JOURNAL OF COMMUTATIVE ALGEBRA
Volume 11, Number 1, Spring 2019

ON THE CLASS SEMIGROUP OF THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSION OF THE RATIONAL NUMBERS

YUTAKA KONOMI AND TAKAYUKI MORISAWA

ABSTRACT. For a commutative integral domain, the class semigroup and the class group are defined as the quotient of the semigroup of fractional ideals and the group of invertible ideals by the group of principal ideals, respectively. Let p be a prime number. In algebraic number theory, especially in Iwasawa theory, the class group of the ring of integers $\mathcal{O}$ of the cyclotomic $\mathbb{Z}_p$-extension of the rational numbers has been studied for a long time. However, the class semigroup of $\mathcal{O}$ is not well known. We are interested in the structure of the class semigroup of $\mathcal{O}$. In order to study it, we focus on the structure of the complement set of the class group in the class semigroup of $\mathcal{O}$. In this paper, we prove that the complement set is a group and determine its structure.

1. Introduction and main result. Let R be a commutative integral domain. We denote by $\mathcal{F}(R)$, $\mathcal{I}(R)$ and $\mathcal{P}(R)$ the set of all non-zero fractional, invertible and principal ideals of R, respectively. The quotient $\mathcal{C}(R) = \mathcal{I}(R)/\mathcal{P}(R)$ is a commutative group, called the *class group* of R. If R is the ring of integers of an algebraic number field of finite degree, $\mathcal{C}(R)$ is one of the main objects of investigation in algebraic number theory.

We put $\mathcal{S}(R) = \mathcal{F}(R)/\mathcal{P}(R)$. Then, $\mathcal{S}(R)$ is a commutative monoid and called the *class semigroup* of R. If R is a Dedekind domain, then all ideals of R are invertible, that is,

$$\mathcal{F}(R) = \mathcal{I}(R) \quad \text{and} \quad \mathcal{S}(R) = \mathcal{C}(R).$$

However, in general, they are not equal. Thus, it is interesting to study not only the class group $\mathcal{C}(R)$ but also the class semigroup $\mathcal{S}(R)$ for a

2010 AMS *Mathematics subject classification.* Primary 11R23, 11R29.

Keywords and phrases. Class semigroup, class group, $\mathbb{Z}_p$-extension.

The first author was supported by research grants from the Yoshishige Abe Memorial Fund. The second author was supported by JSPS KAKENHI, grant No. 16K17580.

Received by the editors on April 24, 2016, and in revised form on July 26, 2016.

DOI:10.1216/JCA-2019-11-1-69

non-Dedekind domain R. For example, the class semigroup was studied by Zanardo and Zannier [**5**] and Bazzoni and Salce [**4**]. Moreover, for a Prüfer domain R, Bazzoni [**1, 3**] showed that $\mathcal{S}(R)$ is a Clifford semigroup if and only if R is a Prüfer domain of finite character. She also gave the structure of $\mathcal{S}(R)$ as a Clifford semigroup in [**2**].

In this paper, we focus on the ring of integers of the cyclotomic $\mathbb{Z}_p$-extension of the rational numbers $\mathbb{Q}$. This extension plays an important role in Iwasawa theory.

Let p be a prime number. We denote by $\mathbb{B}_n$ the unique real subfield of the $2p^{n+1}$th cyclotomic field $\mathbb{Q}(\mu_{2p^{n+1}})$, whose Galois group $\mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. In addition, we put

$$\mathbb{B} = \bigcup_{n=0}^{\infty} \mathbb{B}_n.$$

Then, the Galois group $\mathrm{Gal}(\mathbb{B}/\mathbb{Q})$ is isomorphic to the p-adic integer ring $\mathbb{Z}_p$ as additive groups. The fields $\mathbb{B}$ and $\mathbb{B}_n$ are called the *cyclotomic $\mathbb{Z}_p$-extension* of $\mathbb{Q}$ and its nth *layer*, respectively.

Let $\mathcal{O}$ be the ring of integers of $\mathbb{B}$. Then $\mathcal{O}$ is not a Dedekind domain, but a non-Noetherian Prüfer domain. Thus, the complement of the group of invertible ideals $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ is non-trivial. Furthermore, $\mathcal{O}$ is a Prüfer domain of finite character, see Proposition 2.3. This property does not hold for all rings of integers of algebraic number fields of infinite degree.

By studying the decomposition of ideals, we show the following theorem.

Theorem 1.1. *We have the following*:

(i) *The set $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ is a group with respect to the usual multiplication of ideals.*
(ii) *The set $\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O})$ is a group with respect to the usual multiplication of ideal classes.*
(iii) *The group $\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O})$ is isomorphic to $\mathcal{C}(\mathcal{O}) \times \mathbb{R}/\mathbb{Z}[1/p]$ as $\mathrm{Gal}(\mathbb{B}/\mathbb{Q})$-modules, where $\mathrm{Gal}(\mathbb{B}/\mathbb{Q})$ acts trivially on $\mathbb{R}/\mathbb{Z}[1/p]$.*

Remark 1.2.

(i) The set $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ does not contain $\mathcal{O}$, which is the unit element of the commutative monoid $\mathcal{F}(\mathcal{O})$. Thus, $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ is not a

submonoid of $\mathcal{F}(\mathcal{O})$. However, $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ is a subsemigroup of $\mathcal{F}(\mathcal{O})$. In particular, the unit element of the group $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ is $\mathfrak{p}$ defined in (4.1).

(ii) In the same manner as $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$, the set $\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O})$ is not a submonoid but a subsemigroup of the commutative monoid $\mathcal{S}(\mathcal{O})$. In particular, the unit element of the group $\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O})$ is $[\mathfrak{p}]$, which is not equal to $[\mathcal{O}]$.

(iii) As noted above, Bazzoni gave the structure of the class semigroup of a general Prüfer domain of finite character as a Clifford semigroup. Since we especially deal with the ring of integers of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, our assertion and proof of Theorem 1.1 (iii) are much simpler and more explicit than hers.

2. Invertible ideal. In this section, we explain the properties related to the invertible ideals of $\mathcal{O}$. We recall that p, $\mathbb{B}$, $\mathbb{B}_n$ and $\mathcal{O}$ denote a prime number, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, its nth layer and ring of integers, respectively. For an ideal I of $\mathcal{O}$ and a non-negative integer n, we put $I_n = I \cap \mathbb{B}_n$. In particular, $\mathcal{O}_n = \mathcal{O} \cap \mathbb{B}_n$ is the ring of integers of $\mathbb{B}_n$.

The next lemma is well known in the theory of cyclotomic fields.

Lemma 2.1.

(i) *The cyclotomic $\mathbb{Z}_p$-extension $\mathbb{B}/\mathbb{Q}$ is unramified outside p.*
(ii) *The prime p is totally ramified in $\mathbb{B}/\mathbb{Q}$.*
(iii) *For any prime number ℓ with $\ell \neq p$, there exists a non-negative integer n such that the decomposition field at ℓ in $\mathbb{B}/\mathbb{Q}$ is $\mathbb{B}_n$.*

The following lemma is easy, but essential.

Lemma 2.2. *For a non-zero ideal I of $\mathcal{O}$, the following are equivalent.*

(i) *I is an invertible ideal.*
(ii) *I is finitely generated over $\mathcal{O}$.*
(iii) *There exists a non-negative integer n such that $I = I_n\mathcal{O}$.*

Proof. Firstly, we assume that I is an invertible ideal. By this assumption, there exists an invertible ideal J with $IJ = \mathcal{O}$, and hence,

there exist $x_1, \ldots, x_k \in I$ and $y_1, \ldots, y_k \in J$ such that $\sum_{i=1}^{k} x_i y_i = 1$. Then, $I = \mathcal{O}x_1 + \cdots + \mathcal{O}x_k$, that is, finitely generated over $\mathcal{O}$. In fact, clearly, we have $I \supset \mathcal{O}x_1 + \cdots + \mathcal{O}x_k$. Conversely, if x is contained in I, then we have

$$x = \sum_{i=1}^{k} (xy_i)x_i \in \mathcal{O}x_1 + \cdots + \mathcal{O}x_k$$

since $IJ = \mathcal{O}$ and $xy_i \in IJ$ for any $1 \leq i \leq k$.

Secondly, suppose that I is finitely generated over $\mathcal{O}$, and let $x_1, \ldots, x_k \in I$ be generators of I over $\mathcal{O}$. Since

$$I = \bigcup_{n=1}^{\infty} I_n,$$

there exists a non-negative integer n such that $x_1, \ldots, x_k$ are contained in I_n. Then, $I = I_n\mathcal{O}$. Actually, it is clear that $I_n\mathcal{O}$ is contained in I. Conversely, if x is contained in I, then there exist $y_1, \ldots, y_k \in \mathcal{O}$ with $x = \sum_{i=1}^{k} x_i y_i$. Hence, we have $x \in I_n\mathcal{O}$ since $x_i \in I_n$ for any $1 \leq i \leq k$.

Finally, we assume that there exists a non-negative integer n with $I = I_n\mathcal{O}$. Since $\mathcal{O}_n$ is a Dedekind domain, we have $\mathcal{F}(\mathcal{O}_n) = \mathcal{I}(\mathcal{O}_n)$, and then I_n is an invertible ideal of $\mathcal{O}_n$. Therefore, there exists an invertible ideal I_n^{-1} of $\mathcal{O}_n$ such that $I_n I_n^{-1} = \mathcal{O}_n$. This implies $I(I_n^{-1}\mathcal{O}) = \mathcal{O}$, that is, I is an invertible ideal of $\mathcal{O}$. □

Lemmas 2.1 and 2.2 lead to the following proposition, which gives value to the study of the class semigroup $\mathcal{S}(\mathcal{O})$.

Proposition 2.3. *The ring $\mathcal{O}$ is a Prüfer domain of finite character, that is, a Prüfer domain in which every non-zero ideal is contained but in a finite number of maximal ideals.*

Remark 2.4. From [**1,** Theorem 2.14], we obtain that the class semigroup $\mathcal{S}(\mathcal{O})$ is a Clifford semigroup.

3. Sequence of integers. We want to treat non-invertible ideals of $\mathcal{O}$ to prove Theorem 1.1. For this purpose, we mention the sequence of integers derived from these ideals.

For a real number α and a non-negative integer n, we put

$$\alpha_n = \lfloor p^n \alpha + 1 \rfloor, \tag{3.1}$$

where $\lfloor \beta \rfloor$ denote the greatest integer not exceeding a real number β. We have the following lemmas.

Lemma 3.1. *Let α be a real number.*

(i) *For any non-negative integer n, we have*

$$p^n \alpha < \alpha_n \leq p^n \alpha + 1.$$

(ii) *For any non-negative integer n, we have*

$$p(\alpha_n - 1) + 1 \leq \alpha_{n+1} \leq p\alpha_n.$$

(iii) *We have*

$$\lim_{n \to \infty} \frac{\alpha_n}{p^n} = \alpha.$$

Lemma 3.2. *Let $\{a_n\}_{n=0}^{\infty}$ be a sequence of integers which satisfies an inequality*

$$p(a_n - 1) + 1 \leq a_{n+1} \leq pa_n \tag{3.2}$$

for any non-negative integer n.

(i) *The sequence $\{a_n/p^n\}_{n=0}^{\infty}$ is monotonic decrease and converge.*

(ii) *Put $\alpha = \lim_{n \to \infty}(a_n/p^n)$. For any non-negative integer n, if α satisfies*

$$\alpha < \frac{a_n}{p^n},$$

then we have $a_n = \alpha_n$.

Proof of Lemma 3.1. The inequality in (i) is clear from the definition of α_n.

Let β be a real number. Then, there exist integers a, b and a real number c such that

$$\beta = a + \frac{b}{p} + \frac{c}{p^2},$$

with $0 \leq b, c < p$. This implies

$$\lfloor \beta + 1 \rfloor = a + 1, \quad \lfloor p\beta + 1 \rfloor = pa + b + 1.$$

Hence, we obtain the inequality

$$p(\lfloor \beta + 1 \rfloor - 1) + 1 \leq \lfloor p\beta + 1 \rfloor \leq p\lfloor \beta + 1 \rfloor.$$

By applying this inequality to $\beta = p^n \alpha$, we get assertion (ii).

From the inequality in (i), we have the inequality

$$\alpha < \frac{\alpha_n}{p^n} \leq \alpha + \frac{1}{p^n}.$$

By the squeeze theorem, we obtain

$$\lim_{n \to \infty} \frac{\alpha_n}{p^n} = \alpha. \qquad \square$$

Proof of Lemma 3.2. From inequality (3.2), we have

$$\frac{a_n - 1}{p^n} \leq \frac{a_{n+1} - 1}{p^{n+1}} < \frac{a_{n+1}}{p^{n+1}} \leq \frac{a_n}{p^n}.$$

Hence, the sequences

$$\left\{ \frac{a_n - 1}{p^n} \right\}_{n=0}^{\infty} \quad \text{and} \quad \left\{ \frac{a_n}{p^n} \right\}_{n=0}^{\infty}$$

are bounded, monotonic, increasing and decreasing, respectively. Thus, they are convergent sequences.

Put α as the limit of a_n/p^n, as n tends to infinity. By the above argument and the assumption of (ii), we have

$$\frac{a_n - 1}{p^n} \leq \alpha < \frac{a_n}{p^n}.$$

Hence, we obtain

$$p^n \alpha < a_n \leq p^n \alpha + 1.$$

Since a_n is an integer, we get $a_n = \alpha_n$. $\square$

4. Fractional ideals. The main purpose of this section is to prove Theorem 4.2, which is analogous to a prime factorization of non-invertible ideals of $\mathcal{O}$. Moreover, we explain why the complement set $\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O})$ has the group structure as a corollary of this theorem (cf., Corollary 4.4).

Let $\mathfrak{p}_n$ be the prime ideal of $\mathcal{O}_n$ above p. Note that $\mathfrak{p}_n$ is a principal ideal for any non-negative integer n. We set

$$\mathfrak{p} = \bigcup_{n=0}^{\infty} \mathfrak{p}_n. \tag{4.1}$$

Then, $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$ above p.

For any real number α, we define an ideal $\mathfrak{p}^\alpha$ as

$$\mathfrak{p}^\alpha = \bigcup_{n=0}^{\infty} \mathfrak{p}_n^{\alpha_n}.$$

In particular, we have $\mathfrak{p}^0 = \mathfrak{p}$.

Lemma 4.1. *Let α and β be real numbers.*

(i) *We have $(\mathfrak{p}^\alpha)_n = \mathfrak{p}_n^{\alpha_n}$.*
(ii) *We have*
$$\mathfrak{p}^\alpha \mathfrak{p}^\beta = \bigcup_{n=0}^{\infty} \mathfrak{p}_n^{\alpha_n+\beta_n}.$$
(iii) *We have $\mathfrak{p}^\alpha \mathfrak{p}^\beta = \mathfrak{p}^{\alpha+\beta}$.*
(iv) *Any ideal $\mathfrak{p}^\alpha$ is a non-invertible ideal.*

Proof. From Lemma 3.1 (ii), we have

$$p(\alpha_n - 1) + 1 \leq \alpha_{n+1} \leq p\alpha_n$$

for any non-negative integer n. This inequality and Lemma 2.1 (ii) imply

$$\mathfrak{p}_{n+1}^{\alpha_{n+1}} \cap \mathbb{B}_n = \mathfrak{p}_n^{\alpha_n}.$$

Hence, we obtain $(\mathfrak{p}^\alpha)_n = \mathfrak{p}_n^{\alpha_n}$.

From the definition of $\mathfrak{p}^\alpha$ and $\mathfrak{p}^\beta$, we have

$$\mathfrak{p}^\alpha \mathfrak{p}^\beta \supset \mathfrak{p}_n^{\alpha_n+\beta_n}$$

for any non-negative integer n, and we get

$$\mathfrak{p}^\alpha \mathfrak{p}^\beta \supset \bigcup_{n=0}^{\infty} \mathfrak{p}_n^{\alpha_n+\beta_n}.$$

Conversely, let z be an element in $\mathfrak{p}^\alpha\mathfrak{p}^\beta$. We can take $x_1, \dots, x_k \in \mathfrak{p}^\alpha$ and

$$y_1, \dots, y_k \in \mathfrak{p}^\beta \quad \text{as } z = \textstyle\sum_{i=1}^k x_i y_i.$$

Then, there exists a non-negative integer n such that $x_i, y_i \in \mathbb{B}_n$ for any $1 \le i \le k$. From (i), x_i and y_i are contained in $\mathfrak{p}_n^{\alpha_n}$ and $\mathfrak{p}_n^{\beta_n}$, respectively; hence, we have

$$z \in \mathfrak{p}_n^{\alpha_n+\beta_n} \subset \bigcup_{n=0}^{\infty} \mathfrak{p}_n^{\alpha_n+\beta_n}.$$

Therefore, we obtain

$$\mathfrak{p}^\alpha\mathfrak{p}^\beta = \bigcup_{n=0}^{\infty} \mathfrak{p}_n^{\alpha_n+\beta_n}.$$

In order to prove (iii), we note that the sequences

$$\left\{\frac{\alpha_n}{p^n}\right\}_{n=0}^{\infty}, \qquad \left\{\frac{\beta_n}{p^n}\right\}_{n=0}^{\infty} \quad \text{and} \quad \left\{\frac{(\alpha+\beta)_n}{p^n}\right\}_{n=0}^{\infty}$$

are monotonically decreasing, and

$$\lim_{n\to\infty}\left(\frac{\alpha_n}{p^n}+\frac{\beta_n}{p^n}\right) = \alpha+\beta = \lim_{n\to\infty}\frac{(\alpha+\beta)_n}{p^n}.$$

From the above equality and Lemma 3.1 (i), for any non-negative integer n, there exists an integer $m \ge n$ such that

$$\frac{\alpha_m}{p^m}+\frac{\beta_m}{p^m} \le \frac{(\alpha+\beta)_n}{p^n}.$$

Hence, we have

$$\mathfrak{p}_n^{(\alpha+\beta)_n} \subset \mathfrak{p}_m^{\alpha_m}\mathfrak{p}_m^{\beta_m} \subset \mathfrak{p}^\alpha\mathfrak{p}^\beta.$$

This implies

$$\mathfrak{p}^{\alpha+\beta} \subset \mathfrak{p}^\alpha\mathfrak{p}^\beta.$$

By the same argument, we obtain

$$\mathfrak{p}_n^{\alpha_n+\beta_n} \subset \mathfrak{p}^{\alpha+\beta}$$

and

$$\mathfrak{p}^\alpha\mathfrak{p}^\beta = \bigcup_{n=0}^{\infty} \mathfrak{p}_n^{\alpha_n+\beta_n} \subset \mathfrak{p}^{\alpha+\beta}$$

from (ii). Therefore, we obtain

$$\mathfrak{p}^{\alpha}\mathfrak{p}^{\beta} = \mathfrak{p}^{\alpha+\beta}.$$

From (iii) and $\mathfrak{p} = \mathfrak{p}^0$, we have $\mathfrak{p}^{\alpha} = \mathfrak{p}^{\alpha}\mathfrak{p}$. If $\mathfrak{p}^{\alpha}$ were invertible, then we would have $\mathcal{O} = \mathfrak{p}$. Hence, $\mathfrak{p}^{\alpha}$ is not an invertible ideal. □

Now, we can show the following theorem which is the aim of this section.

Theorem 4.2. *Let I be a non-zero ideal of $\mathcal{O}$ which is not invertible. Then, there exist an invertible ideal $\mathfrak{a}$ of $\mathcal{O}$ and a real number α such that $I = \mathfrak{a}\mathfrak{p}^{\alpha}$.*

Proof. Let I be a non-zero ideal of $\mathcal{O}$ which is not invertible. For any non-negative integer n, there exist an invertible ideal $\mathfrak{a}_n$ of $\mathcal{O}_n$ and an integer a_n such that

$$I_n = \mathfrak{a}_n\mathfrak{p}_n^{a_n}$$

and $\mathfrak{a}_n$ is coprime to $\mathfrak{p}_n$. We put

$$\mathfrak{a} = \bigcup_{n=0}^{\infty} \mathfrak{a}_n.$$

Since $\mathbb{B}/\mathbb{Q}$ is the cyclotomic $\mathbb{Z}_p$-extension, from Lemma 2.1 (iii), there exists an n_0 such that $\mathfrak{a}_n = \mathfrak{a}_{n_0}\mathcal{O}_n$ for any integer $n \geq n_0$. Hence, we have $\mathfrak{a} = \mathfrak{a}_{n_0}\mathcal{O}$. From Lemma 2.2, this implies that $\mathfrak{a}$ is an invertible ideal.

From the equality $\mathfrak{p}_{n+1}^{a_{n+1}} \cap \mathbb{B}_n = \mathfrak{p}_n^{a_n}$, we have an inequality

$$p(a_n - 1) + 1 \leq a_{n+1} \leq pa_n.$$

From Lemma 3.2 (i), the sequence $\{a_n/p^n\}_{n=0}^{\infty}$ is monotonically decreasing and convergent. Let α be the limit of a_n/p^n as n tends to ∞. Then, we obtain an inequality

$$\frac{a_n - 1}{p^n} \leq \alpha \leq \frac{a_n}{p^n}.$$

Assume that there exists a non-negative integer n_1 such that $a_{n_1}/p^{n_1} = \alpha$. Since the sequence $\{a_n/p^n\}_{n=0}^{\infty}$ is monotonically decreasing and

convergent to α, we have

$$\frac{a_n}{p^n} = \alpha = \frac{a_{n_1}}{p^{n_1}}$$

for any integer $n \geq n_1$. We set $m = \max\{n_0, n_1\}$. Then, we have

$$I_n = \mathfrak{a}_m \mathfrak{p}_m^{a_m} \mathcal{O}_n$$

for any integer $n \geq m$. Hence, $I = \mathfrak{a}_m \mathfrak{p}_m^{a_m} \mathcal{O}$, that is, I is an invertible ideal from Lemma 2.2. This is a contradiction. Therefore, we have an inequality

$$\frac{a_n - 1}{p^n} \leq \alpha < \frac{a_n}{p^n};$$

hence, the equality $a_n = \alpha_n$ follows from Lemma 3.2 (ii). Thus, we obtain

$$I = \mathfrak{a}\mathfrak{p}^{\alpha}. \qquad \square$$

We obtain Theorem 1.1 (i) and (ii) as corollaries of Theorem 4.2 and Lemma 4.1 (iii).

Corollary 4.3. *The set $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$ is a group with respect to the usual multiplication of ideals, that is,*

$$\mathfrak{a}\mathfrak{p}^{\alpha} \cdot \mathfrak{b}\mathfrak{p}^{\beta} = \mathfrak{a}\mathfrak{b}\mathfrak{p}^{\alpha+\beta}.$$

Moreover, the identity element is $\mathfrak{p}$, and the inverse element of $\mathfrak{a}\mathfrak{p}^{\alpha}$ is $\mathfrak{a}^{-1}\mathfrak{p}^{-\alpha}$.

Corollary 4.4. *We have*

$$\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O}) = \{[\mathfrak{a}\mathfrak{p}^{\alpha}] \in \mathcal{S}(\mathcal{O}) \mid \mathfrak{a} \in \mathcal{I}(\mathcal{O}), \alpha \in \mathbb{R}\},$$

and the set $\mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O})$ is a group with respect to the usual multiplication of ideal classes, that is,

$$[\mathfrak{a}\mathfrak{p}^{\alpha}] \cdot [\mathfrak{b}\mathfrak{p}^{\beta}] = [\mathfrak{a}\mathfrak{b}\mathfrak{p}^{\alpha+\beta}].$$

Moreover, the identity element is $[\mathfrak{p}]$, and the inverse element of $[\mathfrak{a}\mathfrak{p}^{\alpha}]$ is $[\mathfrak{a}^{-1}\mathfrak{p}^{-\alpha}]$.

Remark 4.5. Corollary 4.3 implies that $\mathcal{F}(\mathcal{O})$ is the disjoint union of two groups $\mathcal{I}(\mathcal{O})$ and $\mathcal{F}(\mathcal{O}) \setminus \mathcal{I}(\mathcal{O})$, and their identity elements are $\mathcal{O}$ and $\mathfrak{p}$, respectively. Then, the idempotents of $\mathcal{F}(\mathcal{O})$ are $\mathcal{O}$ and $\mathfrak{p}$.

5. Proof of Theorem 1.1 (iii). We define the natural map ρ as

$$\rho \ : \ \mathcal{C}(\mathcal{O}) \times \mathbb{R} \longrightarrow \mathcal{S}(\mathcal{O}) \setminus \mathcal{C}(\mathcal{O}); \quad ([\mathfrak{a}], \alpha) \longmapsto [\mathfrak{a}\mathfrak{p}^{\alpha}].$$

From Theorem 4.2, ρ is a surjective group homomorphism. On the kernel of ρ, we have the following lemma.

Lemma 5.1. *We have*

$$\operatorname{Ker}\rho = \{[\mathcal{O}]\} \times \mathbb{Z}[1/p].$$

Proof. Let $([\mathfrak{a}], \alpha)$ be an element in $\operatorname{Ker}\rho$. Then, there exists an $x \in \mathbb{B}$ such that

$$x\mathfrak{p} = \mathfrak{a}\mathfrak{p}^{\alpha}.$$

We may assume that $x \in \mathbb{B}_n$ and $\mathfrak{a} = \mathfrak{a}_n\mathcal{O}$. Thus, we have

$$x\mathfrak{p}_n = \mathfrak{a}_n\mathfrak{p}_n^{\alpha_n}.$$

Since $\mathfrak{p}_n$ is a principal ideal, $\mathfrak{a}_n$ is principal. Hence, we obtain $[\mathfrak{a}] = [\mathcal{O}]$. Then, there exists a $y \in \mathbb{B}$ such that

$$y\mathfrak{p} = \mathfrak{p}^{\alpha}.$$

We may assume that $y \in \mathbb{B}_n$. Therefore, we obtain

$$\mathfrak{p}_n^{\alpha_n - 1}\mathcal{O}_m = y\mathcal{O}_m = \mathfrak{p}_m^{\alpha_m - 1}$$

for any integer $m \geq n$. Thus, we have

$$\frac{\alpha_n - 1}{p^n} = \frac{\alpha_m - 1}{p^m}$$

for any integer $m \geq n$. Since the sequence $\{(\alpha_n - 1)/p^n\}_{n=0}^{\infty}$ converges to α, we have

$$\alpha = \frac{\alpha_n - 1}{p^n} \in \mathbb{Z}[1/p].$$

Conversely, we take $\alpha \in \mathbb{Z}[1/p]$. Then, there exist an integer a and a non-negative integer n with

$$\alpha = \frac{a}{p^n}.$$

For any integer $m \geq n$, we have

$$\alpha_m = \lfloor p^m\alpha + 1 \rfloor = p^{m-n}a + 1.$$

Hence, we obtain

$$\mathfrak{p}^{\alpha} = \mathfrak{p}_n^{a}\mathfrak{p}.$$

Since $\mathfrak{p}_n$ is a principal ideal, we obtain

$$\rho([\mathcal{O}], \alpha) = [\mathfrak{p}^{\alpha}] = [\mathfrak{p}],$$

that is, $([\mathcal{O}], \alpha)$ is contained in $\operatorname{Ker}\rho$. □

From Corollary 4.4 and Lemma 5.1, we obtain the isomorphism in Theorem 1.1 (iii). Since $\mathfrak{p}_n^{\sigma} = \mathfrak{p}_n$ for any $\sigma \in \mathrm{Gal}(\mathbb{B}/\mathbb{Q})$, we have $\mathfrak{p}^{\sigma} = \mathfrak{p}$. Therefore, $\mathrm{Gal}(\mathbb{B}/\mathbb{Q})$ acts trivially on $\mathbb{R}/\mathbb{Z}[1/p]$.

Acknowledgments. The authors are most grateful to Professor Shoichi Nakajima and Professor Shin Nakano who gave them continuous encouragement and valuable advice.

REFERENCES

1. S. Bazzoni, *Class semigroups of Prüfer domains*, J. Algebra **184** (1996), 613–631.

2. ———, *Groups in the class semigroup of a Prüfer domain of finite character*, Comm. Algebra **28** (2000), 5157–5167.

3. ———, *Clifford regular domains*, J. Algebra **238** (2001), 703–722.

4. S. Bazzoni and L. Salce, *Groups in the class semigroups of valuation domains*, Israel J. Math. **95** (1996), 135–155.

5. P. Zanardo and U. Zannier, *The class semigroup of orders in number fields*, Math. Proc. Cambr. Philos. Soc. **115** (1994), 379–391.

Gakushuin University, Department of Mathematics,Mejiro, Toshima-ku, Tokyo, 171-8588 Japan
Email address: **konomi@math.gakushuin.ac.jp**

Kogakuin University, Division of Liberal Arts, 2665-1 Nakano, Hachioji, Tokyo, 192-0015, Japan
Email address: **morisawa@cc.kogakuin.ac.jp**