Kummer's Lemma and Picard Groups of Integer Group Rings

Ola Helenius

September 10, 1999

THESIS FOR THE DEGREE OF LICENTIATE OF PHILOSOPHY

Kummer's Lemma and Picard Groups of Integer Group Rings

OLA HELENIUS

Department of Mathematics
CHALMERS UNIVERSITY OF TECHNOLOGY
AND GÖTEBORG UNIVERSITY
Göteborg, Sweden 1999

Kummer's Lemma and Picard Groups of Integer Group Rings
OLA HELENIUS
ISSN 0347-2809
Preprint 1999:39

Department of Mathematics
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg
Sweden
Telephone + 46(0)31-7721000

Matematiskt Centrum
Göteborg, Sweden 1999

Abstract

In this paper we prove two different generalizations of Kummer's Lemma that describes when a unit of a cyclotomic field is a p-th power of another unit. One of these results is then used to prove a theorem about the Picard group of the integer group ring $\mathbb{Z}C$, where C is a cyclic group of prime power order. The theorem was first proved by Kervaire and Murthy; we use a more elementary method to reprove it in the case where p is a regular prime.

Keywords: Picard groups, Kummer's lemma, cyclotomic units

AMS Subject classification: 11R65, 11R21, 19A31.

Acknowledgements

I would like to thank my advisor Alexander Stolin for his invaluable enthusiasm, guidance and support.

Contents

1 Introduction

Fermat's last theorem has undoubtedly been one of the greatest sources of inspiration for the development of number theory. One of the first breakthroughs in the search for a proof was made by Kummer in the mid eighteen-hundreds. Kummer proved the theorem in the case when the exponent, p, is a so called regular prime. This means that p does not divide the class number of the p-th cyclotomic field. One of the main steps in Kummer's proof is the following result.

Kummer's Lemma. *Let p be a regular prime and let ζ be a primitive p-th root of unity. If ϵ is a unit in $\mathbb{Z}[\zeta]$ such that ϵ is congruent to a rational integer modulo p, then ϵ is the p-th power of another unit.*

There are several ways to prove this. The proof in [B-S] relies on the fact that the p-adic integers with zero trace can be uniquely presented as a (finite) sum $\sum c_k \log \theta_k^{p-1}$, where the c_k are p-adic integers and θ_k are the so called cyclotomic units. As it is done in for example [W], one can also use class field theory to prove Kummer's Lemma. In this case one first use the p-adic logarithm and exponential functions to show the result in the λ-adic completion of $\mathbb{Z}[\zeta]$, where λ is the prime above p. Class field theory then implies that the result must also hold in $\mathbb{Z}[\zeta]$.

In chapter 2 we will generalize Kummer's Lemma in two directions. Let ζ_n be a primitive p^{n+1}-th root of unity. Theorem 2.3 says that if p is regular and $\epsilon \in \mathbb{Z}[\zeta_0]^*$ is congruent to 1 modulo p^n, then ϵ is a p^n-th power of another unit. The proof is similar to the first one of the proofs described above and the only extra ingredient is some calculations.

For our second generalization we consider prime power cyclotomic fields, $\mathbb{Q}(\zeta_n)$ and their rings of integers $\mathbb{Z}[\zeta_n]$. Let λ_n be the (unique) prime above (p) in $\mathbb{Z}[\zeta_n]$. Theorem 2.7 says that if p is a regular prime and $\epsilon \in \mathbb{Z}[\zeta_n]^*$ is congruent to 1 modulo $\lambda_n^{p^{n+1}-1}$, then ϵ is a p-th power of another unit. Note that this restricts to the usual version of Kummer's Lemma when n is zero. The proof of this generalization is similar to the second one of the proofs of Kummer's Lemma described above. The main extra ingredient is Lemma 2.15 that tells us that if a unit is congruent to 1 modulo $\lambda_n^{p^{n+1}-1}$, then it is also congruent to 1 modulo $\lambda_n^{p^{n+1}}$. This important Lemma was proved in [ST1] but for completeness we prove it here too.

The second part of this paper is devoted to algebraic K-theory. In 1958, in his work on the Riemann-Roch theorem, Grothendieck introduced the functor K, now known as K_0 ([BSG]). The best known application of this functor is the topological K-theory developed by Atiya and Hirzebruch in [A-H]. The next step was taken by Bass (see [B]) who defined K_1 functors in the category of rings. These functors turned out to be the same as the ones introduced by

Whitehead in [W] 1939. In 1969 Milnor showed how, starting from a Cartesian square (or pullback), one could construct an exact sequence involving K_0 and K_1 of the respective rings. This sequence is now called the Mayer-Vietoris sequence of algebraic K-theory after the Mayer-Vietoris exact sequence of algebraic topology to which it is similar in appearance.

One important problem in algebraic K-theory is simply to compute $K_0(R)$ for various rings R. Because of important topological applications, rings ZC, where C is a cyclic group, are of particular interest. In the article [K-M], Kervaire and Murthy took a step towards a solution of this problem in the case when C is a cyclic group of prime power order. When p is a so called semi regular prime (meaning that p does not divide the class group of the maximal real subfield of $\mathbb{Q}(\zeta_0)$), they explicitly gave an exact sequence involving the group $\tilde{K}_0(\mathbb{Z}C)$. $(K_0(\mathbb{Z}C) = \mathbb{Z} \oplus \tilde{K}_0(\mathbb{Z}C))$.

The aim of this paper is to reprove the result by Kervaire and Murthy in the case where p is regular, using a different method. Our proof relies on one of our generalizations of Kummer's Lemma and we thus link Kummer's work on Fermat's theorem with our K-theoretical problem.

Remark: In this paper we actually study the picard group, Pic R, of a ring R, but since $\tilde{K}_0(\mathbb{Z}C) \cong \operatorname{Pic} \mathbb{Z}C$ when C is a cyclic group of prime power order, this is equivalent to the study of $\tilde{K}_0(\mathbb{Z}C)$.

1.1 A Short Introduction to K_0, K_1 and Picard Groups

In this paper all rings will be commutative and have a identity element, usually denoted by 1. All ring homorphisms $f : A \to B$ are assumed to satisfy $f(1_A) = 1_B$. As usual, A^* denotes the multiplicative group of units of A.

An A-module P is called projective if there exists an A-module Q such that $P \oplus Q$ is free. A module M is called finitely generated if there exists a finite subset N of M such that $RN = M$.

It is easy to see that a module P is finitely generated and projective if and only if there exists a module Q such that $P \oplus Q \cong A^n := \bigoplus_{i=1}^n A$ for some natural number n

Let $\mathfrak{p}$ be a prime ideal of A and let $A_\mathfrak{p}$ denote the localization of A at $\mathfrak{p}$. If M is an A-module the localization $M_\mathfrak{p}$ of M at $\mathfrak{p}$ is isomorphic to $A_\mathfrak{p} \otimes_A M$. Suppose M is finitely generated and projective. Then, since $A_\mathfrak{p}$ is a local ring, $M_\mathfrak{p}$ is a free, finitely generated $A_\mathfrak{p}$-module and hence $M_\mathfrak{p} \cong A_\mathfrak{p}^n$ for some n. We can hence define $\operatorname{rank}_\mathfrak{p}(M) = n$.

An A-module M is called invertible if it satisfies any of the following equivalent conditions:

i) M is projective and finitely generated of constant rank 1.

ii) $M^* \otimes_A M \cong A$, where $M^* := \mathrm{Hom}_A(M, A)$.

iii) There exists an A-module N with $N \otimes_A M \cong A$.

We will now define the Picard group, $\mathrm{Pic}\, A$ of the ring A. If P is an invertible A-module, let $< P >$ denote the isomorphism class of P. If Q is another invertible module, define an operation by

$$< P >< Q > := < P \otimes_A Q > .$$

This set of isomorphism classes of invertible modules together with the operation defined above forms the group $\mathrm{Pic}\, A$. The identity element is the class of A, considered as a module over itself, and the inverse of an element $< P >$ is $< P^* >$.

Let A_1, A_2 and D be commutative rings with unity and let $j_k : A_k \mapsto D$, $k = 1, 2$ be homomorphisms. A ring A and maps $i_k : A \mapsto A_k$, $k = 1, 2$, is called a pullback (of A_1 and A_2 over D) if the following condition holds. For all rings B and maps $\alpha_k : B \mapsto A_k$, $k = 1, 2$ such that the outer part of the diagram below commutes, there is a unique θ such that the whole diagram commutes.

$$\begin{tikzcd}
B \arrow[drr, "\alpha_1"] \arrow[ddr, "\alpha_2"'] \arrow[dr, dotted, "\theta"] & & \\
& A \arrow[r, "i_1"] \arrow[d, "i_2"'] & A_1 \arrow[d, "j_1"] \\
& A_2 \arrow[r, "j_2"] & D
\end{tikzcd}$$

If A is a pullback of A_1 and A_2 over D we will call the rectangular part of the diagram above a pullback diagram. It is easy to see that a pullback is unique up to isomorphism. One can show that

$$A = \{(a_1, a_2) \in A_1 \times A_2 \, : \, j_1(a_1) = j_2(a_2)\}$$

is a pullback of A_1 and A_2 over D. Often we will identify any pullback with A defined above. The following result is well known and easy to prove.

Lemma 1.1. *If A is a commutative ring with unity and α and β ideals in A, then*

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

is a pullback diagram.

Following Milnor, we now indicate how starting from a pullback diagram

$$\begin{tikzcd} A \arrow[r, "i_1"] \arrow[d, "i_2"'] & A_1 \arrow[d, "j_1"] \\ A_2 \arrow[r, "j_2"] & D \end{tikzcd} \tag{1.1}$$

and projective (finitely generated) modules P_1 and P_2 over A_1 and A_2 respectively, one can extract projective (finitely generated) modules over D and A and get a commutative square of additive groups where each group has a module structure over the corresponding ring in the pullback diagram. We will need to make the extra assumption that j_1 or j_2 is surjective. For a full treatment of the matters below we refer to [M].

First consider a ring homomorphism $f : A \to A'$. If M is a projective (finitely generated) A-module, then we can define a projective (finitely generated) A'-module $f_\# M := A' \otimes_A M$. We can also define a A-linear map $f_* : M \to f_\# M$ by $f_*(m) = 1 \otimes m$. Now return to the pullback diagram above and suppose that there exists a D-module isomorphism $h : j_{1\#}P_1 \to j_{2\#}P_2$. Define

$$M = M(P_1, P_2, h) := \{(p_1, p_2) \in P_1 \times P_2 \ : \ hj_1(p_1) = j_2(p_2)\}.$$

We get a A-module structure on M by setting

$$a(p_1, p_2) = (i_1(a)p_1, i_2(a)p_2).$$

The following results are Theorem 2.1, 2.2 and 2.3 of [M].

Proposition 1.2. *Let M be the module constructed above. Then,*

i) M is projective over A and if P_1 and P_2 are finitely generated over A_1 and A_2 respectively, then M is finitely generated over A.

ii) Every projective A-module is isomorphic to $M(P_1, P_2, h)$ for some suitably chosen P_1, P_2 and h.

iii) The modules P_1 and P_2 are naturally isomorphic to $i_{1\#}M$ and $i_{2\#}M$ respectively.

This gives us a commutative diagram of additive groups

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

The definition of pullbacks for abelian groups is similar to the one for rings. It is easy to see that our in commutative square M is actually a pullback of P_1 and P_2 over $j_{2\#}P_2$.

In this paper we are not concerned with the groups K_0 and K_1 but we will still devote this section to a short description of them as they are closely related to the Picard group.

Let A be a ring. The group K_0A can be seen as the group of (differences of isomorphism classes of) projective finitely generated A-modules. Formally, if P and Q are such modules we let brackets denote the isomorphism class and define an operation by

$$[P] + [Q] := [P \oplus Q].$$

The set of all isomorphism classes with this operation is a monoid. The group K_0A is defined as the quotient of the free abelian group generated by this monoid modulo the subgroup generated by all expressions $[P] + [Q] - [P \oplus Q]$. It is easy to see that every element of K_0A can be represented as [P]-[Q] for some suitably choosen P and Q.

The group K_1A can be seen as a group of infinite matrices. Let $\mathrm{GL}(n, A)$ be the group of $n \times n$ invertible matrices. For each $n = 1, 2, \ldots,$ consider the embedding of $\mathrm{GL}(n, A)$ into $\mathrm{GL}(n + 1, A)$ defined by

$$H \mapsto \begin{pmatrix} H & 0 \\ 0 & 1 \end{pmatrix}$$

for $H \in \mathrm{GL}(n, A)$. Define the group $GL(A)$ as the union of the sequence

$$\mathrm{GL}(1, A) \subset \mathrm{GL}(2, A) \subset \mathrm{GL}(3, A) \subset \cdots .$$

A matrix in $GL(A)$ is called elementary if it coincides with the identity matrix except for a single off-diagonal entry. It can be shown that the multiplicative group $E(A)$ generated by the elementary matrices coincides with the commutator subgroup of $GL(A)$. We define the group K_1A as the quotient $GL(A)/E(A)$. If $f : A \to A'$ is a ring homomorphism we can in the obvious way define a group homomorphism $f_* : K_1A \to K_1A'$.

For more facts about these groups and proofs of the statements above, see [M] and [Si].

We are now ready to present the (K_1, K_0)-Mayer-Vietoris Sequence, originally obtained by Milnor. The reason why the sequence below bears the name Mayer-Vietoris is the resemblance with the Mayer-Vietoris long exact sequence of algebraic topology (see [R] p. 177).

Proposition 1.3. *Consider the pullback diagram of rings (1.1) with j_1 or j_2 surjective. There is an exact sequence of additive groups*

$$K_1A \overset{\alpha_1}{\to} K_1A_1 \oplus K_1A_2 \overset{\beta_1}{\to} K_1D \overset{\partial}{\to} K_0A \overset{\alpha_0}{\to} K_0A_1 \oplus K_0A_2 \overset{\beta_0}{\to} K_0D.$$

Consider the groups as additive. The homomorphisms α_i and β_i, $i = 0, 1$, are defined by

$$\begin{aligned}\alpha_1(a_1) &= (i_{1*}(a_1), i_{2*}(a_1))\\ \beta_1(b_1, c_1) &= j_{1*}(b_1) - j_{2*}(c_1)\\ \alpha_0(a_0) &= (i_{1*}(a_0), i_{2*}(a_0))\\ \beta_0(b_0, c_0) &= j_{1*}(b_0) - j_{2*}(c_0)\end{aligned}$$

for $a_i \in K_iA$, $b_i \in K_iA_1$ and $c_i \in K_iA_2$. To define ∂ we first observe that an element d of K_1D can be represented by a matrix in $\mathrm{GL}(n, D)$ for some n. This matrix determines an isomorphism h_d from the free D-module $j_{1\#}A_1^n$ to the free D-module $j_{2\#}A_2^n$. Let $M = M(A_1^n, A_2^n, h_d)$ and define

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

The verification that ∂ is a well defined homomorphism and that the sequence is exact is routine. We will now indicate how one can obtain from the (K_0, K_1)-Mayer-Vietoris sequence a similar sequence involving unit groups and Picard groups.

Proposition 1.4. *Let A be a ring. There exist surjective maps* $\det_0 : K_0A \to \operatorname{Pic} A$ *and* $\det_1 : K_1A \to A^*$

The proof of this can be found in [Si] p. 57 and p. 112. The map $\det_0$ is defined using exterior (or alternating) product $\bigwedge_A^n$ (see [L] p 731). If M is a projective finitely generated A-module of constant rank m, then $\bigwedge_A^n M$ is a projective finitely generated A-module of constant rank $\binom{m}{n}$. One can show that there exists subrings H and RK_0A of K_0A such that $K_0A \cong H \oplus RK_0A$, where every module in RK_0A can be presented as $[M] - [A^n]$ for some M and n. The map $\det_0$ is defined as the composition of the surjection $K_0A \to RK_0A$ with the map

$$RK_0A \to \operatorname{Pic} A \qquad [M] - [A^n] \mapsto \textstyle\bigwedge_A^m M,$$

where $m = \text{rank } M$.

With our definition of K_1A we can define $\det_1 : K_1A \to A^*$ as the map induced by the usual determinant $GL(A) \to A^*$. This is well defined since any elementary matrix has trivial determinant.

Proposition 1.5. *Consider the pullback diagram of rings (1.1) with j_1 or j_2 surjective. The diagram*

$$\begin{tikzcd}
K_1A \arrow[r, "\alpha_1"] \arrow[d, "\det_1"] & K_1A_1 \oplus K_1A_2 \arrow[r, "\beta_1"] \arrow[d, "\det_1 \oplus \det_1"] & K_1D \arrow[r, "\partial"] \arrow[d, "\det_1"] & {} \\
A^* \arrow[r, "\alpha_1"'] & A_1^* \oplus A_2^* \arrow[r, "\beta_1"'] & D^* \arrow[r, "\partial"'] & {}
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[r, "\partial"] & K_0A \arrow[r, "\alpha_0"] \arrow[d, "\det_0"] & K_0A_1 \oplus K_0A_2 \arrow[r, "\beta_0"] \arrow[d, "\det_0 \oplus \det_0"] & K_0D \arrow[d, "\det_0"'] \\
{} \arrow[r, "\partial"'] & \operatorname{Pic} A \arrow[r, "\alpha_0"'] & \operatorname{Pic} A_1 \oplus \operatorname{Pic} A_2 \arrow[r, "\beta_0"'] & \operatorname{Pic} D
\end{tikzcd}$$

is commutative and the rows are exact.

The bottom row is called the $(*, \operatorname{Pic})$-Mayer-Vietoris exact sequence corresponding to the pullback diagram 1.1. The maps in the this sequence are defined as follows:

$$\begin{aligned}
\alpha_1(a) &= (i_1(a), i_2(a)) \\
\beta_1(a_1, a_2) &= j_1(a_1)j_2(a_2)^{-1} \\
\alpha_0(P) &= (i_{1*}(P), i_{2*}(P)) \\
\beta_0(P_1, P_2) &= j_{1*}(P_1)j_{2*}(P_2)^{-1}
\end{aligned}$$

for $a \in A^*$, $a_i \in A_i^*$, $P \in \operatorname{Pic} A$ and $P_i \in \operatorname{Pic} A_i$. To define ∂ we first observe that an element d of $D*$ can be thought of as an isomorphism between $j_{1\#}A_1 \cong D$ and $j_{2\#}A_2 \cong D$. Let $\partial(d) := M(A_1, A_2, h)$. The proof of the proposition can be found in [Si].

2 Some generalizations of Kummer's Lemma

Kummer's Lemma is one of the fundamental parts of Kummer's proof of Fermat's theorem for regular primes. In this section we will genarilize Kummer's result in two different directions. We start by stating the original result.

Kummer's Lemma. *Let p be a regular prime and let ζ be a primitive p-th root of unity. If ϵ is a unit in $\mathbb{Z}[\zeta]$ such that ϵ is congruent to a rational integer modulo p, then ϵ is a p-th power of another unit.*

The first of our generalizations is Theorem 2.3 where we exploit Kummer's result a little further, staying in the field $\mathbb{Q}(\zeta)$. The second of one is Theorem 2.7. Here we find a result in the prime power case, that is when ζ is a primitive p^n-th root of unity, comparable to the original result.

We start by stating some preliminary, well known facts about prime power cyclotomic fields. Fix a prime number p. For $n = 0, 1, 2...$, let ζ_n be a primitive p^{n+1}-th root of unity and consider the field $\mathbb{Q}(\zeta_n)$. Let $\lambda_n = \zeta_n - 1$ in $\mathbb{Q}(\zeta_n)$. By abuse of notation we will also denote the ideal $(\zeta_n - 1)$ in $\mathbb{Z}[\zeta_n]$ by λ_n. The following well known facts can be found in for example [J].

Lemma 2.1. *The following statements hold:*

i) *$\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ is a Galois extension of degree $p^n(p-1)$.*

ii) *When $p^{n+1} > 2$, no embeddings of $\mathbb{Q}(\zeta_n)$ into $\mathbb{C}$ are real.*

iii) *$\mathbb{Z}[\zeta_n]$ is the ring of integers in $\mathbb{Q}(\zeta_n)$, and the ideal λ_n is a prime ideal in $\mathbb{Z}[\zeta_n]$.*

iv) *If $p^{n+1} > 2$, then (p) is the only prime ideal in $\mathbb{Z}$ that ramifies in $\mathbb{Q}(\zeta_n)$.*

v) *$\lambda_n \cap \mathbb{Z} = (p)$ and the ramification index $e(\lambda_n/(p))$ is $p^n(p-1)$.*

vi) *$\lambda_n = (\zeta_n - \zeta_n^{-1})$ as ideals in $\mathbb{Z}[\zeta_n]$.*

vii) *The maximal real subfield of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and the ring of integers in $\mathbb{Q}(\zeta_n)^+$ is $\mathbb{Z}[\zeta_n]^+ = \mathbb{Z}(\zeta_n + \zeta_n^{-1})$.*

The following lemma is also sometimes called "Kummer's lemma". In this paper we will for obvious reasons refrain from doing this.

Lemma 2.2. *For every unit ϵ in $\mathbb{Z}[\zeta_n]^*$ there is a natural number k and a unit $\epsilon_r \in (\mathbb{Z}[\zeta_n]^+)^*$ such that $\epsilon = \epsilon_r \zeta^k$.*

The proof can be found in for example [W] p. 3.

2.1 The p-adic logarithm and a generalization in $\mathbb{Q}(\zeta_0)$

Here we will prove the following theorem.

Theorem 2.3. *Let p be a regular prime. Let $\epsilon \in \mathbb{Z}(\zeta_0)$ be a unit. Then, if $\epsilon \equiv 1$ mod p^n, there exists a unit γ such that $\epsilon = \gamma^{p^n}$.*

The proof, which can be found at the end of this section, uses induction, starting with the regular version of Kummer's Lemma. The induction step itself is similar to one of the proofs of Kummer's Lemma where one uses the fact that one can find a certain basis for λ_0-adic real integer with zero trace. The main extra ingredient we need is lemma 2.5, about the the p-adic logarithm function.

Suppose p is an odd prime. Let $n = 0$, $\lambda = \lambda_0 = \zeta_0 - 1$, $\zeta = \zeta_0$, and $\lambda_r = \zeta - \zeta^{-1} = \zeta - \bar{\zeta}$. Recall that (λ) is a prime ideal and that $(p) = (\lambda)^{p-1}$. Moreover, $\lambda_r = \zeta^{-1}(\zeta^2 - 1) = \zeta^{-1}(\zeta + 1)(\zeta - 1)$ and since ζ and $\zeta + 1 = \frac{1-\zeta^2}{1-\zeta}$

are units, $(\lambda) = (\lambda_r)$ as ideals (Lemma 2.1 *vi*)). We let v_λ denote the valuation on $\mathbb{Q}(\zeta_0)$ with respect to the prime ideal λ.

The set $\{1, \lambda_r, ..., \lambda_r^{p-2}\}$ forms an integral basis for $\mathbb{Q}(\zeta_0)$ over $\mathbb{Q}$ and $\bar{\lambda}_r = -\lambda_r$. Hence if $a \in \mathbb{Z}[\zeta]$ is real there exists $a_i \in \mathbb{Z}$, $i = 0, 1, .., p-2$ such that $a = a_0 + a_1\lambda_r + ... + a_{p-2}\lambda_r^{p-2}$ and $0 = a - \bar{a} = 2a_1\lambda_r + 2a_3\lambda_r^3 + ... + 2a_{p-2}\lambda_r^{p-2}$. Hence $a_i = 0$ for odd i and $a = a_0 + a_2\lambda_r^2 + ... + a_{p-3}\lambda_r^{p-3}$. It easily follows that $v_\lambda(a)$ is a multiple of 2 and that a is congruent to a rational integer $\mod \lambda_r^2$.

Let $\mathbb{Q}(\zeta)_\lambda$ be the λ-adic completion of the field $\mathbb{Q}(\zeta)$. The logarithm function is defined by

$$\log(1+x) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k}$$

for all x such that the series converges (in the norm induced by the λ-adic valuation). The following facts can be found for example in [B-S] p. 376, p. 370 and p. 362.

Lemma 2.4. *Let E be the group of positive real units of $\mathbb{Z}(\zeta)$ and let E_0 be the subgroup generated by the units $\theta_k = \frac{\sin k\pi/p}{\sin \pi/p}$ for $k = 2, 3, ..., \frac{p-1}{2}$. Then,*

1. *If p is a regular prime the real λ-adic integers with zero trace are uniquely represented as*

$$\sum_{k=2}^{m} a_k \log \theta_k^{p-1}$$

where the a_k are p-adic integers.

2. *If ϵ is a unit such that $\epsilon \equiv 1 \mod \lambda$, then $\log \epsilon$ has zero trace.*
3. *The index $[E : E_0]$ is finite*

Lemma 2.5. *Let $\gamma \in \mathbb{Q}(\zeta_0)$ and suppose $v_\lambda(\gamma - 1) \geq 2$. Then $\log \gamma \equiv \frac{\gamma^{p^n} - 1}{p^n}$ mod p^n for all positive integers n.*

Proof. Let $x = 1 - \gamma$. By definition,

$$\log \gamma = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k} := L_n(\gamma) + \sum_{p^n+1}^{\infty} (-1)^{k+1} \frac{x^k}{k}.$$

For $k \geq p^n + 1$, write $k = p^a k'$ where (p, k')=1. Then $p^a \leq k$ so $v_\lambda(k) \leq e(\lambda/p) \frac{\log k}{\log p} = (p-1) \frac{\log k}{\log p}$. Hence

$$\begin{aligned} v_\lambda(\frac{x^k}{k}) &\geq 2k - (p-1)\frac{\log k}{\log p} \geq \\ &\geq p^n + (k - p^n) + \frac{(p^n-1)k}{\log p^n}(\frac{\log p}{p^n - 1} - \frac{\log k}{k-1}) \geq p^n \geq (p-1)n. \end{aligned}$$

This implies that $\log \gamma \equiv L_n(\gamma) \bmod p^n$.

Now,

$$\begin{aligned} L_n(\gamma) - \frac{\gamma^{p^n}-1}{p^n} &= \sum_{k=1}^{p^n} (-1)^{k+1}\frac{x^k}{k} - \frac{(1-x)^{p^n}-1}{p^n} = \\ &= A_2\frac{x^2}{k!} + A_3\frac{x^3}{k!} + \ldots + A_{p^n}\frac{x^{p^n}}{k!}, \end{aligned}$$

where

$$\begin{aligned} A_k &= (-1)^{k-1}(k-1)! - (p^n-1)(p^n-2)\cdots(p^n-(k-1)) = \\ &= p^n m_k \end{aligned}$$

for some $m_k \in \mathbb{Z}$. Hence $p^n | A^k$ so $v_\lambda(A_k) \geq n(p-1)$. Since $v_\lambda(\frac{x^k}{k!}) \geq 0$ if $v_\lambda(x) \geq 1$ ([B-S] p 285), we get that

$$\begin{aligned} v_\lambda\Big(L_n(\gamma) - \frac{\gamma^{p^n}-1}{p^n}\Big) &\geq \min_{2\leq k \leq p^n} v_\lambda(A_k\frac{x^k}{k!}) = \\ &= \min_{2\leq k\leq p^n}\Big(v_\lambda(A_k) + v_\lambda(\frac{x^k}{k!})\Big) \geq n(p-1). \end{aligned}$$

This implies that $L_n(\gamma) - \frac{\gamma^{p^n}-1}{p^n} \equiv 0 \bmod p^n$ which proves the lemma. □

The following corollary can be seen as a p-adic version of the well known real identity $\lim_{x\to 0}\frac{a^x-1}{x} = \ln a$.

Corollary 2.6. $\lim_{n\to\infty}\frac{\gamma^{p^n}-1}{p^n} = \log\gamma$.

Proof of Theorem 2.3. We will use induction on n. The case $n=1$ is the standard version of Kummer's lemma and a proof can be found in [B-S] p. 377. Suppose the statement holds for $n-1$. Then there is a unit ϵ_1 such that $\epsilon = \epsilon_1^{p^{n-1}}$. By assumption, $\frac{\epsilon_1^{p^{n-1}}-1}{p^{n-1}} \equiv 0 \bmod p$. We can assume that ϵ_1 is real since if $\epsilon_1 = \zeta_0^k\epsilon_r$ for some real unit ϵ_r, then

$$\epsilon = \epsilon_1^{p^{n-1}} = \zeta_0^{p^{n-1}k}\epsilon_r^{p^{n-1}} = \epsilon_r^{p^{n-1}},$$

so we can, if we have to, replace ϵ_1 by ϵ_r. This implies that $\epsilon_1 \equiv b \bmod \lambda^2$ for some $b \in \mathbb{Z}$. But then

$$\epsilon_1^{p^{n-1}} \equiv b^{p^{n-1}} \bmod \lambda^2$$

so

$$b^{p^{n-1}} - 1 \equiv \epsilon - 1 \equiv 0 \bmod \lambda.$$

By lemma 2 p158 [B-S], this implies $b^{p^{n-1}} - 1 \equiv 0 \bmod p$ and by Fermat's theorem, $b \equiv b^{p^{n-1}} \equiv 1 \bmod p$ so $\epsilon_1 - 1 \equiv 0 \bmod \lambda$. Since $\epsilon_1 - 1$ is real,

$\epsilon_1 - 1 \equiv 0 \bmod \lambda^2$. By lemma 2.5, $\log \epsilon_1 \equiv \frac{\epsilon_1^{p^{n-1}}-1}{p^{n-1}} \equiv 0 \bmod p$ and hence by lemma 2.4 we have a unique representation

$$\log \epsilon_1 = p \sum_{k=2}^{m} c_k \log \theta_k^{p-1}, \tag{2.1}$$

where the c_k are p-adic integers.
On the other hand, since $(-\epsilon_1)^{p^{n-1}} = -\epsilon_1^{p^{n-1}}$ we can assume that $\epsilon_1 > 0$, that is $\epsilon_1 \in E$. By lemma 2.4 $[E : E_0]$ is finite so there exists a positive rational integer a such that $\epsilon_1^a \in E_0$. Hence $\epsilon_1^a = \prod_{k=2}^{m} \theta_k^{d_k}$ for some rational integers d_k and $m := \frac{p-1}{2}$. Since there are no elements of finite order in E we can assume that $(a, d_1, ..., d_m) = 1$. This gives us

$$a \log \epsilon_1^{p-1} = \log\left((\epsilon_1^a)^{p-1}\right) = \log\left(\prod_2^m \theta_k^{d_k}\right)^{p-1} = \sum_2^m d_k \log \theta_k^{p-1}.$$

By combining this with 2.1 we get

$$\sum_2^m a(p-1)pc_k \log \theta_k^{p-1} = \sum_2^m d_k \log \theta_k^{p-1}$$

so by uniqueness, $a(p-1)pc_k = d_k$. Since $a(p-1)c_k$ are p-adic integers, $p|d_k$ so there exists d_k' such that $d_k = pd_k'$. This gives

$$\epsilon_1^a = \left(\prod_2^m \theta_k^{d_k'}\right)^p := \epsilon_2^p.$$

$(a, d_1, ..., d_m) = 1$ implies $(a, p) = 1$ so there exists $u, v \in \mathbb{Z}$ such that $1 = au + pv$. Hence,

$$\epsilon_1 = \epsilon_1^{au+pv} = (\epsilon_2^p)^u \epsilon_1^{pv} = (\epsilon_2^u \epsilon_1^v)^p := \gamma_0^p$$

which proves the statement. □

2.2 The Norm Residue Symbol and the prime power case $\mathbb{Q}(\zeta_n)$

In this section we will prove the following theorem, which can be seen as Kummer's Lemma in the prime power case.

Theorem 2.7. *Let p be a regular prime. Let $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and suppose $\epsilon \equiv 1$ mod $\lambda_n^{p^{n+1}-1}$. Then $\epsilon = \gamma^p$ for some unit $\gamma \in \mathbb{Z}[\zeta_n]^*$.*

Recall that in $\mathbb{Z}[\zeta_0]$ we have $(p) = \lambda_0^{p-1}$ so with $n = 0$ the theorem above restricts to the classical version of Kummer's Lemma except that we have to have ϵ has to be congruent to 1, not just any rational integer.

The rest of this section is devoted to a proof of theorem 2.7. We start by indicating how one could prove the usual Kummer's Lemma with the help of some class field theory. The proof can be broken down into four steps.

Step 1: Prove a version of the theorem in the λ_0-adic completion of $\mathbb{Z}[\zeta_0]$ that says that a unit is a p-th power if it is congruent to 1 modulo λ_0^{p+1}. This can for example be done by using p-adic exponential and logarithm functions (we define these later in the general case) and observe that the series $\exp(1/p\log(\epsilon))$ converges.
Step 2: Show that $\epsilon \equiv 1 \mod \lambda_0^{p-1}$ implies $\epsilon \equiv 1 \mod \lambda_0^{p}$. This can easily be proved with the help of some simple observations and the norm map $N_{\mathbb{Q}(\zeta_0)/\mathbb{Q}}$.
Step 3: Show that $\epsilon \equiv 1 \mod \lambda_0^{p}$ implies $\epsilon \equiv 1 \mod \lambda_0^{p+1}$. This follows from the fact that our unit ϵ must in fact be real and that the λ_0-adic valuation of any real integer is an even natural number.
Step 4: Show that the extension $\mathbb{Q}(\zeta_0) \subseteq \mathbb{Q}(\zeta_0, \sqrt[p]{\epsilon})$ is of degree one. This is done by observing that in this extension, the only prime that can possibly ramify is λ_0. Since ramification numbers does not change when we complete, step 1 tells us that λ_0 does not ramify either. Then $\mathbb{Q}(\zeta_0, \sqrt[p]{\epsilon})$ is a subfield of the maximal unramified extension which has degree $\mathrm{Cl}(\mathbb{Q}(\zeta_0))$ over $\mathbb{Q}(\zeta_0)$. If the degree of our original extension is not 1 it must be p, but this is a contradiction since p is assumed to be regular.

Our proof of theorem 2.7 is based on the same four steps, lemmas 2.9, 2.15, 2.8 and 2.11 respectively. The only step that is significantly harder is step 2 which in our proof correspond to lemma 2.15 which is due to Stolin (see [ST1]). In our proof of this lemma we follow Stolin and use the so-called norm residue symbol.

As in the case $n = 0$, it is easy to see that the numbers $(\zeta_n - \zeta_n^{-1})^i$ $i = 0, 1, ..., m := p^n(p-1) - 1$ form an integral basis for $\mathbb{Q}(\zeta_n)$. If $y \in \mathbb{Z}[\zeta_n]^+$ and $y = a_0 + a_1(\zeta_n - \zeta_n^{-1}) + ... + a_m(\zeta_n - \zeta_n^{-1})^m$ we get that $0 = y - \bar{y} = 2a_1(\zeta_n - \zeta_n^{-1}) + 2a_3(\zeta_n - \zeta_n^{-1})^3 + ... + a_{m-1}(\zeta_n - \zeta_n^{-1})^{m-1}$ so $a_i = 0$ for all odd indices i. Hence y is congruent to a rational integer modulo $(\zeta_n - \zeta_n^{-1})^2 = \lambda_n^2$.

Lemma 2.8. *Let p be an odd prime. Let $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and suppose that $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}}$. Then $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$.*

Proof. By lemma 2.2, $\epsilon = \epsilon_r \zeta^k$ for some $\epsilon_r \in (\mathbb{Z}[\zeta_n]^+)^*$. Since $\zeta_n^k = (1 + (\zeta_n - 1))^k \equiv 1 + k(\zeta_n - 1) \mod \lambda_n^2$, $\epsilon_r \equiv a \mod \lambda_n^2$ for some $a \in \mathbb{Z}$ and $\epsilon_r\zeta_n^k = \epsilon \equiv 1 \mod \lambda_n^2$, we get that λ_n divides k and hence that p divides k and $k = pk_1$ for some $k_1 \in \mathbb{Z}$. It is easy to see that $\bar{\epsilon}^{-1} \equiv 1 \mod \lambda_n^{p^{n+1}}$ and this shows that $\zeta_n^{2k} = \epsilon\bar{\epsilon}^{-1} \equiv 1 \mod \lambda_n^{p^{n+1}}$. This in turn means that $p | \zeta_n^{2k} = \zeta_{n-1}^{2k_1}$ in $\mathbb{Z}[\zeta_n]$. But since then, $\zeta_{n-1}^{2k_1}/p \in \mathbb{Z}[\zeta_{n-1}]$ we get that $\lambda_{n-1}^{p^n - p^{n-1}} = p | \zeta_n^{2k} = \zeta_{n-1}^{2k_1}$ in $\mathbb{Z}[\zeta_{n-1}]$. Since $p^n - p^{n-1} \geq 2$ this implies $\lambda_{n-1} | (\zeta_{n-1}^{2k_1-1} + \ldots + \zeta_{n-1} + 1) \equiv 2k_1 \mod \lambda_{n-1}$ so $\lambda_{n-1} | 2k_1$ and hence we get that $p | k_1$ and $p^2 | k$. This argument can be repeated in $\mathbb{Z}[\zeta_{n-2}]$ to show that $p^3 | k$ and so on until we, from a similar argument in

$\mathbb{Z}[\zeta_0]$ get that $p^{n+1}|k$. But this means that $\epsilon = \epsilon_r\zeta^k = \epsilon_r$ so ϵ is real. Since $(\zeta_n - \zeta_n^{-1}) = \lambda_n$ as ideals, $\epsilon \equiv 1 \mod (\zeta_n - \zeta_n^{-1})^{p^{n+1}}$. By representing ϵ in the basis $(\zeta_n - \zeta_n^{-1})^i$, $i = 0, 1, 2, \ldots, p^n(p-1)-1$ and observing that all coefficients with odd index must be zero we get the desired result. □

We also need a local result. If R is the ring of integers of a number field K and λ a prime, we let K_λ denote the completion of K at λ and R_λ the valuation ring. By abuse of notation we let λ denote the (unique) maximal ideal of the local ring R_λ. Note that with the notations above, $(\mathbb{Z}[\zeta_n])_{\lambda_n} \cong \mathbb{Z}_p[\zeta_n]$.

In the proof of the following lemma we will use the (p-adic) logarithm function, log, and exponential, exp. For $x \in (\mathbb{Q}(\zeta_n))_{\lambda_n}$ we define

$$\log(1+x) = \sum_{k=1}^{\infty}(-1)^{k-1}\frac{x^k}{k}$$

and

$$\exp(x) = \sum_{k=0}^{\infty}\frac{x^k}{k!}.$$

It is well known that $\log(1+x)$ converges if $v_{\lambda_n}(x) \geq 1$ and that $\exp(x)$ converges if $v_{\lambda_n}(x) \geq p^n + 1$ (see chapter 4 of [B-S]). Moreover, provided that all series converge, the usual logarithmic and exponential rules hold. In particular $\exp(\log(1+x)) = 1 + x$ and $y\log(x) = \log(x^y)$.

Lemma 2.9. *Let ϵ be a unit in $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ with $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$, then there exists a unit γ in $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ such that $\epsilon = \gamma^p$. Moreover, $\gamma \equiv 1 \mod \lambda_n^{p^n+1}$.*

Proof. Let v_{λ_n} denote the valuation with respect to λ_n and let $\epsilon = 1 + x$. Then $v_{\lambda_n}(x) \geq p^{n+1} + 1$ and hence $v_{\lambda_n}(x^k) \geq k(p^{n+1}+1)$. If $1 \leq k \leq p-1$ we get

$$v_{\lambda_n}(x^k/k) \geq k(p^{n+1}+1).$$

Now suppose $k \geq p$. Let ln be the usual natural logarithm. If $k = lp^r$ where $l \in \mathbb{Z}$ and $(l, p) = 1$, then $p^r \leq k$ and

$$v_{\lambda_n}(k) = e(\lambda_n/(p))r = (p^{n+1} - p^n)r \geq (p^{n+1} - p^n)(\ln(k)/\ln(p)).$$

With this in mind,

$$\begin{aligned} v_{\lambda_n}(x^k/k) - (p^{n+1}+1) &\geq (k-1)(p^{n+1}+1) - v_{\lambda_n}(k) \geq \\ &\geq (k-1)(p^{n+1}+1) - (p^{n+1}-p^n)(\ln(k)/\ln(p)) = \\ &= (p^{n+1}-p^n)\frac{k-1}{\ln(p)}\Big(\frac{(p^{n+1}+1)\ln(p)}{p^{n+1}-p^n} - \frac{\ln(k)}{k-1}\Big) > \\ &> (p^{n+1}-p^n)\frac{k-1}{\ln(p)}\Big(\frac{\ln(p)}{p-1} - \frac{\ln(k)}{k-1}\Big) \geq 0, \end{aligned}$$

where the last inequality follows from the fact that $\frac{\ln(t)}{t-1}$ is strictly decreasing for $t \geq 2$. The calculation above shows that $v_{\lambda_n}(\log(1+x)) \geq p^{n+1}+1$. Hence

$$\begin{aligned} v_{\lambda_n}(\frac{1}{p}\log(1+x)) &= v_{\lambda_n}(log(1+x)) - v_{\lambda_n}(p) \geq \\ &\geq p^{n+1}+1-(p^{n+1}-p^n) = p^n+1 \end{aligned}$$

and we can define $\gamma := \exp(\frac{1}{p}\log(1+x))$. Trivially, $\gamma^p = \epsilon$ and since $pv_{\lambda_n}(\gamma) = v_{\lambda_n}(\gamma^p) = v_{\lambda_n}(\epsilon) \geq 0$, $\gamma \in (\mathbb{Z}[\zeta_n])_{\lambda_n}$. In the same way $\gamma^{-1} \in (\mathbb{Z}[\zeta_n])_{\lambda_n}$ so γ is a unit. To show that $\gamma \equiv 1 \mod \lambda_n^{p^n+1}$ we need to examine the sum

$$\exp(y) = \sum_{k=0}^{\infty} \frac{y^k}{k!},$$

where $y = \frac{1}{p}\log(1+x) \equiv 0 \mod \lambda_n^{p^n+1}$. If i is a natural number, the number of p-factors in $i!$ is given by $\left[\frac{i}{p}\right] + \left[\frac{i}{p^2}\right] + \ldots$, where $\left[a\right]$ stands for the (rational) integer part of a. Hence $v_{\lambda_n}(i!) < (p^{n-1}-p^n)\frac{i}{p-1}$ and $v_{\lambda_n}(\frac{y^k}{k!}) > k$. This shows that

$$\exp(y) \equiv \sum_{k=0}^{p^n-1} \frac{y^k}{k!} \mod \lambda_n^{p^n+1}.$$

To examine this sum it is enough to consider the worst case which is when $k = p^{n-1}$. By counting p-factors as above, we see that

$$v_{\lambda_n}(p^{n-1}!) = (p^{n+1}-p^n)(p^{n-2}+p^{n-3}+\ldots+p+1) = p^{2n-1}-p^n.$$

This finishes the proof since now

$$v_{\lambda_n}(\frac{y^{p^{n-1}}}{p^{n-1}!}) \geq p^{n-1}(p^n+1) - (p^{2n-1}-p^n) = p^n + p^{n-1} \geq p^n + 1.$$

□

If K is a number field we let h_K denote the class number of K.

Lemma 2.10. *If p is a prime and n an positive rational integer, then $p|h_{\mathbb{Q}(\zeta_n)}$ is equivalent to $p|h_{\mathbb{Q}(\zeta_0)}$.*

The proof of this can be found in [W] p. 187.

Lemma 2.11. *Let p be a regular prime. If $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$ then $\epsilon = \gamma^p$ for some unit $\gamma \in \mathbb{Z}[\zeta_n]^*$.*

Proof. Suppose ω is a prime in $\mathbb{Q}(\zeta_n)$ that ramifies in $\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})$. Since all archimedian primes are complex, they do not ramify so ω is not archimedian. Then ω divides the discriminant $\Delta(\mathbb{Z}[\zeta_n]/S)$ where S is the ring of integers in

$\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})$. Let $N = N_{\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})/\mathbb{Q}(\zeta_n)}$ denote the relative norm and let f be the minimal polynomial $x^p - \epsilon$. By a known theorem $\Delta(\mathbb{Z}[\zeta_n]/S)|N(f'(\sqrt[p]{\epsilon})$. But $N(f'(\sqrt[p]{\epsilon}) = N(p\epsilon^{(p-1)/p}) = up^p = u\lambda^{p^{n+1}(p-1)}$ for some unit u, so $\omega = \lambda_n$. Assume that ϵ is not a p-th power. Then, since $\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})$ is the splitting field of $f(x) = x^p - \epsilon$, $\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon}) \supseteq \mathbb{Q}(\zeta_n)$ is an abelian extension of degree p . By lemma 2.9, $(\mathbb{Q}(\zeta_n))_{\lambda_n} = (\mathbb{Q}(\zeta_n))_{\lambda_n}(\sqrt[p]{\epsilon})$ so λ_n does not ramify in $(\mathbb{Q}(\zeta_n))_{\lambda_n}(\sqrt[p]{\epsilon})$. Since the ramification indices does not change when we complete, λ_n does not ramify in $\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})$ either. Hence $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})$ is an unramified abelian extension of degree p. $\mathbb{Q}(\zeta_n)(\sqrt[p]{\epsilon})$ is thus a subfield of the Hilbert class field $\mathbb{H}$ of $\mathbb{Q}(\zeta_n)$ and since $[\mathbb{H} : \mathbb{Q}(\zeta_n)] = h_{\mathbb{Q}(\zeta_n)}$ we get that $p|h_{\mathbb{Q}(\zeta_n)}$. But this is a contradiction since p is regular and since $p|h_{\mathbb{Q}(\zeta_n)}$ implies $p|h_{\mathbb{Q}(\zeta_0)}$ by lemma 2.10. □

We will now define the norm residue symbol. Let $K = \mathbb{Q}(\zeta_n)$. If w is a valuation on K and $a \in K^*$, we have a local Artin map

$$\Psi_w : K_w^* \longrightarrow Gal(K_w(\sqrt[p]{a})/K_w).$$

We will use the following results:

Lemma 2.12. *Let $N = N_{K_w(\sqrt[p]{a})/K_w}$ be the norm and let $b \in K_w^*$. Then*

i) $\Psi_w(b)$ *is the identity if and only if* $b \in N(K_w(\sqrt[p]{a})^*)$

ii) $\Psi_w(b)$ *is the identity if* $K_w(\sqrt[p]{a})/K_w$ *is unramified and* b *is a unit in* K_w.

iii) *If* $b \in K^*$, *then* $\prod_w \Psi_w(b) = 1$, *where the product is taken over all valuations of* K.

The proofs can be found in for example [J], p. 224-226.

If $a \in K$, we will denote the action of $\Psi_w(b)$ on a by $a^{\Psi_w(b)}$. We define the norm residue symbol

$$(\ ,\ )_w : K_w^* \times K_w^* \longrightarrow \mu_p,$$

where μ_p is the group of p-th roots of unity, by $(a,b)_w = (\sqrt[p]{a})^{\Psi_w(b)}(\sqrt[p]{a})^{-1}$. It is easy to see that $(a,b)_w$ actually is a p-th root of unity.

Lemma 2.13. *Let $a, b \in K_w^*$. Then,*

i) $(a,b)_w = 1$ *if and only if* $b \in N(K_w(\sqrt[p]{a})^*)$

ii) $(a,b)_w = 1$ *if* $a + b \in (K_w)^p$

iii) $\prod_w (a,b)_w = 1$, *where the product is taken over all valuations of* K.

Proof. *i)*: If b is a local norm, then by lemma 2.12, $\Psi_w(b)$ is the identity map and $(a,b)_w$ is clearly 1. If $(a,b)_w = 1$, then we must have $(\sqrt[p]{a})^{\Psi_w(b)} = \sqrt[p]{a}$ so $\Psi_w(b)$ must be the identity map. Again by lemma 2.12, b is a local norm.

ii): If F is any field that contains the p-th roots of unity, $y \in F^*$ and $x \in F$, then the element $x^p - y$ is a norm from $F(\sqrt[p]{y})$ since if ζ is a fixed primitive p-th root of unity, then

$$x^p - y = \prod_{k=0}^{p-1}(x - \zeta^k \sqrt[p]{y}) = N_{F(\sqrt[p]{a})/F}(x - \sqrt[p]{y}).$$

This fact applied to $F = (\mathbb{Q}(\zeta_n))_{\lambda_n}$, $y = a$ and $x^p = a + b$ shows that b is a local norm and hence, by *i)* that $(a, b)_w = 1$.

iii): It is well known that b is a local unit for almost all valuations. Let $\mathfrak{M}$ consist of the primes that ramify and the primes where b is not a local unit. Then $\mathfrak{M}$ is a finite set and by lemma 2.12 *ii)*,

$$\prod_{w \notin \mathfrak{M}} \Psi_w(b) = 1.$$

By lemma 2.12 *iii)*,

$$\prod_{w \in \mathfrak{M}} \Psi_w(b) = 1$$

so

$$\prod_w (a, b)_w = \prod_{w \in \mathfrak{M}} (a, b)_w = (\sqrt[p]{a})^{\prod_{w \in \mathfrak{M}} \Psi_w(b)}(\sqrt[p]{a})^{-1} = (\sqrt[p]{a})(\sqrt[p]{a})^{-1} = 1$$

which completes the proof of the lemma. □

Now fix n and let $\lambda = \lambda_n$. Let for $i = 1, 2, \ldots$, $\eta_i = 1 - \lambda^i$.

Lemma 2.14. *For any valuation w of K we have*

i) $(\eta_i, \eta_j)_w = (\eta_i, \eta_{i+j})_w (\eta_{i+j}, \eta_j)_w (\lambda^j, \eta_{i+j})_w$

ii) If $i + j > p^{n+1}$ then $(\eta_i, \eta_j)_w = 1$

iii) If $i + j = p^{n+1}$ and $1 \leq i \leq p - 1$, then $(\eta_i, \eta_j)_w \neq 1$.

Proof. *i)*: Since p is odd, $(a, -1)_w = 1$ and by lemma 2.13 *ii)*, $(a, -a)_w = 1 = (a, 1-a)_w$ for all $a \in K^*$. It is easy to see that $(\ ,\ )_w$ is (multiplicatively) bilinear so $(a, -b)_w = (a, -1)_w (a, b)_w = (a, b)_w$ for all $a, b \in K^*$. Hence $(a, a)_w = (a, -a)_w = 1$. This implies

$$\begin{aligned} 1 &= (ab, -ab)_w = \\ &= (a, -a)_w (b, -a)_w (a, b)_w (b, b)_w = \\ &= (a, b)_w (b, a)_w. \end{aligned}$$

Now note that $\eta_j + \lambda^j \eta_i = \eta_{i+j}$, so $\frac{\eta_j}{\eta_{i+j}} + \frac{\lambda^j \eta_i}{\eta_{i+j}} = 1$. By lemma 2.13 *ii*), bilinearity and the identities above we get

$$\begin{aligned} 1 &= \left(\frac{\eta_j}{\eta_{i+j}}, \frac{\lambda^j \eta_i}{\eta_{i+j}}\right)_w = \\ &= (\eta_j, \lambda^j)_w (\eta_j, \eta_i)_w (\eta_j, \eta_{i+j})_w^{-1} (\eta_{i+j}, \lambda^j)_w^{-1} (\eta_{i+j}, \eta_i)_w^{-1} (\eta_{i+j}, \eta_{i+j})_w = \\ &= (\lambda^j, 1 - \lambda^j)_w (\eta_i, \eta_j)_w^{-1} (\eta_{i+j}, \eta_j)_w (\eta_{i+j}, \lambda)_w^{-j} (\eta_i, \eta_{i+j})_w = \\ &= (\eta_i, \eta_j)_w^{-1} (\eta_{i+j}, \eta_j)_w (\eta_{i+j}, \lambda)_w^{-j} (\eta_i, \eta_{i+j})_w \end{aligned}$$

which proves *i*).

ii): Suppose $i + j > p^{n+1}$. Then $\eta_{i+j} \equiv 1 \mod \lambda_n^{p^{n+1}+1}$. By lemma 2.9 any such element is a p-th power and hence a norm in any extension $K_\lambda(\sqrt[p]{\eta_k})/K_\lambda$. By *i*),

$$(\eta_i, \eta_j)_w = (\eta_{i+j}, \eta_i)_w^{-1} (\eta_{i+j}, \eta_j)_w (\eta_{i+j}, \lambda^j)_w^{-1} = 1.$$

If on the other hand $i + j = p^{n+1}$ and $1 \leq i \leq p - 1$, then $i + j + i > p^{n+1}$ and $i + j + j > p^{n+1}$ so,

$$(\eta_j, \eta_i)_w = (\eta_{i+j}, \eta_j)_w^{-1} (\eta_{i+j}, \eta_i)_w (\eta_{i+j}, \lambda^j)_w^{-1} = (\eta_{p^{n+1}}, \lambda^i)_w^{-1} \neq 1$$

by lemma 2.13 since λ^i cannot be a norm in the extension $K_\lambda(\sqrt[p]{\eta_{p^{n+1}}})/K_\lambda$. □

We will now use the norm residue symbol to extract a very useful fact about units in the cyclotomic fields, $\mathbb{Q}(\zeta_n)$. A more general version of this lemma was proved by Stolin and our proof follows the one in [ST1].

Lemma 2.15. *Let* $\epsilon \in \mathbb{Z}[\zeta_n]^*$ *and suppose that* $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}-1}$. *Then* $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}}$.

Before the proof we need to recall some simple facts. Let $K = \mathbb{Q}(\zeta_n)$, $R = \mathbb{Z}[\zeta_n]$, $\lambda = \lambda_n$ and let for $k = 1, 2, \ldots$, $U_k = \{u \in R_\lambda^* : u \equiv 1 \mod \lambda^k\}$. Then (the image of) η_k generates the group U_k/U_{k+1} of order p. This means that if $u \in U_k \setminus U_{k+1}$ there exists i such that $(i, p) = 1$ and $u^i \eta_k^{-1} = t \in U_{k+1}$.

Proof. Let ϵ satisfy the conditions of the lemma. Let w be a valuation of $K = \mathbb{Q}(\zeta_n)$. Let $v = v_{\lambda_n}$ be the valuation of K with respect to the prime λ_n and suppose $w \neq v$. From for example the proof of lemma 2.11, we know that the extension $K_w(\sqrt[p]{u})/K_w$ is unramified for every unit $u \in \mathbb{Z}[\zeta_n]$, so ϵ is a norm in every such extension. By 2.13 *i*), $(u, \epsilon)_w = 1$ and then, by 2.13 *iii*), $(u, \epsilon)_v = 1$.
Now let $u = \eta_1$. By the assumptions $\epsilon \in U_{p^{n+1}-1}$. Suppose $\epsilon \notin U_{p^{n+1}}$. Choose i such that $(i, p) = 1$ and $\epsilon^i \eta_{p^{n+1}-1}^{-1} = t \in U_{p^{n+1}}$ and in a similar way j such

that $t\eta_{p^{n+1}}^{-1} = s \in U_{p^{n+1}+1}$. Then by lemma 2.9 and 2.14 we have $(u,s)_v = (u,\eta_{p^{n+1}})_v = 1$. All this implies

$$\begin{aligned}(u,\epsilon)_v^i &= (u,\eta_{p^{n+1}-1}t)_v = (u,\eta_{p^{n+1}-1})_v(u,t)_v = \\ &= (u,\eta_{p^{n+1}-1})_v(u,\eta_{p^{n+1}})_v(u,s)_v = \\ &= (u,\eta_{p^{n+1}-1})_v \neq 1.\end{aligned}$$

Hence $(u,\epsilon)_v \neq 1$ which is a contradiction by the first part of the proof, so $= \epsilon \in U_{p^{n+1}}$ and this finishes the proof. □

We are now ready to prove the Kummer's Lemma in the prime power case.

Proof of Theorem 2.7. By lemma 2.15 we get, $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}}$ and by lemma 2.8 we then get, $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$. By lemma 2.11 ϵ is a p-th power of some unit γ. □

3 Construction of Norm Maps

In this section, following Stolin, [ST3], we will construct certain multiplicative maps from the rings $\mathbb{Z}[\zeta_n]$ to rings close to them. We will make extensive use of these maps in section 4.

3.1 Rings Close to $\mathbb{Z}[\zeta_n]$

We will in the sequel make extensive use of rings of the type $\mathbb{Z}[x]/(f(x))$ for some special polynomials f and will for simplicity have a special notation for these rings.

Define for $k \geq 0$ and $i \geq 1$

$$A_{k,i} := \frac{\mathbb{Z}[x]}{\left(\frac{x^{p^{k+i}}-1}{x^{p^k}-1}\right)}.$$

Denote the class of x in $A_{k,i}$ by $x_{k,i}$. We will sometimes, by abuse of notation and when we only deal with one of the rings, drop the index and write x for $x_{k,i}$. Note that $A_{k,1} \cong \mathbb{Z}[\zeta_k]$ by the isomorphism $x_{k,1} \mapsto \zeta_k$, where ζ_n is a primitive p^{n+1}-th root of unity. We will consider this as an identification.

We also define

$$D_{k,i} := \frac{A_{k,i}}{(p)} \cong \frac{\mathbb{F}_p[x]}{(x-1)^{p^{k+i}-p^k}}.$$

Lemma 3.1. *The commutative diagram*

$$\begin{tikzcd}
A_{k,i} \arrow[r, "i_{k,i}"] \arrow[d, "j_{k,i}"'] & A_{k+i-1,1} \arrow[d, "f_{k,i-1}"] \\
A_{k,i-1} \arrow[r, "g_{k,i-1}"] & D_{k,i-1}
\end{tikzcd}$$

where $i_{k,i}(x_{k,i}) = x_{k+i-1,1} = \zeta_{k+i-1}$, $j_{k,i}(x_{k,i}) = x_{k,i-1}$, $f_{k,i-1}(x_{k+i-1,1}) = \bar{x}$ *and* $g_{k,i-1}(x_{k,i-1}) = \bar{x}$, *is a pullback diagram for all* $k \geq 0$ *and* $i \geq 1$.

Proof. In Lemma 1.1, put $A = \mathbb{Z}[x]$, $\alpha = ((x^{p^{k+i}} - 1)/(x^{p^{k+i-1}} - 1))$ and $\beta = ((x^{p^{k+i-1}} - 1)/(x^{p^k} - 1))$. Since A is a unique factorization domain and α and β principal ideals, $\alpha \cap \beta = \alpha\beta = ((x^{p^{k+i}} - 1)/(x^{p^k} - 1))$.
We now need to find $\alpha + \beta$. A straightforward calculation gives

$$\frac{x^{p^{k+i}} - 1}{x^{p^{k+i-1}} - 1} = p + r(x)\frac{x^{p^{k+i-1}} - 1}{x^{p^k} - 1},$$

for some polynomial r. Hence $\alpha + \beta = \left(p, \frac{x^{p^{k+i-1}}-1}{x^{p^k}-1}\right)$ and

$$A/(\alpha+\beta) = \frac{A}{\left(p, \frac{x^{p^{k+i-1}}-1}{x^{p^k}-1}\right)} = \frac{A_{k,i-1}}{(p)} = \frac{\mathbb{F}_p[x]}{(x-1)^{p^{k+i-1}-p^k}} = D_{k,i-1}$$

which is exactly what we need. □

The map $i : A_{k,i} \to A_{k+1,i}$, $i(x_{k,i}) = x_{k+1,i}^p$ defines a $A_{k,i}$-module structure on $A_{k+1,i}$. We will need the following simple result.

Lemma 3.2. *For all* $k \geq 0$ *and* $i \geq 1$ $A_{k+1,i}$ *is a free* $A_{k,i}$*-module.*

Its clear that $\{1, x_{k+1,i}, \dots, x_{k+1,i}^{p-1}\}$ generate $A_{k+1,i}$ over $A_{k,i}$ and the proof, which can be found in for example [ST2], involves showing that there are no relations among these generators.

3.2 Construction of Norm Maps

In this section we will construct norm maps $N_{k,i} : \mathbb{Z}[\zeta_{k+i}] = A_{k+i,1} \to A_{k,i}$ such that the diagrams

$$\begin{tikzcd}
 & \mathbb{Z}[\zeta_{k+i}] \arrow[dl, "N_{k,i}"'] \arrow[d, "f_{k,i}"] \\
A_{k,i} \arrow[r, "g_{k,i}"] & D_{k,i}
\end{tikzcd} \tag{3.1}$$

commute. The maps f_{k+i} and $g_{k,i}$ are defined in Lemma 3.1. The construction will be inductive with respect to i.

If $i = 1$ and is k arbitrary, let $N_{k,1}$ be the usual norm map $\mathbb{Z}[\zeta_{k+1}] \to \mathbb{Z}[\zeta_k] = A_{k,1}$. It is well known that $N_{k,1}(\zeta_{k+1}) = \zeta_k$, so the following lemma will make it clear that the diagram above, with $i = 1$, commutes.

Lemma 3.3. *$N_{k,1}(a+b) \equiv N_{k,1}(a) + N_{k,1}(b) \mod (p)$ for all $a, b \in \mathbb{Z}[\zeta_{k+1}]$.*

Proof. First note that $\mathbb{Z}[\zeta_{k+1}]$ is free as a $\mathbb{Z}[\zeta_k]$-module and that $\mathbb{Z}[\zeta_{k+1}](p)$ is free as a $\mathbb{Z}[\zeta_k]/(p)$-module. $N_{k,1}$ hence induces a map $\widetilde{N} : \mathbb{Z}[\zeta_{k+1}]/(p) \to \mathbb{Z}[\zeta_k]/(p)$ and it is enough to show that $\widetilde{N}(\bar{a}) = \bar{a}^p$ since this implies $N_{k,1}(a) \equiv a^p \mod (p)$ and $N_{k,1}(a+b) \equiv (a+b)^p \equiv a^p + b^p \equiv N_{k,1}(a) + N_{k,1}(b)$. The last congruence follows from the fact that $p | \binom{p}{k}$ for $1 \leq k \leq p-1$. Since

$$\mathbb{Z}[\zeta_n]/(p) \cong \frac{\mathbb{F}_p[x]}{\frac{x^{p^{n+1}}-1}{x^{p^n}-1}} \cong \frac{\mathbb{F}_p[t]}{(t-1)^{p^{n+1}-p^n}} \cong \frac{\mathbb{F}_p[y]}{y^{p^{n+1}-p^n}},$$

we can view the extension $\mathbb{Z}[\zeta_{k+1}]/(p) \supset \mathbb{Z}[\zeta_k]/(p)$ as an extension $\mathbb{F}_p[y] \supset \mathbb{F}_p[z]$ with $y^p = z$. In this case it is well known that the norm is given by $r \mapsto r^p$ for all $r \in \mathbb{F}_p[y]$ and this finishes the proof. □

Now suppose $N_{k,j}$ is constructed for all k and all $j \leq i-1$. We want to construct $N_{k,i}$ for a given but arbitrary k. First note, that by Lemma 3.1 we can view $A_{k+1,i}$ as the ring $\{(a,b) \in \mathbb{Z}[\zeta_{k+i}] \oplus A_{k+1,i-1} : f_{k,i}(a) = g_{k+1,i}(b)\}$. By the assumption there is a norm map $N_{k+1,i-1} : \mathbb{Z}[\zeta_{k+i}] \to A_{k+1,i-1}$ such that the diagram

$$\begin{tikzcd}
 & \mathbb{Z}[\zeta_{k+i}] \arrow[dl, "N_{k+1,i-1}"'] \arrow[d, "f_{k,i}"] \\
A_{k+1,i-1} \arrow[r, "g_{k+1,i-1}"] & D_{k+1,i-1}
\end{tikzcd}$$

commutes. Define $\varphi : \mathbb{Z}[\zeta_{k+i}] \to A_{k+1,i}$ by $\varphi(a) = (a, N_{k+1,i-1}(a))$. Its clear that φ is multiplicative. Since $A_{k+1,i}$ is a free $A_{k,i}$-module, by Lemma 3.2, we can in the usual way define a norm map

$$N : A_{k+1,i} \to A_{k,i},\ N(a) = \det r_a,$$

where r_a the multiplication map $r_a(b) = ab$. N is clearly multiplicative and by the same reasoning as in the proof of Lemma 3.3 we have the following.

Lemma 3.4. *$N(a+b) \equiv N(a) + N(b) \mod (p)$ for all a,b $\in A_{k+1,i}$.*

Now define $N_{k,i} := N \circ \varphi : \mathbb{Z}[\zeta_{k+i}] \to A_{k,i}$. $N_{k,i}$ is multiplicative as a composition of multiplicative maps. We need to prove that the diagram 3.1 commutes.

By assumption, $N_{k+1,i-1}(\zeta_{k+i}) = x_{k+1,i-1}$ so $\varphi(\zeta_{k+i}) = (\zeta_{k+i}, x_{k+1,i-1}) = x_{k+1,i} \in A_{k+1,i}$. If we use the basis $\{x_{k+1,i}^{p-1}, 1, x_{k+1,i}, \dots, x_{k+1,i}^{p-2}\}$ for $A_{k+1,i}$ over $A_{k,i}$, the matrix for the multiplication map $r_{x_{k+1,i}}$ is diagonal with the first diagonal element being $x_{k,i}$ and the others being ones. Hence $N(x_{k+1,i}) = \det r_{x_{k+1,i}} = x_{k,i}$. As in the case $i = 1$ we now only need to show the following Lemma.

Lemma 3.5. *$N_{k,i}(a+b) \equiv N_{k,i}(a) + N_{k,i}(b) \mod (p)$ for all $a, b \in \mathbb{Z}[\zeta_{k+i}]$.*

Proof. For some $\alpha + (\frac{x^{p^{k+i+1}}-1}{x^{p^{k+1}}-1}) = \bar{\alpha} \in A_{k+1,i}$ we have $\varphi(a+b) - \varphi(a) - \varphi(b) = (0, N_{k+1,i-1}(a+b) - N_{k+1,i-1}(a) - N_{k+1,i-1}(b)) = \bar{\alpha}$. This means $i_{k,i}(\bar{\alpha}) = 0$ and hence that $\alpha \in (\frac{x^{p^{k+i+1}}-1}{x^{p^{k+i}}-1})$. By the fact that $N(x_{k+1,i}^{p^{k+i}}) = x_{k,i}^{p^{k+i}} = 1$, and by Lemma 3.4 we now, for some $r \in A_{k+1,i}$, get

$$\begin{aligned} & N_{k,i}(a+b) - N_{k,i}(a) - N_{k,i}(b) \equiv \\ & \qquad \equiv N(\varphi(a+b) - \varphi(a) - \varphi(b)) = N(\frac{x_{k+1,i}^{p^{k+i+1}} - 1}{x_{k+1,i}^{p^{k+i}} - 1} \cdot r) = \\ & \qquad = N(x_{k+1,i}^{p^{k+i+1}-p^{k+i}} + x_{k+1,i}^{p^{k+i+1}-2p^{k+i}} + \ldots + 1)N(r) = \\ & \qquad = (x_{k,i}^{p^{k+i+1}-p^{k+i}} + x_{k,i}^{p^{k+i+1}-2p^{k+i}} + \ldots + 1)N(r) = \\ & \qquad\qquad = \bar{p}N(r) \equiv 0 \mod (p) \end{aligned}$$

□

We have now proved the existence of the norm maps and put this down as a proposition.

Proposition 3.6. *For each $k \geq 0$ and $i \geq 1$ there exists a multiplicative map $N_{k,i}$ such that the diagram*

$$\begin{tikzcd} & \mathbb{Z}[\zeta_{k+i}] \arrow[dl, "N_{k,i}"'] \arrow[d, "f_{k,i}"] \\ A_{k,i} \arrow[r, "g_{k,i}"] & D_{k,i} \end{tikzcd}$$

is commutative.

Note that it is clear from the definition that $N_{k,i}(1) = 1$ for all maps $N_{k,i}$. Whenever B_2 is a free B_1-module we let N denote the usual norm map defined by the determinant. An element in $A_{k,i}$ can be represented as a pair $(a, b) \in \mathbb{Z}[\zeta_{k+i-1}] \times A_{k,i-1}$ and an element in $A_{k,i-1}$ can be represented as a pair $(c, d) \in$

$\mathbb{Z}[\zeta_{k+i-2}] \times A_{k,i-2}$. If (a,b) represents an element in $A_{k,i}$ we get have that $N(a,b) = (N(a), N(b)) \in A_{k,i-1}$.

Proposition 3.7. *The diagram*

$$\begin{tikzcd}
A_{k+1,i} \arrow[d, "N"] & \mathbb{Z}[\zeta_{k+i}] \arrow[l, "N_{k+1,i}"'] \arrow[d, "N"] \\
A_{k,i} & \mathbb{Z}[\zeta_{k+i-2}] \arrow[l, "N_{k,i}"']
\end{tikzcd}$$

is commutative

Proof. Induction with respect to i. If $i = 1$ the statement is trivial. Suppose the diagram corresponding to the one above, but with i replaced by $i-1$, is commutative for all k. If $a \in \mathbb{Z}[\zeta_{k+i}]$ we have

$$N(N_{k+1,i}(a)) = (N(N(a)), N(N(N_{k+2,i-1}(a))))$$

and

$$N_{k,i}(N(a)) = (N(N(a)), N(N_{k+1,i-1}(N(a)))).$$

By the induction hypothesis $N \circ N_{k+2,i-1} = N_{k+1,i-1} \circ N$ and this proves the proposition. □

Corollary 3.8. *Let $N : \mathbb{Z}[\zeta_{k+i}] \to \mathbb{Z}[\zeta_{k+i-1}]$ be the usual norm map. Then, $N_{k,i}(a) = (N(a), N_{k,i-1}(N(a)))$.*

In the same way as an element in $A_{k,i}$ can be represented by a pair $(a_i, b) \in \mathbb{Z}[\zeta_{k+i-1}] \oplus A_{k,i-1}$, the element $b \in A_{k,i-1}$ can be represented by some $(a_{i-1}, c) \in \mathbb{Z}[\zeta_{k+i-2}] \oplus A_{k,i-2}$. By applying this i times we see that we can actually represent any element in $A_{k,i}$ as an i-tuple $(a_i, \ldots, a_m, \ldots, a_1)$ where $a_m \in \mathbb{Z}[\zeta_{k+m-1}]$. Let for $s \geq 0$ and $0 \leq t \leq s$ $\tilde{N}_{s,t} : \mathbb{Z}[\zeta_s] \to \mathbb{Z}[\zeta_{s-t}]$ denote the usual norm maps. We let $\tilde{N}_{s,0}$ be the identity map.

Corollary 3.9. *If $a \in \mathbb{Z}[\zeta_{k+i}]$ then*

$$N_{k,i}(a) = (\tilde{N}_{k+i,1}(a), \tilde{N}_{k+i,2}(a), \ldots, \tilde{N}_{k+i,i}(a))$$

It is important to note that even though not all elements of $\mathbb{Z}[\zeta_{k+i-1}] \oplus \ldots \oplus \mathbb{Z}[\zeta_k]$ represent an element of $A_{k,i}$ we have that if $(a_i, \ldots, a_m, \ldots, a_1)$ represents an element of $A_{k,i}$, then $(a_{i-1}, \ldots, a_m, \ldots, a_1)$ represents an element of $A_{k,i-1}$.

4 The Picard Group of $\mathbb{Z}C_{p^n}$

In this section we want to study the group $\operatorname{Pic}\mathbb{Z}C_{p^n}$ where C_{p^n} is the cyclic group of order p^n and p is a regular prime. The main result is that there is an exact sequence

$$0 \to V_n \to \operatorname{Pic}\mathbb{Z}C_{p^n} \to \operatorname{Cl}\mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic}\mathbb{Z}C_{p^{n-1}} \to 0.$$

This was proved in [K-M] and the structure of the group V_n was given explicitly. We will reprove this result using a different method. The proof in [K-M] relies on Iwasawa theory and action of Galois groups on the rings involved. This is enough to show the result not only for regular primes, but also for so called semi regular primes. In our proof, which works for regular primes, we use the norm maps constructed in section 3 and our generalization of Kummer's lemma from section 2.

D.S. Rim proved in [Rim] that $\mathrm{K}_0\mathbb{Z}C_p \cong \mathrm{K}_0\mathbb{Z}[\zeta_0]$. We start of by stating a well known generalisation of this.

Proposition 4.1. $\operatorname{Pic}\mathbb{Z}C_{p^n} \cong \operatorname{Pic}A_{0,n}$ *for all* $n \geq 1$.

The proof can be found in [ST1] and is inductive starting with a version of Rim's theorem for $n = 1$. For the induction step one uses the pullback diagram

$$\begin{tikzcd}
\mathbb{Z}C_{p^n} \arrow[r, "t\mapsto x_{0,n}"] \arrow[d, "t\mapsto 1"'] & A_{0,n} \arrow[d, "x_{0,n}\mapsto 1(\mathrm{mod} p^n)"] \\
\mathbb{Z} \arrow[r, "1\mapsto 1(\mathrm{mod} p^n)"] & \mathbb{Z}/p^n\mathbb{Z}
\end{tikzcd}$$

One then show that that the map β_1 in the corresponding Mayer-Vietoris sequence is a surjection (see Proposition 1.5). After that the results follows.

The proposition above shows that we only need to consider $\operatorname{Pic}A_{0,n}$.

Consider the pullback diagram

$$\begin{tikzcd}
A_{0,n} \arrow[r, "i_{0,n}"] \arrow[d, "j_{0,n}"'] & \mathbb{Z}[\zeta_{n-1}] \arrow[d, "f_{0,n-1}"] \\
A_{0,n-1} \arrow[r, "g_{0,n-1}"] & D_{0,n-1}
\end{tikzcd}$$

from Lemma 3.1. This gives us a Mayer-Vietoris sequence

$$\mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^* \to D_{0,n-1}^* \to \operatorname{Pic}A_{0,n} \to$$
$$\to \operatorname{Pic}\mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic}A_{0,n-1} \to \operatorname{Pic}D_{0,n-1}.$$

By using that $D_{0,n-1}$ is local and hence has trivial Picard group and that $\operatorname{Pic}\mathbb{Z}[\zeta_{n-1}] \cong \operatorname{Cl}\mathbb{Z}[\zeta_{n-1}]$ we get the following exact sequence:

$$0 \to \frac{D^*_{0,n-1}}{\operatorname{Im}\{\mathbb{Z}[\zeta_{n-1}]^* \oplus A^*_{0,n-1} \to D^*_{0,n-1}\}} \to \operatorname{Pic} A_{0,n} \to$$

$$\to \operatorname{Cl}\mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic} A_{0,n-1} \to 0.$$

The only thing we have to do is to find the cokernel

$$\frac{D^*_{0,n-1}}{\operatorname{Im}\{\mathbb{Z}[\zeta_{n-1}]^* \oplus A^*_{0,n-1} \to D^*_{0,n-1}\}}.$$

In short, what we will do is to decompose $D^*_{0,n-1}$ as a sum

$$D^*_{0,n-1} = \mathbb{F}^*_p \oplus (\widetilde{D^*_{0,n-1}})^+ \oplus (\widetilde{D^*_{0,n-1}})^-$$

and then find the structure of these groups. This is merely a simple calculation. Then we concentrate on the image and show that it is isomorphic to $\mathbb{F}^*_p \oplus (\widetilde{D^*_{0,n-1}})^+ \oplus C_{p^{n-1}}$ and this gives us our main theorem

Theorem 4.2. *Let p be a regular prime and let $n \geq 2$. Then the sequence*

$$0 \to \prod_{j=1}^{n-1} C_{p^j}^{k_j} \to \operatorname{Pic} A_{0,n} \to \operatorname{Cl}\mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic} A_{0,n-1} \to 0,$$

where $k_j = \frac{(p-1)^2 p^{n-j-2}}{2}$ for $1 \leq j \leq n-2$ and $k_{n-1} = \frac{p-3}{2}$, is exact.

Remark. When $n = 1$, proposition 4.1 and the fact that $\operatorname{Pic}\mathbb{Z}[\zeta_0] \cong \operatorname{Cl}\mathbb{Z}[\zeta_0]$ tells us that $\operatorname{Pic}\mathbb{Z}C_p \cong \operatorname{Cl}\mathbb{Z}[\zeta_0]$.

4.1 Structure of $D^*_{0,n-1}$

By setting $y = x-1$ we see that $D_{0,n-1} = \mathbb{F}_p[x]/(x-1)^{p^{n-1}-1} \cong \mathbb{F}_p[y]/(y^{p^{n-1}-1}) \cong \{a_0 + a_1 y + \ldots + a_{p^{n-1}-2} y^{p^{n-1}-2} \ : \ a_i \in \mathbb{F}_p,\ y^{p^{n-1}-1} = 0\}$. This shows that $|D_{0,n-1}| = p^{p^{n-1}-1}$. Every element with $a_0 = 0$ is nilpotent and hence not a unit. Since $a_0 + (y^{p^{n-1}-1} - 1)$ is a unit in $\mathbb{F}_p[y]/(y^{p^{n-1}-1})$ if $a_0 \neq 0$, this also implies that every element with $a_0 \neq 0$ is a unit and that $|D^*_{0,n-1}| = (p-1)p^{p^{n-1}-2}$. Clearly, $\mathbb{F}^*_p \subset D^*_{n-1}$ and by the structure theorem for abelian groups, $D^*_{0,n-1} = \mathbb{F}^*_p \oplus \widetilde{D^*_{0,n-1}}$ where $\widetilde{D^*_{0,n-1}}$ is a p-group so $\widetilde{D^*_{0,n-1}} = C_p^{r_1} \oplus C_{p^2}^{r_2} \oplus C_{p^3}^{r_3} \oplus \ldots$ for some $r_i \in \mathbb{Z}_{\geq 0}$.

Observe that if $u = 1 + a_1 y + \ldots + a_{p^{n-1}-2} y^{p^{n-1}-2}$ then $u^p = 1 + a_1 u^p + a_2 y^{2p} + \ldots + a_{p^{n-2}-1} y^{(p^{n-2}-1)p}$. Hence if $u^p = 1$ we must have $a_1 = a_2 = \ldots = a_{p^{n-2}-1} = 0$ and this shows that the set $\{u \in \widetilde{D^*_{0,n-1}} \ : \ u^p = 1\}$

has $p^{p^{n-1}-2-(p^{n-1}-1)} = p^{p^{n-1}-p^{n-2}-1}$ elements. A similar argument gives that $|\{u \in \widetilde{D^*_{0,n-1}} \, : \, a^{p^k} = 1\}| = p^{p^{n-1}-p^{n-(k+1)}-1}$ for $k = 1, 2, \ldots, n-1$ and that no element has order greater than p^{n-1}. Hence $r_i = 0$ for all $i > n-1$ and by counting elements of different orders in the groups C_{p^k} and in $\widetilde{D^*_{0,n-1}}$, we get the following system of equations for the exponents r_i.

$$\begin{aligned}
r_1 + 2r_2 + \ldots + (n-3)r_{n-3} + (n-2)r_{n-2} + (n-1)r_{n-1} &= p^{n-1} - 2 \\
r_1 + 2r_2 + \ldots + (n-3)r_{n-3} + (n-2)r_{n-2} + (n-2)r_{n-1} &= p^{n-1} - p - 1 \\
r_1 + 2r_2 + \ldots + (n-3)r_{n-3} + (n-3)r_{n-2} + (n-3)r_{n-1} &= p^{n-1} - p^2 - 1 \\
&\vdots \\
r_1 + r_2 + \ldots + r_{n-3} + r_{n-2} + r_{n-1} &= p^{n-1} - p^{n-2} - 1.
\end{aligned}$$

Solving this system gives us the proposition stated below.

Proposition 4.3. *$D^*_{0,n-1} = \mathbb{F}_p^* \oplus C_p^{r_1} \oplus C_{p^2}^{r_2} \oplus \ldots \oplus C_{p^{n-1}}^{r_{n-1}}$, where $r_1 = p^{n-1} - 2p^{n-2} + p^{n-3} - 1$, $r_{n-1} = p - 1$ and $r_k = p^{n-k} - 2p^{n-(k+1)} + p^{n-(k+2)}$ for $k = 2, 3, \ldots, n-2$.*

Let c be the map $t \mapsto t^{-1}$ in $D_{k,i} \cong \mathbb{F}_p[t]/(t-1)^{p^{k+i}-p^k}$. Let $(\widetilde{D^*_{0,i}})^+ = \{u \in \widetilde{D^*_{0,i}} \, : \, c(u) = u\}$ and $(\widetilde{D^*_{0,i}})^- = \{u \in \widetilde{D^*_{0,i}} \, : \, c(u) = u^{-1}\}$. Since $\widetilde{D^*_{0,i}}$ is an finite abelian group of odd order and since c has order 2 we get $\widetilde{D^*_{0,i}} \cong (\widetilde{D^*_{0,i}})^+ \oplus (\widetilde{D^*_{0,i}})^-$. $\widetilde{D^*_{0,i}}$ can be presented as $\{1 + a_1(x - x^{-1}) + \ldots + a_{p^i-2}(x - x^{-1})^{p^i-2}\}$ and $c((x - x^{-1})^j) = (-1)^j(x - x^{-1})^j$ so it is not hard to see that $(\widetilde{D^*_{0,i}})^+$ can be represented as $\{1 + a_2(x - x^{-1})^2 + a_4(x - x^{-1})^4 + \ldots + a_{p^i-3}(x - x^{-1})^{p^i-3}\}$. By a similar calculation as in section 4.1 we get the following proposition.

Proposition 4.4. *Let $(\widetilde{D^*_{0,i}})^+$ and $(\widetilde{D^*_{0,i}})^-$ be defined as above. Then*

$$(\widetilde{D^*_{0,i}})^+ \cong C_p^{s_1} \oplus C_{p^2}^{s_2} \oplus \ldots \oplus C_{p^i}^{s_i}$$

and

$$(\widetilde{D^*_{0,i}})^- \cong C_p^{k_1} \oplus C_{p^2}^{k_2} \oplus \ldots \oplus C_{p^i}^{k_i},$$

where $s_1 = \frac{p^i - 2p^{i-1} + p^{i-2} - 2}{2}$, $k_1 = \frac{p^i - 2p^{i-1} + p^{i-2}}{2}$, $s_i = k_i = \frac{p-1}{2}$ and $s_j = k_j = \frac{p^{i-j+1} - 2p^{i-j} + p^{i-j-1}}{2}$ for $2 \leq j \leq i-1$.

4.2 Structure of $\operatorname{Im}\{\mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^* \to D_{0,n-1}^*\}$

By Lemma 3.1 and 3.6 we have the pullback diagram

$$\begin{tikzcd}
A_{0,n} \arrow[r, "i_{0,n}"] \arrow[d, "j_{0,n}"'] & \mathbb{Z}[\zeta_{n-1}] \arrow[d, "f_{0,n-1}"] \arrow[dl, "N_{0,n-1}"'] \\
A_{0,n-1} \arrow[r, "g_{0,n-1}"] & D_{0,n-1}
\end{tikzcd}$$

where the lower right triangle commutes.

Lemma 4.5. $\operatorname{Im}\{\mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^* \to D_{0,n-1}^*\} = \operatorname{Im}\{A_{0,n-1}^* \to D_{0,n-1}^*\}$

Proof. In the diagram above, observe that $N_{0,n-1}$ maps units to units since it is a multiplicative map that maps 1 to 1. By the commutativity of the lower right triangle above, we have $f_{0,n-1}(\mathbb{Z}[\zeta_{n-1}]) \subseteq g_{0,n-1}(N_{0,n-1}(\mathbb{Z}[\zeta_{n-1}])) \subseteq g_{0,n-1}(A_{0,n-1}^*)$. □

This means that we can concentrate our efforts on analysing

$$\operatorname{Im}\{A_{0,n-1}^* \xrightarrow{g_{0,n-1}} D_{0,n-1}^*\}$$

Recall that, by lemma 2.2, any unit in $\mathbb{Z}[\zeta_k]$ can be represented as a product of a real unit and a power of ζ_k. We need a similar representation for the rings $A_{k,i}$. Let $c : A_{k,i} \to A_{k,i}$ be the homomorphism defined by $c(x_{k,i}) = x_{k,i}^{-1}$. The function c plays the role of complex conjugation and a unit u in $A_{k,i}$ such that $c(u) = u$ will sometimes be refered to as real. We will, by abuse of notation, denote this map by just c regardless of which of the rings $A_{k,i}$ we are dealing with. Moreover, we will sometimes also denote both complex conjugation in the rings $\mathbb{Z}[\zeta_k]$ and the map $t \mapsto t^{-1}$ in $D_{k,i-1} \cong \mathbb{F}_p[t]/(t-1)^{p^{k+i}-p^k}$ by c.

Lemma 4.6. *For every unit $\epsilon \in A_{0,i}^*$ there exists a natural number k and a unit ϵ_r with $c(\epsilon_r) = \epsilon_r$ such that $\epsilon = x_{0,i}^k \epsilon_r$.*

Proof. Induction with respect to i: If $i = 1$, this is Lemma 2.2. Fix $i \geq 2$ and suppose that the statement holds with i replaced by $i-1$. Consider the commutative diagram

$$\begin{tikzcd}
A_{0,i} \arrow[r] \arrow[d] & \mathbb{Z}[\zeta_{i-1}] \arrow[d, "f"] \\
A_{0,i-1} \arrow[r, "g"] & D_{0,i-1}
\end{tikzcd}$$

Let t be a generator of $D_{0,i-1}$ Take $\epsilon \in A_{0,i}^*$ and let ϵ be represented by $(\epsilon', u) \in A_{0,i}^* \oplus \mathbb{Z}[\zeta_{i-1}]^*$. By the assumption there exists real $\epsilon_r' \in A_{0,i-1}^*$ and $u_r \in \mathbb{Z}[\zeta_{i-1}]^*$

such that $\epsilon' = x_{0,i-1}^{k_1}\epsilon'_r$ and $u = \zeta_{i-1}^{k_2}u_r$. It is easy to see that the maps c commute with the diagram. We now have $c(\epsilon'_r, u_r) = (\epsilon'_r, u_r)$ and $(e', u) = (x_{0,i-1}^{k_1}, \zeta_{i-1}^{k_2})(\epsilon'_r, u_r)$. Since $f(u) = g(\epsilon')$ is equivalent to $f(c(u)) = g(c(\epsilon'))$, we get

$$t^{k_1}g(\epsilon'_r) = t^{k_2}f(u_r)$$

and

$$t^{-k_1}g(\epsilon'_r) = t^{-k_2}f(u_r)$$

so we get $t^{2(k_1-k_2)} = 1$ in $D_{0,i-1}$. Since we deal with an odd prime we get $k_1 - k_2 \equiv 0 \mod p^{i-1}$. This means that $x_{0,i-1}^{k_1} = x_{0,i-1}^{k_2}$ and finally that $(\epsilon', u) = (\epsilon'_r, u_r)(x_{0,i-1}, \zeta_{i-1})^{k_2}$. □

Take $\epsilon \in A_{0,i}^*$. By Lemma 4.6 there exists k and ϵ_r with $c(\epsilon_r) = \epsilon_r$ such that $\epsilon = x_{0,i}^k\epsilon_r$. Hence $g_{0,i}(\epsilon) = t^k g(\epsilon_r)$, where $t = t_{0,i}$ is a generator of $D_{0,i}$. Since $g(\epsilon_r) \in (\widetilde{D_{0,i}^*})^+ \oplus \mathbb{F}_p^*$, we get the following proposition.

Lemma 4.7. *Let $t = t_{0,n-1}$ be a generator of $D_{0,i}$. Then*

$$\mathrm{Im}\{A_{0,n-1}^* \to D_{0,n-1}^*\} \subset \mathbb{F}_p^* \oplus < t > \oplus (\widetilde{D_{0,n-1}^*})^+.$$

We also have

Lemma 4.8. $\mathrm{Im}\{A_{0,n-1}^* \to D_{0,n-1}^*\} \supset \mathbb{F}_p^* \oplus < t >$.

Proof. Take an arbitrary $k \in \mathbb{F}_p^*$. By Fermat's little theorem, $k \equiv k^{p^{n-1}-1}$ mod p. Consider $\frac{x^k-1}{x-1} \in A_{0,n-1}$. There exists natural numbers s and r such that $kr - sp^{n-1} = 1$ and

$$\begin{aligned} \frac{x^k-1}{x-1}\frac{x^{1+sp^{n-1}}-1}{x^k-1} - 1 &= \frac{x^{1+sp^{n-1}}-1}{x-1} - 1 = \\ &= \frac{x^{1+sp^{n-1}}-x}{x-1} = x\frac{x^{sp^{n-1}}-1}{x-1} = \\ &= x(x^{s(p^{n-1}-1)} + \ldots + x^s + 1)\frac{x^{p^{n-1}}-1}{x-1} \equiv 0 \end{aligned}$$

in $A_{0,n-1}$. Moreover, $\frac{x^{1+sp^{n-1}}-1}{x^k-1} = \frac{x^{kr}-1}{x^k-1} = x^{r(k-1)} + \ldots + x^r + 1 \in A_{0,n-1}$ so $\frac{x^k-1}{x-1} \in A_{0,n-1}^*$. Now,

$$\begin{aligned} \frac{x^k-1}{x-1} - k &= x^{k-1} + \ldots + x + 1 - k = \\ &= (x-1)f(x) \end{aligned}$$

for some $f \in \mathbb{Z}[x]$, so $\frac{x^k-1}{x-1} - k \equiv 0 \mod (x-1)$. Finally, in $D_{0,n-1}$ we have

$$\begin{aligned} g(\frac{x^k-1}{x-1})^{p^{n-1}-1} - k &= g(\frac{x^k-1}{x-1})^{p^{n-1}-1} - k^{p^{n-1}-1} \\ &= g(\frac{x^k-1}{x-1} - k)^{p^{n-1}-1} = (t-1)^{p^{n-1}-1} = \\ &= 0, \end{aligned}$$

which shows that $k \in g(A^*_{0,n-1})$. Since it is obvious that $< t >$ is contained in the image we are finished. □

Lemma 4.9. *There exists an injection* $\varphi = \varphi_{k,i} : \mathbb{Z}[\zeta_{k+i-1}]^* \to A^*_{k,i}$ *where* $\varphi(\epsilon) = (\epsilon, N_{k,i-1}(\epsilon))$. *Moreover,* $A^*_{k,i} \cong \mathbb{Z}[\zeta_{k+i-1}]^* \oplus B_{k,i-1}$ *for some* $B_{k,i-1}$.

Proof. Consider the pullback

$$\begin{tikzcd} A_{k,i} \arrow[r, "i"] \arrow[d, "j"'] & \mathbb{Z}[\zeta_{k+i-1}] \arrow[d, "f"] \arrow[dl, "N_{k,i-1}"'] \\ A_{k,i-1} \arrow[r, "g"] & D_{k,i-1} \end{tikzcd}$$

where the bottom triangle commutes. Recall that we identify $A_{k,i}$ and the subset of $\mathbb{Z}[\zeta_{k+i-1}] \oplus A_{k,i-1}$ consisting of pairs (a,b) such that $f(a) = g(b)$ so φ is well defined. It is clear that φ is an injective group homomorphism. Let $N = N_{k,i-1}$ If $(a,b) \in A^*_{k,i}$ we can write $(a,b) = (a, N(a))(1, bN(a^{-1}))$ and define B as the subgroup of all elements $((1, bN(a^{-1}))$. All such elements lie in $A_{k,i}$ since $g(bN(a^{-1})) = g(b)g(N(a^{-1})) = g(b)f(a^{-1}) = 1 = f(1)$ □

Under the above injection we consider $\mathbb{Z}[\zeta_{k+i-1}]^*$ as a subset of $A^*_{k,i}$.

Lemma 4.10. $\ker(g_{k,i}|_{Z[\zeta_{k+i-1}]^*}) = \{\epsilon \in Z[\zeta_{k+i-1}]^* : \epsilon \equiv 1 \mod \lambda_{k+i-1}^{p^{k+i}-p^k}\}$

This is Theorem I.2.7 in [ST3] and the proof can be found there. For completeness we will give it here too.

Proof. Induction with respect to i. If $i = 1$ the statement is trivially true. If $i = 2$ we have the following pullback diagram

$$\begin{tikzcd} A_{k,2} \arrow[r, "i"] \arrow[d, "j"'] & \mathbb{Z}[\zeta_{k+1}] \arrow[d, "f"] \arrow[dl, "N_{k,1}"'] \\ A_{k,1} \arrow[r, "g"] & D_{k,1} \end{tikzcd}$$

Recall that $A_{k,1} = \mathbb{Z}[\zeta_k]$ and that $N = N_{k,1}$ is the usual norm. Suppose $g_{k,2}(\varphi(a)) = 1$, that is $(a, N(a)) \equiv 1 \mod p$ in $A_{k,2}$. This means that $a \equiv 1 \mod p$ in $\mathbb{Z}[\zeta_{k+1}]$, $N(a) \equiv 1 \mod p$ in $\mathbb{Z}[\zeta_k]$ and that $f(\frac{a-1}{p}) = g(\frac{N(a)-1}{p})$. Since the bottom triangle in the diagram commute, we get

$$N(\frac{a-1}{p}) \equiv \frac{N(a)-1}{p} \mod p.$$

Now observe that $a = 1+pt$ for some $t \in \mathbb{Z}[\zeta_{k+1}]$. By viewing N as a product of the automorphisms of $\mathbb{Q}[\zeta_{k+1}]$ it is easy to see that $N(a) = N(1+pt) \equiv 1+p\mathrm{Tr}(t)$ and since it is well known that p divides $\mathrm{Tr}(t)$ for all t, we get that $N(a) \equiv 1 \mod p^2$. This and the congruence above shows that $N(\frac{a-1}{p}) \equiv 0 \mod p$. By expressing $(a-1)/p$ as a sum $\sum_{j=0}^{\infty} a_j \lambda_{k+1}^j$ in the λ_{k+1}-adic completion of $\mathbb{Z}[\zeta_{k+1}]$, applying the norm and then evaluating in the λ_k-adic completion of $\mathbb{Z}[\zeta_k]$ we see that $(a-1)/p \equiv 0 \mod \lambda_{k+1}^{p^{k+1}-p^k}$ so $a \equiv 1 \mod \lambda_{k+1}^{p^{k+2}-p^k}$.

Now suppose the statement holds for $i-1 \geq 2$ and that $g_{k,i}(a, N_{k,i-1}(a)) = 1$. As in the case $i = 2$ this means that $a \equiv 1 \mod p$, $N_{k,i-1}(a) \equiv 1 \mod p$ and that $N_{k,i-1}(\frac{a-1}{p}) \equiv \frac{N_{k,i-1}(a)-1}{p}$. The diagram

$$\begin{tikzcd}
& \mathbb{Z}[\zeta_{k+i-1}] \arrow[dl, "\varphi_{k,i}"'] \arrow[dr, "\varphi_{k+1,i-1}"] & \\
A_{k,i} \arrow[rr] & & A_{k+1,i-1}
\end{tikzcd}$$

is commutative, so by the induction hypothesis we get that $a \equiv 1 \mod \lambda_{k+i-1}^{p^{k+i}-p^{k+1}}$.

Observe that if $c \equiv 0 \mod p$ in $A_{k,i}$ and c is represented by $(a_i, \ldots, a_m, \ldots, a_1)$ where $a_m \in \mathbb{Z}[\zeta_{k+m-1}]$ (we consider this an equality) then, as in the case $i = 2$, we have

$$N_{k,i-1}(\frac{a_i}{p}) - \frac{(a_{i-1}, \ldots, a_1)}{p} \equiv 0 \mod p$$

in $A_{k,i-1}$. If we repeat this argument and use lemma 3.9, we get

$$N_{k,i-2}\Bigl(\frac{\tilde{N}_{k+i-1,1}\bigl(\frac{a_i}{p}\bigr) - \frac{a_{i-1}}{p}}{p}\Bigr) - \frac{\bigl(\tilde{N}_{k+i-1,2}\bigl(\frac{a_i}{p}\bigr) - \frac{a_{i-3}}{p}, \ldots, \tilde{N}_{k+i-1,i-1}\bigl(\frac{a_i}{p}\bigr) - \frac{a_k}{p}\bigr)}{p} \equiv 0 \mod p$$

in $A_{k,i-2}$. This process can be repeated a number of times until we get a congruence in $A_{k,1} = \mathbb{Z}[\zeta_k]$. To get an expression for this last congruence we need to introduce some new notation. If $x \in \mathbb{Z}[\zeta_q]$ is divisible by p, let

$$\begin{aligned} T_q(x) &= \tilde{N}_{q,1}(\frac{x}{p}), \\ Q_q(x) &= \frac{\tilde{N}_{q,1}(x)}{p} \quad \text{and} \\ S_q(x) &= \frac{x}{p}. \end{aligned}$$

Let T_q^s and S_q^s be the obvious compositions of s maps T and S respectively, starting with T_q and S_q. Let $c = \varphi_{k,i}(a) - 1$ Then, remembering that all norm maps are additive modulo p, we get that the congruence in $\mathbb{Z}[\zeta_k]$ that follows from the congruence $c \equiv 1 \mod p$ in $A_{k,i}$, is

$$\begin{aligned} &T^{i-1}_{k+i-1}(a-1) + S^{i-1}_{k+i-1}(\tilde{N}_{k+i-1,i-1}(a)) + \\ &\qquad + \sum_{m=1}^{i-1} (-1)^m X^m_{k+i-1}(S^m_{k+i-1}(\tilde{N}_{k+i-1,m})) \equiv 0 \mod p. \end{aligned}$$

Here the maps X^m_{k+i-1} are compositions of appropriate maps T and Q using a total of $i-1-m$ maps.

Lemma 4.11. *Suppose $a \equiv 1 \mod p$. Then*

$$S^m_{k+i-1-m}(\tilde{N}_{k+i-1,m}(a) - 1) \equiv 0 \mod \lambda^{[(p^{k+i}-p^{k+1})/m]}_{k+i-1-m}$$

Proof. If we prove the statement for $m = 1$ the rest follows easily. In this case, for some t, we have $a = 1 + t\lambda^{p^{k+i}-p^{k+1}}_{k+i-1}$ and

$$\begin{aligned} \tilde{N}_{k+i-1,1}(a) &= \tilde{N}_{k+i-1,1}(1 + t\lambda^{p^{k+i}-p^{k+1}}_{k+i-1}) = \\ &= \tilde{N}_{k+i-1,1}(1 + t'\lambda^{p^{k+i-1}-p^k}_{k+i-2}) \equiv \\ &\equiv 1 + \operatorname{Tr}(t')\lambda^{p^{k+i-1}-p^k}_{k+i-2} \mod \lambda^{2(p^{k+i-1}-p^k)}_{k+i-2}. \end{aligned} \tag{4.1}$$

Since p divides $\operatorname{Tr}(t')$ we get that $(\tilde{N}_{k+i-1,1}(a) - 1)/p \equiv 0 \mod \lambda^{p^{k+i-1}-p^k}_{k+i-2}$ which is what we needed to prove. □

From this lemma and equation 4.1 we get $T^{i-1}_{k+i-1}(a-1) \equiv 0 \mod p$ in $\mathbb{Z}[\zeta_k]$. Moreover,

$$\begin{aligned} T(a-1) &= \tilde{N}_{k+i-1,1}\Big(\frac{t\lambda^{p^{k+i}-p^{k+1}}_{k+i-1}}{p}\Big) = \\ &= \tilde{N}_{k+i-1,1}(tu_1\lambda^{p^{k+i-1}-p^{k+1}}_{k+i-1}) = \\ &= \tilde{N}_{k+i-1,1}(tu_1)\lambda^{p^{k+i-1}-p^{k+1}}_{k+i-2}, \end{aligned}$$

for some unit u_1. If we repeat this $i-1$ times we, for some unit u_{i-1}, get $T^{i-1}_{k+i-1}(a-1) = \tilde{N}_{k+i-1,i-1}(tu_{i-1}) = \tilde{N}_{k+i-1,i-1}(t)$. This implies that $\lambda_{k+i-1}^{p^{k+1}-p^k}$ divides t so $\lambda_{k+i-1}^{p^{k+i}-p^k}$ divides $a-1$. This proves that

$$\ker(g_{k,i}|_{\mathbb{Z}[\zeta_{k+i-1}]^*}) \subseteq \{\epsilon \in \mathbb{Z}[\zeta_{k+i-1}]^* \,:\, \epsilon \equiv 1 \mod \lambda_{k+i-1}^{p^{k+i}-p^k}\}.$$

The opposite inclusion is trivial. □

Theorem 4.12. *Let p be a regular prime. Then*

$$\mathrm{Im}\{A^*_{0,n-1} \xrightarrow{g_{0,n-1}} D^*_{0,n-1}\} = \mathbb{F}_p^* \oplus < t > \oplus (\widetilde{D^*_{0,n-1}})^+.$$

Recall that t is defined as a generator of $D_{0,n-1}$ so $< t >$ is a cyclic group of order p^{n-1}.

Proof. By Lemma 4.7 and Lemma 4.8 we need only prove that

$$g_{0,n-1}(A^*_{0,n-1}) \supset (\widetilde{D^*_{0,n-1}})^+.$$

With $\mathbb{Z}[\zeta_{n-2}]$ considered as a subset of $A_{0,n-1}$ as before, we will show that we have

$$g_{0,n-1}((\mathbb{Z}[\zeta_{n-2}]^*)^+) \supseteq (\widetilde{D^*_{0,n-1}})^+.$$

For $m = 1, 2, \dots,$ define

$$\tilde{U}_m := \{\epsilon \in \mathbb{Z}[\zeta_{n-2}]^* \,:\, \epsilon \equiv 1 \mod \lambda_{n-2}^m\}.$$

It is clear that $\tilde{U}_1 \supseteq \tilde{U}_2 \supseteq \dots$ and that $\tilde{U}_1 = \mathbb{Z}[\zeta_{n-2}]^*$. Let $\tilde{U}_1^+$ be the subgroup of real units in $\tilde{U}_1$. Since $g_{0,n-1}$ commutes with complex conjugation we have $g_{0,n-1}(\tilde{U}_1^+) \subseteq (\widetilde{D^*_{0,n-1}})^+$. To prove the theorem it is obviously enough to show that we actually have equality. We will prove this statement with induction with respect to n, but we only use this in the very last part of the proof. First, by Lemma 4.10, we for any $n \geq 2$ have that $\ker(\tilde{U}_1^+ \xrightarrow{g} (\widetilde{D^*_{0,n-1}})^+) = \tilde{U}^+_{p^{n-1}-1}$. Hence

$$g_{0,n-1}(\tilde{U}_1^+) \cong \frac{\tilde{U}_1^+}{\tilde{U}^+_{p^{n-1}-1}}.$$

Since $g_{0,n-1}(\tilde{U}_1^+) \subset g_{0,n-1}((\mathbb{Z}[\zeta_{n-2}]^*)^+) \subset \widetilde{D^*_{0,n-1}})^+$ the group $\frac{\tilde{U}_1^+}{\tilde{U}^+_{p^{n-1}-1}}$ is finite. This shows that $|\frac{(\mathbb{Z}[\zeta_{n-2}]^*)^+}{\tilde{U}_1^+}|$ is finite since

$$|\frac{(\mathbb{Z}[\zeta_{n-2}]^*)^+}{\tilde{U}_1^+}||\frac{\tilde{U}_1^+}{\tilde{U}^+_{p^{n-1}-1}}| = |\frac{(\mathbb{Z}[\zeta_{n-2}]^*)^+}{\tilde{U}^+_{p^{n-1}-1}}|.$$

If $n = 2$, this and Dirichlet's theorem on units tells us that both $\tilde{U}_1^+$ and $\tilde{U}_{p^{n-1}-1}^+ = \tilde{U}_{p-1}^+$ are isomorphic to $\mathbb{Z}^{\frac{p-3}{2}}$. By the classical version of Kummer's lemma we get $\tilde{U}_{p-1}^+ = (\tilde{U}_1^+)^p$. Hence

$$\frac{\tilde{U}_1^+}{\tilde{U}_{p-1}^+} \cong \frac{\mathbb{Z}^{\frac{p-3}{2}}}{(p\mathbb{Z})^{\frac{p-3}{2}}} \cong C_p^{\frac{p-3}{2}}.$$

This shows that

$$|g_{0,1}(\tilde{U}_1^+)| = p^{\frac{p-3}{2}} = |(\widetilde{D_{0,1}^*})^+|$$

so we have proved our statement for $n = 2$.

Now fix $n > 2$ and assume the statement holds with n replaced by $n - 1$. We can write

$$|\frac{\tilde{U}_1^+}{\tilde{U}_{p^{n-1}-1}^+}| = |\frac{\tilde{U}_1^+}{\tilde{U}_{p^{n-2}-1}^+}||\frac{\tilde{U}_{p^{n-2}-1}^+}{\tilde{U}_{p^{n-2}+1}^+}||\frac{\tilde{U}_{p^{n-2}+1}^+}{\tilde{U}_{p^{n-1}-1}^+}| \tag{4.2}$$

By Dirichlet's theorem on units we have $(\mathbb{Z}[\zeta_{n-2}]^*)^+ \cong \mathbb{Z}^{\frac{p^{n-1}-p^{n-2}}{2}-1}$ Since all involved quotient groups are finite we get that $\tilde{U}_1^+$, $\tilde{U}_{p^{n-1}-1}^+$, $\tilde{U}_{p^{n-2}-1}^+$ and $\tilde{U}_{p^{n-2}+1}^+$ all are isomorphic to $\mathbb{Z}^{\frac{p^{n-1}-p^{n-2}}{2}-1}$. The rest of the proof is devoted to the analysis of the three right hand factors of 4.2.

By Theorem 2.7, Kummer's Lemma in the prime power case, we have $\tilde{U}_{p^{n-1}-1}^+ = (\tilde{U}_{p^{n-2}+1}^+)^p$ so

$$\frac{\tilde{U}_{p^{n-2}+1}^+}{\tilde{U}_{p^{n-1}-1}^+} \cong \frac{\mathbb{Z}^{\frac{p^{n-1}-p^{n-2}}{2}-1}}{(p\mathbb{Z})^{\frac{p^{n-1}-p^{n-2}}{2}-1}} \cong C_p^{\frac{p^{n-1}-p^{n-2}}{2}-1}.$$

This shows that

$$|\frac{\tilde{U}_{p^{n-2}+1}^+}{\tilde{U}_{p^{n-1}-1}^+}| = p^{\frac{p^{n-1}-p^{n-2}}{2}-1}.$$

We now turn to the second factor of the right hand side of 4.2. We will show that this number is p by finding a unit $\epsilon \notin \tilde{U}_{p^{n-2}+1}^+$ such that

$$< \epsilon >= \frac{\tilde{U}_{p^{n-2}-1}^+}{\tilde{U}_{p^{n-2}+1}^+}.$$

Since we know that the p-th power of any unit in $\tilde{U}_{p^{n-2}-1}^+$ belongs to $\tilde{U}_{p^{n-2}+1}^+$ this is enough. Let $\zeta = \zeta_{n-2}$ and $\eta := \zeta^{\frac{p^{n-1}+1}{2}}$. Then $\eta^2 = \zeta$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^{n-2}+1}-\eta^{-(p^{n-2}+1)}}{\eta-\eta^{-1}}$. Then $c(\epsilon) = \epsilon$ and

$$\begin{aligned} \epsilon = \eta^{-p^{n-2}} \frac{\eta^{2p^{n-2}+1} - \eta^{-1}}{\eta - \eta^{-1}} &= \eta^{-p^{n-2}} \frac{\eta^{2(p^{n-2}+1)} - 1}{\eta^2 - 1} = \\ &= \eta^{-p^{n-2}} \frac{\zeta^{p^{n-2}+1} - 1}{\zeta - 1} \in \mathbb{Z}[\zeta_{n-2}]^*. \end{aligned}$$

Now,

$$\frac{\zeta^{p^{n-2}+1}-1}{\zeta-1}=\zeta\frac{\zeta^{p^{n-2}}-1}{\zeta-1}+1$$

and for some $t_1\in\mathbb{Z}[\zeta]$ we have $(\zeta-1)^{p^{n-2}}=\zeta^{p^{n-2}}-1+pt_1$. With this in mind,

$$\begin{array}{rcl} \dfrac{\zeta^{p^{n-2}}-1}{\zeta-1} &=& \dfrac{(\zeta-1)^{p^{n-2}}}{\zeta-1}-\dfrac{pt_1}{\zeta-1}= \\ &=& (\zeta-1)^{p^{n-2}-1}-t_2\dfrac{(1-\zeta)^{p^{n-1}-p^{n-2}}}{1-\zeta}= \\ &=& (\zeta-1)^{p^{n-2}-1}+t_2(\zeta-1)^{p^{n-1}-p^{n-2}-1}, \end{array}$$

for some $t_2\in\mathbb{Z}[\zeta]$, and

$$\begin{array}{rcl} \dfrac{\zeta^{p^{n-2}+1}-1}{\zeta-1} &=& 1+(1+(\zeta-1))\big((\zeta-1)^{p^{n-2}-1}+(\zeta-1)^{p^{n-1}-p^{n-2}-1}t_2\big)= \\ &=& 1+(\zeta-1)^{p^{n-2}-1}+(\zeta-1)^{p^{n-2}}+(\zeta-1)^{p^{n-1}-p^{n-2}-1}t_3, \end{array}$$

for some $t_3\in\mathbb{Z}[\zeta]$. Similarly, for some $t_4\in\mathbb{Z}[\zeta]$,

$$\zeta^{p^{n-2}}=(1-(1-\zeta))^{p^{n-2}}=1+(1-\zeta)^{p^{n-2}}+p^{n-2}t_4$$

so for some $t_5\in\mathbb{Z}[\zeta]$,

$$\zeta^{-p^{n-2}}=1+(1-\zeta)^{p^{n-2}}+(1-\zeta)^{2p^{n-2}}t_5$$

and for some $t_6\in\mathbb{Z}[\zeta]$,

$$\eta^{-p^{n-2}}=(\zeta^{\frac{p^{n-1}+1}{2}})^{-p^{n-2}}=1+\frac{p^{n-1}+1}{2}(1-\zeta)^{p^{n-1}}+(1-\zeta)^{p^{n-2}+1}t_6.$$

From this, for some $t_7\in\mathbb{Z}[\zeta]$, we finally get that

$$\begin{array}{rcl} \epsilon &=& \eta^{-p^{n-2}}\dfrac{\zeta^{p^{n-2}+1}-1}{\zeta-1}= \\ &=& \big(1+\dfrac{p^{n-1}+1}{2}(1-\zeta)^{p^{n-1}}+(1-\zeta)^{p^{n-2}+1}t_6\big)\cdot \\ && \cdot\big(1+(\zeta-1)^{p^{n-2}-1}+(\zeta-1)^{p^{n-2}}+(\zeta-1)^{p^{n-1}-p^{n-2}-1}t_3\big)= \\ &=& 1-(1-\zeta)^{p^{n-2}-1}+(1-\zeta)^{p^{n-2}}t_7\notin\tilde{U}^+_{p^{n-2}+1}. \end{array}$$

To show that ϵ generates $\frac{\tilde{U}^+_{p^{n-2}-1}}{\tilde{U}^+_{p^{n-2}+1}}$ it is enough to show that for any $a\in\tilde{U}^+_{p^{n-2}-1}$ there is $b\in\tilde{U}^+_{p^{n-2}+1}$ and $k\in\mathbb{Z}$ such that $a=\epsilon^k b$. First recall that $\epsilon\equiv-1 \mod (1-\zeta)^{p^{n-2}-1}$ is equivalent to $\epsilon\equiv-1 \mod (\zeta-\zeta^{-1})^{p^{n-2}-1}$ so we can write $\epsilon=1-(\zeta-\zeta^{-1})^{p^{n-2}-1}+\dots$. For $k=0,1,2,\dots,p-1$ we have $\epsilon^k=1-k(\zeta-\zeta^{-1})^{p^{n-2}-1}+\dots$. Now take arbitrary $a=1+a_{p^{n-2}-1}(\zeta-\zeta^{-1})^{p^{n-2}-1}+\dots\in$

$\tilde{U}^+_{p^{n-2}-1}$. Write $a_{p^{n-2}-1} = a'_{p^{n-2}-1} + pt$, where $-(p-1) \geq a'_{p^{n-2}-1} \geq 0$. Choose $k = a'_{p^{n-2}-1}$ and $b = a\epsilon^k$. Then

$$\begin{aligned} b &= (1 + a_{p^{n-2}-1}(\zeta - \zeta^{-1})^{p^{n-2}-1} + \dots) \cdot \\ &\quad \cdot (1 - k(\zeta - \zeta^{-1})^{p^{n-2}-1} + \dots) = \\ &= 1 + pt(\zeta - \zeta^{-1})^{p^{n-2}} + \dots . \end{aligned}$$

Since b is clearly a real unit this means $b \in \tilde{U}^+_{p^{n-2}+1}$ which is what we wanted to show. Our conclusion is that

$$\left|\frac{\tilde{U}^+_{p^{n-2}-1}}{\tilde{U}^+_{p^{n-2}+1}}\right| = p.$$

We now turn to

$$\left|\frac{\tilde{U}^+_1}{\tilde{U}^+_{p^{n-2}-1}}\right|.$$

Consider the commutative diagram

$$\begin{tikzcd} & \mathbb{Z}[\zeta_{n-2}]^* \arrow[dl, "N_{0,n-2}"'] \arrow[d, "f_{0,n-2}"] \\ A^*_{0,n-2} \arrow[r, "g_{0,n-2}"] & D^*_{0,n-2} \end{tikzcd}$$

Let $\tilde{W}_m := \{\epsilon \in \mathbb{Z}[\zeta_{n-3}] \, : \, \epsilon \equiv 1 \mod \lambda^m_{n-3}\}$. It is clear that $f_{0,n-2}(\tilde{U}^+_1) \subseteq (\widetilde{D^*_{0,n-2}})^+$ and that $g_{0,n-2}(\tilde{W}^+_1) \subseteq (\widetilde{D^*_{0,n-2}})^+$. Recall that $A^*_{0,n-2} \cong \mathbb{Z}[\zeta_{n-3}]^* \oplus B$ and that the norm map $N_{0,n-2}$ acts like the usual norm map $N = \tilde{N}_{n-2,1} : \mathbb{Z}[\zeta_{n-2}]^* \to \mathbb{Z}[\zeta_{n-3}]^*$. It is well known that $N(\zeta_{n-2}) = \zeta_{n-3}$. By finding the constant term of the minimal polynomial $(x-1)^p - \zeta_{n-3}$ of λ_{n-2} we see that $N(\lambda_{n-2}) = \lambda_{n-3}$ and by a similar argument that $N(\zeta^k_{n-2} - 1) = \zeta^k_{n-3} - 1$ when $(k,p) = 1$. Since N is additive modulo p we get that $N_{0,n-2}(\tilde{U}^+_1) \subseteq \tilde{W}^+_1$. Hence we have a commutative diagram

$$\begin{tikzcd} & \tilde{U}^+_1 \arrow[dl, "N"'] \arrow[d, "f"] \\ \tilde{W}^+_1 \arrow[r, "g"] & (\widetilde{D^*_{0,n-2}})^+ \end{tikzcd}$$

We want to show that N is surjective. In $\mathbb{Z}[\zeta_j]$, let $w_j := -\zeta_j^{\frac{p^{j+1}+1}{2}}$ and consider

$$\gamma_{j,l} := \frac{w^l_j - w^{-l}_j}{w_j - w^{-1}_j}.$$

If we fix $\zeta_j = e^{(2\pi\sqrt{-1}/p^{j+1})}$ we see that

$$\gamma_{j,l} := \frac{\sin(l\pi/p^{j+1})}{\sin(\pi/p^{j+1})}$$

and hence real. Moreover,

$$\gamma_{j,l} = w^{-l+1}\frac{\zeta_j^l - 1}{\zeta_j - 1}$$

so when $(l,p) = 1$, $\gamma_{j,l}$ are units. Let J_j be the group of positive real units in $\mathbb{Z}[\zeta_j]$ and let $J_{0,j}$ be the subgroup generated by $\gamma_{j,l}$, $l = 2,3,\dots,(p^{j+1} - 1)/2$ $(l,p) = 1$. This is a well known construction and the details can be found in [W] p 144. Since $\gamma_{j,l}$ is real, it is congruent to a rational integer a mod (λ_j^2). Off course, $a \not\equiv 0 \mod (p)$. Hence $a^{p-1} = 1 \mod (p)$ and this shows that $\gamma_{j,l}^{p-1} \equiv 1 \mod \lambda_j$. With $j = n-2$ this shows that $\gamma_{n-2,l}^{p-1} \in \tilde{U}_1^+$ and with $j = n-3$ that $\gamma_{n-3,l}^{p-1} \in \tilde{W}_1^+$. Now, a straightforward calculation shows that $N(\gamma_{n-2,l}^{p-1}) = \gamma_{n-3,l}^{p-1}$ so $J_{0,n-2}^{p-1} \subset N(\tilde{U}_1^+)$. Let h^+ be the class number of $\mathbb{Q}(\zeta_{n-3})^+$. It is well known that $h^+ | h_{\mathbb{Q}(\zeta_{n-3})}$. Since p is regular we get that $(p, h^+) = 1$. By Theorem 8.2 on p. 145 of [W] we have

$$|\frac{J_{n-3}}{J_{0,n-3}}| = h^+.$$

Now take arbitrary $\epsilon \in \tilde{W}_1^+$. Then ϵ^2 is positive and hence an element of J_{n-3}. By the fact above there exists $s \in \mathbb{Z}$ such that $(s,p) = 1$ and $e^{2s} \in J_{0,n-3}$. This means that $e^{2s(p-1)} \in N(\tilde{U}_1^+)$. Since $(2s(p-1), p) = 1$ we can find $u, v \in \mathbb{Z}$ such that $2s(p-1)u + pv = 1$ so $\epsilon = \epsilon^{2s(p-1)u+pv} = (\epsilon^{2s(p-1)})^u(\epsilon^p)^v \in N(\tilde{U}_1^+)$. This shows that N is surjective.

We will now use our inductive assumption. This means that $g(\tilde{W}_1^+) = (\widetilde{D_{0,n-2}^*})^+$, that is, the map g is surjective. But since the diagram above is commutative this implies that f is also surjective. It is easy to see that $\ker(f) = \tilde{U}_{p^{n-2}-1}^+$ so

$$\frac{\tilde{U}_1^+}{\tilde{U}_{p^{n-2}-1}^+} \cong (\widetilde{D_{0,n-2}^*})^+$$

and

$$|\frac{\tilde{U}_1^+}{\tilde{U}_{p^{n-2}-1}^+}| = |(\widetilde{D_{0,n-2}^*})^+| = p^{\frac{p^{n-2}-3}{2}}.$$

This finally gives

$$|\frac{\tilde{U}_1^+}{\tilde{U}_{p^{n-1}-1}^+}| = p^{\frac{p^{n-2}-3}{2}} \cdot p \cdot p^{\frac{p^{n-1}-p^{n-2}}{2}-1} = p^{\frac{p^{n-1}-3}{2}}.$$

Hence $|g_{0,n-1}(\tilde{U}_1^+)| = |\widetilde{D_{0,n-1}^*})^+|$ and this proves the theorem. □

Proof of Theorem 4.2. Apply Proposition 4.4 and Theorem 4.12 to the exact sequence

$$0 \to \frac{D^*_{0,n-1}}{\operatorname{Im}\{\mathbb{Z}[\zeta_{n-1}]^* \oplus A^*_{0,n-1} \to D^*_{0,n-1}\}} \to \operatorname{Pic} A_{0,n} \to$$

$$\to \operatorname{Cl} \mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic} A_{0,n-1} \to 0.$$

□

References

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

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

[B-S] Borevich, Z.I. and Shafarevich, I.R, *Number theory.*
Academic Press: London and New York, 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

[J] Janusz, Gerald J, *Algebraic Number Fields, Second Edition*
American Mathematics Society, 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, Serge, *Algebra, Third Edition*
Addison-Wesley, 1993.

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

[Rim] Rim, D.S., *Modules over Finite Groups*
Annals of Mathemathica 69 (1959), 700-712.

[R] Rotman, Joseph J., *An Introduction to Homological Algebra*
Academic Press, 1979.

[S] Serre, Jean-Pierre, *Local Fields*
Springer-Verlag, 1979.

[Si] Silvester, John R., *Introduction to Algebraic K-Theory*
Chapman and Hall, 1981.

[ST1] Stolin, Alexander. *An Explicit Formula for the Picard Group of the Cyclic Group of Order p^2.*
Proceedings of the American Mathematical Society, Vol. 121 (1994), 375-383.

[ST2] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Rings Close to It.*
Proc. of the 2nd Int. Conf in Comm. Alg. 1997, 443-455.

[ST3] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Certain Galois Groups.*
Journal of Number Theory 72, 1998, 28-66.

[W] Washington, Lawrence C, *Introduction to Cyclotomic Fields*
Springer Verlag, 1997.