Picard Groups of Integral Group Rings of Cyclic p-Groups

Staffan Jönsson

Abstract: The aim of our paper is to review the results obtained in [K-M] and some other relevant papers ([G1, G2, O, St1, U1, U2]) on the structure of $K_0(\mathbb{Z}\pi)$ for a cyclic group π of prime power order. Using a new method, we also reprove results of [K-M] for a cyclic group of order p^3 in the case p is a regular prime number (results obtained in [K-M] are based on an advanced Iwasawa theory while we use more elementary methods).

Acknowledgements: I would like to thank my advisor Alexander Stolin for patience, guidance and support. I am also very grateful to Yumi Karlsson and Ola Helenius for their help in the preparation of this paper.

Contents

§1 Introduction **1**

1.1 Preliminaries . . . 1

1.2 Properties of K_0A . . . 2

1.3 Dedekind Domains . . . 3

1.4 Milnor's Construction of Projective Modules . . . 4

1.5 K_1A and the Mayer-Vietoris Sequence . . . 5

1.6 Integral Group Rings . . . 7

1.7 Rim's Theorem . . . 10

§2 Some General Results on $\mathbb{Z}C_{p^n}$ **12**

2.1 Results of Kervaire and Murthy . . . 12

2.2 Results of Galovich . . . 20

2.3 Refinements and Other Important Results . . . 21

2.4 Some Results from Class Field Theory . . . 22

§3 On Pic($\mathbb{Z}C_{p^3}$) **23**

3.1 Presentation of the Problem . . . 23

3.2 Structure of $U(D_2)$ . . . 23

3.3 Im $\{E_2 \oplus U(A_2) \to U(D_2)\}$ . . . 25

3.4 The c -map and Kummer's Lemma . . . 26

3.5 Structure of Im $\{U(A_2) \to U(D_2)\}$ . . . 27

3.6 A Variant of Kummer's Theorem . . . 32

§4 References **41**

§1 Introduction

The algebraic K-theory has a rather long history. Some early works by Higman in 1940 [Hig] and Whitehead in 1939 [W] are recognized as first papers of the K-theory. However the subject really began with Grothendieck's work [BSG] on the Riemann-Roch theorem in 1958. Here Grothendieck introduced the functor K, now known as K_0. The best known application of his functor K_0 is the topological K-theory developed by Atiyah and Hirzebruch in 1961 in [A-H]. The next step in the algebraic K-theory was done by Bass [B1] who defined K_1-functor in the case of rings. It turned out to be the same as one introduced by Whitehead. In 1969 Milnor showed how to define all the projective modules over a Cartesian diagram of ring homomorphisms. He succeeded in constructing an exact Mayer-Vietoris sequence for the Cartesian diagram, which links K_1- and K_0-functors (see [M]).

One of the most important initial problems in algebraic K-theory is simply to compute the groups $K_0(R)$ for various rings R, among which group rings $\mathbb{Z}\pi$ play an important role because of topological applications.

On the International Congress of Mathematicians in 1970, in Nice, R.G. Swan announced that $K_0(\mathbb{Z}\pi)$ was computed by Kervaire and Murthy for π cyclic of prime power order. However when they published their paper in 1977 ([K-M]), it turned out that this was just partially true.

The aim of our paper is to review the results obtained in [K-M] and some other relevant papers ([G1, G2, O, St1, U1, U2]) on a structure of $K_0(\mathbb{Z}\pi)$ for the cyclic group π of prime power order. Using a new method, we also reprove results of [K-M] for a cyclic group of order p^3 in the case p is a regular prime number (results obtained in [K-M] are based on an advanced Iwasawa theory while we use more elementary methods).

1.1 Preliminaries

In the sequel p will denote a prime number ≥ 3. As usual $\mathbb{Z}$ is the ring of rational integers and $\mathbb{Q}$ is the field of rational numbers.

Let ζ_n be a primitive p^{n+1}-th root of unity, $n = 0, 1, \ldots$. It is well known that the ring $\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_n)$([R], pp. 265-268) and that $\mathbb{Z}[\zeta_n]$ is a Dedekind domain ([A-M], p. 96; [M], p.10).

In this paper we deal with associative unital rings and all ring homomorphisms map the unity to the unity.

If A_i, A' are rings and $j_i : A_i \to A'$, $i = 1, 2$, are ring homomorphisms, we can define a fibre product of the pair $\{j_1, j_2\}$ as

$$A := \{(a_1, a_2) | a_i \in A_i,\ j_1(a_1) = j_2(a_2)\}.$$

A turns out to be a ring and the diagram

$$\begin{tikzcd}
A \arrow[r, "i_1"] \arrow[d, "i_2"'] & A_1 \arrow[d, "j_1"'] \\
A_2 \arrow[r, "j_2"'] & A'
\end{tikzcd} \qquad (*)$$

is commutative with $i_k(a_1, a_2) = a_k$, $k = 1, 2$. We will say that A is the product of A_1 and A_2 over A'. The following example of this construction will arise in our applications: Let α, β be two-sided ideals of a ring A. Then one has the fibre product diagram (Cartesian square)

$$\begin{tikzcd}
A/\alpha \cap \beta \arrow[r] \arrow[d] & A/\alpha \arrow[d] \\
A/\beta \arrow[r] & A/(\alpha + \beta)
\end{tikzcd} \qquad (**)$$

where the maps are all canonical ring surjections ([C-R], Vol I, pp. 22-23; [M], p. 19).

1.2 Properties of K_0A

Let P be a finitely generated projective module over a ring A and let $[P]$ denote the isomorphism class of P. Define $[P] + [Q] = [P \oplus Q]$. It is easy to see that the sum is independent of the choice of representatives P and Q. Let E be the set of isomorphism classes with the operation defined above. Then E is a monoid. Now let $\mathcal{F}$ be the free abelian group generated by E with elements $\sum n_P < P >$, $n_P \in \mathbb{Z}$, where $< P >$ is the generator of $\mathcal{F}$ corresponding to $[P] \in E$. Note that $< P >=< Q >$ if and only if $[P] = [Q]$. Let $\mathcal{B}$ be the subgroup of $\mathcal{F}$ generated by all expressions $< P > + < Q > - < P \oplus Q >$. Then K_0A is defined as the quotient of $\mathcal{F}$ by $\mathcal{B}$.

It is easy to show that every element of K_0A can be represented as $[P] - [Q]$ for some $[P], [Q] \in E$.

The following lemma is well known (see for instance [M]).

Lemma 1.1. *If A is a local ring or a principal ideal domain, then every finitely generated, projective module over A is free, and $K_0A \cong \mathbb{Z}$.*

Now consider a homomorphism $f : A \to A'$ between two rings. For any A-module M we define the following A'-module

$$f_\# M := A' \otimes_A M$$

Note that $f_\# M$ is finitely generated and projective if M is finitely generated and projective. The map

$$[P] \mapsto [f_\# P]$$

provides a homomorphism

$$f_* : K_0A \to K_0A'$$

with $(\text{identity})_* = \text{identity}$ and $(f \circ g)_* = f_* \circ g_*$.

Let us consider the unique homomorphism

$$i : \mathbb{Z} \to A.$$

Clearly $K_0\mathbb{Z} \cong \mathbb{Z}$ (see above) and $i_*K_0\mathbb{Z} \cong \mathbb{Z}$. The cokernel

$$K_0A/i_*K_0\mathbb{Z}$$

is called the projective class group of A.

Suppose we have a homomorphism $j : A \to F$ into a field or skew-field F. Then we get

$$\begin{tikzcd}
K_0\mathbb{Z} \arrow[r, "i_*"] \arrow[d, equal] & K_0A \arrow[r, "j_*"] & K_0F \arrow[d, equal] \\
\mathbb{Z} & & \mathbb{Z}
\end{tikzcd}$$

Since $j_* \circ i_* = \text{identity map}$, we obtain a decomposition $K_0A = (\text{Im } i_*) \oplus (\text{Ker } j_*)$. Furthermore, since $\text{Im } i_* \cong \mathbb{Z}$ we obtain that Ker j_* is isomorphic to the projective class group of A usually denoted by $\tilde{K}_0A$.

If A is commutative, then K_0A has a commutative ring structure if we define

$$[P][Q] := [P \otimes Q].$$

Moreover, $\tilde{K}_0A$ becomes an ideal in K_0A and $K_0A \cong \mathbb{Z} \oplus \tilde{K}_0A$ ([M], pp. 6-8).

1.3 Dedekind Domains

Suppose we have two non-zero ideals α, β in a Dedekind domain A. They are said to belong to the same ideal class if there exist non-zero ring elements x and y so that $x\alpha = y\beta$. These ideal classes form an abelian group under multiplication. The class of principal ideals acts as identity element. The notation $Cl(A)$ will be used for the ideal class group of A ([M], p. 9).

Lemma 1.2. *Every ideal in a Dedekind domain A is projective over A. Moreover, every finitely generated projective module over A is isomorphic to a direct sum $\alpha_1 \oplus \ldots \oplus \alpha_k$ of ideals.*

Lemma 1.3. *If α and β are non-zero ideals in a Dedekind domain A, then the module $\alpha \oplus \beta$ is isomorphic to $A \oplus (\alpha\beta)$.*

Theorem 1.1. *Let A be a Dedekind domain. Then $K_0A \cong \mathbb{Z} \oplus \tilde{K}_0A$, where the additive group of $\tilde{K}_0A$ is canonically isomorphic to the ideal class group $Cl(A)$. Moreover, the product of any two elements in the ideal $\tilde{K}_0A$ is zero.*

The second isomorphism assertion in the theorem follows from Lemma 1.2 above and the correspondence

$$\begin{gathered} K_0A \to \mathbb{Z} \oplus Cl(A) \\ [\alpha_1 \oplus \ldots \oplus \alpha_r] \mapsto (r, \{\alpha_1 \cdots \alpha_r\}). \end{gathered}$$

Here $\{\alpha_1 \cdots \alpha_r\} \in Cl(A)$ is the ideal class of $\alpha_1 \cdots \alpha_r$.

A module M, over a commutative ring A, is said to be invertible if there exists a module N over A so that $M \otimes_A N \cong A$ (i.e., $M \otimes_A N$ is free on one generator). The set of isomorphism classes of invertible modules forms a group under the tensor product. We call this group the Picard group and denote it by Pic (A).

It is a well-known fact that for Dedekind domains Pic $(A) \cong Cl(A)$ ([A-M], cf. below). Hence $K_0A \cong \mathbb{Z} \oplus$ Pic (A) and Pic $(A) \cong \tilde{K_0}A$ ([M], pp. 10-15).

Let A be a local ring. If $M, N \in$ Pic (A), they are finitely generated and projective ([M], p. 15). Suppose N is inverse to M. By Lemma 1.1, $M \otimes N \cong A^m \otimes A^n \cong A^1$. Thus $m = n = 1$ and Pic $(A) = 0$.

Assume A is the ring of algebraic integers in an algebraic number field (A is Dedekind). Then $Cl(A)$ is finite. The order of this group is called the class number of the algebraic number field ([A-M], p. 98; [I-R], p. 178).

1.4 Milnor's Construction of Projective Modules

Now let us return to the Cartesian square $(*)$. We assume that at least one of j_1 and j_2 is surjective. Our purpose is to construct projective modules over A, using projective modules over A_1 and A_2.

First, let $f : A \to A_1$ be a ring homomorphism, and M a left A-module. As above, the A_1-module $A_1 \otimes_A M$ is denoted by $f_\# M$. Then we have an A-linear map

$$\begin{gathered} f_* : M \to f_\# M \\ f_*(m) := 1 \otimes_A m. \end{gathered}$$

$f_\# M$ is free over A_1 with basis $\{f_*(a_\alpha)\}$ if M is free over A with basis $\{a_\alpha\}$.

Basic construction: given projective modules P_k over A_k, $k = 1, 2$, how do we construct a projective module over A?

One now has

$$\begin{gathered} j_{k*} : P_k \to A' \otimes_{A_k} P_k \\ j_{k*}(p_k) = 1 \otimes_{A_k} p_k, \ k = 1, 2. \end{gathered}$$

The two A'-modules $j_{1\#}P_1 = A' \otimes_{A_1} P_1$ and $j_{2\#}P_2 = A' \otimes_{A_2} P_2$ must be isomorphic. Thus take a fixed isomorphism

$$h : j_{1\#}P_1 \to j_{2\#}P_2$$

over A'. Set

$$\begin{aligned} M = M(P_1, P_2, h) &:= \\ &:= \{(p_1, p_2) \in P_1 \times P_2 | h(j_{1*}(p_1)) = j_{2*}(p_2)\}. \end{aligned}$$

Clearly there is a commutative square

$$\begin{tikzcd} M \arrow[r] \arrow[d] & P_1 \arrow[d, "h \circ j_{1*}"] \\ P_2 \arrow[r, "j_{2*}"] & j_{2\#}P_2 \end{tikzcd}$$

where M is isomorphic to the product of P_1 and P_2 over $j_{2\#}P_2$.

M becomes a left A-module if we let

$$a \cdot (p_1, p_2) = (i_1(a) \cdot p_1, i_2(a) \cdot p_2);\ a \in A$$

([M], pp. 19-20).

The following result is valid.

Theorem 1.2. a) *The module $M = M(P_1, P_2, h)$ is projective over A. Furthermore if P_1 and P_2 are finitely generated over A_1 and A_2 respectively, then M is finitely generated over A.*

b) *Every projective A-module is isomorphic to $M(P_1', P_2', h)$ for some suitably chosen h and projective modules P_1', P_2' over A_1 and A_2 respectively.*

c) *The modules P_1 and P_2 are naturally isomorphic to $i_{1\#}M$ and $i_{2\#}M$, respectively. (*[M]*, p. 20).*

1.5 K_1A and the Mayer-Vietoris Sequence

We let $GL(n, A)$ be the general linear group of all $n \times n$ invertible matrices over a ring A. $GL(A)$ is the union of the sequence $GL(1, A) \subset GL(2, A) \subset GL(3, A) \subset \dots$, where each $GL(n, A)$ is embedded in $GL(n+1, A)$ by the injection

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

A matrix in $GL(A)$ is called elementary, if it coincides with the identity matrix, except for a single off-diagonal entry.

Lemma 1.4. *The elementary matrices in $GL(A)$ generate a subgroup $E(A) \subset GL(A)$. $E(A)$ is precisely equal to the commutator subgroup of $GL(A)$.*

Due to the properties of the commutator subgroup, we can say that $E(A)$ is normal in $GL(A)$ and the quotient $GL(A)/E(A)$ is an abelian group. The abelian group $GL(A)/E(A)$ – called the Whitehead group – is denoted by K_1A ([M], p. 25).

Now suppose A to be commutative. Then the determinant is defined. Let A^* denote the multiplicative group of units of A. The composition

$$A^* = GL(1, A) \subset GL(A) \overset{\det}{\to} A^*$$

is an identity map.

If $SL(A) \subset GL(A)$ is the kernel of the determinant homomorphism, we get a direct sum decomposition

$$K_1A \cong A^* \oplus (SL(A)/E(A))$$

(compare $K_0A \cong \mathbb{Z} \oplus \tilde{K}_0A$). Here $U \in SL(A) \Leftrightarrow \det U = 1$.

In applications $SL(A)$ is often generated by elementary matrices, i.e. $K_1A \cong A^*$. This is true for example if A is a local ring or the ring of integers in a finite extension of $\mathbb{Q}$ ([M], pp. 27-28, 159).

We start with the diagram $(*)$ in 1.1, satisfying the same conditions as before. It is now possible to construct the following exact sequence called the Mayer-Vietoris sequence

$$K_1A \overset{\alpha_1}{\to} K_1A_1 \oplus K_1A_2 \overset{\beta_1}{\to} K_1A' \overset{\partial}{\to} K_0A \overset{\alpha_0}{\to} K_0A_1 \oplus K_0A_2 \overset{\beta_0}{\to} K_0A'.$$

Here α_n, $n = 0, 1$, is induced by the homomorphisms $i_k : A \to A_k$ for $k = 1, 2$, $\beta_1(x, y) = j_{1*}(x)j_{2*}(y)^{-1}$ and $\beta_0(a, b) = j_{1*}(a) - j_{2*}(b)$.

The crucial part is to constuct $\partial : K_1A' \to K_0A$.

Let us represent $x \in K_1A'$ by a matrix in $GL(n, A')$. Then x is an isomorphism from the A'-module $j_{1\#}(A_1^n) = A_1^n \otimes_{A_1} A' \cong (A')^n$ to the A'-module $j_{2\#}(A_2^n) = A_2^n \otimes_{A_2} A' \cong (A')^n$. Hence, by the basic construction described above, we can form the projective module

$$M = M(A_1^n, A_2^n, x)$$

over A. Set

$$\partial(x) := [M] - [A^n] \in K_0A.$$

Write for simplicity $\partial(x) = M - A^n \in K_0A$. One can show that ∂ is well defined. We summarize:

Theorem 1.3. *The Mayer-Vietoris sequence is exact.*

([M], p. 28). A proof can be found in [C-R], Vol II, pp. 106-108. Here we will reproduce the exactness at K_0A.

The image of ∂ is the set

$$\{M(A_1^n, A_2^n, x) - A^n | x \in K_1A'\} = \{M(A_1^n, A_2^n, x) - M(A_1^n, A_2^n, 1) | x \in K_1A'\}$$

in a simplified notation.

We also have

$$\begin{aligned} &\alpha_0 : K_0A \to K_0A_1 \oplus K_0A_2 \\ &M(P_1, P_2, x) \overset{\alpha_0}{\mapsto} P_1 \oplus P_2, \end{aligned}$$

whence

$$M(A_1^n, A_2^n, x) - M(A_1^n, A_2^n, 1) \overset{\alpha_0}{\mapsto} (A_1^n - A_1^n) \oplus (A_2^n - A_2^n) \cong (0, 0),$$

i.e.,

$$\text{Im } \partial \subseteq \text{Ker } \alpha_0.$$

But

$$\begin{aligned} &\text{Ker } (K_0A \overset{\alpha_0}{\to} K_0A_1 \oplus K_0A_2) = \{M(P_1, P_2, h) - M(P_1, P_2, g) | P_i \in K_0A_i\} = \\ &\quad = \{M(A_1^n, A_2^n, h_1) - M(A_1^n, A_2^n, g_1)\} = \{\partial(h_1) - \partial(g_1)\} \end{aligned}$$

for some isomorphisms h, g, h_1, g_1 ([M], pp. 22-23). It follows

$$\text{Ker } \alpha_0 \subseteq \text{Im } \partial$$

and

$$\text{Ker } \alpha_0 = \text{Im } \partial.$$

Therefore the sequence is exact at K_0A.

1.6 Integral Group Rings

Let $G := \{g_1, g_2, \dots, g_k\}$ be a finite group. Form the ring $\mathbb{Z}G := \{a_1g_1 + \dots + a_kg_k | a_i \in \mathbb{Z}\}$ with operations

$$\sum_i a_ig_i + \sum_i b_ig_i = \sum_i (a_i + b_i)g_i \text{ and } (\sum_i a_ig_i)(\sum_j b_jg_j) = \sum_{i,j} a_ib_jg_ig_j.$$

We now assume that G is a cyclic group of order p^n. Then

$$G := C_{p^n} := \{1, g, g^2, \dots, g^{p^n-1} | g^{p^n} = 1\} \cong \mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}.$$

The ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}C_{p^n}$ sending x to g shows that $\mathbb{Z}C_{p^n} \cong \mathbb{Z}[x]/(x^{p^n} - 1)$.

As before $\zeta_n = e^{2\pi i/p^{n+1}}$, $n = 0, 1, \dots$. The number ζ_n and all its powers satisfy $x^{p^{n+1}} - 1 = 0$. Hence

$$x^{p^{n+1}} - 1 = (x-1)(x-\zeta_n)\cdot \ldots \cdot (x - \zeta_n^{p^{n+1}-1}).$$

Form the polynomial

$$\Phi_{p^{n+1}}(x) := \prod_{\substack{(a,p)=1 \\ 1 \le a < p^{n+1}}} (x - \zeta_n^a) = \frac{x^{p^{n+1}} - 1}{(x-\zeta_n^{1\cdot p})(x - \zeta_n^{2\cdot p}) \cdot \ldots \cdot (x - \zeta_n^{(p^n-1)\cdot p})(x-1)} =$$

$$= \frac{x^{p^{n+1}} - 1}{(x - \zeta_{n-1})(x - \zeta_{n-1}^2) \cdot \ldots \cdot (x - \zeta_{n-1}^{(p^n-1)})(x-1)} = \frac{x^{p^{n+1}} - 1}{x^{p^n} - 1}, \text{ (put } \zeta_{-1} = 1).$$

This is the so-called p^{n+1}-th cyclotomic polynomial. It is irreducible in $\mathbb{Z}[x]$ ([I-R], p. 195). Consequently $\Phi_{p^{n+1}}(x)$ is minimal polynomial for ζ_n over $\mathbb{Z}$. Consider the ring homomorphism

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[\zeta_n]$$

such that

$$x \mapsto \zeta_n.$$

By above, Ker $\phi = (\Phi_{p^{n+1}}(x))$. Hence

$$\mathbb{Z}[\zeta_n] \cong \mathbb{Z}[x]/(\Phi_{p^{n+1}}(x)) = \mathbb{Z}[x] \Big/ \left(\frac{x^{p^{n+1}} - 1}{x^{p^n} - 1} \right).$$

We would like to prove that $\tilde{K}_0 A \cong \text{Pic }(A)$ for $A = \mathbb{Z}C_{p^n}$.

Any projective A-module M defines a function $\text{rank}_M : \text{Spec } A \to \mathbb{Z}$ which can be defined as follows: Let v be a prime ideal of A and $R(A/v)$ the fraction field of A/v. $M^v := (M \otimes_A (A/v)) \otimes_{A/v} R(A/v)$ is a finite dimensional vector space over $R(A/v)$. We set $\text{rank}_M(v) = \dim_{R(A/v)} M^v$. A subset V of Spec A is called closed if there exists an ideal $\mathfrak{a} \subseteq A$ such that V consists of those prime ideals $\mathfrak{p}$ such that $\mathfrak{a} \subset \mathfrak{p}$. This defines a topology on Spec A called the Zarisky topology . It is well known that rank_M is a continuous function with respect to the discrete topology on $\mathbb{Z}$ and the Zarisky topology on Spec A (see [B]).

Corollary 1.1. *If Spec A is connected, then rank_M is constant.*

We shall also use the fact that Spec A is connected if A has no non-trivial, orthogonal idempotents (that is, non-trivial $e_1 \neq 0, e_2 \neq 0, e_1^2 = e_1, e_2^2 = e_2, e_1 + e_2 = 1, e_1 e_2 = 0$).

Theorem 1.4. *$\mathbb{Z}C_{p^n}$ has no non-trivial idempotents.*

Proof: Induction over n.

Consider the diagram $(**)$ in 1.1 with $A := \mathbb{Z}[x], \alpha := \left(\frac{x^{p^n}-1}{x^{p^{n-1}}-1}\right)$, $\beta := (x^{p^{n-1}}-1)$. First, the case $n=1$: Here $\alpha = (\frac{x^p-1}{x-1})$, $\beta = (x-1)$. It is easily checked that $\alpha \cap \beta = (x^p-1)$, $\alpha+\beta = (p,\ x-1)$.

Therefore, we have the following Cartesian square:

$$\begin{tikzcd}
\mathbb{Z}[x]/(x^p-1) \cong \mathbb{Z}C_p \arrow[r, "i_1"] \arrow[d, "i_2"] & \mathbb{Z}[\zeta_0] \cong \mathbb{Z}[x]/(\frac{x^p-1}{x-1}) \arrow[d] \\
\mathbb{Z}[x]/(x-1) \cong \mathbb{Z} \arrow[r] & \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[x]/(p, x-1)
\end{tikzcd}$$

Here $i_1(x) = x \in \mathbb{Z}[x]/(\frac{x^p-1}{x-1})$, $i_2(x) = x \in \mathbb{Z}[x]/(x-1)$.

Now $\mathbb{Z}$ and $\mathbb{Z}[\zeta_0]$ are integral domains and every element in $\mathbb{Z}C_p$ can be represented as a pair (a,b), where $a \in \mathbb{Z}[\zeta_0]$ and $b \in \mathbb{Z}$. We get: $(a,b)^2 = (a,b) \Rightarrow (a^2,b^2) = (a,b) \Rightarrow a^2 = a, b^2 = b \Rightarrow a = 0$ or $a = 1$ and $b = 0$ or $b = 1$. Using that a and b have the same image in $\mathbb{Z}/p\mathbb{Z}$ we get that $(a,b) = (0,0)$ or $(1,1)$. Thus all idempotents are trivial.

For general n, we have $\alpha \cap \beta = (x^{p^n}-1)$. Further $\frac{x^{p^n}-1}{x^{p^{n-1}}-1} = 1 + x^{p^{n-1}} + \ldots + x^{(p-1)\cdot p^{n-1}} = p + t_1 \cdot (x^{p^{n-1}}-1)$ for some polynomial $t_1 \in \mathbb{Z}[x]$. Thus $\alpha + \beta = (p, x^{p^{n-1}}-1)$. Analogous to the case $n=1$, we have the Cartesian square

$$\begin{tikzcd}
\mathbb{Z}C_{p^n} \arrow[r] \arrow[d] & \mathbb{Z}[\zeta_{n-1}] \arrow[d] \\
\mathbb{Z}C_{p^{n-1}} \arrow[r] & (\mathbb{Z}C_{p^{n-1}})/(p)
\end{tikzcd}$$

Also here, every element of $\mathbb{Z}C_{p^n}$ can be represented as a pair (a,b) with $a \in \mathbb{Z}[\zeta_{n-1}]$, $b \in \mathbb{Z}C_{p^{n-1}}$.

Clearly $\mathbb{Z}[\zeta_{n-1}]$ has no non-trival idempotents and $\mathbb{Z}C_{p^{n-1}}$ has no non-trivial idempotents by the induction assumption. Using exactly the same considerations as in the case $n=1$, we obtain the desired result. □

Consequently, Spec $\mathbb{Z}C_{p^n}$ is connected and rank_M is constant on this space for any $\mathbb{Z}C_{p^n}$-module M. Since the Krull dimension of $\mathbb{Z}C_{p^n}$ is 1, it follows

$$\tilde{K}_0\mathbb{Z}C_{p^n} \cong \text{Pic }(\mathbb{Z}C_{p^n})$$

([B], Ch. 4, Cor. 2.7 and Ch. 9, Prop. 3.7). The relationship between K_0- and Pic- groups can be considered as follows. Let

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d] & A_2 \arrow[d] \\
A_3 \arrow[r] & A_4
\end{tikzcd}$$

be a Cartesian square of rings. By [B], pp. 466-467, we have determinant surjections:

$$\begin{aligned}&\det_0 : K_0A_i \to \text{Pic } (A_i) \quad \text{and}\\ &\det_1 : K_1A_i \to U(A_i) := \{\text{units in } A_i\},\end{aligned}$$

for $i = 1, 2, 3, 4$. For $\det_1$ and $U(A)$, see [M], §3. The discussion above and Ch.9, Prop. 3.6 in [B] yield two exact Mayer-Vietoris sequences, the (K_1, K_0)-sequence and the (U, Pic)-sequence.

$$\begin{tikzcd}
K_1A_1 \arrow[r] \arrow[d, "\det_1"] & K_1A_2 \arrow[r, phantom, "\oplus"] \arrow[d, "\det_1"] & K_1A_3 \arrow[r] \arrow[d, "\det_1"] & K_1A_4 \arrow[r] \arrow[d, "\det_1"] & K_0A_1 \arrow[r] \arrow[d, "\det_0"] & K_0A_2 \arrow[r, phantom, "\oplus"] \arrow[d, "\det_0"] & K_0A_3 \arrow[r] \arrow[d, "\det_0"] & K_0A_4 \arrow[d, "\det_0"] \\
U(A_1) \arrow[r] & U(A_2) \arrow[r, phantom, "\oplus"] & U(A_3) \arrow[r] & U(A_4) \arrow[r] & \mathrm{Pic}(A_1) \arrow[r] & \mathrm{Pic}(A_2) \arrow[r, phantom, "\oplus"] & \mathrm{Pic}(A_3) \arrow[r] & \mathrm{Pic}(A_4)
\end{tikzcd}$$

In our particular case it follows that $\det_0 : K_0\mathbb{Z}C_{p^n} \to \text{Pic}(\mathbb{Z}C_{p^n})$ is an epimorphism with kernel $\mathbb{Z}$.

1.7 Rim's Theorem

In [M], p. 29, a variant of Rim's theorem is

$$K_0\mathbb{Z}C_p \cong K_0\mathbb{Z}[\zeta_0].$$

If we decompose both sides, in accordance with previous paragraphs, and drop the $\mathbb{Z}$-components, the formula reads

$$\text{Pic } (\mathbb{Z}C_p) \cong Cl(\mathbb{Z}[\zeta_0]),$$

or

$$\text{Pic } (\mathbb{Z}[x]/(x^p - 1)) \cong \text{Pic } (\mathbb{Z}[x]/(\frac{x^p - 1}{x - 1})).$$

Here we shall prove the generalization of this.

Theorem 1.5.

$$\textit{Pic } (\mathbb{Z}C_{p^n}) \cong \textit{Pic } (\mathbb{Z}[x]/(\frac{x^{p^n} - 1}{x - 1})).$$

Proof: Start with the square

$$\begin{tikzcd}
\mathbb{Z}C_{p^n} \cong \mathbb{Z}[x]/(x^{p^n} - 1) \arrow[r, "\bar{x} \mapsto \bar{x}"] \arrow[d, "\bar{x} \mapsto 1"'] & \mathbb{Z}[x]/(\frac{x^{p^n}-1}{x-1}) \arrow[d, "\bar{x} \mapsto 1 \pmod{p^n}"] \\
\mathbb{Z} \cong \mathbb{Z}[x]/(x - 1) \arrow[r, "1 \mapsto 1 \ (\mathrm{mod}\ p^n)"] & \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}[x]/(x - 1, \frac{x^{p^n}-1}{x-1})
\end{tikzcd}$$

$\bar{x}$ denotes the coset of x. If we set $\lambda := (\frac{x^{p^n}-1}{x-1})$, $\mu := (x-1)$, one gets easily for these ideals

$$\lambda \cap \mu = \lambda\mu = (x^{p^n} - 1)$$

and

$$\lambda + \mu = (x-1) + (x^{p^n-1} + \ldots + x + 1) = (x-1, p^n).$$

Furthermore,

$$\mathbb{Z}[x]/(\lambda + \mu) \cong \mathbb{Z}[x]/(x-1, p^n) \cong \mathbb{Z}/(p^n),$$

as in the figure, where the maps also are indicated. Thus, there is a Cartesian square of type $(**)$ in 1.1.

This fact and the already discussed theory yield a (U, Pic)-sequence

$$\begin{aligned}
&U(\mathbb{Z}C_{p^n}) \to U(\mathbb{Z}) \oplus U\Big(\mathbb{Z}[x]\Big/\Big(\frac{x^{p^n}-1}{x-1}\Big)\Big) \xrightarrow{\alpha} \\
&\xrightarrow{\alpha} U(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\beta} \text{Pic } (\mathbb{Z}C_{p^n}) \xrightarrow{\gamma} \\
&\xrightarrow{\gamma} \text{Pic } (\mathbb{Z}) \oplus \text{Pic } \Big(\mathbb{Z}[x]\Big/\Big(\frac{x^{p^n}-1}{x-1}\Big)\Big) \to \\
&\to \text{Pic } (\mathbb{Z}/p^n\mathbb{Z}).
\end{aligned}$$

Here $U(\mathbb{Z}) = \{-1, 1\}$. The ring $\mathbb{Z}$ is a principal ideal domain, hence a Dedekind domain ([A-M], p. 96). Therefore, Pic $(\mathbb{Z}) \cong Cl(\mathbb{Z}) \cong (0)$.

Now, $\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, 2, \ldots, p^n - 1\}$ is a local ring with maximal ideal generated by p.

We have earlier seen that Pic-groups for local rings are 0, hence Pic $(\mathbb{Z}/p^n\mathbb{Z}) = 0$.

Take $k \in U(\mathbb{Z}/p^n\mathbb{Z})$. Then $(k, p) = 1$. There exists $r, s \in \mathbb{Z}, r > 0 : \; k \cdot s + p^n \cdot (-r) = 1$, that is, $k | (1 + p^n \cdot r)$.

Consider $\frac{(\bar{x})^k - \bar{1}}{\bar{x} - \bar{1}} \in \mathbb{Z}[x]/(\frac{x^{p^n}-1}{x-1})$. Evidently,

$$\frac{(\bar{x})^k - \bar{1}}{\bar{x} - \bar{1}} \cdot \frac{(\bar{x})^{1+p^n \cdot r} - \bar{1}}{(\bar{x})^k - \bar{1}} \equiv \bar{1},$$

because $(\bar{x})^{p^n} = x^{p^n} + (\frac{x^{p^n}-1}{x-1}) = 1 + (\frac{x^{p^n}-1}{x-1}) = \bar{1}$ and both fractions belong to $\mathbb{Z}[x]/(\frac{x^{p^n}-1}{x-1})$. This implies

$$\frac{(\bar{x})^k - \bar{1}}{\bar{x} - \bar{1}} \in U\Big(\mathbb{Z}[x]\Big/\Big(\frac{x^{p^n}-1}{x-1}\Big)\Big).$$

The homomorphism α, in the (U, Pic)-sequence above, gives $\alpha(\frac{(\bar{x})^k - \bar{1}}{\bar{x} - \bar{1}}) = \alpha((\bar{x})^{k-1} + \ldots + \bar{x} + \bar{1}) = k$ since $\alpha(\bar{x}) = 1$. It follows that α is surjective.

Since the sequence is exact, Im $\alpha = U(\mathbb{Z}/p^n\mathbb{Z}) =$ Ker β. Hence Im $\beta = 0 =$ Ker γ and γ is injective. Thus, Im $\gamma \cong$ Pic $(\mathbb{Z}C_{p^n})$. But γ is surjective (Pic $(\mathbb{Z}/p^n\mathbb{Z}) = 0 =$ Pic $(\mathbb{Z})$), from which Im $\gamma =$ Pic $(\mathbb{Z}[x]/(\frac{x^{p^n}-1}{x-1}))$. □

§2 Some General Results on $\mathbb{Z}C_{p^n}$

Let us look at some papers which deal with the problem of calculating Picard groups of $\mathbb{Z}C_{p^n}$. Most of these essays are written about 15-25 years ago.

2.1 Results of Kervaire and Murthy

The article [K-M] gives a very clear introduction to the subject. It circulated as a preprint in the late 1960s, but was published in 1977.

A prime p is said to be regular if p does not divide the class number of $\mathbb{Q}(\zeta_0)$, where ζ_0 is a p-th root of unity. By [B-S], cor. p. 377, this is equivalent to $\delta_p = 0$, where $\delta_p :=$ number of Bernoulli numbers among $B_2, B_4, \ldots, B_{p-3}$ whose numerators (in reduced form) are divisible by p. Recall that Bernoulli numbers $B_m (m \geq 1)$ are defined by

$$\frac{t}{e^t - 1} = 1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} \cdot t^m.$$

A prime p is said to be semi-regular if it does not divide the order of the ideal class group of $\mathbb{Q}(\zeta_0 + \zeta_0^{-1})$ (the maximal real subfield of $\mathbb{Q}(\zeta_0)$). It is conjectured that every prime is semi-regular. However, $\delta_p \neq 0$ for infinitely many primes p ([B-S], pp. 381-382; [I-R], p. 241).

The authors of [K-M] essentially start with the Cartesian square

$$\begin{tikzcd}
\mathbb{Z}[X]/(X^{p^{n+1}} - 1) \arrow[r, "i_2"] \arrow[d, "i_1"'] & \mathbb{Z}[\zeta_n] \arrow[d, "j_2"] \\
\mathbb{Z}[X]/(X^{p^n} - 1) \arrow[r, "j_1"] & \mathbb{F}_p[x]/(x^{p^n} - 1)
\end{tikzcd}$$

where $i_2(X) = \zeta_n$, $j_2(\zeta_n) = x$ and $j_1(X) = x$. Note that $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}[\zeta_n] \cong \mathbb{Z}[X]/(\frac{X^{p^{n+1}}-1}{X^{p^n}-1})$, (see 1.6).

Set $R_n := \mathbb{F}_p[x]/(x^{p^n} - 1)$ and write $t = x - 1$. Then $x^{p^n} - 1 \equiv t^{p^n} \pmod{p}$, that is, $R_n \cong \mathbb{F}_p[t]/(t^{p^n})$.

Every element in $R_n \backslash (t)$ is of the form $a_0 + a_1 t + \ldots + a_{p^n-1} t^{p^n-1} + (t^{p^n})$; $a_0 \neq 0$. These elements are units in R_n because $a_0 + (t^{p^n})$ is a unit in R_n, and the t-terms form nilpotent cosets in R_n. Hence R_n is a local ring with maximal ideal (t). Thus, by Lemma 1.1, $K_0 R_n \cong \mathbb{Z}$ which implies that $\tilde{K}_0(R_n) = (0)$.

R_n local implies $K_1(R_n) \cong U(R_n)$, (see 1.5). Since det : $K_1 A \to U(A)$ is (split) surjective for a commutative ring A with identity, the (U, Pic) version of the Mayer-Vietoris sequence gives us the exact sequence

$$U(\mathbb{Z}C_{p^n}) \oplus E_n \to U(R_n) \to \tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^n}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_n]) \to 0,$$

where $E_n := U(\mathbb{Z}[\zeta_n])$; (1.6).

Denote by j and i the following maps

$$j : U(\mathbb{Z}C_{p^n}) \oplus E_n \to U(R_n)$$
$$i : U(R_n) \to \tilde{K}_0(\mathbb{Z}C_{p^{n+1}})$$

and let V_n be the cokernel $U(R_n)/\mathrm{Im}\ j$ of the map j. We can define a map

$$\bar{i} : V_n \to \tilde{K}_0(\mathbb{Z}C_{p^{n+1}})$$

by sending the class of $\epsilon \in U(R_n)$ to $i(\epsilon)$. It is easy to see that $\bar{i}$ is injective and that the sequence

$$0 \to V_n \to \tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^n}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_n]) \to 0 \qquad (1)$$

is exact.

Now, let $G_n := \mathrm{Gal}\ (\mathbb{Q}(\zeta_n)/\mathbb{Q})$ be the Galois group. It is well known that $G_n \cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^n}$. If $s \in G_n$, then $s(\zeta_n) = \zeta_n^\kappa$ for some $\kappa = \kappa(s) \in U(\mathbb{Z}/p^{n+1}\mathbb{Z})$. This defines an isomorphism

$$\kappa : G_n \to U(\mathbb{Z}/p^{n+1}\mathbb{Z}).$$

Hence $x^{\kappa(s)}$ is well defined when x is the generator corresponding to X in $\mathbb{Z}[X]/(X^{p^{n+1}} - 1) = \mathbb{Z}C_{p^{n+1}}, \mathbb{Z}[X]/(X^{p^n} - 1) = \mathbb{Z}C_{p^n}$ or $\mathbb{F}_p[X]/(X^{p^n} - 1) = R_n$.

The formula $s(x) = x^{\kappa(s)}$ turns G_n into a group of automorphisms of the rings $\mathbb{Z}C_{p^{n+1}}$, $\mathbb{Z}C_{p^n}$ and R_n. All the maps in the diagram at the beginning of 2.1 commute with the action of G_n.

If we view $C_{p^{n+1}}$ as the group $\{1, \zeta_n, \dots, \zeta_n^{p^{n+1}-1}\}$ we hence get that Aut $(C_{p^{n+1}}) \cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^n}$, where the action is, again, given by $\zeta_n \xrightarrow{s} \zeta_n^{\kappa(s)}$, $s \in \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^n}$. Note that $(p, \kappa(s)) = 1$.

This action of G_n on the rings above induces an action on the groups in (1) that hence turns into an exact sequence of G_n-modules.

If we let $c \in G_n$ be complex conjugation, then, since $c(\zeta_n) = \bar{\zeta}_n = \zeta_n^{-1}$, we get that the action of c on $\mathbb{Z}C_{p^{n+1}}, \mathbb{Z}C_{p^n}$ and R_n, is given by $c(x) = x^{-1}$.

If M is a multiplicative G_n-module, define $M^+ := \{v \in M | c(v) = v\}$, $M^- := \{v \in M | c(v) = v^{-1}\}$. Obviously, if M is a finite abelian group of odd order, then $M = M^+ \oplus M^-$. We also define Char (M) as Hom (M, μ), where μ is the group of roots of unity in $\bigcup_{n \geq 0} \mathbb{Q}(\zeta_n)$.

A principal part of [K-M] is devoted to a proof and discussions of the following theorem:

Theorem 2.1. *Let $U_n = U(R_n)$, and let $X_n \subset U_n$ be the cyclic subgroup generated by $x = 1 + t$, where $R_n = \mathbb{F}_p[t]/(t^{p^n})$, $n \geq 1$. Then $V_n = V_n^+ \oplus V_n^-$, and there is a surjective map of V_n onto $U_n/(X_n \cdot U_n^+)$.*

If p is semi-regular, we have

$$V_n^- \cong U_n/(X_n \cdot U_n^+) \quad \textit{and} \quad \textit{Char}\ (V_n^+) \subset S^{-1}(\mathbb{Q}(\zeta_{n-1})) = S(\mathbb{Q}(\zeta_{n-1})),$$

by a canonical injection, where $S(\mathbb{Q}(\zeta_\nu))$ is the p-primary component of the ideal class group of $\mathbb{Q}(\zeta_\nu)$.

Remark to Theorem 2.1: It is asserted that $V_n^- \cong U_n/(X_n \cdot U_n^+)$ if p is semi-regular. However, the latter condition is not necessary. This will be clear from the proof later on. The isomorphism is thus valid for all odd primes.

Define W_n to be the kernel of the map

$$i_* : \tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \oplus_{\nu=0}^n \tilde{K}_0(\mathbb{Z}[\zeta_\nu]),$$

which is induced by the inclusion

$$i : \mathbb{Z}C_{p^{n+1}} \to \mathbb{Z} \oplus (\oplus_{\nu=0}^n \mathbb{Z}[\zeta_\nu])$$

of $\mathbb{Z}C_{p^{n+1}}$ into the maximal order of

$$\mathbb{Q}C_{p^{n+1}} \cong \mathbb{Q} \oplus (\oplus_{\nu=0}^n \mathbb{Q}(\zeta_\nu))$$

([B-S], [C-R]).

Using Theorem 2.1 we can now prove the following theorem.

Theorem 2.2. *Let p be a regular prime. Then there is an exact sequence*

$$0 \to W_n \to \tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \xrightarrow{i_*} \oplus_{\nu=0}^n \tilde{K}_0(\mathbb{Z}[\zeta_\nu]) \to 0,$$

where W_n is an abelian p-group with a filtration

$$W_n = H_1 \supset H_2 \supset \ldots \supset H_n \supset H_{n+1} = 0,$$

such that $H_m/H_{m+1} \cong V_m$ as given by the above formulas.

Sketch of proof. Define

$$p_m : \tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^m}),$$

to be the homomorphisms induced by the obvious projections for $m = 1, \ldots, n+1$ and put $H_m := W_n \cap \text{Ker } (p_m)$.

The exact sequence (1) shows that all maps in the sequence

$$\begin{aligned} &\tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^n}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_n]) \to \\ &\to \ldots \to \tilde{K}_0(\mathbb{Z}C_{p^m}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_m]) \oplus \\ &\oplus \tilde{K}_0(\mathbb{Z}[\zeta_{m+1}]) \oplus \ldots \oplus \tilde{K}_0(\mathbb{Z}[\zeta_n]) \end{aligned} \tag{2}$$

are surjective.

The surjectivity of i_* follows from Rim's theorem and the case $m = 1$. This also gives $W_n \subset \text{Ker } (p_1)$, i.e., $H_1 = W_n$. From

$$\tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^{m+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^m}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_m])$$

we see that

$$H_{m+1} = W_n \cap \text{Ker } (p_{m+1}) \subset W_n \cap \text{Ker } (p_m) = H_m.$$

Now consider

$$\phi := p_{m+1}|H_m : H_m \to \tilde{K}_0(\mathbb{Z}C_{p^{m+1}})$$

and

$$\alpha : \tilde{K}_0(\mathbb{Z}C_{p^{m+1}}) \to \tilde{K}_0(\mathbb{Z}C_{p^m}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_m]).$$

Since $H_m = W_n \cap \text{Ker } (p_m)$, it is clear that ϕ maps into $V_m = \text{Ker } \alpha$.

Take $v_m \in V_m$. Then $\alpha(v_m) = (0,0)$. In the sequence of surjective maps (2)

$$v'_m := (v_m, \overbrace{0, \ldots, 0}^{n-m}) \in \tilde{K}_0(\mathbb{Z}C_{p^{m+1}}) \oplus \tilde{K}_0(\mathbb{Z}[\zeta_{m+1}]) \oplus \ldots \oplus \tilde{K}_0(\mathbb{Z}[\zeta_n])$$

(only the first term remains if $m = n$). There is an element $y \in \tilde{K}_0(\mathbb{Z}C_{p^{n+1}})$ mapping on v'_m. Of course, $y \in W_n$. Further, $p_{m+1}(y) = v_m$, so $y \in \text{Ker } (\alpha \circ p_{m+1}) \subset \text{Ker } (p_m)$, i.e., $y \in H_m$. $\phi = p_{m+1}|H_m : H_m \to V_m$ is surjective.

Finally,

$$\begin{aligned} \text{Ker } \phi &= \{x \in H_m | \phi(x) = 0\} = \\ &= H_m \cap \text{Ker } (p_{m+1}) = \\ &= W_n \cap \text{Ker } (p_m) \cap \text{Ker } (p_{m+1}) = \\ &= W_n \cap \text{Ker } (p_{m+1}) = H_{m+1}. \end{aligned}$$

It follows:

$$V_m \cong H_m / H_{m+1}.$$

Let $|M| = \#M$ denote the number of elements in a finite set M. We want to determine $|W_n|$. For this purpose one first needs to calculate $|V_n|$. Since p is assumed to be regular in Theorem 2.2, it follows from Theorem 2.1 that

$$V_n = V_n^- \cong U_n / (X_n \cdot U_n^+).$$

So

$$|V_n| = |U_n| / (|X_n| \cdot |U_n^+|).$$

Now

$$\begin{aligned} &|U_n| = |U(R_n)| = \\ &= \#\{a_0 + a_1 x + a_2 x^2 + \ldots + a_{p^n-1} x^{p^n-1} | a_i \in \mathbb{F}_p, a_0 \neq 0, x^{p^n} = 1\} = \\ &= (p-1) \cdot p^{p^n-1}. \end{aligned}$$

By definition

$$\begin{aligned}|U_n^+| = \#\{&a_0 + a_1 x + \ldots + a_{p^n-1}x^{p^n-1} \equiv \\ &\equiv a_0 + a_1 x^{-1} + \ldots + a_{p^n-1}x^{-(p^n-1)} | a_i \in \mathbb{F}_p, a_0 \neq 0, x^{p^n} = 1\}.\end{aligned}$$

Here, we have $x^{-i} = x^{p^n-i}$, so $a_i = a_{p^n-i}$, $i = 1, 2, \ldots, p^n - 1$. Therefore $|U_n^+| = (p-1) \cdot p^{\frac{1}{2}(p^n-1)}$. Finally

$$|X_n| = \#\{1, x, x^2, \ldots, x^{p^n-1}\} = p^n.$$

Hence $|V_n| = p^{v_n}$ with $v_n = \frac{1}{2}(p^n - 1) - n$.

It now follows that

$$\begin{aligned}&|W_n| = |H_1| = |H_2| \cdot |H_1/H_2| = |H_3| \cdot |H_2/H_3| \cdot |H_1/H_2| = \ldots = \\ &= |H_{n+1}| \cdot |H_n/H_{n+1}| \cdot |H_{n-1}/H_n| \cdot \ldots \cdot |H_1/H_2| = 1 \cdot |V_n| \cdot |V_{n-1}| \cdot \ldots \cdot |V_1| = \\ &= p^{w_n},\end{aligned}$$

where

$$\begin{aligned}w_n &= \frac{1}{2}(p^n - 1) - n + \frac{1}{2}(p^{n-1} - 1) - (n-1) + \ldots + \\ &\quad + \frac{1}{2}(p^2 - 1) - 2 + \frac{1}{2}(p - 1) - 1 = \\ &= \frac{1}{2}\frac{p^n - 1}{p - 1} \cdot p - \frac{n}{2} - \frac{n(n+1)}{2} = \\ &= \frac{1}{2}\Big(\frac{p^{n+1} - p}{p - 1} - (n+1)^2 + 1\Big) = \\ &= \frac{1}{2}\Big(\frac{p^{n+1} - 1}{p - 1} - (n+1)^2\Big).\end{aligned}$$

□

Next, observe that $U(R_n)$ splits as a direct product

$$U(R_n) = \mathbb{F}_p^* \oplus U_n^{(1)},$$

where $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$, and $U_n^{(1)}$ is the subgroup of $U(R_n)$ consisting of units congruent to 1 mod tR_n. Let us set $T := tR_n := (t)$, the maximal ideal of R_n.

The subgroups $U_n^{(i)} := 1 + T^i$, $i \geq 1$, define a filtration on $U(R_n)$. Define maps $T^i \to 1 + T^i$ by $f \mapsto 1 + f$. Then the homomorphism

$$\begin{aligned}&\psi : T^i \to U_n^{(i)}/U_n^{(i+1)}, \\ &\psi(f) = (1 + f)U_n^{(i+1)}\end{aligned}$$

is surjective and Ker $\psi = \{f \in T^i | (1 + f)U_n^{(i+1)} = U_n^{(i+1)}\} = T^{i+1}$, so $T^i/T^{i+1} \cong U_n^{(i)}/U_n^{(i+1)}$ for $i \geq 1$.

We now make a slight change of notation and put $U_n := U_n^{(1)}$. Since $t^i + T^{i+1}$ generates T^i/T^{i+1}, it follows: Any set of elements $\xi_i \in U(R_n)$, $i = 1, \dots , p^n - 1$, satisfying

$$\xi_i \equiv 1 + t^i \bmod T^{i+1},$$

is a set of generators of U_n.

The rest of the notations are preserved analogously: For $c : R_n \to R_n$, with a generator x, we have $c(x) = x^{-1}$. If $c(u) = u$ for $u \in U(R_n)$, u is called a symmetric unit. U_n^+ is the subgroup of U_n consisting of symmetric units. X_n means the subgroup of U_n generated by $x = 1 + t$. Note:

$$U_n/(X_n \cdot U_n^+) \cong U(R_n)/(\mathbb{F}_p^* \oplus (X_n \cdot U_n^+)).$$

Set $\alpha_i := 1+t^i$ for $i = 1, \dots , p^n-1$, and let γ_i be the class of α_i in $U_n/(X_n \cdot U_n^+)$. The structure of this group is now given by

Lemma 2.1. *If p is a prime ≥ 3, the elements γ_{2i+1}, with $1 \leq i \leq \frac{1}{2}(p^n - 3)$ and $2i + 1$ prime to p, form an independent set of generators of $U_n/(X_n \cdot U_n^+)$. The order of γ_{2i+1} is p^{a_i}, where a_i is uniquely determined by the inequalities*

$$p^{n-a_i} \leq 2i + 1 < p^{n-a_i+1}.$$

Regard $p = 3, n = 1$ as a trivial special case.

Outline of proof. Consider $s := x + x^{-1} - 2 = x^{-1}t^2 \in U_n^+$ and $\sigma_i := 1 + s^i \in U_n^+$, $i = 1, \dots , \frac{1}{2}(p^n - 1)$. Now $\alpha_{2i+1} = 1 + t^{2i+1}$ and $\sigma_i \equiv 1 + t^{2i} \bmod T^{2i+1}$, whence by a remark above, the set $\{\alpha_{2i+1}, \sigma_{i+1} | i = 0, 1, \dots , \frac{1}{2}(p^n - 3)\}$ generates U_n. But $\alpha_1 = 1 + t \in X_n$ and $\sigma_{i+1} \in U_n^+$ so $\{\gamma_{2i+1} | i = 1, \dots , \frac{1}{2}(p^n - 3)\}$ generates $U_n/(X_n \cdot U_n^+)$. Further, $\alpha_{(2i+1)\cdot p} = (\alpha_{2i+1})^p$. Hence $\{\gamma_{2i+1} | i = 1, \dots , \frac{1}{2}(p^n - 3)$ and $2i + 1$ prime to $p\}$ suffices to generate $U_n/(X_n \cdot U_n^+)$.

We have $(\alpha_{2i+1})^{p^{a_i}} = 1 + t^{(2i+1)\cdot p^{a_i}} = 1$, where $p^{n-a_i} \leq 2i + 1 < p^{n-a_i+1}$, so α_{2i+1} has order p^{a_i} in U_n. Therefore the order of γ_{2i+1} divides p^{a_i}.

If $|U_n/(X_n \cdot U_n^+)| = \prod_i p^{a_i}$, where the product is taken over $i = 1, \dots , \frac{1}{2}(p^n - 3)$ with $2i + 1$ prime to p, then it follows: The order of γ_{2i+1} is precisely p^{a_i} and $\gamma_3, \gamma_5, \dots , \gamma_{p^n-2}$, with indices prime to p, form an independent set of generators of $U_n/(X_n \cdot U_n^+)$.

Earlier we saw that $|U_n/(X_n \cdot U_n^+)| = p^{\frac{1}{2}(p^n-1)-n}$.

But for given a, the set $\{i | p^{n-a} \leq 2i + 1 < p^{n-a+1}\} = \{i | a_i = a\}$ has $\frac{1}{2}(p - 1) \cdot p^{n-a}$ integers for $a < n$ and $\frac{1}{2}(p - 3)$ for $a = n(2i + 1 \geq 3)$. Among these, there are $\frac{1}{2}(p - 1) \cdot p^{n-a-1}$ multiples of p, except if $a = n$, in which case there are none.

All this gives $\prod_i p^{a_i} = p^{r_n}$ with

$$r_n = \sum_{a=1}^{n-1} a \cdot \frac{1}{2}(p - 1)^2 p^{n-a-1} + n \cdot \frac{1}{2}(p - 3).$$

It is easily verified that $r_n = v_n = \frac{1}{2}(p^n - 1) - n$. □

Corollary 2.1.

$$U_n/(X_n \cdot U_n^+) \cong \oplus_{\nu=1}^{n-1}\frac{1}{2}(p-1)^2 p^{n-\nu-1} \cdot \mathbb{Z}/p^\nu\mathbb{Z} \oplus$$
$$\oplus\, \frac{1}{2}(p-3) \cdot \mathbb{Z}/p^n\mathbb{Z},\ p \geq 3.$$

Here $N \cdot \mathbb{Z}/p^k\mathbb{Z}$ is the direct sum of N copies of the group $\mathbb{Z}/p^k\mathbb{Z}$.

Recall that $E_n = U(\mathbb{Z}[\zeta_n])$, $R_n = \mathbb{F}_p[t]/(t^{p^n})$. If x is a generator of C_{p^n}, then $j(x) = j(\zeta_n) = 1 + t; C_{p^n} = \{1, x, \dots , x^{p^n-1}\}$ and $j : U(\mathbb{Z}C_{p_n} \oplus E_n) \to U(R_n)$.

Now it is proved that Im$j \subset \mathbb{F}_p^* \oplus (X_n \cdot U_n^+)$, with the new notations of this section. We need

Lemma 2.2 (Kummer's Lemma). *Let $u \in E_n$. Then for some integer i, the unit $\zeta_n^i u$ is real, i.e., $c(\zeta_n^i u) = \zeta_n^i u$, where c is complex conjugation.*

This lemma extends to our group rings: Let $c : \mathbb{Z}C_{p^n} \to \mathbb{Z}C_{p^n}$ be the automorphism induced by $c(x) = x^{-1}$, where x is a generator of C_{p^n}.

Lemma 2.3. *Let $u \in U(\mathbb{Z}C_{p^n})$. Then, for some integer i, one has $c(x^i u) = x^i u$.*

The proofs of the last two lemmas are sketched in [K-M], with references to [He], 3.4 and [Hig] (Higman's theorem).

Lemma 2.4. *With our new notations, we have*

$$Im\ j \subset \mathbb{F}_p^* \oplus (X_n \cdot U_n^+);\ p \geq 3.$$

Proof: The conjugation c operates on $U(\mathbb{Z}C_{p^n})$, E_n and $U(R_n)$. The map

$$j : U(\mathbb{Z}C_{p^n}) \oplus E_n \to U(R_n)$$

is a map of C-modules where C is the cyclic group of order 2, generated by c. Lemma 2.4 now follows from Kummer's lemma and its extension to $\mathbb{Z}C_{p^n}$. □

No regularity assumptions on the prime p are done here. Thus the

Corollary 2.2. *For $p \geq 3$ and $n \geq 0$, there is a surjection*

$$V_n = U(R_n)/Im\ j \to U_n/(X_n \cdot U_n^+).$$

This is one of the statements in Theorem 2.1. It follows rather quickly from Lemma 2.4. Here again observe that

$$U_n/(X_n \cdot U_n^+) \cong U(R_n)/(\mathbb{F}_p^* \oplus (X_n \cdot U_n^+)).$$

Recall $V_n = U(R_n)/\text{Im } j$, where $j : U(\mathbb{Z}C_{p^n}) \oplus E_n \to U(R_n)$. Put $j_0 : E_n \to U(R_n)$ and $\mathcal{V}_n := U(R_n)/\text{Im } j_0$. We get Im $j_0 \subset$ Im j, whence

$$V_n = (U(R_n)/\text{Im } j_0)/(\text{Im } j/\text{Im } j_0) = \mathcal{V}_n/(\text{Im } j/\text{Im } j_0).$$

Thus $\mathcal{V}_n$ maps surjectively on V_n and the same holds for $\mathcal{V}_n^+, \mathcal{V}_n^-$ onto V_n^+, V_n^-, respectively.

If $v \in \mathcal{V}_n^-$ maps to $1 \in V_n^-$, v can be lifted to $u \in U(R_n)$ so that $c(u) = u^{-1}$ and $u \in j\{U(\mathbb{Z}C_{p^n}) \oplus E_n\} \subset \mathbb{F}_p^* \oplus (X_n \cdot U_n^+)$. Then $u \in X_n = \{1, x, \dots, x^{p^n-1}\}$. Since $j(\zeta_n) = x$, we have $u \in j(E_n) = j_0(E_n)$, hence $v = 1$ (trivial kernel), so $V_n^- \cong \mathcal{V}_n^-$.

Further in Theorem 2.1, one has Char $(V_n^+) :=$ Hom (V_n^+, μ), i.e., the group of homomorphisms from V_n^+ to μ. Here μ, the group of roots of unity in $\cup_{n \geq 0} \mathbb{Q}(\zeta_n)$, is equipped with the discrete topology.

We also have $S(\mathbb{Q}(\zeta_\nu))$, the p-primary component of the ideal class group $Cl(\mathbb{Z}[\zeta_\nu])$ of $\mathbb{Z}[\zeta_\nu]$, $\nu \in \{0, 1, 2, \dots\}$. This means the direct sum of all direct sums $(\mathbb{Z}/p^k\mathbb{Z})^{\alpha_k} := \alpha_k \cdot (\mathbb{Z}/p^k\mathbb{Z})$, $k = 1, 2, \dots$ (see Cor 2.1) in the decomposition of $Cl(\mathbb{Z}[\zeta_\nu])$ into cyclic subgroups.

Now $\mathcal{V}_n^+ \to V_n^+$ is surjective, so the dual map Char $(V_n^+) \to$ Char $(\mathcal{V}_n^+)$ is injective. (Hint: $i : A \to B$, $i_0 :$ Char $(B) \to$ Char (A) and $\gamma \in$ Char (B).

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[rr, bend right, "i_0(\gamma)"'] & B \arrow[r, "\gamma"] & \mu \end{tikzcd} \quad ; i_0(\gamma) \in \text{Char } (A).$$

Thus i surjective $\Leftrightarrow i_0$ injective.)

It follows that a canonical injection Char $(\mathcal{V}_n^+) \to S(\mathbb{Q}(\zeta_{n-1}))$ induces a canonical injection Char $(V_n^+) \to S(\mathbb{Q}(\zeta_{n-1}))$ as originally stated.

All this reasoning shows that it suffices to prove Theorem 2.1 with $\mathcal{V}_n$ in place of V_n.

By a remark before Theorem 2.1, we obtain $\mathcal{V}_n = \mathcal{V}_n^+ \oplus \mathcal{V}_n^- (|\mathcal{V}_n|$ is odd according to [K-M], p. 436).

Lemma 2.2 gives $E_n = \langle \zeta_n \rangle \cdot E_n^+$. Therefore $\mathcal{V}_n$ maps surjectively on $U_n/(X_n \cdot U_n^+)$ (this also follows from Corollary 2.2 and the fact that $\mathcal{V}_n$ maps onto V_n). But $U_n/(X_n \cdot U_n^+) = (U_n/(X_n \cdot U_n^+))^-$ because $U_n/(X_n \cdot U_n^+) = (U_n^+ \oplus U_n^-)/(X_n \cdot U_n^+) \cong U_n^-/X_n$. Hence there is a surjection

$$\mathcal{V}_n^- \to U_n/(X_n \cdot U_n^+).$$

Let $v \in \mathcal{V}_n^-$ map to $1 \in U_n/(X_n \cdot U_n^+)$. Then v can be represented by a unit $x^i u \in U_n$ with u, both symmetric and antisymmetric: $v = x^i u, c(u) = u, c(v) = v^{-1} = x^{-i}u^{-1} = x^{-i}c(u) = x^{-i}u$, i.e., $u^{-1} = u, u^2 = 1$. Now $|U_n| = p^{p^n-1}$ is odd, whence $u = 1$. Further, $j_0(E_n) \supset X_n(j_0(\zeta_n) = x)$, so $v = 1$. Thus for all primes $p \geq 3$:

$$\mathcal{V}_n^- \cong U_n/(X_n \cdot U_n^+).$$

The more difficult part of Theorem 2.1 (as well as this counterpart for the prime 2) is based on works by Iwasawa, about cyclotomic fields ([I1], [I2], [I3]), and on class field theory ([A-T], [Ha], [L]). It would take us too far ahead to develop these ideas. However, a couple of facts ought to be mentioned ([I1], [I3]): $S(\mathbb{Q}(\zeta_n + \zeta_n^{-1})) \cong S^+(\mathbb{Q}(\zeta_n))$ for all $n \geq 0$. $S(\mathbb{Q}(\zeta_0 + \zeta_0^{-1})) = 0 \Rightarrow S(\mathbb{Q}(\zeta_n + \zeta_n^{-1})) = 0$, $n \geq 0$. $S(\mathbb{Q}(\zeta_0)) = 0 \Rightarrow S(\mathbb{Q}(\zeta_n)) = 0$, $n \geq 0$.

Hence: If p is semi-regular, i.e., $S(\mathbb{Q}(\zeta_0 + \zeta_0^{-1})) = 0$, then $S(\mathbb{Q}(\zeta_n)) \cong S^-(\mathbb{Q}(\zeta_n))$ for all $n \geq 0$ (cf. Theorem 2.1).

Keep the notations, and assume for a moment that p is regular. By Theorem 2.1

$$\begin{aligned} &U(R_n)/(\mathbb{F}_p^* \oplus (X_n \cdot U_n^+)) \cong U_n/(X_n \cdot U_n^+) \cong \\ &\cong V_n^- = V_n = U(R_n)/j(U(\mathbb{Z}C_{p^n}) \oplus E_n). \end{aligned}$$

Lemma 2.4 stated that Im j is included in $\mathbb{F}_p^* \oplus (X_n \cdot U_n^+)$ for all primes $p \geq 3$. In our present case we get

$$j(U(\mathbb{Z}C_{p^n}) \oplus E_n) = \mathbb{F}_p^* \oplus (X_n \cdot U_n^+),\ p \text{ regular prime } \geq 3.$$

Recall the group W_n defined befor Th. 2.2. In [K-M] a formula for W_n for regular primes is also deduced. This is done with the aid of theorems and theories mentioned in this section. In a separate part a determination of V_1 is done in the case when p is a semi-regular prime. This is carried through without appeal to class field theory. The result is that $V_1 =$ Coker $j \cong (\frac{1}{2}(p-3) + \delta_p) \cdot \mathbb{Z}/p\mathbb{Z}$. If p is regular, i.e., $\delta_p = 0$, then $V_1^+ = 0; V_1 = V_1^- \cong \frac{1}{2}(p-3) \cdot \mathbb{Z}/p\mathbb{Z}$. Otherwise, for p semi-regular, we get $V_1^+ \cong \delta_p \cdot \mathbb{Z}/p\mathbb{Z}$.

2.2 Results of Galovich

Our aim to find the composition of $\tilde{K}_0(\mathbb{Z}C_{p^{n+1}})$ leads – as we have seen – to a thorough study of W_n.

S. Galovich announced an explicit formula for W_n (p regular, odd) in an article ([G1]) published in 1974. The expression contains direct sums of groups like $\mathbb{Z}/p^k\mathbb{Z}$, but nothing else. Unfortunately, a mistake was made in the proof, so the general formula (in [G1], p. 369) is not correct.

The error, which is of a more serious nature than a calculation lapse, was discovered by Ullom. He gave in [U1] a counterexample, using the cyclic group $\mathbb{Z}/3^4\mathbb{Z}$: Here $n = 3, p = 3$ (regular) and $W_3 = (\mathbb{Z}/9\mathbb{Z})^4 \oplus (\mathbb{Z}/3\mathbb{Z})^4$ instead of $(\mathbb{Z}/9\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^6$, as predicted incorrectly in [G1]. Yet the order is 3^{12} for both groups. See also [G2].

However, in [G2] and [U1] is noted that Galovich's result for p regular, odd, is valid for W_1 and W_2.

For the rest Galovich too uses Mayer-Vietoris sequences and algebraic K-theory. A great deal of the article is devoted to units in cyclotomic fields and it relies on theory from [He], [Hil], and [Se1].

In a separate part in [G1], a formula of W_1 is deduced for properly irregular primes p (cf. [K-M]). Such a prime is defined as: p is properly irregular if p divides the class number of $\mathbb{Q}(\zeta_0)$, but p does not divide the class number of $\mathbb{Q}(\zeta_0 + \zeta_0^{-1})$. The proof here for W_1 rests on cyclotomic field theory.

In a remark in [G1] it is stated that in the sequence $0 \to W_n \to \tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \oplus_{\nu=0}^{n} \tilde{K}_0(\mathbb{Z}[\zeta_\nu]) \to 0$, p does not divide the order of $\tilde{K}_0(\mathbb{Z}[\zeta_\nu]) \cong Cl(\mathbb{Z}[\zeta_\nu])$ for all ν if p is regular. Hence the sequence is split exact, i.e., $\tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \cong W_n \oplus (\oplus_{\nu=0}^{n} \tilde{K}_0(\mathbb{Z}[\zeta_\nu]))$, p odd, regular.

2.3 Refinements and Other Important Results

As above, we start with cyclic p-groups and p odd. By a general theorem, concerning p-groups ([C-R], Vol. II, p. 254) it follows that $W_n, n \geq 0$ is also a p-group and thus has odd order. Hence $W_n = W_n^+ \oplus W_n^-$.

A result by Fröhlich ([F], II) implies $|W_n^-| = p^{w_n^-}$, all primes ≥ 3, where $w_n^- = \frac{1}{2}\{\frac{p^{n+1}-1}{p-1} - (n+1)^2\}$. If p is regular, we get $V_n^+ = W_n^+ = 0$ and $|W_n| = |W_n^-| = p^{w_n^-}$, $n \geq 0$, see [K-M].

For all semi-regular primes $\geq 3, n \geq 1$ and under certain conditions on the so-called Iwasawa invariants, Ullom in [U2] proves: $W_n^+ \cong (\oplus_{j=1}^{n} \mathbb{Z}/p^j\mathbb{Z})^{\delta(p)}$ and $|W_n^+| = p^m$, with $m = \delta(p) \cdot \frac{n(n+1)}{2}$; $\delta(p)$ is defined in Part 2.1. See also [C-R], Vol. II, p.290.

In [O], Oliver completely describes the structure of W_n^-, viewed as an abelian group.

Let

$$\mathbb{Q}C_{p^{n+1}} := \mathbb{Q} \oplus (\oplus_{\nu=0}^{n} \mathbb{Q}(\zeta_\nu)).$$

At the end of the preceding section it was pointed out that the map $\tilde{K}_0(\mathbb{Z}C_{p^{n+1}}) \to \tilde{K}_0$(maximal order of $\mathbb{Q}C_{p^{n+1}}$), $n \geq 1$, is split for p odd, regular. Ullom proves ([U1]) that this map is not split if p is a properly irregular prime.

However, in [U1] is described an algorithm, with help of which Pic $(\mathbb{Z}C_{p^2})$ can be determined, for p properly irregular.

Stolin sharpens this result to an explicit expression, valid for all odd primes ([St 1]). Moreover, by a different method he proves Ullom's special case. The formula here – for Pic $(\mathbb{Z}C_{p^2})$ and p properly irregular – is expressed in terms of Bernoulli numbers.

In [C-R], Vol. II – essentially pp. 282-291 – a good survey of many important works on our subject can be found, up to the printing year 1987. Both Vol. I and II will also generally furnish the reader with several mathematical notions and definitions used in the articles mentioned above.

Matters for this paper, but treating the cases for the prime 2, can be found in some of the articles named above.

2.4 Some Results from Class Field Theory

Put $F_n := \mathbb{Q}(\zeta_n)$. Let $H_n = H_n(F_n)$ be the so-called ray ideal group, i.e., the group of those principal, fractional ideals in F_n, which possess a generating element, a, such that $a \equiv 1 \bmod \gamma_n^{p^n}$, where γ_n is the ideal generated by $\zeta_n - 1$ in F_n. Thus $H_n = \{(a) | a \in F_n, a \equiv 1 \bmod \gamma_n^{p^n}\}$; $a \equiv 1 \bmod \gamma_n^{p^n}$ signifies that the γ_n-valuation of $a - 1$ is at least p^n.

Let K_n/F_n be the p-part of the ray class field extension associated with the ray group H_n, that is, K_n/F_n is an abelian extension with Galois group

$$\text{Gal }(K_n/F_n) \cong (I_0(F_n)/H_n)_p,$$

where $I_0(F_n)$ is the group of ideals of F_n, which are prime to γ_n, and $(I_0(F_n)/H_n)_p$ is the p-primary component of $I_0(F_n)/H_n$.

No prime of F_n ramifies in K_n/F_n, except those dividing the conductor of H_n and therefore, γ_n is the only possibly ramified prime in K_n/F_n. See, for example, [Ha], Führer-Verzweigungs-Satz, page 136.

The other class field L_n we need is the p-part of the Hilbert class field of F_n. It is also an abelian extension, with Galois group.

$$\text{Gal }(L_n/F_n) \cong (I(F_n)/P(F_n))_p = S(F_n),$$

where $I(F_n)$ is the ideal group of F_n, and $P(F_n)$ the subgroup of principal ideals. Thus as above, $S(F_n)$ is the p-primary component of the ideal class group of F_n. The extension L_n/F_n is the p-part of the class field extension associated with the ray group $P(F_n)$.

Since $H_n \subset P(F_n)$, we have the inclusions

$$\mathbb{Q} \subset F_n \subset L_n \subset K_n.$$

Since $K_n/\mathbb{Q}$ and $L_n/\mathbb{Q}$ are Galois extensions, the group $G_n := \text{Gal }(F_n/\mathbb{Q})$ operates on Gal (K_n/F_n) and its subgroup Gal (K_n/L_n) via the group extension

$$1 \to \text{Gal }(K_n/F_n) \to \text{Gal }(K_n/\mathbb{Q}) \to G_n \to 1.$$

The following result unites class field theory with our topical problem.

Lemma 2.5. *There is a canonical isomorphism of G_n-modules*

$$\Theta : \textit{Gal }(K_n/L_n) \to U(R_n)/j_0(E_n) = \mathcal{V}_n,$$

where R_n, E_n and j_0 are defined in 2.1.

This class field theory, and more above that, can be found in [K-M], [A-T], [Ha] and [L].

§3 On Pic$(\mathbb{Z}C_{p^3})$

3.1 Presentation of the Problem

Define

$$A_2 := \mathbb{Z}[x]\Big/\left(\frac{x^{p^2}-1}{x-1}\right), A_3 := \mathbb{Z}[x]\Big/\left(\frac{x^{p^3}-1}{x-1}\right).$$

Our aim is to compute the kernel of the epimorphism $\mathrm{Pic}(A_3) \to \mathrm{Pic}(\mathbb{Z}[\zeta_2]) \oplus \mathrm{Pic}(A_2)$ for odd regular primes, using a generalization of Kummer's theorem.

As before, with $\zeta_2 = e^{2\pi i/p^3}$, one has $\mathbb{Z}[\zeta_2] \cong \mathbb{Z}[x]\Big/\left(\frac{x^{p^3}-1}{x^{p^2}-1}\right)$.

Set $\alpha := \left(\frac{x^{p^3}-1}{x^{p^2}-1}\right), \beta := \left(\frac{x^{p^2}-1}{x-1}\right)$. Then $\alpha \cap \beta = \left(\frac{x^{p^3}-1}{x-1}\right)$. Further $\alpha + \beta = \left(p, \frac{x^{p^2}-1}{x-1}\right)$. It follows that $\mathbb{Z}[x]/(\alpha+\beta) \cong A_2/(p) \cong \mathbb{F}_p[x]/(x-1)^{p^2-1} := D_2$. Thus with usual maps f_2, g_2

$$\begin{tikzcd}
A_3 \arrow[r] \arrow[d] & \mathbb{Z}[\zeta_2] \arrow[d, "f_2:\zeta_2\mapsto x"] \arrow[dl, "N"'] \\
A_2 \arrow[r, "g_2", "a\mapsto a\,\mathrm{mod} p"'] & D_2
\end{tikzcd} \qquad \text{(I)}$$

this diagram is a Cartesian square (for N see Section 3.3).

The (U, Pic)-variant of the Mayer-Vietoris sequence applied to (I) gives:

$$E_2 \oplus U(A_2) \to U(D_2) \to \mathrm{Pic}\ (A_3) \to \mathrm{Pic}\ (\mathbb{Z}[\zeta_2]) \oplus \mathrm{Pic}\ (A_2) \to 0$$

or

$$\begin{aligned} 0 \to \frac{U(D_2)}{\mathrm{Im}\ \{E_2 \oplus U(A_2) \to U(D_2)\}} \to \mathrm{Pic}\ (A_3) \to \\ \to Cl(\mathbb{Z}[\zeta_2]) \oplus \mathrm{Pic}\ (A_2) \to 0 \end{aligned}$$

where $E_n := U(\mathbb{Z}[\zeta_n])$. We have used that D_2 is a local ring and hence Pic $(D_2) = 0$. Note that Pic $(\mathbb{Z}C_{p^3}) \cong$ Pic (A_3) by Rim's theorem.

3.2 Structure of $U(D_2)$

With $x - 1 = y$ one gets

$$\begin{aligned} D_2 &= \mathbb{F}_p[y]/(y^{p^2-1}) = \\ &= \{a_0 + a_1 y + \ldots + a_{p^2-2} y^{p^2-2} + (y^{p^2-1}) | a_i \in \mathbb{F}_p\}. \end{aligned}$$

Hence D_2 contains p^{p^2-1} elements.

All elements in D_2, with $a_0 = 0$, are nilpotent in D_2 and $a_0 + (y^{p^2-1})$ is a unit, if $a_0 \neq 0$. Therefore $U(D_2)$ contains $(p-1) \cdot p^{p^2-2}$ elements.

Every finite abelian group is a direct sum of cyclic subgroups. This and theorems by Lagrange and Sylow give

$$U(D_2) \cong \mathbb{F}_p^* \oplus \tilde{U}(D_2),$$

where $\tilde{U}(D_2)$ is a p-group and $\tilde{U}(D_2) \cong (\mathbb{Z}_p)^{r_1} \oplus (\mathbb{Z}_{p^2})^{r_2} \oplus (\mathbb{Z}_{p^3})^{r_3} \oplus \ldots$.

Let us first consider the set $\{u \in \tilde{U}(D_2) | u^p = 1\}$. Let us study the equation $(1 + b_1 y + \ldots + b_{p^2-2} y^{p^2-2})^p = 1$ in $\mathbb{F}_p[y]$ with $y^{p^2-1} = 0$. Coefficients containing p disappear ($p = 0$ in $\mathbb{F}_p$). Further, $b_i^p = b_i$ (Fermat). We see that

$$\{u \in \tilde{U}(D_2) | u^p = 1\} = \{1 + b_p y^p + \ldots + b_{p^2-2} y^{p^2-2} | y^{p^2-1} = 0\}$$

and

$$\#\{u \in \tilde{U}(D_2) | u^p = 1\} = p^{p^2-2-(p-1)} = p^{p^2-p-1}.$$

Now

$$(1 + b_1 y + \ldots + b_{p^2-2} y^{p^2-2})^{p^2} = (1 + b_1 y^p + \ldots + b_{p-1} y^{p(p-1)})^p \equiv 1$$

in $\mathbb{F}_p[y]$ with $y^{p^2-1} = 0$. This implies that every element in $\tilde{U}(D_2)$ has order at most p^2. Thus $r_3 = r_4 = \ldots = 0$.

However in

$$\tilde{U}(D_2) \cong (\mathbb{Z}_p)^{r_1} \oplus (\mathbb{Z}_{p^2})^{r_2}$$

there are p elements in $\mathbb{Z}_{p^2}$ of order at most p. From the preceding facts, it thus follows that $|\tilde{U}(D_2)| = p^{p^2-2} = p^{r_1} \cdot (p^2)^{r_2}$ and $p^{p^2-p-1} = p^{r_1} \cdot p^{r_2}$, which gives

$$\left.\begin{array}{l} r_1 + 2r_2 = p^2 - 2 \\ r_1 + r_2 = p^2 - p - 1 \end{array}\right\}.$$

Hence $r_1 = p^2 - 2p$, $r_2 = p - 1$ and we have proved the following:

Proposition 3.1. $U(D_2) \cong \mathbb{F}_p^* \oplus (\mathbb{Z}_p)^{p^2-2p} \oplus (\mathbb{Z}_{p^2})^{p-1}$.

In the sequel, we will need one more expression for $U(D_2)$: Let us interpret D_2 as the set of polynomials in $x - 1$ over $\mathbb{F}_p$ with the subordinate condition $(x-1)^{p^2-1} = 0$. First, we see that $x^{p^2} - 1 = (x-1)^{p^2} = 0$, i.e., $x^{p^2} = 1$, so x is a unit. Now

$$x - x^{-1} = (x-1) \cdot x^{-1} \cdot (x+1) = (x-1) \cdot \frac{2 + (x-1)}{x}.$$

It follows that $2 + (x-1) \in U(D_2)$. This implies the following lemma.

Lemma 3.1. $U(D_2) = \{a_0 + b_1(x - x^{-1}) + \ldots + b_{p^2-2}(x - x^{-1})^{p^2-2} | \, a_0 \in \mathbb{F}_p^*, \, b_i \in \mathbb{F}_p\}$.

3.3 Im $\{E_2 \oplus U(A_2) \to U(D_2)\}$

At one lower step than (I), there is an analogous Cartesian square:

$$\begin{tikzcd}
A_2 \arrow[r] \arrow[d] & \mathbb{Z}[\zeta_1] \arrow[dl, "N_1"'] \arrow[d, "f_1:\zeta_1 \mapsto x"] \\
\mathbb{Z}[\zeta_0] \arrow[r, "g_0:\zeta_0 \mapsto x"'] & D_1
\end{tikzcd} \qquad \text{(II)}$$

Here N_1 is the usual norm map ([B-S], [C-R]), and $A_2 := \mathbb{Z}[x]/(\frac{x^{p^2}-1}{x-1})$, $\mathbb{Z}[\zeta_1] \cong \mathbb{Z}[x]/(\frac{x^{p^2}-1}{x^p-1})$, $\mathbb{Z}[\zeta_0] \cong \mathbb{Z}[x]/(\frac{x^p-1}{x-1})$, $D_1 := \mathbb{Z}[\zeta_0]/(p) \cong \mathbb{F}_p[x]/(x-1)^{p-1}$.

Lemma 3.2. *The lower, right triangle in diagram (II) is commutative.*

This is Lemma 1, p. 377 in [St 1], where a proof can be found. The lemma and (II) give:

$$\left.\begin{array}{ll} g_0(N_1(a)) = f_1(a), & a \in \mathbb{Z}[\zeta_1], \\ g_0(b) = b \bmod p \in D_1, & b \in \mathbb{Z}[\zeta_0]. \end{array}\right\}$$

Interpret A_2 as all possible pairs (a, b), where $a \in \mathbb{Z}[\zeta_1]$, $b \in \mathbb{Z}[\zeta_0]$, such that

$$g_0(b) = f_1(a).$$

Let us consider the following chain of the natural norm maps:

$$\mathbb{Z}[\zeta_2] \overset{N_2}{\to} \mathbb{Z}[\zeta_1] \overset{N_1}{\to} \mathbb{Z}[\zeta_0].$$

We can construct the map

$$N : \mathbb{Z}[\zeta_2] \to A_2$$

by $N(d) = (N_2(d), N_1(N_2(d)))$, $d \in \mathbb{Z}[\zeta_2]$, (see diagram (I)). Now $N_2(d) \in \mathbb{Z}[\zeta_1]$, $N_1(N_2(d)) \in \mathbb{Z}[\zeta_0]$. Since $N(d)$ has to be in A_2, we must check that

$$f_1(N_2(d)) = g_0(N_1(N_2(d))).$$

But, this is exactly what Lemma 3.2 tells us in the case $a = N_2(d) \in \mathbb{Z}[\zeta_1]$. Thus N is well defined.

Since N_1 and N_2 are usual norms, it follows that $N(uv) = N(u) \cdot N(v)$, $\forall u, v \in \mathbb{Z}[\zeta_2]$. Further, $N_1(1) = 1$, $N_2(1) = 1$, so $N(1) = (1, 1)$, the unit element in A_2. Hence, if ϵ is a unit in $\mathbb{Z}[\zeta_2]$, we get

$$(1, 1) = N(1) = N(\epsilon\epsilon^{-1}) = N(\epsilon) \cdot N(\epsilon^{-1});$$

$N(\epsilon)$ is a unit in A_2, and $N(\epsilon)^{-1} = N(\epsilon^{-1})$.

Proposition 3.2. *The lower, right triangle in diagram (I) is commutative.*

There is a proof of this in [St 2], pp. 448-450. Therefore we obtain the following diagram:

$$\begin{tikzcd}
& \epsilon \in E_2 = U(\mathbb{Z}[\zeta_2]) \arrow[dl, "N"'] \arrow[d, "f_2"] \\
U(A_2) \ni \underbrace{N(\epsilon)}_{\text{unit}} \arrow[r, "g_2"'] & \epsilon' \in U(D_2)
\end{tikzcd}$$

Here

$$\epsilon' = f_2(\epsilon) = g_2(N(\epsilon)) \qquad \text{(Prop. 3.2)}$$

Corollary 3.1.

$$\mathit{Im}\ \{E_2 \oplus U(A_2) \to U(D_2)\} = \mathit{Im}\ \{U(A_2) \to U(D_2)\}$$

3.4 The c -map and Kummer's Lemma

Let us introduce again a function c, which plays role of the complex conjugation in $A_2 = \mathbb{Z}[x]/(\frac{x^{p^2}-1}{x-1})$ and $D_i = \mathbb{F}_p[t]/(t-1)^{p^i-1}$. This function c can be defined by its action on generators: $c(x) = x^{-1}, c(t) = t^{-1}$.

We recall the following result (Kummer's lemma) for $E_n = U(\mathbb{Z}[\zeta_n])$.

Lemma 3.3. *Any element of E_n can represented uniquely in the form $\zeta_n^k \epsilon$, where ϵ is a real unit.*

As a corollary we obtain Kummer's lemma for A_2.

Lemma 3.4. *Any element of $U(A_2)$ can represented uniquely in the form $x^k \epsilon_r$, where $c(\epsilon_r) = \epsilon_r$.*

Proof: Take $\epsilon = (\epsilon_1, \epsilon_0) \in U(A_2)$, where $\epsilon_1 \in E_1, \epsilon_0 \in E_0$. By Lemma 3.3, $\epsilon_i = \zeta_i^{k_i} \epsilon_{i,r}$, where $i = 0, 1$ and $\epsilon_{i,r}$ is real.

Since the action of c commutes with the homomorphisms in the diagram

$$\begin{tikzcd}
U(A_2) \arrow[r] \arrow[d] & E_1 \arrow[d, "\zeta_1 \to t"] \\
E_0 \arrow[r, "\zeta_0 \to t"'] & U(D_1)
\end{tikzcd}$$

we see that $\epsilon_r = (\epsilon_{1,r}, \epsilon_{0,r}) \in U(A_2)$, and is real, that is $c(\epsilon_r) = \epsilon_r$, while $k_1 = k_0 + ps,\ s \in \mathbb{Z}$. Finally we get $\epsilon = x^{k_1}\epsilon_r$ and Kummer's lemma for A_2 is proved. □

We already know that $U(D_2) = \mathbb{F}_p^* \oplus \tilde{U}(D_2)$ with $\tilde{U}(D_2) = \{1 + b_1(t - t^{-1}) + \ldots + b_{p^2-2}(t - t^{-1})^{p^2-2} | \, b_i \in \mathbb{F}_p\}$ (Lemma 3.1). Observe that $\tilde{U}(D_2)$ is a finite abelian group of odd order $(= p^{p^2-2})$. By elementary group theory we hence get

$$\begin{aligned} \tilde{U}(D_2) &= \tilde{U}(D_2)^+ \oplus \tilde{U}(D_2)^-, \quad \text{where} \\ \tilde{U}(D_2)^+ &= \{u \in \tilde{U}(D_2) | c(u) = u\}, \\ \tilde{U}(D_2)^- &= \{u \in \tilde{U}(D_2) | c(u) = u^{-1}\}. \end{aligned}$$

Let us determine the structures of these two subgroups of $\tilde{U}(D_2)$. Obviously $c(t-t^{-1}) = t^{-1}-t = -(t-t^{-1}), c((t-t^{-1})^2) = (t-t^{-1})^2$, $c((t-t^{-1})^3) = -(t-t^{-1})^3$ and so on. Hereby, one sees that

$$\tilde{U}(D_2)^+ = \{1 + b_2(t - t^{-1})^2 + \ldots + b_{p^2-3}(t - t^{-1})^{p^2-3} | (t - t^{-1})^{p^2-1} = 0, \, b_i \in \mathbb{F}_p\}.$$

Therefore, $|\tilde{U}(D_2)^+| = p^{\frac{p^2-3}{2}}$. Further, there are $p^{\frac{p^2-3}{2} - \frac{p-1}{2}} = p^{\frac{p^2-p-2}{2}}$ elements in the set

$$\begin{aligned} &\{u \in \tilde{U}(D_2)^+ | u^p = 1\} = \{1 + b_{p+1}(t - t^{-1})^{p+1} + \ldots + \\ &+ b_{p^2-3}(t - t^{-1})^{p^2-3} | \, b_i \in \mathbb{F}_p\}. \end{aligned}$$

From Section 3.2, we know that

$$\tilde{U}(D_2)^+ \cong (\mathbb{Z}_p)^{s_1} \oplus (\mathbb{Z}_{p^2})^{s_2},$$

where s_1, s_2 satisfy the following equations

$$p^{\frac{p^2-3}{2}} = p^{s_1} \cdot (p^2)^{s_2}; \quad p^{\frac{p^2-p-2}{2}} = p^{s_1} \cdot p^{s_2} \quad \text{or} \quad \left. \begin{aligned} \frac{p^2-3}{2} &= s_1 + 2s_2 \\ \frac{p^2-p-2}{2} &= s_1 + s_2 \end{aligned} \right\},$$

i.e., $s_1 = \dfrac{p^2-2p-1}{2}$, $s_2 = \dfrac{p-1}{2}$. Finally using the structure of $U(D_2)$ obtained in Section 3.2, we get

Proposition 3.3.

$$\begin{aligned} \tilde{U}(D_2)^+ &\cong (\mathbb{Z}_p)^{\frac{p^2-2p-1}{2}} \oplus (\mathbb{Z}_{p^2})^{\frac{p-1}{2}}, \\ \tilde{U}(D_2)^- &\cong (\mathbb{Z}_p)^{\frac{p^2-2p+1}{2}} \oplus (\mathbb{Z}_{p^2})^{\frac{p-1}{2}}. \end{aligned}$$

3.5 Structure of Im $\{U(A_2) \to U(D_2)\}$

We start with the following version of Kummer's lemma:

Proposition 3.4. *Im* $\{U(A_2) \to U(D_2)\} \subset \mathbb{F}_p^* \oplus < t > \oplus \tilde{U}(D_2)^+$*, where* $< t >$ *is a cyclic group of order* p^2 *generated by* t.

On the other hand, we have:

Lemma 3.5. *Im*$\{U(A_2) \to U(D_2)\} \supset \mathbb{F}_p^* \oplus < t >$.

Proof: Since $< t >$ is obviously contained in the image of $U(A_2)$ in $U(D_2)$, we only have to show that $\mathbb{F}_p^*$ is contained in the image as well. Let $k \in \mathbb{F}_p^*$. We have $\frac{x^k-1}{x-1} \equiv k \bmod (x-1)$. Then $g_2\big(\frac{x^k-1}{x-1} - k\big)^{p^2} = 0$ and

$$g_2\Big(\frac{x^k-1}{x-1}\Big)^{p^2} = k^{p^2} = k,$$

since $k^{p^2} \equiv k \bmod p$. □

One of our principal goals is to prove the following

Theorem 3.1. *For* p *an odd regular prime*

$$Im\ \{U(A_2) \to U(D_2)\} = \mathbb{F}_p^* \oplus < t > \oplus \tilde{U}(D_2)^+.$$

It follows from Proposition 3.4 and Lemma 3.5 that what remains to be proved is that $g_2(U(A_2)) \supset \tilde{U}(D_2)^+$ if p is regular.

Consider the following diagram.

$$\begin{tikzcd}
U(A_2) \arrow[r, shift left] \arrow[d] & U(\mathbb{Z}[\zeta_1]) = E_1 \arrow[l, shift left, "F"] \arrow[dl, "N_1"] \arrow[d] \\
U(\mathbb{Z}[\zeta_0]) \arrow[r] & U(D_1)
\end{tikzcd}$$

Here N_1 is the restriction of the usual norm map and $F : E_1 \to U(A_2)$ is defined by

$$F(\epsilon) = (\epsilon, N_1(\epsilon)),\ \forall \epsilon \in E_1.$$

Observe that $(\epsilon, N_1(\epsilon)) \in U(A_2)$ due to Lemma 3.2. We see that F is a group homomorphism. Clearly, $F(\epsilon) = (1,1) \Rightarrow \epsilon = 1$, i.e., F is a monomorphism. Hence E_1 is embedded in $U(A_2)$.

Take $(\epsilon_1, \epsilon_0) \in U(A_2); \epsilon_1 \in E_1,\ \epsilon_0 \in E_0$. Write $(\epsilon_1, \epsilon_0) = (\epsilon_1, N_1(\epsilon_1)) \cdot (1, \epsilon_0 \cdot N_1(\epsilon_1^{-1})) = (\epsilon_1, N_1(\epsilon_1)) \cdot (1, \gamma)$, where $\gamma = \epsilon_0 \cdot N_1(\epsilon_1^{-1}) \in E_0$. By the above embedding, $(\epsilon_1, N_1(\epsilon_1)) \in E_1$. Of course, γ is mapped on $1 \in U(D_1)$ because $(1, \gamma) \in U(A_2)$. One concludes: $\gamma \equiv 1 \bmod p$. The division of (ϵ_1, ϵ_0) into products gives:

$$U(A_2) \cong E_1 \oplus B,$$

where B is a subgroup of $U(A_2)$ of the elements $(1,\gamma)$ above.

We are going to show: $g_2(E_1) \supset \tilde{U}(D_2)^+$, p regular. When this is done, Theorem 3.1 will be proved since $g_2(U(A_2)) \supset g_2(E_1)$.

Put $\tilde{U}(A_2) := \{\epsilon \in U(A_2) | \epsilon = 1 + a_1(x-1) + a_2(x-1)^2 + \ldots + a_{p^2-2}(x-1)^{p^2-2} | a_i \in \mathbb{Z}\}$. It is clear that $\tilde{U}(A_2)$ is mapped into $\tilde{U}(D_2)$. Similarly set $\tilde{U}(\mathbb{Z}[\zeta_1]) := \{\epsilon \in E_1 | \epsilon \equiv 1 \bmod (1-\zeta_1)\}$. From the earlier embedding of E_1 it follows

$$\tilde{U}(A_2) = \tilde{U}(\mathbb{Z}[\zeta_1]) \oplus \tilde{B}$$

for some subgroup $\tilde{B}$. Let $\tilde{U}(\mathbb{Z}[\zeta_1])^+$ be the subgroup of real units in $\tilde{U}(\mathbb{Z}[\zeta_1])$. The statement of Theorem 3.1 will follow from

Proposition 3.5. *$g_2(\tilde{U}(\mathbb{Z}[\zeta_1])^+) = \tilde{U}(D_2)^+$ when p is regular.*

We consider the map

$$g_2 : U(A_2) \overset{\text{mod} p}{\to} U(D_2) = U(A_2/(p)).$$

A key step in the proof of Proposition 3.5 is the following

Lemma 3.6. *Ker $\{E_1 \to U(D_2)\} \cong \{\epsilon \in \tilde{U}(\mathbb{Z}[\zeta_1]) | \epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-1}\}$.*

Proof: Suppose $(\epsilon, N_1(\epsilon)) \equiv (1,1) \bmod p$. Let $A_2 \ni (a,b) \equiv (1,1) \bmod p$. Then one gets $(a-1, b-1) \in A_2$ and

$$\begin{gathered} a \equiv 1 \bmod p \text{ in } \mathbb{Z}[\zeta_1], \\ b \equiv 1 \bmod p \text{ in } \mathbb{Z}[\zeta_0]; \\ p | (a-1, b-1), \quad \text{i.e.,} \end{gathered}$$

$$\left(\frac{a-1}{p}, \frac{b-1}{p}\right) \in A_2.$$

Therefore

$$f_1\left(\frac{a-1}{p}\right) = g_0\left(\frac{b-1}{p}\right) \quad \text{in} \quad D_1,$$

(diagram (II) in 3.3).

For all $z \in \mathbb{Z}[\zeta_1]$ we have

$$f_1(z) = g_0(N_1(z)).$$

Hence $g_0(N_1(\frac{a-1}{p})) = g_0(\frac{b-1}{p})$ in D_1. Since $g_0(y) = y \bmod p, \forall y \in \mathbb{Z}[\zeta_0]$, we conclude

$$\begin{gathered} A_2 \ni (a,b) \equiv (1,1) \bmod p \Leftrightarrow \\ N_1\left(\frac{a-1}{p}\right) \equiv \frac{b-1}{p} \bmod p. \end{gathered}$$

Both quantities in the latter congruence belong to $\mathbb{Z}[\zeta_0]$.

Our special case gives

$$\begin{aligned} E_1 \ni (\epsilon, N_1(\epsilon)) \equiv (1,1) \bmod p \Leftrightarrow \\ N_1\left(\frac{\epsilon - 1}{p}\right) \equiv \frac{N_1(\epsilon) - 1}{p} \bmod p \end{aligned} \tag{1}$$

Repeat: $N_1 : \mathbb{Z}[\zeta_1] \to \mathbb{Z}[\zeta_0]$ and

$$\dim(\mathbb{Q}(\zeta_1)/\mathbb{Q}(\zeta_0)) = [\mathbb{Q}(\zeta_1) : \mathbb{Q}(\zeta_0)] = p.$$

Now take $\epsilon \in E_1$ with $\epsilon \equiv 1 \bmod p$. That means $\epsilon = 1 + pt$ for some $t \in \mathbb{Z}[\zeta_1]$. By standard theory ([B-S], p. 404; [I-R], p. 173), we have

$$N_1(\epsilon) = \prod_{\gamma \in G} \gamma(\epsilon).$$

Here $G :=$ Gal $(\mathbb{Q}(\zeta_1)/\mathbb{Q}(\zeta_0)) :=$ the Galois group of $\mathbb{Q}(\zeta_1)$ over $\mathbb{Q}(\zeta_0)$, and $\gamma(u) = u$, if $u \in \mathbb{Q}(\zeta_0)$. Thus

$$\begin{aligned} N_1(\epsilon) &= \prod_{\gamma \in G} \gamma(1 + pt) = \prod_{\gamma \in G}(1 + p\gamma(t)) = \\ &= (1 + pt_1)(1 + pt_2) \cdot \ldots \cdot (1 + pt_p) = \\ &= 1 + p\sigma_1 + p^2\sigma_2 + \ldots + p^p\sigma_p, \end{aligned}$$

where

$$\sigma_1 := \sum_{i=1}^{p} t_i,\ \sigma_2 := \sum_{i<j} t_i t_j,\ \sigma_3 := \sum_{i<j<k} t_i t_j t_k, \ldots, \sigma_p := t_1 \cdot t_2 \cdot \ldots \cdot t_p$$

are the so-called elementary symmetric functions in $t_1, \ldots, t_p$ and $t_i := \gamma_i(t)$, $i = 1, \ldots, p$, i.e., the γ_i's constitute the group G.

Further we see that

$$Tr(t) = \sum_{\gamma \in G} \gamma(t) = \sigma_1 \in \mathbb{Z}[\zeta_0].$$

We claim that $p | Tr(t)$.
Proof: $1, \zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1}$ is a base for $\mathbb{Z}[\zeta_1]$ over $\mathbb{Z}[\zeta_0]$ because $\zeta_1^p = \zeta_0$. Moreover: $Tr(1) = \sum_{\gamma \in G} \gamma(1) = p$. For fixed $k \in \{1, 2, \ldots, p-1\}, \zeta_1^k$ satisfies the equation $x^p - \zeta_0^k = 0$. But here $0 = \sum_{\gamma \in G} \gamma(\zeta_1^k) = Tr(\zeta_1^k)$,
$k = 1, \ldots, p-1$. By the above

$$t \in \mathbb{Z}[\zeta_1] = \{a_0 + a_1\zeta_1 + \ldots + a_{p-1}\zeta_1^{p-1} | a_i \in \mathbb{Z}[\zeta_0]\}.$$

$\forall r, s \in \mathbb{Z}[\zeta_1]$, $u \in \mathbb{Z}[\zeta_0]$ is as well:

$$Tr(r+s) = Tr(r) + Tr(s); T(ur) = uTr(r).$$

So $Tr(t) = a_0 p$, some $a_0 \in \mathbb{Z}[\zeta_0]$.

That fact implies at once:

$$N_1(\epsilon) \equiv 1 \bmod p^2.$$

This, together with our basic assumption, $(\epsilon, N_1(\epsilon)) \equiv (1,1) \bmod p$, results via the congruence (1) in

$$N_1\left(\frac{\epsilon - 1}{p}\right) \equiv 0 \bmod p \tag{2}$$

in $\mathbb{Z}[\zeta_0]$.

It is well known that if $b_0 \in \mathbb{Z}$ then $(1-\zeta_1)|b_0$ is equivalent to $p|b_0$. Hence

$$\frac{\mathbb{Z}[\zeta_1]}{(1-\zeta_1)} \cong \{b_0 \bmod p | b_0 \in \mathbb{Z}\} = \mathbb{Z}/(p) = \mathbb{F}_p.$$

In other words, $\mathbb{F}_p$ is a complete system of residues (containing 0) of the ring $\mathbb{Z}[\zeta_1]$ modulo the prime ideal $(1-\zeta_1)$. With $\lambda_1 := (1-\zeta_1)$ the λ_1-adic completion to $\mathbb{Z}[\zeta_1]$ will consequently be

$$\Lambda := \{a_0 + a_1(1-\zeta_1) + \ldots + a_n(1-\zeta_1)^n + \ldots | a_i \in \mathbb{F}_p\}.$$

We can regard our unit ϵ as an element of Λ. Since $((1-\zeta_1)^{p^2-p}) = (p)$ one sees that the assumption $\epsilon \equiv 1 \bmod p$ is equivalent to $\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-p}$ in Λ. But $(1-\zeta_1)^{p^2-p} = p \cdot \kappa$ for some unit κ, so

$$\frac{\epsilon - 1}{p} = \sum_{k=0}^{\infty} a_{p^2-p+k} \cdot \kappa \cdot (1-\zeta_1)^k,$$

where $a_i \in \{0, 1, \ldots, p-1\}$.

In the proof of Lemma 1, p. 377 in [St 1] is shown

$$N_1(a+b) \equiv (N_1(a) + N_1(b)) \bmod p.$$

Further, $N_1(a_i) = a_i^p = a_i$ when $a_i \in \mathbb{F}_p$. It can be proved from the definition of N_1 that $N_1(1-\zeta_1) = 1 - \zeta_0$.

All this applied to congruence (2), derived earlier, gives

$$N_1\left(\frac{\epsilon - 1}{p}\right) \equiv \sum_{k=0}^{\infty} a_{p^2-p+k} \cdot N_1(\kappa) \cdot (1-\zeta_0)^k \equiv 0 \bmod p$$

in Λ. That the sum is divisible by p means $a_{p^2-p+k} = 0$ for all $k = 0, 1, \ldots, p-2$ because $((1-\zeta_0)^{p-1}) = (p)$ in $\mathbb{Z}[\zeta_0]$ ($N_1(\kappa)$ a unit). Hence $\frac{\epsilon-1}{p} = \sum_{k=p-1}^{\infty} a_{p^2-p+k} \cdot \kappa \cdot (1-\zeta_1)^k$ in Λ, i.e., $\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-1}$ since $(p) = ((1-\zeta_1)^{p^2-p})$ in $\mathbb{Z}[\zeta_1]$.

If conversely, we begin with $\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-1}$ in Λ, it is easily seen that the original condition $(\epsilon, N_1(\epsilon)) \equiv (1,1) \bmod p$ holds. □

Supplement for Section 3.5

Let us first mention that the ring $\mathbb{Z}[\zeta_1]$ is everywhere dense in its λ_1-adic completion Λ (in the topology, defined by the λ_1-adic valuation and its metric), $\lambda_1 = (1-\zeta_1)$. This fact makes it possible to translate the congruences unaffected between these two sets.

However, for future use we will state some basic theory regarding these matters.

Start with $K := \mathbb{Q}(\zeta_1)$ which is the quotient field of the Dedekind ring $\mathbb{Z}[\zeta_1]$. Consider the prime ideal $\lambda_1 = (1-\zeta_1)$ in $\mathbb{Z}[\zeta_1]$. For a fixed arbitrary $c, 0 < c < 1$, define $\varphi_{\lambda_1}(x) := c^{\nu_{\lambda_1}(x)}$, $\forall x \in K$, where ν_{λ_1} is the usual exponential valuation with respect to λ_1. φ_{λ_1} is a metric on K.

The valuation ring $R := \{x \in K | \varphi_{\lambda_1}(x) \leq 1\}$ is local with a maximal ideal $\mathfrak{p}_1$ and quotient field $K = \mathbb{Q}(\zeta_1)$. Since R is a principal ideal domain, R is a discrete valuation ring (DVR).

Let $K_{\mathfrak{p}_1}$ denote the $\mathfrak{p}_1$-adic (here λ_1-adic) completion of K and let $\bar{\varphi}_{\lambda_1}$ be the valuation on $K_{\mathfrak{p}_1}$ corresponding to φ_{λ_1}. The valuation ring $\hat{R}$ in $K_{\mathfrak{p}_1}$ is also a DVR with a maximal ideal $\hat{\mathfrak{p}}_1$.

It is a fact that the $\mathfrak{p}_1$-adic (λ_1-adic) valuation on $\mathbb{Q}$ is equivalent to the p-adic valuation on $\mathbb{Q}$.

The p-adic completion of $\mathbb{Q}$ is $\mathbb{Q}_p$, the field of p-adic numbers. Let $O_p \subset \mathbb{Q}_p$ be the ring of p-adic integers. We see that the λ_1-adic completion of $\mathbb{Q}$ is $\mathbb{Q}_p$. Moreover, $K_{\mathfrak{p}_1} = \mathbb{Q}_p(\zeta_1)$ and $\hat{R} = O_p[\zeta_1]$ ($\mathbb{Z}[\zeta_1]$ is dense in $O_p[\zeta_1]$).

In $\mathbb{Q}_p(\zeta_1)$ and $O_p[\zeta_1]$ we have representations

$$\mathbb{Q}_p(\zeta_1) = \{a_0 + a_1(1-\zeta_1) + \ldots + a_{p^2-p-1}(1-\zeta_1)^{p^2-p-1} | a_i \in \mathbb{Q}_p\},$$
$$O_p[\zeta_1] = \{b_0 + b_1(1-\zeta_1) + \ldots + b_{p^2-p-1}(1-\zeta_1)^{p^2-p-1} | b_i \in O_p\}$$

and every nonzero element in $K_{\mathfrak{p}_1}$ can be uniquely expressed by

$$(1-\zeta_1)^r(s_0 + s_1(1-\zeta_1) + \ldots + s_n(1-\zeta_1)^n + \ldots),$$

where $r \in \mathbb{Z}, s_i \in S, s_0 \neq 0$ and where we may set $S = \{0, 1, \ldots, p-1\} = \mathbb{F}_p$. The power series, in the brackets above, is a unit in $\hat{R}$ $(s_0 \neq 0)$. Clearly

$$\hat{R} = \{s_0 + s_1(1-\zeta_1) + \ldots + s_n(1-\zeta_1)^n + \ldots | s_i \in \mathbb{F}_p\}.$$

A comparison shows that this set is our ring Λ which was introduced earlier in a slightly different manner. Hence $\Lambda = O_p[\zeta_1]$.

For proofs and further discussion see for example [B-S], Ch. 1 and Ch. 4; [J], Ch. II and [Se 2], Ch. II.

3.6 A Variant of Kummer's Theorem

Theorem 3.2. *If p is an odd regular prime, and $\epsilon \in E_1 = U(\mathbb{Z}[\zeta_1])$ satisfies $\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-1}$, then $\epsilon = \gamma^p$ for some unit $\gamma \in E_1$ with $\gamma \equiv 1 \bmod (1-\zeta_1)^{p+1}$.*

Proof: We start with the following statement:

Lemma 3.7. *Let $q \in \mathbb{Z}[\zeta_{n-1}]$, where $\zeta_{n-1}^{p^n} = 1$. Let also $q \equiv 1 \bmod (1-\zeta_{n-1})^{p^n-1}$ and $(q) = I^p$ for some ideal I in $\mathbb{Z}[\zeta_{n-1}]$. Then $q \equiv 1 \bmod (1-\zeta_{n-1})^{p^n}$, $n = 1, 2, \ldots$; p an arbitrary odd prime.*

This is Lemma 2, p. 377 in [St 1], where a proof is given.

In Theorem 3.2, $n = 2, q = \epsilon \in E_1$. Assume $\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-1}$. Clearly, since ϵ is a unit, $(\epsilon) = \mathbb{Z}[\zeta_1] = (\mathbb{Z}[\zeta_1])^p$. Lemma 3.7 implies

$$\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2} \qquad (*)$$

Lemma 3.8. *The unit ϵ in $(*)$ is real.*

Proof: Lemma 3.3 and $(*)$ give $\epsilon = \zeta_1^k \cdot \theta \equiv 1 \bmod (1-\zeta_1)^{p^2}$ for some $k \in \mathbb{Z}$; $c(\theta) = \bar{\theta} = \theta$. Since $\zeta_1^{p^2} = 1$, we may assume $k > 0$. Let us work on $\mathbb{Z}[\zeta_1]$.

Writing $\epsilon = 1 + (1-\zeta_1)^{p^2} \cdot t$, $t \in \mathbb{Z}[\zeta_1]$, one has for the complex conjugate: $\bar{\epsilon} = 1 + (1-\bar{\zeta_1})^{p^2} \cdot \bar{t} = 1 + (1-\frac{1}{\zeta_1})^{p^2} \cdot \bar{t} = 1 + (\zeta_1 - 1)^{p^2} \cdot \bar{t}$. So also $\bar{\epsilon} \equiv 1 \bmod (1-\zeta_1)^{p^2}$. From this we clearly have $(\bar{\epsilon})^{-1} \equiv 1 \bmod (1-\zeta_1)^{p^2}$. But $(\bar{\epsilon})^{-1} = \zeta_1^k \cdot \theta^{-1}$, whence

$$\zeta_1^{2k} = \epsilon \cdot (\bar{\epsilon})^{-1} \equiv 1 \bmod (1-\zeta_1)^{p^2}.$$

Now it is obvious that $(1-\zeta_1)^{p^2} | (1-\zeta_1^{2k}) = (1-\zeta_1) \cdot \frac{1-\zeta_1^{2k}}{1-\zeta_1}$. If $(2k, p) = 1$, $(1-\zeta_1^{2k})/(1-\zeta_1)$ is a unit. Then, $(1-\zeta_1)^{p^2} | (1-\zeta_1)$, which is absurd, since $1-\zeta_1$ is not a unit. Therefore $k = p \cdot k_0$, $k_0 \in \mathbb{Z}$ (p odd).

Now we have, $(1-\zeta_1)^{p^2} | (1-\zeta_0^{2k_0})$ in $\mathbb{Z}[\zeta_1]$ because $\zeta_1^p = \zeta_0$. The ideal relation $((1-\zeta_1)^{p^2-p}) = (p)$ implies that $p | (1-\zeta_0^{2k_0})$ in $\mathbb{Z}[\zeta_1]$. Thus there is $\ell \in \mathbb{Z}[\zeta_1]$: $1-\zeta_0^{2k_0} = \ell \cdot p$. Further, $\ell = (1-\zeta_0^{2k_0})/p \in \mathbb{Q}(\zeta_0)$ is an algebraic integer, i.e., $\ell \in \mathbb{Z}[\zeta_0]$. Recall that $((1-\zeta_0)^{p-1}) = (p)$ as ideals in $\mathbb{Z}[\zeta_0]$.

One gets for instance, $(1-\zeta_0)^2 | (1-\zeta_0^{2k_0})$ $(p \geq 3)$ and so $1-\zeta_0 | (1+\zeta_0+\ldots+\zeta_0^{2k_0-1}) \equiv 2k_0 \bmod (1-\zeta_0)$ in $\mathbb{Z}[\zeta_0]$. Hereby $p | 2k_0$ ([B-S], p. 158, Lemma 2) and $p^2 | k = p \cdot k_0$. Finally $\epsilon = \theta$, a real unit in $\mathbb{Z}[\zeta_1]$. □

Of course, $1 + \zeta_1 = \frac{1-\zeta_1^2}{1-\zeta_1}$ is a unit in $\mathbb{Z}[\zeta_1]$. But, $\zeta_1 - \zeta_1^{-1} = (\zeta_1 - 1) \cdot \frac{\zeta_1+1}{\zeta_1}$, whence $\zeta_1 - \zeta_1^{-1}$ and $\zeta_1 - 1$ are associates. They generate the same maximal ideal in $\mathbb{Z}[\zeta_1]$.

Following the technique in 3.2 and 3.4 for $U(D_2)$, we get from the congruence $(*)$: $\epsilon = 1 + b_{p^2}(\zeta_1 - \zeta_1^{-1})^{p^2} + b_{p^2+1}(\zeta_1 - \zeta_1^{-1})^{p^2+1} + \ldots$, $b_i \in \mathbb{Z}$. Since ϵ is real, $\epsilon - \bar{\epsilon} = 0$, and all coefficients with odd indices vanish. Hence

$$\epsilon \equiv 1 \bmod (\zeta_1 - \zeta_1^{-1})^{p^2+1}$$

or equivalently,

$$\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2+1} \qquad (**)$$

Proposition 3.6. *Suppose that $\epsilon \in E_1$ and $\epsilon \equiv 1 \bmod (1-\zeta_1)^{p^2-1}$. Then $\sqrt[p]{\epsilon} \in O_p[\zeta_1]$.*

Proof: One has $\epsilon \in O_p[\zeta_1]$ (see supplement at the end of Section 3.5). Recently we saw that ϵ must satisfy (**) and be real. Therefore,

$$\epsilon = 1 + a_{p^2+1}(\zeta_1 - \zeta_1^{-1})^{p^2+1} + a_{p^2+3}(\zeta_1 - \zeta_1^{-1})^{p^2+3} + \ldots = 1 + \beta\lambda^{p^2+1},$$

where $a_i \in O_p$ = ring of p-adic integers, $\lambda := \zeta_1 - \zeta_1^{-1} \in O_p[\zeta_1], \beta := a_{p^2+1} + a_{p^2+3}(\zeta_1 - \zeta_1^{-1})^2 + \ldots \in O_p[\zeta_1]$. Accordingly study the quantity

$$\begin{aligned}\epsilon^{1/p} &= (1 + \beta\lambda^{p^2+1})^{1/p} = \\ &= 1 + \sum_{\nu=1}^{\infty}\left[\frac{1}{\nu!}\cdot\frac{1}{p}\left(\frac{1}{p}-1\right)\cdot\ldots\cdot\left(\frac{1}{p}-\nu+1\right)\cdot\beta^{\nu}\cdot\lambda^{(p^2+1)\cdot\nu}\right].\end{aligned}$$

Employing the relation $((\zeta_1 - \zeta_1^{-1})^{p^2-p}) = (p)$, one arrives at

$$\begin{aligned}\epsilon^{1/p} &= 1 + \sum_{\nu=1}^{\infty}\left[\frac{1}{\nu!}\cdot p^{-\nu}\cdot\lambda^{(p^2+1)\cdot\nu}\cdot\gamma'_{\nu}\right] = \\ &= 1 + \sum_{\nu=1}^{\infty}\left[\gamma_{\nu}\cdot\frac{1}{\nu!}\cdot\lambda^{(p^2+1)\cdot\nu-(p^2-p)\cdot\nu}\right] = \\ &= 1 + \sum_{\nu=1}^{\infty}\left[\gamma_{\nu}\cdot\frac{1}{\nu!}\cdot\lambda^{(p+1)\cdot\nu}\right],\end{aligned}$$

where $\gamma'_{\nu}, \gamma_{\nu} \in O_p[\zeta_1]$. Here we recall that the set of rational numbers $\{\frac{r}{s} | s \not\equiv 0 \bmod p\}$ forms a subring of O_p ([B-S], p.22). This indicates that we have to examine whether the p-factors in $\nu!$ will be sufficiently "compensated" by the λ-factors in the numerator.

Let k_{ν} be the number of p-factors in $\nu!$. Then $\epsilon^{1/p} = 1 + \sum_{\nu=1}^{\infty}[\delta_{\nu}\cdot\lambda^{e_{\nu}}]$, where $\delta_{\nu} \in O_p[\zeta_1]$ and $e_{\nu} := (p+1)\cdot\nu - (p^2-p)\cdot k_{\nu}$. Since ν increases linearly, it is clear that we need to control only the most critical points $\nu = p^n$, $n = 1, 2, \ldots$. If for $z \in \mathbb{R}$, $[z]$ is the biggest rational integer $\leq z$, a well-known formula gives $k_{p^n} = [\frac{p^n}{p}] + [\frac{p^n}{p^2}] + \ldots + [\frac{p^n}{p^n}] = p^{n-1} + p^{n-2} + \ldots + p + 1$. Hence $e_{p^n} = (p+1)\cdot p^n - (p^2-p)(p^{n-1} + \ldots + p + 1) = p^n + p$.

Let us now refer to the supplement of Section 3.5. With our definitions we have $\lambda = \zeta_1 - \zeta_1^{-1}$ and the ideal $\lambda_1 = (1-\zeta_1) = (\zeta_1 - \zeta_1^{-1})$, both in $\mathbb{Z}[\zeta_1]$ and $O_p[\zeta_1]$. The partial sums $s_n = 1 + \sum_{\nu=1}^{n}(\delta_{\nu}\cdot\lambda^{e_{\nu}})$, $n = 1, 2, \ldots$, are of interest to us. Since $\delta_{\nu} \in O_p[\zeta_1]$ and $e_{p^n} = p^n + p$, our analysis implies that the general term and so also the partial sums lie in $O_p[\zeta_1] = \hat{R}$.

From the supplement is obtained: $\bar{\varphi}_{\mathfrak{p}_1}(\delta_{p^n}\cdot\lambda^{e_{p^n}}) = \bar{\varphi}_{\mathfrak{p}_1}(\delta_{p^n})\cdot c^{p^n+p} \leq c^{p^n+p} \to 0$, $n \to \infty$ because $0 < c < 1$. Our reasoning gives the same limit for the general term in s_n. It follows that $\{s_n\}$ is a Cauchy sequence in $K_{\mathfrak{p}_1}$ which is complete in respect of the valuation $\bar{\varphi}_{\mathfrak{p}_1}$. Therefore $\{s_n\}$ converges to an element in $K_{\mathfrak{p}_1}$. This element was denoted $\epsilon^{1/p}$, the existence of which thus is established.

Now $\hat{R} = O_p[\zeta_1]$ is a closed set in $K_{\mathfrak{p}_1}$ ([B-S], p. 254). In fact, $\hat{R}$ is compact. Since $\{s_n\}$ lies in $\hat{R}$, it is a consequence that its limit $\epsilon^{1/p} = \sqrt[p]{\epsilon}$ is an element in $\hat{R} = O_p[\zeta_1]$. Proposition 3.6 is proved. □

Again, studying the proof of Proposition 3.6, one easily checks that $e_\nu \geq p+1$ for all ν. Hence we get

Corollary 3.2. *In Proposition 3.6,* $\sqrt[p]{\epsilon} \equiv 1 \bmod (1-\zeta_1)^{p+1}$ *is valid in* $O_p[\zeta_1]$.

Consider the finite, separable, algebraic extension $K = \mathbb{Q}(\zeta_1) \subset K(\epsilon^{1/p})$; ϵ as before. Let $\mathbb{Z}_\epsilon$ be the integral closure of $\mathbb{Z}[\zeta_1]$ in $K(\epsilon^{1/p})$. Then $\mathbb{Z}_\epsilon$ is integral over $\mathbb{Z}[\zeta_1]$ and we can to a given prime ideal α of $\mathbb{Z}[\zeta_1]$, find a prime ideal β of $\mathbb{Z}_\epsilon$ such that $\beta \cap \mathbb{Z}[\zeta_1] = \alpha$.

Suppose $\alpha \neq (0) \neq \beta$ and form the completions K_α of $K = \mathbb{Q}(\zeta_1)$ and $(K(\epsilon^{1/p}))_\beta$. The valuation rings $(\mathbb{Z}[\zeta_1])_\alpha$ and $(\mathbb{Z}_\epsilon)_\beta$ are DVR's, i.e. principal ideal domains with a single nonzero prime ideal which is also maximal.

Thus α corresponds to a principal ideal (a) in $(\mathbb{Z}[\zeta_1])_\alpha$ and β to a principal ideal (b) in $(\mathbb{Z}_\epsilon)_\beta$. All nonzero ideals in the two rings are powers of the respective maximal ideals. But $(a) \subset (\mathbb{Z}[\zeta_1])_\alpha \subset (\mathbb{Z}_\epsilon)_\beta$ so $(a)(\mathbb{Z}_\epsilon)_\beta = (b)^n$ for some $n \in \{1, 2, \ldots\}$. Hence (a) is ramified in $(\mathbb{Z}_\epsilon)_\beta$ if n is bigger than 1 and non-ramified if $n = 1$. The ramification indices $e(\beta/\alpha)$ and $e((b)/(a)) = n$ are in fact equal by [C-F], p. 18 or [J], p. 106. We are going to show that the extension $K \subset K(\epsilon^{1/p})$ is non-ramified.

Example: Put $\alpha = \lambda_1 = (1-\zeta_1)$ and let ϵ be as in Proposition 3.6. Take $\beta \subset \mathbb{Z}_\epsilon : \beta$ prime, $\beta \cap \mathbb{Z}[\zeta_1] = \alpha = \lambda_1$. Complete the fields K and $K(\epsilon^{1/p})$ with respect to α and β respectively. In this case, we get for the corresponding rings: $(\mathbb{Z}[\zeta_1])_\alpha = (\mathbb{Z}[\zeta_1])_{\mathfrak{p}_1} = \hat{R} = O_p[\zeta_1] \subset \mathbb{Q}_p(\zeta_1)(\mathbb{Q}_p = \{p - \text{adic numbers}\})$ and $(\mathbb{Z}_\epsilon)_\beta = (\mathbb{Z}[\zeta_1])_{\mathfrak{p}_1}(\epsilon^{1/p}) = (O_p[\zeta_1])(\epsilon^{1/p})$. By Proposition 3.6, $\epsilon^{1/p} \in O_p[\zeta_1] \subset K_\alpha = \mathbb{Q}_p(\zeta_1)$. Hence $K_\alpha = (K(\epsilon^{1/p}))_\beta = (\mathbb{Q}_p(\zeta_1))(\epsilon^{1/p})$, and so the rings – with their induced maximal ideals $(a), (b)$ from α, β respectively – coincide. Using our theorem about ramification indices, we get $e(\beta/\alpha) = e((b)/(a)) = n = 1$. It follows that $\alpha = \lambda_1 = (1-\zeta_1)$ is not ramified in $\mathbb{Z}_\epsilon$.

Consider all bases of $K(\epsilon^{1/p})$ over $K = \mathbb{Q}(\zeta_1)$ that lie in $\mathbb{Z}_\epsilon$. The corresponding discriminants lie in $\mathbb{Z}[\zeta_1]$ and generate the so-called discriminant ideal Δ of $\mathbb{Z}_\epsilon$ over $\mathbb{Z}[\zeta_1]$. So $\Delta \subset \mathbb{Z}[\zeta_1]$.

Lemma 3.9. *The prime ideals of* $\mathbb{Z}[\zeta_1]$*, which are ramified in* $\mathbb{Z}_\epsilon$*, are those containing the discriminant ideal,* Δ *([C-F], p. 22; [J], p. 35).*

Lemma 3.10. *The ideal* Δ *– in the extension* $K \subset K(\epsilon^{1/p})$ *– contains* $(p^p\epsilon^{p-1}) = (p^p) = ((1-\zeta_1)^{p(p^2-p)}) = \lambda_1^{p^2(p-1)}; \lambda_1 = (1-\zeta_1)$ *([C-F], p. 91; [J], pp. 39-40).*

Proof of Theorem 3.2: Take a prime ideal ω in $\mathbb{Z}[\zeta_1]$. Suppose that ω is ramified in $\mathbb{Z}_\epsilon$. We get $\omega \supset \Delta \supset \lambda_1^{p^2(p-1)}$. Since ω is a prime ideal, it follows $\omega \supset \lambda_1$. Hence there is an ideal $\tau \subset \mathbb{Z}[\zeta_1] : \lambda_1 = \omega\tau$ because $\mathbb{Z}[\zeta_1]$ is a Dedekind domain. But λ_1 is also a prime ideal, whence $\omega = \lambda_1(\tau = \mathbb{Z}[\zeta_1])$. So λ_1 is the only prime ideal in $\mathbb{Z}[\zeta_1]$ that possibly ramifies in $K(\epsilon^{1/p})$. Now we saw from the example, recently given, that λ_1 does not ramify, either. The finite, separable, algebraic extension $K \subset K(\epsilon^{1/p})$ therefore is a non-ramified extension.

Now $\epsilon \in E_1 = U(\mathbb{Z}[\zeta_1]) \subset K = \mathbb{Q}(\zeta_1)$. The polynomial $x^p - \epsilon$ lies in $K[x]$ and K contains $\zeta_1^p = \zeta_0$, a primitive p-th root of unity. If L is the splitting field over K for $x^p - \epsilon$, then $\epsilon^{1/p} \in L$ since $\epsilon^{1/p}$ is a root of $x^p - \epsilon$. Clearly $L \supset K$, whence $K \subset K(\epsilon^{1/p}) \subset L$. By a theorem ([A], p. 61) now is valid, either 1) $L = K$ and $x^p - \epsilon$ is split in $K[x]$, or 2) $x^p - \epsilon$ is irreducible over K.

Let us consider the second case. Then, by definition $\epsilon^{1/p}$ is algebraic of degree p over K. By elementary theory, the degree of $K(\epsilon^{1/p})$ over K equals p. Point 2) above and the preceding analysis, accordingly imply – under the hypothesis about ϵ in Theorem 3.2 (and Proposition 3.6): $K \subset K(\epsilon^{1/p})$ is non-ramified of degree p. But now we also assumed p to be regular. However, by theories developed by Iwasawa, it is known that $K = \mathbb{Q}(\zeta_1)$ has no non-ramified extensions of degree p, if p is a regular odd prime. Consequently, if all the conditions of Theorem 3.2 are fulfilled, then 1) above must hold. This implies $K = K(\epsilon^{1/p})$ and so $\gamma := \epsilon^{1/p} \in K$.

Further, we have $\epsilon = \gamma^p \in E_1 \subset \mathbb{Z}[\zeta_1]$ and $\mathbb{Z}[\zeta_1]$ is the ring of algebraic integers in K. From this it follows easily that $\gamma \in E_1$. Finally, also recall that $\gamma \equiv 1 \bmod (1 - \zeta_1)^{p+1}$ by Corollary 3.2. This completes the proof of Theorem 3.2. □

Now we can finish the proof of Theorem 3.1. Define $\tilde{U}_m := \tilde{U}_m(\mathbb{Z}[\zeta_1]) := \{\epsilon \in U(\mathbb{Z}[\zeta_1]) | \epsilon \equiv 1 \bmod (1 - \zeta_1)^m\}$, $m = 1, 2, \ldots$. Then $\tilde{U}_1 \supset \tilde{U}_2 \supset \tilde{U}_3 \supset \ldots$ are subgroups of $\tilde{U}_1 = \tilde{U}(\mathbb{Z}[\zeta_1]) = \tilde{U}$. Recall that $E_1 = U(\mathbb{Z}[\zeta_1])$ was embedded in $U(A_2)$ and $\tilde{U}_1$ in $\tilde{U}(A_2)$. Further, let $\tilde{U}_m^+$ be the subgroup of real units in $\tilde{U}_m$, $m = 1, 2, \ldots$. We observe that g_2 maps $\tilde{U}_1^+$ into $\tilde{U}(D_2)^+$ because g_2 and c (conjugation) commute. Finally we see that what is left to prove is that $g_2(\tilde{U}_1^+) = \tilde{U}(D_2)^+$, when p is an odd regular prime. By elementary group theory

$$g_2(\tilde{U}_1^+) \cong \frac{\tilde{U}_1^+}{\text{Ker } \{\tilde{U}_1^+ \to \tilde{U}(D_2)^+\}} = \frac{\tilde{U}_1^+}{\tilde{U}_{p^2-1}^+}.$$

The last equality holds by Lemma 3.6.

By Dirichlet's unit theorem $E_1 \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}^{\frac{p^2-p}{2}-1}$.

If E_1^+ is the set of real units in E_1, then

$$\text{Ker } \{\tilde{U}_1^+ \to \tilde{U}(D_2)^+\} = \text{Ker } \{E_1^+ \to U(D_2)^+\} \qquad \text{(L. 3.6)}$$

and $|g_2(E_1^+)| = \left|\frac{E_1^+}{\tilde{U}_{p^2-1}^+}\right| = \left|\frac{E_1^+}{\tilde{U}_1^+}\right| \cdot \left|\frac{\tilde{U}_1^+}{\tilde{U}_{p^2-1}^+}\right| < \infty$, because $g_2(E_1^+) \subset U(D_2)^+$ and

$|g_2(E_1^+)| \leq |U(D_2)^+| < \infty$. Thus $\left|\frac{E_1^+}{\tilde{U}_1^+}\right| < \infty$. It is clear that the complex component disappears for real units, so $E_1^+ \cong \mathbb{Z}^{\frac{p^2-p}{2}-1} \cong \tilde{U}_1^+$.

Obviously,

$$\left|\frac{\tilde{U}_1^+}{\tilde{U}_{p^2-1}^+}\right| = \left|\frac{\tilde{U}_1^+}{\tilde{U}_{p-1}^+}\right| \cdot \left|\frac{\tilde{U}_{p-1}^+}{\tilde{U}_{p+1}^+}\right| \cdot \left|\frac{\tilde{U}_{p+1}^+}{\tilde{U}_{p^2-1}^+}\right| < \infty \tag{a}$$

This partition is a trick in the proof. First, it follows:

$$\tilde{U}_k^+ \cong \mathbb{Z}^{\frac{p^2-p}{2}-1} \quad \text{for} \quad k = p-1, p+1, p^2-1.$$

Theorem 3.2 easily implies: $\tilde{U}_{p^2-1}^+ = (\tilde{U}_{p+1}^+)^p$. Hence $\frac{\tilde{U}_{p+1}^+}{\tilde{U}_{p^2-1}^+} \cong \frac{\mathbb{Z}^{\frac{p^2-p}{2}-1}}{(p\mathbb{Z})^{\frac{p^2-p}{2}-1}} = \mathbb{Z}_p^{\frac{p^2-p}{2}-1}$, because $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}_p$. The last factor in (a) thus becomes $p^{\frac{p^2-p}{2}-1}$.

Let us pay attention to $\frac{\tilde{U}_{p-1}^+}{\tilde{U}_{p+1}^+}$. We may write $\tilde{U}_{p-1}^+ = \{\epsilon \in E_1 | \epsilon = 1 + a_{p-1}(\zeta_1 - \zeta_1^{-1})^{p-1} + a_{p+1}(\zeta_1 - \zeta_1^{-1})^{p+1} + \dots\}$ and $\tilde{U}_{p+1}^+ = \{\epsilon \in E_1 | \epsilon = 1 + b_{p+1}(\zeta_1 - \zeta_1^{-1})^{p+1} + b_{p+3}(\zeta_1 - \zeta_1^{-1})^{p+3} + \dots\}$. Of course, $a_i, b_j \in \mathbb{Z}$. However, put $a_{p-1} = a'_{p-1} + pt$ with $t \in \mathbb{Z}$ so that $0 \leq a'_{p-1} \leq p-1$. Use $p = \epsilon_0 \cdot (\zeta_1 - \zeta_1^{-1})^{p^2-p}$, where $\epsilon_0 = c_0 + c_2(\zeta_1 - \zeta_1^{-1})^2 + \dots$ is a real unit in E_1 and $p \nmid c_0$. Then $\tilde{U}_{p-1}^+ = \{\epsilon \in E_1 | \epsilon = 1 + a'_{p-1}(\zeta_1 - \zeta_1^{-1})^{p-1} + a_{p+1} \cdot (\zeta_1 - \zeta_1^{-1})^{p+1} + \dots + \epsilon_0 t(\zeta_1 - \zeta_1^{-1})^{p^2-1} + \dots\}$. If $\epsilon' = 1 + a'_{p-1}(\zeta_1 - \zeta_1^{-1})^{p-1} + \dots$ is a unit in $\tilde{U}_{p-1}^+$ with $a'_{p-1} \neq 0$, one gets $(\epsilon')^k = 1 + ka'_{p-1}(\zeta_1 - \zeta_1^{-1})^{p-1} + \dots$, and the numbers ka'_{p-1} range over a complete residue system modulo p when k runs through the set $\{0, 1, \dots, p-1\}$ or the set $\{1, 2, \dots, p\}$. For $ka'_{p-1} \not\equiv 0 \bmod p$, we see that $(\epsilon')^k \in \tilde{U}_{p-1}^+$, but $(\epsilon')^k \notin \tilde{U}_p^+ = \tilde{U}_{p+1}^+$. Further, it is clear: $(\epsilon')^p \in \tilde{U}_{p(p-1)}^+ \subset \tilde{U}_{p+1}^+$. Thus the element (coset) $\epsilon'\tilde{U}_{p+1}^+$ generates the group $\frac{\tilde{U}_{p-1}^+}{\tilde{U}_{p+1}^+}$ of order p, i.e., $\left|\frac{\tilde{U}_{p-1}^+}{\tilde{U}_{p+1}^+}\right| = p$. It remains to be proved that a unit ϵ' with the above properties actually exists:

Set $\eta := \zeta_1^{\frac{p^2+1}{2}}$. Then $\eta^2 = \zeta_1^{p^2+1} = \zeta_1$ and $c(\eta) = \zeta_1^{-\frac{p^2+1}{2}} = \eta^{-1}$. Put $\rho := \frac{\eta^{p+1} - \eta^{-p-1}}{\eta - \eta^{-1}}$. This gives $c(\rho) = \rho$ and $\rho = \eta^{-p} \cdot \frac{\eta^{2p+2}-1}{\eta^2-1} = \eta^{-p} \cdot \frac{\zeta_1^{p+1}-1}{\zeta_1-1}$, so $\rho \in E_1^+$.

Write $\frac{\zeta_1^{p+1}-1}{\zeta_1-1} = \frac{\zeta_1^{p+1}-\zeta_1+\zeta_1-1}{\zeta_1-1} = \zeta_1 \cdot \frac{\zeta_1^p-1}{\zeta_1-1} + 1$. Also one has $(\zeta_1-1)^p = \zeta_1^p - 1 + pt_1$, some $t_1 \in \mathbb{Z}[\zeta_1]$, whence $\frac{\zeta_1^p-1}{\zeta_1-1} = (\zeta_1-1)^{p-1} + \frac{pt_1}{1-\zeta_1} = (\zeta_1-1)^{p-1} + (\zeta_1-1)^{p^2-p-1} \cdot t_2$, some $t_2 \in \mathbb{Z}[\zeta_1]$. Thus

$$\begin{aligned} \frac{\zeta_1^{p+1}-1}{\zeta_1-1} &= 1 + [1 - (1-\zeta_1)] \cdot [(\zeta_1-1)^{p-1} + \\ &+ (\zeta_1-1)^{p^2-p-1} \cdot t_2] = 1 + (\zeta_1-1)^{p-1} + (\zeta_1-1)^p + \\ &+ (\zeta_1-1)^{p^2-p-1} \cdot t_3;\ t_3 \in \mathbb{Z}[\zeta_1]. \end{aligned}$$

Similarly, $\zeta_1^p = (1-(1-\zeta_1))^p = 1-(1-\zeta_1)^p + p\cdot t_4$, so $\zeta_1^{-p} = 1+(1-\zeta_1)^p + (1-\zeta_1)^{p+1}\cdot t_5$; $t_4, t_5 \in \mathbb{Z}[\zeta_1]$. This yields $\eta^{-p} = (\zeta_1^{-p})^{\frac{p^2+1}{2}} = 1+\frac{p^2+1}{2}(1-\zeta_1)^p + (1-\zeta_1)^{p+1}\cdot t_6$; $t_6 \in \mathbb{Z}[\zeta_1]$.

Consequently,

$$\begin{aligned}
&\rho = \eta^{-p}\cdot\frac{\zeta_1^{p+1}-1}{\zeta_1-1} = \\
&= [1+\frac{p^2+1}{2}(1-\zeta_1)^p + (1-\zeta_1)^{p+1}\cdot t_6]\cdot[1+(1-\zeta_1)^{p-1}+(1-\zeta_1)^p\cdot t_7] = \\
&= 1+(1-\zeta_1)^{p-1}+(1-\zeta_1)^p\cdot t_8;\ t_7, t_8 \in \mathbb{Z}[\zeta_1].
\end{aligned}$$

Evidently, ρ is one of the assumed units ϵ', described before (with $a'_{p-1} = 1$). Note: $\rho \in \tilde{U}_{p-1}^+$, $\rho \notin \tilde{U}_p^+ = \tilde{U}_{p+1}^+$.

Finally, the first factor on the right-hand side of (a) must be determined. Define $\tilde{W}_m := \tilde{W}_m(\mathbb{Z}[\zeta_0]) := \{\epsilon \in U(\mathbb{Z}[\zeta_0]) | \epsilon \equiv 1 \bmod (1-\zeta_0)^m\}$, $m = 1, 2, \ldots$. Let $\tilde{W}_m^+$ be the subgroup of real units in $\tilde{W}_m$, $m = 1, 2, \ldots$.

Let $k \in \mathbb{Z}, (k,p) = 1$. $\mathbb{Q}(\zeta_1)$ is the splitting field over $\mathbb{Q}(\zeta_0)$ for $x^p - \zeta_0^k$ which is irreducible in $\mathbb{Q}(\zeta_0)$. So $\mathbb{Q}(\zeta_1)$ is a normal extension of degree p over $\mathbb{Q}(\zeta_0)$ ([A], pp. 59-61).

Since $\zeta_1^p = \zeta_0$, ζ_1 and all its conjugates satisfy $x^p - \zeta_0 = 0$. Therefore $N_1(\zeta_1) = (-1)^p$ times the constant term $= (-1)^p\cdot(-\zeta_0) = \zeta_0$ ([B-S], pp. 401, 404; [I-R], pp. 173, 186). Now $(k,p) = 1$; ζ_1^k satisfies $x^p - \zeta_0^k = 0$. Put $1-\zeta_1^k = y$ and we have $(1-y)^p - \zeta_0^k = 0$ or $(y-1)^p + \zeta_0^k = 0$; note irreducibility in $y-1$ and y. Hence $N_1(1-\zeta_1^k) = (-1)^p\cdot(\zeta_0^k - 1) = 1-\zeta_0^k$.

If π is the natural surjection, we now see that

$$\tilde{U}_1^+ \xrightarrow{N_1} \tilde{W}_1^+ \xrightarrow{\pi} \frac{\tilde{W}_1^+}{\tilde{W}_{p-1}^+} \tag{t}$$

is a well-defined transformation (Im $N_1 \subset \tilde{W}_1^+$).

Let us first show that the mapping N_1 in (t) is surjective. Here N_1 works as a group homomorphism. Define $\omega_0 := -\zeta_0^{(p+1)/2}$, $\omega_1 := -\zeta_1^{(p+1)/2}$. Then $\omega_0^2 = \zeta_0^{p+1} = \zeta_0$ and $N_1(\omega_1) = \omega_0$ ($N_1(-1) = (-1)^p = -1$). Writing $\omega_0 = -e^{\frac{2\pi i}{p}\cdot\frac{p+1}{2}} = -e^{\pi i}\cdot e^{\frac{\pi i}{p}} = e^{\frac{\pi i}{p}}$, one has $\dfrac{\omega_0^k - \omega_0^{-k}}{\omega_0 - \omega_0^{-1}} = \dfrac{e^{k\pi i/p} - e^{-k\pi i/p}}{e^{\pi i/p} - e^{-\pi i/p}} = \dfrac{\sin(k\pi/p)}{\sin(\pi/p)}$, $k \in \mathbb{Z}$. Set

$$J := \{\text{all positive real units in } \mathbb{Z}[\zeta_0]\}$$

and $J_0 :=$ group generated by the units $\dfrac{\sin(k\pi/p)}{\sin(\pi/p)}$, $k \in \{1, 2, \ldots, \dfrac{p-1}{2}\}$. Of course, J is a subgroup of $E_0 = U(\mathbb{Z}[\zeta_0])$. The trigonometric quotients clearly are real and positive for the marked k:s. That they indeed are units can be seen from above, since $\dfrac{\omega_0^k - \omega_0^{-k}}{\omega_0 - \omega_0^{-1}} = \omega_0^{-k+1}\cdot\dfrac{\zeta_0^k - 1}{\zeta_0 - 1}$ and $(k,p) = 1$ for $k \in \{1, 2, \ldots, \frac{p-1}{2}\}$.

So J_0 is a subgroup of J ([B-S], pp. 360 and 362). Raising these units to $(p-1)$-th power will give — as we have seen — principal ones, i.e., units in $\tilde{W}_1^+$. An analogous construction with ζ_0 exchanged for ζ_1 produces real principal units in $\mathbb{Z}[\zeta_1]$, that is elements in $\tilde{U}_1^+$. The connection between the two kinds of units is naturally

$$\begin{aligned}
&N_1\left(\left(\frac{\omega_1^k-\omega_1^{-k}}{\omega_1-\omega_1^{-1}}\right)^{p-1}\right) = \\
&= N_1\left(\left(\omega_1^{-k+1}\cdot\frac{\zeta_1^{(p+1)\cdot k}-1}{\zeta_1^{p+1}-1}\right)^{p-1}\right) = \\
&= \left(N_1(\omega_1^{-k+1})\cdot\frac{N_1(\zeta_1^{(p+1)\cdot k}-1)}{N_1(\zeta_1^{p+1}-1)}\right)^{p-1} = \\
&= \left(\omega_0^{-k+1}\cdot\frac{\zeta_0^{(p+1)\cdot k}-1}{\zeta_0^{p+1}-1}\right)^{p-1} = \\
&= \left(\frac{\sin(k\pi/p)}{\sin(\pi/p)}\right)^{p-1},\ k\in\{1,2,\dots,\frac{p-1}{2}\}.
\end{aligned}$$

The generators of $(J_0)^{p-1}$ thus are elements in Im N_1, which clearly is a group. This results in $(J_0)^{p-1}\subset$ Im N_1.

Recall the class number $h := \#Cl(\mathbb{Z}[\zeta_0])$ for the ideal class group of $\mathbb{Z}[\zeta_0]$ (Section 1.3). Now $h = h(p)$ can be written $h = h_0\cdot h^*$, where h_0 and h^* are natural numbers. As usual h_0 stands for the class number of the subfield $\mathbb{Q}(\zeta_0+\zeta_0^{-1})$, which is of degree $(p-1)/2$ over $\mathbb{Q}$ ([B-S], pp. 358-359). Theorem 2, p. 362 in [B-S] tells us that $h_0 = |\frac{J}{J_0}|$.

Let $z\in\tilde{W}_1^+$ be arbitrary. Since z is real, $z^2\in J$. In this proof we assume p to be regular, i.e., $p\nmid h$. Then it follows $(|\frac{J}{J_0}|, p) = 1$. Hence there is $s\in\mathbb{Z}, (s,p)=1 : (z^2)^s = z^{2s}\in J_0$. So $z^{2s(p-1)}\in(J_0)^{p-1}\subset$ Im N_1. But $z\in\mathbb{Q}(\zeta_0)$ gives $N_1(z) = z^p$, that is, $z^p\in$ Im N_1. For the latter exponents of z one can find $u,v\in\mathbb{Z} : 2s(p-1)\cdot u+p\cdot v = 1$, because $(2s(p-1),p)=1$. This implies $z = z^1 = z^{2s(p-1)\cdot u+p\cdot v} = (z^{2s(p-1)})^u\cdot(z^p)^v\in$ Im N_1. Here is used that Im N_1 is a group. The surjectivity of N_1 in (t) is proved.

However, much more information can be extracted from the chain (t). That $\pi\circ N_1$ is surjective is immediate. The kernel of this group homomorphism interests us. An element in $\frac{\tilde{W}_1^+}{\tilde{W}_{p-1}^+}$ may be written as

$$(1+b_1(1-\zeta_0)+b_2(1-\zeta_0)^2+\dots)\tilde{W}_{p-1}^+,\ b_i\in\mathbb{Z}.$$

This equals the unit element $(=\tilde{W}_{p-1}^+)$ iff $p|b_i$ for $1\le i\le p-2$, by the definition of $\tilde{W}_{p-1}^+$. Again remember that $(p) = ((1-\zeta_0)^{p-1})$ in $\mathbb{Z}[\zeta_0]$. If ϵ is a unit in $\tilde{U}_1^+$, it is enough to calculate $N_1(\epsilon)$ in $\tilde{W}_1^+$ up to mod p. Then N_1 is also — as known — additive.

Now take $\epsilon \in \tilde{U}^+_{p-1} \subset \tilde{U}^+_1$, i.e., $\epsilon = 1 + a_{p-1}(1-\zeta_1)^{p-1} + a_p(1-\zeta_1)^p + \dots$, a finite sum; $a_i \in \mathbb{Z}$. Thus

$$\begin{aligned} N_1(\epsilon) &\equiv N_1(1) + a^p_{p-1}(N_1(1-\zeta_1))^{p-1} + \dots \equiv \\ &\equiv 1 + a_{p-1}(1-\zeta_0)^{p-1} + a_p(1-\zeta_0)^p + \dots \equiv \\ &\equiv 1 \bmod p. \end{aligned}$$

Of course, 1 by π is mapped on $\tilde{W}^+_{p-1}$, the unit element of $\frac{\tilde{W}^+_1}{\tilde{W}^+_{p-1}}$, so $\tilde{U}^+_{p-1} \subset$ Ker $(\pi \circ N_1)$.

Let instead $\epsilon_0 \in \tilde{U}^+_1 \setminus \tilde{U}^+_{p-1} : \epsilon_0 = 1 + a_n(1-\zeta_1)^n + \dots ; n \in \{2, \dots, p-2\}$, $p > 3$, $p \nmid a_n \in \mathbb{Z}$. Hence $N_1(\epsilon_0) \equiv (1 + a_n(1-\zeta_0)^n + \dots) \bmod p$, but the right side of this congruence is not mapped by π on the unit element of $\frac{\tilde{W}^+_1}{\tilde{W}^+_{p-1}} \cdot$ Ker $(\pi \circ N_1) = \tilde{U}^+_{p-1}$ now follows. (If $p = 3$, $U^+_1 = U^+_{p-1}$.)

The surjection $\pi \circ N_1$ in (t) in this way yields

$$\frac{\tilde{U}^+_1}{\tilde{U}^+_{p-1}} \cong \frac{\tilde{W}^+_1}{\tilde{W}^+_{p-1}} \tag{j}$$

Take $\kappa \in \tilde{W}^+_{p-1}$, i.e., $\kappa \equiv 1 \bmod (1-\zeta_0)^{p-1}$ or $\kappa \equiv 1 \bmod p$. Since p is regular, Theorem 3, p. 377 in [B-S] (Kummer) implies: $\kappa = \delta^p$; δ a real unit in $\mathbb{Z}[\zeta_0]$ (see the proof). If $\delta = a_0 + a_1(1-\zeta_0) + \dots$, $a_i \in \mathbb{Z}$, one has $1 \equiv \kappa = \delta^p \equiv a_0^p \equiv a_0 \bmod p$, that is, $\delta \equiv 1 \bmod (1-\zeta_0)$ or $\delta \in \tilde{W}^+_1$. Thus $\kappa = \delta^p \in (\tilde{W}^+_1)^p$; $\tilde{W}^+_{p-1} \subset (\tilde{W}^+_1)^p$. The opposite inclusion is almost trivial and we conclude: $\tilde{W}^+_{p-1} = (\tilde{W}^+_1)^p$.

We know that $E_0 \cong \mathbb{Z}_p \oplus \mathbb{Z}^{\frac{p-3}{2}}$. The group of real units, $\tilde{W}^+_1$, becomes $\tilde{W}^+_1 \cong \mathbb{Z}^{\frac{p-3}{2}}$. From the isomorphism (j) one finally gets

$$\begin{aligned} \left|\frac{\tilde{U}^+_1}{\tilde{U}^+_{p-1}}\right| &= \left|\frac{\tilde{W}^+_1}{\tilde{W}^+_{p-1}}\right| = \left|\frac{\tilde{W}^+_1}{(\tilde{W}_1)^p}\right| = \\ &= \left|\frac{\mathbb{Z}^{\frac{p-3}{2}}}{(p\mathbb{Z})^{(p-3)/2}}\right| = \left|(\mathbb{Z}_p)^{(p-3)/2}\right| = p^{(p-3)/2}. \end{aligned}$$

Equation (a) and $\frac{\tilde{U}^+_1}{\tilde{U}^+_{p^2-1}} \cong g_2(\tilde{U}^+_1)$ now gives

$$|g_2(\tilde{U}^+_1)| = p^{\frac{p-3}{2}} \cdot p \cdot p^{\frac{p^2-p}{2}-1} = p^{\frac{p^2-3}{2}}.$$

But $g_2(\tilde{U}^+_1) \subset \tilde{U}(D_2)^+$ and $|\tilde{U}(D_2)^+| = p^{(p^2-3)/2}$. Theorem 3.1 is completely proved. □

As a consequence of Theorem 3.1 we get the following exact sequence, originally obtained in [K-M]:

Corollary 3.3. *The sequence*

$$0 \to (\mathbb{Z}_p)^{(p^2-2p+1)/2} \oplus (\mathbb{Z}_{p^2})^{(p-3)/2} \to Pic\ (\mathbb{Z}C_{p^3}) \to Cl(\mathbb{Z}[\zeta_2]) \oplus Pic\ (\mathbb{Z}C_{p^2}) \to 0$$

is exact.

§4 References

[A] Artin, E., Galois Theory, Notre Dame, Indiana, 1959.

[A-H] Atiyah, M.F and Hirzebruch, F., Vector Bundles and Homgeneous Spaces, Proc. of Symp in Pure Math., Amer. Math. Soc. 3 (1961)

[A-M] Atiyah, M. F. and MacDonald, I. G., Introduction to Commutative Algebra, Addison-Wesley Publ. Comp., London, 1969.

[A-T] Artin, E. and Tate, J., Class Field Theory, Benjamin, New York, 1968.

[B] Bass, H., Algebraic K-theory, Benjamin, New York, 1968.

[B1] Bass, H., K-theory and Stable Algebra, Publ. Math, IHES 22, (1964)

[B-S] Borevich, Z. I. and Shafarevich, I. R., Number Theory, Academic Press, New York and London, 1966.

[BSG] Borel, A. et Serre, J.-P., Le theoreme de Riemann-Roch (d'apres Grothendieck), Bull. Soc. Math. France 86 (1958), 94-136.

[C-F] Cassels, J. W. S. and Fröhlich, A., Algebraic Number Theory, Academic Press, London and New York, 1967.

[C-R] Curtis, C. W. and Reiner, I., Methods of Representation Theory, Vol. I, II, Wiley, New York, 1981 and 1987.

[F] Fröhlich, A., On the classgroup of integral group rings of finite abelian groups, I, II: Mathematika 16 (1969), 143-152 resp. 19 (1972), 51-56.

[G1] Galovich, S., The Class Group of a Cyclic p-Group, Journal of Algebra 30 (1974), 368-387.

[G2] Galovich, S., Corrigendum (to [G1]), Journal of Algebra 47 (1977), 547-548.

[Ha] Hasse, H., Vorlesungen über Klassenkörpertheorie, Physica-Verlag, Würzburg 1967.

[He] Hecke, E., Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea, New York 1948, 1970.

[Hig] Higman, G., The units of group rings, Proc. London Math. Soc. 46 (1940), 231-248.

[Hil] Hilbert, D., Gesammelte Abhandlungen, Vol. I, Springer-Verlag, New York, 1970.

[I1] Iwasawa, K., A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257-258.

[I2] Iwasawa, K., On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959), 183-226.

[I3] Iwasawa, K., On the theory of cyclotomic fields, Ann. of Math. 70 (1959), 530-561.

[I-R] Ireland, K. and Rosen, M., A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, New York, 1990.

[J] Janusz, G. J., Algebraic Number Fields, 2nd ed., Vol. 7, Graduate Studies in Mathematics, American Math. Soc. 1996.

[K-M] Kervaire, M. A. and Murthy, M. P., On the projective class group of cyclic groups of prime power order, Comment. Math. Helvetici 52 (1977), 415-452.

[L] Lang, S., Algebraic number theory, Addison-Wesley, 2nd edition 1970.

[M] Milnor, J., Introduction to Algebraic K-theory, Annals of Math. Studies 72, Princeton Univ. Press 1971.

[O] Oliver, R., Class groups of cyclic p-groups, Mathematika 30 (1983), 26-57.

[R] Ribenboim, P., Algebraic Numbers, New York, Wiley, 1972.

[Se 1] Serre, J. P., Corps Locaux, Hermann, Paris, 1962.

[Se 2] Serre, J. P., A Course in Arithmetic, Springer-Verlag, 1993.

[St 1] Stolin, A., An explicit formula for the Picard group of the cyclic group of order p^2, Proc. Amer. Math., Soc., Vol. 121 (1994), 375-383.

[St 2] Stolin, A., On the Picard Group of the Integer Group Ring of the Cyclic p-Group and of Rings Close to It, Proc. of the 2nd Int. Conf. in Comm. Alg. 1997, 443-455.

[U1] Ullom, S., Fine Structure of Class Groups of Cyclic p-Groups, J. Algebra 49 (1977), 112-124.

[U2] Ullom, S., Class groups of cyclotomic fields and group rings, J. London Math. Soc. 17 (1978), 231-239.

[W] Whitehead, J.H.C.,Simplicial Spaces, Nuclei and m-groups. Proc. London Math. Soc. 45 (1939), 243-327.