π-adic approach of $p$-class group and unit group of $p$-cyclotomic fields

Roland Quême

2005 fev 04

Contents

1 Introduction 3
  1.1 Some π-adic congruences connected to $p$-class group of cyclotomic field $\mathbb{Q}(\zeta)$ 3
  1.2 Some π-adic congruences on $p$-unit group the cyclotomic field 5

2 Cyclotomic Fields : some definitions 7

3 π-adic congruences on $p$-subgroup $C_p$ of the class group of $\mathbb{Q}(\zeta)$ 9
  3.1 Some definitions and notations 9
  3.2 Representations of Galois group $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ in characteristic $p$ 10
  3.3 On the structure of the $p$-class group of subfields of $\mathbb{Q}(\zeta)$ 14
    3.3.1 Some definitions and notations 15
    3.3.2 On the irregularity index 16
    3.3.3 Inequalities involving degrees $r_1, r_d, r_p$ of minimal polynomials $P_{r_1}(V), P_{r_d}(V), P_{r_p}(V)$ annihilating ideal $b$ 17
    3.3.4 On Stickelberger’s ideal in field $\mathbb{Q}(\zeta)$ 18
  3.4 π-adic congruences connected to $p$-class group $C_p$ 19
    3.4.1 π-adic congruences connected to relative $p$-class group $C_p^c$ 19
    3.4.2 π-adic congruences connected to $p$-class group $C_p^+$ 27
    3.4.3 π-adic congruences connected to $p$-class group $C_p^c$ 29

4 On structure of the $p$-unit group of the cyclotomic field $\mathbb{Q}(\zeta)$ 34
  4.1 Definitions and preliminary results 34
  4.2 π-adic congruences on $p$-unit group $F$ of $\mathbb{Q}(\zeta)$ 36
Abstract

Roland Quême
13 avenue du château d’eau
31490 Brax
France
2005 fev 04
tel : 0033561067020
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/
Mathematical subject classification: Primary 11R18, Secondary 11R27, 11R29

Let $p > 2$ be a prime. Let $\mathbb{Q}(\zeta)$ be the $p$-cyclotomic field. Let $\mathbb{Q}(\zeta)^+$ be its maximal totally real subfield. Let $\pi$ be the prime ideal of $\mathbb{Q}(\zeta)$ lying over $p$. This article aims to describe some $\pi$-adic congruences characterising the structure of the $p$-class group and of the $p$-unit group of the fields $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta)^+$. For the unit group, this paper supplements the papers of Dénes of 1954 and 1956. A complete summarizing of the results obtained in the paper follows in the Introduction section from p. 3 to 6. This paper is at elementary level.
1 Introduction

Let $p > 2$ be a prime. Let $\mathbb{Q}(\zeta)$ be the $p$-cyclotomic fields. Let $\mathbb{Z}[\zeta]$ be the ring of integers of $\mathbb{Q}(\zeta)$. Let $\pi = (1 - \zeta)\mathbb{Z}[\zeta]$ be the prime ideal of $\mathbb{Q}(\zeta)$ lying over $p$. This monograph contains two parts:

1. a description of $\pi$-adic congruences strongly connected to $p$-class group of $\mathbb{Q}(\zeta)$ and its structure.

2. a description of $\pi$-adic congruences on $p$-unit group of $\mathbb{Q}(\zeta)$.

1.1 Some $\pi$-adic congruences connected to $p$-class group of cyclotomic field $\mathbb{Q}(\zeta)$

This topic is studied in section 3 p. of this paper. Let us give at first some definitions:

1. Let $p$ be an odd prime. Let $\zeta$ be a root of the equation $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. Let $\mathbb{Q}(\zeta)$ be the $p$-cyclotomic field and $\mathbb{Z}[\zeta]$ be the ring of integers of $\mathbb{Q}(\zeta)$.

2. Let $\sigma : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta)$ be a $\mathbb{Q}$-isomorphism of the field $\mathbb{Q}(\zeta)$ generating the cyclic Galois group $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. There exists $u \in \mathbb{N}$, primitive root mod $p$, such that $\sigma(\zeta) = \zeta^u$.

3. Let $C_p, C_p^+, C_p^-$ be respectively the subgroups of exponent $p$ of the $p$-class group of $\mathbb{Q}(\zeta)$, of the $p$-class group of $\mathbb{Q}(\zeta + \zeta^{-1})$ and the relative $p$-class group $C_p^- = C_p/C_p^+$. Let $r_p, r_p^+, r_p^-$ be respectively the $p$-rank of $C_p, C_p^+, C_p^-$, seen as $\mathbb{F}_p[G]$ modules.

4. It is possible to write $C_p$ in the form $C_p = \bigoplus_{i=1}^{r_p} \Gamma_i$, where $\Gamma_i$ is a cyclic group of order $p$, subgroup globally invariant under the action of the Galois group $G$.

5. Let $b_i, \ i = 1, \ldots, r_p$, be a not principal integral ideal of $\mathbb{Q}(\zeta)$ whose class belongs to the group $\Gamma_i$. Observe at first that $b_i^{p\mu}$ is principal and that $\sigma(b_i) \simeq b_i^{\mu_i}$ where $\simeq$ is notation for class equivalence and $\mu_i \in \mathbb{F}_p^*$ with $\mathbb{F}_p^*$ the set of $p-1$ no null elements of the finite field of cardinal $p$. Let the ideal $b = \prod_{i=1}^{r_p} b_i$, which generates $C_p$ under action of the group $G$.

6. A number $a \in \mathbb{Q}(\zeta)$ is said singular if there exists a not principal ideal $a$ of $\mathbb{Q}(\zeta)$ such that $a\mathbb{Z}[\zeta] = a^p$. A singular number $a \in \mathbb{Q}(\zeta)$ is said primary if there exists $\alpha \in \mathbb{N}, \ \alpha \not\equiv 0 \pmod{p}$ such that $a \equiv \alpha^p \pmod{\pi^p}$. 

3
7. Let \( d \in \mathbb{N}, \ p-1 \equiv 0 \mod d \). Let \( G_d \) be the subgroup of order \( \frac{p-1}{d} \) of the Galois group \( G \). Let us define the minimal polynomial \( P_{r_d}(X) \) of degree \( r_d \) in the indeterminate \( X \), where \( P_{r_d}(\sigma^d) \in \mathbb{F}_p[G_d] \) annihilates the ideal class of \( b \), written also \( b^P_{r_d(\sigma^d)} \simeq \mathbb{Z}[\zeta] \). The polynomial \( P_{r_d}(\sigma^d) \) is of form \( P_{r_d}(\sigma^d) = \prod_{i=1}^{r_d}(\sigma^d - \mu_i^d) \), \( \mu_i \in \mathbb{F}_p^* \). When \( d = 1 \), then \( G_d = G \), Galois group of \( \mathbb{Q}(\zeta)/\mathbb{Q} \), and \( r_d = r_1 \). Note that if \( d > 1 \) then \( r_d \leq r_1 \).

We obtain the following results:

1. For \( d_1, d_2 \) co-prime natural integers with \( d_1 \times d_2 = p-1 \), the degrees in the indeterminate \( X \) of minimal polynomials \( P_{r_{d_1}}(X) \) and \( P_{r_{d_2}}(X) \) verify: if \( r_{d_1} \geq 1 \) and \( r_{d_2} \geq 1 \) then \( r_{d_1} \times r_{d_2} \geq r_1 \).

2. Let us set \( d = 1 \). Let us note \( r_1 = r_1^+ + r_1^- \), where \( r_1^+ \) and \( r_1^- \) are respectively the degrees of the minimal polynomials \( P_{r_1^+}(\sigma) \) and \( P_{r_1^-}(\sigma) \), corresponding to annihilation of groups \( C_p^+ \) and \( C_p^- \) with \( C_p = C_p^+ \oplus C_p^- \). The following result connects strongly the degree \( r_1^- \) to Bernoulli Numbers: the degree \( r_1^- \) is the index of irregularity of \( \mathbb{Q}(\zeta) \) (the number of even Bernoulli Numbers \( B_{p-1-2m} \equiv 0 \mod p \) for \( 1 \leq m \leq \frac{p-3}{2} \)). Moreover the degree \( r_1^- \) verifies the inequality \( r_p^- - r_p^+ \leq r_1^- \leq r_p^- \).

3. Let the ideal \( \pi = (\zeta - 1)\mathbb{Z}[\zeta] \). The following results are \( \pi \)-adic congruences strongly connected to structure of \( p \)-class group \( C_p \) of \( \mathbb{Q}(\zeta) \):

   (a) There exists singular algebraic integers \( B_i \in \mathbb{Z}[\zeta] - \mathbb{Z}[\zeta]^* \), \( i = 1, \ldots, r_p \), verifying:
      i. \( B_i \mathbb{Z}[\zeta] = b_i^p \) with \( b_i \) defined above
      ii. \( \sigma(b_i) \simeq b_i^{\mu_i} \).
      iii. \( \sigma(B_i) = B_i^{\mu_i} \times \alpha_i^p \), \( \alpha_i \in \mathbb{Q}(\zeta), \ \mu_i \in \mathbb{F}_p^* \).
      iv. \( \sigma(B_i) \equiv B_i^\mu_i \mod p \).
      v. For the value \( m_i \in \mathbb{N} \) verifying \( \mu_i = u^m_i \mod p, \ 1 \leq m_i \leq p-2 \), then
         \[ \pi^{m_i} \mid B_i - 1. \]

   (b) We can precise the previous result: with it a certain reordering of indexing of \( B_i, \ i = 1, \ldots, r_p \),
      i. For \( i = 1, \ldots, r_p^+ \), then the \( B_i \) are primary, so \( \pi^p \mid B_i - 1 \).
      ii. For \( i = r_p^+ + 1, \ldots, r_p^- \), then the \( B_i \) are not primary. They verify the congruence
         \[ \pi^{m_i} \parallel B_i - 1. \]
iii. For \( i = r_p^- + 1, \ldots, r_p \), then the \( B_i \) are primary or not primary (without being able to have a more precise result) with

\[
\pi^{m_i} \mid B_i - 1.
\]

(c) Let \( \mu_i = u^{2n_i} \mod p \) with \( 1 \leq n_i \leq \frac{p-3}{2} \) corresponding to an ideal \( b_i \) whose class belongs to \( C_p^- \), relative \( p \)-class group of \( \mathbb{Q}(\zeta) \). In that case define \( C_i = \frac{B_i}{B_i - 1} \) with \( B_i \) already defined, so with \( C_i \in \mathbb{Q}(\zeta) \). If 

\[
2m_i + 1 > \frac{p-1}{2}
\]

then it is possible to prove the explicit very straightforward formula for \( C_i \mod \pi^{p-1} \):

\[
C_i \equiv 1 - \frac{\gamma_{p-3}}{1 - \mu_i} \times (\zeta + \mu_i^{-1} \zeta^u + \cdots + \mu_i^{(-p-2)} \zeta^{-u^{p-2}}) \mod \pi^{p-1}, \quad \gamma_{p-3} \in \mathbb{F}_p^*.
\]

### 1.2 Some \( \pi \)-adic congruences on \( p \)-unit group the cyclotomic field

This topic is studied in section 4 p. 33. We apply in following results to unit group \( \mathbb{Z}[\zeta + \zeta^{-1}]^* \) the method applied to \( p \)-class group in previous results:

1. There exists a fundamental system of units \( \eta_i, \quad i = 1, \ldots, \frac{p-3}{2} \), of the group \( F = \{ \mathbb{Z}[\zeta + \zeta^{-1}]^*/(\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p \}/ < -1 > \) verifying the relations:

\[
\eta_i \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad i = 1, \ldots, \frac{p-3}{2},
\]

\[
\sigma(\eta_i) = \eta_i^{\mu_i} \times \epsilon_i^p,
\]

\[
\epsilon_i \in \mathbb{Z}[\zeta + \zeta^{-1}]^*,
\]

\[
(1)
\]

\[
n_i \in \mathbb{N}, \quad \text{with } \mu_i = u^{2n_i} \mod p, \quad 1 \leq n_i \leq \frac{p-3}{2},
\]

\[
\eta_i \equiv 1 \mod \pi^{2n_i}, \quad i = 1, \ldots, \frac{p-3}{2},
\]

\[
\sigma(\eta_i) \equiv \eta_i^{\mu_i} \mod \pi^{p+1}, \quad i = 1, \ldots, \frac{p-3}{2}.
\]

2. With a certain reordering of indexing of \( i = 1, \ldots, \frac{p-3}{2} \),

(a) For \( i = 1, \ldots, r_p^+ \) then \( \eta_i \) are not primary units and

\[
\pi^{2n_i} \parallel \eta_i - 1.
\]

(b) For \( i = r_p^++1, \ldots, r_p^- \), then \( \eta_i \) are primary units and

\[
\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i > 0.
\]
(c) For $i = r_p^- + 1, \ldots, r_p$, then $\eta_i$ are not primary or primary units and

$$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i \geq 0.$$ 

(d) For $i = r_p + 1, \ldots, \frac{p-3}{2}$, then $\eta_i$ are not primary units and

$$\pi^{2n_i} \parallel (\eta_i - 1).$$

3. If $2n_i > \frac{p-1}{2}$ then it is possible to prove the very straightforward explicit formula for $\eta_i$:

$$\eta_i \equiv 1 - \frac{\gamma_{p-3}}{1 - \mu_i} \times (\zeta + \mu_i^{-1} \zeta^u + \cdots + \mu_i^{-(p-2)} \zeta^{u^{p-2}}) \mod \pi^{p-1}, \quad \gamma_{p-3} \in F^*_p.$$
2 Cyclotomic Fields : some definitions

In this section, we fix notations used in all this paper.

• For \( a \in \mathbb{R}^+ \), we note \([a]\) the integer part of \(a\) or the integer immediately below \(a\).

• We denote \([a, b]\), \(a, b \in \mathbb{R}\), the closed interval bounded by \(a, b\).

• Let us denote \(< a >\) the cyclic group generated by the element \(a\).

• Let \(p \in \mathbb{N}\) be an odd prime.

• Let \(Q(\zeta_p)\), or more briefly \(Q(\zeta)\) when there is no ambiguity of the context, be the \(p\)-cyclotomic number field.

• Let \(\mathbb{Z}[\zeta]\) be the ring of integers of \(Q(\zeta)\).

• Let \(\mathbb{Z}[\zeta]^*\) be the group of units of \(\mathbb{Z}[\zeta]\).

• Let \(Q(\zeta + \zeta^{-1})\) be the maximal real subfield of \(Q(\zeta)\), with \([Q(\zeta) : Q(\zeta + \zeta^{-1})] = 2\). The ring of integers of \(Q(\zeta + \zeta^{-1})\) is \(\mathbb{Z}[\zeta + \zeta^{-1}]\). Let \(\mathbb{Z}[\zeta + \zeta^{-1}]^*\) be the group of units of \(\mathbb{Z}[\zeta + \zeta^{-1}]\).

• Let \(F_p\) be the finite field with \(p\) elements. Let \(F_p^* = F_p - \{0\}\).

• Let us denote \(a\) the integral ideals of \(\mathbb{Z}[\zeta]\). Let us note \(a \simeq b\) when the two ideals \(a\) and \(b\) are in the same class of the class group of \(Q(\zeta)\). The relation \(a \simeq \mathbb{Z}[\zeta]\) means that the ideal \(a\) is principal.

• Let us denote \(Cl(a)\) the class of the ideal \(a\) in the class group of \(Q(\zeta)\). Let us note \(< Cl(a) >\) the finite group generated by the class \(Cl(a)\).

• If \(a \in \mathbb{Z}[\zeta]\), we note \(a\mathbb{Z}[\zeta]\) the principal integral ideal of \(\mathbb{Z}[\zeta]\) generated by \(a\).

• We have \(p\mathbb{Z}[\zeta] = \pi^{p-1}\) where \(\pi\) is the principal prime ideal \((1 - \zeta)\mathbb{Z}[\zeta]\). Let us denote \(\lambda = \zeta - 1\), so \(\pi = \lambda\mathbb{Z}[\zeta]\).

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

• 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 [6], last paragraph of page 118. This notation is largely used in the sequel of this monograph.
For $d \in \mathbb{N}$, $p - 1 \equiv 0 \mod d$, let $G_d$ be the cyclic subgroup of $G$ of order $\frac{p-1}{d}$ generated by $\sigma^d$, so with $G_1 = G$. The group $G_d$ is the Galois group of the extension $\mathbb{Q}(\zeta)/K_d$ where $K_d$ is a field with $\mathbb{Q} \subseteq K_d \subseteq \mathbb{Q}(\zeta)$ and $[K_d : \mathbb{Q}] = d$.

- Let $C_p$ be the subgroup of exponent $p$ of the $p$-class group of the field $\mathbb{Q}(\zeta)$.
- Let $C_p^+$ be the subgroup of exponent $p$ of the $p$-class group of the field $\mathbb{Q}(\zeta + \zeta^{-1})$.
- Let $C_p^-$ be the relative class group defined by $C_p^- = C_p / C_p^+$.

Let $h$ be the class number of $\mathbb{Q}(\zeta)$. The class number $h$ verifies the formula $h = h^- \times h^+$, where $h^+$ is the class number of the maximal real field $\mathbb{Q}(\zeta + \zeta^{-1})$, so called also second factor, and $h^-$ is the relative class number, so called first factor.

- Let us define respectively $e_p, e_p^-, e_p^+$ by $h = p^{e_p} \times h_2$, $h_2 \not\equiv 0 \mod p$, by $h^- = p^{e_p^-} \times h_2^-$, $h_2^- \not\equiv 0 \mod p$ and by $h^+ = p^{e_p^+} \times h_2^+$, $h_2^+ \not\equiv 0 \mod p$.

- Let $r_p, r_p^+, r_p^-$ be respectively the $p$-rank of the $p$-class group of $\mathbb{Q}(\zeta)$, of the $p$-class group of $\mathbb{Q}(\zeta + \zeta^{-1})$ and of the relative class group seen as $\mathbb{F}_p[G]$-modules, so with $r_p \leq e_p$, $r_p^+ \leq e_p^+$ and $r_p^- \leq e_p^-$.

The abelian group $C_p$ is a group of order $p^{r_p}$ with $C_p = \bigoplus_{i=1}^{r_p} C_i$ where $C_i$ are cyclic group of order $p$. 
3 \( \pi \)-adic congruences on \( p \)-subgroup \( C_p \) of the class group of \( \mathbb{Q}(\zeta) \)

- The two first subsections 3.1 p.9 and 3.2 p.10 give some definitions, notations and general classical properties of the \( p \)-class group of the extension \( \mathbb{Q}(\zeta)/\mathbb{Q} \). They can be omitted at first and only looked at for fixing notations.

- In subsection 3.3 p. 14, we get several results on the structure of the \( p \)-class group \( C_p \) of \( \mathbb{Q}(\zeta) \) and on class number \( h \) of \( \mathbb{Q}(\zeta) \):
  - A formulation, with our notations, of a Ribet’s result on irregularity index.
  - Let \( d, g \in \mathbb{N} \) coprime with \( d \times g = p - 1 \). For groups generated by the action of Galois groups \( G \) and of subgroups \( G_d, G_g \) of \( G \) on ideals \( b \) of \( \mathbb{Q}(\zeta) \), an inequality between degrees \( r_1, r_d, r_g \) of minimal polynomials \( P_{r_1}(\sigma) \in \mathbb{F}_p[G], P_{r_d}(\sigma^d) \in \mathbb{F}_p[G_d], P_{r_g}(\sigma^g) \in \mathbb{F}_p[G_g] \) annihilating ideal class of \( b \).
  - Some \( \pi \)-adic congruences connected to structure of \( p \)-class group \( C_p \) of \( \mathbb{Q}(\zeta) \).

3.1 Some definitions and notations

In this subsection, we fix or recall some notations used in all this section.

- Let \( G \) be the Galois group of \( \mathbb{Q}(\zeta)/\mathbb{Q} \). Let \( d \in \mathbb{N}, \ p - 1 \equiv 0 \mod d \). Let \( G_d \) be the subgroup of the cyclic group \( G \). Then \( G_d \) is of order \( \frac{p - 1}{d} \). If \( \sigma \) generates \( G \), then \( \sigma^d \) generates \( G_d \).

- Let \( b \) be an ideal of \( \mathbb{Z}[\zeta] \), not principal and with \( b^p \) principal.

- Let \( c_i = Cl(\sigma^i(b)) \), \( i = 0, \ldots, p - 2 \), be the class of \( \sigma^i(b) \) in the \( p \)-class group of \( \mathbb{Q}(\zeta) \).

- Recall that \( Cl(b) \) is the class of the ideal \( b \) of \( \mathbb{Z}[\zeta] \). Observe that exponential notations \( b^\sigma \) can be used indifferently in the sequel. With this notation, we have
  - \( b^{\sigma^d} = \sigma^d(b) \).
  - For \( \lambda \in \mathbb{F}_p \), we have \( b^{\sigma + \lambda} = b^\lambda \times \sigma(b) \).
  - Let \( P(\sigma) = \sigma^m + \lambda_{m-1}\sigma^{m-1} + \cdots + \lambda_1\sigma + \lambda_0 \in \mathbb{F}_p[\sigma] \); then \( b^{P(\sigma)} = \sigma^m(b) \times \sigma^{m-1}(b)^{\lambda_{m-1}} \times \cdots \times \sigma(b)^{\lambda_1} \times b^{\lambda_0} \).
Let us note $b^{P(\sigma)} \simeq \mathbb{Z}[\zeta]$, if the ideal $\sigma^m(b) \times \sigma^{m-1}(b)^{\lambda_{m-1}} \ldots \sigma(b)^{\lambda_1} \times b^{\lambda_0}$ is principal.

- Let $P(\sigma), Q(\sigma) \in \mathbb{F}_p[\sigma]$; if $b^{P(\sigma)} \simeq \mathbb{Z}[\zeta]$, then $b^{Q(\sigma) \times P(\sigma)} \simeq \mathbb{Z}[\zeta]$.
- Observe that trivially $b^{\sigma^{p-1}} \simeq \mathbb{Z}[\zeta]$.

There exists a monic minimal polynomial $P_{rd}(V) \in \mathbb{F}_p[V]$, polynomial ring of the indeterminate $V$ verifying the relation, for $V = \sigma^d$:

$$(2) \quad b^{P_{rd}(\sigma^d)} \simeq \mathbb{Z}[\zeta].$$

This minimality implies that, for all polynomials $R(V) \in \mathbb{F}_p(V)$, $R(V) \neq 0$, $\deg(R(V)) < \deg(P_{rd}(V))$, we have $b^{R(\sigma^d)} \not\simeq \mathbb{Z}[\zeta]$. It means, with another formulation in terms of ideals, that $\prod_{i=0}^{r_d} \sigma^{id}(b)^{\lambda_i,d}$ is a principal ideal and that $\prod_{i=0}^{\alpha} \sigma^{id}(b)^{\beta_i}$ is not principal when $\alpha < r_d$ and $\beta_i, \ i = 0, \ldots, \alpha$, are not all simultaneously null.

- $P_{rd}(U)$ is the minimal polynomial of the indeterminate $U$ with $P_{rd}(\sigma^d) \in \mathbb{F}_p[G_d]$ annihilating the ideal class of $b$.

### 3.2 Representations of Galois group $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ in characteristic $p$.

In this subsection we give some general properties of representations of $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ in characteristic $p$ and obtain some results on the structure of the $p$-class group of $\mathbb{Q}(\zeta)$. Observe that we never use characters theory.

**Lemma 3.1.** Let $d \in \mathbb{N}$, $p - 1 \equiv 0 \mod d$. Let $V$ be an indeterminate. Then the minimal polynomial $P_{rd}(V)$ with $P_{rd}(\sigma^d) \in \mathbb{F}_p[G_d]$ annihilating ideal class of $b$ verifies the factorization

$$P_{rd}(V) = \prod_{i=1}^{r_d} (V - \mu_{i,d}), \quad \mu_{i,d} \in \mathbb{F}_p, \quad i_1 \neq i_2 \Rightarrow \mu_{i_1} \neq \mu_{i_2}.$$

**Proof.** Let us consider the polynomials $A(V) = V^{p-1} - 1$ and $P_{rd}(V) \in \mathbb{F}_p[V]$. It is possible to divide the polynomial $A(V)$ by $P_{rd}(V)$ in the polynomial ring $\mathbb{F}_p[V]$ to obtain

$$A(V) = P_{rd}(V) \times Q(V) + R(V), \quad Q(V), R(V) \in \mathbb{F}_p[V],$$

$$d_R = \deg(V(R(V))) < r_d = \deg(V(P_{rd}(V))).$$
For $V = \sigma^d$, we get $b^{(p-1)} \simeq \mathbb{Z}[\zeta]$ and $b^R_{\sigma^d} \simeq \mathbb{Z}[\zeta]$, so $s^R_{\sigma^d} \simeq \mathbb{Z}[\zeta]$.

Suppose that $R(V) = \sum_{i=0}^{dR} R_i V^i$, $R_i \in \mathbb{F}_p$, is not identically null; then, it leads to the relation

$$\sum_{i=0}^{dR} R_i \sigma^{di}(b) \simeq \mathbb{Z}[\zeta],$$

where the $R_i$ are not all zero, with $d_R < r_d$, which contradicts the minimality of the polynomial $P_d(V)$. Therefore, $R(V)$ is identically null and we have

$$V^{p-1} - 1 = P_d(V) \times Q(V).$$

The factorization of $V^{p-1} - 1$ in $\mathbb{F}_p[V]$ is $V^{p-1} - 1 = \prod_{i=1}^{p-1} (V - i)$. The factorization is unique in the euclidean ring $\mathbb{F}_p[V]$ and so $P_{r_d}(V) = \prod_{i=1}^{r_d} (V - \mu_i d)$, $\mu_{i,d} \in \mathbb{F}_p$, $i \neq i_2 \Rightarrow \mu_{i_1} \neq \mu_{i_2}$, which achieves the proof.

Lemma 3.2. Let $d \in \mathbb{N}$, $p - 1 \equiv 0 \mod d$. Let $U, W$ be two indeterminates. Let $P_{r_1}(U)$ be the minimal polynomial with $P_{r_1}(\sigma) \in \mathbb{F}_p[G]$ annihilating the ideal class of $b$. Let $P_{r_d}(W)$ be the minimal polynomial with $P_{r_d}(\sigma^d) \in \mathbb{F}_p[G_d]$ annihilating the ideal class of $b$. Then

1. $P_{r_1}(U) = \prod_{i=1}^{r_1} (U - \mu_i)$, $\mu_i \in \mathbb{F}_p$.
2. $P_{r_d}(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_i d) = P_{r_1}(U) \times Q_d(U)$, $r_d \leq r_1$, $Q_d(U) \in \mathbb{F}_p[U]$.
3. The $p$-ranks $r_1$ and $r_d$ verify the inequalities

$$r_d \times d \geq r_1 \geq r_d.$$

4. Let $K_d$ be the intermediate field $\mathbb{Q} \subseteq K_d \subset \mathbb{Q}(\zeta)$, $[K_d : \mathbb{Q}] = d$. Suppose that $p$ does not divide the class number of $K_d/\mathbb{Q}$; then $\mu_i d \neq 1$ for $i = 1, \ldots, r_d$. In particular $\mu_i = 1$ for $i = 1, \ldots, r_1$.

Proof.

- Observe, at first, that $\deg_U(P_{r_d}(U^d)) = d \times r_d \geq r_1$; if not, for the polynomial $P_{r_d}(U^d)$ seen in the indeterminate $U$, we should have $\deg_U(P_{r_d}(U^d)) < r_1$ and $P_{r_d}(\sigma^d) \circ b \simeq \mathbb{Z}[\zeta]$ and, as previously, the polynomial $P_{r_d}(U^d)$ of the indeterminate $U$ should be identically null.

- We apply euclidean algorithm in the polynomial ring $\mathbb{F}_p[U]$ of the indeterminate $U$. Therefore,

$$P_{r_d}(U^d) = P_{r_1}(U) \times Q(U) + R(U), \quad Q(U), R(U) \in \mathbb{F}_p[U],$$

$$\deg(R(U)) < \deg(P_{r_1}(U)).$$
But we have $b^{Pr_d(U)} \simeq \mathbb{Z}[\zeta]$, $b^{Pr_1(U)} \simeq \mathbb{Z}[\zeta]$, therefore $b^{Rd(U)} \simeq \mathbb{Z}[\zeta]$. Then, similarly to proof of lemma 3.1 p.10, $R(U)$ is identically null and $Pr_d(U) = Pr_1(U) \times Q(U)$.

- Applying lemma 3.1 p.10 we obtain

$$Pr_1(U) = \prod_{i=1}^{r_1} (U - \mu_i), \quad \mu_i \in \mathbb{F}_p,$$

$$Pr_d(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_{i,d}), \quad \mu_{i,d} \in \mathbb{F}_p.$$  

- Then, we get

$$Pr_d(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_{i,d}) = \prod_{i=1}^{r_1} (U - \mu_i) \times Q(U).$$

There exists at least one $i$, $1 \leq i \leq r_d$, such that $(U^d - \mu_{i,d}) = (U - \mu_1) \times Q_1(U)$: if not, for all $i = 1, \ldots, r_d$, we should have $U^d - \mu_{i,d} \equiv R_i \text{ mod } (U - \mu_1)$, $R_i \in \mathbb{F}_p^*$, a contradiction because $\prod_{i=1}^{r_d} R_i \neq 0$. We have $\mu_{i,d} = \mu_1^d$; if not $U - \mu_1$ should divide $U^d - \mu_{i,d}$ and $U^d - \mu_1^d$ and also $U - \mu_1$ should divide $(\mu_{i,d} - \mu_1^d) \in \mathbb{F}_p^*$, a contradiction. Therefore, there exists at least one $i$, $1 \leq i \leq r_d$, such that $\mu_{i,d} = \mu_1^d$ and $U^d - \mu_{i,d} = U^d - \mu_1^d = (U - \mu_1) \times Q_1(U)$.

Then, generalizing to $\mu_{i,d}$ for all $i = 1, \ldots, r_d$, we get with a certain reordering of index $i$

$$Pr_d(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_i^d) = \prod_{i=1}^{r_1} (U - \mu_i) \times Q(U).$$

- We have

$$Pr_d(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_i^d).$$

This relation leads to

$$Pr_d(U^d) = \prod_{i=1}^{r_d} \prod_{j=1}^d (U - \mu_i \mu_d^j),$$

where $\mu_d \in \mathbb{F}_p$, $\mu_d^d = 1$. We have shown that $Pr_d(U^d) = Pr_1(U) \times Q_d(U)$ and so $\deg_U(Pr_d(U)) = d \times r_d \geq r_1$; thus $d \times r_d \geq r_1$. 

12
• We finish by the proof of item 4): suppose that, for some $i, 1 \leq i \leq r_d$, we have $\mu_i^d = 1$ and search for a contradiction: there exists, for the indeterminate $V$, a polynomial $P_i(V) \in \mathbb{F}_p(V)$ such that $P_{r_d}(V) = (V - \mu_i^d) \times P_i(V) = (V - 1) \times P_i(V)$. But for $V = \sigma^d$, we have $b^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]$, so $b^{(\sigma^d P_1(\sigma^d)-P_1(\sigma^d))} \simeq \mathbb{Z}[\zeta]$. So, $b^{P_1(\sigma^d)}$ is the class of an ideal $c$ of $\mathbb{Z}[\zeta]$ with $Cl(\sigma^d(c)) = Cl(c)$; then $Cl(\sigma^d(c)) = Cl(\sigma^d(c)) = Cl(c)$. Then $Cl(\sigma^d(c) \times \sigma^d(c) \times \cdots \times \sigma^{(p-1)d/d}(c)) = Cl(c^{(p-1)/d})$. Let $\tau = \sigma^d$, then $Cl(\tau(c) \times \tau^2(c) \times \cdots \times \tau^{(p-1)/d}(c)) = Cl(c^{(p-1)/d})$; Then we deduce that $Cl(N_{Q(\zeta)/K_d}(c)) = Cl(c^{(p-1)/d})$ and thus $c$ is a principal ideal because the ideal $N_{Q(\zeta)/K_d}(c)$ of $K_d$ is principal, (recall that, from hypothesis, $p$ does not divide $h(K_d/Q)$); so $b^{P_1(\sigma^d)} \simeq \mathbb{Z}[\zeta]$, which contradicts the minimality of the minimal polynomial equation $b^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]$ because, for the indeterminate $V$, we would have $\deg(P_i(V)) < \deg(P_{r_d}(V))$, which achieves the proof.

\[\square\]

**Remark:** As an example, the item 4) says that:

1. If $d = 2$, then classically $p \nmid h(K_2/Q)$ and so item 4) shows that $\mu_i \neq -1$: there is no ideal $b$ whose class belongs to $C_p$ which is annihilated by $\sigma - u_{(p-1)/2} = \sigma + 1$.

2. if $h^+ \neq 0 \mod p$, (Vandiver’s conjecture) then $\mu_i^{(p-1)/2} = -1$ for $i = 1, \ldots, r_1$.

We summarize results obtained in:

**Lemma 3.3.** Let $b$ be an ideal of $\mathbb{Z}[\zeta]$, $b^p \simeq \mathbb{Z}[\zeta]$, $b \not\simeq \mathbb{Z}[\zeta]$. Let $d \in \mathbb{N}$, $p-1 \equiv 0 \mod d$. Let $U, W$ be two indeterminates. Let $P_{r_1}(U)$ be the minimal polynomial with $P_{r_1}(\sigma) \in \mathbb{F}_p[G]$ annihilating the ideal class of $b$. Let $P_{r_d}(W)$ be the minimal polynomial with $P_{r_d}(\sigma^d) \in \mathbb{F}_p[G_d]$ annihilating the ideal class of $b$. Then there exists $\mu_1, \mu_2, \ldots, \mu_{r_1} \in \mathbb{F}_p$, with $i \neq i' \Rightarrow \mu_i \neq \mu_i'$, such that, for the indeterminate $U$,

- the minimal polynomials $P_{r_1}(U)$ and $P_{r_d}(U^d)$ are respectively given by

\[
P_{r_1}(U) = \prod_{i=1}^{r_1} (U - \mu_i),
\]

\[
P_{r_d}(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_i^d), \quad r_d \leq r_1,
\]

\[
P_{r_1}(U) \mid P_{r_d}(U^d).
\]
• The coefficients of $P_r(U^d)$ are explicitly computable by

\[ P_r(U^d) = 
U^{dr_d} - S_1(d) \times U^{d(r_d-1)} + S_2(d) \times U^{d(r_d-2)} + \cdots + (-1)^{r_d-1}S_{r_d-1}(d) \times U^d + (-1)^{r_d}S_{r_d}(d), \]

\[ S_0(d) = 1, \]

\[ S_1(d) = \sum_{i=1}^{r_d} \mu_i^d, \]

\[ S_2(d) = \sum_{1 \leq i_1 < i_2 \leq r_d} \mu_{i_1}^d \mu_{i_2}^d, \]

\[ \vdots \]

\[ S_{r_d}(d) = \mu_1^d \mu_2^d \cdots \mu_{r_d}^d. \]

• Then the ideal

\[ (4) \prod_{i=0}^{r_d} \sigma^{di}(b)^{(-1)^{r_d-i} \times S_{r_d-i}(d)} = bP_{r_d}(\sigma^d) \]

is a principal ideal.

**Remark:** For other annihilation methods of $Cl(Q(\zeta)/\mathbb{Q})$ more involved, see for instance Kummer, in Ribenboim [6] p 119, (2C) and (2D) and Stickelberger in Washington [9] p 94 and 332.

### 3.3 On the structure of the $p$-class group of subfields of $Q(\zeta)$

In this subsection we get several results on the structure of the $p$-class group of $Q(\zeta)$ and on class number $h$ of $Q(\zeta)$:

• A formulation, with our notations, of a Ribet’s result on irregularity index.

• Let $d, g \in \mathbb{N}$ coprime with $d \times g = p - 1$. For groups generated by the action of Galois groups $G$ and of subgroups $G_d, G_g$ of $G$ on ideals $b$ of $Q(\zeta)$, an inequality between degrees $r_1, r_d, r_g$ in the indeterminate $X$ of minimal polynomials $P_{r_1}(X), P_{r_d}(X), P_{r_g}(X) \in \mathbb{F}_p[X]$, with $P_{r_1}(\sigma), P_{r_d}(\sigma^d), P_{r_g}(\sigma^g)$ annihilating ideal class of $b$.

• Some $\pi$-adic congruences connected to structure of $p$-class group $C_p$ of $Q(\zeta)$.
3.3.1 Some definitions and notations

- Recall that:
  - $r_p$ is the $p$-rank of the class group of $\mathbb{Q}(\zeta)$.
  - $C_p$ is the subgroup of exponent $p$ of the $p$-class group of $\mathbb{Q}(\zeta)$.

- The $\mathbb{Q}$-isomorphism $\sigma$ of $\mathbb{Q}(\zeta)$ generates $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, Galois group of the field $\mathbb{Q}(\zeta)$. For $d \mid p - 1$, let $G_d$ be the subgroup of $d$ powers $\sigma^d$ of elements $\sigma$ of $G$. This group is of order $\frac{p - 1}{d}$.

- Suppose that $r_p > 0$. There exists an ideal class with representants $b \subset \mathbb{Z}[\zeta]$, with $b^0 \simeq \mathbb{Z}[\zeta]$, $b \not\simeq \mathbb{Z}[\zeta]$, which verifies, in term of representations, for some ideals $b_i$ of $\mathbb{Z}[\zeta]$, $i = 1, \ldots, r_p$,

\begin{equation}
\begin{aligned}
b &\simeq \prod_{i=1}^{r_p} b_i, \\
b_i^P &\simeq \mathbb{Z}[\zeta], \quad b_i \not\simeq \mathbb{Z}[\zeta], \quad i = 1, \ldots, r_p, \\
\sigma(b_i) &\simeq b_i^{\mu_i}, \quad \mu_i \in \mathbb{F}_p, \quad b_i + \pi = \mathbb{Z}[\zeta], \quad i = 1, \ldots, r_p, \\
C_p &\simeq \bigoplus_{i=1}^{r_p} < Cl(b_i) >, \\
P_{r_1}(U) &\simeq \prod_{i=1}^{r_1}(U - \mu_i), \quad b^{P_{r_1}(\sigma)} \simeq \mathbb{Z}[\zeta], \quad 1 \leq r_1 \leq r_p,
\end{aligned}
\end{equation}

where $P_{r_1}(U)$ is the minimal polynomial in the indeterminate $U$ for the action of $G$ on the ideal $b$, such that $P_{r_1}(\sigma) \in \mathbb{F}_p[G]$ annihilates the ideal class of $b$, see theorem 3.3, p 13. Recall that it is possible to encounter the case $\mu_i = \mu_j$ in the set $\{\mu_1, \ldots, \mu_{r_p}\}$; by opposite if $U - \mu_i$ and $U - \mu_j$ divide the minimal polynomial $P_{r_1}(U)$ then $\mu_i \neq \mu_j$. Therefore $r_1$ is the degree of the minimal polynomial $P_{r_1}(U)$.

- With a certain indexing assumed in the sequel, the ideals classes $Cl(b_i) \in C_p^-$ for $i = 1, \ldots, r_p^-$, and ideal classes $Cl(b_i) \in C_p^+$ for $i = r_p^- + 1, \ldots, r_p$.
  - The ideal $b$ verifies $b \simeq b^- \times b^+$ where $b^-$ and $b^+$ are two ideals of $\mathbb{Q}(\zeta)$ with $Cl(b^-) \in C_p^-$ and $Cl(b^+) \in C_p^+$.
  - With this notation, the minimal polynomial $P_{r_1}(U)$ factorize in a factor corresponding to $C_p^-$ and a factor corresponding to $C_p^+$, with:

\begin{equation}
P_{r_1}(U) = P_{r_1^-}(U) \times P_{r_1^+}(U), \quad r_1 = r_1^- + r_1^+.
\end{equation}
- $P_{r_1^-}(U)$ is the minimal polynomial with $P_{r_1^-}(\sigma) \in \mathbb{F}_p[G]$ annihilating the class of ideal $b^- \in C_p^-.$
- $P_{r_1^+}(U)$ is the minimal polynomial with $P_{r_1^+}(\sigma) \in \mathbb{F}_p[G]$ annihilating the class of ideal $b^+ \in C_p^+.$

- Let us denote $M_{r_1} = \{\mu_i \mid i = 1, \ldots, r_1\}.$

- Let $d \in \mathbb{N}, \ d \mid p - 1, \ 2 \leq d \leq \frac{p-1}{2}.$ Let $K_d$ be the field $\mathbb{Q} \subset K_d \subset \mathbb{Q}(\zeta), \ [K_d : \mathbb{Q}] = d.$

- Let $P_{r_d}(V)$ be the minimal polynomial in the indeterminate $V$ of the action of the group $G_d$ on the ideal class group $<b>$ of order $p,$ such that $P_{r_d}(\sigma^d) \in \mathbb{F}_p[G_d]$ annihilates ideal class of $b.$ Let $r_d$ be the degree of $P_{r_d}(V).$

### 3.3.2 On the irregularity index

Recall that $r_p$ is the $p$-rank of the group $C_p.$ The irregularity index is the number

$$i_p = \text{Card}\{B_{p-1-2m} \mid B_{p-1-2m} \equiv 0 \mod p, \ 1 \leq m \leq \frac{p-3}{2}\},$$

where $B_{p-1-2m}$ are even Bernoulli Numbers. The next theorem connects irregularity index and degree $r_p^-$ of minimal polynomial $P_{r_1^-}(U)$ defined in relations (5) p. 15 and (6) p. 16.

**Theorem 3.4.** ***With meaning of degree $r_p^-$ of minimal polynomial $P_{r_1^-}(U)$ defined in relation (6) p. 15, then the irregularity index is equal to the degree $r_p^-$ and verifies:

$$r_p^- - r_p^+ \leq i_p = r_p^- \leq r_p^-.$$**

**Proof.** Let us consider in relation (5) the set of ideals $\{b_i \mid i = 1, \ldots, r_p\}.$ The result of Ribet using theory of modular forms [7] mentionned in Ribenboim [6] (8C) p 190 can be formulated, with our notations,

$$B_{p-1-2m} \equiv 0 \mod p \Leftrightarrow \exists i, \ 1 \leq i \leq r_p, \ b_i^{\sigma-u_{2m+1}} \simeq \mathbb{Z}[\zeta].$$

There exists at least one such $i,$ but it is possible for $i \neq i'$ that $b_i^{\sigma-u_{2m+1}} \simeq b_i'^{\sigma-u_{2m+1}} \simeq \mathbb{Z}[\zeta].$

- The relation (8) p. 16 implies that $i_p = r_1^-.$
- The inequality (7) p. 16 is an immediate consequence of independant forward structure theorem [3, 15] p. 27.
3.3.3 Inequalities involving degrees \( r_1, r_d, r_g \) of minimal polynomials \( P_{r_1}(V), P_{r_d}(V), P_{r_g}(V) \) annihilating ideal \( b \).

In this subsection, we always assume that \( b \) is defined by relation \( \mathbf{[5]} \) p. \( \mathbf{[15]} \).

Let \( p \) be an odd prime. Let \( d, g \in \mathbb{N} \), with \( \gcd(d, g) = 1 \) and \( d \times g = p - 1 \). Recall that \( r_1, r_d \) and \( r_g \) are the degrees of the minimal polynomials \( P_{r_1}(V), P_{r_d}(V), P_{r_g}(V) \) of the indeterminate \( V \) with \( b^{P_{r_1}(\sigma)} \simeq b^{P_{r_d}(\sigma^d)} \simeq b^{P_{r_g}(\sigma^g)} \simeq \mathbb{Z} [\zeta] \). The next theorem is a relation between the three degree \( r_1, r_d \) and \( r_g \).

**Theorem 3.5.** *** Let \( d, g \in \mathbb{N}, \ \gcd(d, g) = 1, \ d \times g = p - 1. \) Suppose that \( r_d \geq 1 \) and \( r_g \geq 1. \) Then

\[
(9) \quad r_d \times r_g \geq r_1.
\]

and if \( r_d = 1 \) then \( r_g = r_1. \)

**Proof.**

- Let us consider the minimal polynomials \( P_{r_d}(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_i^d) \) and \( P_{r_g}(U^g) = \prod_{j=1}^{r_g} (U^g - \nu_j^g) \) of the indeterminate \( U \) with \( b^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z} [\zeta] \) and \( b^{P_{r_g}(\sigma^g)} \simeq \mathbb{Z} [\zeta] \).
- From lemma 3.2 p.\( \mathbf{[11]} \) we have seen that \( P_{r_1}(U) \mid P_{r_d}(U^d) \) and that similarly \( P_{r_1}(U) \mid P_{r_g}(U^g) \), thus \( P_{r_1}(U) \mid \gcd(P_{r_d}(U^d), P_{r_g}(U^g)) \).
- Let \( M_{r_1} = \{ \mu_i \mid i = 1, \ldots, r_1 \} \). Let us define the sets
  \[
  C_1(\mu_i) = \{ \mu_i \times \alpha_j \mid \alpha_j^d = 1, \ j = 1, \ldots, d \} \cap M_{r_1}, \quad i = 1, \ldots, r_d.
  \]
  Let us define in the same way the sets
  \[
  C_2(\nu_i) = \{ \nu_i \times \beta_j \mid \beta_j^g = 1, \ j = 1, \ldots, g \} \cap M_{r_1}, \quad i = 1, \ldots, r_g.
  \]
- We have proved in lemma 3.2 p.\( \mathbf{[11]} \) that \( P_{r_1}(U) \mid P_{r_d}(U^d) \). Therefore the sets \( C_1(\mu_i), \ i = 1, \ldots, r_d, \) are a partition of \( M_{r_1} \) and \( r_1 = \sum_{i=1}^{r_d} \text{Card}(C_1(\mu_i)) \).
- In the same way \( P_{r_1}(U) \mid P_{r_g}(U^g) \). Therefore the sets \( C_2(\nu_i), \ i = 1, \ldots, r_g, \) are a partition of \( M_{r_1} \) and \( r_1 = \sum_{i=1}^{r_g} \text{Card}(C_2(\nu_i)) \).
- There exists at least one \( i \in \mathbb{N}, \ 1 \leq i \leq r_d, \) such that \( \text{Card}(C_1(\mu_i)) \geq \frac{r_d}{2}. \) For this \( i, \) let \( \nu_1 = \mu_i \times \alpha_1, \ \alpha_1^d = 1, \ \nu_1 \in M_{r_1} \) and, in the same way, let \( \nu_2 = \mu_i \times \alpha_2, \ \alpha_2^d = 1, \ \nu_2 \in M_{r_1}, \ \nu_2 \neq \nu_1. \) We have \( \nu_1^g \neq \nu_2^g : \) if not we should simultaneously have \( \alpha_1^g = \alpha_2^g \) and \( \alpha_1^g = \alpha_2^g, \) which should imply, from \( \gcd(d, g) = 1, \) that \( \alpha_1 = \alpha_2, \) contradicting \( \nu_1 \neq \nu_2 \) and therefore we get \( C_2(\nu_1) \neq C_2(\nu_2). \)
Therefore, extending the same reasoning to all elements of $C_1(\mu_i)$, we get $\frac{r_1}{r_d} \leq \text{Card}(C_1(\mu_i)) \leq r_g$, which leads to the result.

If $r_d = 1$ then $r_g \geq r_1$ and in an other part $r_g \leq r_1$ and so $r_g = r_1$.

Remarks:

As an example, consider an odd prime $p$ verifying $p \not\equiv 1 \mod 4$. Suppose also that $h^+ \not\equiv 0 \mod p$. Then $P_{r(p-1)/2}(\sigma) = \sigma^{(p-1)/2} + 1 = U + 1$ for the indeterminate $U = \sigma^{(p-1)/2}$. Therefore $r_{(p-1)/2} = 1$ and thus $r_2 = r_1$.

Observe that $1 \leq r_d < r_1$ implies that $r_g > 1$.

3.3.4 On Stickelberger’s ideal in field $\mathbb{Q}(\zeta)$

In this subsection, we give a result resting on the annihilation of class group of $\mathbb{Q}(\zeta)$ by Stickelberger’s ideal.

Let us denote $a \simeq c$ when the two ideals $a$ and $c$ of $\mathbb{Q}(\zeta)$ are in the same ideal class.

Let $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Let $\tau_a : \zeta \to \zeta^a, \ a = 1, \ldots, p - 1$, be the $p - 1$ $\mathbb{Q}$-isomorphisms of the field $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Recall that $u$ is a primitive root mod $p$, and that $\sigma : \zeta \to \zeta^u$ is a $\mathbb{Q}$-isomorphism of the field $\mathbb{Q}(\zeta)$ which generates $G$. Recall that, for $i \in \mathbb{N}$, then we denote $u_i$ for $u^i \mod p$ and $1 \leq u_i \leq p - 1$.

Let $b$ be the not principal ideal defined in relation (5) p.15. Let $P_{r_1}(\sigma) \in \mathbb{F}_p[G]$ be the polynomial of minimal degree such that $P_{r_1}(\sigma)$ annihilates $b$, so such that $b^{P_{r_1}(\sigma)}$ is principal ideal, see lemma 3.4 p.10 and so

$$P_{r_1}(\sigma) = \prod_{i=1}^{r_1}(\sigma - \mu_i), \ \mu_i \in \mathbb{F}_p, \ i \neq i' \Rightarrow \mu_i \neq \mu_i'.$$

In the next result we shall explicitly use the annihilation of class group of $\mathbb{Q}(\zeta)$ by the Stickelberger’s ideal.

Lemma 3.6. Let $P_{r_1}(U) = \prod_{i=1}^{r_1}(U - \mu_i)$ be the polynomial of the indeterminate $U$, of minimal degree, such that $b^{P_{r_1}(\sigma)}$ is principal. Then $\mu_i \neq u, \ i = 1, \ldots, r_1$. 

18
Proof.

• Let \( i \in \mathbb{N}, \; 1 \leq i \leq r_1 \). From relation (5) p.15, there exists ideals \( b_i \in \mathbb{Z}[\zeta], \; i = 1, \ldots, r_p \), not principal and such that \( b = \prod_{i=1}^{r_p} b_i \), with \( b_i^{\sigma - \mu_i} \) principal.

• Suppose that \( \mu_i = u \), and search for a contradiction: Let us consider \( \theta = \sum_{a=1}^{p-1} \frac{a}{p} \times \tau_a^{-1} \in \mathbb{Q}[G] \). Then \( p\theta \in \mathbb{Z}[G] \) and the ideal \( b^{p\theta} \) is principal from Stickelberger’s theorem, see for instance Washington [9], theorem 6.10 p 94.

• We can set \( a = u^m, \; a = 1, \ldots, p - 1 \), and \( m \) going through all the set \( \{0, \ldots, p - 2\} \), because \( u \) is a primitive root mod \( p \). Then \( \tau_a : \zeta \rightarrow \zeta^a \) and so \( \tau_a^{-1} : \zeta \rightarrow \zeta^{(a^{-1})} = \zeta^{((u^m)^{-1})} = \zeta^{(u^{-m})} = \zeta^{(u^{p-1-m})} = \sigma^{p-1-m} = \sigma^{-m} \).

Therefore, \( p\theta = \sum_{m=0}^{p-2} u^m \sigma^{-m} \). The element \( \sigma - \mu_i = \sigma - u \) annihilates the class of \( b_i \) and also the element \( u \times \sigma^{-1} - 1 \) annihilates the class of \( b_i \). Therefore \( u^m \sigma^{-m} - 1, \; m = 0, \ldots, p - 2 \), annihilates the class of \( b_i \) and finally \( p - 1 \) annihilates the class of \( b_i \), so \( b^{p-1} \) is principal, but \( b^p \) is also principal, and finally \( b_i \) is principal which contradicts our hypothesis and achieves the proof.

\[ \square \]

3.4 \( \pi \)-adic congruences connected to \( p \)-class group \( C_p \)

In a first subsection, we examine the case of relative \( p \)-class group \( C_p^- \). In a second subsection, we examine the case of \( p \)-class group \( C_p^+ \). In last subsection, we summarize our results to all \( p \)-class group \( C_p \). These important congruences (subjective) characterize structure of \( p \)-class group.

3.4.1 \( \pi \)-adic congruences connected to relative \( p \)-class group \( C_p^- \)

In this subsection, we shall describe some \( \pi \)-adic congruences connected to \( p \)-relative class group \( C_p^- \).

Some definitions and a preliminary result

• Let \( C_p \) be the subgroup of exponent \( p \) of the \( p \)-class group of \( \mathbb{Q}(\zeta) \).

• Let \( r_p \) be the \( p \)-rank of \( C_p \), let \( r_p^+ \) be the \( p \)-rank of \( C_p^+ \) and \( r_p^- \) be the relative \( p \)-rank of \( C_p^- \). Let us recall the structure of the ideal \( B \) already defined in
\[ B = b_1 \times \cdots \times b_{r_p} \times b_{r_p+1} \times \cdots \times b_{r_p}, \]
\[ C_p = \oplus_{i=1}^{r_p} < Cl(b_i) >, \]
\[ b_i^p \simeq \mathbb{Z}[\zeta], \quad b_i \not\simeq \mathbb{Z}[\zeta], \quad i = 1, \ldots, r_p, \]
\[ \sigma(b_i) \simeq b_i^{\mu_i}, \quad \mu_i \in \mathbb{F}_p, \quad i = 1, \ldots, r_p, \]
\[ Cl(b_i) \in C_p^-, \quad i = 1, \ldots, r_p, \]
\[ Cl(b_i) \in C_p^+, \quad i = r_p + 1, \ldots, r_p, \]
\[ B_{P_{r_1}^{+}}(\sigma) \simeq \mathbb{Z}[\zeta], \]
\[ B_{P_{r_1}^{-}}(\sigma) \simeq \mathbb{Z}[\zeta]. \]

(Observe that we replace here notation \( b \) by \( B \) to avoid conflict of notation in the sequel.) In the sequel, we are using also the natural integers \( m_i \), with \( 0 \leq m_i \leq \frac{p^2 - 3}{2} \), defined by \( \mu_i = u_2m_i+1 = u_2m_i+1 \mod p \).

• Recall that it is possible to have \( \mu_i = \mu_j = \mu \): observe that, in that case, the decomposition \( < Cl(b_i) > \oplus < Cl(b_j) > \) is not unique. We can have
\[ < Cl(b_i) > \oplus < Cl(b_j) > = < Cl(b'_i) > \oplus < Cl(b'_j) >, \]
\[ \sigma(b_i) \simeq b_i^{\mu_i}, \quad \sigma(b_j) \simeq b_j^{\mu_i}, \quad \sigma(b'_i) \simeq (b'_i)^{\mu_i}, \quad \sigma(b'_j) \simeq (b'_j)^{\mu_i}, \]
\[ < Cl(b_i) > \not\simeq \{ < Cl(b_j) >, \quad < Cl(b'_i) >, \quad < Cl(b'_j) > \}. \]

• Recall that \( P_{r_1}^{+}(\sigma) \in \mathbb{F}_p[G] \) is the minimal polynomial such that \( b^{P_{r_1}^{+}(\sigma)} \simeq \mathbb{Z}[\zeta] \) with \( r_1 \leq r_p \).

• Recall that \( P_{r_1}^{-}(\sigma) \in \mathbb{F}_p[G] \) is the minimal polynomial such that \( (b^{-1}_P)^{P_{r_1}^{+}(\sigma)} \simeq \mathbb{Z}[\zeta] \) with \( r_1 \leq r_p ^- \).

• We say that the algebraic number \( C \in \mathbb{Q}(\zeta) \) is singular if \( C\mathbb{Z}[\zeta] = c^p \) for some ideal \( c \) of \( \mathbb{Q}(\zeta) \). We say that \( C \) is singular primary if \( C \equiv c^p \mod \pi^p, \quad c \in \mathbb{Z}, \quad c \neq 0 \mod p \).

At first, a general lemma dealing with congruences on \( p \)-powers of algebraic numbers of \( \mathbb{Q}(\zeta) \).

**Lemma 3.7.** Let \( \alpha, \beta \in \mathbb{Z}[\zeta] \) with \( \alpha \not\equiv 0 \mod \pi \) and \( \alpha \equiv \beta \mod \pi \). Then \( \alpha^p \equiv \beta^p \mod \pi^{p+1} \).
Proof. Let $\lambda = (\zeta - 1)$. Then $\alpha - \beta \equiv 0 \pmod{\pi}$ implies that $\alpha - \zeta^k \beta \equiv 0 \pmod{\pi}$ 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 $(\alpha - \zeta^k \beta) \equiv \lambda a_k \pmod{\pi^2}$. For another value $l$, $0 \leq l \leq p - 1$, we have, in the same way, $(\alpha - \zeta^l \beta) \equiv \lambda a_l \pmod{\pi^2}$, hence $(\zeta^k - \zeta^l)\beta \equiv \lambda(a_k - a_l) \pmod{\pi^2}$. For $k \neq l$ we get $a_k \neq a_l$, because $\pi \parallel (\zeta^k - \zeta^l)$ and because hypothesis $\alpha \not\equiv 0 \pmod{\pi}$ implies that $\beta \not\equiv 0 \pmod{\pi}$. Therefore, there exists one and only one $k$ such that $(\alpha - \zeta^k \beta) \equiv 0 \pmod{\pi^2}$. Then, we have $\prod_{j=0}^{p-1}(\alpha - \zeta^j \beta) = (\alpha^p - \beta^p) \equiv 0 \pmod{\pi^{p+1}}. \Box$

For $i = 1, \ldots, r^-_p$, to simplify notations in this lemma, let us note respectively $b, B, C, \mu = u^-_{2m+1}$ for $b_i, B_i, C_i, \mu_i = u^-_{2m_i+1}$ as defined in the two relations \[10\] p. 20 and \[14\] p. 22

Lemma 3.8. For $i = 1, \ldots, r^-_p$, there exists algebraic integers $B \in \mathbb{Z}[\zeta]$ such that

\[ B\mathbb{Z}[\zeta] = B, \]

\[ \sigma(B) = \left(\frac{b}{B}\right)^{-\mu} \equiv \left(\frac{\alpha}{B}\right)^p \pmod{\pi^{p+1}}, \quad \alpha \in \mathbb{Q}(\zeta), \quad \alpha\mathbb{Z}[\zeta] + \pi = \mathbb{Z}[\zeta], \]

\[ \sigma(B) \equiv B \pmod{\pi^{p+1}}. \]

Proof.

1. Observe that we can neglect in this proof the values $\mu = u^-_{2m}$ such that $\sigma - \mu$ annihilates ideal classes $\in C^-_p$, because we consider only quotients $B/B$, with ideal classes $Cl(b)$ in $C^-_p$. The ideal $b^p$ is principal. So let one $\beta \in \mathbb{Z}[\zeta]$ with $\beta \mathbb{Z}[\zeta] = b^p$. We have seen in relation \[15\] p. 15 that $g(b) \simeq b^\mu$, therefore there exists $\alpha \in \mathbb{Q}(\zeta)$ such that $\frac{\alpha b}{B} = \alpha \mathbb{Z}[\zeta]$, also $\frac{\sigma(b)}{B} = \varepsilon \times \alpha^p + \varepsilon \in \mathbb{Z}[\zeta]^*$. Let $B = \delta^{-1} \times \beta$, $\delta \in \mathbb{Z}[\zeta]^*$, for a choice of the unit $\delta$ that we shall explicit in the next lines. We have $\sigma(\delta \times B) = \alpha^p \times (\delta \times B)^\mu \times \varepsilon$. Therefore

\[ \sigma(B) = \alpha^p \times B^\mu \times (\sigma(\delta^{-1}) \times \delta^\mu \times \varepsilon). \]

From Kummer’s lemma on units, we can write

$\delta = \zeta^{v_1} \times \eta_1, \quad v_1 \in \mathbb{Z}, \quad \eta_1 \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$;

$\varepsilon = \zeta^{v_2} \times \eta_2, \quad v_2 \in \mathbb{Z}, \quad \eta_2 \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$.

Therefore

$\sigma(\delta^{-1}) \times \delta^\mu \times \varepsilon = \zeta^{-v_1 u + v_1 \mu + v_2} \times \eta, \quad \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$.
From lemma 3.6 p.18 we deduce that \( \mu \neq u \), therefore there exists one \( v_1 \) with 
\[-v_1 u + v_1 \mu + v_2 \equiv 0 \mod p. \]
Therefore, chosing this value \( v_1 \) for the unit \( \delta \),
\[
\sigma(B) = \alpha^p \times B^\mu \times \eta, \quad \alpha \mathbb{Z}[\zeta] + \pi = \mathbb{Z}[\zeta], \quad \eta \in \mathbb{Z}[\zeta + \zeta^{-1}],
\]
\( \sigma(B) = \overline{\alpha^p} \times \overline{B}^\mu \times \eta. \)

We have \( \alpha \equiv \overline{\alpha} \mod \pi \) and we have proved in lemma 3.7 p.20 that \( \alpha^p \equiv \overline{\alpha}^p \mod \pi^{p+1} \), which leads to the result.

\[\square\]

\( \pi \)-adic congruences connected to relative \( p \)-class group \( C_p^- \): For \( i = 1, \ldots, r_p^- \), to simplify notations in this lemma, let us note respectively \( b, B, C, \mu = u_{2m+1} \) for \( b_i, B_i, C_i, \mu_i = u_{2m_i+1} \) as defined in the two relations (10) p. 20 and (14) p. 22.

**Lemma 3.9.** For each \( i = 1, \ldots, r_p^- \), there exists singular algebraic integers \( B \in \mathbb{Z}[\zeta] \), such that
\[
\mu = u_{2m+1}, \quad m \in \mathbb{N}, \quad 1 \leq m \leq \frac{p-3}{2},
\]
\[
B \mathbb{Z}[\zeta] = b^p,
\]
\[
C = \frac{B}{B} \equiv 1 \mod \pi^{2m+1}.
\]
Then, either \( C \) is singular not primary with \( \pi^{2m+1} \parallel C - 1 \) or \( C \) is singular primary with \( \pi^p \parallel C - 1 \).

**Proof.**

- The definition of \( C \) implies that \( C \equiv 1 \mod \pi \), and so that \( \sigma(C) \equiv 1 \mod \pi \).

There exists a natural integer \( \nu \) such that \( \pi^\nu \parallel C - 1 \), therefore we can write
\[
C \equiv 1 + c_0 \lambda^\nu \mod \lambda^{\nu+1},
\]
\[
c_0 \in \mathbb{Z}, \quad c_0 \neq 0 \mod p.
\]
We have to prove that \( \nu < p \) implies that \( \nu = 2m + 1 \) for the integer \( m < p - 1 \) verifying \( \mu = u_{2m+1} \).

- From lemma 3.8 p.21 it follows that \( \sigma(C) = C^\mu \times \sigma^p \), with some \( \sigma \in \mathbb{Q}(\zeta) \), and so that \( 1 + c_0 \sigma(\lambda)^\nu \equiv (1 + \mu c_0 \lambda^\nu) \times \sigma^p \mod \pi^{\nu+1} \). This congruence implies that \( \alpha \equiv 1 \mod \pi \) and then, from lemma 3.7 \( \alpha^p \equiv 1 \mod \pi^{p+1} \). 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 \( u^\nu \lambda^\nu \equiv \mu \lambda^\nu \mod \pi^{\nu+1} \), with simplification \( u^\nu - \mu \equiv 0 \mod \pi \). Therefore, we have proved that \( \nu = 2m + 1 \) or that, when \( \pi^p \nmid C - 1 \), then \( \pi^{2m+1} \| C - 1 \).

Remarks:

1. In considering \( b^p \) in place of \( b \), we consider \( B^p \) and \( C^p \) in place of \( B \) and \( C \), such that we can always assume without loss of generality that \( B \equiv C \equiv 1 \mod \pi \). We suppose implicitly this normalization in the sequel.

2. In relation (15) we can suppose without loss of generality that \( c_0 = 1 \) because we can consider \( b^n \) with \( 1 \leq n \leq p - 1 \) in place of \( b \) with \( n \times c_0 \equiv 1 \mod p \).

As previously, for \( i = 1, \ldots, r_p \), to simplify notations in this lemma, let us note respectively \( b, B, C, \mu = u_{2m+1} \) for \( b_i, B_i, C_i, \mu_i = u_{2m_i+1} \) as defined in the two relations (10) p. 20 and (14) p. 22. In the following lemma, we connect \( \pi \)-adic congruences on \( C - 1 \) with \( C = B \) to some \( \pi \)-adic congruences on algebraic integer \( B \).

**Theorem 3.10.***

1. If the singular number \( B \) is not primary, there exists a primary unit \( \eta \in \mathbb{Z}[\zeta + \zeta^{-1}] - \{1, -1\} \) and a singular not primary number \( B' = \frac{B^2}{\eta} \), such that

\[
\sigma(B') = B'^\mu \times \alpha^p, \quad \alpha \in \mathbb{Q}(\zeta),
\]

\[
B' \mathbb{Z}[\zeta] = b^{2p}, \quad B' \in \mathbb{Z}[\zeta],
\]

\[
\pi^{2m+1} \| (B')^{p-1} - 1.
\]

2. If the singular number \( B \) is primary then

\[
\sigma(B) = B^\mu \times \alpha^p, \quad \alpha \in \mathbb{Q}(\zeta),
\]

\[
B \mathbb{Z}[\zeta] = b^p,
\]

\[
\pi^{p-1} \| B - 1.
\]

**Proof.** 1. We have \( C \mathbb{Z}[\zeta] = b^p \) where the ideal \( b \) verifies \( \sigma(b) \simeq b^\mu \) and \( Cl(b) \in C_p \). From relation (13) p. 22 and from \( Cl(b) \in C_p \), we can choose \( B \) such
that
\[ C = \frac{B}{B}, \quad B \in \mathbb{Z}[\zeta], \]
\[ B\overline{B} = \eta \times \gamma^p, \quad \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad \gamma \in \mathbb{Q}(\zeta), \quad v_\pi(\gamma) = 0, \]
\[ \sigma(B) = B^\mu \times \alpha^p \times \varepsilon, \quad \mu = u_{2m+1}, \quad \alpha \in \mathbb{Q}(\zeta), \quad v_\pi(\alpha) = 0, \quad \varepsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^*. \]

We derive that
\[ \sigma(B\overline{B}) = \sigma(\eta) \times \sigma(\gamma^p) \]
\[ \sigma(B\overline{B}) = (B\overline{B})^\mu \times (\alpha\overline{\alpha})^p \times \varepsilon^2 = \eta^p \gamma^p \times (\alpha\overline{\alpha})^p \times \varepsilon^2, \]
and so
\[ \sigma(\eta) = \eta^p \times \varepsilon^2 \times \varepsilon_1^p, \quad \varepsilon_1 \in \mathbb{Z}[\zeta + \zeta^{-1}]^*. \]

We have seen that
\[ \sigma(B^2) = B^{2\mu} \times \alpha^{2p} \times \varepsilon^2, \]
and so
\[ \sigma(B^2) = B^{2\mu} \times \alpha^{2p} \times (\sigma(\eta)\eta^{-p} \varepsilon_1^{-p}) \]
which leads to
\[ \sigma\left(\frac{B^2}{\eta}\right) = (\frac{B^2}{\eta})^\mu \times \alpha_2^p, \quad \alpha_2^p = \alpha^{2p} \times \varepsilon_1^{-p}, \quad \alpha_2 \in \mathbb{Q}(\zeta), \quad v_\pi(\alpha_2) = 0. \]

Let us note \( B' = \frac{B^2}{\eta}, \quad B' \in \mathbb{Z}(\zeta), \quad v_\pi(B') = 0. \) We get
\[ \sigma(B') = (B')^\mu \times \alpha_2^p. \]

This relation (18) is similar to hypothesis used to prove lemma 3.9 p. 22.
This leads in the same way to \( B' \equiv d^p \mod \pi^{2m+1}, \quad d \in \mathbb{Z}, \quad d \not\equiv 0 \mod p. \)
Therefore \( (B')^{p-1} \equiv 1 \mod \pi^{2m+1}, \) which achieves the proof of the first part.

2. We have
\[ \sigma(B) = B^\mu \times \alpha^p \times \eta, \quad \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \]
\[ \sigma(\overline{B}) = \overline{B}^\mu \times \overline{\alpha}^p \times \eta. \]

From simultaneous application of a Furtwangler theorem, see Ribenboim (6C) p. 182 and of a Hecke theorem on class field theory, see Ribenboim (6D) p. 182, it results that
\[ B \times \overline{B} = \beta^p \]
where \( \beta \in \mathbb{Z}[[\zeta] - \mathbb{Z}[\zeta + \zeta^{-1}]^*. \) From these two relations, it follows that \( \eta \in (\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p, \) which achieves the proof of the second part.
On structure of $p$-class group $C_p^-$

In this paragraph, the indexing of singular primary and of singular not primary $C_i$ with usual previously defined meaning of index $i = 1, \ldots, r_p^+, \ldots, r_p^-$, is used to describe the structure of relative $p$-class group $C_p^-$: we shall show that, with a certain ordering of index, then $C_i$ are singular primary for $i = 1, \ldots, r_p^+$ and $C_i$ are singular not primary for $i = r_p^* + 1, \ldots, r_p^-$.

**Theorem 3.11.*** Let $C = C_1^{\alpha_1} \times \cdots \times C_i^{\alpha_i} \times \cdots \times C_n^{\alpha_n}$ with $\alpha_i \in \mathbb{F}_p^*$, $1 \leq n \leq r_p^-$ and with $\mu_i = u_{2m_i+1}$ pairwise different for $i = 1, \ldots, n$. Then $C$ is singular primary if and only if all the $C_i$, $i = 1, \ldots, n$, are all singular primary.

**Proof.**

- If $C_i$, $i = 1, \ldots, n$, are all singular primary, then $C$ is clearly singular primary.

- Suppose that $C_i$, $i = 1, \ldots, l$, are not singular primary and that $C_i$, $i = l + 1, \ldots, n$, are singular primary. Then, from Lemma 3.9 p. 22 and remark following it, $\pi^{2m_i+1} \parallel C_i - 1$, $i = 1, \ldots, l$, where we suppose, without loss of generality, that $1 < 2m_1 + 1 < \cdots < 2m_l + 1$. Then $\pi^{2m_1+1} \parallel C - 1$ and so $C$ is not singular primary, contradiction which achieves the proof.

**Lemma 3.12.** Let $C$ of relation (14) p. 22. If $C$ is not singular primary, then

$$C \equiv 1 + V(\mu) \mod \pi^{p-1}, \quad \mu = u_{2m+1} \quad V(\mu) \in \mathbb{Z}[\zeta],$$

where $V(\mu) \mod p$ depends only on $\mu$ with $\pi^{2m+1} \parallel V(\mu)$.

**Proof.** The congruence $\sigma(C) \equiv C^\mu \mod \pi^{p-1}$ and the normalization $C \equiv 1 + \lambda^{2m+1} \mod \pi^{2m+2}$ explained in remark following Lemma 3.9 p. 22 implies the result.

**Theorem 3.13.*** Let $C_1, C_2$ singular not primary defined with relation (14) p. 22. If $\mu_1 = \mu_2$ then $C_1 \times C_2^{-1}$ is singular primary.

**Proof.** Let $\mu_1 = \mu_2 = \mu = u_{2m+1}$. Therefore $\sigma(C_1) \equiv C_1^\mu \mod \pi^{p+1}$ and $\sigma(C_2) \equiv C_2^\mu \mod \pi^{p+1}$. From previous lemma 3.12 p. 22 we get

$$C_1 = 1 + V(\mu) + pW_1, \quad W_1 \in \mathbb{Q}(\zeta), \quad v_\pi(V(\mu)) \geq 2m + 1, \quad v_\pi(W_1) \geq 0,$$

$$C_2 = 1 + V(\mu) + pW_2, \quad W_2 \in \mathbb{Q}(\zeta), \quad v_\pi(V(\mu)) \geq 2m + 1, \quad v_\pi(W_2) \geq 0,$$

$\pi^{2m+1} \parallel V(\mu)$,
Elsewhere, $C_1, C_2$ verify
\[
\sigma(C_1) \equiv C_1^\mu \mod \pi^{p+1},
\]
\[
\sigma(C_2) \equiv C_2^\mu \mod \pi^{p+1},
\]
which leads to
\[
1 + \sigma(V(\mu)) + p\sigma(W_1) \equiv 1 + A(\mu) + p\mu W_1 \mod \pi^{p+1},
\]
\[
1 + \sigma(V(\mu)) + p\sigma(W_2) \equiv 1 + A(\mu) + p\mu W_2 \mod \pi^{p+1},
\]
where $A(\mu) \in \mathbb{Q}(\zeta), \ v_\pi(A(\mu)) \geq 0$ depends only on $\mu$. By difference, we get
\[
p(\sigma(W_1 - W_2)) \equiv p\mu(W_1 - W_2) \mod \pi^{p+1},
\]
which implies that
\[
\sigma(W_1 - W_2) \equiv \mu(W_1 - W_2) \mod \pi^2.
\]
Let $W_1 - W_2 = a\lambda + b, \ a, b \in \mathbb{Z}, \ \lambda = \zeta - 1$. The previous relation implies that $b(1 - \mu) \equiv 0 \mod p$ and so that $a\sigma(\lambda) + b \equiv \mu a\lambda + \mu b \mod \pi^2$, and so that $b \equiv 0 \mod p$, because $\mu \neq 1$. Thus $W_1 - W_2 \equiv 0 \mod \pi$ and finally $C_1 \equiv C_2 \mod \pi^p$ and also $C_1 C_2^{-1} \equiv 1 \mod \pi^p$ and $C_1 C_2^{-1}$ is singular primary.

**Corollary 3.14.** Let $C_1, \ldots, C_\nu, \ 1 \leq \nu \leq r_p^-$, singular not primary, defined by relation (14) p. 22.

1. If $\mu_1 = \cdots = \mu_\nu = \mu$ then $C'_1 = C_1 \times C_\nu^{-1}, \ldots, C'_{\nu-1} = C_{\nu-1} \times C_\nu^{-1}$ are singular primary.

2. In term of ideals, it implies that
\[
\bigoplus_{i=1}^\nu < Cl(b_i) > = \bigoplus_{i=1}^{\nu-1} < Cl(b_i b_\nu^{-1}) > \oplus < Cl(b_\nu) >,
\]
where $\sigma(b_i b_\nu^{-1}) \simeq (b_i b_\nu^{-1})^\mu$

**Proof.**

1. Immediate consequence of theorem 3.13 p. 25

2. $\bigoplus_{i=1}^\nu < Cl(b_i) >$ is a $p$-group of rank $\nu$. $\bigoplus_{i=1}^{\nu-1} < Cl(b_i b_\nu^{-1}) >$ is a $p$-group of rank $\nu - 1$. $< Cl(b_\nu) >$ is a $p$-group of rank 1.
Remark: It follows that, when \( \mu_1 = \cdots = \mu_\nu = \mu \), we can suppose without loss of generality, with usual meaning of indexing \( i = 1, \ldots, r_p^− \), that the representants \( C_1, \ldots, C_\nu−1 \) chosen are singular primary.

**Theorem 3.15.** ***On structure of \( p \)-class group \( C_p^− \).***

Let \( b_i \) be the ideals defined in relation (17) p. 24. Let \( C_p^− = \bigoplus_{i=1}^{r_p^-} < Cl(b_i) >. \)

Let \( C_i = \frac{B_i}{B_i} \), \( B_i \mathbb{Z}[\zeta] = b_i^p \), \( Cl(b_i) \in C_p^−, \) \( i = 1, \ldots, r_p^- \), where \( B_i \) is defined in relation (13) p. 22. Let \( r_1^- \) be the degree of the minimal polynomial \( P_{r_1}(\sigma) \) defined in relation (16) p. 21. With a certain ordering of \( C_i, \) \( i = 1, \ldots, r_p^- \),

1. \( C_i \) are singular primary for \( i = 1, \ldots, r_p^+ \), and \( C_i \) are singular not primary for \( i = r_p^+ + 1, \ldots, r_p^- \).

2. (a) If \( j > i \geq r_p^+ + 1 \) then \( \mu_j \neq \mu_i \).
   (b) If \( \mu_i = \mu_j \) then \( j < i \leq r_p^+ \).

3. \( r_p^- - r_p^+ \leq r_1^- \leq r_p^- \).

**Proof.**

1. It is an application of a theorem of Furwangler, see Ribenboim [6] (6C) p. 182 and of a theorem of Hecke, see Ribenboim [6] (6D) p. 182.

2. See lemma 3.13 p. 25.

3. Apply corollary 3.14 p. 26.

\[ \square \]

### 3.4.2 \( \pi \)-adic congruences connected to \( p \)-class group \( C_p^+ \)

For \( i = r_p^+ + 1, \ldots, r_p \), to simplify notations in this lemma, let us note respectively \( b, B \) for ideal \( b_i \) and algebraic integer \( B_i \), as defined in the two relations (10) p. 20 and (14) p. 22.

**Theorem 3.16.** ***

Let the ideals \( b \), such that \( Cl(b) \in C_p^+ \) defined in relation (10) p. 22. There exists \( B \in \mathbb{Z}[\zeta] \) such that:

- \( \mu = u_{2n}, \) \( 1 \leq n \leq \frac{p-3}{2} \)
- \( \sigma(b) \simeq b^\mu, \)
- \( B \mathbb{Z}[\zeta] = b^p, \)
- \( \sigma(B) = B^\mu \times \alpha^p, \) \( \alpha \in \mathbb{Q}(\zeta), \)
- \( B \equiv 1 \mod \pi^{2n}. \)

(21) 27
Proof. Similarly to relation (13) p. 22, there exists $B$ with $BZ[\zeta] = b^p$ such that

$$\sigma(B) = B^\mu \times \alpha^p \times \eta, \quad \alpha \in \mathbb{Q}(\zeta), \quad \eta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*.$$  

From relation (32) p. 36, independent forward reference in section dealing of unit group $\mathbb{Z}[\zeta+\zeta^{-1}]^*$, we can write

$$\eta = \eta_1^{\lambda_1} \times \left( \prod_{j=2}^{N} \eta_j^{\lambda_j} \right), \quad \lambda_j \in \mathbb{F}_p, \quad 1 \leq N < \frac{p-3}{2},$$

$$\sigma(\eta_1) = \eta_1^\mu \times \beta_1^p, \quad \eta_1, \beta_1 \in \mathbb{Z}[\zeta+\zeta^{-1}]^*,$$

$$\sigma(\eta_j) = \eta_j^{\nu_j} \times \beta_j^p, \quad \eta_j, \beta_j \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad j = 2, \ldots, N,$$

$$2 \leq j < j' \leq N \Rightarrow \nu_j \neq \nu_{j'},$$

$$\nu_j \neq \mu, \quad j = 2, \ldots, N.$$  

Let us note

$$E = \eta_1^{\lambda_1}, \quad U = \prod_{j=2}^{N} \eta_j^{\lambda_j}.$$  

Show that there exists $V \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$ such that

$$\sigma(V) \times V^{-\mu} = U^{-1} \times \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta+\zeta^{-1}]^*.$$  

Let us suppose that $V$ is of form $V = \prod_{j=2}^{N} \eta_j^{\rho_j}$. Then, it suffices that

$$\eta_j^{\rho_j \nu_j} \times \eta_j^{-\rho_j \mu} = \eta_j^{-\lambda_j} \times \varepsilon_j^p, \quad \varepsilon_j \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad j = 2, \ldots, N.$$  

It suffices that

$$\rho_j \equiv -\lambda_j \mod p, \quad j = 2, \ldots, N,$$

which is possible, because $\nu_j \neq \mu, \quad j = 2, \ldots, N$. Therefore, for $B' = B \times V$, we get $B = B'V^{-1}$ and so

$$\sigma(B) = \sigma(B'V^{-1}) = B^\mu \alpha^p \eta = (B'V^{-1})^\mu \alpha^p \eta = (B'V^{-1})^\mu \times \alpha^p \times E \times U,$$

so

$$\sigma(B') = (B')^\mu \sigma(V) V^{-\mu} \times \alpha^p \times E \times U,$$

so

$$\sigma(B') = (B')^\mu (U^{-1} \varepsilon^p \times \alpha^p \times E \times U),$$

so we get simultaneously

$$\sigma(B') = (B')^\mu \times \alpha^p \times \varepsilon^p \times E, \quad \alpha \in \mathbb{Q}(\zeta),$$

$$\sigma(E) = E^\mu \times \varepsilon_1^p, \quad \varepsilon_1 \in \mathbb{Z}[\zeta+\zeta^{-1}]^*.$$  

28
Show that

\( (22) \quad \sigma(B') = B'^\mu \times \alpha'^p. \)

1. If \( E \in (\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p \), then we get

\( (23) \quad \sigma(B') = B'^\mu \times \alpha'^p. \)

2. If \( E \notin (\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p \) then by conjugation \( \sigma \),

\[
\begin{align*}
\sigma(B') &= (B')^\mu \times \alpha_1^p \times E, \quad \alpha_1 \in \mathbb{Q}(\zeta), \\
\sigma^2(B') &= \sigma(B')^\mu \times E^\mu \times \beta^p, \quad \beta \in \mathbb{Q}(\zeta),
\end{align*}
\]

so gathering these relations

\[
\begin{align*}
\sigma(B')^\mu &= (B')^\mu \times \alpha_1^p \times E^\mu, \\
\sigma^2(B') &= \sigma(B')^\mu \times E^\mu \times \beta^p,
\end{align*}
\]

and so

\[
c^p \times \sigma(B')^\mu (B')^{-\mu^2} = \sigma^2(B') \sigma(B')^{-\mu}, \quad c \in \mathbb{Q}(\zeta)
\]

which leads to

\[
c^p B'^\mu (B')^{-\mu^2} = B'^{\mu^2} (B')^{-\mu^2},
\]

and so

\[
(B')^{(\sigma^p - 1)} = c^p, \quad c \in \mathbb{Q}(\zeta).
\]

Elsewhere \( (B')^{p-2} = 1 \), so

\[
(B')^{p\mu^2} = \beta^p, \quad \beta \in \mathbb{Q}(\zeta),
\]

and so \( \sigma(B') = (B')^\mu \times \alpha_3^p \).

The end of proof is similar to proof of previous lemma \( \text{3.10 p. 23} \) \( \square \)

### 3.4.3 \( \pi \)-adic congruences connected to \( p \)-class group \( C_p \)

Let us consider the ideals \( b_i, \quad i = 1, \ldots, r_p \), defined in relation \( \text{10 p. 20} \) Then \( Cl(b_i) \in C_p \). From theorem \( \text{3.10 p. 23} \) and theorem \( \text{3.16 p. 27} \) we can choose the corresponding singular primary number \( B_i \) with \( B_i \mathbb{Z}([\zeta]) = b_i^p \); then \( \sigma(B_i) = B_i^\mu \times \alpha_i^p, \quad \alpha_i \in \mathbb{Q}(\zeta), \quad \mu_i = u_{m_i}, \quad 1 \leq m_i \leq \pi - 2 \). Observe that if \( m_i \) is odd then \( Cl(b_i) \in C_p^- \) and if \( m_i \) is even then \( Cl(b_i) \in C_p^+ \).

The next important theorem \textbf{summarize} for all the \( p \)-class group \( C_p \) the previous theorems \( \text{3.9 p. 22} \) and \( \text{3.10 p. 23} \) for relative \( p \)-class group \( C_p^- \) and \( \text{3.16 p. 27} \) for \( p \)-class group \( C_p^+ \) and give explicit \( \pi \)-adic congruences connected to \( p \)-class group of \( \mathbb{Q}(\zeta) \).
Theorem 3.17. *** \( \pi \)-adic structure of \( p \)-class group \( C_p \)

Let the ideals \( b_i \), \( i = 1, \ldots, r_p \), such that \( Cl(b_i) \in C_p \) and defined by relation (10) p. 20. Then, there exists singular algebraic integers \( B_i \in \mathbb{Z}[\zeta] \), \( i = 1, \ldots, r_p \), such that

\[
\mu_i = u_{m_i}, \quad 1 \leq m_i \leq p - 2, \quad i = 1, \ldots, r_p,
\]
\[
\sigma(b_i) \simeq b_i^{\mu_i},
\]
\[
(B_i) = B_i^p, \quad \sigma(B_i) = B_i^{\mu_i} \times \alpha_i^p, \quad \alpha_i \in \mathbb{Q}(\zeta),
\]
\[
B_i \equiv 1 \mod \pi^m_i.
\]

Moreover, with a certain reindexing of \( i = 1, \ldots, r_p \):

1. The \( r_p^+ \) singular integers \( B_i \), \( i = 1, \ldots, r_p^+ \), corresponding to \( b_i \in C_p^- \) are primary with \( \pi^m_i \mid B_i - 1 \).

2. The \( r_p^- - r_p^+ \) singular integers \( B_i \), \( i = r_p^+ + 1, \ldots, r_p^- \), corresponding to \( b_i \in C_p^- \) are not primary and verify \( \pi^m_i \parallel (B_i - 1) \).

3. The \( r_p^+ \) singular numbers \( B_i \), \( i = r_p^- + 1, \ldots, r_p \), corresponding to \( b_i \in C_p^+ \) are primary or not primary (without being able to say more) and verify \( \pi^m_i \mid (B_i - 1) \).

Proof.

1. For the case \( C_p^- \), apply lemmas 3.10 p. 23 and theorem 3.15 p. 27. Toward this result, observe also that if \( B_i \) is not primary, then \( \pi^{2m_i+1} \parallel (B'_i)^{p-1} - 1 \) and so \( \pi^{p-1} \parallel (B'_i)^{p-1} - 1 \) and \( C' = \frac{(B'_i)^{p-1} - 1}{B'_i} \) is not singular primary, therefore \( B'_i \) primary \( \iff \ C'_i = \frac{B'_i}{B'_i} \) primary.

2. For the case \( C_p^+ \) apply the theorem 3.16

\( \square \)

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

In the next lemma 3.18 p. 31 and theorem 3.19 p. 32, we shall investigate more deeply the consequences of the congruence \( C \equiv 1 \mod \pi^{2m+1} \) of lemma 3.9 p. 22 when \( 2m + 1 > \frac{p-1}{2} \).
Lemma 3.18. Let $C$ with $\mu = u_{2m+1}$, $2m + 1 > \frac{p-1}{2}$ written in the form:

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

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

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

Then $C$ verifies the congruences

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

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

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

$$ \vdots $$

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

Proof. We have seen in lemma 3.8 p. 21 that $\sigma(C) \equiv C^\mu \mod \pi^{p+1}$. From $2m + 1 > \frac{p-1}{2}$ we derive that

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

Elsewhere, we get by conjugation

$$ (25) \quad \sigma(C) = 1 + \gamma + \gamma_0 \zeta^u + \gamma_1 \zeta^{u^2} + \cdots + \gamma_{p-3} \zeta^{u_{p-2}}. $$

We have the identity

$$ \gamma_{p-3} \zeta^{u_{p-2}} = -\gamma_{p-3} - \gamma_{p-3} \zeta - \cdots - \gamma_{p-3} \zeta^{u_{p-3}}. $$

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

The next theorem gives an explicit important formulation of $C$ when $2m+1 > \frac{p-1}{2}$.

**Theorem 3.19.*** Let $\mu = u_{2m+1}$, $p - 2 \geq 2m + 1 > \frac{p-1}{2}$, corresponding to $C$ defined in lemma 3.18 p. 31, so $\sigma(C) \equiv C^\mu \mod \pi^{p+1}$. Then $C$ verifies the formula:

$$C \equiv 1 - \frac{\gamma_{p-3}}{\mu - 1} \times (\zeta + \mu^{-1}\zeta u + \cdots + \mu^{-2}\zeta u_{p-2}) \mod \pi^{p-1}.$$  

**Proof.** 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 3.18 p. 31, we obtain the relations

$\mu = u_{2m+1},$

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

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

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

$\vdots$

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

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

From these relations we get

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

Then

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

Then

$V \equiv -\gamma_{p-3} \times \left(\frac{1}{\mu - 1} + \mu^{-1}(\frac{(\mu^{-1} - 1)\zeta + (\mu^{-(p-1)} - 1)\zeta u_{p-3}}{\mu^{-1} - 1})}\right) \mod p.$

32
Then

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

Then \(-\zeta - \zeta^u - \ldots - \zeta^{u_{p-3}} = 1 + \zeta^{u_{p-2}}\) and \(\mu^{- (p-1)} \equiv 1 \mod p\) implies that

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

Then

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

Then \(\frac{1}{\mu - 1} + \frac{\mu^{-1}}{\mu^{-1} - 1} = 0\) and so

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

\[ \Box \]
4 On structure of the $p$-unit group of the cyclotomic field $\mathbb{Q}(\zeta)$

Let us consider the results obtained in subsection 3.4 for the action of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ on $C_p^{-}$. In the present section, we assert that this approach can be partially translated mutatis mutandis to the study of the $p$-group of units of $\mathbb{Q}(\zeta)$

$$F = \{\mathbb{Z}[\zeta + \zeta^{-1}]^*/(\mathbb{Z}[\zeta + \zeta^{-1}]^p)^p\}/\langle -1 \rangle.$$ 

This section contains:

- Some general definitions and properties of the $p$-unit group $F$.
- Some $\pi$-adic congruences strongly connected to structure of the $p$-unit group $F$.

These congruences are of the same kind as those found in previous chapter for $p$-class group $C_p$.

4.1 Definitions and preliminary results

- When $h^{-} \equiv 0 \mod p$, from Hilbert class field theory, there exists primary units $\eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$, so that

$$\eta \equiv d^p \mod p, \quad d \in \mathbb{Z}, \quad d \neq 0,$$

$$\sigma(\eta) = \eta^\sigma \times \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^*.$$ (27)

- The group $\mathbb{Z}[\zeta + \zeta^{-1}]^*$ is a free group of rank $\frac{p-1}{2}$. It contains the subgroup $\{-1, 1\}$ of rank 1. For all $\eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* - \{-1, 1\}$

$$\eta \times \sigma(\eta) \times \cdots \times \sigma(\frac{p-3}{2})(\eta) = \pm 1.$$ 

Therefore, for each unit $\eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$, there exists a minimal $r_\eta \in \mathbb{N}$, $r_\eta \leq \frac{p-3}{2}$, such that

$$\eta \times \sigma(\eta)^{l_1} \times \cdots \times \sigma^{r_\eta}(\eta)^{l_{r_\eta}} = \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^*,$$

$$0 \leq l_i \leq p - 1, \quad i = 1, \ldots, r_\eta, \quad l_{r_\eta} \neq 0.$$ (28)

- Let us define an equivalence on units of $\mathbb{Z}[\zeta + \zeta^{-1}]^*$: $\eta, \eta' \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$ are said equivalent if there exists $\varepsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$ such that $\eta' = \eta \times \varepsilon^p$. Let us denote $E(\eta)$ the equivalence class of $\eta$.

- We have $E(\eta_a \times \eta_b) = E(\eta_a) \times E(\eta_b)$; the set of class $E(\eta)$ is a group. The group $< E(\eta) >$ generated by $E(\eta)$ is cyclic of order $p$. 

34
Lemma 4.1. Let \( \mu \) for \( \eta \). Suppose that \( \mu \) null and therefore \( E(\eta) = 1 \). There exists a group \( F = \{ \mathbb{Z}[\zeta + \zeta^{-1}] \} / (\mathbb{Z}[\zeta + \zeta^{-1}]^p, \langle -1 \rangle \) so defined is a group of rank \( \frac{p-3}{2} \), see for instance Ribenboim [6] p 184 line 14.

Similarly to relation (5) p.15, there exists \( \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \) such that
\[
E(\eta) = E(\eta_1) \times \cdots \times E(\eta_{(p-3)/2}),
\]
\[
E(\sigma(\eta_i)) = E(\eta_i^{\mu_i}), \quad i = 1, \ldots, \frac{p-3}{2},
\]
\( \mu_i \in \mathbb{N}, \quad 1 < \mu_i \leq p - 1, \)
\[
F = \langle E(\eta_1) > \oplus \cdots \oplus E(\eta_{(p-3)/2}) >, \]
where \( F \) is seen as a \( F_p[G] \)-module of dimension \( \frac{p-3}{2} \).

For each unit \( \eta \), there is a minimal polynomial \( P_{r_{\eta}}(V) = \prod_{i=1}^{r_{\eta}} (V - \mu_i) \) where \( r_{\eta} \leq \frac{p-3}{2} \), such that
\[
E(\eta)^{P_{r_{\eta}}(\sigma)} = E(1),
\]
\[
1 \leq i \leq j \leq r_{\eta} \Rightarrow \mu_i \neq \mu_j.
\]

Let \( \beta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \). Observe that if \( E(\beta) = E(\sigma(\beta)) \) then \( E(\sigma^2(\beta)) = E(\beta) \) and so \( E(1) = E(\beta^{p-1}) \) and \( E(\beta) = 1 \).

Recall that a unit \( \beta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \) is said primary if \( \beta \equiv b^p \mod \pi^{p+1} \), \( b \in \mathbb{Z} \).

**Lemma 4.1.** Let \( \beta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* - \langle \mathbb{Z}[\zeta + \zeta^{-1}]^* \rangle^p \). Then the minimal polynomial \( P_{r_{\beta}}(V) \) is of the form
\[
P_{r_{\beta}}(V) = \prod_{i=1}^{r_{\beta}} (V - u_{2m_i}), \quad 1 \leq m_i \leq \frac{p-3}{2}, \quad r_{\beta} > 0.
\]

**Proof.** There exists \( \eta_1 \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \), \( E(\eta_1) \neq E(1) \), with \( E(\eta_1)^{\sigma - \mu_1} = E(1) \). Suppose that \( \mu_1^{(p-1)/2} = -1 \) and search for a contradiction: we have \( E(\eta_1)^{\sigma - \mu_1} = E(1) \), therefore \( E(\eta_1)^{\sigma(p-1)/2 - \mu_1^{(p-1)/2}} = E(1) \); but, from \( \eta_1 \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \), we get \( \eta_1^{(p-1)/2} = \eta_1 \) and so \( E(\eta_1)^{1 - \mu_1^{(p-1)/2}} = E(1) \), or \( E(\eta_1)^2 = E(1) \), so \( E(\eta_1)^2 \) is of rank null and therefore \( E(\eta_1) = E(\eta_1)^{2(p+1)/2} \) is also of rank null, contradiction. The same for \( \mu_i, \quad i = 1, \ldots, r_{\beta} \). \( \square \)
4.2 $\pi$-adic congruences on $p$-unit group $F$ of $\mathbb{Q}(\zeta)$

The results on structure of relative $p$-class group $C_{p}^{-}$ of subsection 3.4 p. 19 can be translated to some results on structure of the group $F$: from $\eta_i^{p-1} \equiv 1 \mod \pi$ and from $< E(\eta_i^{p-1}) > = < E(\eta_i) >$, we can always, without loss of generality, choose the determination $\eta_i$ such that $\eta_i \equiv 1 \mod \pi$. We have proved that

$$\eta_i \equiv 1 \mod \pi,$$

$$\sigma(\eta_i) \equiv \eta_i^{\mu_i} \mod \pi^{b+1}.$$  

Then, starting of this relation (31), similarly to lemma 3.9 p. 22 we get:

$\pi$-adic congruences of unit group $F = \{\mathbb{Z}[(\zeta + \zeta^{-1})^p]/\mathbb{Z}[(\zeta + \zeta^{-1})^p]/ < -1 >$

This theorem summarize our $\pi$-adic approach on group of $p$-units $F$.

**Theorem 4.2.** ***With a certain ordering of index $i = 1, \ldots, \frac{p-3}{2}$, there exists a fundamental system of units $\eta_i$, $i = 1, \ldots, \frac{p-3}{2}$, of the group $F = \{\mathbb{Z}[(\zeta + \zeta^{-1})^p]/\mathbb{Z}[(\zeta + \zeta^{-1})^p]/ < -1 >$ verifying the relations:

$$\eta_i \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad i = 1, \ldots, \frac{p-3}{2},$$

$$\mu_i = u_{2\eta_i}, \quad 1 \leq \eta_i \leq \frac{p-3}{2}, \quad i = 1, \ldots, \frac{p-3}{2},$$

$$\sigma(\eta_i) = \eta_i^{\mu_i} \times \varepsilon_i^p, \quad \varepsilon_i \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad i = 1, \ldots, \frac{p-3}{2},$$

$$\sigma(\eta_i) \equiv \eta_i^{\mu_i} \mod \pi^{p+1}, \quad i = 1, \ldots, \frac{p-3}{2},$$

$$\pi^{2\eta_i} \parallel \eta_i - 1, \quad i = 1, \ldots, r_p^+, \quad \eta_i \ not \ primary,$$

$$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i > 0, \quad i = r_p^+ + 1, \ldots, r_p, \quad \eta_i \ primary, $$

$$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i \geq 0, \quad i = r_p^+ + 1, \ldots, r_p, \quad \eta_i \ primary \ or \ not \ primary$$

$$\pi^{2\eta_i} \parallel \eta_i - 1, \quad i = r_p + 1, \ldots, \frac{p-3}{2}, \quad \eta_i \ not \ primary.$$  

**Proof.**

1. We are applying in this situation the same $\pi$-adic theory to $p$-group of units $F = \mathbb{Z}[(\zeta + \zeta^{-1})^p]/\mathbb{Z}[(\zeta + \zeta^{-1})^p]$ than to relative $p$-class group $C_{p}^{-}$ in subsection 3.4 p. 19 with a supplementary result for units due to Denes, see Denes [1] and Ribenboim [6] (8D) p. 192.
2. Similarly to decomposition of components of $C_p$ in singular primary and singular not primary components, the rank $\frac{p^3}{2} - \rho_1$ of $F$ has two components $\rho_1$ and $\frac{p^3}{2} - \rho_1$ where $\rho_1$ corresponds to the maximal number of independent units $\eta_i$ primary and $\rho_2 = \frac{p^3}{2} - \rho_1$ to the units $\eta_i$ not primary.

The next lemma for the unit group $\mathbb{Z}[\zeta + \zeta^{-1}]^*$ is the translation of similar lemma 3.13 p. 25 for the relative $p$-class group $C_p^\ast$.

**Lemma 4.3.*** Let $\eta_1, \eta_2$ defined by relation (32) p. 36. If $\mu_1 = \mu_2$ then $\eta_1 \times \eta_2^{-1}$ is a primary unit.

The group $F = \mathbb{Z}[\zeta + \zeta^{-1}]^*/(\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p$ can be written as the direct sum $F = F_1 \oplus F_2$ of a subgroup $F_1$ with $\rho_1$ primary units ($p$-rank $\rho_1$ of $F_1$) and of a subgroup $F_2$ with $\rho_2 = \frac{p^3}{2} - \rho_1$ fundamental not primary units ($p$-rank $\rho_2$ of $F_2$): towards this assertion, observe that if $\eta_1$ and $\eta_2$ are two not primary units with $\sigma(\eta_1) \times \eta_2^{-\mu} \in (\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p$ and $\sigma(\eta_2) \times \eta_1^{-\mu} \in (\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p$ then $\eta_1 \times \eta_2^{-1}$ is a primary unit and it always possible to replace $\{\eta_1, \eta_2\}$ by $\{\eta_1 \times \eta_2^{-1}, \eta_2\}$ in the basis of $F$, so to push all the primary units in $F_1$ and to make the set $F_2$ of not primary units as a group. Observe that $\rho_1$ can be seen also as the maximal number of independent primary units in $F$.

**Structure theorem of unit group** $F = \mathbb{Z}[\zeta + \zeta^{-1}]^*/(\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p$

**Theorem 4.4.*** Let $r_p^-$ be the relative $p$-class group of $Q(\zeta)$. Let $r_p^+$ be the $p$-class group of $Q(\zeta + \zeta^{-1})$. Let $\rho_1$ be the number of independent primary units of $F$. Then

$$r_p^- - r_p^+ \leq \rho_1 \leq r_p^-. \quad (33)$$

**Proof.** We apply Hilbert class field theory: for a certain order of the indexing of $i = 1, \ldots, \frac{p^3}{2}$:

1. There are exactly $r_p^+$ independent unramified cyclic extensions $Q(\zeta, \omega_i)/Q(\zeta)$, $\omega_i^p \in \mathbb{Z}[\zeta + \zeta^{-1}] - \mathbb{Z}[\zeta + \zeta^{-1}]^*$, $i = 1, \ldots, r_p^+$.

2. There are exactly $r_p^- - r_p^+ = r_p^-$ independent unramified cyclic extensions $Q(\zeta, \omega_i)/Q(\zeta)$, $\omega_i^p \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$, $i = r_p^+ + 1, \ldots, r_p^-$.  

37
3. There is a number \( n \) on independant unramified cyclic extensions with \( 0 \leq n \leq r_p^+ \) with

\[
\mathbb{Q}(\zeta, \omega_i)/\mathbb{Q}(\zeta), \quad \omega_i^p \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad i = r_p^- + 1, \ldots, r_p.
\]

4. There are no independant unramified cyclic extensions with

\[
\mathbb{Q}(\zeta, \omega_i)/\mathbb{Q}(\zeta), \quad \omega_i^p \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad i = r_p + 1, \ldots, \frac{p - 3}{2}.
\]

The case \( \mu = u_{2n} \) with \( 2n > \frac{p-1}{2} \)

In the next theorem we shall investigate more deeply the consequences of the congruence \( \eta_i \equiv 1 \mod \pi^{2n} \) when \( 2n_i > \frac{p-1}{2} \). We give an explicit congruence formula in that case. To simplify notations, we take \( \eta, \mu, n \) for \( \eta_i, \mu_i, n_i \). The next theorem for the \( p \)-unit group \( F = \{ \mathbb{Z}[\zeta + \zeta^{-1}]^*/(\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p \}/ < -1 > \) is the translation of similar theorem 3.19 p. 32 for the relative \( p \)-class group \( C_p^- \).

**Theorem 4.5.** *** Let \( \mu = u_{2n}, \quad p - 3 \geq 2n > \frac{p-1}{2}, \) corresponding to \( \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \) defined in relation (32) p. 30 so \( \sigma(\eta) = \eta^\mu \times \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^* \). Then \( \eta \) verifies the explicit formula:

\[
(34) \quad \eta \equiv 1 - \frac{\gamma_{p-3}}{\mu - 1} \times (\zeta + \mu^{-1} \zeta^u + \cdots + \mu^{-(p-2)} \zeta_u p^{-2}) \mod \pi^{p-1}, \quad \gamma_{p-3} \in \mathbb{Z}.
\]
References

[1] P. Dénes, *Uber irregulare Kreiskörper*, Publ. Math. Debrecen, 3, 1954, pp. 17-23.

[2] P. Dénes, *Uber Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzzeigenchaften*, Publ. Math. Debrecen, 1954, pp. 195-204.

[3] P. Dénes, *Uber den zweiten Faktor der Klassenzahl und den Irregularitätsgrad der irregulären Kreiskörper*, Publ. Math. Debrecen, 4, 1956, pp. 163-170.

[4] P. Furtwangler, *Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers*, Math Annalen, 63, 1907, 1-37.

[5] E. Hecke, *Uber nicht-reguläre Primzahlen und der Fermatschen Satz*, Nachr Akad. d. Wiss. Gottingen, 1910, 429-434.

[6] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[7] K. Ribet, *A modular construction of unramified $p$–extensions of $\mathbb{Q}(\mu_p)$*, Invent. Math. no 34, 1976, pp. 151-162.

[8] L. Stickelberger *Über eine Verallgemeinerung der Kreistheilung*, Math. Annal., 37 , 1890, pp 321-367.

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

Roland Quême
13 avenue du château d’eau
31490 Brax
France
2005 fev 04
tel : 0033561067020
mailto: roland.queme@wanadoo.fr
home page: [http://roland.queme.free.fr/](http://roland.queme.free.fr/)