On $\pi$-adic expansion of singular integers of the $p$-cyclotomic field

Roland Quême

2006 nov 12

Abstract

Let $p$ be an odd prime. Let $K = \mathbb{Q}(\zeta)$ be the $p$-cyclotomic field and let $O_K$ be the ring of integers of $K$. Let $\pi$ be the prime ideal of $K$ lying over $p$. An integer $B \in O_K$ is said singular if $B^{1/p} \not\in K$ and if $BO_K = b^p$ where $b$ is an ideal of $O_K$. An integer $B \in O_K$ is said semi-primary if $B \equiv b \mod \pi^2$ where $b \in \mathbb{Z}$, $b \not\equiv 0 \mod p$. Let $\sigma$ be a $\mathbb{Q}$-isomorphism of the field $K$ generating the Galois group $\text{Gal}(K/\mathbb{Q})$. When $p$ is irregular, there exists at least one subgroup $\Gamma$ of order $p$ of the class group of $K$ annihilated by a polynomial $\sigma - \mu$ with $\mu \in \mathbb{F}_p^*$. We prove the existence, for each $\Gamma$, of singular semi-primary integers $B$ where $BO_K = b^p$ with class $\text{Cl}(b) \in \Gamma$ and $B^{\sigma - \mu} \in K^p$ and we describe their $\pi$-adic expansion. This paper is at a strictly elementary level.

1 Some definitions on cyclotomic fields

In this section, we fix some definitions and notations and remind reader of some classical properties of cyclotomic fields used in the article.

1. Let $p$ be an odd prime. Let $K = \mathbb{Q}(\zeta)$ be the $p$-cyclotomic number field. Let $O_K = \mathbb{Z}[\zeta]$ be the ring of integers of $K$. Let $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ be the maximal totally real subfield of $K$. The ring of integers of $K^+$ is $O_{K^+} = \mathbb{Z}[\zeta + \zeta^{-1}]$. Let us denote $O_{K^+}^*$ the group of units of $O_{K^+}$. Let $\mathbb{F}_p$ be the finite field with $p$ elements and $\mathbb{F}_p^*$ its multiplicative group.

2. Let us denote $a$ the ideals of $O_K$ and $\text{Cl}(a)$ their classes in the class group of $K$. Let us denote $< \text{Cl}(a) >$ the finite group generated by the class $\text{Cl}(a)$. If $a \in O_K$ then $aO_K$ is the principal ideal of $O_K$ generated by $a$. The ideal $pO_K = \pi^{p-1}$ where $\pi$ is the principal prime ideal $(1 - \zeta)O_K$. Let us denote $\lambda = \zeta - 1$, so $\pi = \lambda O_K$. 

1
3. Let \( G = \text{Gal}(K/\mathbb{Q}) \) be the Galois group of the field \( K \). Let \( \sigma \) be a \( K \)-isomorphism generating the cyclic group \( G \). \( \sigma \) is defined by \( \sigma(\zeta) = \zeta^u \) where \( u \) is a primitive root \( \mod p \).

4. For this primitive root \( u \mod p \) and \( i \in \mathbb{N} \), let us denote \( u_i \equiv u^i \mod p \), \( 1 \leq u_i \leq p - 1 \). For \( i \in \mathbb{Z} \), \( i < 0 \), this is to be understood as \( u_i u^{-i} \equiv 1 \mod p \).

This notation follows the convention adopted in Ribenboim [3], last paragraph of page 118. This notation is largely used in the sequel of this article.

5. Let \( C_p, C_p^+ \) be the subgroups of exponent \( p \) of the class groups of the field \( K \) and \( K^+ \). Then \( C_p = C_p^+ \oplus C_p^- \) where \( C_p^- \) is the relative \( p \)-class group \( C_p/C_p^+ \).

Let \( r \) be the rank of the groups \( C_p \). The abelian group \( C_p \) is a group of order \( p^r \) with

\[
C_p = \bigoplus_{i=1}^{r} \Gamma_i,
\]

where each \( \Gamma_i \) is a cyclic groups of order \( p \) annihilated by \( \sigma - \mu_i \) with \( \mu_i \in \mathbb{F}_p^* \).

6. Similarly the \( p \)-unit group \( U = O_{K+}^*/O_{K+}^{p} \) is a direct sum

\[
U = \bigoplus_{i=1}^{(p-3)/2} U_i,
\]

where \( U_i = \langle \eta_i \rangle \) is a cyclic group of order \( p \) with \( \eta_i^{\sigma - \mu_i} \in O_{K+}^{p} \) and where \( \mu_i = u_{2m_i} \mod p \) with \( 1 \leq m_i \leq \frac{p-3}{2} \).

7. We say that an algebraic number \( C \in K \) is singular if \( C^{1/p} \notin K \) and \( CO_K = e^p \) for some ideal \( e \) of \( K \). If \( C \) is integer then \( C \) is called a singular integer. Observe that with this definition a unit is a singular integer. We say that \( C \) is singular primary if \( C \) is singular and \( C \equiv e^p \mod \pi^p \), \( c \in \mathbb{Z} \), \( c \neq 0 \mod p \). We say that the singular number \( C \) is semi-primary if \( C \equiv c \mod \pi^{2} \), \( c \in \mathbb{Z} \), \( c \neq 0 \mod p \). Observe that if \( C \) is primary then \( C \) is semi-primary.

8. When \( p \) is irregular, there exists at least one subgroup \( \Gamma \) of order \( p \) of the class group of \( K \) annihilated by a polynomial \( \sigma - \mu \) with \( \mu \in \mathbb{F}_p^* \). In this article we prove, for each \( \Gamma \), the existence of singular semi-primary integers \( B \) where \( BO_K = b^p \) with class \( Cl(b) \in \Gamma \) and \( B^{\sigma - \mu} \in K^p \) and we describe their \( \pi \)-adic expansion.

2 On \( \pi \)-adic expansion of singular integers

In this section we consider the singular integers \( B \) with \( BO_K = b^p \) where \( Cl(b) \) is annihilated by \( \sigma - \mu \) for one \( \mu \in \mathbb{F}_p^* \). The singular integer \( B \) is said respectively negative when \( Cl(b) \in C_p^- \) and positive when \( Cl(b) \in C_p^+ \). Observe that \( \mu^{(p-1)/2} \equiv -1 \mod p \) when \( Cl(b) \in C_p^- \) and that \( \mu^{(p-1)/2} \equiv 1 \mod p \) when \( Cl(b) \in C_p^+ \).
2.1 $\pi$-adic expansion of singular negative integers

At first, we give a general lemma dealing with congruences on $p$-powers of algebraic numbers of $K$.

**Lemma 2.1.** Let $\alpha, \beta \in O_K$ with $\alpha \neq 0 \mod \pi$ and $\alpha \equiv \beta \mod \pi$. Then $\alpha^p \equiv \beta^p \mod \pi^{p+1}$.

**Proof.** Let $\lambda = (\zeta - 1)$. Then $\alpha - \beta \equiv 0 \mod \pi$ implies that $\alpha - \zeta^k \beta \equiv 0 \mod \pi$ for $k = 0, 1, \ldots, p-1$. Therefore, for all $k$, $0 \leq k \leq p-1$, there exists $a_k \in \mathbb{N}$, $0 \leq a_k \leq p-1$, such that $(\alpha - \zeta^k \beta) \equiv \lambda a_k \mod \pi^2$. For another value $l$, $0 \leq l \leq p-1$, we have, in the same way, $(\alpha - \zeta^l \beta) \equiv \lambda a_l \mod \pi^2$, hence $(\zeta^k - \zeta^l)\beta \equiv \lambda(a_k - a_l) \mod \pi^2$.

For $k \neq l$ we get $a_k \neq a_l$, because $\pi ||(\zeta^k - \zeta^l)$ and because hypothesis $\alpha \equiv 0 \mod \pi$ implies that $\beta \equiv 0 \mod \pi$. Therefore, there exists one and only one $k$ such that $(\alpha - \zeta^k \beta) \equiv 0 \mod \pi^2$. Then, we have $\prod_{k=0}^{p-1}(\alpha - \zeta^k \beta) = (\alpha^p - \beta^p) \equiv 0 \mod \pi^{p+1}$. □

**Lemma 2.2.** Let $b$ be an ideal of $O_K$ such that $Cl(b) \in C^-_p$ is annihilated by $\sigma - \mu$. There exist singular semi-primary negative integers $B$ with $BO_K = b^p$. They verify the relation

$$
\left(\frac{B}{B}\right)^{\sigma-\mu} = \left(\frac{\alpha}{\alpha}\right)^p, \quad \alpha \in K.
$$

**Proof.** The ideal $b^p$ is principal. So let one $\beta \in \mathbb{Z}[\zeta]$ with $\beta O_K = b^p$. There exists a natural number $w$ such that the integer $B = \beta \zeta^w$ is semi-primary. $b^{\sigma-\mu}$ is principal, therefore there exists $\alpha \in K$ such that $\sigma(b) = b^\mu \alpha O_K$, thus there exists a natural number $w'$ with

$$
\sigma(B) = B^\mu \eta^w \alpha^p, \quad \eta \in O_{K^+}, \quad w' \in \mathbb{Z}.
$$

$B$ is semi-primary, hence $\sigma(B)$ is semi-primary. $\eta$ and $\alpha^p$ are semi-primary, hence $w' = 0$. Then $\sigma(B) = B^\mu \eta^w \alpha^p$ and by conjugation $\sigma(B) = \overline{B^{\mu}} \eta^{\overline{w}} \alpha^p$ and the result follows. □

**Lemma 2.3.** The singular semi-primary negative integer $B$ defined in previous lemma verifies $\mu = u_{2m+1}$ for a natural integer $m$, $1 \leq m \leq \frac{p-3}{2}$. If the singular number $C = \frac{B}{B}$ is non-primary then $\pi^{2m+1} \parallel C - 1$.

**Proof.**

1. $Cl(b) \in C^-_p$, hence $\mu^{(p-1)/2} \equiv -1 \mod p$, thus $\mu = u_{2m+1}$ for a natural number $m$, $0 \leq m \leq \frac{p-3}{2}$. From Stickelberger theorem $\sigma - u$ does not annihilate $Cl(b)$, hence $m \neq 0$. 

3
2. The definition of \( C \) implies that \( C \equiv 1 \mod \pi \). Observe that \( v_\pi(C-1) \) is odd because \( C \overline{C} = 1 \). Therefore the hypothesis \( C \) non-primary implies that \( v_\pi(C-1) \leq p-2 \). There exists a natural integer \( \nu \) such that \( \pi^\nu \parallel C-1 \), hence

\[
C \equiv 1 + c_0 \lambda^\nu \mod \lambda^{\nu+1}, \; \nu \leq p-2,
\]

\[
c_0 \in \mathbb{Z}, \; c_0 \neq 0 \mod p.
\]

We have to prove that \( \nu \leq p-2 \) implies that \( \nu = 2m+1 \):

3. From lemma 2.2 it follows that \( \sigma(C) = C^\mu \times \alpha_1^p \), with \( \alpha_1 = \frac{a}{2} \), and so that \( 1 + c_0 \sigma(\lambda)^\nu \equiv (1 + \mu c_0 \lambda^\nu) \times \alpha_1^p \mod \pi^{\nu+1} \). In the other hand \( \alpha_1 \equiv 1 \mod \pi \) and then, from lemma 2.1 \( \alpha_1^p \equiv 1 \mod \pi^{\nu+1} \). Then \( 1 + c_0 \sigma(\lambda)^\nu \equiv 1 + \mu c_0 \lambda^\nu \mod \lambda^{\nu+1} \), and so \( \sigma(\lambda^\nu) \equiv \mu \lambda^\nu \mod \pi^{\nu+1} \). This implies that \( \sigma(\zeta-1)^\nu \equiv \mu \lambda^\nu \mod \pi^{\nu+1} \), so that \( (\zeta^u - 1)^\nu \equiv \mu \lambda^\nu \mod \pi^{\nu+1} \), so that \( (\lambda + 1)^u - 1)^\nu \equiv \mu \lambda^\nu \mod \pi^{\nu+1} \) and finally \( u^\nu \lambda^\nu \equiv \mu \lambda^\nu \mod \pi^{\nu+1} \), hence \( u^\nu - \mu \equiv 0 \mod \pi \).

Therefore, we have proved that \( \nu = 2m+1 \).

\[
\Box
\]

In this theorem we generalize to singular integers \( B \) the results obtained for singular numbers \( C \) in lemma 2.2 and 2.3.

**Theorem 2.4.** Let \( B \) be a singular semi-primary negative integer. There exist a unit \( \eta \in O_{K^+}^* \) given by \( B \overline{B} = \eta \times \beta^p \), \( \beta \in O_K \), and a singular negative integer \( B' = \frac{B^2}{\eta} \) such that

\[
\sigma(B') = B'^\mu \times \alpha'^p, \; \alpha' \in K,
\]

If \( B' \) is non-primary then \( \pi^{2m+1} \parallel (B')^{p-1} - 1 \).

**Proof.** From lemma 2.2 we have \( (\frac{B}{\overline{B}})^{\sigma-\mu} = (\frac{a}{b})^p \). \( Cl(b) \in C^{-}_p \) implies that \( b \overline{B} \) is principal and so that \( B \overline{B} = \eta \beta^p \) with \( \beta \in O_K \) and \( \eta \in O_{K^+}^* \). Therefore

\[
\left( \frac{B^2}{\eta} \right)^{\sigma-\mu} = \left( \frac{B^2}{B \overline{B}} \right)^{\sigma-\mu} = \left( B \times \beta^p \right)^{\sigma-\mu} = \left( \frac{\alpha}{\alpha} \times \beta^{\sigma-\mu} \right)^p.
\]

Let us denote \( B' = \frac{B^2}{\eta}, \; B' \in O_K, \; v_\pi(B') = 0 \). We get

\[
\sigma(B') = (B')^\mu \times \alpha'^p, \; \alpha' \in K.
\]

This relation leads to

\[
\sigma(B')^{p-1} \equiv (B')^{(p-1)\mu} \mod \pi^{p+1}.
\]
If $B'$ is non-primary then it leads in the same way than in lemma 2.3 p. 3 to the congruence

$$\pi^{2m+1} \parallel (B')^{p-1} - 1,$$

which achieves the proof.

**Remark:** If $B$ is singular primary then $\eta = 1$ from a theorem of Furtwangler, see Ribenboim [3] (6C) p. 182.

**The case $\mu = u_{2m+1}$ with $2m + 1 > \frac{p-1}{2}$**

Let us consider the singular number $C$ defined in lemma 2.3 p. 3. The number $C$ can be written in the form

$$C = 1 + \gamma + \gamma_0 \zeta + \gamma_1 \zeta^u + \ldots + \gamma_{p-3} \zeta^{u_{p-3}},$$

$\gamma \in \mathbb{Q}, \quad v_p(\gamma) \geq 0, \quad \gamma_i \in \mathbb{Q}, \quad v_p(\gamma_i) \geq 0, \quad i = 0, \ldots, p-3,$

$$\gamma + \gamma_0 \zeta + \gamma_1 \zeta^u + \ldots + \gamma_{p-3} \zeta^{u_{p-3}} \equiv 0 \mod \pi^{2m+1}.$$

In the theorem 2.6 p. 6, we shall compute the coefficients $\gamma$ and $\gamma_i \mod p$.

**Lemma 2.5.** $C$ verifies the congruences

$$\gamma \equiv -\frac{\gamma_{p-3}}{\mu - 1} \mod p,$$

$$\gamma_0 \equiv -\mu^{-1} \times \gamma_{p-3} \mod p,$$

$$\gamma_1 \equiv -(\mu^{-2} + \mu^{-1}) \times \gamma_{p-3} \mod p,$$

$$\vdots$$

$$\gamma_{p-4} \equiv -(\mu^{-(p-3)} + \ldots + \mu^{-1}) \times \gamma_{p-3} \mod p.$$

**Proof.** We have seen in lemma 2.2 p. 3 that $\sigma(C) \equiv C^\mu \mod \pi^{p+1}$. From $2m+1 > \frac{p-1}{2}$ we derive that

$$C^\mu \equiv 1 + \mu \times (\gamma + \gamma_0 \zeta + \gamma_1 \zeta^u + \ldots + \gamma_{p-3} \zeta^{u_{p-3}}) \mod \pi^{p-1}.$$

In the other hand, we get by conjugation

$$\sigma(C) = 1 + \gamma + \gamma_0 \zeta^u + \gamma_1 \zeta^u^2 + \ldots + \gamma_{p-3} \zeta^{u_{p-2}}.$$

We have the identity

$$\gamma_{p-3} \zeta^{u_{p-2}} = -\gamma_{p-3} - \gamma_{p-3} \zeta - \ldots - \gamma_{p-3} \zeta^{u_{p-3}}.$$
This leads to

$$\sigma(C) = 1 + \gamma - \gamma_{p-3} - \gamma_{p-3} \zeta + (\gamma_0 - \gamma_{p-3}) \zeta^u + \cdots + (\gamma_{p-4} - \gamma_{p-3}) \zeta^{u_{p-3}}.$$  

Therefore, from the congruence $\sigma(C) \equiv C^\mu \mod \pi^{p+1}$ we get the congruences in the basis $1, \zeta, \zeta^u, \ldots, \zeta^{u_{p-3}},$

$$1 + \mu \gamma \equiv 1 + \gamma - \gamma_{p-3} \mod p,$$

$$\mu \gamma_0 \equiv -\gamma_{p-3} \mod p,$$

$$\mu \gamma_1 \equiv \gamma_0 - \gamma_{p-3} \mod p,$$

$$\mu \gamma_2 \equiv \gamma_1 - \gamma_{p-3} \mod p,$$

$$\vdots$$

$$\mu \gamma_{p-4} \equiv \gamma_{p-5} - \gamma_{p-3} \mod p,$$

$$\mu \gamma_{p-3} \equiv \gamma_{p-4} - \gamma_{p-3} \mod p.$$  

From these congruences, we get $\gamma \equiv -\frac{2p-3}{\mu-1} \mod p$ and $\gamma_0 \equiv -\mu^{-1} \gamma_{p-3} \mod p$ and then $\gamma_1 \equiv \mu^{-1} (\gamma_0 - \gamma_{p-3}) \equiv \mu^{-1} (-\mu^{-1} \gamma_{p-3} - \gamma_{p-3}) \equiv -(\mu^{-2} + \mu^{-1}) \gamma_{p-3} \mod p$ and $\gamma_2 \equiv \mu^{-1} (\gamma_1 - \gamma_{p-3}) \equiv \mu^{-1} (-\mu^{-2} + \mu^{-1}) \gamma_{p-3} - \gamma_{p-3}) \equiv -(\mu^{-3} + \mu^{-2} + \mu^{-1}) \gamma_{p-3} \mod p$ and so on.

Theorem 2.6. If $2m + 1 > \frac{p-1}{2}$ then $C$ verifies the congruence

$$C \equiv 1 - \delta \times (\zeta + \mu^{-1} \zeta^u + \cdots + \mu^{-(p-2)} \zeta^{u_{p-2}}) \mod \pi^{p-1},$$

where $\delta \in \mathbb{Z}$ is coprime with $p$ when $C$ is non-primary.

Proof. The result is trivial if $C$ is primary. Suppose that $C$ is not primary. From definition of $C$, setting $C = 1 + V$, we get :

$$C = 1 + V,$$

$$V = \gamma + \gamma_0 \zeta + \gamma_1 \zeta^u + \cdots + \gamma_{p-3} \zeta^{u_{p-3}},$$

$$\sigma(V) \equiv \mu \times V \mod \pi^{p+1}.$$  

Then, from lemma 2.5 p. 5, observing that $\mu^{-(p-2)} + \cdots + \mu^{-1} \equiv -1 \mod p$, we
obtain the relations

\[ \mu = u_{2m+1}, \]
\[ \gamma \equiv -\frac{\gamma_{p-3}}{\mu - 1} \mod p, \]
\[ \gamma_0 \equiv -\mu^{-1} \times \gamma_{p-3} \mod p, \]
\[ \gamma_1 \equiv -(\mu^{-2} + \mu^{-1}) \times \gamma_{p-3} \mod p, \]
\[ \vdots \]
\[ \gamma_{p-4} \equiv - (\mu^{-2} + \cdots + \mu^{-1}) \times \gamma_{p-3} \mod p, \]
\[ \gamma_{p-3} \equiv - (\mu^{-2} + \cdots + \mu^{-1}) \times \gamma_{p-3} \mod p. \]

From these relations we get

\[ V \equiv -\gamma_{p-3} \times \left( \frac{1}{\mu - 1} + \mu^{-1} \zeta + (\mu^{-2} + \mu^{-1}) \zeta u + \cdots + (\mu^{-2} + \cdots + \mu^{-1}) \zeta u_{p-3} \right) \mod p, \]

hence

\[ V \equiv -\gamma_{p-3} \times \left( \frac{1}{\mu - 1} + \mu^{-1} \left( \frac{\mu^{-1} \zeta + (\mu^{-2} - 1) \zeta u + \cdots + (\mu^{-2} - 1) \zeta u_{p-3}}{\mu^{-1} - 1} \right) \right) \mod p, \]

hence

\[ V \equiv -\gamma_{p-3} \times \left( \frac{1}{\mu - 1} + \mu^{-1} \left( \frac{\mu^{-1} \zeta + \mu^{-2} \zeta u + \cdots + \mu^{-2} \zeta u_{p-3} - \zeta - \zeta u - \cdots - \zeta u_{p-3}}{\mu^{-1} - 1} \right) \right) \mod p. \]

In the other hand \(-\zeta - \zeta u - \cdots - \zeta u_{p-3} = 1 + \zeta u_{p-3}\) and \(\mu^{-1} \equiv 1 \mod p\) implies that

\[ V \equiv -\gamma_{p-3} \times \left( \frac{1}{\mu - 1} + \mu^{-1} \left( \frac{1 + \mu^{-1} \zeta + \mu^{-2} \zeta u + \cdots + \mu^{-2} \zeta u_{p-3} + \mu^{-1} \zeta u_{p-2}}{\mu^{-1} - 1} \right) \right) \mod p, \]

hence

\[ V \equiv -\gamma_{p-3} \times \left( \frac{\mu^{-1}}{\mu - 1} \right) \times \left( 1 - (1 + \mu^{-1} \zeta + \mu^{-2} \zeta u + \cdots + \mu^{-2} \zeta u_{p-3} + \mu^{-1} \zeta u_{p-2}) \right) \mod p, \]

hence

\[ V \equiv -\gamma_{p-3} \times \left( \frac{\mu^{-1}}{\mu - 1} \right) \times (\zeta + \mu^{-1} \zeta u + \cdots + \mu^{-1} \zeta u_{p-3} + \mu^{-1} \zeta u_{p-2}) \mod p, \]

which achieves the proof.
Remark: we have a similar result with $(B')^{p-1}$ in place of $C$.

2.2 $\pi$-adic expansion of singular positive integers

Let $b$ be an ideal of $O_K$ whose class $Cl(q) \in C_p^+$ is annihilated by $\sigma - \mu$. In that case $\mu^{(p-1)/2} \equiv 1 \mod p$ and $\mu = u_2 m \mod p$, $1 \leq m \leq \frac{p-3}{2}$.

Theorem 2.7.

1. There exists singular semi-primary positive integers $B \in O_K$ such that:

\[ BO_K = b^p, \]
\[ \sigma(B) = B^\mu \times \alpha^p, \quad \alpha \in K, \]

2. If $B$ is non-primary then $\pi^{2m} \parallel B^{p-1} - 1$.

Proof. There exists semi-primary integers $B'$ with $B'O_K = b^p$ such that

\[ \sigma(B') = B'^\mu \times \alpha^p \times \eta, \quad \alpha \in K, \quad \eta \in O_{K^+}^*. \]

From independent forward theorem 3.1 p. 10 dealing with unit group $O_{K^+}^*$, the unit $\eta$ verifies the relation

\[ \eta = \eta_1^l_1 \times \left( \prod_{j=2}^N \eta_j^{l_j} \right), \quad l_j \in \mathbb{F}_p, \quad 1 \leq N < \frac{p^3 - 3}{2}, \]

\[ \sigma(\eta_1) = \eta_1^\mu \times \beta_1^p, \quad \eta_1, \beta_1 \in O_{K^+}^*, \]
\[ \sigma(\eta_j) = \eta_j^{\nu_j} \times \beta_j^p, \quad \eta_j, \beta_j \in O_{K^+}^*, \quad j = 2, \ldots, N, \]

where $\nu_j \neq \nu_{j'}$ for $2 \leq j < j' \leq N$ and $\nu_j \neq \mu$ for $j = 2, \ldots, N$. Let us denote $E = \eta_1^l_1$ and $U = \prod_{j=2}^N \eta_j^{l_j}$, hence $\eta = EU$. Show that there exists $V \in O_{K^+}^*$ of form $V = \prod_{j=2}^N \eta_j^{\rho_j}$ such that

\[ \sigma(V) \times V^{-\mu} = U^{-1} \times \varepsilon^p, \quad \varepsilon \in O_{K^+}^* \]

It is sufficient that

\[ \eta_j^{\rho_j \nu_j} \times \eta_j^{-\rho_j \mu} = \eta_j^{-l_j} \times \varepsilon_j^p, \quad \varepsilon_j \in O_{K^+}^*, \quad j = 2, \ldots, N, \]

hence that

\[ \rho_j \equiv \frac{-l_j}{\nu_j - \mu} \mod p, \quad j = 2, \ldots, N, \]
which is possible, because \( \nu_j \neq \mu, \quad j = 2, \ldots, N \). Therefore, for \( B = B' \times V \), we get
\[
B' = BV^{-1}
\]
and so
\[
\sigma(B') = \sigma(BV^{-1}) = B'^{\mu} \alpha^p \eta = (BV^{-1})^{\mu} \alpha^p \eta = (BV^{-1})^{\mu} \times \alpha^p \times E \times U,
\]
hence
\[
\sigma(B) = B^\mu \sigma(V)V^{-\mu} \times \alpha^p \times E \times U.
\]
From relation (12) we get
\[
\sigma(B) = B^\mu (U^{-1} \epsilon^p \times \alpha^p \times E \times U),
\]
hence we get the two simultaneous relations
\[
\begin{align*}
\sigma(B) &= B^\mu \times \alpha^p \times \epsilon^p \times E, \quad \alpha \in K, \\
\sigma(E) &= E^\mu \times \epsilon_1^p, \quad \epsilon_1 \in O_{K^+}^+.
\end{align*}
\]
(13)

Show that
\[
B^{\sigma - \mu} \in K^p.
\]
1. If \( E \in O_{K^+}^{sp} \), it is clear from relation (13).
2. If \( E \notin O_{K^+}^{sp} \)

\[
\sigma(B) = B^\mu \times \alpha_1^p \times E, \quad \alpha_1 \in K,
\]
(15)

hence raising (15) to \( \mu \)-power we get
\[
\sigma(B)^{\mu} = B^{\mu^2} \times \alpha_1^{p \mu} \times E^\mu, \quad \alpha_1 \in K,
\]
(16)

and also applying \( \sigma \) to relation (15) we get
\[
\sigma^2(B) = \sigma(B)^{\mu} \times E^\mu \times b^p, \quad b \in K,
\]
(17)

Then, gathering these two relations (16) and (17) we get
\[
c^p B^\mu \sigma B^{-\mu^2} = B^{\sigma^2} B^{-\mu^2},
\]
thus
\[
B^{(\sigma - \mu)^2} = c^p, \quad c \in K.
\]

In the other hand \( B^{\sigma^p - 1} - 1 = 1 \). But in the euclidean field \( \mathbf{F}_p[X] \), we have \( \gcd((X^{p-1} - 1), (X - \mu)^2)) = X - \mu \). Therefore \( B^{\sigma - \mu} = \alpha_3^p \), \( \alpha_3 \in K \), and so
\[
\sigma(B) = B^\mu \times \alpha_3^p.
\]
The end of proof is similar to the proof of previous lemma [2.4] p. 4.

**Theorem 2.8.** Let $B$ be the singular positive number defined in theorem [2.7]. If $m > \frac{p-1}{4}$ then $B$ verifies the congruence $\mod p$:

\[(18) \quad B^{p-1} \equiv 1 - \delta \times (\zeta + \mu^{-1}\zeta^u + \ldots + \mu^{-(p-2)}\zeta^{u(p-2)}) \mod \pi^{p-1},\]

where $\delta \in \mathbb{Z}$ is coprime with $p$ when $B$ is non-primary.

**Proof.** If $B$ is primary then it results of definition of primary numbers. If $B$ is non-primary the proof is similar to theorem [2.6] proof.

## 3 On $\pi$-adic expansion of singular units

Let us fix $\eta$ for one of the units $\eta_i$ of definition relation [2]. The singular units $\eta$ verify $\eta^{p^\mu} \in O_{K+}^p$. Therefore the results on singular integers $B$ non-units of section [2] p. 2 can be translated \textit{mutatis mutandis} to get similar results for the unit $p$-group $U = O_{K+}^*/O_{K+}^p$:

**Theorem 3.1.** Let $m$ be a natural number $1 \leq m \leq m$. There exists singular units $\eta \in O_{K+}^*$ verifying $\sigma(\eta) = \eta^{\mu} \times \varepsilon^p$ with $\mu = u_{2m}$ and $\varepsilon \in O_{K+}^*$. If $\eta$ is non-primary then $\pi^{2m} \parallel \eta^{p^\mu} - 1$.

The case $\mu = u_{2m}$ with $2m > \frac{p-1}{2}$

The next theorem for the $p$-unit group $U = O_{K+}^*/O_{K+}^p$ is the translation of the similar theorem [2.6] p. 6 for the singular negative integers.

**Theorem 3.2.** Let $\mu = u_{2m}$, $p - 3 \geq 2m > \frac{p-1}{2}$. The singular units $\eta$ with $\eta^{p^\mu} \in O_{K+}^*$ verify the explicit congruence:

\[(19) \quad \eta^{p^\mu} \equiv 1 - \delta \times (\zeta + \mu^{-1}\zeta^u + \ldots + \mu^{-(p-2)}\zeta^{u(p-2)}) \mod \pi^{p-1},\]

where $\delta \in \mathbb{Z}$ is coprime with $p$ when $\eta$ is non-primary.

References

[1] K. Ireland, M. Rosen, \textit{A Classical Introduction to Modern Number Theory}, Springer-Verlag, 1982.

[2] P. Ribenboim, \textit{13 Lectures on Fermat’s Last Theorem}, Springer-Verlag, 1979.
[3] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

[4] L.C. Washington, *Introduction to cyclotomic fields*, Springer, 1996.

Roland Quême
13 avenue du château d’eau
31490 Brax
France
mailto: roland.queme@wanadoo.fr