THE CONDUCTOR IDEAL OF AN ORDER

KEITH CONRAD

1. Introduction

Let $\mathcal{O}$ be an order in the number field K. When $\mathcal{O} \neq \mathcal{O}_K$, $\mathcal{O}$ is Noetherian and one-dimensional, but is not integrally closed. There is at least one nonzero prime ideal in $\mathcal{O}$ that's not invertible and some nonzero ideal in $\mathcal{O}$ does not have a unique prime ideal factorization, since otherwise $\mathcal{O}$ would turn out to be be integrally closed. We will define a special ideal in $\mathcal{O}$, called its conductor, that is closely related to the noninvertible prime ideals in $\mathcal{O}$. The nonzero ideals in $\mathcal{O}$ that are relatively prime to the conductor are invertible in $\mathcal{O}$ and have unique factorization into prime ideals in $\mathcal{O}$.

Definition 1.1. The *conductor* of an order $\mathcal{O}$ in the number field K is

$$\mathfrak{c} = \mathfrak{c}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subset \mathcal{O}\}.$$

This is a subset of $\mathcal{O}$ since $1 \in \mathcal{O}_K$, so

$$\mathfrak{c} = \{x \in \mathcal{O}_K : x\mathcal{O}_K \subset \mathcal{O}\} = \{x \in \mathcal{O} : x\mathcal{O}_K \subset \mathcal{O}\},$$

and the last formula for $\mathfrak{c}$ shows us that $\mathfrak{c}$ is the annihilator of $\mathcal{O}_K/\mathcal{O}$ as an $\mathcal{O}$-module:

$$\mathfrak{c} = \mathrm{Ann}_{\mathcal{O}}(\mathcal{O}_K/\mathcal{O}).$$

Example 1.2. Let $K = \mathbf{Q}(i)$ and $\mathcal{O} = \mathbf{Z}[2i] = \mathbf{Z} + \mathbf{Z}2i$. For $x = a + 2bi$ in $\mathcal{O}$, where a and b are integers, we have $x\mathbf{Z}[i] \subset \mathcal{O}$ if and only if $xi \in \mathcal{O}$, which is equivalent to a being even. Therefore $\mathfrak{c} = \{2m + 2ni : m, n \in \mathbf{Z}\}$.

Writing the condition $x \in \mathfrak{c}$ as $\mathcal{O}_K \subset \frac{1}{x}\mathcal{O}$ when $x \neq 0$, the conductor is the set of all common denominators when we write the algebraic integers of K as ratios from $\mathcal{O}$, together with 0. Since K is the fraction field of $\mathcal{O}$ and $\mathcal{O}_K$ is a finitely generated $\mathcal{O}$-module (because it is a finitely generated $\mathbf{Z}$-module) there are such common denominators, so $\mathfrak{c} \neq \{0\}$. Explicitly, since the index $m = [\mathcal{O}_K : \mathcal{O}]$ is finite, $m\mathcal{O}_K \subset \mathcal{O}$, so $m \in \mathfrak{c}$.

The conductor is an ideal in $\mathcal{O}$. Since $\mathcal{O} \subset \mathcal{O}_K$, we have $1 \in \mathfrak{c}$ if and only if $\mathcal{O} = \mathcal{O}_K$. So $\mathfrak{c}$ is a proper ideal in $\mathcal{O}$ when $\mathcal{O}$ is a nonmaximal order. The conductor of $\mathcal{O}$ is also an ideal in $\mathcal{O}_K$: if $x \in \mathfrak{c}$ and $\alpha \in \mathcal{O}_K$ then $\alpha x\mathcal{O}_K \subset x\mathcal{O}_K \subset \mathcal{O}$, so $\alpha x \in \mathfrak{c}$. A nonzero ideal of one ring that is also an ideal of a larger ring might seem a bit peculiar. (The principal ideals (3) in $\mathbf{Z}[i]$ and $\mathbf{Z}[2i]$ are written the same way but are *not* the same; the first contains $3i$ and the second does not.) The property of $\mathfrak{c}$ being an ideal in both $\mathcal{O}$ and $\mathcal{O}_K$ leads to the following characterization of it.

Theorem 1.3. *An ideal in $\mathcal{O}_K$ lies in $\mathcal{O}$ if and only if it is contained in $\mathfrak{c}$, so $\mathfrak{c}$ is the largest ideal of $\mathcal{O}_K$ that is contained in $\mathcal{O}$.*

Proof. If $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ that lies in $\mathcal{O}$ then $\mathfrak{a}\mathcal{O}_K = \mathfrak{a} \subset \mathcal{O}$, so $\mathfrak{a} \subset \mathfrak{c}$. Conversely, an ideal in $\mathcal{O}_K$ that is contained in $\mathfrak{c}$ is contained in $\mathcal{O}$ since $\mathfrak{c} \subset \mathcal{O}$. □

Remark 1.4. While every ideal of $\mathcal{O}_K$ that lies in $\mathcal{O}$ is inside $\mathfrak{c}$, not all ideals of $\mathcal{O}$ that lie in $\mathfrak{c}$ are ideals of $\mathcal{O}_K$. When $\mathcal{O} = \mathbf{Z}[2i] = \mathbf{Z} + \mathbf{Z}2i$, the ideal $2\mathcal{O} = \mathbf{Z}2 + \mathbf{Z}4i$ of $\mathcal{O}$ is contained in $\mathfrak{c} = \mathbf{Z}2 + \mathbf{Z}2i$ but $2\mathcal{O}$ is not an ideal in $\mathbf{Z}[i]$ since it contains 2 but not $2i$.

2. Examples

Example 2.1. Let K be a quadratic field. Then $\mathcal{O}_K$ has a $\mathbf{Z}$-basis $\{1, w\}$ (*e.g*, $w = \sqrt{d}$ or $(1+\sqrt{d})/2$ where d is squarefree with $K = \mathbf{Q}(\sqrt{d})$). The orders in K are the rings $\mathbf{Z} + \mathbf{Z}cw$ for $c \geq 1$ (one of each index c in $\mathcal{O}_K$). Set $\mathcal{O} = \mathbf{Z} + \mathbf{Z}cw$.

Since $c\mathcal{O}_K = \mathbf{Z}c + \mathbf{Z}cw \subset \mathcal{O}$, the conductor $\mathfrak{c}$ of $\mathcal{O}$ contains c and thus $c\mathcal{O}_K \subset \mathfrak{c}$. We will prove the reverse containment, so $\mathfrak{c} = c\mathcal{O}_K$. For $x \in \mathfrak{c}$ we can write $x = a + bcw$ with $a, b \in \mathbf{Z}$, so $a = x - c(bw) \in \mathfrak{c}$. Thus $aw \in \mathcal{O} = \mathbf{Z} + \mathbf{Z}cw$, so $c \mid a$, which means $x \in c(\mathbf{Z} + \mathbf{Z}w) = c\mathcal{O}_K$, so $\mathfrak{c} \subset c\mathcal{O}_K$.

The conductor $c\mathcal{O}_K$ is a principal ideal in $\mathcal{O}_K$ but it is *not* principal as an ideal in $\mathcal{O}$ for $c > 1$: the index $[\mathcal{O} : c\mathcal{O}_K]$ is c, while for each nonzero $\alpha \in c\mathcal{O}_K$ the index $[\mathcal{O} : \alpha\mathcal{O}]$ is $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$, which is a multiple of $\mathrm{N}_{K/\mathbf{Q}}(c) = c^2$ and $c^2 > c$.

That $\mathcal{O}$ has conductor $c\mathcal{O}_K$ and index c in $\mathcal{O}_K$ shows the conductor and index of a quadratic order determine each other (among the orders in a fixed quadratic field). For this reason, it is standard to label the conductor as c rather than $c\mathcal{O}_K$. *This is special to the quadratic case.* That is, for orders in quadratic fields the label "conductor" and "index" (in $\mathcal{O}_K$) mean the same thing. For example, the order of conductor 2 in $\mathbf{Q}(i)$ is $\mathbf{Z}[2i]$ and the order of conductor 2 in $\mathbf{Q}(\sqrt{5})$ is $\mathbf{Z}[2\frac{1+\sqrt{5}}{2}] = \mathbf{Z}[\sqrt{5}]$.

Example 2.2. Let K be a number field, $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$ and set $\mathcal{O} = \mathbf{Z} + \mathfrak{a}$, so $\mathfrak{a} \subset \mathcal{O} \subset \mathcal{O}_K$. Letting $\mathfrak{a} \cap \mathbf{Z} = a\mathbf{Z}$, we will show $\mathfrak{c} = d\mathbf{Z} + \mathfrak{a}$ where d is a certain factor of a.

Since $\mathfrak{a} \subset \mathcal{O}$ we have $\mathfrak{a} \subset \mathfrak{c}$ by Theorem 1.3. By the ring isomorphism $\mathcal{O}/\mathfrak{a} = (\mathbf{Z} + \mathfrak{a})/\mathfrak{a} \cong \mathbf{Z}/a\mathbf{Z}$, each ideal in $\mathcal{O}$ containing $\mathfrak{a}$ is $d\mathbf{Z} + \mathfrak{a}$ where $d \mid a$. Therefore $\mathfrak{c} = d\mathbf{Z} + \mathfrak{a}$ where $d \mid a$. What is this d? Since $\mathfrak{a} \cap \mathbf{Z} = a\mathbf{Z}$ and $d \mid a$, d is the smallest positive integer in $\mathfrak{c}$. The condition $d \in \mathfrak{c}$ is the same as $d\mathcal{O}_K \subset \mathcal{O}$, and such integers d are the multiples of the exponent of $\mathcal{O}_K/\mathcal{O}$ (the exponent of a finite abelian group is the least integer annihilating the whole group). So as d we can use the exponent of $\mathcal{O}_K/\mathcal{O}$:

$$\mathcal{O} = \mathbf{Z} + \mathfrak{a} \Longrightarrow \mathfrak{c}_{\mathcal{O}} = d\mathbf{Z} + \mathfrak{a}, \text{ where } d = \text{exponent of } \mathcal{O}_K/\mathcal{O}.$$

As a special case, consider $\mathfrak{a} = c\mathcal{O}_K$ with $c \in \mathbf{Z}^+$ and take $K \neq \mathbf{Q}$, so $n = [K : \mathbf{Q}] \geq 2$. We will show the order $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$ has conductor $c\mathcal{O}_K$. (This generalizes Example 2.1 since for quadratic K, $\mathbf{Z} + c\mathcal{O}_K$ is a subring of index c in $\mathcal{O}_K$.) To determine the exponent of $\mathcal{O}_K/\mathcal{O}$, write $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbf{Z}e_i$, where $e_1 = 1$ (there is always some $\mathbf{Z}$-basis of $\mathcal{O}_K$ containing 1.) Then $\mathcal{O} = \mathbf{Z} \oplus \bigoplus_{i=2}^n \mathbf{Z}ce_i$, so $\mathcal{O}_K/\mathcal{O} \cong \bigoplus_{i=2}^n \mathbf{Z}/c\mathbf{Z} \cong (\mathbf{Z}/c\mathbf{Z})^{n-1}$, which as an abelian group has exponent c (since $n \geq 2$), so

$$\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K \Longrightarrow \mathfrak{c}_{\mathcal{O}} = c\mathbf{Z} + c\mathcal{O}_K = c\mathcal{O}_K.$$

For $c \geq 2$, the principal ideal $c\mathcal{O}_K$ of $\mathcal{O}_K$ is not principal as an ideal in $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$ by the same reasoning used in Example 2.1: this ideal has index c in $\mathcal{O}$ but each nonzero principal ideal of $\mathcal{O}$ that is contained in $c\mathcal{O}_K$ has index in $\mathcal{O}$ that's at least $c^n > c$.

The index formula $[\mathbf{Z} + c\mathcal{O}_K : c\mathcal{O}_K] = c$ tells us that when $c = p$ is prime, $p\mathcal{O}_K$ is a prime ideal in $\mathbf{Z} + p\mathcal{O}_K$.

Remark 2.3. When $c \geq 2$, the ideal $c\mathcal{O}_K$ of $\mathcal{O}_K$ has another interesting property as an ideal in $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$: its minimal generating set as an ideal of $\mathcal{O}$ has size n, where $n = [K : \mathbf{Q}]$, That is a big contrast with $\mathcal{O}_K$ if $n \geq 3$ since all ideals in $\mathcal{O}_K$ have at most 2 generators.

To show $\mathfrak{a} := c\mathcal{O}_K$ has n generators as an ideal in $\mathcal{O}$, we have $\mathfrak{a} \cong \mathbf{Z}^n$ as an additive group, and a $\mathbf{Z}$-basis of $\mathfrak{a}$ is also a generating set of $\mathfrak{a}$ as an ideal in $\mathcal{O}$, so $\mathfrak{a}$ has an n-element generating set as an ideal in $\mathcal{O}$.

To show $\mathfrak{a}$ has no generating set as an ideal in $\mathcal{O}$ of size less than n, we'll look at $\mathfrak{a}/\mathfrak{a}^2$ as an $\mathcal{O}/\mathfrak{a}$-module. Every generating set of $\mathfrak{a}$ as an ideal in $\mathcal{O}$ reduces to a generating set of $\mathfrak{a}/\mathfrak{a}^2$ as an $\mathcal{O}/\mathfrak{a}$-module, so we'll be done by showing $\mathfrak{a}/\mathfrak{a}^2$ can't be generated by less than n elements as an $\mathcal{O}/\mathfrak{a}$-module.

What is $\mathfrak{a}^2$? The definition of a product of ideals in a ring doesn't make direct reference to the ambient ring, so since $\mathfrak{a} = c\mathcal{O}_K$ is an ideal in both $\mathcal{O}_K$ and $\mathcal{O}$ we will compute $\mathfrak{a}^2$ more easily by viewing it as a principal ideal in $\mathcal{O}_K$: $\mathfrak{a}^2 = c^2\mathcal{O}_K$. Then as an abelian group,

$$\mathfrak{a}/\mathfrak{a}^2 = c\mathcal{O}_K/c^2\mathcal{O}_K \cong \mathcal{O}_K/c\mathcal{O}_K \cong (\mathbf{Z}/c\mathbf{Z})^n,$$

so $|\mathfrak{a}/\mathfrak{a}^2| = c^n$. If $\mathfrak{a}/\mathfrak{a}^2$ has an r-element generating set as an $\mathcal{O}/\mathfrak{a}$-module, then there's a surjective $\mathcal{O}/\mathfrak{a}$-linear map $(\mathcal{O}/\mathfrak{a})^r \twoheadrightarrow \mathfrak{a}/\mathfrak{a}^2$, so $|(\mathcal{O}/\mathfrak{a})^r| \geq |\mathfrak{a}/\mathfrak{a}^2| = c^n$. Since $\mathfrak{a} \cap \mathbf{Z} = c\mathcal{O}_K \cap \mathbf{Z} = c\mathbf{Z}$, $\mathcal{O}/\mathfrak{a} = (\mathbf{Z} + \mathfrak{a})/\mathfrak{a} \cong \mathbf{Z}/c\mathbf{Z}$ as rings, so $|(\mathbf{Z}/c\mathbf{Z})^r| \geq c^n$. Thus $r \geq n$.

We saw in Example 2.2 that orders of the form $\mathbf{Z} + c\mathcal{O}_K$ with $c \in \mathbf{Z}^+$ have conductors that are principal ideals in $\mathcal{O}_K$. To find an order whose conductor ideal is nonprincipal in $\mathcal{O}_K$, we look at cubic orders.

Example 2.4. Let $K = \mathbf{Q}(\sqrt[3]{7})$. The ring of integers is $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{7}]$ and $(3) = \mathfrak{p}^3$, where $\mathfrak{p} = (3, 1 - \sqrt[3]{7})$. Set $\mathcal{O} = \mathbf{Z} + \mathfrak{p}^2$.

Since $\mathfrak{p}^2 \cap \mathbf{Z} = 3\mathbf{Z}$, $\mathcal{O}/\mathfrak{p}^2 \cong \mathbf{Z}/3\mathbf{Z}$, so $[\mathcal{O} : \mathfrak{p}^2] = 3$, which means $\mathfrak{p}^2$ is a prime ideal in $\mathcal{O}$. (It looks a bit strange to say $\mathfrak{p}^2$ is a prime ideal, but we're in the ring $\mathcal{O}$, where $\mathfrak{p}$ isn't even a subset.) Since $[\mathcal{O}_K : \mathfrak{p}^2] = \mathrm{N}(\mathfrak{p})^2 = 9$, $[\mathcal{O}_K : \mathcal{O}] = 3$, a prime, so $\mathcal{O}_K/\mathcal{O}$ has exponent 3. By Example 2.2, the conductor of $\mathcal{O}$ is $\mathfrak{c} = 3\mathbf{Z} + \mathfrak{p}^2 = \mathfrak{p}^2$. This is not a principal ideal in $\mathbf{Z}[\sqrt[3]{7}]$ since it has norm 9 and no element of $\mathbf{Z}[\sqrt[3]{7}]$ has norm ± 9:

$$\mathrm{N}_{K/\mathbf{Q}}(a + b\sqrt[3]{7} + c\sqrt[3]{49}) = a^3 + 7b^3 + 49c^3 - 3 \cdot 7abc,$$

so if $a + b\sqrt[3]{7} + c\sqrt[3]{49}$ has norm ± 9 we reduce mod 7 to get $a^3 \equiv \pm 9 \bmod 7$, which has no solution.

Example 2.5. Let $K = \mathbf{Q}(\sqrt[3]{19})$. The ring of integers is

$$\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\sqrt[3]{19} + \mathbf{Z}\frac{1 + \sqrt[3]{19} + \sqrt[3]{19}^2}{3}. \tag{2.1}$$

We will compute the conductor $\mathfrak{c}$ for the order $\mathbf{Z}[\sqrt[3]{19}]$.

This order has not been constructed as $\mathbf{Z} + \mathfrak{a}$, so we can't appeal to Example 2.2 to compute $\mathfrak{c}$. Instead we will compute $\mathfrak{c}$ using the definition of the conductor. For $x = a + b\sqrt[3]{19} + c\sqrt[3]{19}^2$ in $\mathbf{Z}[\sqrt[3]{19}]$, to have $x \in \mathfrak{c}$ means $x\mathcal{O}_K \subset \mathbf{Z}[\sqrt[3]{19}]$, which is equivalent to $xe_i \in \mathbf{Z}[\sqrt[3]{19}]$, where e_1, e_2, e_3 is a $\mathbf{Z}$-basis of $\mathcal{O}_K$. Using the visible $\mathbf{Z}$-basis of $\mathcal{O}_K$ in (2.1) leads to the conditions a, b, c, and $(a + b + c)/3 \in \mathbf{Z}$. Writing $a + b + c = 3d$,

$$x = a(1 - \sqrt[3]{19}^2) + b(\sqrt[3]{19} - \sqrt[3]{19}^2) + d \cdot 3\sqrt[3]{19}^2,$$

so

$$\mathfrak{c} = \mathbf{Z}(1 - \sqrt[3]{19}^2) + \mathbf{Z}(\sqrt[3]{19} - \sqrt[3]{19}^2) + \mathbf{Z} \cdot 3\sqrt[3]{19}^2. \tag{2.2}$$

Expressing the $\mathbf{Z}$-spanning set for $\mathfrak{c}$ in (2.2) in terms of the $\mathbf{Z}$-basis of $\mathcal{O}_K$,

$$\begin{pmatrix} 1 - \sqrt[3]{19}^2 \\ \sqrt[3]{19} - \sqrt[3]{19}^2 \\ 3\sqrt[3]{19} \end{pmatrix} = \begin{pmatrix} 2 & 1 & -3 \\ 1 & 2 & -3 \\ 0 & 3 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt[3]{19} \\ (1 + \sqrt[3]{19} + \sqrt[3]{19}^2)/3 \end{pmatrix}.$$

The matrix has determinant 9, so $[\mathcal{O}_K : \mathfrak{c}] = 9$: the ideal $\mathfrak{c}$ in $\mathcal{O}_K$ has norm 9.

We show by contradiction that $\mathfrak{c}$ is not principal in $\mathcal{O}_K$. If $\mathfrak{c} = \alpha\mathcal{O}_K$ for some $\alpha \in \mathfrak{c}$, $9 = [\mathcal{O}_K : \alpha\mathcal{O}_K] = |\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$. Writing $\alpha = a + b\sqrt[3]{19} + c\sqrt[3]{19}$ with integers a, b, and c,

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = a^3 + 19b^3 + 19^2c^3 - 3 \cdot 19abc,$$

which reduces mod 19 to a^3. Since ± 9 mod 19 is not a cube, we have a contradiction.

We described $\mathfrak{c}$ as an abelian group in (2.2). Let's describe it instead as an ideal in $\mathcal{O}_K$ using two generators (every ideal in $\mathcal{O}_K$ needs at most two generators). We will find all the ideals in $\mathcal{O}_K$ of norm 9 and then identify which one is $\mathfrak{c}$.

Write (α) for the principal ideal $\alpha\mathcal{O}_K$ (*not* $\alpha\mathbf{Z}[\sqrt[3]{19}]$). We will show

$$(3) = \mathfrak{p}_3^2\mathfrak{p}_3', \quad (2 + \sqrt[3]{19}) = \mathfrak{p}_3\mathfrak{p}_3'^2, \quad (-1 + \sqrt[3]{19}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3', \tag{2.3}$$

where $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are distinct prime ideals with norm 3. If $\mathfrak{p}$ is a prime ideal factor of (3) in $\mathcal{O}_K$ then $\mathcal{O}_K/\mathfrak{p}$ is a field of characteristic 3, so $\sqrt[3]{19} \equiv 1 \equiv -2 \bmod \mathfrak{p}$ (proof: check the cubes are congruent). Thus $\mathfrak{p} \mid (2 + \sqrt[3]{19})$ and $\mathfrak{p} \mid (-1 + \sqrt[3]{19})$. This implies $(3) \mid (2 + \sqrt[3]{19})$ if (3) were squarefree, but that's false since $(2 + \sqrt[3]{19})/3$ is not an algebraic integer, so the ideal (3) can't be squarefree. Therefore the prime ideal factorization of (3) has to look like $\mathfrak{p}_3^2\mathfrak{p}_3'$ or $\mathfrak{p}_3^3$. To decide which is correct we use ideal norms. In $\mathcal{O}_K$, an ideal $(a + \sqrt[3]{19})$ with $a \in \mathbf{Z}$ has norm $|a^3 + 19|$, so $(2 + \sqrt[3]{19})$ has norm $27 = 3^3$ and $(-1 + \sqrt[3]{19})$ has norm $18 = 2 \cdot 3^2$. Since the ideals (3) and $(2 + \sqrt[3]{19})$ have norm 27 and are distinct, we can't have $(3) = \mathfrak{p}_3^3$, so $(3) = \mathfrak{p}_3^2\mathfrak{p}_3'$ Since each prime factor of (3) divides $(2 + \sqrt[3]{19})$ and $(-1 + \sqrt[3]{19})$, we have $(2 + \sqrt[3]{19}) = \mathfrak{p}_3\mathfrak{p}_3'^2$ and $(-1 + \sqrt[3]{19}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$.

From the $\mathbf{Z}$-spanning set for $\mathfrak{c}$ in (2.2) plus some algebra, $\mathfrak{c}$ contains 3 and $-1 + \sqrt[3]{19}$, so $(3, -1 + \sqrt[3]{19}) \subset \mathfrak{c}$. Since $(3, -1 + \sqrt[3]{19}) = \gcd((3), (-1 + \sqrt[3]{19})) = \mathfrak{p}_3\mathfrak{p}_3'$, which has norm 9, and we computed earlier that $\mathfrak{c}$ has norm 9,

$$\mathfrak{c} = (3, -1 + \sqrt[3]{19}) = \mathfrak{p}_3\mathfrak{p}_3'. \tag{2.4}$$

From $3\mathcal{O}_K \subset \mathfrak{c} \subset \mathbf{Z}[\sqrt[3]{19}] \subset \mathcal{O}_K$ with each containment being strict (why?), the index of $\mathfrak{c}$ in $\mathbf{Z}[\sqrt[3]{19}]$ is 3, so $\mathfrak{c}$ is a prime ideal in $\mathbf{Z}[\sqrt[3]{19}]$. That does not contradict the factorization in (2.4) since $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are not ideals in (or subsets of) $\mathbf{Z}[\sqrt[3]{19}]$.

3. Ideals relatively prime to the conductor

A non-maximal order $\mathcal{O}$ doesn't have unique factorization of ideals, so we need to be careful about the use of divisibility terminology for ideals in $\mathcal{O}$. We say two (nonzero) ideals $\mathfrak{b}$ and $\mathfrak{b}'$ in $\mathcal{O}$ are *relatively prime*[1] when $\mathfrak{b} + \mathfrak{b}' = (1) = \mathcal{O}$. This condition implies the only common ideal factor of $\mathfrak{b}$ and $\mathfrak{b}'$ is $\mathcal{O}$, but not conversely if $\mathcal{O} \neq \mathcal{O}_K$. For $\beta \in \mathcal{O}$, we say β and $\mathfrak{b}$ are relatively prime when the ideals $\beta\mathcal{O}$ and $\mathfrak{b}$ are relatively prime. Ideals in $\mathcal{O}$ that are relatively prime to the conductor of $\mathcal{O}$ turn out to have many properties of ideals in $\mathcal{O}_K$.

[1]Also called co-maximal.

Theorem 3.1. *If a nonzero ideal $\mathfrak{b}$ of $\mathcal{O}$ is relatively prime to the conductor, then $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$.*

Proof. Trivially $\mathcal{O} \subset \{x \in K : x\mathfrak{b} \subset \mathfrak{b}\}$. To get the reverse inclusion, pick $x \in K$ such that $x\mathfrak{b} \subset \mathfrak{b}$. Since $\mathfrak{b} \cong \mathbf{Z}^n$ as a $\mathbf{Z}$-module, x is integral over $\mathbf{Z}$, so $x \in \mathcal{O}_K$. Why is $x \in \mathcal{O}$? Since $\mathfrak{b} + \mathfrak{c} = \mathcal{O}$, we can write $b + c = 1$ for some $b \in \mathfrak{b}$ and $c \in \mathfrak{c}$. Then $x = x \cdot 1 = xb + xc$. We have $xb \in \mathfrak{b}$ by the assumption on x and $xc \in \mathcal{O}$ since $c \in \mathfrak{c}$ and $x \in \mathcal{O}_K$. Therefore $x \in \mathcal{O}$. □

The converse of Theorem 3.1 has counterexamples in every nonmaximal order $\mathcal{O}$. For each nonzero principal ideal $\mathfrak{b} = \beta\mathcal{O}$ contained in the conductor $\mathfrak{c}$, $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$ since $\mathfrak{b}$ is invertible (all nonzero principal ideals in $\mathcal{O}$ are invertible), but $\mathfrak{b}$ is not relatively prime to the conductor: $\mathfrak{b} + \mathfrak{c} = \mathfrak{c} \neq \mathcal{O}$.

Lemma 3.2. *Let $\mathfrak{b}$ be a fractional $\mathcal{O}$-ideal.*

(1) *If $\mathfrak{b}$ is invertible as a fractional $\mathcal{O}$-ideal then its inverse must be*
$$\widetilde{\mathfrak{b}} := \{x \in K : x\mathfrak{b} \subset \mathcal{O}\}.$$
(2) *If $\mathfrak{b} \subsetneqq \mathcal{O}$ then $\mathcal{O} \subsetneqq \widetilde{\mathfrak{b}}$. That is, some $x \notin \mathcal{O}$ satisfies $x\mathfrak{b} \subset \mathcal{O}$.*

Proof. 1) Suppose $\mathfrak{b}$ has an inverse as a fractional $\mathcal{O}$-ideal, say $\mathfrak{b}\mathfrak{b}' = \mathcal{O}$. Then $\mathfrak{b}' \subset \widetilde{\mathfrak{b}}$. Multiplying both sides by $\mathfrak{b}$, we get $\mathcal{O} \subset \mathfrak{b}\widetilde{\mathfrak{b}} \subset \mathcal{O}$, so $\mathfrak{b}\widetilde{\mathfrak{b}} = \mathcal{O}$. Multiplying both sides by $\mathfrak{b}'$, $\widetilde{\mathfrak{b}} = \mathfrak{b}'$.

2) Choose a maximal ideal $\mathfrak{p} \supset \mathfrak{b}$. Then $\widetilde{\mathfrak{b}} \supset \widetilde{\mathfrak{p}}$, so it suffices to show $\mathcal{O} \subsetneqq \widetilde{\mathfrak{p}}$, which is proved in the same way as in the case of $\mathcal{O}_K$ itself, as that argument only depends on $\mathcal{O}_K$ being a Noetherian one-dimensional domain, which is true of $\mathcal{O}$ too. □

Remark 3.3. In a nonmaximal order $\mathcal{O}$, a nonzero ideal $\mathfrak{b}$ in both $\mathcal{O}$ and $\mathcal{O}_K$ is *not* invertible as a fractional $\mathcal{O}$-ideal: if it were then
$$\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O},$$
but since $\mathfrak{b}$ *is* invertible as a fractional $\mathcal{O}_K$-ideal,
$$\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}_K.$$
This is a contradiction since $\mathcal{O} \neq \mathcal{O}_K$.

Theorem 3.4. *For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the following are equivalent:*

(1) *$\mathfrak{p}$ is invertible as a fractional $\mathcal{O}$-ideal,*
(2) *$\{x \in K : x\mathfrak{p} \subset \mathfrak{p}\} = \mathcal{O}$.*

Proof. (1) $\Rightarrow$ (2): This is true of all ideals in $\mathcal{O}$, not just primes.

(2) $\Rightarrow$ (1): We prove the contrapositive. By Lemma 3.2, there is $y \notin \mathcal{O}$ such that $y\mathfrak{p} \subset \mathcal{O}$. Then
$$\mathfrak{p} \subset (\mathcal{O} + y\mathcal{O})\mathfrak{p} \subset \mathfrak{p} + y\mathfrak{p} \subset \mathcal{O},$$
so $(\mathcal{O}+y\mathcal{O})\mathfrak{p}$ is either $\mathfrak{p}$ or $\mathcal{O}$. If $\mathfrak{p}$ is not invertible, $(\mathcal{O}+y\mathcal{O})\mathfrak{p} = \mathfrak{p}$. Therefore $\{x \in K : x\mathfrak{p} \subset \mathfrak{p}\}$ contains y, which is not in $\mathcal{O}$. □

Example 3.5. In Theorem 3.4, (2) does not imply (1) in general when $\mathfrak{p}$ is replaced by a nonprime ideal. In the order $\mathcal{O} = \mathbf{Z} + 2\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}2\sqrt[3]{2} + \mathbf{Z}2\sqrt[3]{4}$ of $K = \mathbf{Q}(\sqrt[3]{2})$, the $\mathbf{Z}$-lattice $\mathfrak{b} = \mathbf{Z}8+\mathbf{Z}2\sqrt[3]{2}+\mathbf{Z}2\sqrt[3]{4}$ is an ideal in $\mathcal{O}$ that is not a prime ideal since $\mathcal{O}/\mathfrak{b} \cong \mathbf{Z}/8\mathbf{Z}$. Check as an exercise that $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$ and $\mathfrak{b}\widetilde{\mathfrak{b}} = 2\mathcal{O}_K \subsetneqq \mathcal{O}$, so Lemma 3.2 tells us $\mathfrak{b}$ is not invertible as a fractional $\mathcal{O}$-ideal.

Theorem 3.6. *An ideal in $\mathcal{O}$ that is relatively prime to the conductor is a product of invertible prime ideals. In particular, every ideal in $\mathcal{O}$ that is relatively prime to the conductor is invertible.*

The first part of the theorem applies to the ideal $\mathcal{O}$ itself using an empty product of invertible prime ideals.

Proof. If $\mathfrak{b}$ is a prime ideal relatively prime to the conductor then it is invertible by Theorems 3.1 and 3.4. Now assume $\mathfrak{b}$ is relatively prime to the conductor and is not prime, and $\mathfrak{b} \neq \mathcal{O}$. Let $\mathfrak{p} \supset \mathfrak{b}$ for a maximal ideal $\mathfrak{p}$. Then $\mathfrak{p} + \mathfrak{c} \supset \mathfrak{b} + \mathfrak{c} = \mathcal{O}$, so $\mathfrak{p}$ is relatively prime to the conductor, hence $\mathfrak{p}$ is invertible. Let $\mathfrak{b}' = \mathfrak{p}^{-1}\mathfrak{b}$, so $\mathfrak{b}' \subset \mathcal{O}$ and $\mathfrak{p}\mathfrak{b}' = \mathfrak{b}$. Since $\mathfrak{b} \neq \mathfrak{p}$, $\mathfrak{b}' \neq \mathcal{O}$. Since $\mathfrak{p}\mathfrak{b}' \subset \mathfrak{b}'$ and the inclusion is strict (if $\mathfrak{b}' = \mathfrak{p}\mathfrak{b}'$ then for all $k \geq 0$ we have $\mathfrak{b}' = \mathfrak{p}^k\mathfrak{b}' \subset \mathfrak{p}^k$, which is a contradiction for large k since $[\mathcal{O} : \mathfrak{p}^k]$ gets large with k while $[\mathcal{O} : \mathfrak{b}']$ is finite), $\mathfrak{b}'$ has smaller index in $\mathcal{O}$ than $\mathfrak{b}$. Since $\mathfrak{b}' \supset \mathfrak{b}$ and $\mathfrak{b} + \mathfrak{c} = \mathcal{O}$, $\mathfrak{b}' + \mathfrak{c} = \mathcal{O}$, so by induction on the index $\mathfrak{b}'$ is a product of invertible prime ideals. Therefore $\mathfrak{b} = \mathfrak{p}\mathfrak{b}'$ is such a product. □

Being relatively prime to the conductor is sufficient to imply invertibility, but it is not necessary. Nonzero principal ideals contained in the conductor are trivially invertible but are not relatively prime to the conductor (if $\mathcal{O} \neq \mathcal{O}_K$).

Corollary 3.7. *If $\mathfrak{b}$ is an ideal in $\mathcal{O}$ that is relatively prime to the conductor, let*

$$\mathcal{O} = \mathfrak{b}_0 \supset \mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_{\ell-1} \supset \mathfrak{b}_\ell = \mathfrak{b}$$

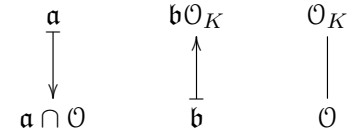
provide a Jordan-Hölder filtration of $\mathcal{O}/\mathfrak{b}$ (that is, each $\mathfrak{b}_i/\mathfrak{b}_{i+1}$ is a simple $\mathcal{O}$-module). Writing $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathcal{O}/\mathfrak{p}_i$ for a nonzero prime ideal $\mathfrak{p}_i$, $\mathfrak{b} = \mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_{\ell-1}$.

Proof. By Theorem 3.6 there is a factorization $\mathfrak{b} = \mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_{k-1}$ where the $\mathfrak{q}_i$'s are invertible prime ideals. This leads to a Jordan-Hölder filtration for $\mathcal{O}/\mathfrak{b}$ using $\mathfrak{b}'_0 = \mathcal{O}$ and $\mathfrak{b}'_i = \mathfrak{q}_0 \cdots \mathfrak{q}_{i-1}$ for $1 \leq i \leq k$. Then $\mathfrak{b}'_i/\mathfrak{b}'_{i+1} = \mathfrak{b}'_i/\mathfrak{b}'_i\mathfrak{q}_i \cong \mathcal{O}/\mathfrak{q}_i$ since $\mathfrak{b}'_i$ is invertible. Comparing this Jordan-Hölder filtration of $\mathcal{O}/\mathfrak{b}$ to the filtration with the $\mathfrak{b}_i$'s, the uniqueness in the Jordan-Hölder theorem for $\mathcal{O}$-modules[2] says $\ell = k$ and $\mathfrak{q}_i = \mathfrak{p}_i$ after reindexing. □

Here is the main theorem connecting ideals in $\mathcal{O}$ with ideals in $\mathcal{O}_K$. We get a one-to-one correspondence as long as we stay relatively prime to the conductor.

Theorem 3.8. *Let $\mathcal{O}$ be an order in K with conductor $\mathfrak{c}$.*

1. *For each $\mathcal{O}_K$-ideal $\mathfrak{a}$ that is relatively prime to $\mathfrak{c}$, $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal relatively prime to $\mathfrak{c}$ and the natural ring homomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ is an isomorphism.*
2. *For each $\mathcal{O}$-ideal $\mathfrak{b}$ that is relatively prime to $\mathfrak{c}$, $\mathfrak{b}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal relatively prime to $\mathfrak{c}$ and the natural ring homomorphism $\mathcal{O}/\mathfrak{b} \to \mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$ is an isomorphism.*
3. *The nonzero ideals relatively prime to $\mathfrak{c}$ in $\mathcal{O}_K$ and in $\mathcal{O}$ are in bijection by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ and $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ and these bijections are multiplicative: $(\mathfrak{a} \cap \mathcal{O})(\mathfrak{a}' \cap \mathcal{O}) = \mathfrak{a}\mathfrak{a}' \cap \mathcal{O}$ and $(\mathfrak{b}\mathcal{O}_K)(\mathfrak{b}'\mathcal{O}_K) = \mathfrak{b}\mathfrak{b}'\mathcal{O}_K$.*



[2]See Theorem 8.9 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

Proof. (1) When $\mathfrak{a}+\mathfrak{c} = \mathcal{O}_K$,

$$\mathcal{O} = \mathcal{O}_K \cap \mathcal{O} = (\mathfrak{a}+\mathfrak{c}) \cap \mathcal{O} \subset \mathfrak{a} \cap \mathcal{O} + \mathfrak{c} \subset \mathcal{O},$$

so $\mathfrak{a} \cap \mathcal{O} + \mathfrak{c} = \mathcal{O}$. The natural ring homomorphism $\mathcal{O} \to \mathcal{O}_K/\mathfrak{a}$ has kernel $\mathfrak{a} \cap \mathcal{O}$ and it is surjective since the equation $\mathcal{O}_K = \mathfrak{a} + \mathfrak{c}$ shows $\mathcal{O}_K/\mathfrak{a}$ is represented by $\mathfrak{c} \subset \mathcal{O}$.

(2) When $\mathfrak{b} + \mathfrak{c} = \mathcal{O}$ we have $1 \in \mathfrak{b} + \mathfrak{c}$, so $\mathfrak{b}\mathcal{O}_K + \mathfrak{c} = \mathcal{O}_K$ and

$$\mathfrak{b} \subset \mathfrak{b}\mathcal{O}_K \cap \mathcal{O} = (\mathfrak{b}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} \subset \mathfrak{b}(\mathfrak{b}+\mathfrak{c}) \subset \mathfrak{b},$$

so $\mathfrak{b}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{b}$. The natural ring homomorphism $\mathcal{O} \to \mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$ has kernel $\mathfrak{b}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{b}$ and it is surjective since the equation $\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K + \mathfrak{c}$ shows $\mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$ is represented by $\mathfrak{c} \subset \mathcal{O}$.

(3) If $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ such that $\mathfrak{a} + \mathfrak{c} = \mathcal{O}_K$, we saw in (1) that $\mathfrak{a} \cap \mathcal{O} + \mathfrak{c} = \mathcal{O}$, so

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + \mathfrak{c}) \subset \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}) + \mathfrak{a}\mathfrak{c} \subset \mathcal{O}_K(\mathfrak{a} \cap \mathcal{O}) + (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K \subset \mathfrak{a}.$$

Therefore $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$. If $\mathfrak{b}$ is an ideal in $\mathcal{O}$ such that $\mathfrak{b} + \mathfrak{c} = \mathcal{O}$, we saw in (2) that $\mathfrak{b}\mathcal{O}_K + \mathfrak{c} = \mathcal{O}_K$ and $\mathfrak{b}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{b}$.

To show these maps are multiplicative, we only need to check one of them since the correspondence is a bijection, and the identity $(\mathfrak{b}\mathcal{O}_K)(\mathfrak{b}'\mathcal{O}_K) = \mathfrak{b}\mathfrak{b}'\mathcal{O}_K$ is obvious. □

Corollary 3.9. *The nonzero prime ideals $\mathfrak{P}$ in $\mathcal{O}_K$ and $\mathfrak{p}$ in $\mathcal{O}$ that are relatively prime to the conductor $\mathfrak{c}$ of $\mathcal{O}$ are in bijection by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$ and $\mathfrak{p} \mapsto \mathfrak{p}\mathcal{O}_K$.*

Proof. When $\mathfrak{P}$ in $\mathcal{O}_K$ is relatively prime to $\mathfrak{c}$ and $\mathfrak{p}$ in $\mathcal{O}$ is relatively prime to $\mathfrak{c}$, Theorem 3.8 says the rings $\mathcal{O}_K/\mathfrak{P}$ and $\mathcal{O}/(\mathfrak{P} \cap \mathcal{O})$ are isomorphic, as are the rings $\mathcal{O}/\mathfrak{p}$ and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. So one is a domain if and only if the other one is. □

Corollary 3.10. *If $\beta \in \mathcal{O}$ and the principal ideal $\beta\mathcal{O}_K$ is relatively prime to the conductor of $\mathcal{O}$ then $\beta\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$.*

Proof. The indices $[\mathcal{O} : \beta\mathcal{O}_K \cap \mathcal{O}]$ and $[\mathcal{O}_K : \beta\mathcal{O}_K]$ are equal by Theorem 3.8 and $[\mathcal{O}_K : \beta\mathcal{O}_K]$ and $[\mathcal{O} : \beta\mathcal{O}]$ are equal since each is $|\mathrm{N}_{K/\mathbf{Q}}(\beta)|$. Therefore $[\mathcal{O} : \beta\mathcal{O}_K \cap \mathcal{O}] = [\mathcal{O} : \beta\mathcal{O}]$, so the inclusions $\beta\mathcal{O} \subset \beta\mathcal{O}_K \cap \mathcal{O} \subset \mathcal{O}$ imply $[\beta\mathcal{O}_K \cap \mathcal{O} : \beta\mathcal{O}] = 1$, so $\beta\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$. □

Corollary 3.11. *The ideals in $\mathcal{O}$ that are relatively prime to the conductor have unique factorization into prime ideals relatively prime to the conductor. All but finitely many prime ideals in $\mathcal{O}$ are relatively prime to the conductor.*

Proof. Let $\mathfrak{c}$ be the conductor of $\mathcal{O}$. The bijection $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ from ideals in $\mathcal{O}$ relatively prime to $\mathfrak{c}$ to ideals in $\mathcal{O}_K$ relatively prime to $\mathfrak{c}$ is multiplicative by Theorem 3.8 and is a bijection between the primes in both sets by Corollary 3.9, so unique factorization of ideals in $\mathcal{O}_K$ relatively prime to $\mathfrak{c}$ implies unique factorization of ideals in $\mathcal{O}$ relatively prime to $\mathfrak{c}$.

For each prime ideal $\mathfrak{p}$ in $\mathcal{O}$, $\mathfrak{p} + \mathfrak{c}$ is either $\mathfrak{p}$ or $\mathcal{O}$. We have $\mathfrak{p}$ not relatively prime to $\mathfrak{c}$ if and only if $\mathfrak{p} + \mathfrak{c} = \mathfrak{p}$, which is the same as $\mathfrak{c} \subset \mathfrak{p}$. Since $\mathcal{O}/\mathfrak{c}$ is finite, there are finitely many prime ideals in $\mathcal{O}$ containing $\mathfrak{c}$ and these are the only primes no relatively prime to $\mathfrak{c}$. (Or, since $\mathcal{O}$ is a Noetherian domain, $\mathfrak{c} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some nonzero primes $\mathfrak{p}_i$, and every prime $\mathfrak{p} \supset \mathfrak{c}$ is some $\mathfrak{p}_i$.) □

If we take away the condition of being relatively prime to the conductor, Theorem 3.8 and Corollaries 3.9, 3.10, and 3.11 all break down.

Theorem 3.8: Let $K \neq \mathbf{Q}$ and $\mathcal{O}$ be a nonmaximal order in K, with conductor $\mathfrak{c}$. Then $\mathfrak{c} \cap \mathcal{O} = \mathfrak{c}$ since $\mathfrak{c} \subset \mathcal{O}$ and $\mathfrak{c}\mathcal{O}_K = \mathfrak{c}$ since $\mathfrak{c}$ is an ideal in $\mathcal{O}_K$. The natural ring homomorphism $\mathcal{O}/\mathfrak{c} \to \mathcal{O}_K/\mathfrak{c}$ is injective but it is not surjective since $\mathcal{O}$ is smaller than $\mathcal{O}_K$.

For the particular order $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$ where $c > 1$, with conductor $\mathfrak{c} = c\mathcal{O}_K$, the ideal $\mathfrak{b} = c\mathcal{O}$ in $\mathcal{O}$ satisfies $\mathfrak{b}\mathcal{O}_K \cap \mathcal{O} = c\mathcal{O}_K \cap \mathcal{O} = c\mathcal{O}_K \supsetneq \mathfrak{b}$.

Let p be a prime that ramifies in K and take $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$, with conductor $p\mathcal{O}_K$. Pick a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ lying over p with $e(\mathfrak{p}|p) \geq 2$ and set $\mathfrak{a}_i = \mathfrak{p}^i$ for $1 \leq i \leq e(\mathfrak{p}|p)$, so $p \in \mathfrak{a}_i$. Since $[\mathcal{O} : p\mathcal{O}_K] = p$, from $p\mathcal{O}_K \subset \mathfrak{a}_i \cap \mathcal{O} \subsetneq \mathcal{O}$ we get $\mathfrak{a}_i \cap \mathcal{O} = p\mathcal{O}_K$. There are $e(\mathfrak{p}|p) \geq 2$ ideals $\mathfrak{a}_i$ and they all meet $\mathcal{O}$ in the same ideal. For $1 \leq i \leq e(\mathfrak{p}|p) - 1$, $(\mathfrak{a}_i \cap \mathcal{O})\mathcal{O}_K = p\mathcal{O}_K \subsetneq \mathfrak{a}_i$, and this holds at $i = e(\mathfrak{p}|p)$ too unless p is totally ramified in K.

Corollary 3.9: For $K \neq \mathbf{Q}$, p ramifying in K, and $\mathfrak{p}$ lying over p in $\mathcal{O}_K$ with $e(\mathfrak{p}|p) \geq 2$, the ideals $\mathfrak{a}_i = \mathfrak{p}^i$ in $\mathcal{O}_K$ for $2 \leq i \leq e(\mathfrak{p}|p)$ are not prime but in $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$ the ideals $\mathfrak{a}_i \cap \mathcal{O} = p\mathcal{O}_K$ are all the same prime. (If $\mathfrak{a}$ is prime then $\mathfrak{a} \cap \mathcal{O}$ must be prime since $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O})$ embeds into the domain $\mathcal{O}_K/\mathfrak{a}$.)

Suppose $K \neq \mathbf{Q}$ and p is inert in K. (Some K have no inert primes, but every quadratic field has infinitely many inert primes, so we don't lack for lots of examples of this.) Set $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$. The ideal $\mathfrak{b} = p\mathcal{O}$ is not prime in $\mathcal{O}$ since it is not maximal: $p\mathcal{O} \subsetneq p\mathcal{O}_K \subsetneq \mathcal{O}$. But $\mathfrak{b}\mathcal{O}_K = p\mathcal{O}_K$ is prime in $\mathcal{O}_K$ since p is inert in K.

Corollary 3.10: Let $K \neq \mathbf{Q}$ and $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$ for $c > 1$, with conductor $c\mathcal{O}_K$. Then $c \in \mathcal{O}$, but $c\mathcal{O}_K \cap \mathcal{O} = c\mathcal{O}_K \neq c\mathcal{O}$. (In fact, $c\mathcal{O}_K$ is not even a principal ideal in $\mathcal{O}$ by Example 2.2.)

Corollary 3.11: For $K \neq \mathbf{Q}$, set $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$ with $c > 1$. For a prime factor p of c, the ideal $p\mathcal{O}$ in $\mathcal{O}$ is not a product of prime ideals in $\mathcal{O}$.

Returning to Theorem 3.8, rather than just remove the relative primality to the conductor let's replace it with the weaker condition of being an invertible fractional ideal. Is the theorem true then? No: in a nonmaximal order $\mathcal{O}$, the conductor $\mathfrak{c}$ is invertible in $\mathcal{O}_K$ but $\mathfrak{c} \cap \mathcal{O} = \mathfrak{c}$ is not invertible in $\mathcal{O}$ (Remark 3.3). If we add the assumption (not automatic!) that $\mathfrak{a} \cap \mathcal{O}$ is invertible in $\mathcal{O}$, is $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \cong \mathcal{O}_K/\mathfrak{a}$ by the natural map? And if we assume $\mathfrak{b}$ is invertible in $\mathcal{O}$, is $\mathcal{O}/\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$? For a counterexample to the second question, suppose $K \neq \mathbf{Q}$ contains an inert prime p. The order $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$ contains the ideal $\mathfrak{b} = p\mathcal{O}$, which is not maximal since $\mathcal{O} \supsetneq p\mathcal{O}_K \supsetneq p\mathcal{O}$, and that means $\mathcal{O}/\mathfrak{b} = \mathcal{O}/p\mathcal{O}$ is not a field but $\mathcal{O}_K/\mathfrak{b}\mathcal{O}_K = \mathcal{O}_K/p\mathcal{O}_K$ is a field since p is inert in K. (The rings $\mathcal{O}/p\mathcal{O}$ and $\mathcal{O}_K/p\mathcal{O}_K$ have the same size, but the natural map between them is neither injective nor surjective.) Let's go back to the first question: is $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \cong \mathcal{O}_K/\mathfrak{a}$ when $\mathfrak{a} \cap \mathcal{O}$ is invertible in $\mathcal{O}$? By what we've seen so far you should think there is a counterexample for some non-maximal $\mathcal{O}$, but there isn't:

Theorem 3.12. *Let $\mathcal{O}$ be an order in K and $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$ such that $\mathfrak{a} \cap \mathcal{O}$ is invertible as a fractional $\mathcal{O}$-ideal. Then the natural ring homomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ is an isomorphism.*

The proof of Theorem 3.12 will use localization and is at the end of Section 6.

We now turn to some positive illustrations of Theorem 3.8 and its corollaries.

Example 3.13. We examine the ideals in $\mathbf{Z}[2i]$ that are relatively prime to its conductor $\mathfrak{c} = 2\mathbf{Z}[i]$. The ideals in $\mathbf{Z}[i]$ relatively prime to $\mathfrak{c}$ are $\alpha\mathbf{Z}[i]$ where $\mathrm{N}(\alpha)$ is odd, since $\mathfrak{c} = (1+i)^2$ and $(1+i)$ is the unique prime over 2 in $\mathbf{Z}[i]$. Writing $\alpha = a + bi$, one of a or b is even and the other is odd. Since $\alpha\mathbf{Z}[i] = i\alpha\mathbf{Z}[i]$, we can choose the generator α

to have b even, so $\alpha \in \mathbf{Z}[2i]$. Then $\alpha\mathbf{Z}[i] \cap \mathbf{Z}[2i] = \alpha\mathbf{Z}[2i]$ by Corollary 3.10. From this and the bijection in Theorem 3.8, every ideal in $\mathbf{Z}[2i]$ relatively prime to $\mathfrak{c}$ is a principal ideal $\alpha\mathbf{Z}[2i]$ where $\mathrm{N}(\alpha)$ is odd. Therefore the elements of $\mathbf{Z}[2i]$ with odd norm have unique factorization, although $\mathbf{Z}[2i]$ is not a UFD (consider $8 = (2+2i)(2-2i) = 2 \cdot 2 \cdot 2$ in $\mathbf{Z}[2i]$).

Example 3.14. What ideals in $\mathbf{Z}[\sqrt{-3}]$ are relatively prime to the conductor $\mathfrak{c} = 2\mathbf{Z}[\zeta_3]$? Since $\mathbf{Z}[\sqrt{-3}] = \mathbf{Z}[-1+\sqrt{-3}] = \mathbf{Z}[2\zeta_3] = \{a + b \cdot 2\zeta_3 : a, b \in \mathbf{Z}\}$, the ring $\mathbf{Z}[\zeta_3]$ is a PID in which $\mathfrak{c}$ is the only prime ideal over 2, so $\alpha\mathbf{Z}[\zeta_3]$ is relatively prime to $\mathfrak{c}$ if and only if $\mathrm{N}(\alpha)$ is odd. Every ideal in $\mathbf{Z}[\zeta_3]$ with odd norm has a generator in $\mathbf{Z}[\sqrt{-3}]$ (multiply a generator of the ideal by ζ_3 or $\zeta_3^2 = -1 - \zeta_3$ if necessary to make the coefficient of ζ_3 even). Using Corollary 3.10, the ideals in $\mathbf{Z}[\sqrt{-3}]$ relatively prime to $\mathfrak{c}$ are principal with a generator of odd norm. The elements of $\mathbf{Z}[\sqrt{-3}]$ with odd norm have unique factorization.

The ring $\mathbf{Z}[\sqrt{-3}]$ was introduced into number theory by Euler in his first proof of Fermat's last theorem for exponent 3. The proof relies on factorizations in $\mathbf{Z}[\sqrt{-3}]$, which is not a UFD. However, the numbers in $\mathbf{Z}[\sqrt{-3}]$ that appear in Euler's proof have odd norm, so his use of unique factorization in $\mathbf{Z}[\sqrt{-3}]$ is legitimate even though the whole ring $\mathbf{Z}[\sqrt{-3}]$ doesn't have unique factorization. (Conceptually it is easier to carry out Euler's proof in the larger ring $\mathbf{Z}[\zeta_3]$, which is a UFD.)

Let's look at prime ideals in orders $\mathbf{Z} + c\mathcal{O}_K$, where $K \neq \mathbf{Q}$ and $c > 1$. Its conductor is $c\mathcal{O}_K$. For primes p not dividing c, there is a bijection between the prime ideals over p in $\mathcal{O}_K$ and in $\mathbf{Z} + c\mathcal{O}_K$ by $\mathfrak{p} \mapsto \mathfrak{p} \cap (\mathbf{Z} + c\mathcal{O}_K)$. What happens when p divides c?

Theorem 3.15. *Let $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$, where $c > 1$. For each prime p dividing c, the ideal $p\mathbf{Z} + c\mathcal{O}_K$ in $\mathcal{O}$ has index p in $\mathcal{O}$ and is the unique prime ideal over p in $\mathcal{O}$.*

Proof. Set $\mathfrak{p} = p\mathbf{Z} + c\mathcal{O}_K$ and $\mathfrak{b} = p\mathcal{O} = p\mathbf{Z} + pc\mathcal{O}_K$. Both are ideals in $\mathcal{O}$ and neither contains 1 so they are proper. (Here we use $p \mid c$.) The ring $\mathcal{O}/\mathfrak{p} = (\mathbf{Z}+c\mathcal{O}_K)/(p\mathbf{Z}+c\mathcal{O}_K)$ is represented by $\{1, 2, \ldots, p-1\}$, so it has size p and must be isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Therefore $\mathfrak{p}$ is a maximal ideal in $\mathcal{O}$ and it trivially lies over p. (If p did not divide c then $\mathfrak{p}$ would equal $\mathcal{O}$.) If $\mathfrak{q}$ is a prime ideal in $\mathcal{O}$ lying over p then $\mathfrak{q} \supset p\mathcal{O} = \mathfrak{b}$. Since

$$\mathfrak{p}^2 = (p\mathbf{Z} + c\mathcal{O}_K)(p\mathbf{Z} + c\mathcal{O}_K) = p^2\mathbf{Z} + pc\mathcal{O}_K + c^2\mathcal{O}_K = p^2\mathbf{Z} + pc\mathcal{O}_K \subset \mathfrak{b},$$

we get $\mathfrak{p}^2 \subset \mathfrak{q}$, so $\mathfrak{p} \subset \mathfrak{q}$, so $\mathfrak{q} = \mathfrak{p}$ (all nonzero primes in $\mathcal{O}$ are maximal). □

Let $p\mathcal{O}_K$ have the prime factors $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ in $\mathcal{O}_K$. When p divides c, the diagram of primes over p in $\mathcal{O}_K$ and $\mathbf{Z} + c\mathcal{O}_K$ is g-to-1, as illustrated in Figure 1.

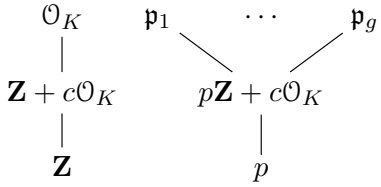


FIGURE 1. Primes lying over p in $\mathcal{O}_K$ and $\mathbf{Z} + c\mathcal{O}_K$ when $p \mid c$.

Figures 2 and 3 compare primes in $\mathbf{Z}[i]$ and the orders $\mathbf{Z}[2i] = \mathbf{Z} + 2\mathbf{Z}[i]$ and $\mathbf{Z}[65i] = \mathbf{Z}+65\mathbf{Z}[i]$. (Note $(2+3i)$ means different things in $\mathbf{Z}[i]$ and $\mathbf{Z}[2i]$, since the ideals it generates in the two rings are not equal.) In Figure 2 the map $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathbf{Z}[2i]$ is a bijection between

the primes in $\mathbf{Z}[i]$ and $\mathbf{Z}[2i]$ because of the quirk that there is only one prime over 2 in $\mathbf{Z}[i]$. We see more visibly in Figure 3 how the bijection between primes relatively prime to the conductor might *not* extend to primes containing the conductor.

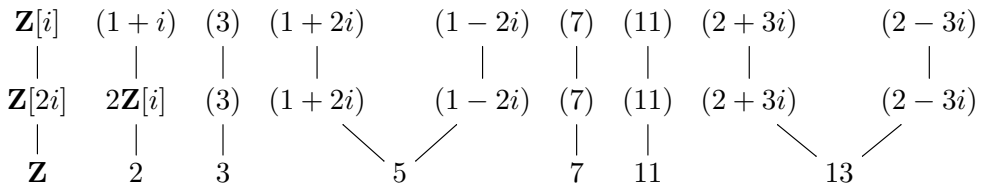


FIGURE 2. Primes lying over primes in $\mathbf{Z}[i]$ and $\mathbf{Z}[2i]$.

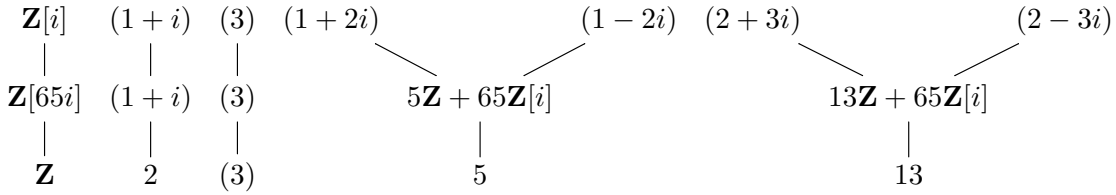


FIGURE 3. Primes lying over primes in $\mathbf{Z}[i]$ and $\mathbf{Z}[65i]$.

Remark 3.16. Theorem 3.15 is about orders $\mathbf{Z} + c\mathcal{O}_K$ (for $c > 1$) and its conclusion can fail in other orders. Consider $\mathcal{O} = \mathbf{Z}[\alpha]$, where $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$. In $K = \mathbf{Q}(\alpha)$, $\mathcal{O}$ has index 2 in the ring of integers $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}(\alpha^2 + \alpha)/2$, so the conductor $\mathfrak{c}$ of $\mathcal{O}$ contains 2. The prime ideals of $\mathcal{O}$ containing 2 are the lifts to $\mathcal{O}$ of the prime ideals of $\mathcal{O}/2\mathcal{O} \cong \mathbf{F}_2[T]/(T^3 - T^2 - 2T - 8) \cong \mathbf{F}_2[T]/(T^2(T-1)) \cong \mathbf{F}_2[T]/(T^2) \times \mathbf{F}_2[T]/(T-1)$, so these prime ideals in $\mathcal{O}$ are $(2, \alpha)$ and $(2, \alpha - 1)$.[3] Since $\alpha \in \mathfrak{c}$ we have $(2, \alpha) \subset \mathfrak{c}$, so $\mathfrak{c} = (2, \alpha)$ by maximality of $(2, \alpha)$ in $\mathcal{O}$. Thus $\mathfrak{c} \cap \mathbf{Z} = 2\mathbf{Z}$ and, in contrast to Theorem 3.15, there are *two* prime ideals in $\mathcal{O}$ that lie over 2: $(2, \alpha)$ and $(2, \alpha - 1)$.

4. Invertible ideals in an order

Let's review the relations among three properties of ideals $\mathfrak{b}$ in $\mathcal{O}$:

(1) $\mathfrak{b}$ is relatively prime to the conductor of $\mathcal{O}$,
(2) $\mathfrak{b}$ is invertible (as a fractional $\mathcal{O}$-ideal),
(3) $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$.

We have (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), and (1) $\Rightarrow$ (3) (which is Theorem 3.1 and was used in our proof that (1) $\Rightarrow$ (2) in Theorem 3.6). Conditions (1) and (3), and (1) and (2), are not equivalent when $\mathcal{O}$ is nonmaximal (consider a nonzero principal ideal contained in the conductor). Conditions (2) and (3) are not generally equivalent when $\mathcal{O}$ is nonmaximal (Example 3.5), but we always have (2) $\Rightarrow$ (3): multiply the containment $x\mathfrak{b} \subset \mathfrak{b}$ on both sides by the inverse of $\mathfrak{b}$. When $\mathcal{O}$ is a nonmaximal order, its conductor ideal $\mathfrak{c}$ doesn't

[3]Comparing ideals in $\mathcal{O}$ and $\mathcal{O}_K$, we have $2\mathcal{O} + \alpha\mathcal{O} = 2\mathcal{O}_K + \alpha\mathcal{O}_K$ but $2\mathcal{O} + (\alpha - 1)\mathcal{O} \neq 2\mathcal{O}_K + (\alpha - 1)\mathcal{O}_K$.

satisfy (3) since $\{x \in K : x\mathfrak{c} = \mathfrak{c}\} = \mathcal{O}_K \neq \mathcal{O}$. Therefore *the conductor ideal of a non-maximal order is never an invertible ideal in the order*. For example, the conductor ideal of a non-maximal order is not a principal ideal in the order even if it is principal in $\mathcal{O}_K$.

When does (3) imply (2) for all $\mathfrak{b}$? That is, when is (3) a sufficient condition for invertibility of fractional $\mathcal{O}$-ideals and not just a necessary condition?

Theorem 4.1. *For an order $\mathcal{O}$, the following conditions are equivalent:*

(1) *for all fractional $\mathcal{O}$-ideals $\mathfrak{b}$, $\mathfrak{b}$ is invertible if and only if $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$,*
(2) *$\mathcal{O}^\vee$, the $\mathbf{Z}$-dual of $\mathcal{O}$, is invertible as a fractional $\mathcal{O}$-ideal.*

Recall for a $\mathbf{Z}$-lattice $L \subset K$ that its $\mathbf{Z}$-dual is $L^\vee = \{x \in K : \mathrm{Tr}_{K/\mathbf{Q}}(xL) \subset \mathbf{Z}\}$.

Proof. This will be based on the identity

$$\mathfrak{b}\mathfrak{b}^\vee = \mathcal{O}^\vee, \tag{4.1}$$

for every fractional $\mathcal{O}$-ideal $\mathfrak{b}$ satisfying $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$. In the development of the different ideal $\mathcal{D}_{K/\mathbf{Q}}$, (4.1) is proved for fractional $\mathcal{O}_K$-ideals using inverses, in the form $\mathfrak{b}^\vee = \mathfrak{b}^{-1}\mathcal{O}_K^\vee$. We of course can't copy that proof in orders, where inverses may not exist. Instead we will use double duality ($\mathfrak{b}^{\vee\vee} = \mathfrak{b}$) more heavily.

Since $\mathfrak{b}$ is an $\mathcal{O}$-module, $\mathfrak{b}^\vee$ is a fractional $\mathcal{O}$-ideal and $\mathfrak{b}\mathfrak{b}^\vee \subset \mathcal{O}^\vee$ by unwinding definitions. To show the reverse inclusion, pick $x \in (\mathfrak{b}\mathfrak{b}^\vee)^\vee$. Then $\mathrm{Tr}_{K/\mathbf{Q}}(x\mathfrak{b}\mathfrak{b}^\vee) \subset \mathbf{Z}$, so $x\mathfrak{b}^\vee \subset \mathfrak{b}^\vee$. Passing to the $\mathbf{Z}$-dual of both sides, $\frac{1}{x}\mathfrak{b} \supset \mathfrak{b}$, so $x\mathfrak{b} \subset \mathfrak{b}$. Therefore by hypothesis $x \in \mathcal{O}$. So $(\mathfrak{b}\mathfrak{b}^\vee)^\vee \subset \mathcal{O}$. Passing to $\mathbf{Z}$-duals, $\mathfrak{b}\mathfrak{b}^\vee \supset \mathcal{O}^\vee$.

Now we prove (1) and (2) are equivalent.

(1) $\Rightarrow$ (2): We will show $\{x \in K : x\mathcal{O}^\vee \subset \mathcal{O}^\vee\} = \mathcal{O}$. The inclusion $\supset$ follows from $\mathcal{O}^\vee$ being an $\mathcal{O}$-module. To prove $\subset$, dualize the containment $x\mathcal{O}^\vee \subset \mathcal{O}^\vee$ to get $\frac{1}{x}\mathcal{O} \supset \mathcal{O}$, so $x\mathcal{O} \subset \mathcal{O}$. Therefore $x \in \mathcal{O}$ (since $1 \in \mathcal{O}$).

(2) $\Rightarrow$ (1): If $\mathfrak{b}$ is invertible as a fractional $\mathcal{O}$-ideal and $x\mathfrak{b} \subset \mathfrak{b}$ then multiplying both sides by the inverse of $\mathfrak{b}$ implies $x \in \mathcal{O}$, so $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} \subset \mathcal{O}$. The reverse inclusion holds since $\mathfrak{b}$ is an $\mathcal{O}$-module, so $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$. We haven't needed (2). Now assume $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$. To show $\mathfrak{b}$ is invertible as a fractional $\mathcal{O}$-ideal we use (4.1). Since $\mathcal{O}^\vee$ is invertible by (2), we multiply both sides of (4.1) by the inverse of $\mathcal{O}^\vee$ to see $\mathfrak{b}$ is invertible. □

Remark 4.2. By the proof of (4.1), $(LL^\vee)^\vee = \{x \in K : xL \subset L\}$ for all $\mathbf{Z}$-lattices L in K.

The second condition in Theorem 4.1 doesn't just tell us when "$\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$" is a necessary and sufficient criterion for invertibility of fractional $\mathcal{O}$-ideals, but also when the second condition breaks down it immediately gives us a counterexample for that criterion, namely $\mathfrak{b} = \mathcal{O}^\vee$. This fractional ideal can be scaled to an ideal in $\mathcal{O}$ and thus give a counterexample among ordinary ideals. This is how Example 3.5 was found.

If we are given an order $\mathcal{O}$, we can check invertibility of $\mathcal{O}^\vee$ as a fractional $\mathcal{O}$-ideal by following Lemma 3.2: check if $\mathcal{O}^\vee\widetilde{\mathcal{O}^\vee} = \mathcal{O}$. This equality is necessary and sufficient for $\mathcal{O}^\vee$ to be invertible. Since the product $\mathcal{O}^\vee\widetilde{\mathcal{O}^\vee}$ is always an ideal in $\mathcal{O}$, checking if $\mathcal{O}^\vee\widetilde{\mathcal{O}^\vee} = \mathcal{O}$ is equivalent to checking if $1 \in \mathcal{O}^\vee\widetilde{\mathcal{O}^\vee}$.

Corollary 4.3. *If $\mathcal{O} = \mathbf{Z}[\alpha]$ for some α then a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ is invertible as a fractional $\mathcal{O}$-ideal if and only if $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$.*

Proof. When $\mathcal{O} = \mathbf{Z}[\alpha]$, $\mathcal{O}^\vee = \frac{1}{f'(\alpha)}\mathcal{O}$ where $f(T)$ is the minimal polynomial of α over $\mathbf{Q}$. (This formula for $\mathbf{Z}[\alpha]^\vee$ can be found in any textbook treatment of the different ideal.) Since $\frac{1}{f'(\alpha)}\mathcal{O}$ is a principal fractional $\mathcal{O}$-ideal, it is invertible. Now use Theorem 4.1. □

Corollary 4.4. *For each order $\mathcal{O}$ in a quadratic field K, a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ is invertible as a fractional $\mathcal{O}$-ideal if and only if $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$.*

Proof. We will give two proofs. For the first proof, every order in a quadratic field has the form $\mathbf{Z}[\alpha]$, so Corollary 4.3 can be used and we're done.

For the second proof, we give a more self-contained treatment of the quadratic case. If $\mathfrak{b}$ is an invertible fractional $\mathcal{O}$-ideal, with inverse $\mathfrak{a}$, then the condition $x\mathfrak{b} \subset \mathfrak{b}$ for an $x \in K$ implies $x\mathfrak{b}\mathfrak{a} \subset \mathfrak{b}\mathfrak{a}$, so $x\mathcal{O} \subset \mathcal{O}$, and that implies $x \in \mathcal{O}$ since $1 \in \mathcal{O}$. Conversely, suppose $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$. We want to prove $\mathfrak{b}$ has an inverse. To do this we follow notes of Stark [2], which were meant to be Chapter 9 of [1] if a second edition of [1] ever appeared.

Write $\overline{\mathfrak{b}}$ for the set of conjugates of elements of $\mathfrak{b}$. Here we use the conjugation automorphism on the quadratic field K. Check $\overline{\mathfrak{b}}$ is a fractional $\mathcal{O}$-ideal. We will prove the product $\mathfrak{b}\overline{\mathfrak{b}}$ is a principal fractional $\mathcal{O}$-ideal, say $r\mathcal{O}$. From $\mathfrak{b}\overline{\mathfrak{b}} = r\mathcal{O}$ we get $\mathfrak{b}((1/r)\overline{\mathfrak{b}}) = \mathcal{O}$, which shows $\mathfrak{b}$ is invertible.

Since $\mathcal{O}$ is an order in a quadratic field, the fractional $\mathcal{O}$-ideal $\mathfrak{b}$ has a $\mathbf{Z}$-basis of size 2, say $\mathfrak{b} = \mathbf{Z}\alpha + \mathbf{Z}\beta$ for some nonzero α and β in $\mathfrak{b}$. Since $\mathfrak{b}$ is an $\mathcal{O}$-module we also have $\mathfrak{b} = \mathcal{O}\alpha + \mathcal{O}\beta = (\alpha, \beta)$, so $\overline{\mathfrak{b}} = (\overline{\alpha}, \overline{\beta})$. Let $\mathrm{Tr}, \mathrm{N}\colon K \to \mathbf{Q}$ be the trace and norm maps (sum and product of an element and its conjugate). Then

$$\mathfrak{b}\overline{\mathfrak{b}} = (\alpha, \beta)(\overline{\alpha}, \overline{\beta}) = (\alpha\overline{\alpha}, \alpha\overline{\beta}, \overline{\alpha}\beta, \beta\overline{\beta}) = (\mathrm{N}(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, \mathrm{N}(\beta)).$$

Note $\mathrm{Tr}(\alpha\overline{\beta}) = \alpha\overline{\beta} + \overline{\alpha}\beta$. We are going to show the following equality of fractional $\mathcal{O}$-ideals:

$$(\mathrm{N}(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, \mathrm{N}(\beta)) = (\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)), \tag{4.2}$$

which is a bit surprising since the second generator on the right is the sum of the middle two generators on the left. The norm and trace have values in $\mathbf{Q}$ and an $\mathcal{O}$-module with generators in $\mathbf{Q}$ is principal since all fractional ideals in $\mathbf{Q}$ are principal, so the right side of (4.2) is a principal fractional $\mathcal{O}$-ideal and therefore (4.2) implies $\mathfrak{b}\overline{\mathfrak{b}}$ is principal.

It is obvious in (4.2) that the right side is contained in the left side. To prove the left side is contained in the right side, it suffices to show $\alpha\overline{\beta}$ is in the right side, since $\overline{\alpha}\beta = \mathrm{Tr}(\alpha\overline{\beta}) - \alpha\overline{\beta}$.

Let $\gamma = \alpha/\beta \in K^\times$. This is a root of

$$\begin{aligned}(X - \gamma)(X - \overline{\gamma}) &= X^2 - (\gamma + \overline{\gamma})X + \gamma\overline{\gamma} \\ &= X^2 - \left(\frac{\alpha\overline{\beta} + \overline{\alpha}\beta}{\beta\overline{\beta}}\right)X + \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)} \\ &= X^2 - \frac{\mathrm{Tr}(\alpha\overline{\beta})}{\mathrm{N}(\beta)}X + \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)}. \qquad (4.3)\end{aligned}$$

Write ℓ for the least common denominator of the rational numbers $\mathrm{Tr}(\alpha\overline{\beta})/\mathrm{N}(\beta)$ and $\mathrm{N}(\alpha)/\mathrm{N}(\beta)$ (the second number is not 0, so "least common denominator" makes sense). Then

$$\frac{\mathrm{Tr}(\alpha\overline{\beta})}{\mathrm{N}(\beta)} = \frac{a}{\ell}, \quad \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)} = \frac{b}{\ell}, \tag{4.4}$$

where $a, b, \ell \in \mathbf{Z}$ have no common factor greater than 1. (If there were a common factor greater than 1 then the two fractions a/ℓ and b/ℓ both simplify further, contradicting ℓ being a least common denominator.) Therefore

$$(\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)) = \left(\frac{b}{\ell}\mathrm{N}(\beta), \frac{a}{\ell}\mathrm{N}(\beta), \mathrm{N}(\beta)\right) = \frac{\mathrm{N}(\beta)}{\ell}(b, a, \ell) = \frac{\mathrm{N}(\beta)}{\ell}\mathcal{O}, \tag{4.5}$$

where the last equation follows from $\gcd(b, a, \ell) = 1$. Thus

$$\alpha\overline{\beta} \in (\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)) \Longleftrightarrow \alpha\overline{\beta} \in \frac{\mathrm{N}(\beta)}{\ell}\mathcal{O} \Longleftrightarrow \ell\frac{\alpha}{\beta} \in \mathcal{O}.$$

How can we prove $\ell\alpha/\beta \in \mathcal{O}$? It's finally time to use the condition that $\{x \in K : x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}$. That tells us if we show $(\ell\alpha/\beta)\mathfrak{b} \subset \mathfrak{b}$ then $\ell\alpha/\beta$ is in $\mathcal{O}$. Since $\mathfrak{b} = (\alpha, \beta)$, to show $(\ell\alpha/\beta)\mathfrak{b} \subset \mathfrak{b}$ it suffices to show $(\ell\alpha/\beta)\alpha \in (\alpha, \beta)$ and $(\ell\alpha/\beta)\beta \in (\alpha, \beta)$. The second containment is obvious. The first containment is saying $\ell\alpha^2/\beta \in (\alpha, \beta)$. How can we derive that?

Let's go back to the fact that γ is a root of (4.3). Combining this with (4.4),

$$\gamma^2 - \frac{a}{\ell}\gamma + \frac{b}{\ell} = 0 \Longrightarrow \ell\gamma^2 = a\gamma - b \Longrightarrow \ell\frac{\alpha^2}{\beta^2} = a\frac{\alpha}{\beta} - b.$$

Multiplying through by β,

$$\ell\frac{\alpha^2}{\beta} = a\alpha - b\beta \in (\alpha, \beta) = \mathfrak{b},$$

so we're done. □

Remark 4.5. Corollary 4.4 is a special property of quadratic fields! For every number field K of degree at least 3, there are infinitely many orders $\mathcal{O}$ in K such that $\mathcal{O}^\vee$ is not invertible as a fractional $\mathcal{O}$-ideal. Examples of such $\mathcal{O}$ are $\mathbf{Z}+p\mathcal{O}_K$ where p is a prime splitting completely in K. Why these examples work when $[K : \mathbf{Q}] \geq 3$ but not when $[K : \mathbf{Q}] = 2$, very roughly, is that there is more room to move around in K when $[K : \mathbf{Q}] \geq 3$.

5. The ideal class group of an order

We now discuss the ideal class group of $\mathcal{O}$: the group of invertible fractional $\mathcal{O}$-ideals modulo the subgroup of principal fractional $\mathcal{O}$-ideals. For an invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$, its ideal class $[\mathfrak{a}]$ is $\{x\mathfrak{a} : x \in K^\times\}$. The set of ideal classes under multiplication, where $[\mathfrak{a}][\mathfrak{a}'] = [\mathfrak{a}\mathfrak{a}']$, form the ideal class group $\mathrm{Cl}(\mathcal{O})$. This is the usual ideal class group of K when $\mathcal{O} = \mathcal{O}_K$.

How are $\mathrm{Cl}(\mathcal{O})$ and $\mathrm{Cl}(\mathcal{O}_K)$ related when $\mathcal{O}$ is a general order in K? Since a principal ideal in $\mathcal{O}$ extends to a principal ideal in $\mathcal{O}_K$, we get a group homomorphism $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$ by $[\mathfrak{b}] \mapsto [\mathfrak{b}\mathcal{O}_K]$. It need not be injective: a nonprincipal (invertible) ideal in $\mathcal{O}$ can become principal when it is extended to $\mathcal{O}_K$.

Example 5.1. For an odd number $c > 1$, let $\mathcal{O} = \mathbf{Z}[ci]$ and $\mathfrak{a} = (1 + i) \cap \mathcal{O}$, which is the prime ideal in $\mathbf{Z}[ci]$ lying under $(1 + i)$ in $\mathbf{Z}[i]$. Check $\mathfrak{a} = (2, c + ci)$, where the right side means the ideal in $\mathcal{O}$ generated by 2 and $c + ci$. That is a real calculation, not a tautology: show the left and right sides contain each other. The ideal $\mathfrak{a}$ is invertible as a fractional

$\mathcal{O}$-ideal since $\mathfrak{a}^2 = 2\mathcal{O}$:

$$\begin{aligned}\mathfrak{a}^2 = (2, c+ci)(2, c+ci) = (4, 2c+2ci, 2c^2i) &= (2)(2, c+ci, c^2i)\\ &= (2)(2, c+ci, ci) \ \text{ since } c^2i - ci \in (2, c+ci)\\ &= (2)(2, c, ci)\\ &= (2).\end{aligned}$$

The extension of $\mathfrak{a}$ to an ideal in $\mathbf{Z}[i]$ is principal since $\mathbf{Z}[i]$ is a PID. Explicitly, $\mathfrak{a}\mathbf{Z}[i] = (1+i)$ since in $\mathbf{Z}[i]$, $\gcd(2, c+ci) = \gcd((1+i)^2, c(1+i)) = 1+i$. We will show $\mathfrak{a}$ is nonprincipal in $\mathcal{O}$ by showing $\mathfrak{a}$ has index 2 in $\mathcal{O}$ while no principal ideal in $\mathcal{O}$ has index 2. Check as a $\mathbf{Z}$-module that $\mathfrak{a} = \mathbf{Z}\cdot 2 + \mathbf{Z}(c+ci)$ (show the left and right sides contain each other). Since $\mathcal{O} = \mathbf{Z}[ci] = \mathbf{Z}[c+ci] = \mathbf{Z} + \mathbf{Z}(c+ci)$, comparing this to the decomposition $\mathfrak{a} = \mathbf{Z}\cdot 2 + \mathbf{Z}(c+ci)$ – both decompositions are direct sums of $\mathbf{Z}$-modules – shows $[\mathcal{O} : \mathfrak{a}] = 2$. For a nonzero principal ideal (α) in $\mathcal{O}$, $[\mathcal{O} : (\alpha)] = \mathrm{N}(\alpha)$,[4] so the principal ideal $(m+nci)$ in $\mathcal{O}$ has index $m^2 + n^2c^2$ in $\mathcal{O}$, and $m^2 + n^2c^2$ is never 2 since $c > 1$.

Using the conductor ideal we will show the map $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$ where $[\mathfrak{b}] \mapsto [\mathfrak{b}\mathcal{O}_K]$ is surjective. I thank Will Sawin for the following argument.

Lemma 5.2. *Let $\mathfrak{p}$ be a nonzero prime ideal in an order $\mathcal{O}$. Each ideal class in $\mathrm{Cl}(\mathcal{O})$ has a representative that is an ideal in $\mathcal{O}$ and is relatively prime to $\mathfrak{p}$.*

Proof. Pick an ideal class $[\mathfrak{a}]$ in $\mathrm{Cl}(\mathcal{O})$, so $\mathfrak{a}$ is an invertible fractional $\mathcal{O}$-ideal. We want to find some $x \in K^\times$ such that (i) $x\mathfrak{a}$ is an ideal in $\mathcal{O}$ and (ii) $x\mathfrak{a} + \mathfrak{p} = \mathcal{O}$. To have $x\mathfrak{a} \subset \mathcal{O}$, x has to lie in the inverse fractional ideal to $\mathfrak{a}$: recall the inverse of $\mathfrak{a}$ is

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset \mathcal{O}\}.$$

Since $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$, $\mathfrak{a}\mathfrak{a}^{-1}$ contains 1: we can write

$$1 = \alpha_1\alpha_1' + \cdots + \alpha_k\alpha_k'$$

for some $\alpha_i \in \mathfrak{a}$ and $\alpha_i' \in \mathfrak{a}^{-1}$. Each product $\alpha_i\alpha_i'$ is in $\mathcal{O}$ and at least one of them is not in $\mathfrak{p}$ since their sum is not in $\mathfrak{p}$. Let's say $\alpha_j\alpha_j' \notin \mathfrak{p}$. Then $\alpha_j'\mathfrak{a} \subset \mathcal{O}$ and $\alpha_j'\mathfrak{a} \not\subset \mathfrak{p}$ since the particular product $\alpha_j'\alpha_j$ is not in $\mathfrak{p}$. Then

$$\mathfrak{p} \subset \alpha_j'\mathfrak{a} + \mathfrak{p} \subset \mathcal{O}$$

which forces the ideal in the middle to be $\mathfrak{p}$ or $\mathcal{O}$ since $\mathfrak{p}$ is maximal. That ideal is not $\mathfrak{p}$ since it contains $\alpha_j'\alpha_j$, so $\alpha_j'\mathfrak{a} + \mathfrak{p} = \mathcal{O}$. □

Theorem 5.3. *Let $\mathfrak{n}$ be a nonzero ideal in an order $\mathcal{O}$.*

1. *Each ideal class in $\mathrm{Cl}(\mathcal{O})$ has a representative that is an ideal in $\mathcal{O}$ and is relatively prime to $\mathfrak{n}$.*
2. *The group homomorphism $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$ given by $[\mathfrak{b}] \mapsto [\mathfrak{b}\mathcal{O}_K]$ is surjective.*

Proof. (1) There are finitely many prime ideals containing $\mathfrak{n}$, since they correspond to the prime ideals of $\mathcal{O}/\mathfrak{n}$, which is a finite ring and thus has finitely many prime ideals.[5] Let

[4] In an arbitrary order $\mathcal{O}$ in a number field K, each principal ideal (α) of $\mathcal{O}$ has index $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$ in $\mathcal{O}$. When $\mathcal{O}$ is imaginary quadratic, we can drop the absolute value signs.

[5] The finiteness of the number of prime ideals containing $\mathfrak{n}$ is true when $\mathcal{O}$ is an arbitrary one-dimensional Noetherian domain, by a different argument than the one we gave: see https://math.stackexchange.com/questions/1474210.

$\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals in $\mathcal{O}$ that contain $\mathfrak{n}$ and pick an ideal class $[\mathfrak{a}]$ in $\mathrm{Cl}(\mathcal{O})$. Lemma 5.2 tells us for $i = 1, \ldots, r$ there is an $x_i \in K^\times$ such that $x_i\mathfrak{a}$ is an ideal in $\mathcal{O}$ and $x_i\mathfrak{a} + \mathfrak{p}_i = \mathcal{O}$.

Note $x_i \in \mathfrak{a}^{-1}$ since $x_i\mathfrak{a} \subset \mathcal{O}$. The two properties

$$x_i\mathfrak{a} \subset \mathcal{O}, \quad x_i\mathfrak{a} + \mathfrak{p}_i = \mathcal{O}$$

are both *unchanged* if we modify x_i in $\mathfrak{a}^{-1}/\mathfrak{p}_i\mathfrak{a}^{-1}$: if $y_i \equiv x_i \bmod \mathfrak{p}_i\mathfrak{a}^{-1}$ then write $y_i = x_i + z_i$, so $z_i \in \mathfrak{p}_i\mathfrak{a}^{-1}$ and

$$y_i\mathfrak{a} = (x_i + z_i)\mathfrak{a} \subset x_i\mathfrak{a} + z_i\mathfrak{a} \subset \mathcal{O} + \mathfrak{p}_i\mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O} + \mathfrak{p}_i = \mathcal{O}.$$

By writing $1 = x_i a + t_i$ for $a \in \mathfrak{a}$ and $t_i \in \mathfrak{p}_i$,

$$1 = (y_i - z_i)a + t_i = y_i a + t_i - z_i a \equiv y_i a \bmod \mathfrak{p}_i$$

since $t_i \in \mathfrak{p}_i$ and $z_i a \in \mathfrak{p}_i\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{p}_i$. Thus $y_i\mathfrak{a} + \mathfrak{p}_i = \mathcal{O}$.

Since the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise relatively prime in $\mathcal{O}$, the Chinese remainder theorem for modules[6] tells us the diagonal mapping

$$\mathfrak{a}^{-1} \longrightarrow \prod_{i=1}^{r} \mathfrak{a}^{-1}/\mathfrak{p}_i\mathfrak{a}^{-1}$$

where $x \mapsto (x \bmod \mathfrak{p}_1\mathfrak{a}^{-1}, \ldots, x \bmod \mathfrak{p}_r\mathfrak{a}^{-1})$ is onto. Therefore there is some $x \in \mathfrak{a}^{-1}$ such that $x \equiv x_i \bmod \mathfrak{p}_i\mathfrak{a}^{-1}$ for $i = 1, \ldots, r$. Then by the previous paragraph, $x\mathfrak{a}$ is an ideal in $\mathcal{O}$ and $x\mathfrak{a} + \mathfrak{p}_i = \mathcal{O}$ for all i, so $x\mathfrak{a}$ is an ideal of $\mathcal{O}$ that's in the same ideal class as $\mathfrak{a}$ and it is relatively prime to $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Those are all the prime ideals containing $\mathfrak{n}$, and that implies $x\mathfrak{a}$ is relatively prime to $\mathfrak{n}$ as well: since $\mathfrak{n} \subset x\mathfrak{a} + \mathfrak{n} \subset \mathcal{O}$, if the ideal $x\mathfrak{a} + \mathfrak{n}$ were not $\mathcal{O}$ then $x\mathfrak{a} + \mathfrak{n} \subset \mathfrak{p}_i$ for some i, so $x\mathfrak{a} \subset \mathfrak{p}_i$ for that i. This contradicts the property $x\mathfrak{a} + \mathfrak{p}_i = \mathcal{O}$. Thus $x\mathfrak{a} + \mathfrak{n} = \mathcal{O}$.

(2) Let $\mathfrak{c}$ be the conductor of $\mathcal{O}$. This is an ideal in $\mathcal{O}_K$, so by (1) for the order $\mathcal{O}_K$ we can write each ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ as $[\mathfrak{a}]$ where $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_K$ that is relatively prime to $\mathfrak{c}$. By Theorems 3.6 and 3.8, $\mathfrak{a} \cap \mathcal{O}$ is relatively prime to $\mathfrak{c}$ in $\mathcal{O}$, is an invertible fractional $\mathcal{O}$-ideal, and $\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$. Thus $[\mathfrak{a} \cap \mathcal{O}]$ makes sense in $\mathrm{Cl}(\mathcal{O})$ and its image in in $\mathrm{Cl}(\mathcal{O}_K)$ is $[(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K] = [\mathfrak{a}]$. □

Since $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$ is surjective, $h(\mathcal{O})$ is divisible by $h(\mathcal{O}_K)$. A formula for $h(\mathcal{O})/h(\mathcal{O}_K)$ is given in Theorem 5.4 below by determining the kernel of $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$, which leads to a 4-term exact sequence in (5.4).

By Theorem 5.3(1), each ideal class in $\mathrm{Cl}(\mathcal{O})$ is represented by an ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to the conductor $\mathfrak{c}$. For $[\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O})$ to become trivial in $\mathrm{Cl}(\mathcal{O}_K)$ means $\mathfrak{b}\mathcal{O}_K = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$, necessarily prime to $\mathfrak{c}$ since $\mathfrak{b}$ is, so $\mathfrak{b}\mathcal{O}_K$ is too. By Theorem 3.8 we have $\mathfrak{b} = \mathfrak{b}\mathcal{O}_K \cap \mathcal{O}$, so $\mathfrak{b} = \alpha\mathcal{O}_K \cap \mathcal{O}$.[7] Conversely, by Theorem 3.8, if $\alpha\mathcal{O}_K$ is relatively prime to $\mathfrak{c}$ in $\mathcal{O}_K$ then the ideal $\alpha\mathcal{O}_K \cap \mathcal{O}$ in $\mathcal{O}$ is relatively prime to $\mathfrak{c}$ and $(\alpha\mathcal{O}_K \cap \mathcal{O})\mathcal{O}_K = \alpha\mathcal{O}_K$. So $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K))$ is the ideal classes $[\alpha\mathcal{O}_K \cap \mathcal{O}]$ in $\mathrm{Cl}(\mathcal{O})$ where $\alpha \in \mathcal{O}_K$ is relatively prime to $\mathfrak{c}$.

Claim: For nonzero $\alpha, \beta \in \mathcal{O}_K$, if $\alpha \equiv \beta \bmod \mathfrak{c}$ then $\alpha\mathcal{O}_K \cap \mathcal{O} = \frac{\alpha}{\beta}(\beta\mathcal{O}_K \cap \mathcal{O})$.

Proof of claim: Dividing both sides of $\alpha\mathcal{O}_K \cap \mathcal{O} \stackrel{?}{=} \frac{\alpha}{\beta}(\beta\mathcal{O}_K \cap \mathcal{O})$ by α, this equation is equivalent to checking $\mathcal{O}_K \cap \frac{1}{\alpha}\mathcal{O} \stackrel{?}{=} \mathcal{O}_K \cap \frac{1}{\beta}\mathcal{O}$. Write $\alpha = \beta + c$ with $c \in \mathfrak{c}$. If $t \in \mathcal{O}_K \cap \frac{1}{\alpha}\mathcal{O}$

[6] See https://mathoverflow.net/questions/18959.

[7] We can't say this intersection is $\alpha\mathcal{O}$ since there's no reason to believe α is in $\mathcal{O}$ (Corollary 3.10).

then $\alpha t \in \mathcal{O}$, so $(\beta + c)t \in \mathcal{O}$. The product ct is in $c\mathcal{O}_K \subset \mathfrak{c} \subset \mathcal{O}$, so $\beta t \in \mathcal{O}$, so $t \in \mathcal{O}_K \cap \frac{1}{\beta}\mathcal{O}$. That proves one inclusion in the claim and the reverse inclusion is proved in the same way.

The claim shows for $\alpha \in \mathcal{O}_K$ relatively prime to $\mathfrak{c}$ that the ideal class $[\alpha\mathcal{O}_K \cap \mathcal{O}]$ in $\mathrm{Cl}(\mathcal{O})$ depends only on α mod $\mathfrak{c}$, which lies in $(\mathcal{O}_K/\mathfrak{c})^\times$. So $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K))$ is the image of the map $(\mathcal{O}_K/\mathfrak{c})^\times \to \mathrm{Cl}(\mathcal{O})$ given by α mod $\mathfrak{c} \mapsto [\alpha\mathcal{O}_K \cap \mathcal{O}]$. This map is well-defined by the claim and it is a group homomorphism: for α and α' relatively prime to $\mathfrak{c}$ in $\mathcal{O}_K$,

$$(\alpha\mathcal{O}_K \cap \mathcal{O})(\alpha'\mathcal{O}_K \cap \mathcal{O}) = \alpha\alpha'\mathcal{O}_K \cap \mathcal{O}.$$

since this is a special case of the equation $\mathfrak{a}\mathfrak{a}' \cap \mathcal{O} = (\mathfrak{a} \cap \mathcal{O})(\mathfrak{a}' \cap \mathcal{O})$ that is in the last part of Theorem 3.8.

So we have a sequence of group homomorphisms

$$(\mathcal{O}_K/\mathfrak{c})^\times \xrightarrow{\alpha \bmod \mathfrak{c} \mapsto [\alpha\mathcal{O}_K \cap \mathcal{O}]} \mathrm{Cl}(\mathcal{O}) \xrightarrow{[\mathfrak{b}] \mapsto [\mathfrak{b}\mathcal{O}_K]} \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1 \tag{5.1}$$

that is exact at $\mathrm{Cl}(\mathcal{O})$ and $\mathrm{Cl}(\mathcal{O}_K)$. What is the kernel at $(\mathcal{O}_K/\mathfrak{c})^\times$? For $\alpha \in \mathcal{O}_K$ relatively prime to $\mathfrak{c}$, $[\alpha\mathcal{O}_K \cap \mathcal{O}]$ is trivial in $\mathrm{Cl}(\mathcal{O})$ if and only if $\alpha\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$ for some $\beta \in \mathcal{O}$ that is necessarily relatively prime to $\mathfrak{c}$.

Claim: For α in $\mathcal{O}_K$ and β in $\mathcal{O}$ that are both relatively prime to $\mathfrak{c}$, $\alpha\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$ if and only if $\alpha = \beta u$ for some $u \in \mathcal{O}_K^\times$.

Proof of claim: To prove the "only if" direction, extend both sides to ideals in $\mathcal{O}_K$: $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$ by Theorem 3.8, so $\alpha = \beta u$ with $u \in \mathcal{O}_K^\times$. To prove the "if" direction, $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$ and now intersect both sides with $\mathcal{O}$: $\alpha\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$ by Corollary 3.10.

By the claim,

$$\ker((\mathcal{O}_K/\mathfrak{c})^\times \to \mathrm{Cl}(\mathcal{O})) = \{\beta u \bmod \mathfrak{c} : \beta \in \mathcal{O}, (\beta, \mathfrak{c}) = (1), u \in \mathcal{O}_K^\times\}.$$

The unit group $(\mathcal{O}/\mathfrak{c})^\times$ naturally sits in $(\mathcal{O}_K/\mathfrak{c})^\times$ (pass to unit groups for the ring embedding $\mathcal{O}/\mathfrak{c} \hookrightarrow \mathcal{O}_K/\mathfrak{c}$) and fills out the β mod $\mathfrak{c}$'s (use $u = 1$), so (5.1) induces the sequence

$$(\mathcal{O}_K/\mathfrak{c})^\times/(\mathcal{O}/\mathfrak{c})^\times \longrightarrow \mathrm{Cl}(\mathcal{O}) \longrightarrow \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1. \tag{5.2}$$

The kernel of the homomorphism on the left in (5.2) is represented by units $u \in \mathcal{O}_K^\times$, so we can extend (5.2) to

$$\mathcal{O}_K^\times \xrightarrow{u \mapsto (u \bmod \mathfrak{c})(\mathcal{O}/\mathfrak{c})^\times} (\mathcal{O}_K/\mathfrak{c})^\times/(\mathcal{O}/\mathfrak{c})^\times \longrightarrow \mathrm{Cl}(\mathcal{O}) \longrightarrow \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1, \tag{5.3}$$

which is exact at $(\mathcal{O}_K/\mathfrak{c})^\times/(\mathcal{O}/\mathfrak{c})^\times$. The kernel of the homomorphism out of $\mathcal{O}_K^\times$ in (5.3) is

$$\{u \in \mathcal{O}_K^\times : u \bmod \mathfrak{c} \in (\mathcal{O}/\mathfrak{c})^\times\} = \mathcal{O}_K^\times \cap \mathcal{O} = \mathcal{O}^\times$$

since $\mathfrak{c}$ is in $\mathcal{O}$ and $\mathcal{O}_K$, so we finally get the exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times/\mathcal{O}^\times \longrightarrow (\mathcal{O}_K/\mathfrak{c})^\times/(\mathcal{O}/\mathfrak{c})^\times \longrightarrow \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1. \tag{5.4}$$

Theorem 5.4. *For an order $\mathcal{O}$ with conductor $\mathfrak{c}$, the class numbers of $\mathcal{O}$ and $\mathcal{O}_K$ satisfy*

$$h(\mathcal{O}) = h(\mathcal{O}_K)\frac{[(\mathcal{O}_K/\mathfrak{c})^\times : (\mathcal{O}/\mathfrak{c})^\times]}{[\mathcal{O}_K^\times : \mathcal{O}^\times]}.$$

Proof. In an exact sequence of finite abelian groups, the alternating product of the sizes of the groups is 1. So from (5.4),

$$\frac{[\mathcal{O}_K^\times : \mathcal{O}^\times]}{[(\mathcal{O}_K/\mathfrak{c})^\times : (\mathcal{O}/\mathfrak{c})^\times]}\frac{h(\mathcal{O})}{h(\mathcal{O}_K)} = 1.$$

Now rearrange terms. □

Example 5.5. Let's compute $h(\mathbf{Z}[pi])$ for a prime number p. When $\mathcal{O} = \mathbf{Z}[pi]$, $\mathfrak{c} = p\mathbf{Z}[i] = (p, pi)$ as an ideal in $\mathcal{O}$. Then $\mathbf{Z}[i]/\mathfrak{c} = \mathbf{Z}[i]/p\mathbf{Z}[i] \cong \mathbf{Z}[T]/(p, T^2+1) \cong \mathbf{F}_p[T]/(T^2+1)$ and $\mathcal{O}/\mathfrak{c} = \mathbf{Z}[pi]/(p, pi) \cong \mathbf{Z}[T]/(p, T, T^2+p^2) \cong \mathbf{F}_p[T]/(T) \cong \mathbf{F}_p$.[8] Let n_p be the number of units in $\mathbf{F}_p[T]/(T^2+1)$, so Theorem 5.4 says

$$h(\mathbf{Z}[pi]) = 1 \cdot \frac{n_p/(p-1)}{4/2} = \frac{n_p}{2(p-1)}.$$

If $p = 2$ then $\mathbf{F}_p[T]/(T^2+1) = \{0, 1, T, T+1\}$ has two units (1 and T), so $h(\mathbf{Z}[2i]) = 2/(2(1)) = 1$. That means the invertible ideals in $\mathbf{Z}[2i]$ are the principal ideals, so all nonprincipal ideals in $\mathbf{Z}[2i]$ are noninvertible. The invertible ideals in $\mathbf{Z}[2i]$ do *not* have unique factorization since they are the principal ideals and we know $\mathbf{Z}[2i]$ does not have unique factorization of elements.

If $p > 2$ and $-1 \bmod p$ is not a square then $\mathbf{F}_p[T]/(T^2+1)$ is a field of order p^2, so $n_p = p^2-1 = (p-1)(p+1)$. If $p > 2$ and $-1 \bmod p$ is a square then $\mathbf{F}_p[T]/(T^2+1) \cong \mathbf{F}_p \times \mathbf{F}_p$, so $n_p = (p-1)^2$. The rule for $-1 \bmod p$ being a square when p is an odd prime is that $p \equiv 1 \bmod 4$, so for odd primes p, $n_p = (p-1)(p-(-1)^{(p-1)/2})$ and thus

$$h(\mathbf{Z}[pi]) = \frac{p-(-1)^{(p-1)/2}}{2}.$$

A few values of this formula for $p > 2$, together with the case $p = 2$ above, are in the following table.

p	2	3	5	7	11	13	17
$h(\mathbf{Z}[pi])$	1	2	2	4	3	3	8

In Example 5.1, we saw $(2, p+pi)$ is a nonprincipal in $\mathbf{Z}[pi]$ for odd primes p, so when $p = 3$ or 5 every nonprincipal *invertible* ideal in $\mathbf{Z}[pi]$ is equivalent to $(2, p+pi)$ in $\mathrm{Cl}(\mathbf{Z}[pi])$. The conductor $\mathfrak{c} = (p, pi)$ is a nonprincipal noninvertible ideal in $\mathbf{Z}[pi]$.

Example 5.6. When $\mathcal{O} = \mathbf{Z}[\sqrt{-3}]$, $\mathfrak{c} = 2\mathbf{Z}[\zeta_3]$, $\mathcal{O}_K/\mathfrak{c} = \mathbf{Z}[\zeta_3]/(2) \cong \mathbf{F}_2[T]/(T^2+T+1) = \mathbf{F}_4$ has three units, and $\mathcal{O}/\mathfrak{c} = \mathbf{Z}[\sqrt{-3}]/\mathfrak{c} \cong \mathbf{F}_2$ has one unit, so

$$h(\mathbf{Z}[\sqrt{-3}]) = 1 \cdot \frac{3/1}{6/2} = 1.$$

Therefore an ideal in $\mathbf{Z}[\sqrt{-3}]$ is invertible if and only if it is principal.

Corollary 5.7. *The index* $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ *divides the index* $[(\mathcal{O}_K/\mathfrak{c})^\times : (\mathcal{O}/\mathfrak{c})^\times]$.

Proof. Theorem 5.3 says $h(\mathcal{O})/h(\mathcal{O}_K)$ is an integer. Now use Theorem 5.4. □

6. Localization at prime ideals and invertibility

For a nonzero prime ideal $\mathfrak{p}$ in an order $\mathcal{O}$, the notation $\mathcal{O}_\mathfrak{p}$ will always mean the localization of $\mathcal{O}$ at $\mathfrak{p}$, not $\mathcal{O}_K$ at $\mathfrak{p}$. When we localize $\mathcal{O}_K$ at $\mathfrak{p}$ we will write it as $\mathcal{O}_{K,\mathfrak{p}}$. The localization $\mathcal{O}_{K,\mathfrak{p}}$ means denominators are taken from $\mathcal{O} - \mathfrak{p}$ rather than $\mathcal{O}_K - \mathfrak{p}$, which probably isn't even a multiplicative set: $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$.

[8] If you made the mistake of thinking $\mathfrak{c} = p\mathcal{O}$, then you'd compute $\mathcal{O}/p\mathcal{O} \cong \mathbf{Z}[T]/(p, T^2+p) \cong \mathbf{F}_p[T]/(T^2)$, whose unit group has order $(p-1)p$, and for $p > 2$ that doesn't divide the number of units in $\mathbf{F}_p[T]/(T^2+1)$, which is either $(p-1)^2$ or p^2-1 as we'll see shortly. That would be inconsistent with $(\mathcal{O}/\mathfrak{c})^\times$ being a subgroup of $(\mathcal{O}_K/\mathfrak{c})^\times$. Remember: $\mathfrak{c} = p\mathbf{Z}[i]$ is an ideal in $\mathbf{Z}[pi]$ but it is not $p\mathbf{Z}[pi]$. It's bigger, having index p in $\mathbf{Z}[pi]$ rather than index p^2 like $p\mathbf{Z}[pi]$ does.

For a nonmaximal order $\mathcal{O}$, invertibility of an ideal in $\mathcal{O}$ is a stronger condition than relative primality to the conductor, but it turns out to be an equivalent condition when we restrict to prime ideals in $\mathcal{O}$.

Theorem 6.1. *A nonzero prime ideal $\mathfrak{p}$ in $\mathcal{O}$ is invertible if and only if $\mathfrak{p}$ is relatively prime to the conductor of $\mathcal{O}$.*

Proof. ($\Leftarrow$) We know by Theorem 3.6 that each ideal in $\mathcal{O}$ relatively prime to the conductor is invertible. (We really should refer to the earlier Theorems 3.1 and 3.4 for prime ideals.)

($\Rightarrow$) Let $\mathfrak{p}$ be an invertible prime ideal in $\mathcal{O}$. We want to show $\mathfrak{p}$ is relatively prime to the conductor of $\mathcal{O}$. In the localization $\mathcal{O}_\mathfrak{p}$ the unique nonzero prime ideal is $\mathfrak{m} := \mathfrak{p}\mathcal{O}_\mathfrak{p}$ and it is invertible ($\mathfrak{p}\widetilde{\mathfrak{p}} = \mathcal{O} \Rightarrow (\mathfrak{p}\mathcal{O}_\mathfrak{p})(\widetilde{\mathfrak{p}}\mathcal{O}_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}$). We will show every nonzero ideal in $\mathcal{O}_\mathfrak{p}$ is a power of $\mathfrak{m}$.

Since $\mathcal{O}_\mathfrak{p}$ is Noetherian, every nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_\mathfrak{p}$ contains a product of nonzero prime ideals, which must be a power of $\mathfrak{m}$. Write $\mathfrak{a} \supset \mathfrak{m}^n$ and take n to be as small as possible (for the choice of $\mathfrak{a}$). We will prove by induction on the minimal n that $\mathfrak{a} = \mathfrak{m}^n$. If $n = 0$ then $\mathfrak{a} \supset \mathfrak{m}^0 = \mathcal{O}_\mathfrak{p}$, so $\mathfrak{a} = \mathcal{O}_\mathfrak{p} = \mathfrak{m}^0$. Suppose $n \geq 1$. Then $\mathfrak{a} \neq \mathfrak{m}^0$, so $\mathfrak{m} \supset \mathfrak{a} \supset \mathfrak{m}^n$. Multiplying through by $\mathfrak{m}^{-1}$, $\mathcal{O}_\mathfrak{p} \supset \mathfrak{a}\mathfrak{m}^{-1} \supset \mathfrak{m}^{n-1}$. Since n is minimal for $\mathfrak{a}$, it is simple to see that $n-1$ is minimal for $\mathfrak{a}\mathfrak{m}^{-1}$. Therefore by induction $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{m}^{n-1}$, and multiplying through by $\mathfrak{m}$ implies $\mathfrak{a} = \mathfrak{m}^n$.

Since every nonzero ideal in $\mathcal{O}_\mathfrak{p}$ is a power of $\mathfrak{m}$ and $\mathfrak{m}$ is invertible, cancellation of ideals holds in $\mathcal{O}_\mathfrak{p}$, so $\mathcal{O}_\mathfrak{p}$ is integrally closed. Therefore the containment $\mathcal{O} \subset \mathcal{O}_\mathfrak{p}$ implies $\mathcal{O}_K \subset \mathcal{O}_\mathfrak{p}$ by passing to integral closures. Getting the containment $\mathcal{O}_K \subset \mathcal{O}_\mathfrak{p}$ is the key step in the proof. For every $x \in \mathcal{O}_K$, the containment tells us $x = y/z$ where $y \in \mathcal{O}$ and $z \in \mathcal{O} - \mathfrak{p}$. Then $zx \in \mathcal{O}$. Write $\mathcal{O}_K = \sum_{i=1}^n \mathbf{Z}x_i$ with $x_i \in \mathcal{O}$ (since $\mathcal{O}_K$ is finitely generated as a module over $\mathbf{Z}$ it is also finitely generated as a module over the larger ring $\mathcal{O}$) and choose $z_i \in \mathcal{O} - \mathfrak{p}$ such that $z_i x_i \in \mathcal{O}$. Then $z := z_1 \cdots z_n$ is in $\mathcal{O} - \mathfrak{p}$ and $zx_i \in \mathcal{O}$ for all i, so z belongs to the conductor of $\mathcal{O}$. Since $z \notin \mathfrak{p}$, $\mathfrak{p}$ is relatively prime to the conductor of $\mathcal{O}$. □

Corollary 6.2. *For a nonzero prime $\mathfrak{p}$ in $\mathcal{O}$, the following are equivalent:*

1. *$\mathfrak{p}$ is invertible in $\mathcal{O}$,*
2. *$\mathfrak{p}$ is relatively prime to $\mathfrak{c}$,*
3. *the localization $\mathcal{O}_\mathfrak{p}$ is integrally closed.*
4. *the containment $\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_{K,\mathfrak{p}}$ becomes an equality.*

Proof. The equivalence of conditions 1 and 2 is Theorem 6.1. In the proof of the theorem we showed $1 \Rightarrow 3 \Rightarrow 2$, so the first three conditions are equivalent.

The ring extension $\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_\mathfrak{p}$ is integral since it's a localization of the integral ring extension $\mathcal{O}_K/\mathcal{O}$, and $\mathcal{O}_{K,\mathfrak{p}}$ is integrally closed since it's a localization of an integrally closed ring. Therefore the containment $\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_{K,\mathfrak{p}}$ becomes an equality if and only if $\mathcal{O}_\mathfrak{p}$ is integrally closed. □

While the localization of $\mathcal{O}_K$ at every nonzero prime ideal is a PID, this is false for the localization of an order $\mathcal{O}$ at a prime $\mathfrak{p}$ containing the conductor: $\mathcal{O}_\mathfrak{p}$ is not integrally closed so it can't be a PID. In particular, the phenomenon of a localized prime ideal not becoming principal is never observed in the rings $\mathcal{O}_K$ but this always happens for some primes (albeit just finitely many primes) in a non-maximal order.

Corollary 6.3. *In an order $\mathcal{O}$, the following conditions on an ideal $\mathfrak{b}$ are equivalent:*

1. *$\mathfrak{b}$ is a product of invertible prime ideals,*

(2) $\mathfrak{b}$ *is relatively prime to the conductor of* $\mathcal{O}$.

Proof. By Theorem 6.1, the invertible prime ideals in $\mathcal{O}$ are the prime ideals that are relatively prime to the conductor. Now use Corollary 3.11. □

As a final use of localization we are going to prove Theorem 3.12: the natural ring homomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ is an isomorphism when $\mathfrak{a} \cap \mathcal{O}$ is invertible as an ideal in $\mathcal{O}$. (Recall that some constraint on $\mathfrak{a}$ is needed since this is not an isomorphism when $\mathfrak{a} = \mathfrak{c}$ is the conductor of $\mathcal{O}$ and $\mathcal{O}$ is nonmaximal.) The "easy case" when $\mathfrak{a}$ is relatively prime to the conductor was shown in Theorem 3.8. Handling the general case is going to need some new ideas.

Lemma 6.4. *Let R be a local ring that is a domain. A fractional R-ideal is invertible if and only if it is principal.*

Proof. Nonzero principal fractional ideals are obviously invertible. Assume now that $\mathfrak{a}$ is an invertible fractional R-ideal: $\mathfrak{a}\mathfrak{a}' = R$ for some other fractional R-ideal $\mathfrak{a}'$. That means we can write

$$x_1x_1' + \cdot + x_kx_k' = 1 \tag{6.1}$$

where $k \geq 1$, $x_i \in \mathfrak{a}$, and $x_i' \in \mathfrak{a}'$.

For each $x \in \mathfrak{a}$,

$$x = 1 \cdot x = x_1(x_1'x) + \cdots + x_k(x_k'x),$$

and $x_i'x \in \mathfrak{a}'\mathfrak{a} = R$, so $\mathfrak{a} \subset \sum_{i=1}^k Rx_i \subset \mathfrak{a}$. Thus $\mathfrak{a} = \sum_{i=1}^k Rx_i$. (So far we haven't used that R is local, so this shows every invertible fractional ideal in an integral domain is a finitely generated ideal.)

In (6.1) each product x_ix_i' is in R. In a local ring, if a sum of terms is 1 then one of the terms must be a unit (otherwise all the terms are in the maximal ideal of R and then their sum is, a contradiction). Say $x_ix_i' \in R^\times$. Then $\mathfrak{a} = x_ix_i'\mathfrak{a} \subset x_iR \subset \mathfrak{a}$, so $\mathfrak{a} = Rx_i$. □

Now we prove Theorem 3.12.

Proof. The natural ring homomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ is injective. Its surjectivity is equivalent to $\mathcal{O}_K \stackrel{?}{=} \mathcal{O} + \mathfrak{a}$ and this is what we will check using invertibility of $\mathfrak{a} \cap \mathcal{O}$.

Claim: We have $\mathcal{O}_K = \mathcal{O} + \mathfrak{a}$ if and only if $\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_\mathfrak{p} + \mathfrak{a}_\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p}$ in $\mathcal{O}$.

Proof of claim: The proof of ($\Rightarrow$) is easy. To show ($\Leftarrow$), we show $\mathcal{O}_K \subset \mathcal{O} + \mathfrak{a}$ (the reverse containment is trivial). For $\alpha \in \mathcal{O}_K$ and a nonzero prime ideal $\mathfrak{p}$ in $\mathcal{O}$ we can write $\alpha = x/d + a/d'$ where $x \in \mathcal{O}$, $a \in \mathfrak{a}$, and d and d' are in $\mathcal{O} - \mathfrak{p}$. Therefore $dd'\alpha \in \mathcal{O} + \mathfrak{a}$. So the denominator set $I_\alpha = \{y \in \mathcal{O} : y\alpha \in \mathcal{O} + \mathfrak{a}\}$, which is an ideal in $\mathcal{O}$, contains an element in $\mathcal{O} - \mathfrak{p}$ for every prime $\mathfrak{p}$. That means I_α is contained in no maximal ideal of $\mathcal{O}$, so $I_\alpha = \mathcal{O}$. Thus $1 \in I_\alpha$, so $\alpha \in \mathcal{O} + \mathfrak{a}$.

Returning to the proof of the theorem, since $\mathfrak{a} \cap \mathcal{O}$ is invertible in $\mathcal{O}$ its localization $(\mathfrak{a} \cap \mathcal{O})_\mathfrak{p}$ is invertible in $\mathcal{O}_\mathfrak{p}$ (the localization of the inverse is the inverse of the localization). It is easy to check $(\mathfrak{a} \cap \mathcal{O})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}$. By Lemma 6.4, $\mathfrak{a}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}$ is a principal ideal in $\mathcal{O}_\mathfrak{p}$, say $\mathfrak{a}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ with $\alpha_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} - \{0\}$. Scaling $\alpha_\mathfrak{p}$ by a unit in $\mathcal{O}_\mathfrak{p}$, we can assume $\alpha_\mathfrak{p} \in \mathcal{O}$. Write it now as α, so $\mathfrak{a}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \alpha\mathcal{O}_\mathfrak{p}$. The natural ring homomorphism $\mathcal{O}_\mathfrak{p} \to \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{a}_\mathfrak{p}$ has kernel $\mathfrak{a}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \alpha\mathcal{O}_\mathfrak{p}$, so we get an injection $\mathcal{O}_\mathfrak{p}/\alpha\mathcal{O}_\mathfrak{p} \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{a}_\mathfrak{p}$, so

$$[\mathcal{O}_\mathfrak{p} : \alpha\mathcal{O}_\mathfrak{p}] \leq [\mathcal{O}_{K,\mathfrak{p}} : \mathfrak{a}_\mathfrak{p}]. \tag{6.2}$$

Since $\mathfrak{a}_\mathfrak{p}$ is an ideal in $\mathcal{O}_{K,\mathfrak{p}}$ containing α, $\alpha\mathcal{O}_{K,\mathfrak{p}} \subset \mathfrak{a}_\mathfrak{p} \subset \mathcal{O}_{K,\mathfrak{p}}$, so

$$[\mathcal{O}_{K,\mathfrak{p}} : \mathfrak{a}_\mathfrak{p}] \leq [\mathcal{O}_{K,\mathfrak{p}} : \alpha\mathcal{O}_{K,\mathfrak{p}}]. \tag{6.3}$$

Somehow show

$$[\mathcal{O}_\mathfrak{p} : \alpha\mathcal{O}_\mathfrak{p}] = [\mathcal{O}_{K,\mathfrak{p}} : \alpha\mathcal{O}_{K,\mathfrak{p}}].$$

Then (6.2) and (6.3) become equalities, so the natural map $\mathcal{O}_\mathfrak{p}/\alpha\mathcal{O}_\mathfrak{p} \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{a}_\mathfrak{p}$ is an isomorphism, which means $\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_\mathfrak{p} + \mathfrak{a}_\mathfrak{p}$. This is true for all nonzero primes $\mathfrak{p}$ in $\mathcal{O}$, so by the claim we are done. □

Remark 6.5. If we were in the "de-localized" setting, then $[\mathcal{O} : \alpha\mathcal{O}] = [\mathcal{O}_K : \alpha\mathcal{O}_K]$. So running through the above argument here would show that if $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ such that $\mathfrak{a} \cap \mathcal{O} = \alpha\mathcal{O}$ is principal then $\mathfrak{a} = \alpha\mathcal{O}_K$.

References

[1] H. M. Stark, "An Introduction to Number Theory," MIT Press, Cambridge, 1978.
[2] H. M. Stark, personal notes.