IDEAL FACTORIZATION

KEITH CONRAD

1. Introduction

We will prove here the fundamental theorem of ideal theory in number fields: every nonzero proper ideal in the integers of a number field admits unique factorization into a product of nonzero prime ideals. Then we will explore how far the techniques can be generalized to other domains.

Definition 1.1. For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a commutative ring, write $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for an ideal $\mathfrak{c}$.

Theorem 1.2. *For elements α and β in a commutative ring, $\alpha \mid \beta$ as elements if and only if $(\alpha) \mid (\beta)$ as ideals.*

Proof. If $\alpha \mid \beta$ then $\beta = \alpha\gamma$ for some γ in the ring, so $(\beta) = (\alpha\gamma) = (\alpha)(\gamma)$. Thus $(\alpha) \mid (\beta)$ as ideals. Conversely, if $(\alpha) \mid (\beta)$, write $(\beta) = (\alpha)\mathfrak{c}$ for an ideal $\mathfrak{c}$. Since $(\alpha)\mathfrak{c} = \alpha\mathfrak{c} = \{\alpha c : c \in \mathfrak{c}\}$ and $\beta \in (\beta)$, $\beta = \alpha c$ for some $c \in \mathfrak{c}$. Thus $\alpha \mid \beta$ in the ring. □

Theorem 1.2 says that passing from elements to the principal ideals they generate does not change divisibility relations. However, irreducibility can change.

Example 1.3. In $\mathbf{Z}[\sqrt{-5}]$, 2 is irreducible as an element but the principal ideal (2) factors nontrivially: $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$.

To see that neither of the ideals $(2, 1 + \sqrt{-5})$ and $(2, 1 - \sqrt{-5})$ is the unit ideal, we give two arguments. Suppose $(2, 1 + \sqrt{-5}) = (1)$. Then we can write

$$1 = 2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5})$$

for some integers a, b, c, and d. Collecting real and imaginary parts,

$$1 = 2a + c - 5d, \quad 0 = 2b + c + d.$$

Solving for d in the second equation and substituting that into the first,

$$1 = 2a + 10b + 6c,$$

which is impossible since the right side is even. The proof that $(2, 1 - \sqrt{-5}) \neq (1)$ is similar.

For another proof, complex conjugation is an operation on ideals, $\mathfrak{a} \mapsto \overline{\mathfrak{a}} := \{\overline{\alpha} : \alpha \in \mathfrak{a}\}$ that respects addition and multiplication of ideals, and $\overline{(\alpha, \beta)} = (\overline{\alpha}, \overline{\beta})$. In particular, the conjugate of $(2, 1 + \sqrt{-5})$ is $(2, 1 - \sqrt{-5})$, so if $(2, 1 + \sqrt{-5}) = (1)$ then $(2, 1 - \sqrt{-5}) = (1)$, so the product $(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (2)$ is $(1)(1) = (1)$. But $(2) \neq (1)$ since 2 is not a unit in $\mathbf{Z}[\sqrt{-5}]$.

If $\mathfrak{a} \mid \mathfrak{b}$ then for some ideal $\mathfrak{c}$ we have $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$, so $\mathfrak{a} \supset \mathfrak{b}$. Divisibility implies containment. The converse may fail in some rings (see Example 8.2), but in the ring of integers of a number field it will turn out that containment implies divisibility. So it is useful to think about containment of ideals in a commutative ring as a preliminary form of

divisibility: $\mathfrak{a} \supset \mathfrak{b}$ is something like $\mathfrak{a} \mid \mathfrak{b}$. Consider in this light the following result about containment in prime ideals.

Theorem 1.4. *In a commutative ring A, an ideal $\mathfrak{p}$ is prime if and only if for all ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A,*

$$\mathfrak{p} \supset \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \supset \mathfrak{a} \text{ or } \mathfrak{p} \supset \mathfrak{b}.$$

Proof. First suppose $\mathfrak{p}$ is a prime ideal. If $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b}$ and $\mathfrak{p} \not\supset \mathfrak{a}$, pick $x \in \mathfrak{a}$ with $x \notin \mathfrak{p}$. For every $y \in \mathfrak{b}$, $xy \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, so by primality of $\mathfrak{p}$ we get $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Since $x \notin \mathfrak{p}$, $y \in \mathfrak{p}$. This holds for all $y \in \mathfrak{b}$, so $\mathfrak{b} \subset \mathfrak{p}$, *i.e.*, $\mathfrak{p} \supset \mathfrak{b}$.

Now suppose $\mathfrak{p}$ is an ideal such that, for every pair of ideals $\mathfrak{a}$ and $\mathfrak{b}$, if $\mathfrak{p}$ contains $\mathfrak{a}\mathfrak{b}$ then $\mathfrak{p}$ contains $\mathfrak{a}$ or $\mathfrak{b}$. If $x, y \in A$ and $xy \in \mathfrak{p}$, then $(x)(y) = (xy) \subset \mathfrak{p}$, so (x) or (y) is in $\mathfrak{p}$. Thus x or y is in $\mathfrak{p}$, so $\mathfrak{p}$ is prime. □

Corollary 1.5. *Let K be a number field. In $\mathcal{O}_K$, if $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where all the ideals are nonzero and prime, then $\mathfrak{p} = \mathfrak{p}_i$ for some i.*

Proof. By Theorem 1.4, $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. Since nonzero prime ideals in $\mathcal{O}_K$ are maximal, $\mathfrak{p} = \mathfrak{p}_i$. □

To prove the nonzero proper ideals of $\mathcal{O}_K$ have unique prime factorization, we will first show how to invert a nonzero prime ideal. The inverse will be an $\mathcal{O}_K$-module that is in K but not in $\mathcal{O}_K$ (*e.g.*, in $\mathbf{Q}$ the inverse of $2\mathbf{Z}$ is $(1/2)\mathbf{Z}$), so in Section 2 we will introduce the kinds of $\mathcal{O}_K$-modules we need. That nonzero prime ideals have inverses will be proved in Section 3, and after collecting a few corollaries of this invertibility we will obtain unique factorization of ideals in $\mathcal{O}_K$. Consequences of unique factorization (or, in some cases, consequences of the results used to prove unique factorization) are discussed in Section 4. In Section 5, the methods for $\mathcal{O}_K$ are extended to the integral closure of $F[T]$ in a finite extension of $F(T)$ (the "function field" case). Another approach to unique factorization is discussed in Section 6, which is independent of the other sections. In Section 7 we generalize the norm operation from elements of $\mathcal{O}_K$ to ideals. Finally, in Section 8 we discuss how to extend unique factorization of ideals to non-maximal orders.

2. Fractional Ideals

To invert ideals, we introduce $\mathcal{O}_K$-modules that are "ideals with a denominator."

Definition 2.1. A *fractional ideal* in K is a nonzero $\mathcal{O}_K$-module $I \subset K$ such that for some $d \in \mathcal{O}_K - \{0\}$, $dI \subset \mathcal{O}_K$. Such a d is called a *common denominator* for I.

Since dI is an $\mathcal{O}_K$-module in $\mathcal{O}_K$, dI is an ideal of $\mathcal{O}_K$. Letting $\mathfrak{a}$ denote dI, we have $I = \frac{1}{d}\mathfrak{a}$. Conversely, if $\mathfrak{a} \subset \mathcal{O}_K$ is a nonzero ideal and $d \in \mathcal{O}_K - \{0\}$ then $\frac{1}{d}\mathfrak{a}$ is an $\mathcal{O}_K$-module in K with common denominator d, so $\frac{1}{d}\mathfrak{a}$ is a fractional ideal.

Example 2.2. Since $\mathbf{Z}$ is a PID, the fractional ideals in $\mathbf{Q}$ are subgroups ($\mathbf{Z}$-submodules) of $\mathbf{Q}$ having the form $r\mathbf{Z}$ for $r \in \mathbf{Q}^\times$. Examples include $\frac{1}{2}\mathbf{Z}$ and $\frac{6}{5}\mathbf{Z} = 6 \cdot \frac{1}{5}\mathbf{Z}$.

Theorem 2.3. *The following properties of an $\mathcal{O}_K$-module $I \subset K$ are equivalent:*

1. *I is a fractional ideal: for some $d \in \mathcal{O}_K - \{0\}$, $dI \subset \mathcal{O}_K$,*
2. *$dI \subset \mathcal{O}_K$ for some $d \in \mathbf{Z} - \{0\}$,*
3. *$I = x\mathfrak{a}$ for some $x \in K^\times$ and some nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$,*
4. *I is a nonzero finitely generated $\mathcal{O}_K$-module in K.*

Proof. (1) $\Rightarrow$ (2): Let I be a fractional ideal and $dI \subset \mathcal{O}_K$. Every nonzero $\mathcal{O}_K$-multiple of d is also a common denominator for I. In particular, since $d \mid \mathrm{N}_{K/\mathbf{Q}}(d)$ in $\mathcal{O}_K$ we can use $\mathrm{N}_{K/\mathbf{Q}}(d) \in \mathbf{Z} - \{0\}$ as a common denominator for I.

(2) $\Rightarrow$ (3): Since dI is an $\mathcal{O}_K$-module in $\mathcal{O}_K$, dI is an ideal. Take $\mathfrak{a} = dI$ and $x = 1/d$ to see that $I = x\mathfrak{a}$.

(3) $\Rightarrow$ (4): An ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is finitely generated as a $\mathbf{Z}$-module, and thus finitely generated as an $\mathcal{O}_K$-module. Its scalar multiple $x\mathfrak{a}$ is also finitely generated over $\mathcal{O}_K$.

(4) $\Rightarrow$ (1): Write $I = \mathcal{O}_K x_1 + \cdots + \mathcal{O}_K x_d$ where the x_i's are in K and at least one is nonzero. We want to find a $d \in \mathcal{O}_K - \{0\}$ such that $dI \subset \mathcal{O}_K$. Since $\mathcal{O}_K$ has fraction field K, for each x_i there is a $d_i \in \mathcal{O}_K - \{0\}$ such that $d_i x_i \in \mathcal{O}_K$. Let d be the product of the d_i's, so $dx_i \in \mathcal{O}_K$ for all i. Thus $dI \subset \mathcal{O}_K$. □

Corollary 2.4. *Every fractional ideal in K is a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$.*

Proof. This is true for nonzero ideals in $\mathcal{O}_K$ and a fractional ideal is just a nonzero scalar multiple of such an ideal. □

Not all $\mathcal{O}_K$-submodules of K are fractional ideals. For instance, in $\mathbf{Q}$ the subgroup $\mathbf{Z}[1/2]$ is not a fractional ideal: it admits no common denominator. The fractional ideals of K are the (nonzero) *finitely* generated $\mathcal{O}_K$-submodules of K.

By comparison with fractional ideals, nonzero ideals in $\mathcal{O}_K$ are called *integral ideals*. (Think of the terms integer and fraction.) A fractional ideal of the form $x\mathcal{O}_K$ for $x \in K^\times$ is called *principal*. Writing $x = \alpha/m$ for $\alpha \in \mathcal{O}_K$ and $m \in \mathbf{Z} - \{0\}$, $x\mathcal{O}_K = \frac{1}{m} \cdot \alpha\mathcal{O}_K$, so a principal fractional ideal is the same thing as a nonzero principal ideal in $\mathcal{O}_K$ divided by an integer. When $\mathcal{O}_K$ is a PID, all fractional ideals in K are principal (and conversely).

The $\mathcal{O}_K$-modules in K can be added and multiplied, with multiplication being commutative, associative, distributing over addition, and having multiplicative identity $(1) = \mathcal{O}_K$. The sum and product of ideals in $\mathcal{O}_K$ are ideals, so the sum and product of fractional ideals are fractional ideals.

Definition 2.5. For a fractional ideal I in $\mathcal{O}_K$, set

$$\widetilde{I} = \{x \in K : xI \subset \mathcal{O}_K\}.$$

This is more than the common denominators of I, since we allow $x \in K$ and not just $x \in \mathcal{O}_K - \{0\}$. Each common denominator of I is in $\widetilde{I}$, so $\widetilde{I} \neq \{0\}$. The set $\widetilde{I}$ is an $\mathcal{O}_K$-module. In fact, $\widetilde{I}$ is a fractional ideal. To see this, pick a nonzero $y \in I$. Then $y\widetilde{I} \subset \mathcal{O}_K$, so $\widetilde{I} \subset (1/y)\mathcal{O}_K$. Therefore $\widetilde{I}$ is a submodule of a finite free $\mathbf{Z}$-module, so $\widetilde{I}$ is a finitely generated $\mathbf{Z}$-module, hence finitely generated as an $\mathcal{O}_K$-module too. Thus $\widetilde{I}$ is a fractional ideal by Theorem 2.3(4).

Example 2.6. If $\mathfrak{a} = \alpha\mathcal{O}_K$ is a principal ideal in $\mathcal{O}_K$ with $\alpha \neq 0$ then $\widetilde{\mathfrak{a}} = \{x \in K : x\alpha\mathcal{O}_K \subset \mathcal{O}_K\} = (1/\alpha)\mathcal{O}_K$ and $\mathfrak{a}\widetilde{\mathfrak{a}} = \mathcal{O}_K = (1)$. In particular, $\widetilde{\mathcal{O}}_K = \mathcal{O}_K$.

The importance of $\widetilde{I}$ is that it is the only possible candidate for a multiplicative inverse to I among the fractional ideals in K:

Theorem 2.7. *Let I be a fractional ideal in the number field K. If I admits a fractional ideal inverse then the inverse must be $\widetilde{I}$.*

Proof. Suppose there is a fractional ideal J such that $IJ = \mathcal{O}_K$. For all $y \in J$, $yI \subset JI = IJ = \mathcal{O}_K$, so $J \subset \widetilde{I}$. Multiplying this inclusion by I, $\mathcal{O}_K \subset I\widetilde{I}$. At the same time, for all $x \in \widetilde{I}$ we have $xI \subset \mathcal{O}_K$, so $\widetilde{I}I \subset \mathcal{O}_K$.

Hence $I\widetilde{I} = \mathcal{O}_K$ and $J = J\mathcal{O}_K = JI\widetilde{I} = \mathcal{O}_K\widetilde{I} = \widetilde{I}$. □

We can use Theorem 2.7 in two ways: to show I is not invertible we only have to check $I\overline{I} \neq (1)$, and if we find $IJ = (1)$ for some J then we immediately know $J = \widetilde{I}$ (even if J was not originally defined in that way).

Example 2.8. If I and J are fractional ideals with $IJ = (x)$ a principal fractional ideal, then $\frac{1}{x}J$ is a multiplicative inverse for I, so $\widetilde{I} = \frac{1}{x}J$. For instance, in $\mathbf{Z}[\sqrt{-5}]$ let $I = (3, 1+\sqrt{-5})$ and $J = (3, 1-\sqrt{-5})$. Check that $IJ = (3)$. Therefore

$$\widetilde{I} = \frac{1}{3}J = \frac{1}{3}(3, 1-\sqrt{-5}) = \mathbf{Z}[\sqrt{-5}] + \frac{1-\sqrt{-5}}{3}\mathbf{Z}[\sqrt{-5}].$$

Check that if $I_1 \subset I_2$ are fractional ideals then $\widetilde{I_2} \subset \widetilde{I_1}$. As a special case of this reversed inclusion, if $\mathfrak{a}$ is a nonzero ideal in $\mathcal{O}_K$ then $\mathcal{O}_K \subset \widetilde{\mathfrak{a}}$.

Remark 2.9. In Theorem 2.7, all we used about I is that it is an $\mathcal{O}_K$-module inside of K; the fractional ideal hypothesis (*i.e.*, I is a finitely generated $\mathcal{O}_K$-module) was not explicitly invoked in the proof and the definition of $\widetilde{I}$ makes sense for all $\mathcal{O}_K$-submodules $I \subset K$. However, the scope of validity of Theorem 2.7 is not made broader by this observation, because an invertible $\mathcal{O}_K$-module in K must be finitely generated: if $I\widetilde{I} = \mathcal{O}_K$ then $1 = x_1y_1 + \cdots + x_ry_r$ for some $r \geq 1$, $x_i \in I$, and $y_i \in \widetilde{I}$. Then for all $x \in I$ we have

$$x = x \cdot 1 = (xy_1)x_1 + \cdots + (xy_r)xr \in \mathcal{O}_K x_1 + \cdots + \mathcal{O}_K x_r,$$

so $I \subset \sum \mathcal{O}_K x_i$. The reverse inclusion is immediate since I is an $\mathcal{O}_K$-module, so $I = \sum \mathcal{O}_K x_i$ is a finitely generated $\mathcal{O}_K$-module in K and thus is a fractional ideal (Theorem 2.3).

3. Inverses of Prime Ideals

Prime factorization in $\mathbf{Z}$ can be proved by contradiction: if some integer greater than 1 has no prime factorization then let $n > 1$ be minimal without a prime factorization. Of course n is not prime, so $n = ab$ with $a, b > 1$. Then $a, b < n$, so a and b are products of primes. Hence $n = ab$ is a product of primes, which is a contradiction. Uniqueness of the prime factorization requires more work. We will use the same idea (contradiction from a minimal counterexample) to prove nonzero proper ideals in $\mathcal{O}_K$ have prime ideal factorization. The basic method is to induct on the index $[\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|$.

Lemma 3.1. *Every nonzero ideal in $\mathcal{O}_K$ contains a product of nonzero prime ideals.*

Returning to the intuitive idea that containment is a preliminary kind of divisibility, the idea of this lemma is something like "every nonzero ideal divides a product of primes."

Proof. Every nonzero ideal of $\mathcal{O}_K$ has finite index. Assume the lemma is false and let $\mathfrak{a}$ be a nonzero ideal of least index that does not contain a product of nonzero prime ideals. Then $\mathfrak{a} \neq \mathcal{O}_K$ since $\mathcal{O}_K$ contains nonzero prime ideals, so $[\mathcal{O}_K : \mathfrak{a}] \geq 2$. Since $\mathfrak{a}$ can't be a prime ideal, there must be x and y in $\mathcal{O}_K$ that are not in $\mathfrak{a}$ but $xy \in \mathfrak{a}$. Then the ideals $(x) + \mathfrak{a}$ and $(y) + \mathfrak{a}$ both properly contain $\mathfrak{a}$, so they have smaller index in $\mathcal{O}_K$ than $\mathfrak{a}$ does. Thus $(x) + \mathfrak{a}$ and $(y) + \mathfrak{a}$ contain products of nonzero prime ideals:

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (x) + \mathfrak{a}, \quad \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset (y) + \mathfrak{a}$$

for some nonzero primes $\mathfrak{p}_i$ and $\mathfrak{q}_j$, so

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset ((x) + \mathfrak{a})((y) + \mathfrak{a}) = (xy) + x\mathfrak{a} + y\mathfrak{a} + \mathfrak{a}^2 \subset \mathfrak{a}, \tag{3.1}$$

where we used $xy \in \mathfrak{a}$ for the last step. By (3.1), $\mathfrak{a}$ contains a product of nonzero prime ideals. This is a contradiction. □

Notice this proof is close to the proof that every integer > 1 is a product of primes. Why didn't we prove in Lemma 3.1 that every nonzero proper ideal equals (rather than merely contains) a product of nonzero prime ideals? Because we do *not* know (yet) that every non-prime ideal in $\mathcal{O}_K$ is a product of ideals with smaller index.

The following theorem is the key technical property of nonzero prime ideals in $\mathcal{O}_K$.

Theorem 3.2. *For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the fractional ideal $\widetilde{\mathfrak{p}}$ defined in Definition 2.5 satisfies the following properties:*

(1) $\mathcal{O}_K \subset \widetilde{\mathfrak{p}}$ *and the containment is strict,*
(2) $\mathfrak{p}\widetilde{\mathfrak{p}} = \mathcal{O}_K$.

In particular, every nonzero prime ideal in $\mathcal{O}_K$ is invertible as a fractional ideal.

Proof. Since $\mathfrak{p} \subset \mathcal{O}_K$, $\mathcal{O}_K \subset \widetilde{\mathfrak{p}}$. We need to find an element of $\widetilde{\mathfrak{p}}$ that is not in $\mathcal{O}_K$. The element will arise as a ratio y/x with arbitrary nonzero $x \in \mathfrak{p}$ and a carefully chosen $y \in \mathcal{O}_K$. (For example, in the ring $\mathbf{Z}$ use $\mathfrak{p} = 2\mathbf{Z}$, so $\widetilde{\mathfrak{p}} = (1/2)\mathbf{Z}$. An element of $\widetilde{\mathfrak{p}}$ not in $\mathbf{Z}$ is $n/2$ for odd n. We can write $n/2 = (nm)/(2m)$ for all nonzero m in $\mathbf{Z}$, and $2m$ is an arbitrary nonzero element of $\mathfrak{p}$, but nm is not arbitrary.)

Pick $x \in \mathfrak{p}$ with $x \neq 0$. Then $\mathfrak{p} \supset (x)$. From Lemma 3.1,

$$(x) \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

for some nonzero primes $\mathfrak{p}_i$. Use such a product where r is *minimal*. If $r = 1$ then $\mathfrak{p} \supset (x) \supset \mathfrak{p}_1$, so $\mathfrak{p} = \mathfrak{p}_1$ since both ideals are maximal. Thus $\mathfrak{p} = (x)$, so $\widetilde{\mathfrak{p}} = (1/x)\mathcal{O}_K \neq \mathcal{O}_K$, which is what we wanted (with $y = 1$). Thus we may suppose $r \geq 2$.

Since $\mathfrak{p} \supset (x) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{p} = \mathfrak{p}_i$ for some i by Corollary 1.5. Without loss of generality, $\mathfrak{p} = \mathfrak{p}_1$. Then $(x) \supset \mathfrak{p} \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r$. By the minimality of r, (x) does not contain the product $\mathfrak{p}_2 \cdots \mathfrak{p}_r$. So there is a $y \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ with $y \notin (x)$. Thus $y/x \notin \mathcal{O}_K$. Since $y\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (x) = x\mathcal{O}_K$, $(y/x)\mathfrak{p} \subset \mathcal{O}_K$. This shows $y/x \in \widetilde{\mathfrak{p}}$, and we already saw that $y/x \notin \mathcal{O}_K$. Thus we have settled the first part.

Now we will show why the second part (which is more interesting) follows from the first part. Picking $x \in \widetilde{\mathfrak{p}}$ with $x \notin \mathcal{O}_K$, we have $x\mathfrak{p} \subset \mathcal{O}_K$, so $\mathfrak{p} \subset \mathfrak{p} + x\mathfrak{p} \subset \mathcal{O}_K$. Since $\mathfrak{p}$ is maximal, $\mathfrak{p} + x\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{p} + x\mathfrak{p} = \mathcal{O}_K$. The second option says $\mathfrak{p}(\mathcal{O}_K + x\mathcal{O}_K) = \mathcal{O}_K$, so $\mathcal{O}_K + x\mathcal{O}_K$ is a fractional ideal inverse for $\mathfrak{p}$ and must be $\widetilde{\mathfrak{p}}$ by Theorem 2.7. We will show this option holds by eliminating the first option by contradiction.

Assume $\mathfrak{p} + x\mathfrak{p} = \mathfrak{p}$, or equivalently $x\mathfrak{p} \subset \mathfrak{p}$. That means multiplication by x preserves the finitely generated $\mathbf{Z}$-module $\mathfrak{p}$. Recall the "linear" characterization for an element of K to be an algebraic integer: it lies in a subring of K that's a finitely generated $\mathbf{Z}$-module. The subring aspect is needed only to be sure that multiplication by the particular element preserves the subring. But the condition $x\mathfrak{p} \subset \mathfrak{p}$ has exactly the same feature, even though x need not lie in $\mathfrak{p}$ (and $\mathfrak{p}$ is not a subring of K but an ideal of $\mathcal{O}_K$). Therefore since $\mathfrak{p}$ is a finitely generated $\mathbf{Z}$-module, the linear characterization of integrality can be applied to see from $x\mathfrak{p} \subset \mathfrak{p}$ that x is integral over $\mathbf{Z}$. Hence $x \in \mathcal{O}_K$. But $x \notin \mathcal{O}_K$ by its very definition, so we are done. □

Corollary 3.3. *For nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$ and nonzero prime $\mathfrak{p}$, $\mathfrak{p}\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ if and only if $\mathfrak{a} = \mathfrak{b}$.*

Proof. If $\mathfrak{a} = \mathfrak{b}$ then of course $\mathfrak{p}\mathfrak{a} = \mathfrak{p}\mathfrak{b}$. Conversely, if $\mathfrak{p}\mathfrak{a} = \mathfrak{p}\mathfrak{b}$, multiply both sides by $\widetilde{\mathfrak{p}}$. Since $\mathcal{O}_K$-module multiplication is associative, the $\mathfrak{p}$-terms cancel because $\widetilde{\mathfrak{p}}\mathfrak{p} = \mathcal{O}_K$. □

Corollary 3.4. *For every nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and nonzero prime $\mathfrak{p}$, $\mathfrak{p} \supset \mathfrak{a}$ if and only if $\mathfrak{p} \mid \mathfrak{a}$ as ideals.*

Proof. If $\mathfrak{p} \mid \mathfrak{a}$, obviously $\mathfrak{p} \supset \mathfrak{a}$. Conversely, suppose $\mathfrak{p} \supset \mathfrak{a}$. If we are going to be able to write $\mathfrak{p}\mathfrak{b} = \mathfrak{a}$ for some ideal $\mathfrak{b}$ then it must be the case that $\mathfrak{b} = \widetilde{\mathfrak{p}}\mathfrak{a}$. Thus, *define* $\mathfrak{b} = \widetilde{\mathfrak{p}}\mathfrak{a}$. This is a nonzero $\mathcal{O}_K$-module in K. Since $\mathfrak{p} \supset \mathfrak{a}$, multiplying by $\widetilde{\mathfrak{p}}$ shows $\mathcal{O}_K \supset \widetilde{\mathfrak{p}}\mathfrak{a} = \mathfrak{b}$, so $\mathfrak{b}$ is an $\mathcal{O}_K$-module in $\mathcal{O}_K$, *i.e.*, $\mathfrak{b}$ is an ideal in $\mathcal{O}_K$. Easily $\mathfrak{p}\mathfrak{b} = \mathfrak{a}$, so $\mathfrak{p} \mid \mathfrak{a}$ as ideals. □

Corollary 3.5. *For every nonzero ideal $\mathfrak{b}$ and nonzero prime $\mathfrak{p}$, $\mathfrak{p}\mathfrak{b} \subset \mathfrak{b}$ with strict inclusion.*

This means multiplication by a prime ideal shrinks the ideal.

Proof. Easily $\mathfrak{p}\mathfrak{b} \subset \mathfrak{b}$. If $\mathfrak{p}\mathfrak{b} = \mathfrak{b}$ then $\mathfrak{b} = \mathfrak{p}(\mathfrak{p}\mathfrak{b}) = \mathfrak{p}^2\mathfrak{b}$, and similarly $\mathfrak{b} = \mathfrak{p}^k\mathfrak{b}$ for all $k \geq 1$. Therefore $\mathfrak{b} \subset \mathfrak{p}^k$ for all $k \geq 1$, so

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \cdots \supset \mathfrak{p}^k \supset \cdots \supset \mathfrak{b}.$$

The index $[\mathcal{O}_K : \mathfrak{b}]$ is finite, so the descending chain of powers of $\mathfrak{p}$ must stabilize: $\mathfrak{p}^{k+1} = \mathfrak{p}^k$ for some k. Then cancelling k factors of $\mathfrak{p}$ using Corollary 3.3 implies $\mathfrak{p} = \mathcal{O}_K$, which is a contradiction. Thus $\mathfrak{p}\mathfrak{b} \neq \mathfrak{b}$. □

Now we are (finally) ready to prove unique prime factorization of ideals in $\mathcal{O}_K$. All the hard work is over!

Theorem 3.6. *Every nonzero proper ideal of $\mathcal{O}_K$ is uniquely a product of nonzero prime ideals in $\mathcal{O}_K$.*

Proof. Existence: We will prove by induction on $r \geq 1$ that if a nonzero proper ideal $\mathfrak{a} \subset \mathcal{O}_K$ contains a product of r nonzero prime ideals then it equals a product of nonzero prime ideals. (Every nonzero proper ideal fits this condition for some r since, by Lemma 3.1, every nonzero ideal in $\mathcal{O}_K$ contains a product of nonzero prime ideals.) When $r = 1$, $\mathfrak{a} \supset \mathfrak{p}$ for a nonzero prime $\mathfrak{p}$, so $\mathfrak{p}$ is maximal and $\mathfrak{a} = \mathfrak{p}$. Assuming the result for r, suppose $\mathfrak{a} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_{r+1}$. Since $\mathfrak{a}$ is a proper ideal, $\mathfrak{a} \subset \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$. Then $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_{r+1}$, so $\mathfrak{p} = \mathfrak{p}_i$ for some i. All nonzero prime ideals in $\mathcal{O}_K$ are invertible, so multiplying through the inclusion $\mathfrak{p}_i \supset \mathfrak{a} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_{r+1}$ by $\mathfrak{p}_i^{-1}$ gives $\mathcal{O}_K \supset \mathfrak{p}_i^{-1}\mathfrak{a} \supset \mathfrak{p}_1 \cdots \widehat{\mathfrak{p}}_i \cdots \mathfrak{p}_{r+1}$. (The hat means "omit this term.") Therefore by induction, $\mathfrak{p}_i^{-1}\mathfrak{a}$ is a product of nonzero prime ideals, hence $\mathfrak{a}$ is a product of nonzero prime ideals by multiplying back by $\mathfrak{p}_i$.

Uniqueness: Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ with nonzero primes $\mathfrak{p}_i$ and $\mathfrak{q}_j$. To show $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ after reindexing, we can cancel common prime ideals on both sides (Corollary 3.3) and thus may suppose $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i and j. Since $\mathfrak{p}_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, $\mathfrak{p}_1$ is some $\mathfrak{q}_j$ by Corollary 1.5. This is a contradiction. □

Now we have a simpler proof of Corollary 3.5: if $\mathfrak{p}\mathfrak{b} = \mathfrak{b}$ then $\mathfrak{p} = (1)$ by writing $\mathfrak{b}$ as a product of primes and cancelling common prime factors on both sides.

4. Consequences

Using the existence of prime ideal factorizations and the invertibility of nonzero prime ideals, we can extend some properties of nonzero prime ideals to other (integral or fractional) ideals.

Theorem 4.1. *For every fractional ideal I in K, $\widetilde{I}$ as in Definition 2.5 is an inverse for I: $I\widetilde{I} = \mathcal{O}_K$.*

Proof. If $I = \mathcal{O}_K$ then $\widetilde{I} = \mathcal{O}_K$. Now suppose $I = \mathfrak{a}$ is a nonzero proper ideal of $\mathcal{O}_K$. Then we can write $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some nonzero prime ideals $\mathfrak{p}_i$ and we already know $\mathfrak{p}_i\widetilde{\mathfrak{p}}_i = \mathcal{O}_K$. For $x \in K$,

$$\begin{aligned} x \in \widetilde{\mathfrak{a}} &\iff x\mathfrak{a} \subset \mathcal{O}_K \\ &\iff (x)\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathcal{O}_K \\ &\iff (x)\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \widetilde{\mathfrak{p}}_1 \qquad \text{(multiply both sides by } \widetilde{\mathfrak{p}}_1\text{)} \\ &\ \ \vdots \\ &\iff (x) \subset \widetilde{\mathfrak{p}}_1\widetilde{\mathfrak{p}}_2 \cdots \widetilde{\mathfrak{p}}_r \\ &\iff x \in \widetilde{\mathfrak{p}}_1\widetilde{\mathfrak{p}}_2 \cdots \widetilde{\mathfrak{p}}_r. \end{aligned}$$

Thus

$$\widetilde{\mathfrak{a}} = \widetilde{\mathfrak{p}}_1\widetilde{\mathfrak{p}}_2 \cdots \widetilde{\mathfrak{p}}_r.$$

Since $\mathfrak{p}\widetilde{\mathfrak{p}} = \mathcal{O}_K$ for every nonzero prime ideal $\mathfrak{p}$, we obtain $\mathfrak{a}\widetilde{\mathfrak{a}} = \mathcal{O}_K$. If I is a fractional ideal that is not an ideal of $\mathcal{O}_K$, let d be a common denominator of I: $dI \subset \mathcal{O}_K$. Denote dI as $\mathfrak{a}$, so $I = (1/d)\mathfrak{a}$. Then $\widetilde{I} = \{x \in K : xI \subset \mathcal{O}_K\} = \{x \in K : (x/d)\mathfrak{a} \subset \mathcal{O}_K\} = d\widetilde{\mathfrak{a}}$, so $I\widetilde{I} = Id\widetilde{\mathfrak{a}} = (1/d)\mathfrak{a}d\widetilde{\mathfrak{a}} = \mathfrak{a}\widetilde{\mathfrak{a}} = \mathcal{O}_K$. □

From now on we write $\widetilde{I}$ as I^{-1}. That is,

$$I^{-1} = \{x \in K : xI \subset \mathcal{O}_K\}.$$

We define negative powers of I as positive powers of I^{-1} in the obvious way and the usual rules of exponents (such as $I^{n_1}I^{n_2} = I^{n_1+n_2}$) apply with arbitrary integral exponents.

Corollary 4.2. *The fractional ideals in K form a commutative group under multiplication that is freely generated by the nonzero prime ideals in $\mathcal{O}_K$.*

Proof. Multiplication of $\mathcal{O}_K$-modules in K is commutative and associative, $\mathcal{O}_K = (1)$ is the identity, and the product of two fractional ideals is a fractional ideal (a product of finitely generated $\mathcal{O}_K$-modules is finitely generated). We have just seen that fractional ideals have fractional ideal inverses, so the fractional ideals are a multiplicative group. To show the nonzero prime ideals generate the group, let I be a fractional ideal. For some $d \in \mathcal{O}_K - \{0\}$, $dI \subset \mathcal{O}_K$, so dI is a nonzero ideal in $\mathcal{O}_K$. Factor this into prime ideals: $dI = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Since $dI = (d)I$, we factor (d) into prime ideals, say as $(d) = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, and then obtain

$$I = (d)^{-1} \cdot (d)I = \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Unique factorization says the nonzero prime ideals admit no nontrivial multiplicative relations, so they generate the group of fractional ideals freely. □

Every fractional ideal can be written as a product

$$\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

with $a_i \in \mathbf{Z}$, and by unique factorization this is an integral ideal (that is, an ideal in $\mathcal{O}_K$) if and only if every exponent a_i is nonnegative.

Now we can extend Corollaries 3.3, 3.4, and 3.5 to non-prime ideals in $\mathcal{O}_K$. The results are collected into one theorem.

Theorem 4.3. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$.*

(1) *For nonzero ideals $\mathfrak{b}$ and $\mathfrak{c}$ in $\mathcal{O}_K$, $\mathfrak{ab} = \mathfrak{ac}$ if and only if $\mathfrak{b} = \mathfrak{c}$.*
(2) *For each nonzero ideal $\mathfrak{b}$ in $\mathcal{O}_K$, $\mathfrak{a} \supset \mathfrak{b}$ if and only if $\mathfrak{a} \mid \mathfrak{b}$ as ideals.*
(3) *If $\mathfrak{a} \neq (1)$ then for each nonzero ideal $\mathfrak{b}$ in $\mathcal{O}_K$, $\mathfrak{ab} \subset \mathfrak{b}$ with strict inclusion.*

Proof. For (1), the direction ($\Leftarrow$) is trivial, and multiplication by $\mathfrak{a}^{-1}$ settles ($\Rightarrow$).

For (2), ($\Leftarrow$) is trivial. For ($\Rightarrow$), let $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b} \subset \mathcal{O}_K$, so $\mathfrak{c}$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{ac} = \mathfrak{b}$.

For (3), easily $\mathfrak{ab} \subset \mathfrak{b}$. If $\mathfrak{ab} = \mathfrak{b}$ then $\mathfrak{a} = (1)$ by cancelling $\mathfrak{b}$. □

Corollary 4.4. *Every nonzero ideal in $\mathcal{O}_K$ has a principal ideal multiple.*

Proof. Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$. Pick $\alpha \neq 0$ in $\mathfrak{a}$. Then $(\alpha) \subset \mathfrak{a}$, so $\mathfrak{a} \mid (\alpha)$ by Theorem 4.3. This says (α) is a multiple of $\mathfrak{a}$. □

We can speak of the greatest common divisor and least common multiple of two nonzero ideals in $\mathcal{O}_K$: $\gcd(\mathfrak{a}, \mathfrak{b})$ is a common ideal divisor that all other common ideal divisors divide, and $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b})$ is a common multiple that divides all other common multiples.

Corollary 4.5. *For nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, write $\mathfrak{a} = \prod_i \mathfrak{p}_i^{m_i}$ and $\mathfrak{b} = \prod_i \mathfrak{p}_i^{n_i}$ with the $\mathfrak{p}_i$'s being distinct nonzero prime ideals. Then $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \prod_i \mathfrak{p}^{\min(m_i, n_i)}$ and $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b} = \prod_i \mathfrak{p}_i^{\max(m_i, n_i)}$. In particular, $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{ab}$.*

Proof. Since Theorem 4.3 says divisibility among integral ideals is the same as containment, the greatest common divisor of two integral ideals is the smallest ideal containing both of them, which is their sum. The least common multiple of two integral ideals is the largest ideal contained inside both ideals, which is their intersection. The prime factorization formulas with exponents $\min(m_i, n_i)$ and $\max(m_i, n_i)$ also fit the conditions to be the greatest common divisor and least common multiple using unique prime ideal factorization.

Since $\max(m_i, n_i) + \min(m_i, n_i) = m_i + n_i$, $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{ab}$ because the exponent of each prime ideal on both sides is the same. □

The formulas $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ and $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$ permit the notion of gcd and lcm to extend to the zero ideal: $\gcd(\mathfrak{a}, (0)) := \mathfrak{a}$ and $\operatorname{lcm}(\mathfrak{a}, (0)) := (0)$. We will have no use for this.

Definition 4.6. When $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_K$ with $\mathfrak{a} + \mathfrak{b} = (1)$, we say $\mathfrak{a}$ and $\mathfrak{b}$ are *relatively prime*.

In $\mathcal{O}_K$, the conditions $\mathfrak{a} + \mathfrak{b} = (1)$ and $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ are equivalent, both expressing the fact that $\mathfrak{a}$ and $\mathfrak{b}$ have no common ideal factors except the unit ideal. In a general commutative ring, these conditions are *not* equivalent (*e.g.*, in $\mathbf{Z}[T]$ we have $(2) + (T) = (2, T) \neq (1)$ but $(2) \cap (T) = (2T) = (2)(T)$). However, the condition $\mathfrak{a} + \mathfrak{b} = (1)$ does imply $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ in all commutative rings. Indeed, if $\mathfrak{a} + \mathfrak{b} = (1)$ then

$$\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(1) = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b})\mathfrak{a} + (\mathfrak{a} \cap \mathfrak{b})\mathfrak{b} \subset \mathfrak{ba} + \mathfrak{ab} = \mathfrak{ab},$$

and the reverse inclusion $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ is trivial, so $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.

Theorem 4.7. *Let A be a commutative ring. If ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A satisfy $\mathfrak{a} + \mathfrak{b} = (1)$ then $A/\mathfrak{ab} \cong A/\mathfrak{a} \times A/\mathfrak{b}$ as rings.*

Proof. Since $\mathfrak{a} + \mathfrak{b} = (1)$, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ by the computation preceding the theorem.

Let $f\colon A \to A/\mathfrak{a} \times A/\mathfrak{b}$ by $f(x) = (x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$. This is a ring homomorphism. The kernel is $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, so f induces an injective map $\overline{f}\colon A/\mathfrak{ab} \to A/\mathfrak{a} \times A/\mathfrak{b}$. To show $\overline{f}$

is onto, write $1 = \alpha + \beta$ for $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$. Then, for every pair $(c_1, c_2) \in A^2$, the element $x = c_2\alpha + c_1\beta$ in A satisfies $x \equiv c_1 \bmod \mathfrak{a}$ and $x \equiv c_2 \bmod \mathfrak{b}$. □

Remark 4.8. Theorem 4.7 is called the Chinese remainder theorem. It extends by induction from two ideals whose sum is (1) to every finite set of ideals that pairwise add to the unit ideal. In terms of solving simultaneous congruences, if $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are ideals with $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ for $i \neq j$, and $c_1, \ldots, c_r$ are in the ring, the congruences

$$x \equiv c_1 \bmod \mathfrak{a}_1, \ldots, x \equiv c_r \bmod \mathfrak{a}_r$$

admit a common solution (uniquely modulo $\mathfrak{a}_1 \cdots \mathfrak{a}_r$). The following corollary applies this idea to strengthen Corollary 4.4.

Corollary 4.9. *For all nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, there is an ideal $\mathfrak{c}$ such that $\mathfrak{ac}$ is principal and $\mathfrak{c}$ is relatively prime to $\mathfrak{b}$.*

This becomes Corollary 4.4 when $\mathfrak{b} = (1)$: all ideals in $\mathcal{O}_K$ are relatively prime to (1).

Proof. Write $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and $\mathfrak{b} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}$, with $e_i, f_i \geq 0$. (The exponents f_i will play no role in what follows. What really matters is that the $\mathfrak{p}_i$'s denote the primes showing up in either $\mathfrak{a}$ or $\mathfrak{b}$; only their multiplicities in $\mathfrak{a}$ will matter.) By Corollary 3.5, $\mathfrak{p}_i^{e_i+1}$ is a proper subset of $\mathfrak{p}_i^{e_i}$. Pick $y_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}^{e_i+1}$, so $y_i \equiv 0 \bmod \mathfrak{p}_i^{e_i}$ and $y_i \not\equiv 0 \bmod \mathfrak{p}_i^{e_i+1}$. (If $e_i = 0$ this just means $y_i \in \mathcal{O}_K - \mathfrak{p}_i$.) Use Theorem 4.7 to choose $x \equiv y_i \bmod \mathfrak{p}_i^{e_i+1}$ for all i. Then for all i, $x \equiv 0 \bmod \mathfrak{p}_i^{e_i}$ and $x \not\equiv 0 \bmod \mathfrak{p}_i^{e_i+1}$, so $\mathfrak{p}_i^{e_i}$ divides (x) and $\mathfrak{p}_i^{e_i+1}$ does not divide (x). Thus (x) has the same prime-ideal divisibility as $\mathfrak{a}$ at each $\mathfrak{p}_i$, and since the $\mathfrak{p}_i$ are all the prime ideal factors of $\mathfrak{a}$ or $\mathfrak{b}$, (x) and $\mathfrak{ab}$ have greatest common divisor $\mathfrak{a}$. Writing $(x) = \mathfrak{ac}$, the ideal $\mathfrak{c}$ is not divisible by some $\mathfrak{p}_i$ since (x) and $\mathfrak{a}$ are divisible by the same power of each $\mathfrak{p}_i$. Thus $\mathfrak{c}$ is relatively prime to $\mathfrak{b}$. □

Remark 4.10. Let's isolate a result we obtained in the proof of Corollary 4.9: given a set of prime ideal powers $\mathfrak{p}_i^{e_i}$ in $\mathcal{O}_K$ (the $\mathfrak{p}_i$'s are distinct) there is an $x \in \mathcal{O}_K$ such that (x) is divisible by $\mathfrak{p}_i^{e_i}$ but not $\mathfrak{p}_i^{e_i+1}$ for all i. This says we can construct a principal ideal (x) divisible by a preselected (finite) set of primes to preselected multiplicities, including multiplicity 0. However, in this construction we have no control over which other prime ideals may occur in (x). Usually (x) will be divisible by primes besides the $\mathfrak{p}_i$'s.

Theorem 4.11. *Each nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ has at most 2 generators and one of them can be chosen arbitrarily in $\mathfrak{a} - \{0\}$: for each $\alpha \in \mathfrak{a} - \{0\}$ there is $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = (\alpha, \beta)$.*

Proof. We can assume $\mathfrak{a} \neq (1)$ (otherwise use $\beta = 1$). Pick nonzero α in $\mathfrak{a}$. Then $(\alpha) \subset \mathfrak{a}$, so $\mathfrak{a} \mid (\alpha)$ by Theorem 4.3(2). Write the prime ideal factorization of (α) as $(\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with $r \geq 1$ and all $e_i \geq 1$. Then $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ with $0 \leq a_i \leq e_i$ for all i. From Remark 4.10, there is $\beta \in \mathcal{O}_K$ such that, for all i, (β) is divisible by $\mathfrak{p}_i^{a_i}$ and not by $\mathfrak{p}_i^{a_i+1}$. Then $(\beta) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}\mathfrak{b} = \mathfrak{ab}$ where $\mathfrak{b}$ is not divisible by each $\mathfrak{p}_i$. Therefore $(\alpha, \beta) = (\alpha) + (\beta) = \gcd((\alpha), (\beta))$. From the prime ideal factorizations of (α) and (β), their gcd is $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} = \mathfrak{a}$, so $\mathfrak{a} = (\alpha, \beta)$. □

Theorem 4.12. *The ring $\mathcal{O}_K$ is a unique factorization domain if and only if it is a principal ideal domain.*

Proof. It is a general theorem of algebra that every PID is a UFD. We now show that if $\mathcal{O}_K$ is a UFD then it is a PID. It suffices to show when $\mathcal{O}_K$ is a UFD that every prime ideal is principal, since every nonzero ideal is a product of prime ideals.

For each irreducible π in a UFD, the ideal (π) is prime (check!). Now we will show if $\mathcal{O}_K$ is a UFD that every nonzero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is (π) for some irreducible π. Pick $\alpha \in \mathfrak{p}$ with $\alpha \neq 0$. Since $(\alpha) \subset \mathfrak{p}$, $\mathfrak{p}$ divides (α).

By hypothesis, α has an irreducible factorization in $\mathcal{O}_K$. Write $\alpha = \pi_1 \cdots \pi_r$, where the π_i's are irreducible in $\mathcal{O}_K$. Then $(\alpha) = (\pi_1) \cdots (\pi_r)$. Each of the ideals (π_i) is prime, and $\mathfrak{p} \mid (\alpha)$, so by unique prime ideal factorization in $\mathcal{O}_K$ we must have $\mathfrak{p} = (\pi_i)$ for some i. Thus all prime ideals are principal, so $\mathcal{O}_K$ is a PID. □

For general domains, a UFD need not be a PID: $\mathbf{Z}[T]$ is an example.

5. Analogues in $F[X]$

Many properties of $\mathbf{Z}$ can be carried over to $F[X]$, where F is a field. Both $\mathbf{Z}$ and $F[X]$ have division with remainder, and thus are PIDs. The table below indicates some further similarities. In particular, the units of $F[X]$ are the nonzero constants $F^\times$, so while $\mathbf{Z}$ has only finitely many units, $F[X]$ has finitely many units only when F is a finite field. This is a small indication that analogies between $\mathbf{Z}$ and $F[X]$ are strongest when F is finite, but here we allow arbitrary F (such as $\mathbf{Q}$ or $\mathbf{R}$, not just finite fields).

$\mathbf{Z}$	$F[X]$
Prime	Irreducible
± 1	$F^\times$
Positive	Monic
$\mathbf{Q}$	$F(X)$

We want to adapt the methods from number fields to the "function field" case: if K is a finite extension of $F(X)$, does the integral closure of $F[X]$ in K have unique factorization of ideals?

Example 5.1. In the field $\mathbf{C}(X, \sqrt{X^3 - 1})$, the integral closure of $\mathbf{C}[X]$ is $\mathbf{C}[X, \sqrt{X^3 - 1}]$.

A key idea running through the proofs in the previous two sections was induction on the index of nonzero ideals in a ring of integers. We can't directly use this idea for the integral closure of $F[X]$, since ideals in $F[X]$ don't have finite index if F is an infinite field. For example, representatives in $\mathbf{Q}[X]/(X^3 - 2)$ are $a + bX + cX^2$ with rational a, b, c, and there are infinitely many of these. However, there is something finite about this example: it is finite-dimensional over $\mathbf{Q}$ with dimension 3. More generally, if $f(X)$ has degree $d \geq 0$ in $F[X]$ then $F[X]/(f)$ has dimension d as an F-vector space (with basis $1, X, X^2, \ldots, X^{d-1}$). So if we count dimension over F rather than count index in $F[X]$, then $F[X]/(f)$ has a finiteness property we can take advantage of.[1]

Let $K/F(X)$ be a finite separable extension of degree n and let A be the integral closure of $F[X]$ in K. This is an analogue of the ring of integers of a number field. For $\alpha \in A$, $\mathrm{Tr}_{K/F(X)}(\alpha)$ and $\mathrm{N}_{K/F(X)}(\alpha)$ are in $F[X]$. More generally, the characteristic polynomial of α is in $F[X][T]$.

Theorem 5.2. *With notation as above, A is a finite free $F[X]$-module of rank n, every nonzero ideal $\mathfrak{a}$ in A is a finite free $F[X]$-module of rank n, and $A/\mathfrak{a}$ is finite-dimensional over F.*

[1] Don't confuse $F[X]$ with $\mathbf{Z}[X]$. Quotient rings $\mathbf{Z}[X]/(f)$ with $f \neq 0$ need not be finite free $\mathbf{Z}$-modules: $\mathbf{Z}[X]/(2X - 1) \cong \mathbf{Z}[1/2]$ has no $\mathbf{Z}$-basis.

Proof. The proof that a ring of integers is a finite free $\mathbf{Z}$-module uses the nonvanishing of discriminants and the fact that $\mathbf{Z}$ is a PID. Because $K/F(X)$ is separable, the discriminant of every $F(X)$-basis of K is nonzero. Since $F[X]$, like $\mathbf{Z}$, is a PID, the proof that a ring of integers is a finite free $\mathbf{Z}$-module carries over to show A is a finite free $F[X]$-module. Specifically, there is an $F(X)$-basis of K that is inside A, say $e_1, \ldots, e_n$, and then $\bigoplus_{i=1}^n F[X]e_i \subset A \subset \bigoplus_{i=1}^n F[X]e_i/d$ where $d = \mathrm{disc}_{K/F(X)}(e_1, \ldots, e_n) \in F[X]$. Since A is in between two free $F[X]$-modules of rank n, it too is free of rank n.

Now let $\mathfrak{a}$ be a nonzero ideal in A. Pick $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$, so $(\alpha) \subset \mathfrak{a}$. The ideal (α) is finite free as an $F[X]$-module with rank n: letting $\gamma_1, \ldots, \gamma_n$ be an $F[X]$-basis of A, $\alpha\gamma_1, \ldots, \alpha\gamma_n$ is an $F[X]$-basis of αA. Therefore $\mathfrak{a}$ lies between two finite free $F[X]$-modules of rank n, so it also is finite free of rank n as an $F[X]$-module.

From the structure of finitely generated modules over a PID, there is an $F[X]$-basis $y_1, \ldots, y_n$ of A and nonzero $f_1, \ldots, f_n$ in $F[X]$ such that $f_1y_1, \ldots, f_ny_n$ is an $F[X]$-basis of $\mathfrak{a}$, so

$$A/\mathfrak{a} = (\bigoplus_{i=1}^n F[X]y_i)/(\bigoplus_{i=1}^n F[X]f_iy_i) \cong \bigoplus_{i=1}^n (F[X]/(f_i))\overline{y}_i.$$

Each $F[X]/(f_i)$ has finite dimension over F and there are finitely many of these, so $A/\mathfrak{a}$ is finite-dimensional over F. □

Corollary 5.3. *Every nonzero prime ideal in A is a maximal ideal.*

Proof. For every nonzero prime ideal $\mathfrak{p}$ of A, $A/\mathfrak{p}$ is a domain that is finite-dimensional over F. A domain that is finite-dimensional over a field is itself a field, so $\mathfrak{p}$ is maximal. □

Define a fractional A-ideal I to be a nonzero A-module in K with a common denominator: $aI \subset A$ for some $a \in A - \{0\}$. All the theorems in Section 2 carry over to fractional A-ideals in K. For instance, fractional A-ideals are precisely the nonzero finitely generated A-modules in K and each is a free $F[X]$-module of rank $n = [K : F(X)]$. The proof of Lemma 3.1 carries over to show every nonzero ideal in A contains a product of prime ideals: in the inductive step, instead of saying one ideal containing another has smaller index as in the number field case we now say that if $\mathfrak{a} \subset \mathfrak{a}' \subset A$ with $\mathfrak{a} \neq \mathfrak{a}'$ then $\dim_F(A/\mathfrak{a}') < \dim_F(A/\mathfrak{a})$, so the F-dimension (rather than the index) is smaller.

The proofs of Corollaries 3.3 and 3.4 go through for A with no change at all. In the proof of Corollary 3.5, replace the finiteness of the index of the ideal $\mathfrak{b}$ in the ring of integers with the finiteness of $\dim_F(A/\mathfrak{b})$. Finally, Theorem 3.6 about unique factorization of ideals carries over to A with no new ideas required. Every result in Section 4 applies to A by the same proofs (*e.g.*, in A containment of ideals is the same as divisibility). The only change needed is in the analogue of Theorem 4.12, where the proof that every nonzero nonunit $\alpha \in A$ is a product of irreducible elements in A should proceed by induction on $\deg(\mathrm{N}_{K/F(X)}(\alpha))$.

Example 5.4. The ring $\mathbf{C}[X, \sqrt{X^3 - 1}]$ has unique factorization of ideals.

There is one minor blemish in our treatment here: it was assumed from the outset that the finite extension $K/F(X)$ is separable. The reason for this assumption is that without it discriminants vanish (since the trace map $\mathrm{Tr}_{K/F(X)}$ is identically 0), so our proof that the integral closure of A in $F[X]$ is a free $F[X]$-module breaks down. This doesn't mean A can't have unique factorization of ideals, but our method of proof certainly doesn't work anymore.

Is there a counterexample to unique factorization of ideals if $K/F(X)$ is inseparable? We will find out in the next section.

6. Unique factorization of ideals by commutative algebra

Our proof of unique factorization of ideals relied on the finiteness of $\mathcal{O}_K/\mathfrak{a}$ in the number field case and the finiteness of $\dim_F(A/\mathfrak{a})$ in the function field case. Using some concepts from commutative algebra allows for another approach to unique factorization of ideals that is applicable more broadly. *Proofs in this section are only sketched.*

Definition 6.1. Let A be a commutative ring. An A-module is called *Noetherian* if all of its submodules are finitely generated. We call A a *Noetherian ring* if it is Noetherian as an A-module, *i.e.*, all the ideals of A are finitely generated.

The Noetherian property for modules is preserved under many constructions. For instance, submodules and quotient modules of a Noetherian module are Noetherian, and a finite direct sum of Noetherian modules is Noetherian. (These are derived from the following general fact: if M is an A-module and $N \subset M$ is a submodule, then M is a Noetherian A-module if and only if N and M/N are Noetherian A-modules.)

A PID is a Noetherian ring, since all ideals in a PID are singly generated, but Noetherian rings are stable under many more ring-theoretic constructions than PIDs. For instance, if A is Noetherian then so are $A[T]$ and $A/\mathfrak{a}$ for every ideal $\mathfrak{a}$. Thus $\mathbf{Z}[T_1, \ldots, T_n]$ and $F[T_1, \ldots, T_n]$ for a field F are Noetherian rings for all $n \geq 1$: all ideals in these rings are finitely generated. By comparison, if A is a PID then $A[T]$ is never a PID (unless A is a field), although $A[T]$ is Noetherian.

In a number field K, the ideals in $\mathcal{O}_K$ are finitely generated $\mathbf{Z}$-modules, and thus are finitely generated $\mathcal{O}_K$-modules. Therefore $\mathcal{O}_K$ is a Noetherian ring. Similarly, the integral closure of $F[X]$ in a finite separable extension of $F(X)$ is a Noetherian ring.

Here is the analogue of Lemma 3.1 for Noetherian domains.

Lemma 6.2. *In a Noetherian domain that is not a field, every nonzero proper ideal contains a product of nonzero prime ideals.*

Proof. See [6, p. 626]. □

The proof of Lemma 6.2 is like that of Lemma 3.1, except studying a counterexample with least index is replaced by "Noetherian induction," which is a standard technique that will be found in textbooks that discuss Noetherian modules. Noetherian induction can also be used to prove that in a Noetherian domain every nonzero nonunit can be written as a product of irreducible elements (usually not uniquely).

Definition 6.3. An integral domain is called a *Dedekind domain* if it has the following properties:

(1) Noetherian,
(2) integrally closed,
(3) all of its nonzero prime ideals are maximal.

The ring of integers in a number field is an example of a Dedekind domain. So is $\mathbf{C}[x, y]/(f)$ for an irreducible polynomial f such that the curve $f(x, y) = 0$ in $\mathbf{C}^2$ is smooth [7, p. 56]. (Smooth means there is no solution in $\mathbf{C}^2$ to $f(x, y) = 0$ where both partial derivatives of f vanish.) The ring $\mathbf{Z}[X]$ is not Dedekind, since (X) is a nonzero prime ideal

in $\mathbf{Z}[X]$ that is not maximal. Historically, the ring of integers of a number field and the ring of polynomial functions on a smooth plane curve were the first important examples of Dedekind domains.

Every PID is both a UFD and a Dedekind domain, and the converse turns out to be true too: a ring that is a UFD and a Dedekind domain is a PID.

Remark 6.4. A field fits the conditions to be a Dedekind domain: the third property holds vacuously, since there aren't nonzero prime ideals at all. To say UFDs $\cap$ Dedekind domains = PIDs, we need fields to be Dedekind domains since fields are PIDs and a UFDs (boring ones, of course). On the other hand, for technical reasons related to algebraic geometry it it better to regard fields as *not* being Dedekind domains. That is, a Dedekind domain should have at least one nonzero prime ideal. At the level of our treatment here, whether you want to say a field is a Dedekind domain or not has only minor effects on the validity of theorems about Dedekind domains, so we won't stress this point.

Definition 6.5. In a domain A, a *fractional A-ideal* is a nonzero A-module I in the fraction field of A that admits a common denominator: $dI \subset A$ for some $d \in A - \{0\}$.

Theorem 6.6. *If A is a Dedekind domain then every nonzero prime ideal $\mathfrak{p} \subset A$ is invertible as an A-module. The inverse is the A-module $\widetilde{\mathfrak{p}}$ consisting of x in the fraction field of A such that $x\mathfrak{p} \subset A$, and $\widetilde{\mathfrak{p}}$ is a fractional A-ideal.*

Proof. The proof is essentially like that of Theorem 3.2 (using Lemma 6.2 in place of Lemma 3.1). This is left to the reader to check; each property in the definition of a Dedekind domain is needed in the proof. (The Noetherian property was used in Lemma 6.2.) □

Theorem 6.7. *In a Dedekind domain A, each nonzero proper ideal has unique factorization as a product of nonzero prime ideals. The fractional A-ideals are a commutative group under A-module multiplication and is freely generated by the nonzero prime ideals of A.*

Proof. The existence of a prime ideal factorization follows from Lemma 6.2 and Theorem 6.6 in the same way Theorem 3.6 follows from Lemma 3.1 and Theorem 3.2. The uniqueness of prime ideal factorization follows from Theorem 6.6 by exactly the same argument we gave earlier in the number field setting. In a Dedekind domain, if $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ then $\mathfrak{p} = \mathfrak{p}_i$ for some i by the same proof as Corollary 1.5. □

Theorem 6.8. *The integral closure of a Dedekind domain in a finite extension of its fraction field is also Dedekind.*

Proof. See [6, pp. 633-634]. Notice we do not need to assume the field extension is separable! The proof treats first the case of a separable extension (very much like the number field setting), then a purely inseparable extension (using special features of characteristic p), and then the general case by writing a finite extension as a tower of a purely inseparable extension on top of a separable extension. □

Theorem 6.8 with base ring $\mathbf{Z}$ shows $\mathcal{O}_K$ is Dedekind for a number field K and therefore $\mathcal{O}_K$ has unique factorization of ideals by Theorem 6.7.

Theorem 6.8 is often proved in textbooks only in the case when the field extension is separable (or, even more simply, has characteristic 0). What is special about the separable case is that the trace-pairing and discriminants are available. Moreover, in the case of a separable extension one can prove a little more than Theorem 6.8: the integral closure of the initial Dedekind domain A is a finitely generated A-module. This simplifies the proof

of Theorem 6.8. When the extension is not separable, the integral closure of A may not be finitely generated as an A-module [2, exer. 3, p. 461].

We introduced Dedekind domains in Definition 6.3 by three technical properties. These rings can be characterized in many other ways, such as the following.

Theorem 6.9. *The following conditions on a domain A are equivalent:*

(1) *A is Dedekind,*
(2) *every nonzero proper ideal in A is a product of prime ideals,*
(3) *every nonzero proper ideal in A is a unique product of prime ideals,*
(4) *every nonzero ideal in A is invertible as a fractional A-ideal,*
(5) *every nonzero ideal in A is a projective A-module,*
(6) *A is Noetherian and the localization $A_{\mathfrak{p}}$ is a* PID for all nonzero prime ideals $\mathfrak{p}$.

Proof. See [5, pp. 765–767]. □

Remark 6.10. Another list of properties equivalent to being Dedekind is: Noetherian, integrally closed, and $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ for all ideals $\mathfrak{a}$ and $\mathfrak{b}$.

The integral closure of a UFD in a finite extension of its fraction field might not be a UFD, and if A is Dedekind then $A[T]$ is not Dedekind (unless A is a field and you consider fields to be Dedekind domains). There is a class of domains that includes Dedekind domains and UFDs as special cases and is preserved under both integral closure in a finite extension of the fraction field and under $A \rightsquigarrow A[T]$: Krull rings. A discussion of Krull rings is in [2, Chap. VII, Sect. 1] and [8, Sect. 12]. They are also the main object of study in [1, Chap. 3], where they are called "rings with a theory of divisors." Using terminology from commutative algebra, Dedekind domains are the 1-dimensional Krull rings (this excludes fields) and UFDs are the Krull rings with trivial class group.

7. Ideal Norms

We return to the setting of a number field K and use the finite index of ideals to develop analogues for $\mathcal{O}_K$ of concepts from elementary number theory.

Definition 7.1. For a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, its (ideal) *norm* is $\mathrm{N}\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}| = [\mathcal{O}_K : \mathfrak{a}]$.

On principal ideals this notion of norm is compatible with the ring-theoretic norm on a generator:

Theorem 7.2. *For $\alpha \in \mathcal{O}_K - \{0\}$, $\mathrm{N}((\alpha)) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$.*

Proof. From the structure of modules over a PID, there is a $\mathbf{Z}$-basis $e_1, \ldots, e_n$ of $\mathcal{O}_K$ and nonzero integers $a_1, \ldots, a_n$ such that $a_1e_1, \ldots, a_ne_n$ is a $\mathbf{Z}$-basis of the ideal (α). Then $\mathcal{O}_K/(\alpha) \cong \bigoplus_{i=1}^n (\mathbf{Z}/a_i\mathbf{Z})\overline{e}_i$, so $\mathrm{N}((\alpha)) = \prod_{i=1}^n |a_i| = |a_1 \cdots a_n|$.

Next we compute $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ in a clever way and will get the same value as $\mathrm{N}((\alpha))$, up to sign. The field K has three $\mathbf{Q}$-bases: $\{e_i\}$, $\{a_ie_i\}$, and $\{\alpha e_i\}$. Consider the commutative diagram of $\mathbf{Q}$-linear maps

$$\begin{array}{ccc} K & \xrightarrow{m_\alpha} & K \\ {\scriptstyle e_i \mapsto e_i}\downarrow & & \uparrow{\scriptstyle a_ie_i \mapsto \alpha e_i} \\ K & \xrightarrow[e_i \mapsto a_ie_i]{} & K \end{array} \tag{7.1}$$

where the map along the top is multiplication by α and the maps along the sides and bottom interchange $\mathbf{Q}$-bases of K as indicated. (The map on the left is the identity.) That the diagram commutes follows by examining the effect on each e_i both ways: on the top it goes to αe_i and the other way the effect on it is $e_i \mapsto e_i \mapsto a_i e_i \mapsto \alpha e_i$, which is exactly what m_α does to e_i. So by linearity the two ways around the diagram are the same.

Since all maps are from K to K we can speak about their determinants, and the determinant along the top is the product of the other three determinants. The determinant along the top is $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$, by definition. The determinant on the left is 1. The matrix representing the linear map on the bottom is diagonal with a_i's on the main diagonal, so its determinant is $a_1 \cdots a_n$. What about the determinant on the right? It is not clear what a matrix for it is, so how can we compute the determinant? The key point is that $\{a_1 e_1, \ldots, a_n e_n\}$ and $\{\alpha e_1, \ldots, \alpha e_n\}$ are not just $\mathbf{Q}$-bases of K but $\mathbf{Z}$-bases of a common free $\mathbf{Z}$-module (the ideal (α)). As bases of a finite free $\mathbf{Z}$-module, changing from one basis to the other is a linear map whose determinant is invertible over $\mathbf{Z}$, hence the determinant is ± 1.

Putting it all together, $\det(m_\alpha) = \pm a_1 \cdots a_n$, so $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = |a_1 \cdots a_n| = \mathrm{N}((\alpha))$. □

Example 7.3. The size of $\mathbf{Z}[\sqrt{2}]/(4 + 7\sqrt{2})$ is $|16 - 2 \cdot 49| = 82$.

See [4, pp. 185–186] for a modified definition of the ideal norm that can take negative values so a nonzero principal ideal (α) has ideal norm $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$, even with the correct sign.

Since the ring $\mathcal{O}_K/\mathfrak{a}$ has size $\mathrm{N}\mathfrak{a}$, $\mathrm{N}\mathfrak{a} \equiv 0 \bmod \mathfrak{a}$. Containment implies divisibility, so $\mathfrak{a} \mid (\mathrm{N}\mathfrak{a})$ as ideals. This is analogous to the elementwise divisibility relation $\alpha \mid \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ for $\alpha \in \mathcal{O}_K$.

The following two theorems are the main properties of norms of ideals in $\mathcal{O}_K$.

Theorem 7.4. *The norm of a nonzero prime ideal $\mathfrak{p}$ is a prime power in $\mathbf{Z}^+$. If $\mathrm{N}\mathfrak{p} = p^f$ then $\mathfrak{p} \mid (p)$.*

Proof. Let $\mathfrak{p}$ be a nonzero prime ideal in $\mathcal{O}_K$. The ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field, so from the theory of finite fields it has prime power size. Hence $\mathrm{N}\mathfrak{p}$ is a prime power in $\mathbf{Z}^+$.

Let p be the characteristic of $\mathcal{O}_K/\mathfrak{p}$, so $p = 0$ in $\mathcal{O}_K/\mathfrak{p}$. That means $p \in \mathfrak{p}$, so $(p) \subset \mathfrak{p}$, so $\mathfrak{p} \mid (p)$. □

We call $\mathcal{O}_K/\mathfrak{p}$ the residue field at $\mathfrak{p}$. The number f in Theorem 7.4 can be interpreted as $\dim_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/\mathfrak{p})$ and therefore is called the residue field degree.

Theorem 7.5. *For nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}$.*

Proof. We give two proofs.

First proof: Since every nonzero ideal is a product of prime ideals it suffices to show $\mathrm{N}(\mathfrak{a}\mathfrak{p}) = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{p}$ for nonzero $\mathfrak{a}$ and nonzero prime $\mathfrak{p}$.

Since $\mathcal{O}_K \supset \mathfrak{a} \supset \mathfrak{a}\mathfrak{p}$, $[\mathfrak{a} : \mathfrak{a}\mathfrak{p}] = \mathrm{N}(\mathfrak{a}\mathfrak{p})/\mathrm{N}\mathfrak{a}$ and what we want is equivalent to $|\mathfrak{a}/\mathfrak{a}\mathfrak{p}| = |\mathcal{O}_K/\mathfrak{p}|$. The $\mathcal{O}_K$-module $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ is killed by multiplication by elements of $\mathfrak{p}$, so $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ is naturally an $(\mathcal{O}_K/\mathfrak{p})$-vector space. That's the key point. We will show $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ is 1-dimensional over $\mathcal{O}_K/\mathfrak{p}$, so its size is $|\mathcal{O}_K/\mathfrak{p}|$.

Since $\mathfrak{a}\mathfrak{p}$ is a proper subset of $\mathfrak{a}$, there is an $x \in \mathfrak{a}$ with $x \notin \mathfrak{a}\mathfrak{p}$, so $\overline{x} \neq \overline{0}$ in $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$. We *expect*, if $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ is to be 1-dimensional over $\mathcal{O}_K/\mathfrak{p}$, that each nonzero element of $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ is a spanning set over $\mathcal{O}_K/\mathfrak{p}$. Let's verify $\{\overline{x}\}$ is such a set. Since $(x) \subset \mathfrak{a}$ and $(x) \not\subset \mathfrak{a}\mathfrak{p}$, $\mathfrak{a}$ divides (x) but $\mathfrak{a}\mathfrak{p}$ does not divide (x) (containment is equivalent to divisibility). This implies $\gcd((x), \mathfrak{a}\mathfrak{p}) = \mathfrak{a}$, so $\mathfrak{a} = (x) + \mathfrak{a}\mathfrak{p}$ by Corollary 4.5. So for each $\alpha \in \mathfrak{a}$ we have $\alpha = \beta x + \gamma$ where $\beta \in \mathcal{O}_K$ and $\gamma \in \mathfrak{a}\mathfrak{p}$. Thus in $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$, $\overline{\alpha} = \beta \cdot \overline{x}$, which shows $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ is

spanned as an $(\mathcal{O}_K/\mathfrak{p})$-vector space by the single nonzero element $\overline{x}$: the dimension of $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ over $\mathcal{O}_K/\mathfrak{p}$ is 1. Hence $\mathrm{N}(\mathfrak{a}\mathfrak{p}) = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{p}$.

Second proof: We will show $\mathfrak{a}/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{b}$ as $\mathcal{O}_K$-modules, so $[\mathfrak{a} : \mathfrak{a}\mathfrak{b}] = \mathrm{N}\mathfrak{b}$, which implies $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = [\mathcal{O}_K : \mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K : \mathfrak{a}][\mathfrak{a} : \mathfrak{a}\mathfrak{b}] = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}$. By Corollary 4.9, there is a $\mathfrak{c}$ prime to $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{c}$ is principal. Let $\mathfrak{a}\mathfrak{c} = (x)$. Then $(x) + \mathfrak{a}\mathfrak{b} = \mathfrak{a}(\mathfrak{c} + \mathfrak{b}) = \mathfrak{a}(1) = \mathfrak{a}$. Reducing the equation $(x) + \mathfrak{a}\mathfrak{b} = \mathfrak{a}$ modulo $\mathfrak{a}\mathfrak{b}$ shows $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$ is spanned by $\overline{x}$ as an $\mathcal{O}_K$-module. Therefore the map $f\colon \mathcal{O}_K \to \mathfrak{a}/\mathfrak{a}\mathfrak{b}$ given by $\alpha \mapsto \alpha\overline{x} = \overline{\alpha x}$ is $\mathcal{O}_K$-linear, onto and its kernel is $\{\alpha \in \mathcal{O}_K : \alpha x \in \mathfrak{a}\mathfrak{b}\}$. Since

$$\begin{aligned} \alpha x \in \mathfrak{a}\mathfrak{b} &\iff (\alpha)(x) \subset \mathfrak{a}\mathfrak{b} \\ &\iff (\alpha)\mathfrak{a}\mathfrak{c} \subset \mathfrak{a}\mathfrak{b} \\ &\iff (\alpha)\mathfrak{c} \subset \mathfrak{b}, \end{aligned}$$

for α in the kernel of f we have

$$(\alpha) = (\alpha)(1) = (\alpha)(\mathfrak{c} + \mathfrak{b}) = (\alpha)\mathfrak{c} + (\alpha)\mathfrak{b} \subset \mathfrak{b} + \mathfrak{b} = \mathfrak{b},$$

so $\alpha \in \mathfrak{b}$. Hence $\ker f \subset \mathfrak{b}$. The reverse inclusion is easy since for $y \in \mathfrak{b}$, $yx \in \mathfrak{a}\mathfrak{b}$ because $x \in \mathfrak{a}$. □

Remark 7.6. In a domain where all nonzero ideals have finite index, the multiplicativity of the ideal norm (if true) implies unique factorization of ideals. See [3].

Corollary 7.7. *Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$ and p be a prime number. The ideal $\mathfrak{a}$ is divisible by a prime factor of (p) if and only if $\mathrm{N}\mathfrak{a}$ is divisible by p.*

Proof. Write $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ with distinct $\mathfrak{p}_i$'s. Some $\mathfrak{p}_i$ is a factor of (p) if and only if $\mathrm{N}\mathfrak{p}_i$ is a power of p. Since $\mathrm{N}\mathfrak{a}$ is the product of $\mathrm{N}\mathfrak{p}_i^{a_i}$, $p \mid \mathrm{N}\mathfrak{a}$ if and only if some $\mathfrak{p}_i$ has norm a power of p, which is equivalent to $\mathfrak{p}_i \mid (p)$. □

When $K/\mathbf{Q}$ is Galois, with $G = \mathrm{Gal}(K/\mathbf{Q})$, the group G acts on the ideals in $\mathcal{O}_K$ by the natural rule $\sigma(\mathfrak{a}) = \{\sigma(\alpha) : \alpha \in \mathfrak{a}\}$, which is an ideal of $\mathcal{O}_K$. This could be considered a generalization of the Galois action on elements because of how it behaves on principal ideals: $\sigma((\alpha)) = (\sigma(\alpha))$ (check!). The action of Galois groups on ideals has some aspects that are different from their effect on elements: an element of $\mathcal{O}_K$ fixed by G is in $\mathbf{Z}$, but an ideal of $\mathcal{O}_K$ fixed by G need not come from $\mathbf{Z}$, *e.g.*, in $\mathbf{Z}[i]$, $\overline{(1+i)} = (1-i) = (1+i)$ and $(1+i)$ has no generator in $\mathbf{Z}$, and in $\mathbf{Z}[\sqrt{-5}]$, $\overline{(2, 1+\sqrt{-5})} = (2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})$, but $(2, 1+\sqrt{-5})$ has no generating set in $\mathbf{Z}$. Some aspects of the Galois action on elements and ideals are similar. For example, each $\sigma \in G$ defines a ring isomorphism $\mathcal{O}_K/\mathfrak{a} \to \mathcal{O}_K/\sigma(\mathfrak{a})$ by the natural rule $\alpha \bmod \mathfrak{a} \mapsto \sigma(\alpha) \bmod \sigma(\mathfrak{a})$ (why is this well-defined?), so these rings have the same size: $\mathrm{N}(\sigma(\mathfrak{a})) = \mathrm{N}\mathfrak{a}$, which resembles the formula $\mathrm{N}_{K/\mathbf{Q}}(\sigma(\alpha)) = \mathrm{N}(\alpha)$ for elements $\alpha \in K$. The following theorem presents a result similar to the element formula

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha). \tag{7.2}$$

Theorem 7.8. *For a Galois extension $K/\mathbf{Q}$ with Galois group G and nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\prod_{\sigma \in G} \sigma(\mathfrak{a}) = (\mathrm{N}\mathfrak{a})\mathcal{O}_K$.*

The ideal on the right side is not $(\mathrm{N}\mathfrak{a})\mathbf{Z}$, since a product of ideals in $\mathcal{O}_K$ can't become an ideal in $\mathbf{Z}$. Therefore the formula in this theorem is the best[2] ideal-theoretic analogue of (7.2).

[2]Perhaps "most ideal"?

Proof. By unique factorization, both sides of the desired equation

$$\prod_{\sigma\in G}\sigma(\mathfrak{a}) \stackrel{?}{=} (\mathrm{N}\mathfrak{a})\mathcal{O}_K \tag{7.3}$$

are equal if (and only if) a common power of both sides are equal. Let h be the class number of K, so $\mathfrak{a}^h = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. We will check the h-th power of both sides are equal since that reduces the whole task to the case of principal ideals.

It is straightforward to check G acts multiplicatively on ideals: $\sigma(\mathfrak{a}\mathfrak{b}) = \sigma(\mathfrak{a})\sigma(\mathfrak{b})$ for all ideals $\mathfrak{a}$ and $\mathfrak{b}$. Since $\sigma(x\mathcal{O}_K) = \sigma(x)\mathcal{O}_K$, $\sigma(\mathfrak{a})^h = \sigma(\mathfrak{a}^h) = \sigma((\alpha)) = (\sigma(\alpha))$. Therefore

$$\left(\prod_{\sigma\in G}\sigma(\mathfrak{a})\right)^h = \prod_{\sigma\in G}\sigma(\mathfrak{a}^h) = \prod_{\sigma\in G}\sigma(\alpha\mathcal{O}_K) = \prod_{\sigma\in G}(\sigma(\alpha)\mathcal{O}_K) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)\mathcal{O}_K \tag{7.4}$$

since $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \prod_{\sigma\in G}\sigma(\alpha)$.

On the right side of (7.3) the hth power is $((\mathrm{N}\mathfrak{a})\mathcal{O}_K)^h = \mathrm{N}(\mathfrak{a}^h)\mathcal{O}_K = \mathrm{N}((\alpha))\mathcal{O}_K$ since the ideal norm is multiplicative (Theorem 7.5). We have $\mathrm{N}((\alpha)) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$ by Theorem 7.2, so $\mathrm{N}((\alpha))\mathcal{O}_K = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|\mathcal{O}_K = \mathrm{N}_{K/\mathbf{Q}}(\alpha)\mathcal{O}_K$, which matches (7.4). □

Example 7.9. In $\mathbf{Z}[\sqrt{-5}]$, let $\mathfrak{a} = (1+2\sqrt{-5}, 4+\sqrt{-5})$. Here the Galois group is the identity and complex conjugation, so

$$\begin{aligned}\mathfrak{a}\overline{\mathfrak{a}} &= (1+2\sqrt{-5}, 4+\sqrt{-5})(1-2\sqrt{-5}, 4-\sqrt{-5})\\ &= (21, 14+7\sqrt{-5}, 14-7\sqrt{-5}, 21)\\ &= 7(3, 2+\sqrt{-5}, 2-\sqrt{-5})\\ &= 7\mathcal{O}_K\end{aligned}$$

since $(3, 2+\sqrt{-5}, 2-\sqrt{-5})$ contains 3 and $2+\sqrt{-5}+2-\sqrt{-5} = 4$. Thus $(\mathrm{N}\mathfrak{a})\mathcal{O}_K = 7\mathcal{O}_K$, so $\mathrm{N}\mathfrak{a} = 7u$ where $u \in \mathcal{O}_K^\times$. Both $\mathrm{N}\mathfrak{a}$ and 7 are in $\mathbf{Z}^+$, so $u = 1$ and $\mathfrak{a}$ has norm 7.

By manipulating generators, $(1+2\sqrt{-5}, 4+\sqrt{-5}) = (7, 3-\sqrt{-5})$ (check generators on each side are in the ideal on the other side). Let's compute the norm of $\mathfrak{a}$ using these new generators:

$$\begin{aligned}\mathfrak{a}\overline{\mathfrak{a}} &= (7, 3-\sqrt{-5})(7, 3+\sqrt{-5})\\ &= (49, 21+7\sqrt{-5}, 21-7\sqrt{-5}, 14)\\ &= 7(7, 3+\sqrt{-5}, 3-\sqrt{-5})\\ &= 7\mathcal{O}_K\end{aligned}$$

since the ideal contains 7 and $3+\sqrt{-5}+3-\sqrt{-5} = 6$.

Returning to the general case, where $K/\mathbf{Q}$ need not be Galois, the next theorem generalizes Theorem 7.2 from principal ideals to all (nonzero) ideals in $\mathcal{O}_K$ by describing the norm of an ideal using the ring-theoretic norms of the elements in the ideal.

Theorem 7.10. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$. The positive integer $\mathrm{N}\mathfrak{a}$ is the greatest common divisor of the integers $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ for all $\alpha \in \mathfrak{a}$.*

The gcd here is being taken over norms of *all* elements of $\mathfrak{a}$, not just norms of a set generators of the ideal: while $\mathrm{N}((\alpha)) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$, for an ideal described with more than one generator, say $\mathfrak{a} = (\alpha, \beta)$, $\mathrm{N}\mathfrak{a}$ need not be the gcd of $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ and $\mathrm{N}_{K/\mathbf{Q}}(\beta)$. In Example 7.9, where $\mathfrak{a} = (1+2\sqrt{-5}, 4+\sqrt{-5})$, $1+2\sqrt{-5}$ and $4+\sqrt{-5}$ have norm 21 but $\mathrm{N}\mathfrak{a}$ is 7.

More simply, in $\mathbf{Z}[i]$ the ideal $(1+2i, 1-2i)$ is (1) so it has norm 1, but the Gaussian integers $1+2i$ and $1-2i$ have norm 5.

Proof. If $\mathfrak{a} = (1)$ then the result is clear, so we take $\mathfrak{a} \neq (1)$.

Let d be the gcd of all $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ as α runs over $\mathfrak{a}$. For nonzero $\alpha \in \mathfrak{a}$, $\mathfrak{a} \mid (\alpha)$ so $\mathrm{N}\mathfrak{a} \mid \mathrm{N}((\alpha))$, so $\mathrm{N}\mathfrak{a} \mid \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ by Theorem 7.2. Therefore $\mathrm{N}\mathfrak{a} \mid d$, so each prime power dividing $\mathrm{N}\mathfrak{a}$ also divides d. To show $\mathrm{N}\mathfrak{a} = d$ we will show for every prime number p that the highest power of p dividing $\mathrm{N}\mathfrak{a}$ is also the highest power of p dividing $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ for some $\alpha \in \mathfrak{a}$ (depending on p). Since $d \mid \mathrm{N}_{K/\mathbf{Q}}(\alpha)$, it follows that the highest power of p dividing $\mathrm{N}\mathfrak{a}$ and d agree (why?). Varying this over all primes implies $\mathrm{N}\mathfrak{a} = d$.

In $\mathcal{O}_K$, let $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with distinct prime ideals $\mathfrak{p}_i$ and $e_i \geq 1$. Write $\mathfrak{a} = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r}\mathfrak{b}$ where $c_i \geq 0$ and $\mathfrak{b}$ is not divisible by the ideals $\mathfrak{p}_i$. Since the $\mathfrak{p}_i$'s are all the prime ideals dividing (p), $\mathrm{N}\mathfrak{b}$ is not divisible by p. Writing $\mathrm{N}\mathfrak{p}_i = p^{f_i}$, $\mathrm{N}\mathfrak{a} = p^{c_1 f_1 + \cdots + c_r f_r}\,\mathrm{N}\mathfrak{b}$, so the multiplicity (*i.e.*, exponent) of p in $\mathrm{N}\mathfrak{a}$ is $c_1 f_1 + \cdots + c_r f_r$. We need to find $\alpha \in \mathfrak{a}$ such that $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ has the same p-power divisibility.

By Remark 4.10, there is an $\alpha \in \mathcal{O}_K - \{0\}$ such that (α) is divisible by $\mathfrak{p}_i^{c_i}$ but not $\mathfrak{p}_i^{c_i+1}$ for all i and is also divisible by $\mathfrak{b}$. It follows that (α) is divisible by $\mathfrak{a}$, so $\alpha \in \mathfrak{a}$, and also $\mathrm{N}((\alpha)) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$ is divisible by p with multiplicity $\sum c_i f_i$. □

Remark 7.11. Theorem 7.10 is not an algorithmic formula for computing the norm of an ideal, since it doesn't provide a finite list of elements in the ideal and calculations to make on them that would compute that norm. If you are given an actual nonzero ideal $\mathfrak{a}$ in an actual ring of integers $\mathcal{O}_K$ and you can compute bases for $\mathcal{O}_K$ and $\mathfrak{a}$ as $\mathbf{Z}$-modules, then the absolute value of the determinant of the matrix expressing a $\mathbf{Z}$-basis of $\mathfrak{a}$ in terms of a $\mathbf{Z}$-basis of $\mathcal{O}_K$ is the index $[\mathcal{O}_K : \mathfrak{a}]$, so this is $\mathrm{N}\mathfrak{a}$.

Since the ideal norm is multiplicative, it extends to a multiplicative function on all fractional ideals of K in a unique way. If I is a fractional ideal, $\mathrm{N}(I) \in \mathbf{Q}^\times$, so there is not a combinatorial meaning for the norm of I (but see Theorem 7.12). When I is a principal fractional ideal, its ideal norm coincides with the absolute value of the norm of a generator of I: $\mathrm{N}(x\mathcal{O}_K) = |\mathrm{N}_{K/\mathbf{Q}}(x)|$ for all $x \in K^\times$. This is proved by writing $x = y/z$ for y and z in $\mathcal{O}_K - \{0\}$, so $(x) = (y)(z)^{-1}$ and now apply the ideal norm to both sides and use Theorem 7.2.

Theorem 7.12. *For fractional ideals $J \subset I$, $[I : J] = \mathrm{N}(J)/\mathrm{N}(I)$.*

Proof. Pick $d \in \mathcal{O}_K - \{0\}$ such that dI and dJ are both in $\mathcal{O}_K$. Then $dJ \subset dI \subset \mathcal{O}_K$, and $dI/dJ \cong I/J$ as $\mathcal{O}_K$-modules, so

$$[I : J] = [dI : dJ] = \frac{[\mathcal{O}_K : dJ]}{[\mathcal{O}_K : dI]} = \frac{\mathrm{N}(dJ)}{\mathrm{N}(dI)} = \frac{\mathrm{N}((d))\,\mathrm{N}(J)}{\mathrm{N}((d))\,\mathrm{N}(I)} = \frac{\mathrm{N}(J)}{\mathrm{N}(I)}.$$

□

Example 7.13. For each nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$, we have $\mathcal{O}_K \subset \mathfrak{a}^{-1}$ so $[\mathfrak{a}^{-1} : \mathcal{O}_K] = \mathrm{N}(\mathcal{O}_K)/\mathrm{N}(\mathfrak{a}^{-1}) = 1/(1/\mathrm{N}\mathfrak{a}) = \mathrm{N}\mathfrak{a} = [\mathcal{O}_K : \mathfrak{a}]$. More generally, if $J \subset I$ are fractional ideals then Theorem 7.12 shows $[I : J] = [IM : JM]$ for every fractional ideal M.

Using the ideal norm, especially its multiplicativity, many concepts from elementary number theory for $\mathbf{Z}$ can be carried over to $\mathcal{O}_K$. For example, since $\mathcal{O}_K/\mathfrak{p}$ is a field of size $\mathrm{N}\mathfrak{p}$, we have an analogue of Fermat's little theorem:

$$\alpha \not\equiv 0 \bmod \mathfrak{p} \Longrightarrow \alpha^{\mathrm{N}\mathfrak{p}-1} \equiv 1 \bmod \mathfrak{p}.$$

Define $\varphi_K(\mathfrak{a}) = |(\mathcal{O}_K/\mathfrak{a})^\times|$, which generalizes the Euler function $\varphi(m) = |(\mathbf{Z}/m\mathbf{Z})^\times|$. The standard formula

$$\varphi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right).$$

for the classical φ-function has an $\mathcal{O}_K$-analogue:

$$\varphi_K(\mathfrak{a}) = \mathrm{N}\mathfrak{a}\prod_{\mathfrak{p}|\mathfrak{a}}\left(1 - \frac{1}{\mathrm{N}\mathfrak{p}}\right),$$

where the product runs over the prime ideals dividing $\mathfrak{a}$. The proof is left to the reader.

There is an important difference between the groups $(\mathbf{Z}/m\mathbf{Z})^\times$ and $(\mathcal{O}_K/\mathfrak{a})^\times$. When $m = p^k$ is an odd prime power the group $(\mathbf{Z}/p^k\mathbf{Z})^\times$ is cyclic for all $k \geq 1$. However, when $\mathfrak{a} = \mathfrak{p}^k$ is a prime power ideal and $k > 1$, the group $(\mathcal{O}_K/\mathfrak{p}^k)^\times$ is often not cyclic. For example, 3 is prime in $\mathbf{Z}[i]$ and $(\mathbf{Z}[i]/3^k)^\times$ is not cyclic when $k > 1$. (When $k = 1$, $(\mathcal{O}_K/\mathfrak{p}^k)^\times = (\mathcal{O}_K/\mathfrak{p})^\times$ is cyclic since this is the multiplicative group of a finite field.)

In a different direction, the Riemann zeta-function

$$\zeta(s) = \sum_{n\geq 1}\frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s}$$

generalizes to the zeta-function of K:

$$\zeta_K(s) = \sum_{\mathfrak{a}}\frac{1}{\mathrm{N}\mathfrak{a}^s} = \prod_{\mathfrak{p}}\frac{1}{1 - 1/\mathrm{N}\mathfrak{p}^s},$$

where the series runs over nonzero ideals of $\mathcal{O}_K$ and the product runs over the nonzero prime ideals. The series and product are absolutely convergent for $\mathrm{Re}(s) > 1$. Unlike in $\mathbf{Z}^+$, some positive integers may not be the norm of an ideal in $\mathcal{O}_K$ and other positive integers may be the norm of more than one ideal in $\mathcal{O}_K$. For example, the expansion of $\zeta_{\mathbf{Q}(i)}(s)$ as a series for $\mathrm{Re}(s) > 1$ is

$$1 + \frac{1}{2^s} + \frac{1}{4^s} + \frac{2}{5^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{2}{10^s} + \cdots + \frac{4}{65^s} + \cdots,$$

where there is no term with $1/3^s$ since no ideal in $\mathbf{Z}[i]$ has norm 3 and the term with $1/5^s$ has coefficient 2 since there are two ideals in $\mathbf{Z}[i]$ with norm 5. The equality of the series and product for $\zeta_K(s)$ comes from unique factorization of ideals and the multiplicativity of the ideal norm. The study of distribution of prime numbers involves analytic properties of $\zeta(s)$, and similarly studying the distribution of prime ideals of $\mathcal{O}_K$ uses analytic properties of $\zeta_K(s)$. There is an analytic continuation of $\zeta_K(s)$ to the whole complex plane except for a simple pole at $s = 1$, just like $\zeta(s)$.

8. Analogues for Orders

Let K be a number field and $\mathcal{O}$ be an order in K. That is, $\mathcal{O}$ is a subring of K that is finitely generated as a $\mathbf{Z}$-module and contains a $\mathbf{Q}$-basis of K. Concretely, orders in K are the subrings of $\mathcal{O}_K$ with finite index. A typical example is $\mathbf{Z}[\alpha]$ where α is an algebraic integer of K such that $K = \mathbf{Q}(\alpha)$ and $\mathbf{Z} + \mathfrak{a}$ where $\mathfrak{a}$ is a nonzero ideal in $\mathcal{O}_K$. Are the arguments we developed to prove unique factorization of ideals in $\mathcal{O}_K$ valid if we apply them to an order $\mathcal{O}$ when $\mathcal{O} \neq \mathcal{O}_K$?

To start off, note that orders in K share several features with $\mathcal{O}_K$:

(1) each order in K has fraction field K,

(2) each order has a $\mathbf{Z}$-basis and that basis can be chosen to include 1,
(3) all nonzero ideals in an order are finitely generated as $\mathbf{Z}$-modules (even free with rank $n = [K : \mathbf{Q}]$),
(4) all nonzero ideals in an order have finite index in the order,
(5) all nonzero prime ideals in an order are maximal,
(6) for $x \neq 0$ in an order $\mathcal{O}$, the index $[\mathcal{O} : x\mathcal{O}]$ equals $|\mathrm{N}_{K/\mathbf{Q}}(x)|$,
(7) for each x in an order $\mathcal{O}$, $x \mid \mathrm{N}_{K/\mathbf{Q}}(x)$ in $\mathbf{Z}[x] \subset \mathcal{O}$.
(8) the units of an order $\mathcal{O}$ are $\{u \in \mathcal{O} : \mathrm{N}_{K/\mathbf{Q}}(u) = \pm 1\}$,

Properties 1, 3, 4, and 5 are what we used about $\mathcal{O}_K$ in the results up through and including Theorem 3.2(1), so those results apply to all orders and not just to $\mathcal{O}_K$. For instance, define a fractional $\mathcal{O}$-ideal as a nonzero $\mathcal{O}$-module in K with a common denominator from $\mathcal{O} - \{0\}$. Then fractional $\mathcal{O}$-ideals are the same thing as nonzero finitely generated $\mathcal{O}$-modules in K (analogue of Theorem 2.3(4)) and the only possible inverse of a fractional $\mathcal{O}$-ideal I is $\widetilde{I} = \{x \in K : xI \subset \mathcal{O}\}$, which is always a fractional $\mathcal{O}$-ideal (analogue of Theorem 2.7). Each nonzero ideal in $\mathcal{O}$ contains a product of nonzero prime ideals (analogue of Lemma 3.1). When $\mathfrak{p}$ is a nonzero prime ideal in $\mathcal{O}$, $\mathcal{O} \subset \widetilde{\mathfrak{p}}$ and this containment is strict (analogue of Theorem 3.2(1)).

When we try to prove Theorem 3.2(2) with $\mathcal{O}$ in place of $\mathcal{O}_K$, we run into a problem! For $x \in \widetilde{\mathfrak{p}} - \mathcal{O}$, $x\mathfrak{p} + \mathfrak{p}$ is either $\mathfrak{p}$ or $\mathcal{O}$. If we try to show the first option is not true by contradiction, then we want to show from $x\mathfrak{p} \subset \mathfrak{p}$ that $x \in \mathcal{O}$. Since $\mathfrak{p}$ is a finitely generated $\mathbf{Z}$-module, when $x\mathfrak{p} \subset \mathfrak{p}$ we know x is integral over $\mathbf{Z}$, so $x \in \mathcal{O}_K$, but there is no reason to expect $x \in \mathcal{O}$ (the integral closure of $\mathbf{Z}$ in K is $\mathcal{O}_K$, not $\mathcal{O}$), so we can't get a contradiction.

The three corollaries of Theorem 3.2 for $\mathcal{O}_K$ are formal consequences of $\mathfrak{p}\widetilde{\mathfrak{p}} = (1)$: they would apply to every nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}$ such that $\mathfrak{p}\widetilde{\mathfrak{p}} = \mathcal{O}$ (using the same proofs). The proof of unique prime ideal factorization in $\mathcal{O}_K$ (Theorem 3.6) would also apply to an order whose nonzero prime ideals all satisfy Theorem 3.2(2). Therefore Theorem 3.2(2), the invertibility of all nonzero prime ideals, is really the key step in our proof of unique prime ideal factorization in $\mathcal{O}_K$.

The following theorem implies that every order of K that is smaller than the maximal order $\mathcal{O}_K$ doesn't satisfy Theorem 3.2(2) for at least one nonzero prime ideal.

Theorem 8.1. *If a domain has cancellation of ideals, i.e., always $\mathfrak{ac} = \mathfrak{bc}$ implies $\mathfrak{a} = \mathfrak{b}$ when $\mathfrak{c} \neq (0)$, then the domain is integrally closed.*

Proof. Let A be a domain with cancellation of ideals. Suppose an x in the fraction field of A is integral over A. We want to show x is in A. Write $x = a/b$ where a and b are in A with $b \neq 0$. Since x is integral over A,

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$$

with $n \geq 1$ and $c_i \in A$. Let $R = A[x] = A + Ax + \cdots + Ax^{n-1}$. This is a ring and a nonzero A-module in the fraction field of A. Since x has denominator b, by the definition of R we have $b^{n-1}R \subset A$, so R has common denominator b^{n-1}. Therefore

$$\mathfrak{a} := b^{n-1}R = Ab^{n-1} + Ab^{n-2}a + \cdots + Aa^{n-1}$$

is a nonzero A-module in A, *i.e.*, $\mathfrak{a}$ is a nonzero ideal in A. Since R is a ring, $R^2 = R$, so $\mathfrak{a}^2 = b^{2(n-1)}R^2 = b^{n-1}b^{n-1}R = (b)^{n-1}\mathfrak{a}$. Therefore by cancellation of nonzero ideals in A, $\mathfrak{a} = (b)^{n-1} = b^{n-1}A$, so $b^{n-1}R = b^{n-1}A$. This implies $R = A$, so $x \in R = A$. □

A domain with unique factorization of ideals will have cancellation of ideals and thus will be integrally closed. Therefore, since no order in a number field is integrally closed except for the maximal order (the full ring of integers), non-maximal orders do not have unique factorization of ideals: they must contain a non-invertible prime ideal $\mathfrak{p} \neq (0)$. We give next a basic example of this.

Example 8.2. Let K be an number field field with degree $n > 1$ and p be a prime number. Set

$$\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K.$$

We will show $\mathcal{O}$ has a nonzero ideal with no prime ideal factorization in $\mathcal{O}$ and $\mathcal{O}$ has an explicit nonzero prime ideal that is not invertible.

Set

$$\mathfrak{b} = p\mathcal{O} = p\mathbf{Z} + p^2\mathcal{O}_K, \quad \mathfrak{p} = p\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K,$$

so $\mathfrak{b} \subset \mathfrak{p} \subset \mathcal{O}$. Note $\mathfrak{p}$ is an ideal in both $\mathcal{O}$ and $\mathcal{O}_K$. We will show

(1) the chain of ideals has indices as indicated:

$$\mathfrak{p}^2 \overset{p}{\subset} \mathfrak{b} \overset{p^{n-1}}{\subset} \mathfrak{p} \overset{p}{\subset} \mathcal{O} \overset{p^{n-1}}{\subset} \mathcal{O}_K,$$

(2) $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$ that is not invertible as a fractional $\mathcal{O}$-ideal,
(3) $\mathfrak{b}\mathfrak{p} = \mathfrak{p}^2$,
(4) $\mathfrak{b}$ is not a product of prime ideals in $\mathcal{O}$,
(5) $\mathfrak{p}$ does not divide $\mathfrak{b}$.

(1): Let $\{1, e_2, \ldots, e_n\}$ be a $\mathbf{Z}$-basis of $\mathcal{O}_K$, so

$$\begin{aligned}
\mathcal{O}_K &= \mathbf{Z} \oplus \mathbf{Z}e_2 \oplus \cdots \oplus \mathbf{Z}e_n, \\
\mathcal{O} &= \mathbf{Z} \oplus \mathbf{Z}pe_2 \oplus \cdots \oplus \mathbf{Z}pe_n, \\
p\mathcal{O}_K &= \mathbf{Z}p \oplus \mathbf{Z}pe_2 \oplus \cdots \oplus \mathbf{Z}pe_n, \\
p\mathcal{O} &= \mathbf{Z}p \oplus \mathbf{Z}p^2e_2 \oplus \cdots \oplus \mathbf{Z}p^2e_n, \\
p^2\mathcal{O}_K &= \mathbf{Z}p^2 \oplus \mathbf{Z}p^2e_2 \oplus \cdots \oplus \mathbf{Z}p^2e_n.
\end{aligned}$$

Since $\mathfrak{p}^2 = (p\mathcal{O}_K)^2 = p^2\mathcal{O}_K$, these direct sums explain all the desired ideal indices. The chain of strict inclusions $\mathfrak{p}^2 \subsetneqq \mathfrak{b} \subsetneqq \mathfrak{p}$ in $\mathcal{O}$ would be impossible in a Dedekind domain.

We can see explicitly in this example that the ideal norm in $\mathcal{O}$ is not multiplicative: $[\mathcal{O} : \mathfrak{p}^2] = p^{n+1}$ and $[\mathcal{O} : \mathfrak{p}]^2 = p^2$.

(2): Since $\mathcal{O}/\mathfrak{p} = (\mathbf{Z} + p\mathcal{O}_K)/p\mathcal{O}_K \cong \mathbf{Z}/(p\mathcal{O}_K \cap \mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$, $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$. If $\mathfrak{p}$ had an inverse as a fractional $\mathcal{O}$-ideal then $\{x \in K : x\mathfrak{p} \subset \mathfrak{p}\}$ would equal $\mathcal{O}$. But $\mathfrak{p}$ is an ideal in $\mathcal{O}_K$ and thus invertible as a fractional $\mathcal{O}_K$-ideal, so $\{x \in K : x\mathfrak{p} \subset \mathfrak{p}\}$ actually equals $\mathcal{O}_K$. In particular, although $\mathfrak{p}$ is principal as an ideal in $\mathcal{O}_K$, it is not principal as an ideal in $\mathcal{O}$ since nonzero principal ideals are always invertible. (The ideals $\mathfrak{p} = p\mathcal{O}_K$ and $p\mathcal{O}$ in $\mathcal{O}$ are not the same; the second one is principal in $\mathcal{O}$.)

(3): This a computation: $\mathfrak{b}\mathfrak{p} = p\mathcal{O}p\mathcal{O}_K = p^2\mathcal{O}_K = \mathfrak{p}^2$.

(4): Assume $\mathfrak{b}$ is a product of prime ideals. Since $\mathfrak{p}^2 = \mathfrak{b}\mathfrak{p} \subset \mathfrak{b}$, if a nonzero prime ideal $\mathfrak{q}$ divides $\mathfrak{b}$ then $\mathfrak{q} \supset \mathfrak{b} \supset \mathfrak{p}^2$, so $\mathfrak{q} = \mathfrak{p}$ by the analogue of Corollary 1.5 for orders. Therefore $\mathfrak{b}$ must be a power of $\mathfrak{p}$. From (1), $\mathfrak{b}$ lies strictly between $\mathfrak{p}$ and $\mathfrak{p}^2$, and $\mathfrak{p}^k \subset \mathfrak{p}^2$ for $k \geq 3$, so $\mathfrak{b}$ is not a power of $\mathfrak{p}$.

(5): Assume $\mathfrak{b} = \mathfrak{p}\mathfrak{b}'$. Since $\mathfrak{b} \neq \mathfrak{p}$, $\mathfrak{b}' \neq (1)$. Therefore $\mathfrak{b}' \subset \mathfrak{q}$ for some maximal ideal $\mathfrak{q}$ of $\mathcal{O}$. Then $\mathfrak{q} \supset \mathfrak{b}' \supset \mathfrak{p}\mathfrak{b}' = \mathfrak{b} \supset \mathfrak{p}^2$, so $\mathfrak{q} = \mathfrak{p}$. Thus $\mathfrak{b}' \subset \mathfrak{p}$, so we get $\mathfrak{b} = \mathfrak{p}\mathfrak{b}' \subset \mathfrak{p}^2$. However, $\mathfrak{p}^2$ is a proper subset of $\mathfrak{b}$, so we have a contradiction.

This shows containment of ideals does not imply divisibility ($\mathfrak{p}$ contains $\mathfrak{b}$ but $\mathfrak{p}$ does not divide $\mathfrak{b}$).

Example 8.3. A non-maximal order in a number field can't be a PID because a PID is integrally closed. We can also directly exhibit an example of a non-principal ideal in every non-maximal order. If K is a number field and $\mathcal{O} \subset \mathcal{O}_K$ is a non-maximal order, let $m = [\mathcal{O}_K : \mathcal{O}] \geq 2$. Then $m\mathcal{O}_K \subset \mathcal{O}$ and $m\mathcal{O}_K$ is an ideal of $\mathcal{O}$ (it's an $\mathcal{O}$-module inside of $\mathcal{O}$) but it is not a principal ideal in $\mathcal{O}$: if $m\mathcal{O}_K = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{O}$ then for all $x \in \mathcal{O}_K$ we have $x\alpha \in xm\mathcal{O}_K \subset m\mathcal{O}_K = \alpha\mathcal{O}$, so $x \in \mathcal{O}$. Thus $\mathcal{O}_K \subset \mathcal{O}$. But $\mathcal{O}$ is a proper subset of $\mathcal{O}_K$, so we have a contradiction.

Example 8.4. In a number field K with degree n, all nonzero ideals in an order of K have at most n generators since they have n generators as a $\mathbf{Z}$-module. We showed in Theorem 4.11 that each nonzero ideal in $\mathcal{O}_K$ has at most 2 generators. When $n \geq 3$ we'll construct orders $\mathcal{O}$ in K that have an ideal with a minimal generating set (as an ideal of $\mathcal{O}$) of size n.

For $c \geq 2$, set $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$ and $\mathfrak{a} = c\mathcal{O}_K$. Then $\mathfrak{a}$ is an ideal in $\mathcal{O}$ since it's an ideal of $\mathcal{O}_K$ inside the subring $\mathcal{O}$. Since $\mathfrak{a} \cong \mathbf{Z}^n$ as an additive group, 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 $r \geq n$.

Similar reasoning works if we start with $c \geq 2$ and an order R (not just $R = \mathcal{O}_K$) and use $\mathcal{O} = \mathbf{Z} + cR$. The ideal $\mathfrak{a} = cR$ in $\mathcal{O}$ has index c,[3] and since $R \cong \mathbf{Z}^n$ as an abelian group we have $\mathfrak{a}/\mathfrak{a}^2 = cR/c^2R \cong R/cR \cong (\mathbf{Z}/c\mathbf{Z})^n$ as abelian groups, so every generating set of $\mathfrak{a}$ as an ideal in $\mathcal{O}$ has at least n elements.

Remark 8.5. For the order $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$ of Example 8.2, $p\mathcal{O}_K$ is an ideal in both $\mathcal{O}_K$ and $\mathcal{O}$, so an ideal for one order can also be an ideal for another order. This can lead to different meanings for $\widetilde{I}$. Consider $I = p\mathcal{O}_K$. Viewed in $\mathcal{O}_K$ and $\mathcal{O}$ respectively, we have

$$\widetilde{I} = \{\alpha \in K : \alpha I \subset \mathcal{O}_K\}, \quad \widetilde{I} = \{\alpha \in K : \alpha I \subset \mathcal{O}\},$$

and these are not the same. The first set is $(1/p)\mathcal{O}_K$ (since $I = p\mathcal{O}_K$ is a principal ideal in $\mathcal{O}_K$), while the second set is $\mathcal{O}_K$ ($\mathcal{O}_K \subset \widetilde{I} \subset (1/p)\mathcal{O}$, $[(1/p)\mathcal{O} : \mathcal{O}_K] = p$, and $1/p \notin \widetilde{I}$, so $\widetilde{I}$ must be $\mathcal{O}_K$). This ambiguity in the meaning of $\widetilde{I}$ won't lead to confusion since we're not going to be dealing with more than one order at a time.

Theorem 8.6. *For each order $\mathcal{O}$ in a number field K, all but finitely many nonzero prime ideals in $\mathcal{O}$ are invertible.*

[3]There is a $\mathbf{Z}$-basis of R that includes 1, so $R = \mathbf{Z} \oplus \bigoplus_{i=2}^n \mathbf{Z}e_i$. Then $\mathcal{O} = \mathbf{Z} + cR = \mathbf{Z} \oplus \bigoplus_{i=2}^n \mathbf{Z}ce_i$, so $[R : \mathcal{O}] = c^{n-1}$. Thus $[\mathcal{O} : cR] = [R : cR]/[R : \mathcal{O}] = c^n/c^{n-1} = c$.

Proof. Both $\mathcal{O}_K$ and $\mathcal{O}$ are finite free $\mathbf{Z}$-modules with the same rank, so $\mathcal{O}_K/\mathcal{O}$ is finite. Choose $m \in \mathbf{Z}^+$ such that $m\mathcal{O}_K \subset \mathcal{O}$, such as the index $[\mathcal{O}_K : \mathcal{O}]$. The ideal $(m) = m\mathcal{O}$ contains a product of prime ideals in $\mathcal{O}$, say $(m) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ (analogue of Lemma 3.1 for $\mathcal{O}$). We will show each nonzero prime ideal other than $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ is invertible. (When $\mathcal{O} = \mathcal{O}_K$ we can use $m = 1$ and this recovers the fact that all nonzero primes in $\mathcal{O}_K$ are invertible.)

A prime ideal of $\mathcal{O}$ that contains (m) must be one of the $\mathfrak{p}_i$'s (analogue of Corollary 1.5 for $\mathcal{O}$). Let $\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$, so $\mathfrak{p} \not\supset (m)$. Therefore $\mathfrak{p} + (m) = \mathcal{O}$ by maximality of $\mathfrak{p}$. Write $\pi + mb = 1$ for some $\pi \in \mathfrak{p}$ and $b \in \mathcal{O}$.

Choose $x \in \widetilde{\mathfrak{p}} - \mathcal{O}$ (analogue of Theorem 3.2(1) for $\mathcal{O}$). Then $\mathfrak{p} \subset \mathfrak{p} + x\mathfrak{p} \subset \mathcal{O}$, so $\mathfrak{p} + x\mathfrak{p}$ is either $\mathfrak{p}$ or $\mathcal{O}$. If the second option occurs then $\mathfrak{p}(\mathcal{O} + x\mathcal{O}) = \mathcal{O}$ and $\mathfrak{p}$ is invertible. That's what we want. To eliminate the first option, we argue by contradiction. Suppose $\mathfrak{p} + x\mathfrak{p} = \mathfrak{p}$, so $x\mathfrak{p} \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a finitely generated $\mathbf{Z}$-module, this inclusion implies $x \in \mathcal{O}_K$. Write $x = x \cdot 1 = x\pi + xmb$. Since $mx \in m\mathcal{O}_K \subset \mathcal{O}$, $xmb \in \mathcal{O}$. The product $x\pi$ is in $\mathfrak{p}\widetilde{\mathfrak{p}}$, which is also in $\mathcal{O}$ by the definition of $\widetilde{\mathfrak{p}}$. Thus $x = x\pi + xmb$ is in $\mathcal{O}$. This is a contradiction. □

Example 8.7. Returning to Example 8.2, where $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$ for a prime p, we show every prime ideal of $\mathcal{O}$ except for $\mathfrak{p}$ is invertible. Obviously $p\mathcal{O}_K \subset \mathcal{O}$, so we can take $m = p$ in Theorem 8.6. The ideal $m\mathcal{O} = p\mathcal{O} = \mathfrak{b}$ has $\mathfrak{b} \supset \mathfrak{p}^2$ where $\mathfrak{p} = p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}$, so the only prime that contains $p\mathcal{O}$ is $\mathfrak{p}$. This means every prime in $\mathcal{O}$ other than $\mathfrak{p}$ is invertible. In particular, taking $K = \mathbf{Q}(i)$ and $p = 2$, every prime ideal of $\mathbf{Z}[2i] = \mathbf{Z} + 2\mathbf{Z}[i]$ is invertible except perhaps for $\mathfrak{p} := 2\mathbf{Z}[i]$ (which is not invertible as a $\mathbf{Z}[2i]$-module since $\{x \in \mathbf{Q}(i) : x\mathfrak{p} \subset \mathfrak{p}\}$ is $\mathbf{Z}[i]$ rather than $\mathbf{Z}[2i]$).

Theorem 8.6 is analogous to the fact that a plane algebraic curve is smooth at all but finitely many points.

Although unique prime ideal factorization is false in a non-maximal order, there is a meaningful substitute. Rather than use products of prime ideals in $\mathcal{O}$, we will use filtrations of ideals having simple successive quotients as $\mathcal{O}$-modules.

When passing from finite abelian groups to general finite groups, the use of direct products to decompose a group is replaced with the idea of a normal series (an increasing tower of subgroups, each normal in the next, starting at the identity and ending at the whole group). The Jordan–Hölder theorem guarantees that when a normal series for a finite group has simple quotients (the normal series is then called a composition series), those simple quotients are unique up to isomorphism and multiplicity. In the setting of orders in a number field, we will use the Jordan–Hölder theorem for modules to get a replacement for unique factorization of ideals.

Theorem 8.8 (Jordan-Hölder)**.** *Let M be a module over a commutative ring R and assume it admits a filtration*

$$M = M_0 \supset M_1 \supset \cdots \supset M_k = \{0\}$$

where each quotient module M_i/M_{i+1} is simple. Then each filtration

$$M = M_0' \supset M_1' \supset \cdots \supset M_\ell' = \{0\}$$

where M_i'/M_{i+1}' is simple has $k = \ell$ and there is some permutation $\pi \in S_k$ such that $M_i/M_{i+1} \cong M_{\pi(i)}'/M_{\pi(i)+1}'$ for all i.

This is proved in the same way as the Jordan-Hölder theorem for groups. A finite chain of submodules M_i with M_i/M_{i+1} simple is called a Jordan-Hölder filtration (or composition series) for M.

Theorem 8.9. *Let $\mathcal{O}$ be an order in a number field. For a nonzero proper ideal $\mathfrak{b} \subset \mathcal{O}$, there is a descending series of ideals*

$$\mathcal{O} = \mathfrak{b}_0 \supset \mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_{\ell-1} \supset \mathfrak{b}_\ell = \mathfrak{b} \tag{8.1}$$

such that each $\mathfrak{b}_i/\mathfrak{b}_{i+1}$ is a simple $\mathcal{O}$-module.

For $0 \leq i \leq \ell - 1$, $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathcal{O}/\mathfrak{p}_i$ as $\mathcal{O}$-modules for a unique nonzero prime ideal $\mathfrak{p}_i$ in $\mathcal{O}$. The $\mathfrak{p}_i$'s are the nonzero prime ideals of $\mathcal{O}$ that contain $\mathfrak{b}$ and for each prime $\mathfrak{p} \supset \mathfrak{b}$ the number of $\mathfrak{p}_i$'s equal to $\mathfrak{p}$ is independent of the choice of series (8.1) having simple quotients. Moreover, $[\mathcal{O} : \mathfrak{b}] = \prod_{i=0}^{\ell-1} [\mathcal{O} : \mathfrak{p}_i]$.

Proof. Since $\mathcal{O}/\mathfrak{b}$ is finite it has a composition series as a $\mathcal{O}$-module:

$$\mathcal{O}/\mathfrak{b} = M_0 \supset M_1 \supset \cdots \supset M_\ell = \{0\},$$

where each M_i/M_{i+1} is a simple $\mathcal{O}$-module. Since the M_i's are submodules of $\mathcal{O}/\mathfrak{b}$, $M_i = \mathfrak{b}_i/\mathfrak{b}$ for an ideal $\mathfrak{b}_i$, so $\mathfrak{b}_i \supset \mathfrak{b}_{i+1}$ and $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong M_i/M_{i+1}$ is a simple $\mathcal{O}$-module. The descending chain of ideals $\mathfrak{b}_i$ is a series of the form (8.1).

A simple $\mathcal{O}$-module is isomorphic *as an $\mathcal{O}$-module* to $\mathcal{O}/\mathfrak{p}$ for a unique nonzero prime ideal $\mathfrak{p}$. Indeed, if M is a simple $\mathcal{O}$-module, pick $x_0 \neq 0$ in M. Then $\mathcal{O}x_0$ is a nonzero submodule of M, so by simplicity $M = \mathcal{O}x_0$. We can map $\mathcal{O}$ onto M by $b \mapsto bx_0$. This is $\mathcal{O}$-linear and surjective. Denote its kernel as $\mathfrak{p}$, so $\mathfrak{p}$ is an ideal in $\mathcal{O}$ and $\mathcal{O}/\mathfrak{p} \cong M$ as $\mathcal{O}$-modules. Then $\mathcal{O}/\mathfrak{p}$ is a simple $\mathcal{O}$-module, so $\mathfrak{p}$ must be maximal, since an intermediate ideal $\mathfrak{p} \subset \mathfrak{a} \subset \mathcal{O}$ yields a nonzero proper $\mathcal{O}$-submodule $\mathfrak{a}/\mathfrak{p} \subset \mathcal{O}/\mathfrak{p}$. Intrinsically, $\mathfrak{p} = \mathrm{Ann}_{\mathcal{O}}(M)$ since $\mathfrak{p} = \mathrm{Ann}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p})$ and isomorphic $\mathcal{O}$-modules have *equal* annihilators. Thus, when we write $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathcal{O}/\mathfrak{p}_i$ as $\mathcal{O}$-modules, there is one choice for $\mathfrak{p}_i$: the annihilator ideal $\mathrm{Ann}_{\mathcal{O}}(\mathfrak{b}_i/\mathfrak{b}_{i+1})$.

Since $\mathfrak{p}_i = \mathrm{Ann}_{\mathcal{O}}(\mathfrak{b}_i/\mathfrak{b}_{i+1})$ and $\mathfrak{b}_{i+1}$ kills $\mathfrak{b}_i/\mathfrak{b}_{i+1}$, $\mathfrak{b}_{i+1} \subset \mathfrak{p}_i$. Therefore for $0 \leq i \leq \ell - 1$, $\mathfrak{p}_i \supset \mathfrak{b}_{i+1} \supset \mathfrak{b}_\ell = \mathfrak{b}$, so *every* $\mathfrak{p}_i$ *contains* $\mathfrak{b}$. To prove that each prime ideal containing $\mathfrak{b}$ is some $\mathfrak{p}_i$, we note that $\mathfrak{p}_i\mathfrak{b}_i \subset \mathfrak{b}_{i+1}$ from the formula for $\mathfrak{p}_i$ as an annihilator, so taking $i = \ell - 1, \ell - 2, \ldots, 0$,

$$\mathfrak{b} = \mathfrak{b}_\ell \supset \mathfrak{p}_{\ell-1}\mathfrak{b}_{\ell-1} \supset \mathfrak{p}_{\ell-1}\mathfrak{p}_{\ell-2}\mathfrak{b}_{\ell-2} \supset \cdots \supset \mathfrak{p}_{\ell-1}\cdots\mathfrak{p}_0\mathfrak{b}_0 = \mathfrak{p}_0\cdots\mathfrak{p}_{\ell-1}. \tag{8.2}$$

Therefore if $\mathfrak{p}$ is a prime ideal that contains $\mathfrak{b}$ then $\mathfrak{p} \supset \mathfrak{p}_0 \cdots \mathfrak{p}_{\ell-1}$, so $\mathfrak{p}$ is some $\mathfrak{p}_i$ by the analogue of Corollary 1.5 for orders.

The number of times a prime ideal occurs as an annihilator of quotient modules in the series (8.1) is independent of the choice of series thanks to the Jordan–Hölder theorem, that says the quotient modules in a composition series for $\mathcal{O}/\mathfrak{b}$ are determined up to $\mathcal{O}$-module isomorphism and multiplicity.

Since indices are multiplicative in towers, $[\mathcal{O} : \mathfrak{b}] = \prod_{i=0}^{\ell-1} [\mathfrak{b}_i : \mathfrak{b}_{i+1}]$. Since $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathcal{O}/\mathfrak{p}_i$ as $\mathcal{O}$-modules, $[\mathfrak{b}_i : \mathfrak{b}_{i+1}] = [\mathcal{O} : \mathfrak{p}_i]$. □

Remark 8.10. It might seem wrong that the condition $\mathcal{O}/\mathfrak{p} \cong \mathcal{O}/\mathfrak{p}'$ for nonzero prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ implies $\mathfrak{p} = \mathfrak{p}'$. After all, taking $\mathcal{O} = \mathbf{Z}[i]$, aren't $\mathbf{Z}[i]/(1 + 2i)$ and $\mathbf{Z}[i]/(1 - 2i)$ isomorphic fields (all fields of order 5 are isomorphic) while the ideals $(1+2i)$ and $(1-2i)$ are different? That's true, but the sense in which we refer to an isomorphism with $\mathcal{O}/\mathfrak{p}$ in the proof above is not as fields (or rings), but as $\mathcal{O}$-*modules*: if $\mathcal{O}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{b}$ as $\mathcal{O}$-modules then $\mathfrak{a} = \mathfrak{b}$ because the annihilator ideal of the $\mathcal{O}$-module $\mathcal{O}/\mathfrak{a}$ is $\mathfrak{a}$ and isomorphic $\mathcal{O}$-modules have equal annihilator ideals. Returning to the example of $\mathbf{Z}[i]/(1 + 2i)$ and $\mathbf{Z}[i]/(1 - 2i)$, they are isomorphic as fields, but they are not isomorphic as $\mathbf{Z}[i]$-modules: in $\mathbf{Z}[i]/(1 + 2i)$ we have $i = 2$ (since $1 + 2i = 0$) and in $\mathbf{Z}[i]/(1 - 2i)$ we have $i = 3$, so if there were a

$\mathbf{Z}[i]$-linear map $\mathbf{Z}[i]/(1+2i) \to \mathbf{Z}[i]/(1-2i)$ then the equation $i = 2$ in the domain would become $i = 2$ in the target, so $3 = 2$ in the target, but $3 \neq 2$ in $\mathbf{Z}[i]/(1-2i)$.

Example 8.11. Returning to Example 8.2, where $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$, we will find a Jordan-Hölder filtration for $\mathcal{O}/\mathfrak{b}$, where $\mathfrak{b} = p\mathcal{O}$. Since $\mathfrak{p} = p\mathcal{O}_K$ is the only prime containing $\mathfrak{b}$, Theorem 8.9 says every simple quotient module in a Jordan-Hölder filtration for $\mathcal{O}/\mathfrak{b}$ has to be isomorphic (as an $\mathcal{O}$-module) to $\mathcal{O}/\mathfrak{p} \cong \mathbf{Z}/p\mathbf{Z}$. Since $|\mathcal{O}/\mathfrak{b}| = p^n$, this means there is a chain of ideals

$$\mathcal{O} = \mathfrak{b}_0 \supset \mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_n = \mathfrak{b}$$

such that $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathcal{O}/\mathfrak{p}$.

Let's make such a chain of ideals explicit. Let $\{1, e_2, \ldots, e_n\}$ be a $\mathbf{Z}$-basis of $\mathcal{O}_K$, so

$$\begin{aligned} \mathcal{O} &= \mathbf{Z} \oplus \mathbf{Z}pe_2 \oplus \cdots \oplus \mathbf{Z}pe_n, \\ p\mathcal{O}_K &= \mathbf{Z}p \oplus \mathbf{Z}pe_2 \oplus \cdots \oplus \mathbf{Z}pe_n, \\ p\mathcal{O} &= \mathbf{Z}p \oplus \mathbf{Z}p^2e_2 \oplus \cdots \oplus \mathbf{Z}p^2e_n. \end{aligned}$$

Set $\mathfrak{b}_0 = \mathcal{O}$, $\mathfrak{b}_1 = \mathfrak{p} = p\mathcal{O}_K$, and for $2 \leq i \leq n$ set

$$\mathfrak{b}_i = \mathbf{Z}p \oplus \mathbf{Z}p^2e_2 \oplus \cdots \oplus \mathbf{Z}p^2e_i \oplus \mathbf{Z}pe_{i+1} \oplus \cdots \oplus \mathbf{Z}pe_n.$$

This is an ideal in $\mathcal{O}$ since the product of each basis vector for $\mathcal{O}$, besides 1, and each basis vector for $\mathfrak{b}_i$ is in $p^2\mathcal{O}_K \subset p\mathcal{O} = \mathfrak{b} \subset \mathfrak{b}_i$. We have $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathbf{Z}pe_{i+1}/\mathbf{Z}p^2e_{i+1} \cong \mathbf{Z}/p\mathbf{Z}$. Instead of *factoring* $\mathfrak{b}$ into a product of prime ideals in $\mathcal{O}$ (which Example 8.2 says is impossible) we have *filtered* $\mathcal{O}/\mathfrak{b}$ by the $\mathcal{O}$-modules

$$\mathcal{O}/\mathfrak{b} \supset \mathfrak{b}_1/\mathfrak{b} \supset \mathfrak{b}_2/\mathfrak{b} \supset \cdots \supset \mathfrak{b}_n/\mathfrak{b} = \{0\}$$

with simple quotients $\mathfrak{b}_i/\mathfrak{b}_{i+1} \cong \mathbf{Z}/p\mathbf{Z} \cong \mathcal{O}/\mathfrak{p}$.

In Example 8.2 we saw $[\mathcal{O} : \mathfrak{p}^2] = p^{n+1}$. The Jordan-Hölder filtration for $\mathcal{O}/\mathfrak{p}^2$ comes from $\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{b} \supset \mathfrak{p}^2$, where all successive quotients are isomorphic as $\mathcal{O}$-modules to $\mathcal{O}/\mathfrak{p}$.

Let's see what Theorem 8.9 says for the case when $\mathcal{O} = \mathcal{O}_K$ is the full ring of integers of a number field K. When $\mathfrak{b}$ is a nonzero proper ideal in $\mathcal{O}_K$, the prime factorization of ideals in $\mathcal{O}_K$ lets us make the Jordan–Hölder filtration of $\mathcal{O}_K/\mathfrak{b}$ explicit, as follows. Writing $\mathfrak{b} = \mathfrak{p}_0 \cdots \mathfrak{p}_{r-1}$, set $\mathfrak{b}_0 = \mathcal{O}_K$ and $\mathfrak{b}_i = \mathfrak{p}_0 \cdots \mathfrak{p}_{i-1}$ for $1 \leq i \leq r$. Then

$$\mathcal{O}_K = \mathfrak{b}_0 \supset \mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_r = \mathfrak{b}$$

and $\mathfrak{b}_i/\mathfrak{b}_{i+1} = \mathfrak{b}_i/\mathfrak{b}_i\mathfrak{p}_i \cong \mathcal{O}_K/\mathfrak{p}_i$ as $\mathcal{O}_K$-modules, by the first proof of Theorem 7.5. Thus each $\mathfrak{b}_i/\mathfrak{b}_{i+1}$ is a simple $\mathcal{O}_K$-module. Since the Jordan-Hölder theorem lets us compare each Jordan-Hölder filtration for $\mathcal{O}_K/\mathfrak{b}$ with the particular one we just constructed, we can say that in every Jordan-Hölder filtration for $\mathcal{O}_K/\mathfrak{b}$,

- the prime ideal factors of $\mathfrak{b}$ are the annihilators of the simple quotients in the filtration,
- the multiplicity of each prime ideal as a factor of $\mathfrak{b}$ is its multiplicity as an annihilator of a simple quotient in the filtration.

References

[1] Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
[2] N. Bourbaki, "Commutative Algebra," Addison-Welsey, Reading, MA 1972.
[3] H. S. Butts and L. Wade, *Two Criteria for Dedekind Domains*, Amer. Math. Monthly **73** (1966), 14–21.
[4] H. Cohen, "A Course in Computational Algebraic Number Theory," Springer–Verlag, New York, 1993.
[5] D. Dummit and R. Foote, "Abstract Algebra," 3rd ed., Wiley, New York, 2004.

[6] N. Jacobson, "Basic Algebra II," 2nd ed., W. H. Freeman & Co., New York, 1989.
[7] D. Lorenzini, "An Introduction to Arithmetic Geometry," American Math. Society, Providence, 1996.
[8] H. Matsumura, "Commutative Ring Theory," Cambridge Univ. Press, Cambridge, 1986.