UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

ON THE STRUCTURE OF $(O_K/I)^\times$

By Claus Mazanti Sørensen

Preprint Series No.: 1

January 2000

Ny Munkegade, Bldg. 530
DK-8000 Aarhus C, Denmark

http://www.imf.au.dk
institut@imf.au.dk

ON THE STRUCTURE OF $(O_K/I)^\times$

CLAUS MAZANTI SORENSEN

Abstract. In this paper we investigate the structure of the unit group of O_K/I where K is a global number field, and I is a nonzero ideal in the ring of integers O_K. The case $I = 0$ is given by the Dirichlet unit theorem. By the chinese remainder theorem we may assume that I is a prime power $\mathfrak{p}^n$. We obtain an explicit decomposition of $(O_K/\mathfrak{p}^n)^\times$ in cyclic groups for almost all primes $\mathfrak{p}$, namely those lying above a rational prime p satisfying $p > e$ where $e = e(\mathfrak{p}, \mathbb{Z})$ is the ramification index. In particular we obtain the structure of $(O_K/\mathfrak{p}^n)^\times$ for all unramified $\mathfrak{p}$.

Contents

1. Introduction

In this paper we consider a global number field $K/\mathbb{Q}$ with ring of integers O_K. We will decompose the unit group $(O_K/I)^\times$ in cyclic groups, where I is a nonzero ideal of O_K with prime factors outside the finite set of primes $\mathfrak{p}$ satisfying the inequality $p \le e$, where p is the rational prime under $\mathfrak{p}$ and $e = e(\mathfrak{p}, \mathbb{Z})$ is the ramification index. The case $I = 0$ is classical and due to Dirichlet: $O_K^\times$ is a finitely generated abelian group with rank equal to $r + s - 1$, where r is the number of real primes of K and s is the number of complex primes of K. Thus

$$O_K^\times \approx \mu_K \times \mathbb{Z}^{r+s-1},$$

where μ_K is the finite cyclic group of roots of unity in K. It is easy to find the order of the unit group $(O_K/I)^\times$ for all nonzero I. For by the chinese remainder theorem it follows that, as rings

$$O_K/I \approx O_K/\mathfrak{p}_1^{n_1} \oplus O_K/\mathfrak{p}_2^{n_2} \oplus \cdots \oplus O_K/\mathfrak{p}_t^{n_t},$$

if $I = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\cdots\mathfrak{p}_t^{n_t}$ is the factorization of I in prime powers. Since $O_K/\mathfrak{p}^n$ is a local ring with maximal ideal $\mathfrak{p}/\mathfrak{p}^n$ it follows immediately that

$$\#(O_K/\mathfrak{p}^n)^\times = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}^n) - \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}^n)\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-1} = p^{f(n-1)}(p^f - 1),$$

Document version: 25.11.99.
1991 *Mathematics Subject Classification.* 11A07,11F85,11R04,11R27,13B15.
Key words and phrases. Ramification Theory, Higher Unit Groups.
I would like to thank S. Bentzen and J. Milne for helpful advice in solving this problem.

where $f = f(\mathfrak{p}, \mathbb{Z})$ is the inertia degree and $\mathrm{N}_{K/\mathbb{Q}}(I)$ is the cardinality of the finite ring O_K/I. The idealnorm $\mathrm{N}_{K/\mathbb{Q}}$ is strictly multiplicative. Now we have the order of $(O_K/I)^\times$:

$$\#(O_K/I)^\times = \mathrm{N}_{K/\mathbb{Q}}(I) \prod_{\mathfrak{p}|I} (1 - \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-1}).$$

The first step in finding the structure of $(O_K/I)^\times$ for general nonzero I, is of course to use the chinese remainder theorem to reduce to the case where I is a prime power $\mathfrak{p}^n$, for then we have

$$(O_K/I)^\times \approx (O_K/\mathfrak{p}_1^{n_1})^\times \times (O_K/\mathfrak{p}_2^{n_2})^\times \times \cdots \times (O_K/\mathfrak{p}_t^{n_t})^\times.$$

As already mentioned, all we can do in this paper is to find the structure of $(O_K/\mathfrak{p}^n)^\times$, for primes $\mathfrak{p}$ satisfying the condition $p > e$. The structure theorem that we end up with, is naturally divided in two parts, according to whether $p > e+1$ or $p = e+1$. In the case where $p > e+1$ we obtain the following

Theorem 1.1. *Consider a global number field K with ring of integers O_K. Let $\mathfrak{p}$ be a nonzero prime ideal of O_K satisfying the condition $p > e+1$ where p is the rational prime under $\mathfrak{p}$ and $e = e(\mathfrak{p}, \mathbb{Z})$ is the ramification index relative to $\mathbb{Z}$. Given any positive integer n, the structure of the unit group of $O_K/\mathfrak{p}^n$ is given as follows: Write $n - 1 = qe + r$ where $0 \leq r < e$, then we have the decomposition*

$$(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/(p^f - 1) \oplus \underbrace{\mathbb{Z}/p^q \oplus \cdots \oplus \mathbb{Z}/p^q}_{(e-r)f} \oplus \underbrace{\mathbb{Z}/p^{q+1} \oplus \cdots \oplus \mathbb{Z}/p^{q+1}}_{rf},$$

where $f = f(\mathfrak{p}, \mathbb{Z})$ denotes the inertia degree relative to $\mathbb{Z}$.

In the case where $p = e+1$, nothing is changed if the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$ does not contain all p'th roots of unity. However, if $K_\mathfrak{p}$ *does* contain all p'th roots of unity, a highest order summand decomposes in two cyclic summands and one of them has order p. This is the essence in the case $p = e+1$:

Theorem 1.2. *Consider a global number field K with ring of integers O_K. Let $\mathfrak{p}$ be a nonzero prime ideal of O_K satisfying the condition $p = e+1$ where p is the rational prime under $\mathfrak{p}$ and $e = e(\mathfrak{p}, \mathbb{Z})$ is the ramification index relative to $\mathbb{Z}$. Given any positive integer $n > 1$, the structure of the unit group of $O_K/\mathfrak{p}^n$ is given as follows: Write $n-1 = qe + r$ where $0 \leq r < e$, and define the symbol $\delta = \delta_\mathfrak{p}$ to be 1 if the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$ contains all p'th roots of unity, and to be 0 if not. If $r = 0$ and $q \geq 1$ we have the decomposition*

$$(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/(p^f - 1) \oplus \underbrace{\mathbb{Z}/p \oplus \mathbb{Z}/p^{q-1}}_{\delta} \oplus \underbrace{\mathbb{Z}/p^q \oplus \cdots \oplus \mathbb{Z}/p^q}_{ef-\delta}.$$

If $r > 0$ we have the decomposition

$$(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/(p^f - 1) \oplus \underbrace{\mathbb{Z}/p \oplus \mathbb{Z}/p^q}_{\delta} \oplus \underbrace{\mathbb{Z}/p^q \oplus \cdots \oplus \mathbb{Z}/p^q}_{(e-r)f} \oplus \underbrace{\mathbb{Z}/p^{q+1} \oplus \cdots \oplus \mathbb{Z}/p^{q+1}}_{rf-\delta}.$$

Here $f = f(\mathfrak{p}, \mathbb{Z})$ denotes the inertia degree relative to $\mathbb{Z}$.

For example, theorem 1.2 is perfectly suited for finding the structure of $(\mathbb{Z}[\zeta_m]/\mathfrak{p}^n)^\times$ where $\mathfrak{p}$ lies above a rational prime p dividing m only once: The ramification index is exactly $p-1$, and the completion of $\mathbb{Q}(\zeta_m)$ at $\mathfrak{p}$ (indeed $\mathbb{Q}(\zeta_m)$ itself) contains all p'th roots of unity. In the remaining case where $p \le e$, recent work of A. Vazzana indicates that the structure of the unit group of $O_K/\mathfrak{p}^n$ is not determined by the splitting type of $\mathfrak{p}$. In [V1], Vazzana treats the case of primes dividing 2 for a quadratic field $\mathbb{Q}(\sqrt{d})$, with d squarefree. When 2 is ramified, the structure depends on d. However, by the two theorems above, we know the structure of $(O_K/\mathfrak{p}^n)^\times$ for all unramified $\mathfrak{p}$: If $p > 2$, theorem 1.1 reduces to

$$(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/(p^f-1) \oplus \underbrace{\mathbb{Z}/p^{n-1} \oplus \cdots \oplus \mathbb{Z}/p^{n-1}}_{f}.$$

If $p = 2$, theorem 1.2 reduces to

$$(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/(2^f-1) \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-2} \oplus \underbrace{\mathbb{Z}/2^{n-1} \oplus \cdots \oplus \mathbb{Z}/2^{n-1}}_{f-1},$$

for $n > 1$, because the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$ does contain all 2'th roots of unity, indeed $\pm 1 \in \mathbb{Q}$. If p is totally split in the extension $K/\mathbb{Q}$, we have the canonical isomorphism of rings $O_K/\mathfrak{p}^n \approx \mathbb{Z}/p^n$, and hence $(O_K/\mathfrak{p}^n)^\times \approx (\mathbb{Z}/p^n)^\times$. The structure of this last group $(\mathbb{Z}/p^n)^\times$ is known to coincide with the above when $f = 1$.

2. The structure of $(O_K/\mathfrak{p}^n)^\times$ in the case where $p > e+1$

In this section we will prove theorem 1.1. We consider a global number field $K/\mathbb{Q}$, and a nonzero prime ideal $\mathfrak{p}$ in the ring of integers O_K, satisfying the condition $p > e+1$, where p is the rational prime under $\mathfrak{p}$ and $e = e(\mathfrak{p}, \mathbb{Z})$ is the ramification index relative to $\mathbb{Z}$. Given a positive integer n we will find the structure of the unit group $(O_K/\mathfrak{p}^n)^\times$. First, completion does not change the residue rings, hence

$$O_K/\mathfrak{p}^n \approx O_{K_\mathfrak{p}}/\pi^n,$$

where $O_{K_\mathfrak{p}}$ is the ring of integers in the $p-$adic number field $K_\mathfrak{p}/\mathbb{Q}_p$, and π is the maximal ideal in $O_{K_\mathfrak{p}}$. Now, the n'th unit group $\mathrm{U}_n = 1 + \pi^n$ of $O_{K_\mathfrak{p}}$ fits into the following exact sequence of abelian groups:

$$1 \to \mathrm{U}_n \to O_{K_\mathfrak{p}}^\times \to (O_{K_\mathfrak{p}}/\pi^n)^\times \to 1.$$

The sequence extends to the right since $O_{K_\mathfrak{p}}$ is a local ring with maximal ideal π. Thus we arrive at:

$$(O_K/\mathfrak{p}^n)^\times \approx O_{K_\mathfrak{p}}^\times/\mathrm{U}_n.$$

The next step is to show that for $n = 1$ the above sequence splits. For then $(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/(p^f-1) \oplus \mathrm{U}_1/\mathrm{U}_n$ because $f(\mathfrak{p}, \mathbb{Z}) = f(K_\mathfrak{p}/\mathbb{Q}_p)$, and we are left with studying higher unit groups. To prove this splitting we shall use the following easy corollary of Hensels lemma:

Corollary 2.1. *Let O be a complete discrete valuation ring with residue field k and let $f(X) \in O[X]$. If $\bar{\alpha} \in k$ is a simple root of the reduction $\bar{f}(X) \in k[X]$, there is a unique root $\alpha \in O$ of $f(X)$ with reduction $\bar{\alpha} \in k$, and α is a simple root of $f(X)$.*

The corollary provides a section to the reduction map $O_{K_\mathfrak{p}}^\times \to k_\mathfrak{p}^\times$ as follows: Consider the polynomial $f(X) = X^{q-1} - 1 \in O_{K_\mathfrak{p}}[X]$ where $q = p^f$ is the cardinality of $k_\mathfrak{p}$. The reduction $\bar{f}(X) \in k_\mathfrak{p}[X]$ has the elements of $k_\mathfrak{p}^\times$ as simple roots. Corollary 2.1 implies that each $\bar{\alpha} \in k_\mathfrak{p}^\times$ has a unique lift to a root $\alpha \in O_{K_\mathfrak{p}}^\times$ of $f(X)$. This lift $k_\mathfrak{p}^\times \to O_{K_\mathfrak{p}}^\times$ is a homomorphism and a section to the reduction map. Thus, all we need is the structure of the $p-$group $\mathrm{U}_1/\mathrm{U}_n$. Given any $p-$group A, the number of cyclic components of order p^i in A, is given by the formula

$$\tau_i(A) = \dim_{\mathbb{Z}/p} \frac{p^{i-1}A}{p^iA} - \dim_{\mathbb{Z}/p} \frac{p^iA}{p^{i+1}A},$$

where the quotients are viewed as vector spaces over $\mathbb{Z}/p$ in the canonical way. To see this, prove that this invariant is additive, and then evaluate it on cyclic $p-$groups: $\tau_i(\mathbb{Z}/p^j) = \delta_{ij}$. If we could find the orders of $p^i.\mathrm{U}_1/\mathrm{U}_n$, we could thus read off the dimensions, and hence calculate all the $\tau_i(\mathrm{U}_1/\mathrm{U}_n)$. The next step is obviously to study the $p-$power homomorphism on U_1 and its iterates.

Lemma 2.2. *Put $e_0 = e/(p-1)$. For $\nu > e_0$ the $p-$power homomorphism on U_ν induces an isomorphism $U_\nu \approx U_{e+\nu}$. If $\nu = e_0$ the $p-$power homomorphism $U_\nu \to U_{e+\nu}$ either has kernel and cokernel of order p, or is an isomorphism, according as $K_\mathfrak{p}$ does or does not contain the p'th roots of unity.*

Proof. This is essentially lemma A.4 on page 167 in [M]. A proof is given in the last section. □

Now we use our assumption that $p > e+1$. This is exactly the assumption that $1 > e_0$. Hence the lemma gives us the following string of isomorphisms:

$$p^i : \mathrm{U}_1 \approx \mathrm{U}_{e+1} \approx \mathrm{U}_{2e+1} \approx \cdots \approx \mathrm{U}_{ie+1},$$

and it follows that for $i \geq 0$

$$p^i.\mathrm{U}_1/\mathrm{U}_n = \begin{cases} 1 & \text{if } ie+1 \geq n, \\ \mathrm{U}_{ie+1}/\mathrm{U}_n & \text{if } ie+1 < n. \end{cases} \tag{2.1}$$

The rest is easy: If $(i-1)e+1 \geq n$ we obviously have $\tau_i = 0$. Now suppose that $n-e \leq (i-1)e+1 < n$. Then p^i still kills $\mathrm{U}_1/\mathrm{U}_n$, while p^{i-1} does not. Thus $\tau_i = f(n-1-(i-1)e)$. Next case is where $n-2e \leq (i-1)e+1 < n-e$. Then p^{i+1} still kills $\mathrm{U}_1/\mathrm{U}_n$, while p^i does not. Thus

$$\tau_i = f(n-1-(i-1)e) - f(n-1-ie) - f(n-1-ie) + 0 = -f(n-1-(i+1)e).$$

At last, if $(i-1)e+1 < n-2e$, we have

$$\tau_i = f(n-1-(i-1)e) - f(n-1-ie) - f(n-1-ie) + f(n-1-(i+1)e) = 0.$$

Writing $n-1 = qe+r$ with $0 \leq r < e$ we see that in the case where $r = 0$ and $q \geq 1$ we have

$$\tau_i(\mathrm{U}_1/\mathrm{U}_n) = \begin{cases} 0 & \text{if } i \geq q+1, \\ ef & \text{if } i = q, \\ 0 & \text{if } i = q-1, \\ 0 & \text{if } i < q-1. \end{cases} \tag{2.2}$$

In the case where $r > 0$ we have

$$\tau_i(\mathrm{U}_1/\mathrm{U}_n) = \begin{cases} 0 & \text{if } i \geq q+2, \\ rf & \text{if } i = q+1, \\ (e-r)f & \text{if } i = q, \\ 0 & \text{if } i \leq q-1. \end{cases} \tag{2.3}$$

Thus we have proved theorem 1.1.

3. The structure of $(O_K/\mathfrak{p}^n)^\times$ in the case where $p = e+1$

In this section we will prove theorem 1.2. Most of the proof of theorem 1.1 in the last section can be carried over. The only point where we used that $p > e+1$, was to get the isomorphism $p : \mathrm{U}_1 \approx \mathrm{U}_{e+1}$. If $p = e+1$ we have $e_0 = 1$, and if the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$ does not contain all p'th roots of unity, we *still* have the isomorphism $p : \mathrm{U}_1 \approx \mathrm{U}_{e+1}$ according to lemma 2.2. Thus we have already settled the case $\delta = 0$ of theorem 1.2. Thus, let us assume the following: We consider a global number field $K/\mathbb{Q}$, and a nonzero prime ideal $\mathfrak{p}$ in the ring of integers O_K, satisfying the condition $p = e+1$, where p is the rational prime under $\mathfrak{p}$ and $e = e(\mathfrak{p}, \mathbb{Z})$ is the ramification index relative to $\mathbb{Z}$. We assume that the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$ contains all p'th roots of unity, that is $\delta = 1$. According to lemma 2.2 the $p-$power homomorphism $p : \mathrm{U}_1 \to \mathrm{U}_{e+1}$ has cokernel (and kernel) of order p, and this enables us to calculate the numbers τ_i. We have

$$p^i.\mathrm{U}_1/\mathrm{U}_n = \frac{\mathrm{U}_1^{p^i}\mathrm{U}_n}{\mathrm{U}_n} \subset \frac{\mathrm{U}_{ie+1}\mathrm{U}_n}{\mathrm{U}_n} = \begin{cases} 1 & \text{if } ie+1 \geq n, \\ \mathrm{U}_{ie+1}/\mathrm{U}_n & \text{if } ie+1 < n. \end{cases} \tag{3.1}$$

To find the order of $p^i.\mathrm{U}_1/\mathrm{U}_n$ for all i (and hence all the τ_i), we must find the index above. Now,

$$\mathrm{U}_{ie+1}/\mathrm{U}_1^{p^i} \approx \mathrm{U}_{(i-1)e+1}/\mathrm{U}_1^{p^{i-1}} \approx \cdots \approx \mathrm{U}_{e+1}/\mathrm{U}_1^p \approx \mathbb{Z}/p,$$

for $i \geq 1$. One could therefore hope that the above index is p. This is exactly the case when $ie+1 < n$: All we need to show is that $\mathrm{U}_n \subset \mathrm{U}_1^{p^i}$, and this is easy:

$$\mathrm{U}_n = \mathrm{U}_{n-e}^p = \mathrm{U}_{n-2e}^{p^2} = \cdots = \mathrm{U}_{n-ie}^{p^i} \subset \mathrm{U}_1^{p^i},$$

since $n - ie > 1$. We therefore have all the orders $\#p^i.\mathrm{U}_1/\mathrm{U}_n$:

$$\#p^i.\mathrm{U}_1/\mathrm{U}_n = \begin{cases} p^{f(n-1)} & \text{if } i = 0, \\ 1 & \text{if } i \geq 1 \text{ and } ie+1 \geq n, \\ p^{f(n-1-ie)-1} & \text{if } i \geq 1 \text{ and } ie+1 < n. \end{cases} \tag{3.2}$$

We can now imitate what we did in section 1, and find the numbers τ_i. We will assume that $i \geq 2$ and find τ_1 later. If $(i-1)e+1 \geq n$ we obviously have $\tau_i = 0$. Now suppose that $n - e \leq (i-1)e+1 < n$. Then p^i still kills $\mathrm{U}_1/\mathrm{U}_n$, while p^{i-1} does not. Thus $\tau_i = f(n-1-(i-1)e)-1$. Next case is where $n-2e \leq (i-1)e+1 < n-e$. Then p^{i+1} still kills $\mathrm{U}_1/\mathrm{U}_n$, while p^i does not. Thus

$$\tau_i = f(n-1-(i-1)e)-1-f(n-1-ie)+1-f(n-1-ie)+1 = -f(n-1-(i+1)e)+1.$$

At last, if $(i-1)e+1 < n-2e$, we have

$$\tau_i = f(n-1-(i-1)e)-1-f(n-1-ie)+1-f(n-1-ie)+1+f(n-1-(i+1)e)-1 = 0.$$

Writing $n-1 = qe+r$ with $0 \leq r < e$ we see that in the case where $r=0$ and $q \geq 1$ we have

$$\tau_i(\mathrm{U}_1/\mathrm{U}_n) = \begin{cases} 0 & \text{if } i \geq q+1, \\ ef-1 & \text{if } i = q, \\ 1 & \text{if } i = q-1, \\ 0 & \text{if } i < q-1. \end{cases} \tag{3.3}$$

In the case where $r > 0$ we have

$$\tau_i(\mathrm{U}_1/\mathrm{U}_n) = \begin{cases} 0 & \text{if } i \geq q+2, \\ rf-1 & \text{if } i = q+1, \\ (e-r)f+1 & \text{if } i = q, \\ 0 & \text{if } i \leq q-1. \end{cases} \tag{3.4}$$

To complete the proof of theorem 1.2, we need to show that there is only one component of order p in $\mathrm{U}_1/\mathrm{U}_n$. But we know that the order of $\mathrm{U}_1/\mathrm{U}_n$ is $p^{f(n-1)}$, so in the case $r=0$ we must have

$$f(n-1) = \tau_1 + q - 1 + q(ef-1) \Rightarrow \tau_1 = 1.$$

In the case $r > 0$ we must have

$$f(n-1) = \tau_1 + q((e-r)f+1) + (q+1)(rf-1) \Rightarrow \tau_1 = 1.$$

This completes the proof of theorem 1.2.

4. A few remarks in the case where $p < e+1$

The theorems proved in the previous two sections, show that when $p > e$ the structure of the unit group of $O_K/\mathfrak{p}^n$ is determined by the splitting type of $\mathfrak{p}$ and conversely. When $p \leq e$ this is no longer the case. Let us quote lemma 5.5 on page 258 of [V1] (with a different notation):

Lemma 4.1. *Let d be a squarefree rational integer, and let $K = \mathbb{Q}(\sqrt{d})$. For $n \geq 4$ we have the following:*

(a) If $d \equiv 1$ mod 8, then 2 splits, say $(2) = \mathfrak{p}_1\mathfrak{p}_2$, and

$$(O_K/\mathfrak{p}_i^n)^\times \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-2} \textit{ for } i = 1, 2.$$

(b) If $d \equiv 5$ mod 8, then 2 is inert, say $(2) = \mathfrak{p}$, and

$$(O_K/\mathfrak{p}^n)^\times \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-1} \oplus \mathbb{Z}/2^{n-2} \oplus \mathbb{Z}/3.$$

(c) If $d \equiv 0$ mod 2, then 2 ramifies, say $(2) = \mathfrak{p}^2$, and

$$(O_K/\mathfrak{p}^{2n})^\times \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-2} \oplus \mathbb{Z}/2^n.$$

(d) If $d \equiv 3$ mod 8, then 2 ramifies, say $(2) = \mathfrak{p}^2$, and

$$(O_K/\mathfrak{p}^{2n})^\times \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-1} \oplus \mathbb{Z}/2^{n-1}.$$

(e) If $d \equiv 7$ mod 8, then 2 ramifies, say $(2) = \mathfrak{p}^2$, and

$$(O_K/\mathfrak{p}^{2n})^\times \approx \mathbb{Z}/4 \oplus \mathbb{Z}/2^{n-2} \oplus \mathbb{Z}/2^{n-1}.$$

This is proved in A. Vazzanas thesis [V2]. Note that the cases (a) and (b) are but special cases of theorem 1.2. In the case where $p \leq e$ we cannot give the complete structure of $(O_K/\mathfrak{p}^n)^\times$. However, it is possible to prove, by the methods above, that some components do not appear.

5. A proof of lemma 2.2

For completeness and convenience, we end this paper by giving a detailed proof of lemma 2.2 about the $p-$power homomorphism on U_1. This is essentially lemma A.4 on page 167 in [M]. We want to prove the following:

Lemma 5.1. *Put $e_0 = e/(p-1)$. For $\nu > e_0$ the $p-$power homomorphism on U_ν induces an isomorphism $U_\nu \approx U_{e+\nu}$. If $\nu = e_0$ the $p-$power homomorphism $U_\nu \to U_{e+\nu}$ either has kernel and cokernel of order p, or is an isomorphism, according as $K_\mathfrak{p}$ does or does not contain the p'th roots of unity.*

Proof. In this proof, π denotes a generator for the maximal ideal in $O_{K_\mathfrak{p}}$. For all $a \in O_{K_\mathfrak{p}}$:

$$(1+\pi^\nu a)^p = 1 + p\pi^\nu a + \binom{p}{2}\pi^{2\nu}a^2 + \cdots + \pi^{p\nu}a^p \text{ın} \begin{cases} \mathrm{U}_{\nu+e} & \text{if } \nu \geq e_0, \\ \mathrm{U}_{p\nu} & \text{if } \nu < e_0, \end{cases} \tag{5.1}$$

since p has valuation e, and the binomial coefficients are divisible by p. For $\nu \geq e_0$ the $p-$power homomorphism induces a homomorphism

$$p : \mathrm{U}_\nu/\mathrm{U}_{\nu+1} \to \mathrm{U}_{\nu+e}/\mathrm{U}_{\nu+e+1}.$$

When $\nu > e_0$ this is injective, and hence an isomorphism since both groups have order p^f. Suppose $\nu > e_0$. Given $u \in \mathrm{U}_{\nu+e}$ we will prove that it has a unique p'th root in U_ν. The fact that the p'th root is unique is easy: For suppose $x \in \mathrm{U}_\nu$ and $x^p = 1$. If $x \neq 1$ there is a $\nu_1 \geq \nu$ such that $x \in \mathrm{U}_{\nu_1}$ with ν_1 maximal. Then x gives a nontrivial element in the kernel of the isomorphism

$$\mathrm{U}_{\nu_1}/\mathrm{U}_{\nu_1+1} \approx \mathrm{U}_{\nu_1+e}/\mathrm{U}_{\nu_1+e+1}.$$

Now we will prove that u has a p'th root in U_ν. It will be constructed as the limit of a Cauchy sequence. Claim: There is a sequence $\{x_k\} \subset \mathrm{U}_\nu$ such that

$$u \equiv x_k^p \bmod \mathrm{U}_{\nu+e+k+1} \text{ and } x_{k+1}x_k^{-1} \in \mathrm{U}_{\nu+k+1}.$$

For $k=0$ we choose $x_0 \in \mathrm{U}_\nu$ such that $u \equiv x_0^p \bmod \mathrm{U}_{\nu+e+1}$ via the isomorphism above. Suppose now x_k is given. Then, via the isomorphism, we find $u_{\nu+k+1} \in \mathrm{U}_{\nu+k+1}$ such that

$$u \equiv x_k^p u_{\nu+k+1}^p \bmod \mathrm{U}_{\nu+e+k+2},$$

and put $x_{k+1} = x_k u_{\nu+k+1}$. Now $\mathrm{U}_\nu = 1+\pi^\nu$ is a closed subgroup, so we may find $x \in \mathrm{U}_\nu$ such that $x_k \to x$. But $x_k^p \to u$, so $u = x^p$. This settles the case $\nu > e_0$ of the lemma. Now assume $\nu = e_0$. Let K and C denote the kernel and cokernel of the homomorphism $\mathrm{U}_\nu \to \mathrm{U}_{\nu+e}$, and let $\bar{K}$ and $\bar{C}$ denote the kernel and cokernel of the reduced homomorphism $\mathrm{U}_\nu/\mathrm{U}_{\nu+1} \to \mathrm{U}_{\nu+e}/\mathrm{U}_{\nu+e+1}$. There are unique homomorphisms $K \to \bar{K}$ and $C \to \bar{C}$ that makes the following diagram commute

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & K & \longrightarrow & \mathrm{U}_\nu & \longrightarrow & \mathrm{U}_{\nu+e} & \longrightarrow & C & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \bar{K} & \longrightarrow & \mathrm{U}_\nu/\mathrm{U}_{\nu+1} & \longrightarrow & \mathrm{U}_{\nu+e}/\mathrm{U}_{\nu+e+1} & \longrightarrow & \bar{C} & \longrightarrow & 1 \end{array}$$

The homomorphisms $K \to \bar{K}$ and $C \to \bar{C}$ are isomorphisms as follows from the fact that $p : \mathrm{U}_{\nu+1} \to \mathrm{U}_{\nu+e+1}$ is an isomorphism. Alternatively, one can apply the 3×3 lemma twice to a diagram. If $K_\mathfrak{p}$ does not contain all p'th roots of unity we must have $|K| = |C| = 1$ and $p : \mathrm{U}_\nu \approx \mathrm{U}_{\nu+e}$. If $K_\mathfrak{p}$ *does* contain all p'th roots of unity, we want to to show that they all belong to U_{e_0}. Thus let ζ be a p'th root of unity. If ζ does not belong to U_{e_0}, there is a $\nu < e_0$ such that $\zeta \in \mathrm{U}_\nu$ and we choose ν maximal. Then ζ gives a nontrivial element in the kernel of the isomorphism $\mathrm{U}_\nu/\mathrm{U}_{\nu+1} \approx \mathrm{U}_{p\nu}/\mathrm{U}_{p\nu+1}$. For $\nu = 0$ we have the isomorphism $p^f : \mathrm{U}/\mathrm{U}_1 \approx \mathrm{U}/\mathrm{U}_1$ since $\mathrm{U}/\mathrm{U}_1 \approx k_\mathfrak{p}^\times$ □

References

[M] J. Milnor, *Introduction to Algebraic K−Theory*, Princeton University Press (1971).

[V1] A. Vazzana, *8-Ranks of K_2 of Rings of Integers in Quadratic Number Fields*, Journal of Number Theory 76, 248-264 (1999).

[V2] A. Vazzana, *4-Ranks of K_2 of Rings of Integers in Quadratic Number Fields*, Ph.D. thesis, University of Michigan, 1996.

E-mail address: `mazanti@imf.aau.dk`

Department of Mathematics, Ny Munkegade, 8000 Aarhus C, Denmark