

# MATH 6122: Algebra II

Frank Qiang  
Instructor: Matthew Baker

Georgia Institute of Technology  
Spring 2025

# Contents

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>Jan. 7 — Motivation for Algebraic Number Theory</b>  | <b>2</b> |
| 1.1      | Motivation: Fermat's Last Theorem . . . . .             | 2        |
| 1.2      | Algebraic Integers . . . . .                            | 3        |
| <b>2</b> | <b>Jan. 9 — Algebraic Integers and Dedekind Domains</b> | <b>4</b> |
| 2.1      | More on Algebraic Integers . . . . .                    | 4        |
| 2.2      | Dedekind Domains . . . . .                              | 6        |
| <b>3</b> | <b>Jan. 14 — Unique Factorization of Ideals</b>         | <b>8</b> |
| 3.1      | Norm in a Field . . . . .                               | 8        |
| 3.2      | Unique Factorization of Ideals . . . . .                | 9        |
| 3.3      | Inverse Ideals . . . . .                                | 10       |

# Lecture 1

## Jan. 7 — Motivation for Algebraic Number Theory

### 1.1 Motivation: Fermat's Last Theorem

**Theorem 1.1** (Fermat's last theorem<sup>1</sup>).  $x^n + y^n = z^n$  has no nonzero integer solutions when  $n \geq 3$ .

**Remark.** The  $n = 3$  case was solved by Euler, and the  $n = 4$  case was solved by Fermat. So we will assume  $n \geq 5$ . We can also assume  $n$  is prime, since if  $n = pm$ , then we can instead consider

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

Thus any nonzero solution to  $x^n + y^n = z^n$  also yields a nonzero solution to  $x^p + y^p = z^p$ . So let  $p \geq 5$  be prime, and let  $\zeta = \zeta_p$  be a primitive  $p$ th root of 1. Then consider

$$x^p + y^p = (x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{p-1} y) = z^p.$$

Note that  $x + \zeta^j y \in \mathbb{Z}[\zeta] \subseteq \mathbb{C}$ . Let us pretend for the moment that  $\mathbb{Z}[\zeta]$  is a UFD.<sup>2</sup> One can check that

$$\gcd(x + \zeta^j y, x + \zeta^k y) = 1$$

whenever  $j \neq k$ . If  $\mathbb{Z}[\zeta]$  were a UFD, then we could conclude that

$$x + y\zeta = u\alpha^p$$

for some  $u \in \mathbb{Z}[\zeta]^\times$  and  $\alpha \in \mathbb{Z}[\zeta]$ .<sup>3</sup> For the sake of illustration, suppose  $u = \pm\zeta^j$  for some  $j$ . Then

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

for  $a_i \in \mathbb{Z}$ . This gives

$$\alpha^p = a_0 + a_1 + \cdots + a_{p-2} \pmod{p},$$

using Fermat's little theorem,  $\zeta^p = 1$ , and the binomial theorem. So  $\alpha^p = a \pmod{p}$  with  $a \in \mathbb{Z}$ , and

$$x + y\zeta = \pm a\zeta^j \pmod{p}$$

for some  $0 \leq j \leq p-1$ . Note that  $\zeta^{p-1} = -(1 + \zeta + \cdots + \zeta^{p-2})$ , and one can check as an exercise that this implies  $p|x$  or  $p|y$ . This would have proved the "first case" of Fermat's last theorem.

---

<sup>1</sup>This problem was finally resolved by Wiles-Taylor in 1995.

<sup>2</sup>It is far from it, and this is likely the mistake that Fermat originally made.

<sup>3</sup>In a UFD, if a product of relatively prime elements is a  $p$ th power, then each factor must itself be a  $p$ th power.

**Remark.** However, Kummer (c. 1850) observed that  $\mathbb{Z}[\zeta]$  is rarely a UFD (in fact,  $\mathbb{Z}[\zeta]$  is a UFD if and only if  $p \leq 19$ ).<sup>4</sup> Also, when  $p \geq 5$ , the unit group of  $\mathbb{Z}[\zeta]$  is always infinite (so that  $\mathbb{Z}[\zeta]^\times \neq \{\pm\zeta^j\}$ ).

**Theorem 1.2** (Kummer). *Fermat's last theorem holds for all "regular" primes.*<sup>5</sup>

**Remark.** The first irregular prime is 37, so Kummer's method works for  $3 \leq n \leq 36$ .

## 1.2 Algebraic Integers

**Remark.** To resolve these issues, Kummer realized that one can replace elements of  $\mathbb{Z}[\zeta]$  by "ideal elements." Later on, Dedekind took at Kummer's work and introduced the modern notion of an ideal. We will be working towards the *unique factorization of ideals into prime ideals* in certain cases.

**Remark.** We will work at the level of generality of Dedekind rings (as opposed to just number rings). This is because there is an analogue of such a unique factorization of ideals for function fields of curves in algebraic geometry, and this framework is general enough to capture both cases.

**Definition 1.1.** Let  $K/\mathbb{Q}$  be a finite extension (i.e. a *number field*). Then  $\alpha \in K$  is an *algebraic integer* if there exists a monic polynomial  $f \in \mathbb{Z}[x]$  such that  $f(\alpha) = 0$ .

**Theorem 1.3.** *Let  $A \subseteq B$  be rings and let  $b \in B$ . Then the following are equivalent:*

1.  $b$  is integral over  $A$  (i.e. there exists a monic  $f \in A[x]$  such that  $f(b) = 0$ ).
2.  $A[b]$  is a finitely generated  $A$ -module.<sup>6</sup>
3.  $A[b]$  is contained in a subring  $C \subseteq B$  which is finitely generated as an  $A$ -module.

*Proof.* (1  $\Rightarrow$  2) This direction is standard, one only needs powers up to  $\deg f$  since  $f(b) = 0$ .

(2  $\Rightarrow$  3) This direction is clear since  $A[b]$  itself satisfies the desired conditions.

(3  $\Rightarrow$  1) The idea is to argue via determinants and use the Cayley-Hamilton theorem for modules.  $\square$

**Corollary 1.3.1.** *Integrality is transitive, i.e. if  $B$  is integral over  $A$  and  $C$  is integral over  $B$ , then  $C$  is integral over  $A$ .*<sup>7</sup>

*Proof.* A finitely generated module over a finitely generated module is finitely generated.  $\square$

**Corollary 1.3.2.** *If  $\alpha, \beta$  are integral over  $A$ , then  $\alpha \pm \beta, \alpha\beta$  are also integral over  $A$ .*

*Proof.* This is because  $\alpha \pm \beta, \alpha\beta \in C = A[\alpha][\beta]$ .  $\square$

**Theorem 1.4.** *The set of all algebraic integers in  $K$  (denoted  $\mathcal{O}_K$ ) forms a subring of  $K$ .*<sup>8</sup>

**Remark.** This theorem is not obvious: Given  $f(\alpha) = 0$  and  $g(\beta) = 0$ , one must find a polynomial  $h$  such that  $h(\alpha + \beta) = 0$ . It is not immediately obvious how to do this.

<sup>4</sup>Kummer made the first real progress on Fermat's last theorem in a long time.

<sup>5</sup>A prime  $p$  is *regular* if  $p$  does not divide the order of the *ideal class group* of  $\mathbb{Z}[\zeta]$ .

<sup>6</sup>Here  $A[b]$  is the smallest subring of  $B$  containing  $A$  and  $b$ , so  $A[b] = \{a_0 + a_1b + a_2b^2 + \cdots + a_kb^k : a_i \in A\}$ .

<sup>7</sup>We say that  $B$  is *integral over  $A$*  if every  $b \in B$  is integral over  $A$ .

<sup>8</sup>The ring of algebraic integers  $\mathcal{O}_K$  of a number field  $K$  is called a *number ring*.

# Lecture 2

## Jan. 9 — Algebraic Integers and Dedekind Domains

### 2.1 More on Algebraic Integers

**Proposition 2.1.** *Suppose  $\alpha, \beta \in \overline{\mathbb{Z}} \subseteq \mathbb{C}$ , then  $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$ .<sup>1</sup>*

*Proof.* First, note that every algebraic integer is an eigenvalue of some integer matrix (e.g. take the companion matrix for the minimal polynomial). So take linear maps  $T_\alpha : V_\alpha \rightarrow V_\alpha$  and  $T_\beta : V_\beta \rightarrow V_\beta$  which have  $\alpha$  and  $\beta$  as eigenvalues, respectively. Then one can check that the map on the direct sum

$$T_\alpha \oplus T_\beta : V_\alpha \oplus V_\beta \rightarrow V_\alpha \oplus V_\beta$$

has  $\alpha + \beta$  as an eigenvalue. Similarly, by looking at the map on the tensor product

$$T_\alpha \otimes T_\beta : V_\alpha \otimes V_\beta \rightarrow V_\alpha \otimes V_\beta$$

has  $\alpha\beta$  as an eigenvalue. Hence we see that  $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$  as well. □

**Remark.** This is a constructive proof of what we showed via finitely generated modules last time.

**Lemma 2.1.** *Let  $\alpha \in K$  be an algebraic number. Then  $\alpha$  is an algebraic integer, i.e.  $\alpha \in \mathcal{O}_K$ , if and only if the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ , call it  $f_\alpha \in \mathbb{Q}[x]$ , has integer coefficients.*

*Proof.* ( $\Leftarrow$ ) This direction is clear by the definition of an algebraic integer.

( $\Rightarrow$ ) We need to show that if  $\alpha \in \mathcal{O}_K$ , then  $f_\alpha \in \mathbb{Z}[x]$ . By assumption, there exists some monic integer polynomial  $h \in \mathbb{Z}[x]$  such that  $h(\alpha) = 0$ . From this, we know that  $f_\alpha | h$  in  $\mathbb{Q}[x]$ .<sup>2</sup> Let  $\alpha_1, \dots, \alpha_n$  be the roots of  $f_\alpha$  with  $\alpha_1 = \alpha$ . Since  $f_\alpha | h$ , we know that  $h(\alpha_i) = 0$  for every  $i$ , so  $h \in \mathbb{Z}[x]$  implies that  $\alpha_i \in \overline{\mathbb{Z}}$  for each  $i$ . Thus the coefficients of  $f_\alpha$  are elementary symmetric functions of the  $\alpha_i$ ,<sup>3</sup> so

$$f_\alpha \in (\overline{\mathbb{Z}} \cap \mathbb{Q})[x].$$

Thus it suffices to show that  $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$  to conclude the result. For this, suppose  $r/s \in \mathbb{Q}$  is the root of

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x].$$

---

<sup>1</sup>Here  $\overline{\mathbb{Z}}$  is the set of algebraic integers.

<sup>2</sup>Note that it suffices to show that  $f_\alpha | h$  in  $\mathbb{Z}[x]$ , so alternatively, a suitable version of Gauss's lemma immediately implies the desired result.

<sup>3</sup>These operations preserve the notion of being an algebraic integer.

We can assume  $(r, s) = 1$  without loss of generality.<sup>4</sup> Plugging in, we obtain

$$(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0 = 0.$$

Clearly denominators by multiplying by  $s^n$ , we obtain

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_1s^{n-1}r + a_0s^n = 0$$

The right-hand side is divisible by  $s$  and every term on the left-hand side except  $r^n$  is divisible by  $s$ , so we must have  $s|r^n$ . Since  $(r, s) = 1$ , this implies that  $s = \pm 1$ , i.e.  $r/s \in \mathbb{Z}$ .  $\square$

**Example 2.0.1.** For  $K = \mathbb{Q}$ , we have  $\mathcal{O}_K = \mathbb{Z}$ . This follows from the previous lemma since the minimal polynomial of  $a \in \mathbb{Q}$  is  $x - a$ , which has integer coefficients precisely when  $a \in \mathbb{Z}$ .

**Example 2.0.2.** Let  $K = \mathbb{Q}(\sqrt{d})$ , i.e.  $K$  is *quadratic number field*. Clearly  $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$ , but this is not always an equality. For example,

$$\phi = \frac{1 + \sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}],$$

but  $x^2 - x - 1$  has  $\phi$  as a root.

**Exercise 2.1.** Let  $d$  be a square-free integer and  $K = \mathbb{Q}(\sqrt{d})$ . Show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}[(1 + \sqrt{d})/2] & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

**Definition 2.1.** Let  $S$  be a ring. If  $R \subseteq S$  is a subring, then we say that  $R$  is *integrally closed* in  $S$  if whenever  $\alpha \in S$  is integral over  $R$ , then  $\alpha \in R$ .

**Remark.** Recall that for a domain  $R$ , its *field of fractions*  $K$  is the localization

$$K = S^{-1}R$$

where  $S = R \setminus \{0\}$ . There is a natural embedding of  $R$  into  $K$  via  $r \mapsto r/1$ .

**Lemma 2.2.** *The fraction field of  $\mathcal{O}_K$  is  $K$ . More precisely, for every  $\alpha \in K$ , there exists  $m \in \mathbb{Z}$ ,  $m \neq 0$ , such that  $m\alpha \in \mathcal{O}_K$ .*

*Proof.* Since  $\alpha$  is algebraic, there exists some monic polynomial  $f_\alpha \in \mathbb{Q}[x]$  such that  $f_\alpha(\alpha) = 0$ . By clearing denominators, there exists  $m \in \mathbb{Z}$  such that  $mf_\alpha \in \mathbb{Z}[x]$ . So we have

$$m\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0,$$

and multiplying by  $m^{n-1}$  on both sides, we obtain

$$m^n\alpha^n + m^{n-1}b_{n-1}\alpha^{n-1} + \cdots + m^{n-1}b_1\alpha + m^{n-1}b_0 = 0,$$

which implies

$$(m\alpha)^n + b_{n-1}(m\alpha)^{n-1} + \cdots + m^{n-2}b_1(m\alpha) + m^{n-1}b_0 = 0.$$

This shows that  $m\alpha$  is integral over  $\mathbb{Z}$ , i.e.  $m\alpha \in \mathcal{O}_K$ .  $\square$

---

<sup>4</sup>Here we write  $(r, s)$  to denote  $\gcd(r, s)$ .

**Theorem 2.1.** *The ring of integers  $\mathcal{O}_K$  is integrally closed (in its fraction field).*

*Proof.* Transitivity of integrality implies that  $\mathcal{O}_K$  is integrally closed in  $K$ . The theorem then follows from the fact that  $K$  is the fraction field of  $\mathcal{O}_K$ .  $\square$

**Remark.** This theorem says that (it implies the second equality)

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is integral over } \mathbb{Z}\} = \{\alpha \in K \mid \alpha \text{ is integral over } \mathcal{O}_K\}.$$

## 2.2 Dedekind Domains

**Definition 2.2.** A *Dedekind domain* is a Noetherian integrally closed domain of dimension 1.

**Remark.** Recall that all rings in this class are commutative and have a 1. A *dimension 1 domain* is a domain which is not a field and in which every nonzero prime ideal is maximal. In general, the *dimension* of a ring  $R$  is the maximum length of a chain of prime ideals of the form

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

In dimension 1, this corresponds to  $(0) \subsetneq \mathfrak{p}$  being the maximum chain for every nonzero prime ideal  $\mathfrak{p}$ , which is equivalent to the other definition.

**Remark.** Our goal for now will be to show that  $\mathcal{O}_K$  is a Dedekind domain.

**Definition 2.3.** Let  $k$  be either  $\mathbb{Q}$  or  $\mathbb{R}$  and  $V$  be a finite-dimensional  $k$ -vector space. A *complete lattice* in  $V$  is a discrete additive subgroup  $\Lambda$  of  $V$  which spans  $V$ , where discrete means that any bounded subset of  $\Lambda$  is finite (equivalent to being discrete in the sense of topology).

**Proposition 2.2.** *Let  $V$  be as above (dimension  $n$  over  $k$ ) and  $\Lambda \subseteq V$  an additive subgroup which spans  $V$ . Then the following are equivalent:*

1.  $\Lambda$  is discrete.
2.  $\Lambda$  is generated by  $n$  elements.
3.  $\Lambda \cong \mathbb{Z}^n$  as  $\mathbb{Z}$ -modules.

*Proof.*  $(2 \Leftrightarrow 3)$  This follows by the structure theorem ( $\Lambda$  is torsion-free since  $\Lambda \subseteq V$ ).

$(1 \Rightarrow 2)$  Suppose  $\Lambda$  is discrete, and let  $x_1, \dots, x_n \in \Lambda$  be a basis for  $V$ . Let  $\Lambda_0$  be the  $\mathbb{Z}$ -module which is spanned by  $x_1, \dots, x_n$ . We claim that  $\Lambda/\Lambda_0$  is finite, which implies that  $\Lambda$  is also generated by  $n$  elements (exercise). To see the claim, we note that there exists an integer  $M > 0$  such that if  $x = \sum \lambda_i x_i \in \Lambda$  with  $\lambda_i \in k$  and all  $|\lambda_i| < 1/M$ , then  $x = 0$ . This is standard and follows from all norms being equivalent in a finite-dimensional vector space and the assumption that  $\Lambda$  is discrete.

Now let  $y_1, y_2, \dots$  be coset representatives for  $\Lambda/\Lambda_0$ . Without loss of generality (by translating in the coset), assume each  $y_i \in C$ , where  $C$  is the unit cube. Cover  $C$  by  $M^n$  boxes of the form

$$\frac{m_i}{M} \leq \lambda_i < \frac{m_i + 1}{M}$$

with  $m_i \in \mathbb{Z}$  and  $0 \leq m_i < M$ . We must have  $|\Lambda/\Lambda_0| \leq M^n$ , since otherwise we end up with two  $y_i \neq y_j$  in the same box by the pigeonhole principle, and  $y_i - y_j \in C[1/M] \cap \Lambda = \{0\}$  leads to a contradiction.

$(2 \Rightarrow 1)$  This proof is to be finished next class.  $\square$

**Theorem 2.2.** *If  $I$  is a nonzero ideal in a number ring  $\mathcal{O}_K$ , then  $\mathcal{O}_K/I$  is finite.*

*Proof.* The strategy is to show that if  $[K : \mathbb{Q}] = n$ , then  $\mathcal{O}_K \cong \mathbb{Z}^n$  and  $I \cong \mathbb{Z}^n$  as  $\mathbb{Z}$ -modules. This will imply that  $\mathcal{O}_K/I$  is finite, which follows from the proof of the structure theorem. In fact, we will show that  $I$  and  $\mathcal{O}_K$  are lattices in  $K \cong \mathbb{Q}^n \subseteq \mathbb{R}^n$ . Note that it suffices to show that  $\mathcal{O}_K$  is a lattice, since it immediately follows that  $I \subseteq \mathcal{O}_K$  is also discrete, hence also a lattice as  $I$  is an additive subgroup.

The proof is to be finished next class. □

**Corollary 2.2.1.** *A number ring  $\mathcal{O}_K$  is Noetherian.*

*Proof.* Suppose that we have an ascending chain of ideals

$$I = I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

Suppose without loss of generality that  $I_0 \neq 0$ . Since  $\mathcal{O}_K/I$  is finite, by an isomorphism theorem we see that there are only finitely many ideals in  $\mathcal{O}_K$  containing  $I$ . This implies that the chain must eventually stabilize, i.e. that  $\mathcal{O}_K$  is Noetherian. □

**Corollary 2.2.2.** *A number ring  $\mathcal{O}_K$  is 1-dimensional.*

*Proof.* Verify as an exercise that  $\mathcal{O}_K$  is not a field. Now let  $\mathfrak{p}$  be a nonzero prime ideal, so that  $\mathcal{O}_K/\mathfrak{p}$  is a finite domain, hence a field. This implies that  $\mathfrak{p}$  is maximal, so  $\mathcal{O}_K$  is 1-dimensional. □

**Theorem 2.3.** *A number ring  $\mathcal{O}_K$  is a Dedekind domain.*



# Lecture 3

## Jan. 14 — Unique Factorization of Ideals

### 3.1 Norm in a Field

**Remark.** Let  $K/\mathbb{Q}$  be a finite extension of degree  $n$ . Our goal will be to define a *norm*  $N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$  which also sends  $\mathcal{O}_K \rightarrow \mathbb{Z}$ . Note that there are  $n$  distinct embeddings  $\sigma_1, \dots, \sigma_n : K \rightarrow \mathbb{C}$ , e.g. choose a primitive element  $\theta \in K$  (so that  $K = \mathbb{Q}(\theta)$ ) with minimal polynomial  $f$  of degree  $n$  and define  $\sigma : K \rightarrow \mathbb{C}$  by sending  $\theta$  to some root of  $f$ , of which there are  $n$  choices.<sup>1</sup>

**Definition 3.1.** Given a finite extension  $K/\mathbb{Q}$ , define the *norm*  $N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$  by

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^n \sigma_i(x),$$

where  $\sigma_1, \dots, \sigma_n : K \rightarrow \mathbb{C}$  are the  $n$  distinct embeddings of  $K$  into  $\mathbb{C}$ .

**Exercise 3.1.** Show that in fact  $N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Q}$ . (Hint: One way is via Galois theory.)

**Exercise 3.2.** Define  $[\gamma] : K \rightarrow K$  by  $x \mapsto \gamma x$ , which is a  $\mathbb{Q}$ -linear map. Show that  $N_{K/\mathbb{Q}}(\gamma) = \det[\gamma]$ .

**Proposition 3.1.** *We have the following properties of the norm  $N = N_{K/\mathbb{Q}}$ :*

1.  $N(\gamma) = 0$  if and only if  $\gamma = 0$ ;
2. if  $\gamma \in \mathcal{O}_K$ , then  $N(\gamma) \in \mathbb{Z}$ .

*Proof.* Check these properties as an exercise. □

**Theorem 3.1.** *A number ring  $\mathcal{O}_K$  is a complete lattice in  $K \cong \mathbb{Q}^n \subseteq \mathbb{R}^n$ .*

*Proof.* We need to show that  $\mathcal{O}_K$  is discrete. Note that there exists a basis  $\alpha_1, \dots, \alpha_n$  for  $K/\mathbb{Q}$  such that  $\alpha_i \in \mathcal{O}_K$  for every  $i$ . Now suppose otherwise that  $\mathcal{O}_K$  is not discrete, so there are arbitrarily small  $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$  such that  $\alpha = \sum \lambda_i \alpha_i$  is nonzero and in  $\mathcal{O}_K$ . Then

$$N_{K/\mathbb{Q}}(\alpha) = \phi(\lambda_1, \dots, \lambda_n)$$

for some homogeneous polynomial  $\phi$  of degree  $n$  (since each  $\sigma(\alpha) = \sum \lambda_i \sigma(\alpha_i)$ ). Thus if  $|\lambda_i| \ll 1$ , the polynomial  $\phi$  also gets small and we can obtain  $0 < |N_{K/\mathbb{Q}}(\alpha)| < 1$ , a contradiction since  $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ . □

**Corollary 3.1.1.** *If  $I \subseteq \mathcal{O}_K$  is a nonzero ideal, then  $I$  is also a complete lattice in  $\mathbb{R}^n$ .*

---

<sup>1</sup>As an example of having  $n$  embeddings, consider  $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \subseteq \mathbb{C}$ , where we can send  $\sqrt{2} \mapsto \pm\sqrt{2}$ .

*Proof.* One needs to show that  $I$  contains a basis for  $K/\mathbb{Q}$ . Choose any nonzero  $c \in I$  and consider  $c\alpha_1, \dots, c\alpha_n \in I$  (since  $I$  is an ideal). This will also be a basis for  $K/\mathbb{Q}$  since  $c \neq 0$ .  $\square$

**Corollary 3.1.2.** *We have  $|\mathcal{O}_K/I| < \infty$  for every nonzero ideal  $I \subseteq \mathcal{O}_K$ .*

*Proof.* This is because  $\mathcal{O}_K \cong I \cong \mathbb{Z}^n$  as  $\mathbb{Z}$ -modules, so the result follows by the structure theorem.  $\square$

**Remark.** These details complete the proof from last time that  $\mathcal{O}_K$  is a Dedekind domain.

**Remark.** The following is a preview of what we will do later in the class: We will define the *norm* of an ideal to be  $N(I) = |\mathcal{O}_K/I|$ . One can show that if  $I = (\gamma)$ , then  $N(I) = N(\gamma)$ . An extension of the previous techniques then leads to a proof of the finiteness of the *ideal class group*.

## 3.2 Unique Factorization of Ideals

**Remark.** Recall that for ideals  $I = (\alpha_1, \dots, \alpha_k)$  and  $J = (\beta_1, \dots, \beta_\ell)$ , their *product* is  $IJ = (\alpha_i\beta_j)_{i,j}$ .

**Example 3.1.1.** Consider  $R = \mathbb{Z}[\sqrt{-5}]$ , which is the ring of integers  $\mathcal{O}_K$  in  $K = \mathbb{Q}(\sqrt{-5})$ . Note that

$$6 = 2(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and these elements are irreducible and not associates, so  $R$  is not a UFD. However, let

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \quad \mathfrak{p}_2 = (2, 1 - \sqrt{-5}), \quad \mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_4 = (3, 1 - \sqrt{-5}).$$

None of these ideals are principal, but they are all prime ideals. One can check that

$$\mathfrak{p}_1\mathfrak{p}_2 = (4, 2 - 2\sqrt{-5}, 2 + 2\sqrt{-5}, 6) = (2),$$

that  $\mathfrak{p}_3\mathfrak{p}_4 = (3)$ , that

$$\mathfrak{p}_1\mathfrak{p}_3 = (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, 6) = (1 + \sqrt{-5}),$$

and finally that  $\mathfrak{p}_2\mathfrak{p}_4 = (1 - \sqrt{-5})$ . At the level of ideals, the original equation then becomes

$$(6) = (2)(3) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4) = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

In fact, the previous nonunique factorization is now the same factorization in the language of ideals.

**Lemma 3.1.** *Let  $I_1, \dots, I_n$  be ideals in a commutative ring  $R$ , and let  $\mathfrak{p}$  be a prime ideal. Suppose that  $I_1 I_2 \dots I_n \subseteq \mathfrak{p}$ . Then  $I_j \subseteq \mathfrak{p}$  for some  $j$ .*

*Proof.* Check this as an exercise, it follows from the definition of a prime ideal.  $\square$

**Lemma 3.2.** *Let  $R$  be a Noetherian ring, and  $I \subseteq R$  be a nonzero ideal. Then there exist nonzero prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  such that  $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq I$ .*

*Proof.* Let  $\Sigma$  be the set of all  $I$  for which the lemma is false. If  $\Sigma \neq \emptyset$ , then since  $R$  is Noetherian,  $\Sigma$  has a maximal element (pick  $I_1 \in \Sigma$ , if it is not maximal, then we can find  $I_2 \in \Sigma$  with  $I_1 \subsetneq I_2$ , and we obtain  $I_1 \subsetneq I_2 \subsetneq \dots$  by continuing; this chain must terminate since  $R$  is Noetherian). Let  $J$  be such a maximal element. Now  $J$  cannot be prime, so there exist  $a, b \in R$  such that  $ab \in J$  but  $a, b \notin J$ . Let

$$\mathfrak{a} = (J, a) \supsetneq J \quad \text{and} \quad \mathfrak{b} = (J, b) \supsetneq J.$$

Then  $\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m$  and  $\mathfrak{b} \supseteq \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_n$ . Since  $\mathfrak{ab} = (J^2, Ja, Jb, ab) \subseteq J$ , we obtain

$$J \supseteq \mathfrak{ab} \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_m \mathfrak{q}_1 \dots \mathfrak{q}_n,$$

which is a contradiction. Thus we must have  $\Sigma = \emptyset$ , so the lemma holds for every nonzero ideal  $I$ .  $\square$

### 3.3 Inverse Ideals

**Example 3.1.2.** Consider the problem of finding  $(2)^{-1}$  in  $\mathbb{Z}$ . Logically, the answer should be something like  $(1/2) = (1/2)\mathbb{Z} \subseteq \mathbb{Q}$ , which is not an ideal in  $\mathbb{Z}$ .<sup>2</sup> This will satisfy  $2((1/2)\mathbb{Z}) = \mathbb{Z}$ .

**Definition 3.2.** Let  $R$  be an integral domain with fraction field  $K$ , and let  $I$  be a nonzero ideal in  $R$ . Then the *inverse ideal*  $I^{-1}$  of  $I$  is

$$I^{-1} = \{x \in K \mid xI \subseteq R\}.$$

**Example 3.2.1.** Let  $R = \mathbb{Z}$  and  $I = (2)$ . Then we can see that

$$I^{-1} = \{x \in \mathbb{Q} \mid x(2) \subseteq \mathbb{Z}\} = \frac{1}{2}\mathbb{Z}.$$

**Remark.** Our goal at this point is to show that if  $R$  is Dedekind, then  $II^{-1} = R$ . Note that if  $M, N$  are two  $R$ -submodules of  $K$ , then their product is well-defined:

$$MN = R\text{-submodule of } K \text{ generated by } \{xy \mid x \in M, y \in N\},$$

e.g.  $((1/2)\mathbb{Z})((1/3)\mathbb{Z}) = (1/6)\mathbb{Z}$ . This is how we will make sense of the product  $II^{-1}$ .

**Lemma 3.3.** If  $I = (a)$ , then  $I^{-1} = (a^{-1})$  and  $II^{-1} = (1) = R$ .

*Proof.* Check this as an exercise.  $\square$

**Proposition 3.2.** If  $R$  is Dedekind,  $I \neq 0$  is an ideal, and  $\mathfrak{p} \neq 0$  is a prime ideal, then  $\mathfrak{p}^{-1}I \neq I$ .

*Proof.* First consider the special case  $I = R$ , and we want to show that  $\mathfrak{p}^{-1} \neq R$ . We will find  $x \in \mathfrak{p}^{-1}$  which is not in  $R$ . To do this, we will take  $x = a^{-1}b = b/a$  for some  $a, b \in R$ . We want  $(b/a)\mathfrak{p} \subseteq R$ , so we should look for  $b\mathfrak{p} \subseteq (a)$  with  $b \notin (a)$ . Let  $a \in \mathfrak{p}$  be any nonzero element, and we will find a suitable  $b$ .

Since  $R$  is Noetherian, there exists  $\mathfrak{p}_i$  such that  $\mathfrak{p}_i \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ . Without loss of generality, we can assume  $r$  is minimal. This then implies that  $\mathfrak{p}_i \subseteq \mathfrak{p}$  for some  $i$ , which implies  $\mathfrak{p}_i = \mathfrak{p}$  since  $R$  is 1-dimensional. Assume without loss of generality that  $i = 1$ , so  $\mathfrak{p}_1 = \mathfrak{p}$ .

If  $r = 1$ , then  $\mathfrak{p} = (a)$ , so that  $\mathfrak{p}^{-1} = (a^{-1}) \neq R$  since  $a$  is not a unit. So now assume  $r \geq 2$ . Then

$$\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subseteq (a)$$

by the minimality of  $r$ , so there exists  $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$  such that  $b \notin (a)$ . But  $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq (a)$ , so the element  $x = b/a \in \mathfrak{p}^{-1}$  but is not in  $R$ . This proves that  $I = R$ .

<sup>2</sup>Note that this is not an ideal of  $\mathbb{Q}$  either since it is not closed under multiplication by elements of  $\mathbb{Q}$ . The inverse ideal  $(2)^{-1}$  is instead a  $\mathbb{Z}$ -submodule of  $\mathbb{Q}$ , viewed as a  $\mathbb{Z}$ -module.

In the general case, using the hypothesis that  $R$  is Noetherian, we can write  $I = (\alpha_1, \dots, \alpha_n)$ . Assume otherwise that  $\mathfrak{p}^{-1}I = I$ . Then for  $x \in \mathfrak{p}^{-1}$ , we can write

$$x\alpha_i = \sum_{j=1}^n a_{ij}\alpha_j, \quad a_{ij} \in R.$$

Let  $A = (a_{ij})$  and define  $T = xI_n - A$ . Check as an exercise that  $\det T = 0$ . Since  $\det T$  is a monic polynomial in  $x$  with coefficients in  $R$ , we see that  $x$  is integral over  $R$ . Since  $R$  is integrally closed, we must have  $x \in R$ , so we get  $\mathfrak{p}^{-1} = R$ . This contradicts the above special case.  $\square$

**Remark.** The key idea of the proof is Cayley-Hamilton for modules: Let  $R$  be a commutative ring and  $M$  a finitely generated  $R$ -module. Then if  $JM = M$ , there exists  $a$  with  $1 - a \in J$  such that  $aM = M$ . The proof above uses a similar strategy to the proof of this statement.