeta_\ell)/L)$. Then Δ is canonically isomorphic to a subgroup D of $(\mathbb{Z}/\ell\mathbb{Z})^{\times}$; we denote the automorphism attached to $i \in D$ by δ_i. Since L is linearly disjoint from $\mathbb{Q}(\zeta_\ell)$ over $\mathbb{Q}$, we in fact have $D = (\mathbb{Z}/\ell\mathbb{Z})^{\times}$. (Note that it is possible to weaken the disjointness hypothesis - see Remark 4.6.)

Fix a prime $\mathfrak{P}$ of L above $\mathfrak{p}$ and let $\mathbb{F}$ be the residue field $\mathcal{O}_K/\mathfrak{P} \cap K$. Let η be the restriction of the local Artin map, $\mathbb{F}^{\times} \to \mathrm{Gal}(L/K)$, followed by χ. Then η has image exactly $\mu_\ell \subset L(\zeta_\ell)$ because $e_{\mathfrak{p},L/K} = \ell$. Define $\gamma : \mathbb{F}^{\times} \to \mathbb{F}^{\times}$ by $x \mapsto x^{-f}$ where $f = |\mathbb{F}^{\times}|/\ell$ (note that $|\mathbb{F}^{\times}| = \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{P} \cap \mathcal{O}_K) - 1$ is a multiple of $|(\mathcal{O}_k/\mathfrak{p})^{\times}| = \mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) - 1$, which is divisible by ℓ). It is straightforward to see that γ has image $\mu_\ell \subset \mathbb{F}^{\times}$. Therefore there exists exactly one prime ideal $\mathfrak{Q}$ above $\mathfrak{P}$ in $L(\zeta_\ell)$ such that γ agrees with η followed by reduction modulo $\mathfrak{Q}$ (note that $\mathfrak{P}$ splits completely in $L(\zeta_\ell)$ and all primes $\mathfrak{Q}$ above $\mathfrak{P}$ have the same residue class field as $\mathfrak{P}$.) From [5, Theorem 26 (i)] (the proof of which is a fairly standard argument resting crucially on a certain local calculation involving a Kummer extension) we obtain:

(A) For every prime $\mathfrak{R}$ of L' above $\mathfrak{Q}$, the ideal $I = \mathcal{O}_{L'}(\mathcal{O}_L : \chi)$ has valuation 1 at $\mathfrak{R}$.

Since $\mathfrak{p}$ is totally split in $k(\zeta_\ell)/k$, we know that $\mathfrak{P}$ splits into $\ell - 1$ factors in $L(\zeta_\ell)$; these are permuted by $\Delta = \mathrm{Gal}(L(\zeta_\ell)/L)$. From loc. cit., we also obtain:

(B) For all $i = 1, \ldots, \ell - 1$ and every prime $\mathfrak{R}$ of L' above $\delta_i^{-1}\mathfrak{Q}$, the ideal $I = \mathcal{O}_{L'}(\mathcal{O}_L : \chi)$ has valuation i at $\mathfrak{R}$.



Now let $\mathfrak{Q}_i$ denote the product of all primes of L' over $\delta_i^{-1}\mathfrak{Q}$. Then $\mathfrak{P}\mathcal{O}_{L'} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_{\ell-1}$, where the factors are pairwise coprime. Let

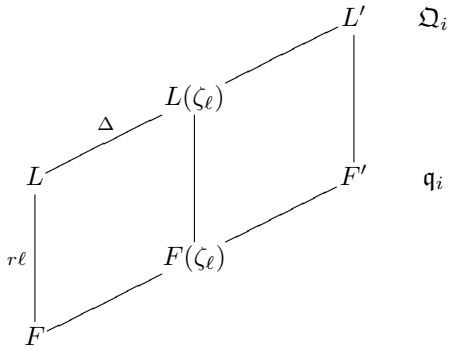
$$\theta = \sum_{i=1}^{\ell-1} i\delta_i^{-1} \in \mathbb{Z}[\Delta].$$

By definition of the $\mathfrak{Q}_i$, the Galois group $\mathrm{Gal}(L'/L)$ acts on them through its quotient Δ. Thus the expression $\mathfrak{Q}_1^\theta$ makes sense, and from (B) we obtain the following key information:

(C) The "above-$\mathfrak{P}$-part" of $I = \mathcal{O}_{L'}(\mathcal{O}_L : \chi)$ is $\mathfrak{Q}_1^\theta$.

(4) We need two auxiliary fields: let F be the inertia field of $\mathfrak{p}$ in L/k and put $F' = F(\zeta_s)$. Then $[L : F] = r\ell$ and $\mathfrak{p}$ is totally ramified in L/F. If r and $\mathfrak{p}$ are coprime, then since $\mathfrak{p}$ is tamely ramified in L/K, it is also tamely ramified in L/F and so $\mathrm{Gal}(L/F)$ must be cyclic. If r and $\mathfrak{p}$ are not coprime, then $\mathfrak{p}$ has wild ramification degree r in L/F and so $\mathrm{Gal}(L/F)$ is isomorphic to a semi-direct product of $(\mathbb{Z}/\ell\mathbb{Z})$ with $(\mathbb{Z}/r\mathbb{Z})$. However, the hypothesis that L/k is abelian forces this product to be direct and so again $\mathrm{Gal}(L/F)$ is cyclic (note that if $r = \ell$, then r is coprime to $\mathfrak{p}$). Furthermore, L must be linearly disjoint from F' over F because F'/F is unramified at $\mathfrak{p}$, whereas L/F is totally ramified at $\mathfrak{p}$. Let $\mathfrak{q}_i$ be the product of all distinct

primes of F' below factors of $\mathfrak{Q}_i$. (Note that because of total ramification, $\mathfrak{p}$-primes in F' and L' correspond bijectively.)



From the definition of resolvents, we see that I is an ambiguous ideal under $\mathrm{Gal}(L'/F')$.

(5) In taking minus parts in what follows, it is important to note that complex conjugation j is just δ_{-1} because L is totally real. Since $\mathrm{Gal}(L'/F')$ is cyclic, we find that $\mathrm{H}^1(L'/F', \mu_{L'}) = \mathrm{Hom}(L'/F', \mu_{L'})$ is also cyclic. By Proposition 3.2 (applied to L'/F' instead of L/K), we see that $\mathrm{Ker}(\varepsilon_{L'/F'})^-$ is a cyclic group.

The group $\Delta = \mathrm{Gal}(L(\zeta_\ell)/L)$, which can be seen as the non-ℓ-part of $\mathrm{Gal}(L'/L)$, acts on both F'/F and L'/L. Let $R = (\mathbb{Z}/r\ell\mathbb{Z})[\Delta]$. Then $\varepsilon_{L'/F'}$ is in fact an R-module homomorphism. We can write $\mathrm{M}(L'/F') = A \oplus B$ where A is the R-module consisting of elements $x = (x_\mathfrak{r})_\mathfrak{r}$ with $x_\mathfrak{r} = 0$ for all $\mathfrak{r} \notin \{\mathfrak{q}_i\}$ and B is the R-module consisting of elements $y = (y_\mathfrak{r})_\mathfrak{r}$ with $y_{\mathfrak{q}_i} = 0$ for all $\mathfrak{q}_i$. By abuse of notation, we do not distinguish between $\theta \in \mathbb{Z}[\Delta]$ and its projection to R. Let $z \in A$ denote the element with entries 1 at all primes dividing $\mathfrak{q}_1$, and zeros elsewhere. Then $\theta z \in A$ and by the partial factorization given in (C), we know that there exists $z' \in B$ such that

$$[I] = \varepsilon_{L'/F'}(\theta z + z').$$

We now proceed by contradiction. Suppose that L/K does in fact have a WNIB. Then by Corollary 2.2, the resolvent ideal I must be principal and so $\theta z + z' \in \mathrm{Ker}(\varepsilon_{L'/F'})$. Let $\pi : A \oplus B \to A$ be the natural projection. Then

$$\pi(\theta z + z') = \theta z \in \pi(\mathrm{Ker}(\varepsilon_{L'/F'}))$$

and so letting $J = R\theta$ be the ideal of R generated by θ, we have

$$J^- z \subseteq \pi(\mathrm{Ker}(\varepsilon_{L'/F'}))^- = \pi(\mathrm{Ker}(\varepsilon_{L'/F'})^-).$$

However, $\pi(\mathrm{Ker}(\varepsilon_{L'/F'})^-)$ is cyclic as an abelian group since the same is true for $\mathrm{Ker}(\varepsilon_{L'/F'})^-$. Therefore in order to show that L/K has no WNIB,

it suffices to show that $(Jz)^- = J^-z$ is not cyclic as an abelian group. Since Rz is a free R-submodule of A of rank 1, we see that J^- and J^-z are isomorphic as R-modules and hence as abelian groups. Thus we are further reduced to showing that J^- is not cyclic as an abelian group.

(6) Assume that $\ell > 3$ (we shall return to the $\ell = 3$ case later). We consider the two elements $\ell\theta$ and $(2-\delta_2)\theta$ in ℓR, which identifies with $(\mathbb{Z}/r\mathbb{Z})[\Delta]$ ("division by ℓ"). Then the two elements take the shape

$$u = 1 \cdot \delta_1^{-1} + 2 \cdot \delta_2^{-1} + \ldots + (\ell-1) \cdot \delta_{\ell-1}^{-1}$$

and

$$v = \delta_{(\ell+1)/2}^{-1} + \delta_{(\ell+3)/2}^{-1} + \ldots + \delta_{\ell-1}^{-1},$$

respectively. We now project them into the minus part, by sending $\delta_{\ell-i}^{-1}$ to $-\delta_i^{-1}$ for $i = 1, \ldots, (\ell-1)/2$. The result is

$$u^- = (2-\ell) \cdot \delta_1^{-1} + (4-\ell) \cdot \delta_2^{-1} + \ldots + (-1) \cdot \delta_{(\ell-1)/2}^{-1},$$

and

$$v^- = -\delta_1^{-1} - \delta_2^{-1} - \ldots - \delta_{(\ell-1)/2}^{-1}.$$

Looking just at the first two coefficients of u^- and v^- and noting that

$$\det \begin{pmatrix} 2-\ell & 4-\ell \\ -1 & -1 \end{pmatrix} = \ell - 2 + 4 - \ell = 2,$$

we see that u^- and v^- between them generate an abelian group of type (r, r). In particular, J^- cannot be cyclic as an abelian group.

(7) Finally, we discuss the case $\ell = 3$. We have $[K : k] = r = q$ by the choice made in step (2). By condition (b), $\zeta_q \notin L' \subset L(\zeta_{3^\infty})$ and so the group $\mathrm{H}^1(L'/F', \mu_{L'})$ has order prime to q. Hence by Proposition 3.2 (applied to L'/F' instead of L/K), we see that $\mathrm{Ker}(\varepsilon_{L'/F'})^-$ also has order prime to q. However, the element θ projected to the minus part of $(\mathbb{Z}/3q\mathbb{Z})[\Delta]$ comes out as $(2-\ell)\delta_1 = -\delta_1$, which has order $q\ell$. The argument is completed as before. □

We now give a corollary that will used in the proof of Theorem 5.5. For this we need a compatibility result for resolvents, which the authors were unable to find in the literature, but seems unlikely to be new. We give a proof for the convenience of the reader.

We retain the notation $K \subset \tilde{L} \subset L$ from step (1) in the above proof, dropping the assumption that L equals $\tilde{L}$. To $\tilde{L}$ we associated a resolvent ideal which we now write $\tilde{I} = \mathcal{O}_{L'}(\mathcal{O}_{\tilde{L}} : \tilde{\chi})$ with $\tilde{\chi}$ a faithful character of $\mathrm{Gal}(\tilde{L}/K)$. We likewise have a resolvent ideal $I = \mathcal{O}_{L'}(\mathcal{O}_L : \chi)$ for any character χ of $\mathrm{Gal}(L/K)$. (A choice for χ will be made in a moment.) Now assume L/K is cyclic and write t for the degree $[L : \tilde{L}]$. Then by

construction $L/\tilde{L}$ is totally ramified at all primes above $\mathfrak{p}$; we pick a faithful character χ of $\mathrm{Gal}(L/K)$ such that $\tilde{\chi}$ inflates to χ^t.

LEMMA 4.3. — *Under the conditions above, we have the following norm compatibility:*

$$(\mathrm{N}_{L'/\tilde{L}'} I)_{\mathfrak{p}} = \tilde{I}_{\mathfrak{p}},$$

where the subscript $\mathfrak{p}$ denotes taking the above-$\mathfrak{p}$ part of an ideal, that is, one omits all powers of prime ideals not above $\mathfrak{p}$ from the factorization of the ideal.

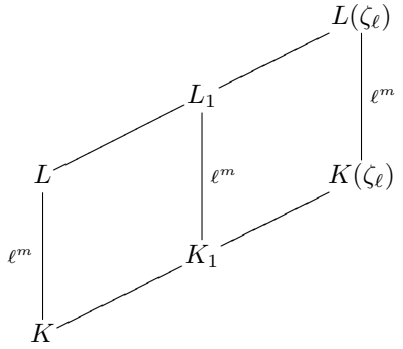
Proof. — The assertion is equivalent to the corresponding assertion for all completions at places above $\mathfrak{p}$. So for the rest of this proof we assume that all our fields are complete (the base field k is replaced by its $\mathfrak{p}$-adic completion), but denote them by the same letters as before.

As in the proof of Theorem 4.2, we look at [5, p.135] (F there being our K), and we consider the characters η and $\tilde{\eta}$ of $\mathcal{O}_K^\times$ afforded via local class field theory by χ and $\tilde{\chi}$ respectively. (Fröhlich's notation is φ instead of η.) Then we have $\tilde{\eta} = \eta^t$, and therefore the integers s and $\tilde{s}$ attached to η and $\tilde{\eta}$ resp. as in loc. cit. are also linked by the relation $\tilde{s} = ts$. From this and again [5, Theorem 26 (i)] we obtain, with v the normalized p-adic valuation:

$$v(\tilde{I}) = t \cdot v(I).$$

Since the degree t extension $L/\tilde{L}$ is totally ramified, the preceding formula amounts exactly to the required norm relation. □

COROLLARY 4.4. — *Assume the hypotheses and notation of Theorem 4.2 and make the further assumption that L/K is cyclic of degree ℓ^m for some $m \geqslant 1$. Suppose that there exist fields L_1 and K_1 with $L \subseteq L_1 \subseteq L(\zeta_\ell)$, $K \subseteq K_1 \subseteq K(\zeta_\ell)$ and $[L_1 : L] = [K_1 : K]$.*



Then L_1/K_1 does not have a WNIB.

Remark 4.5. — Note that Theorem 4.2 does not apply directly to L_1/K_1 because K_1 is not linearly disjoint from $\mathbb{Q}(\zeta_\ell)$ over $\mathbb{Q}$ and is not necessarily totally real.

Proof. — L is linearly disjoint from K_1 over K since $[L : K] = \ell^m$ and $[K_1 : K]$ divides $\ell - 1$. Furthermore, L/K is tamely ramified and K_1/K is only ramified at primes above ℓ, if at all. Therefore L is in fact arithmetically disjoint from K_1 over K, and so for any nontrivial character χ of $\mathrm{Gal}(L_1/K_1) \cong \mathrm{Gal}(L/K)$, we have $\mathcal{O}_{L'}(\mathcal{O}_L : \chi) = \mathcal{O}_{L'}(\mathcal{O}_{L_1} : \chi)$ (note that $L_1 = K_1 L$ and $L' = L(\zeta_{\ell^m})$ in this case). It remains to prove that $I = \mathcal{O}_{L'}(\mathcal{O}_L : \chi)$ is not principal. We closely follow the argument given in the proof of Theorem 4.2, using Lemma 4.3.

There are elements y and y_1 in the above-$\mathfrak{p}$ part (resp. the not-above-$\mathfrak{p}$ part) of $M(L'/F')$, such that $\varepsilon_{L'/F'}(y + y_1) = [I]$. Similarly (and as before) we have $\tilde{z}$ and $\tilde{z}_1$ in the above-$\mathfrak{p}$ part (resp. the not-above-$\mathfrak{p}$ part) of $M(\tilde{L}'/F')$, such that $\varepsilon_{\tilde{L}'/F'}(\tilde{z} + \tilde{z}_1) = [\tilde{I}]$. By Lemma 4.3 and step (5) in the proof of Theorem 4.2 we may choose y and $\tilde{z}$ in such a way that $\theta z = \tilde{z} = \mathrm{N}_{L'/\tilde{L}'} y$. Then y generates a noncyclic $\mathbb{Z}$-submodule of $M(L'/F')^-$ since $\theta z = \mathrm{N}_{L'/\tilde{L}'} y$ generates a noncyclic submodule of $M(\tilde{L}'/F')^-$ as already shown. As at the end of step (5) in the proof of Theorem 4.2, this implies that I is not principal (even more: the class of I is nontrivial in the target of the map $\varepsilon_{L'/F'}$). Hence L'/F' has no WNIB, and as shown in the first paragraph of the proof, this implies that L_1/K_1 does not have a WNIB either. □

We now discuss just a few of the many variants that Theorem 4.2 admits.

Remark 4.6. — Condition (a) of Theorem 4.2 requires that K is linearly disjoint from $\mathbb{Q}(\zeta_\ell)$ over $\mathbb{Q}$, or equivalently, that $K(\zeta_\ell)$ has maximal degree $\ell - 1$ over K. Recall from the proof that D is defined to the subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ that is canonically isomorphic to $\mathrm{Gal}(L(\zeta_\ell)/L)$. Minor modifications of the argument allow condition (a) to be replaced with a weaker, though more cumbersome, hypothesis:

(a′) (i) L is linearly disjoint from $k(\zeta_\ell)$ over k; and
(ii) for g some Fermat prime or $g = 2$, we have $\ell > g^2$ and $\bar{g} \in D \subset (\mathbb{Z}/\ell\mathbb{Z})^\times$.

Note that the only known Fermat primes are $3, 5, 17, 257$ and 65537. Since L is totally real and $L(\zeta_\ell)$ is totally complex, $[L(\zeta_\ell) : L]$ is even and so we always have $\overline{-1} \in D$. Hence (a′) is no improvement over (a) when $\ell \leqslant 11$, but for example if $\ell = 13$, then D could be the subgroup of order 6.

We briefly outline the necessary changes to step (6) of the proof of Theorem 4.2. Consider the elements θ and $(g-\delta_g)\theta$ in ℓR, which we identify with elements u and v in $(\mathbb{Z}/r\mathbb{Z})[\Delta]$, as before. Then using the fact that $g^2 < \ell$, we compute basis representations for u^- and v^-. We have

$$\det \begin{pmatrix} 2-\ell & 2g-\ell \\ 1-g & 1-g \end{pmatrix} = 2(g-1)^2,$$

where the entries of the upper (resp. lower) row of the matrix are the coefficients of u^- (resp. v^-) at δ_1^{-1} and δ_g^{-1}. Since $g = 2$ or is a Fermat prime, $2(g-1)^2$ is some power of 2 and hence relatively prime to r (some odd prime), and the proof concludes as before. Clearly, one could weaken (a′) even further in special cases where, for example, r is known.

THEOREM 4.7. — *Let L/k be a Galois (not necessarily abelian) extension of number fields. Let K be an intermediate field such that K/k and L/K are abelian, K is totally real, and L/K is tame of odd prime degree ℓ. Suppose there exists a prime $\mathfrak{p}$ of k that is (totally) ramified in L/K (so $e_{\mathfrak{p},L/K} = \ell$) and $e_{\mathfrak{p},K/k}$ has a nontrivial odd factor. Assume moreover that conditions (a) and (b) of Theorem 4.2 are satisfied. Then L/K has no WNIB.*

Proof. — This is very similar to, and at some stages slightly simpler than, the proof of Theorem 4.2. We make a brief remark on the necessary changes to part (4) to show that L/F is cyclic when r and $\mathfrak{p}$ are not coprime. A key point here is that F is a subfield of K. Observe that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/\ell\mathbb{Z})$ and $\mathrm{Gal}(K/F) \cong (\mathbb{Z}/r\mathbb{Z})$ where $r \neq \ell$, and L/F is Galois. So $\mathrm{Gal}(L/F)$ is cyclic if and only if it is abelian, which is the case precisely when the action of $\mathrm{Gal}(K/F)$ on $\mathrm{Gal}(L/K)$ is trivial. However, $\mathrm{Gal}(L/K)$ identifies via local class field theory with a quotient of the multiplicative group of the residue class field of K at the prime above $\mathfrak{p}$. Due to total ramification in K/F, this residue field is the same as the residue field of F at $\mathfrak{p}$, so the action of $\mathrm{Gal}(K/F)$ on $\mathrm{Gal}(L/K)$ is indeed trivial. □

Remark 4.8. — Both Theorem 4.7 and Corollary 4.4 still hold when hypothesis (a′) is assumed instead of (a). Of course, Corollary 4.4 can itself be viewed as another weakening of hypothesis (a).

DEFINITION 4.9. — *Let $k \subset K \subset L$ be a tower of number fields. We say that $L/K/k$ has* disjoint ramification *if there is no finite prime $\mathfrak{p}$ that ramifies both in K/k and L/K. (We already remarked on this abuse of language in Definition 4.1.)*

PROPOSITION 4.10. — *Let L/k be an abelian extension of number fields with $[L:k]$ odd and k totally real. Let K be an intermediate field such that L/K is tame and L/K has a WNIB. Suppose that for all prime divisors ℓ of $[L:K]$ we have $[K(\zeta_\ell):K] = \ell - 1$, and that at least one of the following conditions is satisfied:*

(a) *$[L:K]$ is not divisible by 3; or*
(b) *for all primes q dividing $[K:k]$, we have $\zeta_q \notin L(\zeta_{3^\infty})$.*

Then $L/K/k$ has disjoint ramification.

Proof. — By assuming the contrary that there is a finite prime ramified in both K/k and L/K, it follows directly from Theorem 4.2 that conditions (a) and (b) each give the desired conclusion. □

Remark 4.11. — Proposition 4.10 can be modified in a number of ways by using the variants of Theorem 4.2 discussed above.

5. Splitting theorems for normal integral bases

Let K be a number field and let Ω_K denote its absolute Galois group. We fix a finite abelian group G. A G-extension M/K is a commutative K-algebra M with a G-action, such that M is a G-Galois extension in the sense of Galois theory of commutative rings (see [8] for an introduction), also known as a G-Galois algebra. It is known that any such M has the form $\mathrm{ind}_{G_0}^G M_0$, where M_0/K is a G_0-Galois extension in the usual sense (i.e. M_0 is a field), G_0 is a subgroup of G, and as a K-algebra, $\mathrm{ind}_{G_0}^G M_0$ is just a product of $[G:G_0]$ factors M_0. (The "ind" notation is useful for obtaining the G-action on the product.) The field M_0 is called the *core field* of the Galois algebra M.

The set $\mathrm{H}(K,G)$ of all G-extensions M/K modulo G-isomorphism carries the structure of an abelian group. The product of M and N is given as follows: $M \otimes_K N$ is a $G \times G$-extension of K in the natural way; let D (the anti-diagonal) be the kernel of multiplication $G \times G \to G$, so $(G \times G)/D$ is identified with G. Then $M * N$ is (the class of) $(M \otimes_K N)^D$, with the natural structure of $(G \times G)/D = G$-extension. (For this, and more, see for example [10].)

There exists an isomorphism

$$\mathrm{H}^1(\Omega_K, G) = \mathrm{Hom}(\Omega_K^{ab}, G) \longrightarrow \mathrm{H}(K,G), \quad \phi \mapsto M_\phi$$

with the following description: for surjective ϕ, M_ϕ is the fixed field of K^{alg} under the kernel of ϕ, with the G-action resulting from $\Omega_K / \ker(\phi) \cong G$.

In general, let G_0 be the image of ϕ; then $M_{0,\phi}$ is defined as just explained, and M_ϕ is obtained by induction from G_0 to G.

There are canonical subgroups $\mathrm{H}^1_{tame}(\Omega_K, G)$ and $\mathrm{H}^1_{unr}(\Omega_K, G)$ of $\mathrm{H}^1(\Omega_K, G)$: the subgroups afforded by tame (resp. unramified) extensions. In terms of G-extensions, M is tame (resp. unramified) if and only if its core field is tame (resp. unramified). Using the alternative H^1 description above, ϕ is tame (resp. unramified) if and only if it is trivial on all higher ramification groups (resp. all inertia groups).

The class invariant map

$$\mathrm{pic} : \mathrm{H}^1_{tame}(\Omega_K, G) \longrightarrow \mathrm{Pic}(\mathcal{O}_K[G])$$

sends M to the class of the $\mathcal{O}_K[G]$-module $\mathcal{O}_M$. (Note that again $\mathcal{O}_M$ can be described in terms of the core field: it is $\mathrm{ind}_{G_0}^G \mathcal{O}_{M_0}$, or equivalently, the integral closure of $\mathcal{O}_K$ (or $\mathbb{Z}$) in M.) This is a homomorphism when restricted to unramified extensions, but this is not the case in general. However, we do have the following result (this is ascribed to McCulloh by Brinkhuis; it also appears in [5, p.225-226]). We say that two G-extensions are arithmetically disjoint over K if and only if their core fields are.

LEMMA 5.1. — *If M and M' are arithmetically disjoint and tame over K, then*

$$\mathrm{pic}(M * M') = \mathrm{pic}(M)\mathrm{pic}(M').$$

Proof. — We have

$$\mathcal{O}_{M*M'} = \mathcal{O}_{(M\otimes M')^D} = (\mathcal{O}_{M\otimes M'})^D = (\mathcal{O}_M \otimes_{\mathcal{O}_K} \mathcal{O}_{M'})^D,$$

where the third equality comes from the arithmetical disjointness. Let $P = \mathcal{O}_M \otimes_{\mathcal{O}_K} \mathcal{O}_{M'}$. Then P is a locally free $\mathcal{O}_K[G\times G]$-module and is therefore cohomologically trivial. Letting I_D denote the kernel of augmentation, we obtain

$$\begin{aligned} P^D &= \mathrm{Norm}_D \cdot P \cong P/\{x \in P : \mathrm{Norm}_D(x) = 0\} = P/I_D P \\ &= P \otimes_{\mathcal{O}_K[G\times G]} \mathcal{O}_K[G] \end{aligned}$$

as $\mathcal{O}_K[G\times G]$-modules. However, the last term is the finest quotient module of $\mathcal{O}_M \otimes_{\mathcal{O}_K} \mathcal{O}_{M'}$ on which $D = \{(\sigma, \sigma^{-1}) : \sigma \in G\}$ acts trivially, and this is simply the tensor product $\mathcal{O}_M \otimes_{\mathcal{O}_K[G]} \mathcal{O}_{M'}$, which has class $\mathrm{pic}(M)\mathrm{pic}(M')$ in $\mathrm{Pic}(\mathcal{O}_K[G])$. □

DEFINITION 5.2. — *Let $k \subset K \subset L$ be a tower of number fields. We say that $L/K/k$ is* arithmetically split *if there exists an extension L'/k such that $L = L'K$ and L' is arithmetically disjoint from K over k.*

THEOREM 5.3. — *Let L/K be a finite extension of number fields such that $L/\mathbb{Q}$ is abelian, L/K is tame of odd degree and K is totally real. Then $L/K/\mathbb{Q}$ is arithmetically split if and only if L/K has an NIB and $L/K/\mathbb{Q}$ has disjoint ramification.*

Remark 5.4. — If $n > 2$ is not a prime power, then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is unramified at all finite primes (see [11, Proposition 2.15]) and so $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+/\mathbb{Q}$ has disjoint ramification. Furthermore, $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ has an NIB generated by ζ_n but $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+/\mathbb{Q}$ is not arithmetically split. Therefore the hypothesis that $[L : K]$ is odd cannot be completely removed from Theorem 5.3.

Proof. — (1) Suppose that $L/K/\mathbb{Q}$ is arithmetically split, i.e., there exists a number field L' arithmetically disjoint from K over $\mathbb{Q}$ such that $L = L'K$. Then $L'/\mathbb{Q}$ has an NIB by the Hilbert-Speiser Theorem and so L/K also has an NIB by Lemma 2.4. Furthermore, it is clear that $L/K/\mathbb{Q}$ must have disjoint ramification.

(2) Suppose conversely that L/K has an NIB and $L/K/\mathbb{Q}$ has disjoint ramification. Let $\Omega = \Omega_{\mathbb{Q}}^{ab}$ and let $\Delta \subset \Omega$ be the group fixing K. Let $G = \mathrm{Gal}(L/K)$ and $\phi \in \mathrm{H}^1(\Omega_K, G)$ be associated to the G-extension L/K. Then ϕ must factor through Δ because L is abelian over $\mathbb{Q}$. On the other hand, there is the following general fact: if $\psi \in \mathrm{H}^1(\Omega, G)$ belongs to the extension $M/\mathbb{Q}$ for some M under the correspondence explained above, then $\psi|_\Delta$ belongs to the base-changed G-extension $K \otimes_{\mathbb{Q}} M/K$. (Even if M is a field, $K \otimes_{\mathbb{Q}} M$ need not be a field; but it certainly is a G-Galois algebra. This is another advantage of the formalism of Galois algebras.)

(3) Since the maximal abelian extension of $\mathbb{Q}$ is the linearly disjoint compositum of all its inertia fields (each being given in the form $\mathbb{Q}(\zeta_{p^\infty})$, p prime), the group Ω is the direct product of all the inertia groups: $\Omega = \prod_p T_p$, with p running over all primes. For any set Σ of rational primes, let $T_\Sigma = \prod_{p\in\Sigma} T_p \subset \Omega$. Now let S be the set of primes that ramify in $K/\mathbb{Q}$, and S' its complement. Then clearly $\Omega = T_S \times T_{S'}$ and $T_{S'}$ is a subgroup of $\Delta = \mathrm{Gal}(\mathbb{Q}^{ab}/K)$. On the other hand, for every prime of K over p, its inertia group in Δ is given by $T_p \cap \Delta$.

(4) Let L/K be given by $\phi : \Delta \to G$. (Then ϕ is onto since L is a field.) We construct $\psi : \Omega \to G$ as follows:

$$\begin{aligned} \psi|_{T_{S'}} &= \phi|_{T_{S'}}; \\ \psi|_{T_S} &= 1_G. \end{aligned}$$

Let L' be the G-extension of $\mathbb{Q}$ attached to ψ (so $L' = M_\psi$ in the notation used above). By construction, L' is arithmetically disjoint from K over $\mathbb{Q}$.

In particular, the Galois algebra $L_0 := K \otimes_{\mathbb{Q}} L'$ over K is a field, and as said in (2), L_0/K is attached to $\psi|_\Delta$.

We now need an explicit description of the inverse of a G-extension N/K in $\mathrm{H}(K,G)$: this is simply N^{op}, which equals N as a K-algebra, but G acts through the inverse map $\sigma \mapsto \sigma^{-1}$. We define a new G-extension by setting

$$M := L_0 * L^{op}$$

(product in $\mathrm{H}(K,G)$). Then M is attached to the difference $\alpha := \psi|_\Delta - \phi$, which is trivial on $T_{S'}$ by construction. Furthermore, α is trivial on $T_p \cap \Delta$ for each $p \in S$ since ϕ is trivial on $T_p \cap \Delta$ (L/K is unramified at primes above S because $L/K/\mathbb{Q}$ has disjoint ramification), and ψ is trivial on T_p by definition. This means precisely that ψ is trivial on *all* ramification groups in Δ, that is, M/K is unramified.

(5) If M/K is the trivial G-extension (equivalently: its core field is just K), then L_0 and L are the same as G-extensions of K, in particular, they are the same as K-algebras. Hence $L_0 = L$ considered as subfields of $\mathbb{Q}^{ab}$, and we recall that L' is arithmetically disjoint from K over $\mathbb{Q}$. Thus it now suffices to show that the other case, i.e., M/K nontrivial, is impossible.

(6) The class invariant map is compatible with induction, so if M_0 is the core field of M, then $\mathrm{pic}(M) = \mathrm{ind}_{G_0}^{G}\mathrm{pic}(M_0)$. Let $j : G \to G$ be the inversion map on G; by functoriality j induces an involution j_* on $\mathrm{Pic}(\mathcal{O}_K[G])$. In the following, we let X^- denote the subgroup of all $x \in X$ having odd order satisfying $j_* x = -x$. We make two claims:

(A) $\mathrm{pic}(M_0) \in \mathrm{Pic}(\mathcal{O}_K[G_0])^-$; and

(B) induction induces an injection $\mathrm{Pic}(\mathcal{O}_K[G_0])^- \to \mathrm{Pic}(\mathcal{O}_K[G])^-$.

We assume the validity of these claims and return to their proofs later. Since M_0/K is unramified, $[M_0 : K]$ is odd and K is totally real, Theorem 1.2 ([2, Theorem 1]) due to Brinkhuis shows that M_0/K has no NIB, i.e., $\mathrm{pic}(M_0)$ is nontrivial. Hence, by the two claims, $\mathrm{pic}(M)$ is also nontrivial. Now we have

$$M = L_0 * L^{op},$$

which is equivalent to

$$L = L_0 * M^{op}.$$

By the Hilbert-Speiser Theorem, $L'/\mathbb{Q}$ has an NIB since it is tame abelian (this follows from the tameness of L/K and the construction of L'). By Lemma 2.4, it follows that L_0/K also has an NIB since L' is arithmetically disjoint from K over $\mathbb{Q}$. Furthermore, we started from the assumption that L/K has an NIB. Therefore Lemma 5.1 applied to $L = L_0 * M^{op}$ leads to an immediate contradiction.

(7) It remains to establish claims (A) and (B).

Proof of (A): It follows from the fact that pic is a homomorphism on unramified extensions that $|G_0|\mathrm{pic}(M_0)$ is trivial. By functoriality, $\mathrm{pic}(j_*(M_0)) = j_*(\mathrm{pic}(M_0))$. (Here $j_*(M_0)$ is the same algebra as M_0, with inverted action of G.) But $j_*(M_0)$ happens to also be the inverse of M_0 in $\mathrm{H}(K, G_0)$, so again because pic is a homomorphism on unramified extensions, $\mathrm{pic}(j_*(M_0)) = -(\mathrm{pic}(M_0))$.

Proof of (B): This is considerably harder. We write U for G_0. The main obstacle is that $S := \mathcal{O}_K[G]$ is not a Galois extension of the ring $R := \mathcal{O}_K[U]$, so Galois cohomology cannot be used to calculate $\mathrm{Ker}(\mathrm{Pic}(R) \to \mathrm{Pic}(S))$. Instead, we use faithfully flat descent. Of course, S is faithfully flat (even free) over R. The first Amitsur cohomology of the multiplicative group $\mathrm{H}^1_A(S, \mathbb{G}_m)$ is canonically isomorphic to $\mathrm{Ker}(\mathrm{Pic}(R) \to \mathrm{Pic}(S))$. We recall the definition: there is a complex

$$S^\times \xrightarrow{\partial_1} (S \otimes_R S)^\times \xrightarrow{\partial_2} (S \otimes_R S \otimes_R S)^\times,$$

where ∂_1 sends s to $s \otimes s^{-1}$, and ∂_2 sends u to $u_1 \cdot u_2^{-1} \cdot u_3$. Here $u_1, u_2, u_3 \in (S \otimes_R S \otimes_R S)^\times$ denote the respective images of u under the maps defined on $(S \otimes_R S)^\times$, putting in a 1 on the left, in the middle and on the right, so, for example, $u_2(s \otimes t) = s \otimes 1 \otimes t$.

The Amitsur cohomology group is now the cohomology of this complex at the middle. We will show that the odd minus part of this is trivial. This heavily relies on an important result of Lenstra (see [2, p.159]): If K is totally real (and this is the case in our situation), then the "minus part" $(\mathcal{O}_K[\Gamma]^\times)^{1-j}$ of the unit group of the group ring of any abelian odd order group consists only of $\pm\Gamma$ itself. It is obvious that $S \otimes_R S$ can be identified with the group ring $\mathcal{O}_K[G^{(2)}]$, where $G^{(2)}$ is the pushout of G with itself over G_0 (more explicitly: $G \times G$ factored out by all (z, z^{-1}) with $z \in G_0$), and a similar statement holds for the triple tensor product. We exponentiate all terms in the last complex with $1 - j$, and obtain (we neglect ± 1):

$$G \longrightarrow G^{(2)} \longrightarrow G^{(3)},$$

and the maps are in close analogy to the previous maps: $x \in G$ goes to $(x, x^{-1}) \in G^{(2)}$, and $(x, y) \in G^{(2)}$ goes to $(x, y, 1)(x^{-1}, 1, y^{-1})(1, x, y) \in G^{(3)}$. The cohomology of this new complex then is just the minus part of the cohomology of the old one, at least in the odd part. It is now just an exercise to show that this new complex is exact, so its middle cohomology is trivial, and this means that the odd minus part of the Amitsur cohomology is trivial, as required. □

THEOREM 5.5. — *Let L/K be a finite extension of number fields such that $L/\mathbb{Q}$ is abelian, L/K is tame and $[L:\mathbb{Q}]$ is odd. Suppose that either*

(1) *$[L:K]$ is not divisible by 3; or*
(2) *for all primes q dividing $[K:\mathbb{Q}]$, we have $\zeta_q \notin L(\zeta_{3^\infty})$.*

Then L/K has an NIB if and only if $L/K/\mathbb{Q}$ is arithmetically split.

Proof. — Suppose that $L/K/\mathbb{Q}$ is arithmetically split, i.e., there exists a number field L' arithmetically disjoint from K over $\mathbb{Q}$ such that $L = L'K$. Then $L'/\mathbb{Q}$ has an NIB by the Hilbert-Speiser Theorem and so L/K also has an NIB by Lemma 2.4.

Suppose conversely that L/K has an NIB. There exist intermediate fields $L_1, \ldots, L_r$ such that L is equal to the compositum $L_1 \cdots L_r$ and for (not necessarily distinct) odd primes $\ell_1, \ldots, \ell_r$ we have $\mathrm{Gal}(L_i/K) \cong (\mathbb{Z}/\ell_i^{s_i}\mathbb{Z})$ for some $s_i \geqslant 1$. By Lemma 2.3, each extension L_i/K has an NIB. Suppose that each $L_i/K/\mathbb{Q}$ is arithmetically split, i.e., there exist fields L_i' each arithmetically disjoint from K over $\mathbb{Q}$ such that $L_i = L_i' \cdot K$. Let $L' = L_1' \cdots L_r'$. It is straightforward to check that $L = L' \cdot K$ and that L' is arithmetically disjoint from K over $\mathbb{Q}$. Hence $L/K/\mathbb{Q}$ is arithmetically split, as desired. Thus we are reduced to the case where L/K is cyclic and $[L : K] = \ell^s$ for some odd prime ℓ and some $s \geqslant 1$.

Observe that L is linearly disjoint from $K(\zeta_\ell)$ over K since $[L:K] = \ell^s$ and $[K(\zeta_\ell) : K]$ divides $\ell - 1$. Furthermore, L/K is tamely ramified and $K(\zeta_\ell)/K$ is only ramified at primes above ℓ, if at all. Therefore L is in fact arithmetically disjoint from $K(\zeta_\ell)$ over K, and so $L(\zeta_\ell)/K(\zeta_\ell)$ also has an NIB by Lemma 2.4.

Suppose for a contradiction that $L/K/\mathbb{Q}$ does not have disjoint ramification, i.e., there exists a prime p that ramifies in both $K/\mathbb{Q}$ and L/K. (Note that $p \neq \ell$ because L/K is tamely ramified.) It is straightforward to see that p ramifies in both $K(\zeta_\ell)/\mathbb{Q}$ and $L(\zeta_\ell)/K(\zeta_\ell)$.

We now use the theory of Dirichlet characters as described in [11, Chapter 3]. For $n \in \mathbb{N}$, let $X^{(n)}$ denote the group of Dirichlet characters corresponding to $\mathbb{Q}(\zeta_n)$. Let $m\ell^t$ be the conductor of $L(\zeta_\ell)$ over $\mathbb{Q}$ where $\ell \nmid m$. Let X be the group of Dirichlet characters corresponding to $L(\zeta_\ell)$ and let Y be the Sylow-ℓ subgroup of $X^{(\ell^t)}$. Then we have $X^{(\ell)} \subseteq X \subseteq X^{(m)} \times Y \times X^{(\ell)}$ and so X is of the form $Z \times X^{(\ell)}$. Let L' be the field corresponding to Z and construct K' analogously, i.e., "remove $\mathbb{Q}(\zeta_\ell)$". By [11, Theorem 3.5], p is ramified in both L'/K' and $K'/\mathbb{Q}$. Moreover, $[K' : \mathbb{Q}]$ is odd since $[K' : \mathbb{Q}]$ divides $[K : \mathbb{Q}]$ divides $[L : \mathbb{Q}]$, and so K' is totally real. Hence L'/K' satisfies the hypotheses of Theorem 4.2, and so applying Corollary 4.4 shows that $L(\zeta_\ell)/K(\zeta_\ell)$ does not have a WNIB. However, this is a contradiction

because $L(\zeta_\ell)/K(\zeta_\ell)$ has an NIB. We therefore conclude that $L/K/\mathbb{Q}$ must in fact have disjoint ramification. Since $[K:\mathbb{Q}]$ is odd and $K/\mathbb{Q}$ is Galois, K is totally real and so Theorem 5.3 now gives the desired result. □

Remark 5.6. — Condition (b) of Theorem 5.5 can be weakened as follows (we use notation from the proof): for each i with $\ell_i = 3$ and each prime q dividing $[K:\mathbb{Q}]$, we have $\zeta_q \notin L_i(\zeta_{3^\infty})$.

Remark 5.7. — The results of Brinkhuis stated in the introduction can be easily recovered in the special setting of Theorem 5.5. It is straightforward to see that extensions satisfying the hypotheses of Theorem 1.1 cannot be arithmetically split, and Theorem 1.2 for L absolutely abelian becomes a consequence of the fact that there are no nontrivial unramified extensions of $\mathbb{Q}$. Of course, Brinkhuis's results also hold in a much more general setting and it should be noted that the proof of Theorem 5.5 relies on Theorem 1.2.

6. Acknowledgments

The authors are grateful to the Deutscher Akademischer Austausch Dienst (German Academic Exchange Service) for a grant allowing the second named author to visit the first for the 2006-07 academic year, thus making this collaboration possible. Furthermore, the authors are indebted to the referee for several corrections and helpful comments.

BIBLIOGRAPHY

[1] J. Brinkhuis, "Normal integral bases and embedding problems", *Math. Ann.* **264** (1983), no. 4, p. 537-543.

[2] ———, "Normal integral bases and complex conjugation", *J. Reine Angew. Math.* **375/376** (1987), p. 157-166.

[3] N. P. Byott & G. Lettl, "Relative Galois module structure of integers of abelian fields", *J. Théor. Nombres Bordeaux* **8** (1996), no. 1, p. 125-141.

[4] J. Cougnard, "Nouveaux exemples d'extension relatives sans base normale", *Ann. Fac. Sci. Toulouse Math. (6)* **10** (2001), no. 3, p. 493-505.

[5] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 1, Springer-Verlag, Berlin, 1983, x+262 pages.

[6] A. Fröhlich & M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993, xiv+355 pages.

[7] C. Greither, "Relative integral normal bases in $\mathbb{Q}(\zeta_p)$", *J. Number Theory* **35** (1990), no. 2, p. 180-193.

[8] ———, *Cyclic Galois extensions of commutative rings*, Lecture Notes in Mathematics, vol. 1534, Springer-Verlag, Berlin, 1992, x+145 pages.

[9] S. Lang, *Cyclotomic fields II*, Graduate Texts in Mathematics, vol. 69, Springer-Verlag, New York, 1980, xi+164 pages.

[10] L. R. McCulloh, "Galois module structure of abelian extensions", *J. Reine Angew. Math.* **375/376** (1987), p. 259-306.

[11] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, xiv+487 pages.

Manuscrit reçu le 18 février 2008,
accepté le 16 janvier 2009.

Cornelius GREITHER
Universität der Bundeswehr München
Fakultät für Informatik
Institut für theoretische Informatik und Mathematik
85577 Neubiberg (Germany)
cornelius.greither@unibw.de

Henri JOHNSTON
St. John's College
Cambridge CB2 1TP (United Kingdom)
hlj31@cam.ac.uk