ONE-DIMENSIONAL NOETHERIAN DOMAINS AND THEIR CLASS NUMBERS

TYLER GENAO

1. Introduction

These notes will follow Neukirch's treatment [Neu99] of the class number formula for an order in a number field. The only commutative algebra results that we assume are from [AM69], and will be cited accordingly.

The goal of these notes are to answer the following question: given an order in a number field K, is its Picard group finite? And if so, is there an easy way to compute it? Given a number field K and its ring of integers $\mathcal{O}_K$, recall that its *class group* is

$$\mathrm{Cl}(\mathcal{O}_K) := \frac{\{\text{nonzero fractional ideals of } \mathcal{O}_K\}}{\{\text{nonzero principal fractional ideals of } \mathcal{O}_K\}}.$$

Equivalently, $\mathrm{Cl}(\mathcal{O}_K)$ is the group of invertible ideals modulo principal invertible ideals. A central part of basic algebraic number theory is to show that the class group of K is *finite*; that is, up to K-scalars there are only finitely many nonzero ideals of $\mathcal{O}_K$. When one gets further into algebraic number theory, special subrings $\mathcal{O} \subseteq \mathcal{O}_K$ start to appear as endomorphism rings of elliptic curves. Specifically, an elliptic curve E defined over a field k will always have a group law, e.g. see chapter 3 of [Sil09]. When the characteristic of k is zero, its ring of endomorphisms – that is, the ring of algebraic maps from E to itself which fix the point at infinity – is isomorphic either to $\mathbb{Z}$ or to a ring "strictly larger" than $\mathbb{Z}$. In the latter case, its endomorphism ring must be some order $\mathcal{O}$ in an imaginary quadratic number field K.

Orders in imaginary quadratic fields are relatively simple: for such a field K, let us write $K = \mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\omega_K)$, where $d \in \mathbb{Z}_{>0}$ is squarefree and

$$\omega_K := \begin{cases} \frac{1+\sqrt{-d}}{2} & \text{if } -d \equiv 1 \pmod 4 \\ \sqrt{-d} & \text{if } -d \equiv 2, 3 \pmod 4. \end{cases}$$

Then its ring of integers $\mathcal{O}_K$ is monogenic, with $\mathcal{O}_K = \mathbb{Z}[\omega_K]$. An order $\mathcal{O}$ of K will always be of the form $\mathcal{O} = \mathbb{Z}[f\omega_K]$, where $f = [\mathcal{O}_K : \mathcal{O}]$ is the additive index of $\mathcal{O}$ in $\mathcal{O}_K$. Conversely, for any integer $f > 0$ the ring $\mathbb{Z}[f\omega_K]$ will always be an order in K, and its index in $\mathcal{O}_K$ is f. The more general definition of an order $\mathcal{O}$ in an arbitary degree n number field K is a rank n $\mathbb{Z}$-submodule of K with $1 \in \mathcal{O}$ and a $\mathbb{Q}$-basis for K. For a study of imaginary quadratic orders, see e.g. [Cox13].

Unlike its ring of integers $\mathcal{O}_K$, the ring $\mathcal{O}$ may have nonzero ideals which are not invertible; we thus adjust the definition of its Picard group $\mathrm{Pic}(\mathcal{O})$ to only consider nonzero *invertible* fractional ideals of $\mathcal{O}$. As we will prove in the course of these notes,

$\mathrm{Pic}(\mathcal{O})$ will be *finite*, just as $\mathrm{Pic}(\mathcal{O}_K) = \mathrm{Cl}(\mathcal{O}_K)$ is; in fact, its class number will be divisible by the class number $h_K := \#\mathrm{Cl}(\mathcal{O}_K)$.

The main result we are working towards is the beginning of a "class number formula" for an order $\mathcal{O}$; it is Theorem 12.12 [Neu99]. In the following, the *conductor ideal* $\mathfrak{f}$ is defined as the largest ideal of both $\mathcal{O}$ and $\mathcal{O}_K$; for now, we consider it the special ideal of $\mathcal{O}$ where any ideal of $\mathcal{O}$ coprime to $\mathfrak{f}$ must be invertible in $\mathcal{O}$. Certainly $f \in \mathfrak{f}$, and in this way it measures the difference between $\mathcal{O}$ and $\mathcal{O}_K$.

Theorem (A class number formula for orders)**.** *Let K be a number field, and let $\mathcal{O}_K$ denote the maximal order of K (the ring of integers of K). Let $\mathcal{O}$ be an order in K, and let $\mathfrak{f}$ be the conductor of $\mathcal{O}$ in $\mathcal{O}_K$. Then $h_{\mathcal{O}} := \#\mathrm{Pic}(\mathcal{O})$ is finite, and one has*

$$h_{\mathcal{O}} = \frac{h_K}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \frac{\#(\mathcal{O}_K/\mathfrak{f})^\times}{\#(\mathcal{O}/\mathfrak{f})^\times}$$

where $h_K := \#\mathrm{Cl}(\mathcal{O}_K)$ is the class number of K. Furthermore, one has $h_K \mid h_{\mathcal{O}}$.

There are proofs for the class number formula for imaginary quadratic orders which are simpler, see Theorem 7.24 [Cox13]. Our proof will consider a more general class of one-dimensional Noetherian domains, generalizing orders. We will be showing the existence of an exact sequence which, in the number field context, gives rise to our order class number formula. The reason for following this approach is two-fold: First, the general case may have relevance outside the number field case to other fields of interest to number theorists, e.g. function fields. Second, while more technical there is a certain pleasantness to a purely commutative-algebraic proof of something as specific as the class number formula is to number fields; in making less assumptions on the rings of interest, it somehow elucidates the structure of the class groups. It also puts commutative algebra to good use toward number theory.

2. A commutative algebraic number-theoretic approach to the class number formula

Let A be a domain with quotient field K. Recall that a *fractional ideal of A* is an A-submodule M of K with $aM \subseteq A$ for some nonzero $a \in A$, i.e., aM is an integral A-ideal for some $a \neq 0 \in A$. Just as ideals generalize integers, fractional ideals generalize fractions of integers; fractional ideals of A are simply A-submodules of K with a denominator.

For a fractional A-ideal M, let us define the *ideal quotient* of M, or its *colon ideal*, to be the A-module

$$(A : M)_K := \{\alpha \in K \mid \alpha M \subseteq A\}.$$

The ideal quotient is the collection of "denominators" for M in K.

If M is a nonzero fractional ideal, then so is $(A : M)_K$: it is easy to see that $(A : M)_K$ is an A-submodule of K. To check that $(A : M)_K$ is fractional, let us say $aM \subseteq A$ for some nonzero $a \in A$. Let us fix some nonzero $m \in M$; then it follows that $am \in A$ and $am(A : M)_K \subseteq A$: to argue the latter part, note that if we let $\alpha \in (A : M)_K$, then we must have $am\alpha = a\alpha m \in a\alpha M \subseteq aA \subseteq A$.

Recall that a K-fractional ideal M is *invertible* if there is another K-fractional ideal N with $MN = A$; we then write $M^{-1} := N$. In the event that M is invertible, it can be checked that $M^{-1} = (A : M)_K$, so that the inverse ideal of M is the unique inverse of M. Since $M(A : M)_K$ is always an integral ideal, showing that M is invertible is equivalent to showing that $1 \in M(A : M)_K$. In general, one has the following implications for an A-submodule of K:

$$\text{principal} \Rightarrow \text{invertible} \Rightarrow \text{finitely generated over } A \Rightarrow \text{fractional}.$$

It is well-known that a domain A is Dedekind precisely when all nonzero ideals are invertible, e.g. Theorem 9.8 [AM69]. In this case, if we let $I(A)$ denote the set of all nonzero fractional ideals of A, then $I(A)$ is a group; and if $P(A)$ denotes the subgroup of principal A-submodules of K, then the *class group* of A, or the *Picard group*, is defined as the quotient group

$$\mathrm{Pic}(A) := I(A)/P(A).$$

Suppose we want to define a similar class group for an arbitrary integral domain. In such cases, $P(A)$ is still a group under multiplication, but $I(A)$ need not be. If we re-set $I(A)$ to be the group of *invertible* ideals of A, then $I(A)$ is certainly a group. This construction seems rather contrived, doesn't it? Is there a more useful characterization for invertible ideals? For Noetherian domains, there is: we will show that a fractional ideal is invertible if and only if is it locally principal at each prime ideal.

Proposition 1. *Let A be a Noetherian domain. Then a nonzero fractional ideal M of A is invertible if and only if its localization $M_{\mathfrak{p}}$ is principal for every nonzero prime $\mathfrak{p} \subseteq A$.*

Proof. For the forward direction, we suppose that M is an invertible fractional A-ideal. Then $(A : M)_K$ must be its inverse, so that we have $M(A : M)_K = A$. This is equivalent to having $1 \in M(A : M)_K$, so we may write

$$1 = \sum_{i=1}^{n} m_i \alpha_i$$

for some $m_i \in M$ and some $\alpha_i \in (A : M)_K$.

Let $\mathfrak{p}$ be a nonzero prime ideal of A. Since $1 \notin \mathfrak{p}$ and since each $m_i\alpha_i$ is in A, we cannot have all $m_i\alpha_i$ also lie in $\mathfrak{p}$; in particular, for some j we must have $m_j\alpha_j \in A \setminus \mathfrak{p}$, so that $m_j\alpha_j$ is a unit in $A_{\mathfrak{p}}$.

We claim that $MA_{\mathfrak{p}} = m_jA_{\mathfrak{p}}$: it is clear that $m_jA_{\mathfrak{p}} \subseteq MA_{\mathfrak{p}}$. For the other direction, we let $x \in M$. Since $\alpha_j \in (A : M)_K$, it follows that $x\alpha_j \in A$. From this, we see that

$$x = x\frac{m_j\alpha_j}{m_j\alpha_j} = m_j \cdot \left(x\alpha_j \cdot \frac{1}{m_j\alpha_j}\right) \in m_jA_{\mathfrak{p}}.$$

We conclude that M is principally generated at each localization.

For the other direction, let us suppose that $MA_{\mathfrak{p}}$ is a principal fractional ideal at every nonzero prime $\mathfrak{p}$. Since $M \neq 0$, for each $\mathfrak{p}$ we may write $MA_{\mathfrak{p}} = a_{\mathfrak{p}}A_{\mathfrak{p}}$ for some nonzero $a_{\mathfrak{p}} \in A$; it is clear that $a_{\mathfrak{p}} \in M$. For the sake of contradiction, suppose M were not invertible: it follows then that $M(A : M)_K$ is a proper ideal of A, hence $M(A : M)_K$

is contained in some maximal ideal $\mathfrak{m}$. By assumption, we may write $MA_{\mathfrak{m}} = a_{\mathfrak{m}}A_{\mathfrak{m}}$ for some $a_{\mathfrak{m}} \neq 0 \in A$. On the other hand, Since A is Noetherian, we know that M is finitely generated over A, so we may write $M = Am_1 + \ldots + Am_n$ for some $m_i \in M$. It follows then that for each i we have $m_i \in a_{\mathfrak{m}}A_{\mathfrak{m}}$, and so we can write $m_i = \frac{a_{\mathfrak{m}}a_i}{s_i}$ for some $a_i \in A$ and some $s_i \in A \setminus \mathfrak{m}$. If we set $s := s_1 \cdots s_n$, then for each i we find that $sm_i \in a_{\mathfrak{m}}A$. This tells us that $sa_{\mathfrak{m}}^{-1}m_i \in A$ for each i, which implies that $sa_{\mathfrak{m}}^{-1}M \subseteq A$. By definition of the inverse ideal, we get that $sa_{\mathfrak{m}}^{-1} \in (A : M)_K$. We deduce then $s = sa_{\mathfrak{m}}^{-1}a_{\mathfrak{m}} \in (A : M)_K M \subseteq \mathfrak{m}$, so that $s \in \mathfrak{m}$ – a contradiction since each $s_i \notin \mathfrak{m}$ and $\mathfrak{m}$ is prime. Therefore, we must have that $M(A : M)_K = A$ if $MA_{\mathfrak{p}}$ is principal at every nonzero prime ideal $\mathfrak{p}$, which concludes our proof. □

To recap, we let $I(A)$ denote the group of invertible fractional ideals of A and $P(A)$ the group of nonzero principal fractional ideals of A. We then define the *class group* of A to be the quotient

$$\mathrm{Pic}(A) := I(A)/P(A).$$

Similarly, we refer to the cardinality of $\mathrm{Pic}(A)$ as the *class number* of A, written h_A. Then Proposition 1 tells us the following: $I(A)$ consists of the nonzero fractional ideals which are *locally* principal, whereas $P(A)$ consists of the nonzero fractional ideals which are *globally* principal. Additionally, Proposition 1 along with the fact that there exist Noetherian domains with nontrivial class group (e.g. $A := \mathbb{Z}[\sqrt{5}]$), shows us that "being principal" is not a local property for fractional ideals.

Let K be a number field with ring of integers $\mathcal{O}_K$. Basic number theory/commutative algebra shows us that $\mathcal{O}_K$ is a Dedekind domain, and has an integral basis of length $[K : \mathbb{Q}]$; the latter fact is due to $K/\mathbb{Q}$ being a finite and *separable* field extension. As it turns out, there are many more interesting subrings of K which have an integral basis of length $[K : \mathbb{Q}]$, but are not necessarily Dedekind domains. Such rings $\mathcal{O}$ are called *orders* of K; in this case, $\mathcal{O}_K$ is referred to as the *maximal order*, for obvious reasons.

Thanks to an order having an integral basis of length $[K : \mathbb{Q}]$, orders are Noetherian of Krull dimension one – almost Dedekind domains, except they need not be integrally closed. And if perchance an order is integrally closed, then it must be the maximal order. The prototypical example of a nonmaximal order is $\mathcal{O} := \mathbb{Z}[\sqrt{5}]$: it is properly contained in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, the latter of which is known to be the ring of integers of $\mathbb{Q}\left(\sqrt{5}\right)$. We can easily check that $\mathcal{O}$ is not integrally closed: $\frac{1+\sqrt{5}}{2}$ is an algebraic integer (it is a root of monic $x^2 - x - 1 \in \mathbb{Z}[x]$) and lies in its fraction field $\mathbb{Q}(\sqrt{5})$, but $\frac{1+\sqrt{5}}{2}$ is not in $\mathcal{O}$ since $\frac{1}{2} \notin \mathcal{O}$.

In the rest of these notes, $\mathfrak{p}$ will always denote a prime ideal of A. Before we begin the harder proofs, we will need a few lemmas.

Lemma 2. *For a domain A, one has*

$$\bigcap_{\mathfrak{p} \subseteq A} A_{\mathfrak{p}} = A.$$

Proof. The inclusion $\supseteq$ is clear since A is naturally embedded into each $A_{\mathfrak{p}}$ by the map $a \mapsto \frac{a}{1}$, as per their embeddings into K.

For the other direction, suppose $x \in A_\mathfrak{p}$ for each $\mathfrak{p} \subseteq A$. Since $x \in K$, we may write $x = \frac{a}{s}$ for some $a, s \in A$. Consider the set

$$I := \{c \in A \mid ca \in sA\};$$

I is the set of elements $c \in A$ whose product cx is an element of A. Our goal is to show that $1 \in I$, so that s "divides" a and thus $x \in A$.

I is certainly nonzero since $s \in I$, and it is easy to check that I is an ideal. To show that $I = A$, let $\mathfrak{m}$ be an arbitrary maximal ideal; we will show that $I \not\subseteq \mathfrak{m}$. Since $x \in A_\mathfrak{m}$, we may write $x = \frac{a_\mathfrak{m}}{s_\mathfrak{m}}$ for some $a_\mathfrak{m}, s_\mathfrak{m} \in A$ with $s_\mathfrak{m} \in A \smallsetminus \mathfrak{m}$. Then from $\frac{a}{s} = x = \frac{a_\mathfrak{m}}{s_\mathfrak{m}}$ we get

$$as_\mathfrak{m} = sa_\mathfrak{m} \in sA,$$

which implies $s_\mathfrak{m} \in I$. Therefore, $s_\mathfrak{m} \in I$ is an element with $s_\mathfrak{m} \notin \mathfrak{m}$; this shows us that no maximal ideal of A can contain I, thereby forcing $I = A$. We conclude that $x \in A$. □

The following is another lemma, which will rely on some basic commutative algebra results.

Lemma 3. *If A is a one-dimensional Noetherian domain then any nonzero ideal of A is contained in only finitely many maximal ideals.*

Proof. Let I be a nonzero ideal of A. Since A is Noetherian, so is its quotient A/I, cf. Prop. 6.6 [AM69]. Furthermore, the prime ideals of A/I correspond to the prime ideals of A which contain I, under the natural map $\mathfrak{p} \mapsto \mathfrak{p}/I$. In particular, a prime ideal of A/I is also maximal, so we conclude that A/I is a ≤ 1-dimensional Noetherian ring. If A/I has dimension one, then this forces $0/I$ to be prime in A/I, whence $I = 0$, an impossibility. We deduce that A/I is a zero-dimensional Noetherian ring, which is equivalent to being Artinian (cf. Theorem 8.5 [AM69]). The result then follows from Artinian rings containing only finitely many maximal ideals. □

Let us recall the Chinese remainder theorem for rings.

Theorem (Global CRT)**.** *Let A be a ring, and let $\{I_j\}_{j=1}^n$ be a set of ideals of A which are pairwise comaximal: that is, for any $1 \leq j < k \leq n$ we have $I_j + I_k = A$. Then we have a natural isomorphism*

$$A/\left(\bigcap_{j=1}^{n} I_j\right) \cong \bigoplus_{j=1}^{n} A/I_j.$$

The following Theorem is a generalization of the Chinese remainder theorem for one-dimensional Noetherian domains. It will serve very useful in the following work, and is novel in its own right – so we prove it here.

Theorem (Local CRT)**.** *Let A be a one-dimensional Noetherian domain, and let $I \subseteq A$ be a nonzero ideal. Then we have*

$$A/I \cong \bigoplus_{\mathfrak{p}} A_\mathfrak{p}/IA_\mathfrak{p} = \bigoplus_{\mathfrak{p} \supseteq I} A_\mathfrak{p}/IA_\mathfrak{p}.$$

Proof. By Lemma 3, only finitely many prime ideals contain I, so we see that

$$\bigoplus_{\mathfrak{p}} A_{\mathfrak{p}}/IA_{\mathfrak{p}} = \bigoplus_{\mathfrak{p}\supseteq I} A_{\mathfrak{p}}/IA_{\mathfrak{p}}.$$

We claim that

$$I = \bigcap_{\mathfrak{p}\supseteq I} IA_{\mathfrak{p}} \cap A. \tag{1}$$

The inclusion $\subseteq$ is clear. For the other, we let $x \in \bigcap_{\mathfrak{p}} IA_{\mathfrak{p}} \cap A$. Then the set of "$I$-denominators" for x

$$J := \{a \in A \mid ax \in I\}$$

is an ideal of A. In fact, J is not contained in any maximal ideal: the argument for this is identical to that in Lemma 2. In particular, we find that $1 \in J$, whence $x \in I$.

Next, we will show that for two distinct primes $\mathfrak{p}$ and $\mathfrak{q}$, $IA_{\mathfrak{p}} \cap A$ and $IA_{\mathfrak{q}} \cap A$ are comaximal; we will then apply the global CRT to such ideals. We claim the following: if $\mathfrak{p} \supseteq I$ then $\mathfrak{p}$ is the only prime ideal which contains $IA_{\mathfrak{p}} \cap A$. First, we observe that $IA_{\mathfrak{p}} \neq 0$ implies $IA_{\mathfrak{p}}$ contains a power of $\mathfrak{p}A_{\mathfrak{p}}$: this is true since $A_{\mathfrak{p}}$ is Noetherian, hence $IA_{\mathfrak{p}}$ contains a power of its radical (cf. Proposition 7.14 [AM69]); then $A_{\mathfrak{p}}$ being one-dimensional implies its only nonzero prime is $\mathfrak{p}A_{\mathfrak{p}}$.

Write $\mathfrak{p}^n A_{\mathfrak{p}} \subseteq IA_{\mathfrak{p}}$ for some $n > 0$. Now, let us suppose that $\mathfrak{q}$ is another prime ideal which contains $IA_{\mathfrak{p}} \cap A$. By the above, it follows that $\mathfrak{p}^n A_{\mathfrak{p}} \cap A \subseteq \mathfrak{q}$. Since $\mathfrak{p}^n$ is $\mathfrak{p}$-primary (cf. Proposition 4.2 [AM69]) it follows that $\mathfrak{p}^n A_{\mathfrak{p}} \cap A = \mathfrak{p}^n$ (cf. Proposition 4.8.ii [AM69]), hence $\mathfrak{p}^n \subseteq \mathfrak{q}$. It follows that $r(\mathfrak{p}^n) \subseteq r(\mathfrak{q})$, and hence

$$\mathfrak{p} \subseteq \mathfrak{q},$$

which must be equality. We conclude that for any two distinct nonzero primes $\mathfrak{p}$, $\mathfrak{q}$ of A, the sum $IA_{\mathfrak{p}} \cap A + IA_{\mathfrak{q}} \cap A$ is not contained in any maximal ideal, which implies that $IA_{\mathfrak{p}} \cap A, IA_{\mathfrak{q}} \cap A$ are comaximal.

Next, we claim that for any ideals I and $\mathfrak{p} \supseteq I$ we have

$$A/(IA_{\mathfrak{p}} \cap A) \cong A_{\mathfrak{p}}/IA_{\mathfrak{p}}. \tag{2}$$

To see this, we consider the natural homomorphism $A \to A_{\mathfrak{p}}/IA_{\mathfrak{p}}$. It is clear that its kernel is equal to $IA_{\mathfrak{p}} \cap A$, so what's left to show is its surjectivity.

Since A is Noetherian, by Proposition 7.14 [AM69] we have that some power of its radical $r(I)^n \subseteq I$. Furthermore, by Lemma 3 I is contained in only finitely many distinct maximal ideals $\mathfrak{p}, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$. Since the radical of I is the intersection of these prime ideals, it follows that it is also their product, and so

$$r(I)^n = \mathfrak{p}^n \prod_{i=2}^{r} \mathfrak{q}_i^n \subseteq I.$$

This implies that the natural map

$$A_{\mathfrak{p}}/(\mathfrak{p}^n \prod_{i=2}^{r} \mathfrak{q}_i^n A_{\mathfrak{p}}) \to A_{\mathfrak{p}}/IA_{\mathfrak{p}}$$

is surjective. Since the composition of surjective maps is surjective, to show that $A/(IA_{\mathfrak{p}} \cap A) \to A_{\mathfrak{p}}/IA_{\mathfrak{p}}$ is onto it suffices to show that the natural map

$$A \to A_{\mathfrak{p}}/(\mathfrak{p}^n \prod_{i=1}^{r} \mathfrak{q}_i^n A_{\mathfrak{p}})$$

is onto. In fact, since the $\mathfrak{q}_i$ are maximal, each must meet $A \setminus \mathfrak{p}$; in particular, we deduce that $\mathfrak{p}^n \prod_{i=2}^{r} \mathfrak{q}_i^n A_{\mathfrak{p}} = \mathfrak{p}^n A_{\mathfrak{p}}$. Therefore, must show that the natural map

$$A \to A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}} \tag{3}$$

is surjective. We will do better: we claim that

$$A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}.$$

To see this, we first note that localization distributes over quotients– that is to say, we have

$$(A/\mathfrak{p}^n)_{\mathfrak{p}} \cong A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}.$$

Next, we note that $A/\mathfrak{p}^n$ is a local ring, as its only maximal ideal is $\mathfrak{p} + \mathfrak{p}^n$. Then, one can show that the natural map $A/\mathfrak{p}^n \to (A/\mathfrak{p}^n)_{\mathfrak{p}}$ induces an isomorphism by noting that elements $A \setminus \mathfrak{p}$ have invertible cosets mod $\mathfrak{p}^n$ – morally, "fractionalizing" elements of $A \setminus \mathfrak{p}$ does not change the ring since these were already units, From this, surjectivity in (3) follows. We thus conclude that (2) holds, i.e.,

$$A/(IA_{\mathfrak{p}} \cap A) \cong A_{\mathfrak{p}}/IA_{\mathfrak{p}}.$$

Applying the global CRT to the ideals $IA_{\mathfrak{p}} \cap A$ for which $\mathfrak{p} \supseteq I$ and using Equations (1) and (2), we conclude the local CRT

$$A/I \cong \bigoplus_{\mathfrak{p} \supseteq I} A_{\mathfrak{p}}/IA_{\mathfrak{p}}.$$

□

The following proposition will characterize the group of invertible ideals $I(A)$ on A; recall that invertible ideals are locally principal. This proposition will break $I(A)$ up into local pieces. Recall that for a ring R, we let $P(R)$ be the group of nonzero principal ideals of R.

Proposition 4. *For a one-dimensional Noetherian domain A one has*

$$I(A) \cong \bigoplus_{\mathfrak{p} \subseteq A} P(A_{\mathfrak{p}}).$$

Proof. Consider an invertible ideal M. By Lemma 1, $M_{\mathfrak{p}}$ is principal for each prime ideal $\mathfrak{p}$, so that $M_{\mathfrak{p}} \in P(A_{\mathfrak{p}})$. Since M is a fractional ideal, aM is an integral ideal for some nonzero $a \in A$. By Lemma 3, both aM and a are contained in finitely many prime ideals of A. In particular, for all but finitely many prime ideals $\mathfrak{p}$, both a is a unit in $A_{\mathfrak{p}}$ and $aMA_{\mathfrak{p}} = A_{\mathfrak{p}}$, so that $MA_{\mathfrak{p}} = A_{\mathfrak{p}}$ for all but finitely many primes. We conclude that the map $\varphi : I(A) \to \bigoplus_{\mathfrak{p}} P(A_{\mathfrak{p}})$ given by

$$\varphi(M) := (M_{\mathfrak{p}})_{\mathfrak{p} \subseteq A}$$

does have the right codomain. It is also clear that this map is a homomorphism of groups; we will show that φ is an isomorphism.

To check for injectivity: if $\varphi(M) = (1A_{\mathfrak{p}})_{\mathfrak{p}}$, then $MA_{\mathfrak{p}} = A_{\mathfrak{p}}$ for each prime $\mathfrak{p}$. In particular, since already $M \subseteq MA_{\mathfrak{p}}$ for each $\mathfrak{p}$, we deduce that

$$M \subseteq \bigcap_{\mathfrak{p}} A_{\mathfrak{p}},$$

which by Lemma 2 implies that $M \subseteq A$. This means that M is an integral ideal of A. If M is not equal to A, then M is contained in some maximal ideal $\mathfrak{m}$, which would imply that $MA_{\mathfrak{m}} \subseteq \mathfrak{m}A_{\mathfrak{m}} \subsetneq A_{\mathfrak{m}}$, which contradicts $MA_{\mathfrak{p}} = A_{\mathfrak{p}}$ for all $\mathfrak{p}$. This forces $M = A$, whence we conclude that φ is injective.

To prove surjectivity, we must show that for any tuple $(a_{\mathfrak{p}}A_{\mathfrak{p}})_{\mathfrak{p}}$ in $\bigoplus_{\mathfrak{p}} P(A_{\mathfrak{p}})$ there is an invertible fractional ideal M for which $MA_{\mathfrak{p}} = a_{\mathfrak{p}}A_{\mathfrak{p}}$ for all $\mathfrak{p}$. It suffices to show surjectivity on the generators of $\bigoplus_{\mathfrak{p}} P(A_{\mathfrak{p}})$; to this end, we fix a prime $\mathfrak{p}$ and consider a tuple $(a_{\mathfrak{q}}A_{\mathfrak{q}})_{\mathfrak{q}}$ for which $a_{\mathfrak{q}} = 1$ for all $\mathfrak{p} \neq \mathfrak{q}$. Let us set

$$M := \bigcap_{\mathfrak{q}} a_{\mathfrak{q}}A_{\mathfrak{q}}.$$

We observe that

$$M = a_{\mathfrak{p}}A_{\mathfrak{p}} \cap \bigcap_{\mathfrak{q}\neq\mathfrak{p}} A_{\mathfrak{q}} = (a_{\mathfrak{p}}A_{\mathfrak{p}} \cap A_{\mathfrak{p}}) \cap \bigcap_{\mathfrak{q}\neq\mathfrak{p}} A_{\mathfrak{q}} = a_{\mathfrak{p}}A_{\mathfrak{p}} \cap \left(A_{\mathfrak{p}} \cap \bigcap_{\mathfrak{q}\neq\mathfrak{p}} A_{\mathfrak{q}} \right).$$

Thus, by Lemma 2 we deduce that

$$M = a_{\mathfrak{p}}A_{\mathfrak{p}} \cap A; \tag{4}$$

this tells us that M is an integral ideal of A. Furthermore, one has that

$$MA_{\mathfrak{p}} = (a_{\mathfrak{p}}A_{\mathfrak{p}} \cap A)A_{\mathfrak{p}} = a_{\mathfrak{p}}A_{\mathfrak{p}}$$

(extension of contraction of extension is simply extension; cf. Proposition 1.17.ii [AM69]).

What's left to show is that $MA_{\mathfrak{q}} = A_{\mathfrak{q}}$ for any $\mathfrak{q} \neq \mathfrak{p}$. First, we note that the only prime ideal which may contain $a_{\mathfrak{p}}A_{\mathfrak{p}} \cap A$ is $\mathfrak{p}$ itself, just as our proof of the local CRT shows; and so since $M = a_{\mathfrak{p}}A_{\mathfrak{p}} \cap A$ as seen in (4), this implies that $\mathfrak{p}^n \subseteq M$ for some $n > 0$. For any prime $\mathfrak{q}$, by definition of M we have $MA_{\mathfrak{q}} \subseteq A_{\mathfrak{q}}$. If $MA_{\mathfrak{q}} \subsetneq A_{\mathfrak{q}}$, then we must have $MA_{\mathfrak{q}} \subseteq \mathfrak{q}A_{\mathfrak{q}}$, and hence $\mathfrak{p}^n \subseteq \mathfrak{q}A_{\mathfrak{q}} \cap A$. This then implies that $\mathfrak{p}^n \subseteq \mathfrak{q}$ (Prop. 7.14 [AM69]), which forces $\mathfrak{p} = \mathfrak{q}$. In particular, every prime $\mathfrak{q}$ distinct from $\mathfrak{p}$ must have that $MA_{\mathfrak{q}} = A_{\mathfrak{q}}$. From this, we deduce that M is locally principal – hence invertible (cf. Lemma 1) – and maps onto $(a_{\mathfrak{q}}A_{\mathfrak{q}})_{\mathfrak{q}}$ by φ. □

Let A be a one-dimensional Noetherian domain with fraction field K, and let B be the integral closure of A in K; observe that B is a Dedekind domain. Let us make the additional assumption that B is finitely generated as an A-module. For example, for a number field K one has the ring of integers $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$, and thus over any order $\mathcal{O}$ of K. Define the *conductor ideal of* A to be

$$\mathfrak{f} := \{b \in B \mid bB \subseteq A\} = \{a \in A \mid aB \subseteq A\}.$$

It is clear that $\mathfrak{f}$ is both an ideal of A and an ideal of B: if $x \in \mathfrak{f}$, then for any element $y \in A$ or $y \in B$, we have $xy \cdot b = x \cdot (yb) \in A$ for any $b \in B$ since $yb \in B$.

For a nonzero prime $\mathfrak{p} \subseteq A$, we call $\mathfrak{p}$ *regular* if $A_{\mathfrak{p}}$ is integrally closed. Observe that in such cases $A_{\mathfrak{p}}$ is a discrete valuation ring, cf. Proposition 9.2 [AM69].

For two ideals I and J in a ring, let us write $J \mid I$ to mean $I \subseteq J$. The following proposition characterizes all primes in A which are regular.

Lemma 5. *Let A be a one-dimensional Noetherian domain with fraction field K; let B be the integral closure of A in K. Assume B is finitely generated as an A-module. Let $\mathfrak{p} \subseteq A$ be a nonzero prime. Then $\mathfrak{p}$ is regular if and only if $\mathfrak{p} \nmid \mathfrak{f}$. For such $\mathfrak{p}$, we have that $\mathfrak{p}B$ is prime and $A_{\mathfrak{p}} = B_{\mathfrak{p}B}$.*

Proof. First, suppose that $\mathfrak{p}$ is regular. Since B is integral over A and $A \subseteq A_{\mathfrak{p}}$, we have that B is also integral over $A_{\mathfrak{p}}$, which implies $B \subseteq A_{\mathfrak{p}}$ since $A_{\mathfrak{p}}$ is integrally closed. Since B is finitely generated over A, we may thus write

$$B = A\frac{a_1}{s_1} + A\frac{a_2}{s_2} + \ldots + A\frac{a_n}{s_n}$$

for some $a_i \in A$ and $s_i \in A \smallsetminus \mathfrak{p}$. It follows that the product $s := s_1 s_2 \cdots s_n$ is an element of $A \smallsetminus \mathfrak{p}$ with $sB \subseteq A$, which tells us $s \in \mathfrak{f} \smallsetminus \mathfrak{p}$, so that $\mathfrak{p} \nmid \mathfrak{f}$.

Conversely, suppose that $\mathfrak{p} \nmid \mathfrak{f}$; let us fix $x \in \mathfrak{f} \smallsetminus \mathfrak{p}$. It follows that $xB \subseteq A$ and $x \in A \smallsetminus \mathfrak{p}$, hence we have the inclusions

$$B \subseteq \frac{1}{x}A \subseteq A_{\mathfrak{p}}.$$

Since $\mathfrak{p}A_{\mathfrak{p}}$ is a prime ideal, its pullback $\mathfrak{p}A_{\mathfrak{p}} \cap A$ is prime; and since $\mathfrak{p}$ is a maximal ideal and $\mathfrak{p} \subseteq \mathfrak{p}A_{\mathfrak{p}} \cap A$, we deduce that $\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}} \cap A$. We note that the pullback $\mathfrak{p}A_{\mathfrak{p}} \cap B$ is also prime in B, so we may localize at it. We claim that

$$A_{\mathfrak{p}} = B_{\mathfrak{p}A_{\mathfrak{p}} \cap B} \tag{5}$$

as subrings of K. The inclusion $\subseteq$ follows from $A \smallsetminus \mathfrak{p} \subseteq B \smallsetminus \mathfrak{p}A_{\mathfrak{p}} \cap B$. For the other direction, we let $y \in B_{\mathfrak{p}A_{\mathfrak{p}} \cap B}$. Then we may write $y = \frac{b}{s}$ for some $b \in B$ and some $s \in B \smallsetminus \mathfrak{p}A_{\mathfrak{p}} \cap B$. Since $x \in \mathfrak{f} \smallsetminus \mathfrak{p}$, it follows that $xb \in A$ and $xs \in A \smallsetminus \mathfrak{p}$ – for example, to see $xs \in A \smallsetminus \mathfrak{p}$ we note that if $xs \in \mathfrak{p}$, then $xs \in \mathfrak{p}A_{\mathfrak{p}}$; since $s \notin \mathfrak{p}A_{\mathfrak{p}}$, it follows that $s^{-1} \in A_{\mathfrak{p}}$, and thus $xs \in \mathfrak{p}A_{\mathfrak{p}}$ implies $x \in \mathfrak{p}A_{\mathfrak{p}}$, so that $x \in \mathfrak{p}A_{\mathfrak{p}} \cap A = \mathfrak{p}$, an impossibility. Therefore, it follows that $\frac{b}{s} = \frac{xb}{xs} \in A_{\mathfrak{p}}$. We conclude that Equation (5) holds; in particular, since $B_{\mathfrak{p}A_{\mathfrak{p}} \cap B}$ is integrally closed, so is $A_{\mathfrak{p}}$, whence we conclude that $\mathfrak{p}$ is regular. This proves the first part of the statement.

Let $\mathfrak{p} \neq 0 \subseteq A$ be a regular prime. We wish to show that $\mathfrak{p}B = \mathfrak{p}A_{\mathfrak{p}} \cap B$. Observe that $\mathfrak{p}A_{\mathfrak{p}} \cap B$ is the only prime in B lying above $\mathfrak{p}$: if $\mathfrak{Q}$ is another prime of B with $\mathfrak{p} = A \cap \mathfrak{Q}$, then it follows that $A_{\mathfrak{p}} \subseteq B_{\mathfrak{Q}}$, and hence

$$\mathfrak{p}A_{\mathfrak{p}} \cap B \subseteq \mathfrak{Q}B_{\mathfrak{Q}} \cap B = \mathfrak{Q},$$

so by maximality of $\mathfrak{p}A_{\mathfrak{p}} \cap B$ we have $\mathfrak{p}A_{\mathfrak{p}} \cap B = \mathfrak{Q}$. Therefore, since B is Dedekind and $\mathfrak{p}A_{\mathfrak{p}} \cap B$ is the only prime which divides $\mathfrak{p}B$, we get that

$$\mathfrak{p}B = (\mathfrak{p}A_{\mathfrak{p}} \cap B)^n$$

for some $n \geq 1$. Since $\mathfrak{p}$ is regular we see that $B \subseteq A_{\mathfrak{p}}$, which implies

$$\mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}BA_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}} \cap B)^n A_{\mathfrak{p}} \subseteq \mathfrak{p}^n A_{\mathfrak{p}},$$

from which we deduce that $n = 1$. In particular, we conclude that $\mathfrak{p}B = \mathfrak{p}A_{\mathfrak{p}} \cap B$; from this, it also follows that $\mathfrak{p}B$ is prime, and our final conclusion $A_{\mathfrak{p}} = B_{\mathfrak{p}B}$ follows from (5). □

In the following, for a prime $\mathfrak{p}$ of A and a ring B over A, we let $B_{\mathfrak{p}} := (A \smallsetminus \mathfrak{p})^{-1}B$ be the "fractionalization" of B as an A-module. The following remark will be referenced in the upcoming proofs.

Remark. Let A be a one-dimensional Noetherian domain with fraction field K, and let B denote the integral closure of A in K; assume B is finitely generated over A. First, for a domain R we will let $\widetilde{R}$ denote its integral closure in its fraction field. For any prime $\mathfrak{p} \subseteq A$ the integral closure of $A_{\mathfrak{p}}$ is checked to be

$$\widetilde{A_{\mathfrak{p}}} = \widetilde{(A \smallsetminus \mathfrak{p})^{-1}A} = (A \smallsetminus \mathfrak{p})^{-1}\widetilde{A} = B_{\mathfrak{p}}$$

(e.g. Proposition 5.6 [AM69]). Since $A_{\mathfrak{p}}$ is a one-dimensional Noetherian domain, it follows that $\widetilde{A_{\mathfrak{p}}} = B_{\mathfrak{p}}$ is an integrally closed 1-D Noetherian domain, hence B is Dedekind (compare to Theorem 9.3 [AM69]). Furthermore, $B_{\mathfrak{p}}$ has only finitely many prime ideals: if J is a prime ideal of $B_{\mathfrak{p}}$, then we may write $J = (A \smallsetminus \mathfrak{p})^{-1}\mathfrak{Q}$ for some prime ideal $\mathfrak{Q} \subseteq B$ with $\mathfrak{Q} \subseteq B \smallsetminus (A \smallsetminus \mathfrak{p}) = (B \smallsetminus A) \cup \mathfrak{p}$ (cf. Proposition 3.11.iv) [AM69]). Since $J \cap A_{\mathfrak{p}}$ is prime, by $A_{\mathfrak{p}}$ being a local ring we must have $J \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$: to see this, note that either $J \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ or $J \cap A_{\mathfrak{p}} = 0$. If the latter holds, then by Proposition 5.6 [AM69] one has that $B_{\mathfrak{p}}/J$ is integral over $A_{\mathfrak{p}}/J \cap A_{\mathfrak{p}} = A_{\mathfrak{p}}$, which is impossible since $B_{\mathfrak{p}}/J$ is a field (cf. Proposition 5.7 [AM69]). We conclude that any prime ideal of $B_{\mathfrak{p}}$ must lie above $\mathfrak{p}A_{\mathfrak{p}}$. In particular, since $B_{\mathfrak{p}}$ has only finitely many prime ideals lying over any prime of $A_{\mathfrak{p}}$ (e.g. Exercise 9.3 of [Mat86]) we deduce that $B_{\mathfrak{p}}$ is a Dedekind domain with finitely many prime ideals.[1]

In the following, for a ring R we let $R^\times$ denote its unit group.

Proposition 6. *Let A be a one-dimensional Noetherian domain with fraction field K, and let B denote the integral closure of A in K. Suppose B be finitely generated over A. Then we have*

$$\bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times / A_{\mathfrak{p}}^\times \cong (B/\mathfrak{f})^\times / (A/\mathfrak{f})^\times.$$

Proof. By the local CRT, we know that

$$A/\mathfrak{f} \cong \bigoplus_{\mathfrak{p} \subseteq A} A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}}. \tag{6}$$

Local CRT on $\mathfrak{f}$ as a B-ideal also shows us that

$$B/\mathfrak{f} \cong \bigoplus_{\mathfrak{Q} \subseteq B} B_{\mathfrak{Q}}/\mathfrak{f}B_{\mathfrak{Q}}.$$

[1] One can also check that this forces $B_{\mathfrak{p}}$ to be a PID.

Partitioning prime ideals of B by which primes in A they lie above, one has

$$B/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} \bigoplus_{\mathfrak{Q}\supseteq\mathfrak{p}} B_{\mathfrak{Q}}/\mathfrak{f}B_{\mathfrak{Q}}. \tag{a}$$

Let us fix a prime $\mathfrak{p}$ of A. From our Remark on page 10, we have that the integral closure $B_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ has finitely many prime ideals, and they are of the form $\mathfrak{Q}B_{\mathfrak{p}}$ where $\mathfrak{Q}$ is a prime of B which lies above $\mathfrak{p}$. Thus, applying the local CRT to $B_{\mathfrak{p}}$ gives us

$$B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}} \cong \bigoplus_{\mathfrak{Q}\supseteq\mathfrak{p}} (B_{\mathfrak{p}})_{\mathfrak{Q}}/(\mathfrak{f}B_{\mathfrak{p}})_{\mathfrak{Q}}.$$

Since $A \smallsetminus \mathfrak{p} \subseteq B \smallsetminus \mathfrak{Q}$, it follows that $(B_{\mathfrak{p}})_{\mathfrak{Q}} = B_{\mathfrak{Q}}$ and $(\mathfrak{f}B_{\mathfrak{p}})_{\mathfrak{Q}} = \mathfrak{f}B_{\mathfrak{Q}}$, hence by the above isomorphism we have that

$$B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}} \cong \bigoplus_{\mathfrak{Q}\supseteq\mathfrak{p}} B_{\mathfrak{Q}}/\mathfrak{f}B_{\mathfrak{Q}}. \tag{b}$$

Combining Equations (a) and (b) shows us that

$$B/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}}. \tag{7}$$

Noting that the unit group of a product of rings is the product of the unit groups of the rings, we combine Equations (6) and (7) to conclude that

$$(B/\mathfrak{f})^{\times}/(A/\mathfrak{f})^{\times} \cong \bigoplus_{\mathfrak{p}} (B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}})^{\times}/(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times}. \tag{8}$$

The final part of this proof is showing that for all $\mathfrak{p} \subseteq A$ we have

$$(B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}})^{\times}/(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times} \cong B_{\mathfrak{p}}^{\times}/A_{\mathfrak{p}}^{\times}. \tag{9}$$

Before we continue, we note that $\mathfrak{f}A_{\mathfrak{p}} = \mathfrak{f}B_{\mathfrak{p}}$.

Fix $\mathfrak{p}$. Suppose $\mathfrak{p} \mid \mathfrak{f}$, i.e., suppose $\mathfrak{f} \subseteq \mathfrak{p}$. It is easy to check that if u is a unit in $B_{\mathfrak{p}}$, then $u + \mathfrak{f}A_{\mathfrak{p}}$ is a unit in $B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}}$: if not, then u would be contained in $\mathfrak{f}A_{\mathfrak{p}}$, but then from $\mathfrak{f}A_{\mathfrak{p}} \subseteq \mathfrak{p}A_{\mathfrak{p}}$ we would have u contained in $\mathfrak{p}A_{\mathfrak{p}}$, which is impossible since $\mathfrak{p}A_{\mathfrak{p}}$ is contained in all prime ideals of $B_{\mathfrak{p}}$. Thus, we may consider the homomorphism

$$\varphi : B_{\mathfrak{p}}^{\times} \to (B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times}/(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times},\ u \mapsto (u + \mathfrak{f}A_{\mathfrak{p}})(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times}.$$

We claim that this map is surjective. We note that the prime ideals of $B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}} = B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}}$ correspond to the prime ideals of $B_{\mathfrak{p}}$ that contain $\mathfrak{f}B_{\mathfrak{p}}$. Since all prime ideals of $B_{\mathfrak{p}}$ are of the form $\mathfrak{Q}B_{\mathfrak{p}}$ with $\mathfrak{Q} \subseteq B$ where $\mathfrak{Q} \cap A = \mathfrak{p}$, and since $\mathfrak{f} \subseteq \mathfrak{p}$, we actually have that the prime ideals of $B_{\mathfrak{p}}/\mathfrak{f}B_{\mathfrak{p}}$ are in 1-1 correspondence with the prime ideals of $B_{\mathfrak{p}}$. In particular, if $u + \mathfrak{f}A_{\mathfrak{p}}$ is a unit in $B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}}$ then one has that $u + \mathfrak{f}A_{\mathfrak{p}}$ is not contained in any maximal ideal of $B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}}$, all of which are of the form $\mathfrak{Q}B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}}$ where $\mathfrak{Q}B_{\mathfrak{p}}$ is one of the finitely many prime ideals of $B_{\mathfrak{p}}$. This tells us that u is not contained in any maximal ideal of $B_{\mathfrak{p}}$, and hence u is a unit in $B_{\mathfrak{p}}$. We conclude that φ is surjective.

Next, we need to show that $\ker\varphi = A_{\mathfrak{p}}^{\times}$. We first show that $A_{\mathfrak{p}}^{\times} \subseteq \ker\varphi$. Observe that if u is a unit in $A_{\mathfrak{p}}$, then its coset $u + \mathfrak{f}A_{\mathfrak{p}}$ is a unit in $A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}}$: to see this, it suffices to check that u is nonzero in this quotient, but this follows from $\mathfrak{f} \subseteq \mathfrak{p}$.

Now we claim that $\ker\varphi \subseteq A_{\mathfrak{p}}^{\times}$. Observe that if for $u \in B_{\mathfrak{p}}^{\times}$ we have

$$(u + \mathfrak{f}A_{\mathfrak{p}})(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times} = (1 + \mathfrak{f}A_{\mathfrak{p}})(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times} \in (B_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times}/(A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times},$$

then it follows that $u + \mathfrak{f}A_{\mathfrak{p}} \in (A_{\mathfrak{p}}/\mathfrak{f}A_{\mathfrak{p}})^{\times}$, so for some $x \in A_{\mathfrak{p}}$ we have $ux - 1 \in \mathfrak{f}A_{\mathfrak{p}}$. Then multiplying by u^{-1} gives us that $x - u^{-1} \in u^{-1}\mathfrak{f}A_{\mathfrak{p}} \subseteq A_{\mathfrak{p}}$, and thus $u^{-1} \in A_{\mathfrak{p}}$. This forces $u \in A_{\mathfrak{p}}$, and therefore $u \in A_{\mathfrak{p}}^{\times}$. We conclude that $\ker\varphi = A_{\mathfrak{p}}^{\times}$, whence Equation (9) holds.

Next, we suppose that $\mathfrak{p} \nmid \mathfrak{f}$. Then by Lemma 5 we have $A_{\mathfrak{p}} = B_{\mathfrak{p}B}$, so from $B_{\mathfrak{p}} \subseteq B_{\mathfrak{p}B}$ we get $A_{\mathfrak{p}} = B_{\mathfrak{p}}$. In such a case, both sides of Equation (9) are trivial. □

As usual, let us assume that A is a one-dimensional Noetherian domain with fraction field K. Let B denote the integral closure of A in K, and assume that B is a finitely generated A-module. The following proposition contains the most important result necessary to prove the class number formula for a nonmaximal order.

Proposition 7. *The following sequence is exact:*

$$1 \to A^{\times} \to B^{\times} \to \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^{\times}/A_{\mathfrak{p}}^{\times} \to \mathrm{Pic}(A) \to \mathrm{Pic}(B) \to 1.$$

In particular, we have a short exact sequence

$$1 \to A^{\times} \to B^{\times} \to (B/\mathfrak{f})^{\times}/(A/\mathfrak{f})^{\times} \to \mathrm{Pic}(A) \to \mathrm{Pic}(B) \to 1$$

where $\mathfrak{f} := \{x \in K : bB \subseteq A\}$ *is the largest ideal of both* A *and* B

Proof. For any prime $\mathfrak{p} \subseteq A$, by our Remark on page 10 the integral closure $B_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ is a PID, hence $I(B_{\mathfrak{p}}) = P(B_{\mathfrak{p}})$. This and Proposition 4 tells us that for each prime $\mathfrak{p}$ we have

$$P(B_{\mathfrak{p}}) \cong \bigoplus_{J \subseteq B_{\mathfrak{p}} \mid J \text{ prime}} P((B_{\mathfrak{p}})_J). \tag{10}$$

Each prime $J \subseteq B_{\mathfrak{p}}$ is of the form $J = (A \smallsetminus \mathfrak{p})^{-1}\mathfrak{Q}$ for some prime ideal $\mathfrak{Q} \subseteq B$ that doesn't meet $B \smallsetminus (A \smallsetminus \mathfrak{p})$; it follows that $\mathfrak{Q} \subseteq (B \smallsetminus A) \cup \mathfrak{p}$. Furthermore, since $\mathfrak{Q}$ lies above $\mathfrak{p}A_{\mathfrak{p}}$ we also have $\mathfrak{Q}B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Since $\mathfrak{p}A_{\mathfrak{p}}$ lies above $\mathfrak{p}$, we deduce that $\mathfrak{Q}B_{\mathfrak{p}} \cap A = \mathfrak{p}$.

Since $\mathfrak{p} = \mathfrak{Q} \cap A$, we can check that $(B_{\mathfrak{p}})_{\mathfrak{Q}B_{\mathfrak{p}}} = B_{\mathfrak{Q}}$ as subrings of K; morally, inverting elements of B which are in A but not in $\mathfrak{p}$ and then inverting the remaining elements not in $\mathfrak{Q}$, is the same as inverting the elements not in $\mathfrak{Q}$. Therefore, by Equation (10) we have

$$P(B_{\mathfrak{p}}) \cong \bigoplus_{\mathfrak{Q} \subseteq B \mid \mathfrak{Q} \cap A = \mathfrak{p}} P(B_{\mathfrak{Q}}). \tag{11}$$

Making the rearrangement

$$\bigoplus_{\mathfrak{Q} \subseteq B} P(B_{\mathfrak{Q}}) = \bigoplus_{\mathfrak{p} \subseteq A} \bigoplus_{\mathfrak{Q} \subseteq B \mid \mathfrak{Q} \cap A = \mathfrak{p}} P(B_{\mathfrak{Q}}),$$

we conclude from Equation (11) and Proposition 4 that

$$I(B) \cong \bigoplus_{\mathfrak{p} \subseteq A} P(B_{\mathfrak{p}}). \tag{12}$$

Next, we turn our attention to comparing $\mathrm{Pic}(A)$ to $\mathrm{Pic}(B)$. First, we note that we have natural pushforward maps from $I(A)$ to $I(B)$, $P(A)$ to $P(B)$, and $\mathrm{Pic}(A)$ to $\mathrm{Pic}(B)$ by $M \mapsto MB$, $xA \mapsto xB$ and $MP(A) \mapsto MBP(B)$, respectively. This yields the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P(A) & \longrightarrow & I(A) & \longrightarrow & \mathrm{Pic}(A) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & P(B) & \longrightarrow & I(B) & \longrightarrow & \mathrm{Pic}(B) & \longrightarrow & 1 \end{array}$$

By Proposition 4 and Equation (12), this implies the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P(A) & \longrightarrow & \bigoplus_{\mathfrak{p}} P(A_{\mathfrak{p}}) & \longrightarrow & \mathrm{Pic}(A) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & P(B) & \longrightarrow & \bigoplus_{\mathfrak{p}} P(B_{\mathfrak{p}}) & \longrightarrow & \mathrm{Pic}(B) & \longrightarrow & 1 \end{array}$$

Now, we observe that for any integral domain R with fraction field K we have $P(R) \cong K^\times/R^\times$. Thus, we produce the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times/A^\times & \longrightarrow & \bigoplus_{\mathfrak{p}} K^\times/A_{\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(A) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & K^\times/B^\times & \longrightarrow & \bigoplus_{\mathfrak{p}} K^\times/B_{\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(B) & \longrightarrow & 1 \end{array}$$

We apply the well-known snake lemma to this diagram and furnish an exact sequence

$$1 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \mathrm{coker}\ \alpha \to \mathrm{coker}\ \beta \to \mathrm{coker}\ \gamma \to 1,$$

Since α is the map defined by $uA^\times \mapsto uB^\times$, α has kernel equal to $B^\times/A^\times$; furthermore, α is surjective, whence $\mathrm{coker}\ \alpha = 1$. β is defined by sending $(u_{\mathfrak{p}}A_{\mathfrak{p}}^\times)_{\mathfrak{p}}$ to $(u_{\mathfrak{p}}B_{\mathfrak{p}}^\times)_{\mathfrak{p}}$, and is clearly surjective; it is also clear that $\ker\beta = \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times/A_{\mathfrak{p}}^\times$. Therefore, our exact sequence becomes

$$1 \to B^\times/A^\times \to \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times/A_{\mathfrak{p}}^\times \to \ker\gamma \to 1 \to 1 \to \mathrm{coker}\ \gamma \to 1.$$

We note that this portion

$$1 \to B^\times/A^\times \to \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times/A_{\mathfrak{p}}^\times$$

of the exact sequence is equivalent to

$$1 \to A^\times \to B^\times \to \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times / A_{\mathfrak{p}}^\times,$$

and so we procure the exact sequence

$$1 \to A^\times \to B^\times \to \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times / A_{\mathfrak{p}}^\times \to \ker \gamma \to 1.$$

Next, we check that $\gamma : \mathrm{Pic}(A) \to \mathrm{Pic}(B)$ is onto. This follows from our commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times/A^\times & \longrightarrow & \bigoplus_{\mathfrak{p}} K^\times/A_{\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(A) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & K^\times/B^\times & \longrightarrow & \bigoplus_{\mathfrak{p}} K^\times/B_{\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(B) & \longrightarrow & 1 \end{array}$$

In particular, since both the map β and the map from $\bigoplus_{\mathfrak{p}} K^\times/B_{\mathfrak{p}}^\times$ to $\mathrm{Pic}(B)$ are surjective, commutativity of the diagram shows us that γ must be surjective, too. Therefore, since $\gamma : \mathrm{Pic}(A) \to \mathrm{Pic}(B)$ induces a short exact sequence

$$1 \to \ker \gamma \to \mathrm{Pic}(A) \to \mathrm{Pic}(B) \to 1,$$

we modify our exact sequence to conclude that

$$1 \to A^\times \to B^\times \to \bigoplus_{\mathfrak{p}} B_{\mathfrak{p}}^\times / A_{\mathfrak{p}}^\times \to \mathrm{Pic}(A) \to \mathrm{Pic}(B) \to 1.$$

The final part is proven by applying Proposition 6 to this exact sequence. □

Remark. Before proving the main theorem, we will need to know a fact about finite cardinality in a sequence. Let us consider an exact sequence of groups:

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} G_4 \longrightarrow 1.$$

If the index $[G_2 : G_1]$ is finite, then so is $\mathrm{im} f_2 \cong G_2/G_1$; and if G_4 is finite, then from $G_3/\ker f_3 \cong G_4$ we may conclude that G_3 is finite.

We may now prove the main theorem, the *class number formula for orders.*

Theorem (Class number formula for orders)**.** *Let K be a number field, and let $\mathcal{O}_K$ denote the maximal order of K. Let $\mathcal{O}$ be an order in K, and let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then both $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ and $h_{\mathcal{O}} := \#\mathrm{Pic}(\mathcal{O})$ are finite, and one has*

$$h_{\mathcal{O}} = \frac{h_K}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \frac{\#(\mathcal{O}_K/\mathfrak{f})^\times}{\#(\mathcal{O}/\mathfrak{f})^\times}$$

where $h_K := \#\mathrm{Cl}(\mathcal{O}_K)$ is the class number of K. Furthermore, one has $h_K | h_{\mathcal{O}}$.

Proof. By Proposition 7, one has the exact sequence

$$1 \to \mathcal{O}_K^\times/\mathcal{O}^\times \to (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{13}$$

Since $\mathcal{O}_K^\times/\mathcal{O}^\times$ injects into finite $(\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times$, we find that $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ is finite. Then by the previous Remark, $\mathrm{Pic}(\mathcal{O})$ is necessarily a finite group; and the formula for $h_{\mathcal{O}}$ is computed using the exact sequence. The claim that $h_K \mid h_{\mathcal{O}}$ follows from surjectivity of

the pushforward $\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$, which was demonstrated in the proof of Proposition 7. $\square$

Remark. A general fact from abstract algebra is that if M and N are finitely generated $\mathbb{Z}$ modules of equal rank and $N \subseteq M$, then the index $[M : N]$ is finite. Since any order $\mathcal{O}$ has a $\mathbb{Z}$-basis, it follows that any nonzero ideal I of $\mathcal{O}$ also has its own $\mathbb{Z}$-basis, and both have the same rank. In particular, we find that $\#|\mathcal{O}/I| < \infty$; thus, we have shown that both $\mathcal{O}_K/\mathfrak{f}$ and $\mathcal{O}/\mathfrak{f}$ have finite cardinality. It is a standard result from algebraic number theory that $\mathcal{O}_K^\times$ is finitely generated of rank $r_1 + r_2 - 1$, where r_1 is the number of real embeddings of K into $\mathbb{C}$ and r_2 the number of pairs of complex embeddings. Therefore, our exact sequence shows that the index $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ is finite, so that $\mathcal{O}^\times$ is also finitely generated of rank $r_1 + r_2 - 1$. Finally, another classical result that the class group $\mathrm{Cl}(\mathcal{O}_K)$ of a number field is always finite. With these facts, the class number formula for an order readily follows, as we have shown.

References

[Neu99] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999.

[AM69] M. F. Atiyah, M. F. and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., 1969.

[Mat86] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer, 2009.

[Cox13] D. A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd Edition, John Wiley & Sons, Inc., Hoboken, NJ, 2013.