RADAN KUČERA

A note on circular units in $\mathbb{Z}_p$-extensions

Journal de Théorie des Nombres de Bordeaux, tome 15, n° 1 (2003), p. 223-229

<http://www.numdam.org/item?id=JTNB_2003__15_1_223_0>

© Université Bordeaux 1, 2003, tous droits réservés.

A note on circular units in $\mathbb{Z}_p$-extensions

par RADAN KUČERA

RÉSUMÉ. Nous nous intéressons aux limites projectives des groupes de Sinnott et des groupes de Washington des unités circulaires dans la $\mathbb{Z}_p$-extension d’un corps abélien. Nous montrons par un exemple qu’en général ces deux limites ne coïncident pas.

ABSTRACT. In this note we consider projective limits of Sinnott and Washington groups of circular units in the cyclotomic $\mathbb{Z}_p$-extension of an abelian field. A concrete example is given to show that these two limits do not coincide in general.

1. Introduction

For any positive integer $m$, let $\zeta_m = e^{2\pi i/m}$ and let $\mathbb{Q}(m) = \mathbb{Q}(\zeta_m)$ be the $m$th cyclotomic field. Let $K$ be an abelian field of conductor $m$, i.e., $m$ is the smallest positive integer such that $K$ is a subfield of $\mathbb{Q}(m)$. Let $C(K)$ be the Sinnott group of circular units of $K$ (see [S]). It is well known (see [L]) that this group can be defined as the intersection of the group $E(K)$ of all units in $K$ and the subgroup of the multiplicative group of $K$ generated by $-1$ and by all norms $N_{\mathbb{Q}(m)/\mathbb{Q}(m) \cap K}(1 - \zeta_m^r)$, where $1 < r | m$ and $(a,r) = 1$. Let $\bar{C}(K)$ be the group of cyclotomic units of $K$ mentioned in [W, page 143], i.e., $\bar{C}(K) = E(K) \cap C(\mathbb{Q}(m))$. We shall call the latter group the Washington group of cyclotomic units.

Now, let $p$ be an odd prime which does not ramify in $K$. Let $B/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension of the rational numbers, i.e., $\mathbb{Q} = B_0 \subset B_1 \subset B_2 \subset \ldots$ are abelian fields ramified only at $p$, $[B_n : \mathbb{Q}] = p^n$, and $B = \bigcup_{n=0}^{\infty} B_n$. Hence $KB = \bigcup_{n=0}^{\infty} KB_n$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$.

We shall consider the following projective limits (with respect to norms) $C = \varprojlim (C(KB_n) \otimes \mathbb{Z}_p)$, and $\bar{C} = \varprojlim (\bar{C}(KB_n) \otimes \mathbb{Z}_p)$. It has been proved in [KN] that $C$ is of finite index in $\bar{C}$. But there has remained an open question whether $C = \bar{C}$ in general or not. This note is devoted to the negative answer to this question. More precisely, by an explicit construction we shall prove the following

Manuscrit reçu le 3 décembre 2001.
Supported by the grant 201/01/0471 of the Grant Agency of the Czech Republic.
Theorem. For \( p = 3 \), there is an abelian field \( K \) of degree 9 over \( \mathbb{Q} \) such that there is \( \eta = (\eta_n)_{n=0}^\infty \in \varprojlim C(KB_n) \) satisfying \( \eta^3 \in \varprojlim C(KB_n) \) and \( \eta \notin \varprojlim (C(KB_n) \otimes \mathbb{Z}_p) \).

Let us mention that by an easy and straightforward modification of our construction one can get, for any given odd prime \( p \), an example of an abelian field of degree \( p^2 \), ramified at \( 2p + 1 \) primes, whose cyclotomic \( \mathbb{Z}_p \)-extension satisfies \( p \mid [\mathcal{C} : C] \).

A similar example has been given independently by J.-R. Belliard, who describes in [B] an abelian field \( K \) of degree \( p^2 \), ramified at \( p + 1 \) primes, and shows by means of an explicit construction in \( \mathbb{Z}_p \)-extension \( KB/K \) that \( C \) is not a \( \Lambda \)-free \( \Lambda \)-module, where \( \Lambda = \mathbb{Z}_p[[\text{Gal}(KB/K)]] \). Moreover, he proves here that there exists \( \epsilon \in \mathcal{C} \) such that \( \epsilon^p \in C \) and \( \epsilon \notin C \) if and only if \( C \) is not a \( \Lambda \)-free \( \Lambda \)-module. To compare these two constructions: on the one hand our example needs more ramified primes, but on the other hand we do not need to tensor by \( \mathbb{Z}_p \) to be able to define units \( \eta_n \in \mathcal{C}(KB_n) \) giving the norm-coherent sequence \( (\eta_n) \in \mathcal{C} \), so — in some sense — our example is more explicit.

Notation. Let \( q_1, q_2, \ldots, q_7 \) be different primes, all congruent to 1 modulo 9, chosen in such a way that \( q_1 \not\equiv 1 \pmod{27} \) and that for different \( i, j \in \{1, 2, \ldots, 7\} \) the prime \( q_i \) is a cubic residue modulo \( q_j \). For each \( i \in \{1, 2, \ldots, 7\} \), let \( \chi_i \) be a cubic Dirichlet character modulo \( q_i \). Let \( K \) be the abelian field corresponding to the group of Dirichlet characters generated by \( \chi_1 \chi_2 \chi_3 \chi_4 \chi_5 \) and \( \chi_2 \chi_3 \chi_4 \chi_5 \chi_6 \chi_7 \). So \([K : \mathbb{Q}] = 9\) and \( K \) has the following four subfields of degree 3:

- \( K_1 \) corresponding to \( \chi_2 \chi_3 \chi_4 \chi_5 \chi_6 \chi_7 \) of conductor \( f_1 = q_2 q_3 q_4 q_5 q_6 q_7 \),
- \( K_2 \) corresponding to \( \chi_1 \chi_2 \chi_3 \chi_4 \chi_5 \chi_6 \chi_7 \) of conductor \( f_2 = q_1 q_4 q_5 q_6 q_7 \),
- \( K_3 \) corresponding to \( \chi_1 \chi_2 \chi_3 \chi_4 \chi_5 \) of conductor \( f_3 = q_1 q_2 q_3 q_6 q_7 \),
- \( K_4 \) corresponding to \( \chi_1 \chi_2 \chi_3 \chi_4 \chi_5 \) of conductor \( f_4 = q_1 q_2 q_3 q_4 q_5 \).

For the sake of brevity, let us write \( K_0 = K \), \( f_0 = q_1 q_2 q_3 q_4 q_5 q_6 q_7 \), \( K_5 = \mathbb{Q} \), \( f_5 = 1 \).

For any prime \( q \mid 3f_0 \), let \( \text{Frob}(q) \) mean a fixed Frobenius automorphism of \( q \) on \( KB/\mathbb{Q} \), i.e., any chosen extension to \( KB \) of the Frobenius automorphism of \( q \) on the maximal subfield of \( KB \) unramified at \( q \). Since \( q_i \) is a cube modulo \( f_0/q_i \) for any \( i = 1, 2, \ldots, 7 \), the previous choice can be done in such a way that \( \text{Frob}(q_i) \in \text{Gal}(KB/K) \) for each \( i = 1, 2, \ldots, 7 \).

We shall introduce generators of \( C(KB_n) \). For any \( i = 0, 1, \ldots, 4 \) and any integer \( n \geq 0 \) let

\[
\varepsilon_{i,n} = \begin{cases} 
N_{Q(f_i)/K_i}(1 - \zeta_{f_i}) & \text{for } n = 0, \\
N_{Q(q^{3n+1}f_i)/K_iB_n}(1 - \zeta_{3n+1f_i}) & \text{for } n > 0.
\end{cases}
\]
Moreover, let $\varepsilon_{5,0} = -1$ and

$$
\varepsilon_{5,n} = \frac{(1 - \zeta_{3n+1}^4)(1 - \zeta_{3n+1}^{-4})}{(1 - \zeta_{3n+1})(1 - \zeta_{3n+1}^{-1})}
$$

for any positive integer $n$. The following lemma shows that units $\varepsilon_{i,j}$ with $0 < j < n$ are generated by all conjugates of the units $\varepsilon_{i,j}$, where $j = 0$ or $j = n$.

**Lemma 1.** For any integer $n \geq 0$, the Sinnott group of circular units $C(KB_n)$ is the Galois module generated by

$$
\{ \varepsilon_{i,0}; 0 \leq i \leq 5 \} \cup \{ \varepsilon_{i,n}; 0 \leq i \leq 5 \}.
$$

**Proof.** Using [L], $C(KB_n)$ is the intersection of $E(KB_n)$ and of the Galois module $D$ generated by $-1$ and by all norms $N_{Q(r)/Q(r)\cap KB_n}(1 - \zeta_r)$, where $1 < r | 3^{n+1}f_0$. We can write $r = 3^j q$, where $0 \leq j \leq n + 1$, and $q | f_0$. Let $f_l = \max\{f_l; 0 \leq l \leq 5, f_l | q\}$. So, denoting $B_{-1} = Q$, we have $Q(r) \cap KB_n = K_i B_{j-1}$. Therefore

$$
N_{Q(r)/Q(r)\cap KB_n}(1 - \zeta_r) = N_{Q(3^j f_i)/K_i B_{j-1}}(N_{Q(r)/Q(3^j f_i)}(1 - \zeta_r)).
$$

But

$$
N_{Q(r)/Q(3^j f_i)}(1 - \zeta_r) = (1 - \zeta_{3^j f_i}) \prod_{q | r, q \not| 3^j f_i} (1 - \text{Prob}(q)^{-1}),
$$

where $q$ in the product runs over all primes $q | r$, $q \not| 3^j f_i$ (an empty product equals $1$). Hence $D$ is generated by $-1$, by $\varepsilon_{i,j}$ for all $i = 0, 1, \ldots, 4$ and $j = 0, 1, \ldots, n$, and by

$$
N_{Q(3^j)/B_{j-1}}(1 - \zeta_{3^j}) = N_{B_n/B_{j-1}}(N_{Q(3^{n+1})/B_n}(1 - \zeta_{3^{n+1}}))
$$

for $j = 1, 2, \ldots, n + 1$. If $0 < j < n$ then

$$
(1) \quad \varepsilon_{i,j} = N_{K_i B_n/K_i B_j}(\varepsilon_{i,n}).
$$

and $N_{Q(3^{n+1})/B_n}(1 - \zeta_{3^{n+1}}) = (1 - \zeta_{3^{n+1}}) (1 - \zeta_{3^{n+1}}^{-1})$. Therefore $D$ is the Galois module generated by $-1$, by $\varepsilon_{i,j}$ for all $i = 0, 1, \ldots, 4$ and $j \in \{0, n\}$, and by $(1 - \zeta_{3^{n+1}}) (1 - \zeta_{3^{n+1}}^{-1})$. It is well-known that all the numbers but the last one are units and that the quotient of any two conjugates of the last number is a unit. The lemma follows using the fact that the automorphism sending each root of unity to its fourth power generates the Galois group of $B_n/Q$. 

The generators described by Lemma 1 are not independent. For any integers $j \geq 0$ and $i, l \in \{0, 1, \ldots, 5\}$ such that $l = 0$ or $i = 5$ we have the
following relation

\[
N_{K_iB_j/K_iB_j}(\varepsilon_{i,j}) = \varepsilon_{i,j}^{\prod q (1 - \text{Frob}(q)^{-1})},
\]

where \( q \) in the product runs over all primes dividing \( f_i/f_j \). Moreover, for any integer \( j \geq 0 \) and \( i \in \{0, 1, \ldots, 5\} \)

\[
N_{K_iB_j/K_i}(\varepsilon_{i,j}) = \varepsilon_{i,0}^{1 - \text{Frob}(3)^{-1}}.
\]

**Construction.** As we have already mentioned, the Frobenius automorphism \( \text{Frob}(q_i) \in \text{Gal}(KB/K) \) for each \( i = 1, 2, \ldots, 7 \). Moreover, \( q_i \equiv 1 \pmod{9} \) implies that \( \text{Frob}(q_i) \) is a cube in \( \text{Gal}(KB/K) \cong (\mathbb{Z}_3, +) \). Therefore there is unique \( \psi \in \text{Gal}(KB/K) \) such that \( \psi^3 = \text{Frob}(q_1)^{-1} \). Because \( q_1 \not\equiv 1 \pmod{27} \), \( \psi \) is a topological generator of \( \text{Gal}(KB/K) \). Hence, for each \( i = 2, 3, \ldots, 7 \) there is a uniquely determined 3-adic integer \( \alpha_i \) satisfying \( \text{Frob}(q_i)^{-1} = \psi^{3\alpha_i} \).

It is easy to see that \( \text{Gal}(KB_n/B_n) \setminus \{id\} \) is the disjoint union

\[
\text{Gal}(KB_n/B_n) \setminus \{id\} = \bigcup_{i=1}^{4} \left( \text{Gal}(KB_n/K_iB_n) \setminus \{id\} \right).
\]

Therefore

\[
\varepsilon_{0,n}^3 = \left( N_{KB_n/B_n}(\varepsilon_{0,n})^{-1} \right) \prod_{i=1}^{4} N_{KB_n/K_iB_n}(\varepsilon_{0,n}).
\]

Let us consider the group \( C(KB_n)/(C(KB_n))^3 \) written additively, where we shall identify any unit of \( C(KB_n) \) with its image in \( C(KB_n)/(C(KB_n))^3 \). Therefore the identity (4) means

\[
0 = -N_{KB_n/B_n}(\varepsilon_{0,n}) + \sum_{i=1}^{4} N_{KB_n/K_iB_n}(\varepsilon_{0,n}).
\]

Let us fix \( n \geq 2 \). By abuse of notation, we shall denote the restriction of \( \psi \) to \( KB_n \) again by \( \psi \). We shall apply

\[
\tau = (1 - \psi^{2 \cdot 3^{n-1}}) \sum_{r=0}^{3^{n-2}-1} \psi^{3r} \in \mathbb{Z}[\text{Gal}(KB_n/K)]
\]

on (5). Since \( \psi^{3^n} = 1 \), we have

\[
\tau(1 - \psi^3) = (1 - \psi^{2 \cdot 3^{n-1}})(1 - \psi^{3^{n-1}}) = 3 - (1 + \psi^{3^{n-1}} + \psi^{2 \cdot 3^{n-1}}).
\]

It is easy to see that \( 1 + \psi^{3^{n-1}} + \psi^{2 \cdot 3^{n-1}} \) is the norm operator of \( KB_n/KB_{n-1} \). Using (6) and the norm relations (2) and (1) we obtain

\[
\tau N_{KB_n/K_iB_n}(\varepsilon_{0,n}) = \tau(1 - \text{Frob}(q_1)^{-1})\varepsilon_{1,n} = \tau(1 - \psi^3)\varepsilon_{1,n} = 3\varepsilon_{1,n} - N_{KB_n/KB_{n-1}}(\varepsilon_{1,n}) = -\varepsilon_{1,n-1}.
\]
Similarly, for any $i = 2, 3, 4$ using (2) we have

$$\tau N_{KB_n/K_i B_n}(\varepsilon_{0,n}) = \tau(1 - \operatorname{Frob}(q_{2i-1})^{-1})(1 - \operatorname{Frob}(q_{2i-2})^{-1})\varepsilon_{i,n}$$

$$= \tau(1 - \psi^{3\alpha_{2i-1}})(1 - \psi^{3\alpha_{2i-2}})\varepsilon_{i,n}.$$ 

Let $\alpha_j^{(n)}$ be a positive integer satisfying $\alpha_j^{(n)} \equiv \alpha_j \pmod{3^n \mathbb{Z}}$. Then

$$\tau N_{KB_n/K_i B_n}(\varepsilon_{0,n}) = \tau(1 - \psi^{3\alpha_{2i-1}^{(n)}})(1 - \psi^{3\alpha_{2i-2}^{(n)}})\varepsilon_{i,n}$$

$$= \tau(1 - \psi^3)\alpha_{2i-1}^{(n)}(1 - \psi^{3\alpha_{2i-2}^{(n)}})\varepsilon_{i,n},$$

where

$$\alpha_{2i-1}^{(n)} = \sum_{r=0}^{a_i^{(n)} - 1} \psi^{3r},$$

and (6) and (1) give

$$\tau N_{KB_n/K_i B_n}(\varepsilon_{0,n}) = -\alpha_{2i-1}^{(n)}(1 - \psi^{3\alpha_{2i-2}^{(n)}})N_{KB_n/K_{n-1}}(\varepsilon_{i,n})$$

$$= -\alpha_{2i-1}^{(n)}(1 - \psi^{3\alpha_{2i-2}^{(n)}})\varepsilon_{i,n-1}.$$ 

A similar computation gives

$$\tau N_{KB_n/B_n}(\varepsilon_{0,n}) = \tau \left( \prod_{i=1}^{7}(1 - \psi^{3\alpha_i^{(n)}}) \right)\varepsilon_{5,n} = -\left( \prod_{i=2}^{7}(1 - \psi^{3\alpha_i^{(n)}}) \right)\varepsilon_{5,n-1}.$$ 

Putting (5), (7), (8), and (9) together, we obtain

$$\varepsilon_{1,n-1} + \sum_{i=2}^{4} \alpha_{2i-1}^{(n)}(1 - \psi^{3\alpha_{2i-2}^{(n)}})\varepsilon_{i,n-1} - \left( \prod_{i=2}^{7}(1 - \psi^{3\alpha_i^{(n)}}) \right)\varepsilon_{5,n-1} = 0.$$ 

This equality in $C(KB_n)/(C(KB_n))^3$ means that there is $\eta_{n-1} \in C(KB_n)$ such that

$$\eta_{n-1}^3 = \varepsilon_{1,n-1} \cdot \left( \prod_{i=2}^{4} \varepsilon_{i,n-1}^{(n)}(1 - \psi^{3\alpha_{2i-2}^{(n)}}) \right) \cdot \varepsilon_{5,n-1}^7(1 - \psi^{3\alpha_i^{(n)}}).$$

Since $KB_n$ is a real abelian field, $\eta_{n-1}$ is uniquely determined by the previous identity. It is easy to see that $\eta_{n-1}^3 \in C(KB_{n-1})$, so $\eta_{n-1}^3 \in KB_{n-1}$. Since $KB_n/\mathbb{Q}$ is abelian, we have $\eta_{n-1} \in KB_{n-1}$, hence $\eta_{n-1} \in \mathbb{Q}(3^n f_0)$. On the other hand $\eta_{n-1} \in C(KB_n)$ implies $\eta_{n-1} \in C(Q(3^n f_0)).$ But for cyclotomic fields, the Sinnott groups of circular units satisfy the Galois descent (see [GK]), so

$$\eta_{n-1} \in \mathbb{Q}(3^n f_0) \cap C(Q(3^n f_0)) = C(Q(3^n f_0)).$$

This means $\eta_{n-1} \in \overline{C}(KB_{n-1}).$
Since \( a_j^{(n)} \equiv a_j^{(n+1)} \pmod{3^n} \), we have

\[
\varepsilon_i^{1-\psi^{3a_j^{(n)}}} = \varepsilon_i^{1-\psi^{3a_j^{(n+1)}}}.
\]

It is easy to see that for any positive integers \( a \) and \( b \)

\[
(1 - \psi^{3a}) \sum_{r=0}^{b-1} \psi^{3r} = (1 - \psi^3) \left( \sum_{s=0}^{a-1} \psi^{3s} \right) \sum_{r=0}^{b-1} \psi^{3r} = (1 - \psi^{3b}) \sum_{r=0}^{a-1} \psi^{3r}.
\]

Using the previous identities we can easily prove that the numbers \( a_j^{(n)} \) can be replaced by \( a_j^{(n+1)} \) in (10). Using (1) this implies that

\[
N_{KB_n/KB_{n-1}}(\eta_n^3) = \eta_n^3 - 1,
\]

so

\[
N_{KB_n/KB_{n-1}}(\eta_n) = \eta_n - 1.
\]

Denoting \( \eta_0 = N_{KB_1/K}(\eta_1) \), we have proved

\[
\eta = (\eta_n)_{n=0}^{\infty} \in \varprojlim C(KB_n).
\]

But \( \eta^3 \in C(KB_n) \), so \( \eta^3 \in \varprojlim C(KB_n) \). To show that \( \eta \notin \varprojlim C(KB_n) \), it is enough to prove that \( \eta_1 \notin C(KB_1) \). For this purpose we shall describe a basis of \( C(KB_1) \).

**Lemma 2.** There is a basis of \( C(KB_1) \) consisting of

(i) 4 conjugates of each of the units \( \varepsilon_{1,1}, \varepsilon_{2,1}, \varepsilon_{3,1}, \) and \( \varepsilon_{4,1} \),

and

(ii) of 2 conjugates of each of the units \( \varepsilon_{1,0}, \varepsilon_{2,0}, \varepsilon_{3,0}, \varepsilon_{4,0}, \) and \( \varepsilon_{5,1} \).

**Proof.** Since

\[
\text{rank}_\mathbb{Z} C(KB_1) = \text{rank}_\mathbb{Z} E(KB_1) = [KB_1 : \mathbb{Q}] - 1 = 26,
\]

which is the number of units mentioned in the lemma, it is enough to show that they together with \(-1\) generate \( C(KB_1) \). We have chosen the primes \( q_1, \ldots, q_7 \) in such a way that all automorphisms Frob\((q_1), \ldots, q_7\) act trivially on \( KB_1 \). Hence relations (4) and (2) for \( n = 0, 1 \) give \( \varepsilon_{0,n}^3 = 1 \), so \( \varepsilon_{0,0} = \varepsilon_{0,1} = 1 \). Because \( \varepsilon_{5,0} = -1 \), Lemma 1 gives that the multiplicative group, generated by \(-1\) and by all conjugates of units mentioned in the lemma, equals \( C(KB_1) \).

Let us fix any \( i = \{1,2,3,4\} \) and consider \( \varepsilon_{i,1} \in K_i B_1 \). The Galois groups \( \text{Gal}(K_i B_1/K_i) \) and \( \text{Gal}(K_i B_1/B_1) \) are groups of order 3; let \( \mu \) and \( \nu \) be their generators, respectively. Then \( \mu \) and \( \nu \) generate \( \text{Gal}(K_i B_1/\mathbb{Q}) \), so \( \varepsilon_{i,1}^{\mu^r \nu^s} \), with \( r, s = 0, 1, 2 \), is the system of all conjugates of \( \varepsilon_{i,1} \). Using the trivial action of Frobenius automorphisms, (2) implies

\[
\varepsilon_{i,1}^{1+\mu+\nu^2} = N_{K_i B_1/B_1}(\varepsilon_{i,1}) = \varepsilon_{5,1}^{1 - \text{Frob}(q_i)^{-1}} = 1.
\]
Similarly, (3) gives
\[ \varepsilon_{i,1}^{1+\mu+\nu^2} = N_{K_i:B_i/K_i}(\varepsilon_{i,1}) = \varepsilon_{i,0}^{1-\text{Prob}(3)^{-1}}. \]

Therefore all conjugates of \( \varepsilon_{i,1} \) are generated by the four conjugates \( \varepsilon_{i,1}^{r+s} \), with \( r, s = 0, 1 \), and by all three conjugates of \( \varepsilon_{i,0} \).

Similarly, one can show that each of the units \( \varepsilon_{1,0}, \varepsilon_{2,0}, \varepsilon_{3,0}, \varepsilon_{4,0}, \) and \( \varepsilon_{5,1} \) has precisely three conjugates and the product of them (i.e., its absolute norm) equals one. The lemma follows.

Since \( \psi^3 \) acts trivially on \( KB_1 \), equality (10) gives \( \eta_1^3 = \varepsilon_{1,1} \). But Lemma 2 shows that \( \varepsilon_{1,1} \) is not a cube in \( C(KB_1) \), hence \( \eta_1 \notin C(KB_1) \), which gives \( \eta \notin \lim C(KB_n) \).

The theorem will be proved, if we show that there exist primes \( q_1, \ldots, q_7 \) satisfying all assumptions made in the first sentence of Notation. But this can be done either by a standard technique using Tchebotarev density theorem (e.g., see Theorem 3.1 in [R]) or just by checking that primes
\[
\begin{align*}
p_1 &= 19, \quad p_2 = 487, \quad p_3 = 4591, \quad p_4 = 65557, \\
p_5 &= 186391, \quad p_6 = 675253, \quad p_7 = 1414207
\end{align*}
\]
satisfy all these assumptions.

References


Radan Kučera
Department of Mathematics
Masaryk University
Janáčkovo nám. 2a
662 95 Brno
Czech Republic
E-mail: kucera@math.muni.cz