On the Structure of Residue Rings of Prime Ideals in Algebraic Number Fields – Part II: Ramified Primes

Michele Elia
Politecnico di Torino
Corso Duca degli Abruzzi 24
I-10129 Torino, Italy
elia@polito.it

J. Carmelo Interlando
Department of Mathematics & Statistics
San Diego State University, San Diego, CA, USA
carmelo.interlando@sdsu.edu

Ryan Rosenbaum
Department of Mathematics & Statistics
San Diego State University, San Diego, CA, USA
rosenbaum.ryan@gmail.com

Abstract

The explicit description of the additive and multiplicative structures of rings of residues in maximal orders of number fields is useful both in theory and practice. This is the second and last part of a survey intended to offer a full description of those structures in the style of the theory of rings with identity as given by Bernard R. McDonald. The topic of this companion paper concerns the structure of quotient rings of maximal orders of algebraic number fields by powers of ramified prime ideals.

Mathematics Subject Classification: 11R16, 11-04, 11Txx

Keywords and phrases: Remainder rings, Ideals, Algebraic number fields, Ramification
1 Introduction

The objective of this companion paper of [9] is to present a survey of the structures of quotient rings of maximal orders in algebraic number fields by powers of ramified prime ideals. The style maintains the approach, already taken in [9], to the theory of rings with identity as presented in McDonald’s book. The same notations and preliminaries of [9] are assumed. Furthermore, the following notions will be useful to expedite the arguments since the results are described in the unavoidable framework and language of ideals, as we did only partially in [9]. The usual approach with ideals allows us to deal also with non-principal ideals as moduli, however the arithmetics is more costly than in the case of ideals in \( \mathbb{Z} \), see [5, pp. 94–95]. Furthermore, some information is lost in the common representation of the remainders as field elements. To overcome this issue, we adopt a representation of the algebraic field elements that allows us to partially recover lost information and element properties with respect to prime ideal moduli.

Let \( \mathbb{F} \) be an extension field of the rational field \( \mathbb{Q} \) by a root \( \alpha \) of an irreducible polynomial \( \text{irr}(\alpha, \mathbb{Q}) \) of degree \( n \). A principal ideal \( b \) of \( \mathcal{O}_\mathbb{F} \) is defined as the set of multiples of a fixed element \( \beta \in \mathcal{O}_\mathbb{F} \)

\[
    b = \{ \beta \varsigma : \varsigma \in \mathcal{O}_\mathbb{F} \}
\]

It is customary to identify a principal ideal \( g \) of \( \mathbb{F} \) by a field element \( \gamma \) and write \( g = (\gamma) \). The product of principal ideals is simply defined as \( bg = (\beta)(\gamma) = (\beta\gamma) \). A non-principal ideal \( \mathfrak{J} \) of \( \mathcal{O}_\mathbb{F} \) is defined as

\[
    \mathfrak{J} = \{ \beta \varsigma_1 + \gamma \varsigma_2 : \varsigma_1, \varsigma_2 \in \mathcal{O}_\mathbb{F} \},
\]

and represents the greatest common divisor of \( \beta \) and \( \gamma \), which may be not an element of \( \mathcal{O}_\mathbb{F} \) [7]. The product of two ideals \( \mathfrak{J} \) and \( \mathfrak{I} \) is defined as

\[
    \mathfrak{J}\mathfrak{I} = \left\{ \sum_{i=1}^{m} \beta_i \gamma_i : \beta_i \in \mathfrak{J}, \gamma_i \in \mathfrak{I}, m \in \mathbb{Z}^+ \right\}.
\]

The ring \( \mathcal{O}_\mathbb{F} = (1) \) is a principal ideal that plays the role of product identity. An ideal \( \mathfrak{p} \neq (1) \) is called prime if whenever \( \mathfrak{p} = ab \) with \( a \) and \( b \) ideals, then either \( a = (1) \) or \( b = (1) \). Every ideal \( \mathfrak{J} \) can be uniquely decomposed into the product of powers of prime ideals [7]

\[
    \mathfrak{J} = \prod_{j=1}^{s} \mathfrak{p}_j^{n_j}.
\]

Thus, every principal ideal \( (\beta) \) which is not prime can be decomposed into the product \( (\beta) = bc \) of at least two principal or non-principal ideals. We adopt
the convention of writing $\beta = bc$ as a representation of $\beta$, and use $\beta$ or $bc$ interchangeably.

Addition $\hat{+}$ of ideals $J$ and $I$ is defined as

$$J \hat{+} I = \{ \beta + \gamma : \beta \in J, \gamma \in I \},$$

which is the greatest common divisor between the ideals $J$ and $I$ [16, vol II, p. 65, Theorem 2.25]. We remark that as a consequence of the representation of elements of $\mathcal{O}/B_Y$ by ideals, if $(\beta) = ab$ and $(\gamma) = ac$, then $(\beta + \gamma) = af$, thus the following algebra is consistent

$$(\beta + \gamma) = ab + ac = a(b + c) = af,$$

where the formal sum $b + c$ of ideals simply tells us that the factorization of the principal ideal $(\beta + \gamma)$ contains, besides the common factor $a$ of $\beta$ and $\gamma$, an ideal $f$. This notation introduced for the elements of $\mathcal{O}/B_Y$ has the advantage of explicitly showing when an element $\beta$ of the order is divisible by some ideal, principal or not. As a final notational remark, a cyclic group of order $M$ and generated by $g$ will be denoted as $(g)_M$.

**Example 1.** The quadratic number field $\mathbb{Q} (\sqrt{15})$ has class number 2, fundamental unit $4 + \sqrt{15}$, and integral basis $\{1, \sqrt{15}\}$. The principal ideals of the rational primes 2, 3, and 5 ramify, and the respective prime factors $p_2 = (2, 1 + \sqrt{15})$, $p_3 = (3, \sqrt{15})$ and $p_5 = (5, \sqrt{15})$ are non-principal ideals. Also the principal ideal $(7)$ splits into non-principal ideals

$$(7) = p_7 \bar{p}_7 = (7, 9 + 2\sqrt{15})(7, 9 - 2\sqrt{15})$$

where the overbar denotes conjugation by the Galois automorphism.

It is easily checked that the principal ideals $(9 + 2\sqrt{15})$ and $(1 + \sqrt{15})$ split into non-principal factor ideals as $p_7 p_3$ and $p_7 p_2$, respectively. According to our convention, we write $p_7 p_3$ and $p_7 p_2$ for $9 + 2\sqrt{15}$ and $1 + \sqrt{15}$, respectively. Thus, we may immediately see that the algebraic integer $10 + 3\sqrt{15}$, which is the sum of $9 + 2\sqrt{15}$ and $1 + \sqrt{15}$, generates a principal ideal $(10 + 3\sqrt{15})$ which splits as $p_7 f$, with $f = p_5$. Note that we may predict only the norm of $f$ which in our case is $N_F(p_7) = -35/7 = -5$.

The paper organization is as follows. Section 2 presents a description of residue rings modulo powers of prime ideals above a rational prime $p$ in algebraic number fields that do not contain a $p$-th root of unity. Section 3 presents a description of residue rings modulo powers of prime ideals of algebraic number fields that contain a $p$-th root of unity. Lastly, Section 4, presents a set of examples concerning residue rings of ramified prime ideals, and a summary, consisting of several tables, of the structures described in this paper and in [9].
2 The Structure of \( \mathfrak{Z}(\mathfrak{P}^a) \) for Ramified \( \mathfrak{P} \)

Let \( p \) be a rational prime and \( \mathfrak{P} \) be a prime factor of the principal ideal \((p)\) of the maximal order \( \mathfrak{O}_\mathcal{F} \) that has ramification index \( e \geq 2 \). The ring of residues modulo a power \( \mathfrak{P}^a \) is denoted by \( \mathfrak{Z}(\mathfrak{P}^a) \), and our aim is to describe the module structure of the additive group \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \), and the multiplicative group structure of the group of units \( \mathfrak{Z}(\mathfrak{P}^a)^{(\times)} \). In particular, it is convenient to have a description of both \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) and \( \mathfrak{Z}(\mathfrak{P}^a)^{(\times)} \) as free abelian groups, especially in view of numerical computations.

Precisely, this section describes the additive group \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) for every ramified prime ideal \( \mathfrak{P} \) in \( \mathcal{F} \). It is worthwhile to observe that the structure of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) does not depend on any particular subfield contained in \( \mathcal{F} \). On the other hand, the multiplicative group \( \mathfrak{Z}(\mathfrak{P}^a)^{(\times)} \) of units of \( \mathfrak{Z}(\mathfrak{P}^a) \) is different depending whether \( \mathcal{F} \) includes the cyclotomic field \( \mathbb{Q}(\zeta_p) \), with \( \zeta_p \) a primitive \( p \)-th complex root of unity. This section describes the structures of \( \mathfrak{Z}(\mathfrak{P}^a)^{(\times)} \) in fields \( \mathcal{F} \) that do not contain a \( p \)-root of unity, leaving to the next section the case of fields \( \mathcal{F} \) that include a \( p \)-th root of unity.

Leaders of coset ideals of \( \mathfrak{P}^a \) that are of the form \( 1 + \theta a^j \mathfrak{P}^j \), \( 1 \leq j < a \), where \( \theta \in \mathfrak{O}_\mathcal{F} \), \( a \) is an ideal of \( \mathfrak{P}_\mathcal{F} \) that is not divisible by \( \mathfrak{P} \), and \( a \mathfrak{P} \) is a principal ideal \([7]\), are called one-units. Here, \( a^j \mathfrak{P}^j \) is to be regarded as a generator of the principal ideal \((a \mathfrak{P})^j \). Note that \( 1 + \theta a^j \mathfrak{P}^j \) may be not a unit of the order (i.e., an integer of norm equal to \( \pm 1 \)), but it is certainly a unit in the set of remainders modulo \( \mathfrak{P}^a \). In other contexts, see \([11, p. 213]\), one-units are elements of the order of the form \( 1 + \beta \pi \), with \( \beta \in \mathfrak{O}_\mathcal{F} \) and \( \pi \in \mathfrak{P} \), whose field norm is equal to \( \pm 1 \). Furthermore, let \( \Omega = \{\omega_1, \ldots, \omega_n\} \) denote an integral basis for \( \mathcal{F} \). Subsets of \( \mathcal{U} = \{1 + \omega_i a^j \mathfrak{P}^j : \; i = 1, \ldots n, \; j = 1, \ldots a - 1\} \) will be used later on to build free bases for \( \mathfrak{Z}(\mathfrak{P}^a)^{(\times)} \).

2.1 The abelian free group \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \)

If \( a = 1 \), the ring \( \mathfrak{Z}(\mathfrak{P}) \) is a field, a structure that does not require any further discussion, thus only \( a \geq 2 \) will be considered. For every \( e \geq 2 \) define \( t, r \), and \( m \) as follows:

\[
t = \min\{a, e\} \quad , \quad r = a \mod t \quad , \quad m = \frac{a - r}{t} \quad .
\]

Finally, as a notational remark, the symbol \( \bigoplus_{i=r_1}^{r_2} \) is used to denote a direct sum of modules, with the convention that the sum is the zero-module \( \mathbb{Z}_1 = \{0\} \) whenever \( r_1 > r_2 \).

**Theorem 1.** Let \( p \) be a rational prime and \( \mathfrak{P} \) a prime ideal of \( \mathfrak{O}_\mathcal{F} \) above \( (p) \) with ramification index \( e > 1 \) and inertia index \( f \). Let \( \alpha_a \) be a root of an \( f \)-degree irreducible polynomial \( m_f(x) \) modulo \( \mathfrak{P}^a \), where \( m_f(x) \) is the irreducible
factor of \(\text{irr}(\alpha, \mathbb{Q})\) modulo \(p\) that corresponds to \(\mathfrak{P}\) in the Kummer-Dedekind’s correspondence. Let \(\mathfrak{c}\) be an ideal relatively prime with \(\mathfrak{P}\) such that \(\mathfrak{c}\mathfrak{P}\) is a principal ideal \([7, p. 130]\). The set \(\alpha_a^j \mathfrak{c}^j\mathfrak{P}^i\), \(0 \leq j \leq f - 1\), \(0 \leq i \leq t\) is a free basis for the additive group \(\mathfrak{I}(\mathfrak{P}^a)^{(+)}\). The latter is isomorphic to an abelian \(p\)-group of rank \(f \cdot t\), and its elements can be written as

\[
\sum_{i=0}^{r-1} \left( \sum_{j=0}^{t-1} x_{ij} \alpha_a^j \right) \mathfrak{c}^i \mathfrak{P}^i + \sum_{i=r}^{f-1} \left( \sum_{j=0}^{t-1} z_{ij} \alpha_a^j \right) \mathfrak{c}^i \mathfrak{P}^i \quad x_{ij}, z_{ij} \in \mathbb{Z}_{p^{m+1}}, \quad \alpha_a^j, \quad \mathfrak{c}^i \mathfrak{P}^i
\]

where, as before, \(\mathfrak{c}\mathfrak{P}\) is to be regarded as the generator of the principal ideal.

**Proof.** The additive structure \(\mathfrak{I}(\mathfrak{P}^a)^{(+)}\) of \(\mathfrak{I}(\mathfrak{P}^a)\) is not that of an additive cyclic group for every \(e \geq 2\) and every \(a \geq 2\). Let \(\mathfrak{L}\) denote the ideal that includes all prime ideals that are different from \(\mathfrak{P}\) and are above \(p\); actually, the ideal factorization \((p) = \mathfrak{P}^e \mathfrak{L}\) implies \(p\theta = 0 \mod \mathfrak{P}^e\) for every \(\theta\) in \(\mathfrak{L}\), thus \(\mathfrak{I}(\mathfrak{P}^a)^{(+)}\) is not a cyclic group for every \(a \geq 2\) and \(a \leq e\). The same is true for every \(a > e\) because the chain of equalities

\[
(p)^{m+1} = \mathfrak{P}^{e(m+1)} \mathfrak{L}^{m+1} = \mathfrak{P}^{em+e} \mathfrak{L}^{m+1} = \mathfrak{P}^{a+e-r} \mathfrak{L}^{m+1}
\]

shows that \((p)^{m+1} = (0) \mod \mathfrak{P}^e\) since \(e > r\), thus \(p^{m+1} \theta = 0 \mod \mathfrak{P}^a\) and \(m+1 < a\). This observation also shows that any cyclic subgroup of \(\mathfrak{I}(\mathfrak{P}^a)^{(+)}\) has order less than or equal to \(p^{m+1}\).

For demonstration purposes, it is convenient to deal with \(f = 1\) and \(f > 1\) separately.

**\(f = 1\) and \(a \geq 2\).** \(\mathfrak{I}(\mathfrak{P}^a)^{(+)}\) is isomorphic to a direct sum of \(t\) cyclic groups because its elements can be represented as

\[
\sum_{i=0}^{r-1} x_i \mathfrak{c}^i \mathfrak{P}^i + \sum_{i=r}^{f-1} z_i \mathfrak{c}^i \mathfrak{P}^i \quad x_i, z_i \in \mathbb{Z}_{p^{m+1}}, \quad \mathfrak{c}^i \mathfrak{P}^i
\]

This expression is motivated by the following assertions:

1. The number 1 generates a group isomorphic to \(\mathbb{Z}_{p^{m+1}}\) because \(\mathfrak{P}^a\) divides the principal ideal \((p^{m+1})\), but it does not divide the ideal \((p^a)\).

2. Let \(x + c\) be the factor of \(\text{irr}(\alpha, \mathbb{Q})\) modulo \(p\) that is associated to \(\mathfrak{P}\) by the correspondence of Kummer-Dedekind’s, thus the principal ideal \((\alpha + c)\) is strictly divisible by \(\mathfrak{P}\), that is, \((\alpha + c) = c\mathfrak{P}\) and \((\alpha + c)^e\) is strictly divisible by \(\mathfrak{P}^e\). Hence, the set \(\{1, \alpha + c, \ldots, (\alpha + c)^{r-1}\}\) is a basis of a free-group \(M_1\) of rank \(r\) over \(\mathbb{Z}_{p^{m+1}}\) which is a subgroup of \(\mathfrak{I}(\mathfrak{P}^a)^{(+)}\); clearly, \(M_1\) is a direct sum of \(r\) cyclic groups of order \(p^{m+1}\).
3. The set \( \{(\alpha + c)^r, \ldots, (\alpha + c)^{t-1}\} \) is a basis of a free-group \( \mathbb{M}_2 \) of rank \( t - r \) over \( \mathbb{Z}_{p^m} \) which is a subgroup of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \); clearly, \( \mathbb{M}_2 \) is a direct sum of \( t - r \) cyclic groups of order \( p^m \).

The conclusion is immediate after observing that the group \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) is a direct sum of \( \mathbb{M}_1 \) and \( \mathbb{M}_2 \) which have only the element 0 in common, and their respective cardinality \( p^{(m+1)r} \) and \( p^{m(t-r)} \) imply that the order of their direct sum is \( p^{(m+1)r}p^{m(r-t)} = p^{mt+r} = p^a \), i.e. the order of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \).

### 3. The set \( \{(\alpha + c)^r, \ldots, (\alpha + c)^{t-1}\} \) is a basis of a free-group \( \mathbb{M}_2 \) of rank \( t - r \) over \( \mathbb{Z}_{p^m} \) which is a subgroup of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \); clearly, \( \mathbb{M}_2 \) is a direct sum of \( t - r \) cyclic groups of order \( p^m \).

The conclusion is immediate after observing that the group \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) is a direct sum of \( \mathbb{M}_1 \) and \( \mathbb{M}_2 \) which have only the element 0 in common, and their respective cardinality \( p^{(m+1)r} \) and \( p^{m(t-r)} \) imply that the order of their direct sum is \( p^{(m+1)r}p^{m(r-t)} = p^{mt+r} = p^a \), i.e. the order of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \).

\[ f \geq 2 \text{ and } a \geq 2. \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \text{ is isomorphic to a direct sum of } f \cdot t \text{ cyclic groups because its elements can be represented as } \]

\[
\sum_{i=0}^{r-1} \left[ \sum_{j=0}^{f-1} x_{ij} \alpha_a^j \right] c_i \mathfrak{P}^i + \sum_{i=r}^{t-1} \left[ \sum_{j=0}^{t-1} z_{ij} \alpha_a^j \right] c_i \mathfrak{P}^i \quad x_{ij} \in \mathbb{Z}_{p^{m+1}} \quad z_{ij} \in \mathbb{Z}_{p^m}.
\]

This expression is motivated by the following assertions:

1. The number 1 generates the group \( \mathbb{Z}_{p^{m+1}} \) as explained in the case \( f = 1 \).

2. Assume that \( m_f(x) \) is the \( f \)-degree irreducible factor of \( \text{irr}(\alpha, \mathcal{Q}) \) modulo \( p \), which is possible by Lemma 2 in [9, pp. 2803–2804]. The factor is associated to \( \mathfrak{P} \) by the Kummer-Dedekind correspondence. The principal ideal \( (m_f(\alpha)) \) is strictly divisible by \( \mathfrak{P} \), and \( (m_f(\alpha))^e \) is strictly divisible by \( \mathfrak{P}^e \).

3. Let \( \alpha_1 \) be a root of \( m_f(x) \) mod \( \mathfrak{P} \). Then the correspondence \( \ell(\alpha) = \alpha_1 \) defines a linear labelling [12] of the elements of \( \mathbb{O}_\mathfrak{P} \) and establishes an isomorphism between \( \mathfrak{Z}(\mathfrak{P}) \) and \( \text{GF}(p^f) \). The set \( \Lambda = \{1, \alpha_1, \ldots, \alpha_1^{f-1}\} \) is a free basis for \( \mathfrak{Z}(\mathfrak{P})^+, \) but its lifted version is not a complete free basis for \( \mathfrak{Z}(\mathfrak{P}^a)^+ \) as in the case of unramified primes.

4. The principal ideal \( (m_f(\alpha)) \) is strictly divisible by \( \mathfrak{P} \), that is, \( (m_f(\alpha)) = c \mathfrak{P} \), with \( c \) relatively prime with \( \mathfrak{P} \), whence \( (m_f(\alpha))^e \) is strictly divisible by \( \mathfrak{P}^e \). It follows that \( \{1, (m_f(\alpha)), \ldots, ((m_f(\alpha)))^{r-1}\} \) is a set of \( r \) independent elements which together with a lifted version of \( \Lambda \) define a basis of a free-group \( \mathbb{M}_1 \) of rank \( fr \) over \( \mathbb{Z}_{p^{m+1}} \). \( \mathbb{M}_1 \) is a subgroup of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) and also a direct sum of \( fr \) cyclic groups of order \( p^{m+1} \), that is,

\[
\mathbb{M}_1 = \sum_{i=0}^{r-1} \left[ \sum_{j=0}^{f-1} x_{ij} \alpha_a^j \right] c_i \mathfrak{P}^i \quad \forall \quad x_{ij} \in \mathbb{Z}_{p^{m+1}}.
\]

where \( \alpha_a \) modulo \( \mathfrak{P}^a \) is a lifted version of \( \alpha_1 \) modulo \( \mathfrak{P} \).
5. The set \( \{ (m_f(\alpha))^t, \ldots, (m_f(\alpha))^{t-1} \} \) consists of \( t - r \) independent elements that, together with a lifted version of \( \Lambda \), define a basis of a free-group \( \mathbb{M}_2 \) of rank \( f(t - r) \) over \( \mathbb{Z}_{pm} \). \( \mathbb{M}_2 \) is a subgroup of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) and a direct sum of \( f(t - r) \) cyclic groups of order \( p^m \). That is,

\[
\mathbb{M}_2 = \sum_{i=r}^{t-1} \left( \sum_{j=0}^{f-1} z_{ij} \alpha^j \right) \mathfrak{P}^i \quad \forall \ z_{ij} \in \mathbb{Z}_{pm}
\]

is a free-group of rank \( f(t - r) \) over \( \mathbb{Z}_{pm} \); clearly \( \mathbb{M}_2 \) is a direct sum of \( ft - fr \) cyclic groups that are isomorphic to \( \mathbb{Z}_{pm} \).

As in the case \( f = 1 \), the conclusion is immediate after observing that the group \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \) is a direct sum of the groups \( \mathbb{M}_1 \) and \( \mathbb{M}_2 \), since both groups have only the element 0 in common, and the product of their cardinality \( p^{(m+1)fr} \) and \( p^{m(ft - fr)} \) is \( p^{fa} \), the order of \( \mathfrak{Z}(\mathfrak{P}^a)^{(+)} \).

Example 2. Let \( \mathbb{F} = \mathbb{Q}(\alpha) \) be the extension field of degree 4, where \( \alpha \) is a root of the polynomial \( f(x) = x^4 - 2x^3 - 13x^2 + 14x + 19 \). An integral basis for \( \mathfrak{D}_\mathbb{F} \) is \( \{ b_0, b_0, b_1, b_3 \} \) where \( b_i = \alpha^i, i = 0, 1, 2, \) and \( b_3 = (\alpha^3 + 8\alpha^2 + 10\alpha)/19 \). The rational prime 3 ramifies with inertia index 2, thus \( (3) = \mathfrak{P}_3 \), with \( \mathfrak{P}_3 = (3b_0 + 8b_1 + 3b_2 - 7b_3) \). The polynomial \( f(x) \) splits modulo 3 as \( (x^2 + 2x + 2)^2 \).

Let \( \alpha_2 \) be a root of \( x^2 + 2x + 2 \) modulo \( \mathfrak{P}_3^2 \).

The ring \( \mathfrak{Z}(\mathfrak{P}_3^2) \) has order \( (3^2)^2 = 81 \) and can be identified with \( \mathfrak{Z}(3) \). A basis for \( \mathfrak{Z}(3)^{(+)} \) is \( \mathcal{B} = \{ 1, \alpha_2, \mathfrak{P}_3, \alpha_2 \mathfrak{P}_3 \} \). Thus, the elements of \( \mathfrak{Z}(3) \) are

\[
x_1 + x_2 \alpha_2 + z_1 \mathfrak{P}_3 + z_2 \alpha_2 \mathfrak{P}_3 \quad \forall x_1, x_2, z_1, z_2 \in \mathbb{Z}_3
\]

In this particular case \( \mathfrak{Z}(3) \) is clearly a \( \mathbb{Z}_3 \)-module. The ring \( \mathfrak{Z}(\mathfrak{P}_3^3) \) is a \( \mathbb{Z}_9 \)-module because the basis is obtained by replacing \( \alpha_2 \) with \( \alpha_3 \) in \( \mathcal{B} \). Although the representation is not unique [6, p. 11], the \( (3^2)^3 = 729 \) elements in \( \mathfrak{Z}(\mathfrak{P}_3^3) \) are

\[
x_1 + x_2 \alpha_3 + z_1 \mathfrak{P}_3 + z_2 \alpha_3 \mathfrak{P}_3 \quad \forall x_1, x_2 \in \mathbb{Z}_9, z_1, z_2 \in \mathbb{Z}_3
\]

with \( \alpha_3 \) a root of \( x^2 + 2x + 2 \) modulo \( \mathfrak{P}_3^3 \).

2.2 The abelian free group \( \mathfrak{Z}(\mathfrak{P}^a)(\times) \)

A complete detailed description of the structure of the multiplicative group of units \( \mathfrak{Z}(\mathfrak{P}^a)(\times) \) is apparently not available when \( \mathfrak{P} \) is a ramified prime. Nevertheless, the structure of \( \mathfrak{Z}(\mathfrak{P}^a)(\times) \) became fully understood after Hensel's work, see [11, 25]. In [11, p. 245], although Hasse gives a good account of
Hensel’s results, the structure of $\mathfrak{J}(q^a)^{(x)}$ $a \leq \frac{p e}{p - 1}$ is not explicitly specified when $a \leq \frac{pe}{p - 1}$. On a numerical edge, Cohen describes an algorithm for computing the structure of $\mathfrak{J}(q^a)^{(x)}$ [5, p. 195–201].

Our full description of $\mathfrak{J}(\mathfrak{P}^a)^{(x)}$ considers separately prime ideals of odd and even norm, and sub-orderly, fields $\mathbb{F}$ that contain or do not contain a $p$-th root of unity. The following Lemma is useful in the characterization of the free generators of $\mathfrak{J}(q^a)^{(x)}$.

**Lemma 1.** Let $p$ be an odd prime and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_F$ above $(p)$ with ramification index $e > 1$ and inertia index $f$. In the multiplicative group $\mathfrak{J}(\mathfrak{P}^a)^{(x)}$, the elements of order a power of $p$ are one-units, that is, they are elements of the form $1 + \theta a^i \mathfrak{P}^i$, where $\theta \in \mathcal{O}_F$, $i$ is a non-negative integer, and $a$ is an ideal of $\mathcal{O}_F$ that is not divisible by $\mathfrak{P}$ and such that $a\mathfrak{P}$ is a principal ideal.

**Proof.** Every unit $b \in \mathfrak{J}(\mathfrak{P}^a)^{(x)}$ can be written in the form $u + \theta a^i \mathfrak{P}^i$, where $u$ is a non-zero element of $\mathcal{O}_F$ such that the ideal generated by $u$ is not divisible by $\mathfrak{P}$, and $a$ is an ideal of $\mathcal{O}_F$ that is not divisible by $\mathfrak{P}$ if $i \geq 1$ and is zero otherwise. If $b$ is an element of order a power $p^m$, we have $b^{p^m} = 1 \mod \mathfrak{P}^a$, thus a fortiori $u^{p^m} = 1 \mod \mathfrak{P}$, which implies $u = 1$ since the $p$-powers in $\mathfrak{J}(\mathfrak{P}^a)^{(x)}$ are images of the Frobenius automorphism, i.e. the correspondence $u^{p^m} \leftrightarrow u$ is one-to-one, and obviously $1^{p^m} = 1 \mod \mathfrak{P}$.

In view of the observation immediately after the proof of Lemma 2 in [9, pp. 2803–2804], we can always assume that the factorization of $\text{irr}(\alpha, \mathbb{Q})$ modulo $p$ always contains an irreducible factor $m_f(x)$ of degree $f$ that corresponds to $\mathfrak{P} = (p, m_f(\gamma))$ where $\gamma$ modulo $\mathfrak{P}$ is a primitive element of the field $\mathcal{O}_F/\mathfrak{P}$. Moreover, every element of $\mathfrak{J}(\mathfrak{P})$ can be written in the form

$$b_0 + b_1 \gamma + \cdots + b_{f-1} \gamma^{f-1} + \mathfrak{P}, \quad \text{with } b_i \in \mathbb{Z}, i = 1, \ldots, n.$$ 

**Theorem 2.** Let $\mathbb{F}$ be an algebraic number field that does not contain $\zeta_p$, a $p$-th root of unity. Let $p$ be an odd prime and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_F$ above $(p)$ with ramification index $e > 1$ and inertia index $f$. The multiplicative group $\mathfrak{J}(\mathfrak{P}^a)^{(x)}$ has order $\Phi(\mathfrak{P}^a) = p^{f(a-1)}(p^f - 1)$ and can be decomposed into the direct product of two groups of relatively prime orders

$$\mathfrak{J}(\mathfrak{P}^a)^{(x)} = G_1 \times G_2,$$

where $G_1 = \langle \gamma^{p^a - 1} \rangle_{p^f - 1}$ is a cyclic group of order $p^f - 1$, and $G_2$ is an abelian $p$-group of order $p^{f(a-1)}$ whose structure depends on the numerical value of $a$:

If $1 < a \leq e$, we have $t = a$, $r = 0$, and $m = 1$. In this case, $G_2$ is the direct product of $f(a - 1)$ cyclic groups of order $p$ generated by one-units of the
form defined in Lemma 1

\[ G_2 = \bigotimes_{i=1}^{a-1} \bigotimes_{j=0}^{f-1} (1 + \alpha_a^j c^i \mathfrak{P}^i)_p. \]

(1)

If \( a > e \), we have \( t = e, r = a \mod e, \) and \( m = \frac{a-r}{r} \). In this case, \( G_2 \) is a direct product of \( e \) cyclic groups of order \( p^m \) or \( p^{m+1} \), and generated by one-units of the form defined in Lemma 1.

\[
G_2 = \begin{cases} 
\bigotimes_{i=1}^{e-1} \bigotimes_{j=0}^{f-1} (1 + \alpha_a^j c^i \mathfrak{P}^i)_{p^m} & r = 0 \\
\bigotimes_{i=1}^{e} \bigotimes_{j=0}^{f-1} (1 + \alpha_a^j c^i \mathfrak{P}^i)_{p^m} & r = 1 \\
\bigotimes_{i=1}^{e} \bigotimes_{j=0}^{f-1} (1 + \alpha_a^j c^i \mathfrak{P}^i)_{p^m+1} & 2 \leq r \leq e-1 
\end{cases}
\]

(2)

PROOF. By [9, Lemma 2, pp. 2803–2804], \( \gamma \) generates a cyclic group of order \( p^l - 1 \) modulo \( \mathfrak{P} \), hence it generates a group of order \( p^b(p^l - 1) \) modulo \( \mathfrak{P}^a \) for some positive integer \( b \) dividing \( a - 1 \). It follows that \( \gamma^{p^l-1} \mod \mathfrak{P}^a \) has order \( p^l - 1 \) and generates \( G_1 \).

By Lemma 1, \( G_2 \) is generated by elements of the form \( 1 + a \mathfrak{P}^i \) whose order, modulo \( \mathfrak{P}^a \), is the minimum power of exponent \( p^l \) such that \( i + ke \geq a \). In this case we take \( a = \alpha^j_a c^i \), with \( c \) an ideal not divisible by \( \mathfrak{P} \) such that \( c \mathfrak{P} \) is principal [7], and we write the generators as \( 1 + \alpha_a^j c^i \mathfrak{P}^i \). If \( 2 \leq a \leq e \), the condition \( i + ke \geq a \) is always satisfied taking \( k = 1 \). If \( a > e \), we have \( a = me + r \), thus \( k \) is the minimum integer greater than or equal to \( m + \frac{a-e}{e} \); therefore \( k = m + 1 \) if \( i < r \), and \( k = m \), otherwise. Furthermore, for fixed \( i \) the generators \( 1 + \alpha_a^j c^i \mathfrak{P}^i \) are independent because the powers \( \alpha_a^j \), for \( 0 \leq i \leq f-1 \), are linearly independent over \( \mathbb{Z}_p \). Actually, we have

\[
\prod_{j=0}^{f-1} (1 + \alpha_a^j c^i \mathfrak{P}^i)^{n_j} = 1 + \left( \sum_{j=0}^{f-1} n_j \alpha_a^j \right) c^i \mathfrak{P}^i \mod \mathfrak{P}^{i+1},
\]

thus the left side product is 1, if and only if \( \sum_{j=0}^{f-1} n_j \alpha_a^j = 0 \mod \mathfrak{P} \), which forces \( n_j = 0 \) for every \( j \).

In conclusion, if \( a \leq e \) we obtain the equation in (1) since the independence of the generators just proved that the order of the group is \( p^{(a-1)f} \) as it must be. If \( a > e \), we obtain the equation in (2) where it has been necessary to deal some special values of \( r \) separately. Precisely: 1) if \( r = 0 \), then \( a = me \).
and the group generated by $1 + \alpha_a^j c^i \mathfrak{P}^e$ has order $p^{m-1}$, whereas the groups generated by $1 + \alpha_a^j c^i \mathfrak{P}^i$, with $1 \leq i \leq e - 1$, have order $p^m$. In this case the order of the group is $p^{f(m-1)p^{mf(e-1)} = p^{(a-1)f}}$ as it must be; 2) if $r = 1$, then $a = me + 1$ and all $e$ groups generated by $1 + \alpha_a^j c^i \mathfrak{P}^i$, with $1 \leq i \leq e - 1$, have order $p^m$, in this case the order of the group is $p^{me f} = p^{(a-1)f}$ as it must be; 3) if $2 \leq r \leq e - 1$, then the general argument applies without exceptions. In this case the order of the group is $p^{(r-1)f(m+1)p^{mf(e-r)+1}} = p^{(a-1)f}$ as it must be.

\[ \square \]

**Theorem 3.** Let $\mathfrak{P}$ be an ideal of $\mathcal{O}_\mathfrak{P}$ above the principal ideal $(2)$ which has ramification index $e \geq 2$ and inertia index $f$. The multiplicative group of the units $\mathfrak{U}(\mathfrak{P}^a) = G_1 \times G_2$, where $G_1 = \langle \gamma^{2a-1} \rangle_{2f-1}$ is a cyclic group, and $G_2$ is an abelian $2$-group of order $2^{f(a-1)}$ whose structure depends on $a$. Setting $h_i = \lceil \frac{a}{e} \rceil$, we have:

If $2 \leq a \leq e$, then $G_2$ is a direct product of $f(a-1)$ cyclic $2$-groups of order $2$:

\[ G_2 = \bigoplus_{i=0}^{a-2} \bigotimes_{j=0}^{f-1} \langle 1 + \alpha_a^j c^i \mathfrak{P}^i \rangle_{2} \tag{3} \]

If $e + 1 \leq a \leq 2e$, then $G_2$ is a direct product of $fe$ cyclic $2$-groups of order $2^{h_i}$:

\[ G_2 = \bigotimes_{j=0}^{f-1} \langle 1 - 2\alpha_a^j \rangle_{2} \bigotimes_{i=1}^{e-1} \bigotimes_{j=0}^{f-1} \langle 1 + \alpha_a^j c^i \mathfrak{P}^i \rangle_{2^{h_i}} \tag{4} \]

If $2e < a$, then $G_2$ is a direct product of $fe$ cyclic $2$-groups of order $2^{h_i}$:

\[ G_2 = \bigotimes_{i=1}^{e} \bigotimes_{j=0}^{f-1} \langle 1 + \alpha_a^j c^i \mathfrak{P}^i \rangle_{2^{h_i}} \tag{5} \]

Proof. Similarly as in Theorem 2, $\gamma$ generates a cyclic group of order $2^f - 1$ modulo $\mathfrak{P}$, hence it generates a group of order $2^b(2^f - 1)$ modulo $\mathfrak{P}^a$ for some positive integer $b$ dividing $a - 1$. It follows that $\gamma^{2^a - 1} \mod \mathfrak{P}^a$ has order $2^f - 1$ and generates $G_1$.

The $2$-group $G_2$ is a direct product of cyclic groups of order a power of $2$ which are generated by one-units of the form $1 + \alpha_a^j c^i \mathfrak{P}^i$ and possibly by the unit $-1$ when $a > e$, given that $-1 = 1 \mod \mathfrak{P}^a$ whenever $a \leq e$. The order $2^{h_i}$
of the cyclic group $\langle 1 + \alpha_a^j c^j P^i \rangle_{2h_i}$ is specified by the minimum $h_i$ such that $2h_i P^i = (0) \mod P^a$, therefore $h_i$ is the minimum integer such that $eh_i + i \geq a$, that is $h_i = \lceil \frac{a-i}{e} \rceil$.

If $2 \leq a \leq e$, the coset ideals $1 + \alpha_a^j c^j P^i$ are independent generators for every $i$ in the range $0 \leq i \leq a - 2$ and every $j$ in the range $0 \leq j \leq f - 1$. In this case $h_i = 1$ for every $i$, thus $\sum_{i=0}^{a-2} 1 = a - 1$, i.e. the order of the generated group is $2^{f(a-1)}$, and this proves equation (3).

If $e + 1 \leq a \leq 2e$, the coset ideals $1 + \alpha_a^j c^j P^i$ are independent generators for every $i$ in the range $1 \leq i \leq e - 1$ and every $j$ in the range $0 \leq j \leq f - 1$, and the cyclic groups have orders $2^{h_i}$, with $h_i = 1, 2$. Furthermore, the cyclic groups generated by the coset ideals corresponding to $i = 0$ must be of the form $\langle 1 - 2\alpha_a^j \rangle_2$ for every $j$ in the range $0 \leq j \leq f - 1$, and clearly have order 2. In this case $h_i = 2$ if $i < r$, otherwise $h_i = 1$. Thus we have $1 + 2(r - 1) + e - r = e + r - 1 = a - 1$, i.e., the order of the generated group is $2^{f(a-1)}$, and this proves equation (4).

If $2e < a$, then $G_2$ is a direct product of $fe$ cyclic groups of order $2^{h_i}$ which are generated by $1 + \alpha_a^j c^j P^i$, for every $i$ in the range $1 \leq i \leq e$ and every $j$ in the range $0 \leq j \leq f - 1$. The exponent $h_i$ is equal to $m + 1$ if $1 \leq i \leq r - 1$ and is equal to $m$ if $r \leq i \leq e$. Thus we have

$$(m + 1)(r - 1) + m(e - r + 1) = me + r - 1 = a - 1,$$

i.e., the order of the generated group is $2^{f(a-1)}$, and this proves equation (5).

3 The Singular Role of the Cyclotomic Unit $\zeta_p$

Throughout this section, we assume that $\mathbb{F}$ contains $\zeta_p$, a primitive $p$th root of unity, where $p$ is an odd prime. The presence of $\zeta_p$ in $\mathbb{F}$ affects the structure of $\mathcal{O}_\mathbb{F}(\mathcal{P}^a)^{(x)}$, for any prime ideal $\mathcal{P}$ above $p$ that is also above $1 - \zeta_p$, because $p$ fully splits in $\mathbb{Q}(\zeta_p)$ with one of the prime factors equal to $1 - \zeta_p$. This situation is tackled in Hasse’s book [11] using $p$-adic analysis, however, for our purposes, the singular role of $\zeta_p$ is attacked more directly considering algebraic number fields. Some properties that we need are proved in two lemmas.

**Lemma 2.** Let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_\mathbb{F}$ above the ideal $(1 - \zeta_p)$. Then $\zeta_p$ has order $p$ in $\mathcal{O}_\mathbb{F}(\mathcal{P}^a)^{(x)}$ for every $a > \frac{r}{p - 1}$, and $\zeta_p = 1 \mod \mathcal{P}^a$ for every $a \leq \frac{r}{p - 1}$.

**Proof.** The cyclotomic field $\mathbb{Q}(\zeta_p)$ is a subfield of $\mathbb{F}$. Since the prime ideal $(1 - \zeta_p)$ has ramification index $e(p) = p - 1$ in $\mathbb{Q}(\zeta_p)$, a prime ideal $\mathcal{P}$ above
\((1 - \zeta_p)\) is ramified with a ramification index \(e\) that is a multiple of \(p - 1\). Moreover, the power \(P^{e/(p-1)}\) strictly divides the principal ideal \((1-\zeta_p)\), which, in turn, is divisible by \(P^a\) for every \(a \leq \frac{p}{p-1}\). Therefore, modulo \(P^a\), the ideal \((1 - \zeta_p)\) is the zero ideal \((0)\), which is equivalent to saying that \(\zeta_p = 1 \mod P^a\) for every \(a > \frac{p}{p-1}\), in which case \(\zeta_p^a = 1\) independent of the modulo, that is, independent of \(a\). \(\square\)

**Lemma 3.** Assume the hypotheses and notations of Lemma 2. The element \(\pi = 1 + \theta(1 - \zeta_p) \in \mathcal{O}_\mathbb{F}\), where \(\theta\) is relatively prime with \(p\), generates a cyclic group of order \(p\), modulo \(P^\nu\), for every \(\frac{e}{p-1} + 1 \leq \nu \leq \frac{ep}{p-1}\).

**Proof.** Recall that \(p - 1\) is a divisor of \(e\). Then

\[
(1 + \theta(1 - \zeta_p))^p = 1 + p\theta(1 - \zeta_p) + \theta^p(1 - \zeta_p)^p \mod P^\nu = 1 + u\theta(1 - \zeta_p)^{p-1+1} + \theta^p(1 - \zeta_p)^p \mod P^\nu,
\]

where in the binomial expansion only two terms have been retained because all other terms are equal to zero modulo \(P^\nu\). Furthermore, the relation \((1 - \zeta_p)^{p-1} = u^{-1}p\), with \(u\) a field unit, has been used. Therefore, recalling that

\[
(1 - \zeta_p) = vP^{\frac{p}{p-1}}\]

for some \(v \in \mathcal{O}_\mathbb{F}\) relatively prime with \(P\), we have

\[
\pi^p = 1 + (u\theta + \theta^p)(1 - \zeta_p)^p \mod P^\nu = 1 + (u\theta + \theta^p)vP^{\frac{sp}{p-1}} \mod P^\nu,
\]

which clearly shows that \(\pi\) generates, modulo \(P^\nu\), a cyclic group of order \(p\) for every \(\nu\) such that \(\frac{e}{p-1} + 1 \leq \nu \leq \frac{ep}{p-1}\). \(\square\)

**Theorem 4.** Let \(\mathbb{F}\) be a number field containing \(\zeta_p\) and let \(P\) be a prime ideal of \(\mathcal{O}_\mathbb{F}\) above the principal ideal \((p)\) with ramification index \(e > 1\) and inertia index \(f\).

The multiplicative group of units \(\mathfrak{U}(\mathbb{F})^{(\times)}\) has order \(\Phi(\mathfrak{P}^a) = p^f(a-1)(p^f - 1)\) and can be decomposed into the direct product of two groups \(\mathfrak{U}(\mathbb{F})^{(\times)} = G_1 \times G_2\), where

- \(G_1\) is a cyclic group of order \(p^f - 1\) generated by a suitable primitive element of \(\mathbb{Z}_p^{(\times)}\) if \(f = 1\), or by \(\gamma^{p^{f-1}}\) if \(f > 1\);

- \(G_2\) is an abelian \(p\)-group of order \(p^{f(a-1)}\), whose structure is described considering \(f = 1\) and \(f > 1\) separately:
On the structure of residue rings of prime ideals

$f = 1$, $G_2$ is a $p$-group of order $p^{a-1}$ which is the direct product of cyclic $p$-groups as follows

\[
G_2 = \left\{ \begin{array}{ll}
\bigotimes_{i=1}^{a-1} (1 + c^i\mathcal{P}_i)_p & a \leq \frac{e}{p-1}, \\
\langle \zeta_p \rangle \bigotimes_{i=1, i \neq s}^{a-1} \langle 1 + c^i\mathcal{P}_i \rangle_p & e + 1 \leq a \leq e + 1, \\
\langle \zeta_p \rangle \bigotimes_{i=1}^e (1 + c^i\mathcal{P}_i)_p \bigotimes_{i=r, i \neq s}^{e} \langle 1 + c^i\mathcal{P}_i \rangle_p & e + 2 \leq a \leq \frac{pe}{p-1}, \\
\langle \zeta_p \rangle \bigotimes_{i=1}^{w-1} \langle 1 + c^i\mathcal{P}_i \rangle_p \bigotimes_{i=w}^{e} \langle 1 + c^i\mathcal{P}_i \rangle_p & \frac{pe}{p-1} + 1 \leq a \leq 2e + 1, \\
\langle \zeta_p \rangle \bigotimes_{i=1}^{w-1} \langle 1 + c^i\mathcal{P}_i \rangle_p \bigotimes_{i=w}^{w+m} \langle 1 + c^i\mathcal{P}_i \rangle_p & 2e + 2 \leq a \end{array} \right.
\]

where $s = \frac{a}{p-1}$, and $w = a - 1 - me$ is the remainder of the division of $a - 1$ by $e$, if $w = 0$, then set $w = e$. We use the convention that if $e + 2 > \frac{pe}{e-1}$, then the case is disregarded.

$f \geq 2$, $G_2$ is a $p$-group of order $p^{(a-1)f}$ which is a direct product of cyclic $p$-
groups as follows

\[
G_2 = \begin{cases}
\bigotimes_{i=1}^{a-1} (1 + \alpha_a^i c^i \mathfrak{P})_p \\
\bigotimes_{i=0}^{f-1} (1 + \alpha_a^i c^i \mathfrak{P})_p \bigotimes_{j=0}^{f-1} (1 - \alpha_a^j c^j \mathfrak{P})_p & \frac{e}{p - 1} + 1 \leq a \leq e + 1, \\
\bigotimes_{i=0}^{w-1} (1 + c^i \alpha_a^i \mathfrak{P})_p \bigotimes_{j=0}^{f-1} (1 + c^i \alpha_a^j \mathfrak{P})_p \bigotimes_{j=0}^{f-1} (1 - \alpha_a^j c^j \mathfrak{P})_p & e + 2 \leq a \leq \frac{pe}{p - 1}, \\
\bigotimes_{i=0}^{w-1} (1 + c^i \alpha_a^i \mathfrak{P})_p \bigotimes_{j=0}^{w-1} (1 + c^i \alpha_a^j \mathfrak{P})_p \bigotimes_{j=0}^{f-1} (1 - \alpha_a^j c^j \mathfrak{P})_p & 2e + 1 \leq a.
\end{cases}
\]

PROOF. As in Theorem 2, \( \gamma \) generates a cyclic group of order \( p^f - 1 \) modulo \( \mathfrak{P} \), hence it generates a group of order \( p^b(p^f - 1) \) modulo \( \mathfrak{P}^a \) for some positive integer \( b \) dividing \( a - 1 \). It follows that \( \gamma^{p^a-1} \mod \mathfrak{P}^a \) has order \( p^f - 1 \) and generates \( G_1 \).

The group \( G_2 \) is an abelian \( p \)-group of order \( p^{f(a-1)} \), and we consider \( f = 1 \) and \( f > 1 \), separately.

\( f = 1 \). The \( p \)-group \( G_2 \) in \( \mathfrak{P}(\mathfrak{P}^{a})^{(x)} \) has order \( p^{a-1} \) and is a direct product of a certain number of cyclic \( p \)-groups depending on \( a \). It is convenient to distinguish five separate cases:

i) \( a \leq \frac{e}{p - 1} \). In this case, \( \zeta_p = 1 \mod \mathfrak{P}^a \) by Lemma 2, hence

\[
G_2 = \bigotimes_{i=1}^{a-1} (1 + c^i \mathfrak{P})_p ,
\]

since \((1 + c^i \mathfrak{P})^p = 1 + c^i \mathfrak{P}^{i+c} = 1 \mod \mathfrak{P}^a \) holds true for any \( i \leq a - 1 \). Thus, every \( 1 + c^i \mathfrak{P}^i \) generates a cyclic group of order \( p \); finally, the order of \( G_2 \) is a power of \( p \) of exponent \( a - 1 \).
On the structure of residue rings of prime ideals

ii) \( \frac{e}{e-1} + 1 \leq a \leq e + 1 \). In this case, \( \zeta_p \not\equiv 1 \mod p \), hence the group \( \langle \zeta_p \rangle_p \) is a factor of \( G_2 \), and setting \( s = \frac{e}{e-1} \), we have

\[
G_2 = \bigotimes_{i=1}^{s-1} \langle 1 + c^i \mathfrak{P}^i \rangle_p \bigotimes_{i=s+1}^{a-1} \langle 1 + c^i \mathfrak{P}^i \rangle_p \otimes \langle \zeta_p \rangle_p .
\]  

(8)

This is motivated as follows:

1) since \( a \leq e \) the argument of previous point applies equally well and all groups are of order \( p \);
2) by Lemma 3, the group \( \langle \zeta_p \rangle_p \) is included and corresponds to \( 1 + c^e \mathfrak{P}^e = 1 + c^e \mathfrak{P} \); 
3) the case \( a = e + 1 \) is also included because the element \( 1 + c^e \mathfrak{P}^e = 1 + c^e \mathfrak{P} \) clearly generates a group of order \( p \) when considered modulo \( \mathfrak{P}^{e+1} \).

The order of \( G_2 \) is a power of \( p \) with exponent \((s-1)+(a-1-s)+1 = a-1\).

iii) \( e + 2 \leq a \leq \frac{pe}{p-1} \). In this case,

\[
G_2 = \bigotimes_{i=1}^{r-1} \langle 1 + c^i \mathfrak{P}^i \rangle_{p^2} \bigotimes_{i=r}^{s-1} \langle 1 + c^i \mathfrak{P}^i \rangle_p \bigotimes_{i=s+1}^{e} \langle 1 + c^i \mathfrak{P}^i \rangle_p \otimes \langle \zeta_p \rangle_p .
\]  

(9)

The equation in (9) follows from the same arguments used proving equation (2) and the observations that the bounds on \( a \) imply \( m = 1 \), \( r = a - e \), and that

\[
(1 + \mathfrak{P}^i)^p = 1 + \mathfrak{P}^{i+e} \mod \mathfrak{P}^a \neq 1 \quad 1 \leq i \leq a - e - 1 ,
\]

thus we have exactly \( r-1 \) cyclic groups of order \( p^2 \), the remaining groups must have order \( p \). In conclusion, the order of \( G_2 \) is a power of \( p \) of exponent \( 2(r-1) + (s-r) + (e-s) + 1 = e + r - 1 = a - 1 \).

iv) \( \frac{6e}{e-1} \leq a \leq 2e + 1 \), set \( w = a - 1 \mod e \) and \( w = e \) if \( e | (a-1) \). In this case,

\[
G_2 = \bigotimes_{i=1}^{w-1} \langle 1 + c^i \mathfrak{P}^i \rangle_{p^2} \bigotimes_{i=w}^{e} \langle 1 + c^i \mathfrak{P}^i \rangle_p \otimes \langle \zeta_p \rangle_p .
\]  

(10)

Since the group \( \langle \zeta_p \rangle_p \) of order \( p \) is always present, we must have \( w-1 \) groups of order \( p^2 \), with \( w = a - 1 \mod e \), unless \( a - 1 = 0 \mod e \), in which case \( w = e \). The remaining groups must be of order \( p \). In conclusion, the order of \( G_2 \) is a power of \( p \) of exponent \( 2(w-1) + (e - w + 1) + 1 = e + w = a - 1 \).

v) \( 2e + 2 \leq a \). In this case,
\[
G_2 = \bigotimes_{i=1}^{w-1} (1 + c^i \mathfrak{P}^i)_{p^{m+1}} \bigotimes_{i=w}^{e} (1 + c^i \mathfrak{P}^i)_{p^m} \otimes \langle \zeta_p \rangle .
\] (11)

Since the group \(\langle \zeta_p \rangle_p\) is always present, the total order of the remaining factor groups must be \(p^{a-2}\). Therefore, we must have \(w - 1\) groups of order \(p^{m+1}\) to satisfy the condition \(e(m + 1) + i > a\) and the remaining groups of order \(p^m\) are such that the condition \(em + i \geq a\) is satisfied. In conclusion, the order of \(G_2\) is a power of \(p\) of exponent

\[
(m + 1)(w - 1) + m(e - w + 1) = me + w - 1 = a - 1 .
\]

\(f \geq 2\). The group \(G_2\) has order \(p^{f(a-1)}\) and is generated by elements of the form \(1 + (\alpha_a)^j c^i \mathfrak{P}^i\), \(\zeta_p\), and ideal cosets of the form \(1 + (\alpha_a)^j p^m c \mathfrak{P}\). Since generators \(1 + (\alpha_a)^j c^i \mathfrak{P}^i, j = 0, \ldots, f - 1\) are independent, the structure of the group is the same as in the case of \(f = 1\) with each cyclic group \(1 + c^i \mathfrak{P}^i\) replaced by the direct product \(\bigotimes_{j=0}^{f-1} (1 + \alpha_a^j c^i \mathfrak{P}^i)_{p^h}\), and besides the cyclic group \(\langle \zeta_p \rangle_p\) the direct product \(\bigotimes_{j=1}^{f-1} (1 + \alpha_a^j p^{m-1} c^i \mathfrak{P}^i)_{p}\) is considered. The conclusions of this operation translate into (6). The only set of generators that needs to be explained is that corresponding to \(\langle \zeta_p \rangle_p\). In this case, \(f - 1\) \(p\)-groups of order \(p\) are required to provide a factor group of order \(p^f\). Actually, the groups generated by \(1 + \alpha_a^j p^{m-1} c^i \mathfrak{P}^w\) have order \(p\)

\[
(1 + \alpha_a^j p^{m-1} c^i \mathfrak{P}^r)^p = 1 + \alpha_a^j p^m c^i \mathfrak{P}^r \mod \mathfrak{P}^a = 1 + \alpha_a^j v^{-m} c^i \mathfrak{P}^{em+r} \mod \mathfrak{P}^a = 1 .
\]

\(\square\)

4 Conclusion

In this paper the structures of the additive group and the unit multiplicative group of residue rings modulo prime power ideals \(\mathfrak{P}^a\) in algebraic number fields were described in full detail and explicit sets of free generators for each group were provided. The casuistry is relatively complex and is summarized in five tables which consider separately the case of primes with odd and even norms, and suborderly the primes with inertia degree \(f = 1\), and \(f \geq 2\). In each table, for every value of the exponent \(a\), that is, \(a = 1, a = 2,\) and \(a > 2\), the additive and multiplicative group structures are reported in neighboring rows. The glossary of symbols and notations is the following:
$f = 1$ & $f \geq 2$ \\
\hline 
$a = 1$ & \\
$\mathbb{Z}_p$ & $\sum_{i=0}^{f-1} x_i \alpha_1^i \quad x_i \in \mathbb{Z}_p$ \\
$\langle g \rangle_{p-1}$ & $\langle \alpha_1 \rangle_{p-1}$ \\
\hline 
$a = 2$ & \\
$\mathbb{Z}_{p^2}$ & $\sum_{i=0}^{f-1} x_i \alpha_2^i \quad x_i \in \mathbb{Z}_{p^2}$ \\
$\langle g^p \rangle_{p-1}(1 + c\mathfrak{P})_p^1$ & $\langle \alpha_2^p \rangle_{p-1}^1 \bigotimes_{j=0}^{f-1} (1 + \alpha_2^j c\mathfrak{P})_p$ \\
\hline 
a $> 2$ & \\
$\mathbb{Z}_{p^a}$ & $\sum_{i=0}^{f-1} x_i \alpha_a^i \quad x_i \in \mathbb{Z}_{p^a}$ \\
$\langle g^{p^a-1} \rangle_{p-1}(1 + \mathfrak{P})_{p^a-1}$ & $\langle \alpha_a^{p^a-1} \rangle_{p-1}^1 \bigotimes_{j=0}^{f-1} (1 + \alpha_a^j c\mathfrak{P})_{p^a-1}$ \\
\hline 

Table 1: Structures of residue rings modulo primes of odd norm, $e = 1$

| $e$ | ramification index of a prime ideal $\mathfrak{P}$ |
| $f$ | inertia index of a prime ideal $\mathfrak{P}$ |
| $t = \min\{e, a\}$ | inertia index of a prime ideal $\mathfrak{P}$ |
| $r = a \mod t$, | inertia index of a prime ideal $\mathfrak{P}$ |
| $m = \frac{a-r}{t}$ | inertia index of a prime ideal $\mathfrak{P}$ |
| $s = \frac{e}{p-1}$ | inertia index of a prime ideal $\mathfrak{P}$ |
| $c$ | ideal relatively prime with $\mathfrak{P}$ such that $c\mathfrak{P}$ is principal |
| $g$ | primitive element in $\mathbb{Z}_{p^a}$ |
| $\zeta_p$ | $p$-root of unity |
| $\mathbb{Z}_{p^j}$ | additive cyclic group of order $p^j$ |
| $\langle g \rangle_N$ | cyclic multiplicative group of order $N$ generated by $g$ |

The following examples illustrate the theory and show that the computations with ramified principal or non-principal ideals are of the same complexity.

**Example 3.** Consider the cyclotomic field $\mathbb{Q}(\zeta_3)$ where $\zeta_3$ is a root of the cyclotomic polynomial $z^2 + z + 1$ of discriminant $-3$. The rational prime 3 ramifies with ramification index 2 and inertia index 1. The field has class number 1, hence every ideal is principal. The prime ideal $\mathfrak{P}_3 = \langle \zeta_3 - \zeta_3^2 \rangle$ has inertia index 1 and ramification index 2, so $\mathfrak{P}_3^2 = (3)$. Notice that according to
our convention, \( \mathfrak{P}_3 \) represents \( \zeta_3 - \zeta_3^2 \) because it is a principal ideal. With this convention we have \( \mathfrak{P}_3^2 = -3 \). The ring \( \mathcal{O}_F/\mathfrak{P}_3^3 \) has order 27 and its additive structure is isomorphic to a direct sum of cyclic groups of order 9 and 3 that can be written as

\[
x_1 + z_1 \mathfrak{P}_3 \quad x_1 \in \mathbb{Z}_9, \quad z_1 \in \mathbb{Z}_3.
\]

The multiplicative group of units of \( \mathcal{O}_F/\mathfrak{P}_3^3 \) has order 18 and is isomorphic to a direct product of three cyclic groups of order 2, 3, and 3

\[
\langle 8 \rangle_2 \times \langle 1 + \mathfrak{P}_3^2 \rangle_3 \times \langle 1 + \mathfrak{P}_3 \rangle_3 \simeq \langle 2 \rangle_6 \times \langle 1 + \mathfrak{P}_3 \rangle_3,
\]

note that \( 1 + \mathfrak{P}_3^2 = -2 \), and \( 8 = -1 \mod \mathfrak{P}_3^3 \).

**Example 4.** Let \( \mathbb{Q}(\alpha) \) be a quartic field with \( \alpha \) root of \( q(z) = z^4 + 2z^2 + 3z + 1 \). The polynomial \( q(z) \) has discriminant \( 117 = 3^2 \cdot 13 \) and factors, modulo 3, as \( (x^2 + 1)^2 \). Thus, 3 ramifies with ramification index 2 and inertia index 2 according to the Kummer-Dedekind correspondence. The prime ideal \( \mathfrak{P}_3 = \langle \alpha^2 + 1 \rangle \) is principal and its inertia and ramification degrees are both equal to 2. Hence, the factor making \( \mathfrak{P}_3 \) principal is 1. It is direct to check that \( \mathfrak{P}_3^2 = (3) \). The ring \( \mathfrak{J}(\mathfrak{P}_3^3) = \mathcal{O}_F/\mathfrak{P}_3^3 \) has order \( (3^2)^3 = 729 \), and to represent
its elements, let \( \alpha_3 \) denote a root of \( q(z) \) modulo \( \mathfrak{P}_3^3 \), that is, \( \alpha_3 \) is a root of the polynomial \( x^2 + 1 \) modulo \( \mathfrak{P}_3^3 \). Thus,

\[
[x_1 + x_2\alpha_3] + [z_1 + z_2\alpha_3]\mathfrak{P}_3 \quad x_1, x_2 \in \mathbb{Z}_9, \quad z_1, z_2 \in \mathbb{Z}_3.
\]

This representation shows that the additive structure \( \mathfrak{I}(\mathfrak{P}_3^3)^{(+)} \) is isomorphic to a direct product of two cyclic groups of order 9 and two cyclic groups of order 3.

The multiplicative group \( \mathfrak{I}(\mathfrak{P}_3^3)^{(x)} \) of the units has order \( 8 \cdot 81 = 648 \) and is isomorphic to a direct product \( G_1 \times G_2 \) where \( G_1 \) is a cyclic group of order 8 generated by \( 2 + \alpha_3^3 \) modulo \( \mathfrak{P}_3^3 \), and \( G_2 \) is a 3-group of rank four whose generators are \( 1 + \mathfrak{P}_3, 1 + \alpha_3 \mathfrak{P}_3, 1 + 3, 1 + 3\alpha_3 \).

**Example 5.** Let \( \mathbb{Q}(\alpha) \) be a quartic field, where \( \alpha \) is a root of \( p(x) = x^4 + 2x^3 + 3x^2 + 2x + 11 \) whose discriminant is \( 2^6 \cdot 3 \cdot 13^2 \). The factorization \( p(x) = (x^2 + x + 1)^2 \bmod 5 \) shows that the ideal \( (5) \) ramifies with both ramification and inertia indices equal to 2 according to the Kummer-Dedekind correspondence. The only prime ideal above \( (5) \) is \( \mathfrak{P}_5 = (3 + 4\alpha + 2\alpha^2 - \frac{4}{13}(\alpha^3 + 8\alpha^2 + 12\alpha + 9)) \), and has norm \( N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{P}_5) = 25 \). We have \( \mathfrak{P}_5^2 = (5) \). The ring \( \mathfrak{I}(\mathfrak{P}_5^3) \) has order 15625 and its additive structure is an abelian group of order 15625 which is isomorphic to a direct product of 4 cyclic groups, two of order 25 and two of order 5, whose elements are represented as

\[
x_1 + x_2\alpha_3 + (z_1 + z_2\alpha_3)\mathfrak{P}_5 \bmod \mathfrak{P}_5^3: \quad x_1, x_2 \in \mathbb{Z}_{25}, \quad z_1, z_2 \in \mathbb{Z}_5\}
\]

The multiplicative group \( \mathfrak{I}(\mathfrak{P}_5^3)^{(x)} \) of units has order \( 24 \cdot 25^2 = 15000 \) and is isomorphic to a direct product \( G_1 \times G_2 \) where \( G_1 \) is a cyclic group of order 24

\[
G_1 = \{(1 + 3\alpha_3)^j \bmod \mathfrak{P}_5^3, j = 0, \ldots, 23\}
\]

and \( G_2 \) is a 5-group of rank 4

\[
G_2 = \{(1 + \mathfrak{P}_5)^{j_1}(1 + 3\alpha_3 \mathfrak{P}_5)^{j_2}(1 + \mathfrak{P}_5^2)^{j_3}(1 + 3\alpha_3 \mathfrak{P}_5^2)^{j_4} \bmod \mathfrak{P}_5^3, \quad j_1, j_2, j_3, j_4 = 0, \ldots, 4\}
\]

**Example 6.** Let \( \mathbb{Q}(\zeta_{12}) \) be the cyclotomic field generated by a 12-root of unity. The degree of the field is 4 since \( \zeta_{12} \) is a root of the polynomial \( x^4 - x^2 + 1 \). The principal ideal \( (2) \) ramifies with ramification index 2 and inertia index 2. We have the factorization \( (2) = (1 + \zeta_{12}^4)^2 = \mathfrak{P}_2^2 \), thus \( \mathfrak{P}_2 \) is principal. The residue ring \( \mathfrak{I}(\mathfrak{P}_2^4) \) has order \( 2^8 \) and its elements can be written as

\[
(x_1 + x_2\alpha_4) + (z_1 + z_2\alpha_4)\mathfrak{P}_2, \quad x_1, x_2, z_1, z_2 \in \mathbb{Z}_4,
\]

where \( \alpha_4 \) is a root of \( x^2 + x + 1 \) modulo \( \mathfrak{P}_2^4 \), which can be seen as a lifted version of \( \zeta_{12} \) modulo 2. The above representation identifies also the additive
\[ a = 1 \]
\[ \mathbb{Z}_p \]
\[ G_2 = \langle 1 \rangle_1 \]
\[ a = 2 \]
\[ x_1 + x_2 c^p \quad x_1, x_2 \in \mathbb{Z}_p \]
\[ G_2 = \langle 1 + c^p \rangle_p \]
\[ a > 2 \]
\[ \sum_{i=0}^{r-1} x_i c^i + \sum_{i=r}^{t-1} z_i c^i \quad x_i \in \mathbb{Z}_{pm+1}, \quad z_i \in \mathbb{Z}_{pm} \]

\[ \zeta_p \not\in F \quad G_2 \]
\[ \bigotimes_{i=1}^{a-1} (1 + c^i \mathbb{P})_p \quad 3 \leq a \leq e \]
\[ (1 + c^e \mathbb{P}^{e-1}) \bigotimes_{i=1}^{e-1} (1 + c^i \mathbb{P})_p^m \quad a \geq e+1, \quad r = 0 \]
\[ (1 + c^i \mathbb{P})_p^m \quad a \geq e+1, \quad r = 1 \]
\[ (1 + c^i \mathbb{P})_p^{m+1} \bigotimes_{i=r}^{e} (1 + c^i \mathbb{P})_p^m \quad a \geq e+1, \quad e-1 \geq r \geq 2 \]

\[ \zeta_p \in F \quad G_2 \]
\[ \bigotimes_{i=1}^{a-1} (1 + c^i \mathbb{P})_p \quad a \leq \frac{e}{p-1} \]
\[ (\zeta_p)_p \bigotimes_{i=1, i \neq s}^{e-1} (1 + c^i \mathbb{P})_p \quad 1 \leq a < e+1 \]
\[ (\zeta_p)_p \bigotimes_{i=1}^{e-1} (1 + c^i \mathbb{P})_p^{m+1} \bigotimes_{i=r, i \neq s}^{e} (1 + c^i \mathbb{P})_p^m \quad e \leq a \leq \frac{pe}{p-1} \]
\[ (\zeta_p)_p \bigotimes_{i=1}^{e-1} (1 + c^i \mathbb{P})_p^{m+1} \bigotimes_{i=w}^{e} (1 + c^i \mathbb{P})_p^m \quad a \leq 2e+1 \]
\[ (\zeta_p)_p \bigotimes_{i=1, i \neq w}^{e-1} (1 + c^i \mathbb{P})_p^{m+1} \bigotimes_{i=w}^{e} (1 + c^i \mathbb{P})_p^m \quad a \geq 2e+2 \]

Table 3: Structures of residue rings modulo primes of odd norm, \( e \geq 2 \), \( f = 1 \).
The multiplicative structure is \( G_1 \times G_2 \) with \( G_1 = \langle g \rangle_{p-1} \), and \( G_2 \) reported in the Table.
Table 4: Structures of residue rings modulo primes of odd norm, $e \geq 2$ and $f \geq 2$. The multiplicative structure is $G_1 \times G_2$ with $G_1 = \langle \alpha_a^{p-1} \rangle_{p^{a-1}}$ and $G_2$ reported in the Table.
\[ \zeta_p \in \mathbb{F} \]

<table>
<thead>
<tr>
<th>Table 5: Continuation of Table 4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ \otimes_{i=1}^{f-1} \otimes_{j=0}^{a-1} (1 + \alpha_a^i \mathcal{P}^i)^p ]</td>
</tr>
<tr>
<td>( a \leq \frac{e}{p-1} )</td>
</tr>
<tr>
<td>[ \langle \zeta_p \rangle_p \otimes (1 + \alpha_a^j \mathcal{P}^j)^p \otimes (1 + \alpha_a^j \mathcal{P}^s)^p ]</td>
</tr>
<tr>
<td>( \frac{e}{p-1} \leq a \leq e + 1 )</td>
</tr>
<tr>
<td>[ \langle \zeta_p \rangle_p \otimes (1 + \alpha_a^j \mathcal{P}^j)^p \otimes (1 + \alpha_a^j \mathcal{P}^i)^{p^2} \otimes (1 + \alpha_a^j \mathcal{P}^i)^p ]</td>
</tr>
<tr>
<td>( 1 + \frac{pe}{p-1} \leq a \leq 2e + 1 )</td>
</tr>
<tr>
<td>[ \langle \zeta_p \rangle_p \otimes (1 + \alpha_a^j \mathcal{P}^j)^p \otimes (1 + \alpha_a^j \mathcal{P}^i)^{p^{m+1}} \otimes (1 + \alpha_a^j \mathcal{P}^i)^{p^m} ]</td>
</tr>
<tr>
<td>( 2e + 2 \leq a )</td>
</tr>
</tbody>
</table>
On the structure of residue rings of prime ideals

Table 6: Additive and Multiplicative structures of residue rings modulo primes above 2, $e \geq 2$. When $f \geq 2$, the group $\mathfrak{f}(\mathfrak{p}^a)^{(x)}$ is a direct product $\langle \gamma^{2a-1} \rangle_{p-1} \times G_2$ with $G_2$ reported in the Table written using the definition $h_i = \lceil \frac{a_i}{e} \rceil$. 

<table>
<thead>
<tr>
<th>$f = 1$</th>
<th>$f \geq 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a = 1$</td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Z}_2$</td>
<td>$\sum_{i=0}^{f-1} x_i \alpha_1^i \ x_i \in \mathbb{Z}_2$</td>
</tr>
<tr>
<td>$\langle 1 \rangle_1$</td>
<td>$\langle \alpha_1 \rangle_{2^{f-1}}$</td>
</tr>
<tr>
<td>$a = 2$</td>
<td></td>
</tr>
<tr>
<td>$x_1 + x_2 c_2 \ x_1, x_2 \in \mathbb{Z}_2$</td>
<td>$\sum_{j=0}^{f-1} [x_j + y_j c_2] \alpha_2^j \ x_j, y_j \in \mathbb{Z}_2$</td>
</tr>
<tr>
<td>$\langle 3 \rangle_2$</td>
<td>$\bigotimes_{j=0}^{f-1} \langle 1 + \alpha_2^j c_2 \rangle_2$</td>
</tr>
<tr>
<td>$a &gt; 2$</td>
<td></td>
</tr>
<tr>
<td>$\sum_{i=0}^{r-1} x_i c_i \mathfrak{p}<em>2^i + \sum</em>{i=r}^{e-1} z_i c_i \mathfrak{p}<em>2^i \ x_i \in \mathbb{Z}</em>{2^{m+1}}, z_i \in \mathbb{Z}_{2^m}$</td>
<td>$\sum_{i=0}^{r-1} x_{ij} \alpha_a^i c_i \mathfrak{p}<em>2^i + \sum</em>{j=0}^{f-1} z_{ij} \alpha_a^j c_i \mathfrak{p}<em>2^i \ x</em>{ij} \in \mathbb{Z}<em>{2^{m+1}}, z</em>{ij} \in \mathbb{Z}_{2^m}$</td>
</tr>
<tr>
<td>$\bigotimes_{i=0}^{e-2} \langle 1 + c^i \mathfrak{p}_2^i \rangle_2$</td>
<td>$\bigotimes_{j=0}^{f-1} \langle 1 + \alpha_a^j c^i \mathfrak{p}_2^i \rangle_2$ $3 \leq a \leq e$</td>
</tr>
<tr>
<td>$\langle -1 \rangle_2 \bigotimes_{i=1}^{e-1} \langle 1 + c_i \mathfrak{p}<em>2^i \rangle</em>{2^{hi}}$</td>
<td>$\bigotimes_{j=0}^{f-1} \langle 1 - 2 \alpha_a^j 2^i \rangle_2 \bigotimes_{i=1}^{e-1} \langle 1 + \alpha_a^j c_i \mathfrak{p}<em>2^i \rangle</em>{2^{hi}} e + 1 \leq a \leq 2e$</td>
</tr>
<tr>
<td>$\bigotimes_{i=1}^{e-1} \langle 1 + c_i \mathfrak{p}<em>2^i \rangle</em>{2^{hi}}$</td>
<td>$\bigotimes_{j=0}^{f-1} \langle 1 + \alpha_a^j c_i \mathfrak{p}<em>2^i \rangle</em>{2^{hi}} 2e + 1 \leq a$</td>
</tr>
</tbody>
</table>
structure $3(\mathbb{Q}_2^{(4)})^{(+)}$.
The multiplicative group $\mathbb{Z}_2^{(4)}(\times)$ of the units has order $3 \cdot 2^6$ and is a direct product of $G_1 = \langle \zeta_{12}^4 \rangle_3$ and a 2-group whose structure is

$$\langle -1 \rangle_2 \langle 1 - \zeta_{12} \rangle_2 \langle 1 + \mathfrak{P}_2 \rangle_4 \langle 1 + \zeta_{12} \mathfrak{P}_2 \rangle_4$$

since $r = 0$, $m = 2$, and $t = 2$.

References


On the structure of residue rings of prime ideals 589


Received: September, 2010