Appendix : about the Λ-freeness of $\overline{C}_\infty$.

Jean-Robert Belliard

Université de Franche-Comté, Laboratoire de mathématiques UMR 6623,
16 route de Gray, 25030 Besançon cedex, FRANCE.

belliard@math.univ-fcomte.fr

Let F be an abelian totally real number field (without any further restriction). In the paper [Bel98] we gave a sufficient condition to Λ-freeness of the Λ-module $\overline{C}_\infty$ associated to the cyclotomic $\mathbb{Z}_p$-extension F_∞/F. There amongst other hypotheses we assumed that p was unramified in the base field denoted K there and F here. Now due to the applications given in the main part of this paper, it seems worthwhile to write down precisely the relevant condition without assuming anything about ramification at p.

Lemma 0.1 *Let $L \subset F_\infty$ be the maximal subfield of F_∞ such that p is (at most) tamely ramified in L (under hypothesis (R), L is the field F^{tam} of* **??***). Put $\Lambda_L := \mathbb{Z}_p[[\text{Gal}(L_\infty/L)]]$, where L_∞/L is the cyclotomic $\mathbb{Z}_p$-extension of L. Then we have :*

1. *As a group, $\overline{C}_\infty$ only depends on F_∞ not on F.*
2. *$L_\infty = F_\infty$.*
3. *$\overline{C}_\infty$ is Λ-free if and only if $\overline{C}_\infty$ is Λ_L-free.*

Proof. 1 is clear. 2 is lemma 1.2 of [Bel05]. By theorem 2.2 of [Bel02], the Λ-freeness is equivalent to an asymptotic condition (namely the "asymptotic Galois Descent" property for the $\overline{C}_n$'s). But there exists some $N \in \mathbb{N}$ and some $b \in \mathbb{Z}$ such that for all $n \geq N$ we have $F_n = L_{n+b}$: the equivalence in 3 follows.

□

In the light of the lemma 0.1, as far as the Λ-freeness of $\overline{C}_\infty$ is concerned, we can (but shall not) in the sequel assume without loss of generality that p is (at most) tamely ramified in F. We could then just refer to [Bel98] for all proofs. But we thought it would be better to give them here including most of the details, taking this opportunity to simplify the arguments of [Bel98] by translating them at infinite level.

We need a few more notations. They are close to those used in [Bel98] but formally not exactly same. Let $\mathcal{P}$ be the set of rational primes $l \neq p$ which are ramified in $F/\mathbb{Q}$. The case $\mathcal{P} = \emptyset$ is obvious but allowed. For all supernatural numbers t we put $\mathbb{Q}(t) = \mathbb{Q}(\zeta_t)$. For all $J \subset \mathcal{P}$ and all $n \in \mathbb{N} \cup \{\infty\}$, we put $F_n(J) := \mathbb{Q}(\prod_{l \in J} l^\infty p^\infty) \cap F_n$. We shall abbreviate by $F(J) := F_0(J)$, $G(J) = \text{Gal}(F_\infty(J)/\mathbb{B}_\infty)$, where $\mathbb{B}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and $G = G(\mathcal{P})$. For any abelian number field K we write $\text{cond}(K)$ for its conductor, that is the minimal $n \in \mathbb{N}$ such that $K \subset \mathbb{Q}(n)$. For all $n \in \mathbb{N}$ and all $J \subset \mathcal{P}$ we will denote by $\varepsilon_n(J)$ the following cyclotomic number (unit if $J \neq \emptyset$) :

$$\varepsilon_n(J) := N_{\mathbb{Q}(\text{cond}(F_n(J)))/F_n(J)}(1 - \zeta_{\text{cond}(F_n(J))}).$$

It follows from the classical distribution relations that for $n \geq 1$ the $\varepsilon_n(J)$'s form a norm coherent sequence. Therefore, fixing a γ generating $\text{Gal}(\mathbb{B}_\infty/\mathbb{Q})$ we may define $\varepsilon_\infty(J) \in \overline{C}_\infty$ by the following formula :

$$\varepsilon_\infty(J) := \begin{cases} (\varepsilon_n(J))_{n \geq 1} \text{ if } J \neq \emptyset \\ (\varepsilon_n(\emptyset)^{(\gamma-1)})_{n \in \mathbb{N}} \text{ else.} \end{cases}$$

We shall examine the $\Lambda_L[G]$-module structure of $\overline{C}_\infty$ (recall that $G = G(\mathcal{P}) = \mathrm{Gal}(F_\infty/\mathbb{B}_\infty)$), and for that it is more convenient to write additively the multiplication in $\overline{C}_\infty$ and to keep multiplication for the action of $\Lambda[G]$. Consistently for $\mathbb{B}_\infty \subset N \subset K \subset F_\infty$ we will denote by $T_{K/N}$ the trace (actually the algebraic norm map) acting on elements $x \in \overline{C}_\infty^{\mathrm{Gal}(F_\infty/K)}$. The elements $\varepsilon_\infty(J)$ are subject to the following distribution relations :

Lemma 0.2 *Let* $\left(\dfrac{\mathfrak{A}}{N/K}\right)$ *be the (global) Artin symbol for any abelian extension* N/K *and (fractional) ideal* $\mathfrak{A}$ *of* K*. For all* $J \subset \mathcal{P}$ *and all* $I \subset J$*, put* $\mathcal{P}_{I,J}$ *for the set of rational primes* l *dividing* $\mathrm{cond}(F_\infty(J))$ *but not dividing* $\mathrm{cond}(F_\infty(I))$*. We have :*

$$T_{F_\infty(J)/F_\infty(I)}(\varepsilon_\infty(J)) = \left(\prod_{l\in\mathcal{P}_{I,J}} \left(1 - \left(\frac{(l)}{F_\infty(I)/\mathbb{Q}}\right)^{-1}\right)\right)\varepsilon_\infty(I).$$

Proof. The analogous relations at finite levels are well known. We then just take inverse limits. □

Lemma 0.3 *The system* $\{\varepsilon_\infty(J), J \subset \mathcal{P}\}$ *generates* $\overline{C}_\infty$ *over* $\Lambda_L[\mathrm{Gal}(F_\infty/\mathbb{B}_\infty)]$*.*

Proof. This follows from distribution relations (e.g. lemma 0.2) and lemma 2.3 of [Gre92]. □

We now state the ad hoc hypothesis that will ensure the freeness of $\overline{C}_\infty$. This "generalized hypothesis (B)" is an immediate generalization of (HB) in [Bel98].

Definition 0.4 *For all* $J \subset \mathcal{P}$ *we call norm ideal of* J *and denote by* $N(J)$ *the ideal of* $\mathbb{Z}_p[G(J)]$ *generated by traces*

$$N(J) := \left\langle T_{F_\infty(J)/F_\infty(J-\{l\})};\, l \in J\right\rangle.$$

We say that the pair (F,p) *satisfies "generalized Hypothesis B" ((gHB) for short) if and only if for all* $J \subset \mathcal{P}$ *the quotient* $\mathbb{Z}_p[G(J)]/N(J)$ *is torsion free.*

This hypothesis is quite technical, but very natural regarding the proof of theorem 0.6. The following proposition shows that (gHB) holds true in many usual cases. Indeed all known cases of freedom of $\overline{C}_\infty$ are consequence of (gHB) via theorem 0.6.

Proposition 0.5 *For all* $l \in \mathcal{P}$ *let us denote by* $I_l \subset G$ *the inertia subgroup for* l *in* $F_\infty/\mathbb{B}_\infty$*. Recall that for any finite abelian group* H*, we write* $\overline{H}$ *for its* p*-Sylow subgroup (considered also as the maximal* p*-quotient of* H*). The pair* (F,p) *satisfies (gHB) as soon as one of the following properties holds :*

1. *The* $\overline{I}_l$*,* $l \in \mathcal{P}$ *are mutually direct summands. In other words the natural map* $\bigoplus_{l\in\mathcal{P}} \overline{I}_l \longrightarrow \overline{G}$ *is injective.*
2. $\dim_{\mathbb{F}_p}(G/pG) \leq 1$*, or equivalently* $\overline{G}$ *is cyclic.*
3. $\#\mathcal{P} \leq 2$

Proof. These sufficient conditions are the exact analogues of those in section IV.1 of [Bel98]. Note that they concern only the maximal p-quotient of the Galois groups involved. Since the (unique) prime above p of $\mathbb{B}_\infty$ is tamely ramified in $F_\infty/\mathbb{B}_\infty$, everything goes as if p were unramified in the base field F. Taking this into account, we can repeat verbatim the proofs in [Bel98]. □

Theorem 0.6 *Let us denote by* $r(I)$ *the* $\mathbb{Z}_p$*-rank of* $\mathbb{Z}_p[G(I)]/N(I)$*. Assume that* (F,p) *satisfies (gHB). Fix any total order* $\leq$ *on the set of all subsets of* $\mathcal{P}$ *extending the inclusion. Then :*

1. $\forall J \subset \mathcal{P}$ *we have isomorphisms of* $\Lambda_L[G]$*-modules :*

$$\frac{\mathbb{Z}_p[G(J)]}{N(J)} \otimes_{\mathbb{Z}_p} \Lambda_L \cong \frac{\langle\varepsilon_\infty(J)\rangle}{\langle\varepsilon_\infty(I);\, I \subset J,\, I \neq J\rangle \bigcap \langle\varepsilon_\infty(J)\rangle} \cong \frac{\langle\varepsilon_\infty(J)\rangle}{\langle\varepsilon_\infty(I);\, I \leq J,\, I \neq J\rangle \bigcap \langle\varepsilon_\infty(J)\rangle};$$

hence all three $\Lambda_L[G]$*-modules are free over* Λ_L *(of ranks* $r(J)$*).*

2. $\overline{C}_\infty \cong \bigoplus_{I\subset\mathcal{P}} \Lambda_L^{r(I)}$ *as* Λ_L*-modules; in particular* $\overline{C}_\infty$ *is* Λ_L*-free of rank* $[L:\mathbb{Q}]$ *and* Λ*-free of rank* $[F:\mathbb{Q}]$.

Proof. $\overline{C}_\infty$ has the same Λ-rank (resp. Λ_L-rank) as $\overline{U}_\infty$, namely $[F:\mathbb{Q}]$ (resp. $[L:\mathbb{Q}] = [F_\infty : \mathbb{B}_\infty]$) : see e.g. [Kuz72], [Bel02] ... By (gHB) the modules $\frac{\mathbb{Z}_p[G(J)]}{N(J)} \otimes_{\mathbb{Z}_p} \Lambda_L$ are Λ_L-free. We first prove that 1 implies 2. From the tautological (split over Λ_L under (gHB) by 1) exact sequences :

$$\mathrm{ES}(J) \quad \langle \varepsilon_\infty(I);\, I\leq J,\, I\neq J\rangle \hookrightarrow \langle \varepsilon_\infty(I);\, I\leq J\rangle \twoheadrightarrow \frac{\langle\varepsilon_\infty(J)\rangle}{\langle \varepsilon_\infty(I);\, I\leq J,\, I\neq J\rangle \bigcap \langle\varepsilon_\infty(J)\rangle}$$

we see that 1 implies 2 by induction. Let us prove 1.

By lemma 0.2 and by the inclusion $\langle \varepsilon_\infty(I);\, I\subset J,\, I\neq J\rangle \subset \langle \varepsilon_\infty(I);\, I\leq J,\, I\neq J\rangle$ we have surjective morphisms :

$$(\mathrm{Sur}) \quad \frac{\mathbb{Z}_p[G(J)]}{N(J)} \otimes_{\mathbb{Z}_p} \Lambda_L \twoheadrightarrow \frac{\langle\varepsilon_\infty(J)\rangle}{\langle \varepsilon_\infty(I);\, I\subset J,\, I\neq J\rangle \bigcap \langle\varepsilon_\infty(J)\rangle} \twoheadrightarrow \frac{\langle\varepsilon_\infty(J)\rangle}{\langle \varepsilon_\infty(I);\, I\leq J,\, I\neq J\rangle \bigcap \langle\varepsilon_\infty(J)\rangle}.$$

Therefore the required isomorphisms will follow from equalities of Λ_L-ranks. Now :

Lemma 0.7 *Recall that for all* I, $r(I)$ *is the* $\mathbb{Z}_p$*-rank of* $\mathbb{Z}_p[G(I)]/N(I)$*. Put* $d(I) = [F_\infty(I) : \mathbb{B}_\infty]$.

1. *For all* $J\subset\mathcal{P}$ *we have*
$$r(J) = \sum_{I\subset J} (-1)^{\#J-\#I} d(I)$$

2. $$[L:\mathbb{Q}] = [F_\infty : \mathbb{B}_\infty] = d(\mathcal{P}) = \sum_{J\subset\mathcal{P}} r(J)$$

Proof. 1 is proven using character theory and following the same way as proposition 2.11 of [Bel98] : just replace the function $f_n(I)$ there by $d(I)$ here. 2 follows from 1 and the combinatorial lemma 2.14 of [Bel98]. Details are left to the reader.

□

We resume the proof of theorem 0.6. For any Λ_L-module M let us denote its Λ_L-rank by $\mathrm{rank}_{\Lambda_L}(M)$. Put

$$t(J) := \mathrm{rank}_{\Lambda_L}\left(\frac{\langle\varepsilon_\infty(J)\rangle}{\langle \varepsilon_\infty(I);\, I\leq J,\, I\neq J\rangle \bigcap \langle\varepsilon_\infty(J)\rangle}\right).$$

From the surjections (Sur) we see that $r(J)\geq t(J)$. On the other hand, summing ranks in all the sequences (ES(J)), we recover that $\sum_J t(J) = \mathrm{rank}_{\Lambda_L}(\overline{C}_\infty) = d(\mathcal{P}) = \sum_J r(J)$ by 2 of lemma 0.7. Therefore all inequalities $r(J)\geq t(J)$ are actually equalities. This proves theorem 0.6.

□

References

[Bel98] J.-R. Belliard, *Sur la structure galoisienne des unités circulaires dans les* $\mathbb{Z}_p$*-extensions*, J. Number Theory **69** (1998), no. 1, 16–49.

[Bel02] ______, *Sous-modules d'unités en théorie d'Iwasawa*, Théorie des nombres, Années 1998/2001, Publ. Math. UFR Sci. Tech. Besançon, 2002, p. 12.

[Bel05] ______, *Global units modulo circular units : descent without Iwasawa's Main Conjecture*, preprint (2005).

[Gre92] C. Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier (Grenoble) **42** (1992), no. 3, 449–499.

[Kuz72] L. V. Kuz′min, *The Tate module of algebraic number fields*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 267–327.