Quadratic Number Fields

1 ▷ Unique factorisation domains ◁

Let $\mathfrak{D}$ be an integral domain, or domain, for short. Recall that this is a commutative ring without zero-divisors, i.e., without non-zero elements $a, b \in \mathfrak{D}$ such that $ab = 0$.

The **Fundamental Theorem of Arithmetic** says that every integer n can factored, *uniquely* (up to permutation of the prime factors), as a product

$$n = \pm p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}, \quad p_i \in \operatorname{Spec}(\mathbb{Z}).$$

It is reasonable to ask if this can be generalised to other rings $\mathfrak{D}$, not just $\mathfrak{D} = \mathbb{Z}$. Observe that it is essential that $\mathfrak{D}$ is an integral domain (why?).

The answer is in most cases *no*. Let us investigate this a little further. The following definition is a direct generalisation of factors in $\mathbb{Z}$.

Definition 1. Let $\mathfrak{D}$ be a domain and $a, b \in \mathfrak{D}$. Then a **divides** b, or is a **factor** in b, if there is a $c \in \mathfrak{D}$ such that $b = ac$. Just as in $\mathbb{Z}$ we denote this $a \mid b$.

We will from now on use the blanket assumption that $\mathfrak{D}$ is an integral domain.

Definition 2. Let $u \in \mathfrak{D}$. Then u is a **unit** if $u \mid 1$, in other words u has an inverse. Two elements a and b are **associate elements** (or **associates**) if there is a unit u such that $b = au$.

Observe that, since u is a unit,

$$b = au \iff a = u^{-1}b.$$

Clearly, if u is a unit, so too is u^{-1}.

We denote the set of units in $\mathfrak{D}$ by $\mathfrak{D}^\times$ or, sometimes, $U(\mathfrak{D})$. In addition, we put $\mathfrak{D}^\circ := \mathfrak{D} \setminus \{0\}$.

Definition 3. Let $\boldsymbol{\pi} \in \mathfrak{D}^\circ$. Then

(a) $\boldsymbol{\pi}$ is **irreducible** if any factorisation $\boldsymbol{\pi} = ab$, implies that a or b is a unit.

(b) $\boldsymbol{\pi}$ is a **prime element**, or simply **prime**, if any factorisation $\boldsymbol{\pi} = ab$, implies that $\boldsymbol{\pi} \mid a$ or $\boldsymbol{\pi} \mid b$.

We directly note:

Lemma 1. Any prime element is irreducible.

The converse is in general false.

Proof. Let $\boldsymbol{\pi}$ be a prime. Suppose we could factor $\boldsymbol{\pi}$ as $\boldsymbol{\pi} = ab$, with $a, b \notin \mathfrak{D}^\times$. The assumption $\boldsymbol{\pi} = ab$ implies that $\boldsymbol{\pi} \mid (ab)$ since $\boldsymbol{\pi}$ certainly divides the left-hand side. Therefore, since $\boldsymbol{\pi}$ is prime, we have either $\boldsymbol{\pi} \mid a$ or $\boldsymbol{\pi} \mid b$. Suppose that $\boldsymbol{\pi} \mid a$. This is equivalent to $a = k\boldsymbol{\pi}$, for some $k \in \mathfrak{D}^\circ$. Hence, we have $\boldsymbol{\pi} = k\boldsymbol{\pi}b$, which we can rearrange as $\boldsymbol{\pi}(kb - 1) = 0$. Since $\boldsymbol{\pi} \neq 0$, we must have $kb = 1$ and so b is a unit. This is a contradiction to the assumption that $b \notin \mathfrak{D}^\times$. □

Recall the following definition:

Definition 4. An ideal $\mathfrak{a}$ in a ring $\mathfrak{R}$ is a **prime ideal** if $ab \in \mathfrak{a}$ implies that $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$.

The following remark is important.

Remark 1. Let $\mathfrak{a} = (a)$ be a principal ideal. The following equivalences hold

$$\alpha \in \mathfrak{a} \iff \alpha = ba \iff a \mid \alpha.$$

This can be used as a justification for the following *notation*: suppose $\mathfrak{a}$ and $\mathfrak{b} = (\beta)$ are ideals, with $\mathfrak{a}$ not necessarily principal. Then

$$(\beta) \subset \mathfrak{a} \iff \mathfrak{a} \mid (\beta).$$

In particular, if $\mathfrak{a} = (\alpha)$,

$$(\beta) \subset (\alpha) \iff (\alpha) \mid (\beta) \iff \alpha \mid \beta.$$

More generally, we can *define*

$$\mathfrak{b} \subset \mathfrak{a} \iff \mathfrak{a} \mid \mathfrak{b}.$$

Be sure to reconcile this with your intuition.

Definition 5. An integral domain $\mathfrak{D}$ is a **unique factorisation domain** (UFD) if

(U1) Every non-zero $a \notin \mathfrak{D}^\times$ can be factored into a finite product of irreducible elements.

(U2) If

$$a = \prod_{i=1}^{n} \boldsymbol{\pi}_i \qquad \text{and} \qquad a = \prod_{i=1}^{m} \boldsymbol{\pi}'_i$$

are two different factorisations into irreducibles, then $n = m$ and

$$\left\{\boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \ldots, \boldsymbol{\pi}_n\right\} = \left\{\boldsymbol{\pi}'_1, \boldsymbol{\pi}'_2, \ldots, \boldsymbol{\pi}'_n\right\}.$$

Observe that we don't say anything concerning the $\boldsymbol{\pi}_i$ in the factorisation being distinct.

Example 1. Clearly, in $\mathbb{Z}$ the irreducible elements are the prime numbers. Prime numbers are also prime elements (this will follow from a theorem below).

Unique factorisation is guaranteed by the Fundamental Theorem of Arithmetic.

Definition 6. A domain $\mathfrak{D}$ is a **principal ideal domain** (PID) if every ideal in $\mathfrak{D}$ is principal. That is, every ideal $\mathfrak{a} \subset \mathfrak{D}$ can be written as

$$\mathfrak{a} = (a) := \left\{ d \in \mathfrak{D} \;\middle|\; d = xa, \text{ for some } x \in \mathfrak{D} \right\}$$

(i.e., the ideal of all multiples of a).

The statements collected in the following theorem are quite difficult to prove so we will omit the proofs.

Theorem 1. Let $a, b, c, d \in \mathbb{Z}$. Then

(i) every PID is UFD;

(ii) in a PID:

$$\boldsymbol{\pi} \text{ irreducible} \iff \boldsymbol{\pi} \text{ prime};$$

(iii) if $\mathfrak{D}$ is a field, $\mathfrak{D}[x]$ is a PID, and hence a UFD by (i).

Theorem 2. Let $\mathfrak{p} := (\boldsymbol{\pi}) \subset \mathfrak{D}$ be a principal ideal in the domain $\mathfrak{D}$. Then

$$\mathfrak{p} \text{ is a prime ideal} \iff \boldsymbol{\pi} \text{ is a prime element.}$$

Proof. Suppose first that $\mathfrak{p} = (\boldsymbol{\pi})$ is a prime ideal. Hence $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. That $ab \in \mathfrak{p}$ is equivalent to the existence of a $c \in \mathfrak{D}$ such that $ab = c\boldsymbol{\pi}$. Since $\mathfrak{p}$ is principal, $a = \alpha\boldsymbol{\pi}$ and $b = \beta\boldsymbol{\pi}$ which means that $\boldsymbol{\pi} \mid a$ or $\boldsymbol{\pi} \mid b$. Assume now that $\boldsymbol{\pi}$ is prime and that $ab \in \mathfrak{p} = (\boldsymbol{\pi})$. This is equivalent to

$ab = c\boldsymbol{\pi}$ for some $c \in \mathfrak{D}$. Since $\boldsymbol{\pi}$ is prime, $\boldsymbol{\pi} \mid a$ or $\boldsymbol{\pi} \mid b$ which is equivalent to $a \in (\boldsymbol{\pi}) = \mathfrak{p}$ or $b \in (\boldsymbol{\pi}) = \mathfrak{p}$ and so $\mathfrak{p}$ is prime ideal. □

The theorem justifies the following notation:

$$\begin{aligned}\mathrm{PSpec}(\mathfrak{D}) &:= \Big\{\mathfrak{p} \subset \mathfrak{D} \;\Big|\; \mathfrak{p} = (\boldsymbol{\pi}) \text{ for a prime element } \boldsymbol{\pi}\Big\} \\ &\subseteq \mathrm{Spec}(\mathfrak{D}) := \Big\{\mathfrak{p} \subset \mathfrak{D} \;\Big|\; \mathfrak{p} \text{ a prime ideal}\Big\}.\end{aligned}$$

Therefore, if $\mathfrak{D}$ is a PID,

$$\mathrm{PSpec}(\mathfrak{D}) = \mathrm{Spec}(\mathfrak{D}).$$

This equality have some interesting consequences as we will see below.

2 ▷ Euclidean rings ◁

We will now generalise the division algorithm to a class of integral domains.

Definition 7. An integral domain $\mathfrak{D}$ is a **Euclidean domain** if a function

$$\epsilon : \mathfrak{D}^\circ \to \mathbb{Z}_{\geq 0}$$

can be constructed such that

(Val1) for all $a, b \in \mathfrak{D}^\circ$, there are elements $q, r \in \mathfrak{D}$ such that

$$a = qb + r, \qquad \text{where } r = 0 \quad \text{or} \quad 0 \geq \epsilon(r) < \epsilon(b);$$

(Val2) for all $a, b \in \mathfrak{D}^\circ$, $\epsilon(a) \leq \epsilon(ab)$. (Clearly we can switch a and b.)

The function ϵ is called a **Euclidean valuation**.

The similarity with the division algorithm on $\mathbb{Z}$ must not be lost on the reader. Indeed,

Example 2. The absolute value $\|\cdot\|$ on $\mathbb{Z}$ is a Euclidean valuation. Observe that

$$\|ab\| = \|a\| \cdot \|b\| \geq \|a\|, \quad \text{since} \quad \|b\| \geq 1,$$

so axiom (Val1) is satisfied. Axiom (Val2) is the division algorithm.

Example 3. Let $\mathfrak{D} = k$ be a field. The polynomial ring $k[x]$ is a Euclidean domain with valuation

$$\epsilon(P(x)) := \deg(P(x)),$$

If $P(x) \in k$ (recall: k is a field) the degree is 0, so $\epsilon(P(x)) = 0$ for constant polynomials.

The axiom (Val1) is simply polynomial division and (Val2) follows since

$$\begin{aligned}\epsilon(P(x)Q(x)) &= \deg\big(P(x)Q(x)\big) \\ &= \deg(P(x))\deg(Q(x)) \\ &= \epsilon(P(x))\epsilon(Q(x)).\end{aligned}$$

Observe that $\epsilon(0)$ is not defined.

Theorem 3. We have the following implications for a domain $\mathfrak{D}$:

$$\mathfrak{D} \text{ is Euclidean} \implies \mathfrak{D} \text{ is a PID} \overset{\text{Thm. 1(i)}}{\implies} \mathfrak{D} \text{ is a UFD.}$$

Proof. Maybe someday. □

Corollary 4. Let k be a field. Then the polynomial ring $k[x]$ is a PID and a UFD.

Proof. By example 3, $k[x]$ is a Euclidean domain and theorem 3 then gives the desired conclusions. □

Example 4. Since $\mathbb{Z}$ and $k[x]$ (where k is a field) are PIDs we see that $\mathrm{PSpec}(\mathbb{Z}) = \mathrm{Spec}(\mathbb{Z})$ and $\mathrm{PSpec}(k[x]) = \mathrm{Spec}(k[x])$.

Theorems 1 and 2 imply that $\mathfrak{p} = (f(x)) \subset k[x]$ is a prime ideal if $f(x)$ is an irreducible polynomial over k.

Example 5. Primes in $\mathbb{Z}[x]$.

Definition 8. Let $\mathfrak{D}$ be a UFD. Then a **greatest common divisor** between $a, b \in \mathfrak{D}^\circ$ is an element d such that $d \mid a$ and $d \mid b$, such that if $c \mid a$ and $c \mid b$, then $c \mid d$. We write $\gcd(a, b)$ for the element d.

Observe that we say *a* greatest common divisors. The reason is that gcd's are only defined up to multiples of units.

The existence of greatest common divisor that can be defined for $a, b \in \mathfrak{D}^\circ$ is not guaranteed in general. However,

Theorem 5. Let $\mathfrak{D}$ be a PID. Then for all non-zero $a, b \in \mathfrak{D}$ there is a greatest common divisor. In addition, a generalised Bézout's theorem holds: There are elements $x, y \in \mathfrak{D}$ such that

$$\gcd(a, b) = xa + ya.$$

Proof. Maybe someday. □

Corollary 6. If $\mathfrak{E}$ is a Euclidean domain, then there is also a Euclidean algorithm that finds the $\gcd(a, b)$.

I want to point out that it is not straightforward to deduce the corollary from theorem 5. Quite a lot of work is needed to prove the claim. But it should be said that the proof is constructive and so can be turned into a way to compute the gcd.

Finally, a definition that resembles the definition of Euclidean valuation.

Definition 9. A function $\mathrm{Nm} : \mathfrak{D} \to \mathbb{Z}$ such that

(i) $\mathrm{Nm}(a) \geq 0$, for all $a \in \mathfrak{D}$;

(ii) $\mathrm{Nm}(a) = 0 \iff a = 0$, and

(iii) $\mathrm{Nm}(ab) = \mathrm{Nm}(a)\mathrm{Nm}(b)$

is called a **(multiplicative) norm** on $\mathfrak{D}$.

Theorem 7. Let Nm be a norm on $\mathfrak{D}$. Then

(a) $\mathrm{Nm}(1) = 1$ and
$$a \in \mathfrak{D}^\times \implies \mathrm{Nm}(a) = 1;$$

(b) if
$$a \in \mathfrak{D}^\times \iff \mathrm{Nm}(a) = 1,$$
then any element $\boldsymbol{\pi} \in \mathfrak{D}^\times$ with norm $\mathrm{Nm}(\boldsymbol{\pi}) = p \in \mathrm{Spec}(\mathbb{Z})$, is an irreducible element of $\mathfrak{D}$.

Proof. We have, since Nm is multiplicative,

$$\mathrm{Nm}(1) = \mathrm{Nm}(1 \cdot 1) = \mathrm{Nm}(1)\mathrm{Nm}(1) \iff \mathrm{Nm}(1)\big(\mathrm{Nm}(1) - 1\big) = 0$$

from which it follows that $\mathrm{Nm}(1) = 1$ (the first factor cannot be 0 since $\mathrm{Nm}(a) = 0$ if and only if $a = 0$ by definition 9 (ii), and $1 \neq 0$).

Similarly, if $u \in \mathfrak{D}^\times$, then

$$1 = \mathrm{Nm}(1) = \mathrm{Nm}(u \cdot u^{-1}) = \mathrm{Nm}(u)\mathrm{Nm}(u^{-1})$$

so $\mathrm{Nm}(u^{-1}) = \mathrm{Nm}(u)^{-1}$, but since $\mathrm{im}(\mathrm{Nm}) \subseteq \mathbb{Z}$, we conclude that $\mathrm{Nm}(u) = 1$ for $u \in \mathfrak{D}^\times$.

Suppose finally that $\mathrm{Nm}(a) = 1$ implies $a \in \mathfrak{D}^\times$ for all $a \in \mathfrak{D}$, and take an element $\boldsymbol{\pi} \in \mathfrak{D}$ with $\mathrm{Nm}(\boldsymbol{\pi}) = p \in \mathrm{Spec}(\mathbb{Z})$. Assume that π is not irreducible. Then we can factor $\boldsymbol{\pi} = a \cdot b$, where neither a nor b is a unit. Taking norms gives

$$p = \mathrm{Nm}(\boldsymbol{\pi}) = \mathrm{Nm}(ab) = \mathrm{Nm}(a)\mathrm{Nm}(b).$$

Since p is prime we must have that either $\mathrm{Nm}(a) = 1$ or $\mathrm{Nm}(b) = 1$. But by hypothesis this implies that a or b is a unit, which is a contradiction to the assumption that $\boldsymbol{\pi}$ is not irreducible. □

3 ▷ The ring $\mathbb{Z}[\boldsymbol{i}]$, and sums of squares ◁

In this section we will prove a result of Euler (known by Fermat) that states precisely when a prime $p \in \mathrm{Spec}(\mathbb{Z})$ can be written as a sum of squares. In fact,

Theorem 8 (Euler)**.** A prime $p \in \mathrm{Spec}(\mathbb{Z})$ can be written as a sum of squares

$$p = a^2 + b^2$$

if and only if $p \equiv 1 \pmod 4$.

The journey to the proof of this theorem is just as satisfying as the result itself[(a)].

Definition 10. The ring

$$\mathfrak{G} := \mathbb{Z}[\sqrt{-1}] := \left\{ a + b\sqrt{-1} \;\middle|\; a, b \in \mathbb{Z} \right\} \subset \mathbb{C},$$

is called the **Gaussian integers**.

As is customary we put

$$\boldsymbol{i} := \sqrt{-1}.$$

The set $\mathfrak{G}$ is a **subring** of $\mathbb{C}$ and so one add and multiply exactly as is done in $\mathbb{C}$. However, $\mathfrak{G}$ is not a field so division is not defined.

Now, Let $z = a + b\boldsymbol{i}$. We define a norm on $\mathfrak{G}$ by

$$\mathrm{Nm}(z) := z \cdot \bar{z} = (a + b\boldsymbol{i})(a - b\boldsymbol{i}) = a^2 + b^2. \tag{1}$$

Observe that if $z \in \mathbb{Z}$, i.e., $z = a + 0\boldsymbol{i}$, then $\mathrm{Nm}(z) = a^2$.

It is easy to check (do this!) that the first condition in the definition of a norm is satisfied. The second is a bit more tricky.

Theorem 9. The function Nm given in (1) defines a norm and, therefore,

[(a)] It should be remarked that Euler didn't have the machinery used below at his disposal (this machinery is due to Gauss), and so Euler had another proof.

$\mathfrak{G}$ is a Euclidean ring.

In the process of proving this we will actually, in addition, prove that there is a **division algorithm** on $\mathfrak{G}$.

Proof. Let $a, b \in \mathbb{Z}$, with $a \geq b$. The first thing to observe is that any integer u is less than (or equal) to $\frac{1}{2}\|b\|$ from[(b)] any multiple, q, of b. Then $\|a - qb\| \leq \frac{1}{2}\|b\|$.

Put $r := a - qb$. From this follows

$$a = qb + r \text{ and } \|r\| \leq \frac{1}{2}\|b\|. \tag{2}$$

It is very important to observe that this is **not** the division algorithm on $\mathbb{Z}$, even if $a, b \in \mathbb{Z}$. Namely, we are not requiring $r < b$, only that $\|r\| \leq \|b\|$ (in fact, we can even take $\|r\| \leq 1/2\|b\|$ as argued above).

Now, take two elements $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathfrak{G}$, such that $\boldsymbol{\beta} \neq 0$. We now divide $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ and rewrite (using the arithmetic in $\mathbb{C}$)

$$\frac{\boldsymbol{\alpha}}{\boldsymbol{\beta}} = \frac{\boldsymbol{\alpha}\bar{\boldsymbol{\beta}}}{\boldsymbol{\beta}\bar{\boldsymbol{\beta}}} = \frac{\boldsymbol{\alpha}\bar{\boldsymbol{\beta}}}{\mathrm{Nm}(\boldsymbol{\beta})}. \tag{3}$$

Be sure to observe that $\boldsymbol{\alpha}/\boldsymbol{\beta} \notin \mathfrak{G}$. This is an element in

$$\mathbb{Q}(\boldsymbol{i}) := \left\{ x + y\boldsymbol{i} \in \mathbb{C} \;\middle|\; x, y \in \mathbb{Q} \right\} \subset \mathbb{C}.$$

We will come to this ring later.

Put

$$\frac{\boldsymbol{\alpha}\bar{\boldsymbol{\beta}}}{\mathrm{Nm}(\boldsymbol{\beta})} = \frac{u + v\boldsymbol{i}}{\mathrm{Nm}(\boldsymbol{\beta})}, \quad u, v \in \mathbb{Z}. \tag{4}$$

Then using equation (2) we can write

$$u = \mathrm{Nm}(\beta)q_u + r_u, \quad v = \mathrm{Nm}(\beta)q_v + r_v, \quad q_u, q_v \in \mathbb{Z},$$

and where

$$0 \leq r_u, r_v \leq \frac{1}{2}\|b\|.$$

Insertion of this into (3), using (4), gives

$$\frac{\boldsymbol{\alpha}}{\boldsymbol{\beta}} = \boldsymbol{\gamma} + \frac{r_u + r_v\boldsymbol{i}}{\mathrm{Nm}(\beta)}, \quad \boldsymbol{\gamma} := q_u + q_v\boldsymbol{i}.$$

Then

$$\boldsymbol{\rho} := \boldsymbol{\alpha} - \boldsymbol{\beta}\boldsymbol{\gamma} = \frac{r_u + r_v\boldsymbol{i}}{\mathrm{Nm}(\beta)},$$

implying that

$$\mathrm{Nm}(\boldsymbol{\rho}) = \mathrm{Nm}\big(\boldsymbol{\alpha} - \boldsymbol{\beta}\boldsymbol{\gamma}\big) = \mathrm{Nm}\left(\frac{r_u + r_v\boldsymbol{i}}{\mathrm{Nm}(\beta)}\right) = \frac{\mathrm{Nm}(r_u + r_v\boldsymbol{i})}{\mathrm{Nm}(\boldsymbol{\beta})}.$$

Put $\boldsymbol{y} := (r_u + r_v\boldsymbol{i})/\bar{\boldsymbol{\beta}}$. From this we compute

$$\boldsymbol{y}\bar{\boldsymbol{\beta}} = r_u + r_v\boldsymbol{i} \quad \Longrightarrow \quad \mathrm{Nm}(\boldsymbol{y}\bar{\boldsymbol{\beta}}) = \mathrm{Nm}(\boldsymbol{y})\mathrm{Nm}(\bar{\boldsymbol{\beta}}) = r_u^2 + r_v^2.$$

[(b)] The notation $\|b\|$ means absolute value.

This gives that

$$\mathrm{Nm}(\boldsymbol{\rho}) = \frac{r_u^2 + r_v^2}{\mathrm{Nm}(\beta)}.$$

Since $0 \leq r_u, r_v \leq \frac{1}{2}\|b\|$, we find that

$$\mathrm{Nm}(\boldsymbol{\rho}) \leq \frac{\frac{1}{4}\mathrm{Nm}(\boldsymbol{\beta})^2 + \frac{1}{4}\mathrm{Nm}(\boldsymbol{\beta})^2}{\mathrm{Nm}(\boldsymbol{\beta})} = \frac{1}{2}\mathrm{Nm}(\boldsymbol{\beta})$$

which is what we wanted to prove. □

Corollary 10. The Gaussian integers $\mathfrak{G}$ is a PID and hence also a UFD. Hence, there are greatest common divisors and, as a consequence, a corresponding Bézout theorem.

Recall the gcd's are only defined up to units.

Theorem 11. Let $\boldsymbol{\pi} \in \mathfrak{G}$. If $\mathrm{Nm}(\boldsymbol{\pi}) \in \mathrm{Spec}(\mathbb{Z})$, then $\boldsymbol{\pi}$ is a prime element.

Proof. Maybe someday. □

Corollary 12. For the ring $\mathfrak{G}$ we have:

$$a \in \mathfrak{G}^\times \iff \mathrm{Nm}(a) = 1.$$

Proof. This follows from theorem 11 and theorem 7 part (b). □

Lemma 2. We have $U(\mathfrak{G}) = \{\pm 1, \pm \boldsymbol{i}\}$.

Proof. Clearly, these elements are units. For instance, the inverse to $\boldsymbol{i}$ is $-\boldsymbol{i}$. Suppose now that $z = a + b\boldsymbol{i}$ is a unit. Then there is a z^{-1} such that $z \cdot z^{-1} = 1$, so $\mathrm{Nm}(z)\mathrm{Nm}(z^{-1}) = 1$. Therefore, since $\mathrm{Nm} : \mathfrak{G} \to \mathbb{Z}$, we must have that $\mathrm{Nm}(z) = \pm 1$. However, the norm is always positive so, $\mathrm{Nm}(z) = 1$. We see that $\mathrm{Nm}(z) = a^2 + b^2 = 1$. The only solutions to this equation are $z \in \{\pm 1, \pm \boldsymbol{i}\}$. □

Lemma 3. Let $a, b, c \in \mathfrak{G}$ such that $\gcd(a, b) = 1$. Then,

$$a \mid bc \quad \Longrightarrow \quad a \mid c.$$

Proof. The proof here is word-for-word the same as for $\mathbb{Z}$. □

Lemma 4. Let $\boldsymbol{\pi} \in \mathfrak{G}$ be a prime element. Then, for $a_1, a_2 \in \mathfrak{G}$ such

that $\boldsymbol{\pi} \mid a_1 a_2$, we have $\boldsymbol{\pi} \mid a_1$ or $\boldsymbol{\pi} \mid a_2$. An induction argument extends this to finitely many elements $a_1, a_2, \ldots, a_n \in \mathfrak{G}$.

Proof. Suppose that $\boldsymbol{\pi} \nmid a_1$. Since any greatest common divisor $d \in \mathfrak{G}$ between $\boldsymbol{\pi}$ and a, divides $\boldsymbol{\pi}$, i.e., $\boldsymbol{\pi} = kd$ for some $k \in \mathfrak{G}$, we see that k must be a unit because $\boldsymbol{\pi}$ is prime and thus have no non-unit factors. Therefore, $d = 1$ and hence $\gcd(a_1, \boldsymbol{\pi}) = 1$ and so the lemma follows from lemma 3. □

Lemma 5. Let $\boldsymbol{\pi} \in \mathfrak{G}$ be a prime element. Then there is some $p \in \operatorname{Spec}(\mathbb{Z})$ such that $\boldsymbol{\pi} \mid p$.

Proof. Observe first that $\boldsymbol{\pi}$ always divides its norm: $\operatorname{Nm}(\boldsymbol{\pi}) = \boldsymbol{\pi} \cdot \bar{\boldsymbol{\pi}} \in \mathbb{Z}_{\geq 1}$.

Since $\operatorname{Nm}(\boldsymbol{\pi})$ is a positive integer we can factor it as

$$\boldsymbol{\pi}\bar{\boldsymbol{\pi}} = \operatorname{Nm}(\boldsymbol{\pi}) = p_1 p_2 \cdots p_n,$$

not all p_i necessarily distinct. Therefore $\boldsymbol{\pi} \mid (p_1 p_2 \cdots p_n)$ and lemma 4 then shows that $\boldsymbol{\pi} \mid p_i$ for some p_i. □

Finally, we have the following theorem which is the crowning achievement concerning $\mathfrak{G}$:

Theorem 13. Let $p \in \operatorname{Spec}(\mathbb{Z})$.

(a) The following statements are equivalent:

  (i) $p = 2$ or $p \equiv 1 \pmod 4$;

  (ii) $x^2 \equiv -1 \pmod p$ has a solution;

  (iii) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

(b) The following statements hold in $\mathfrak{G}$:

  (i) $2 = (1 + \boldsymbol{i})(1 - \boldsymbol{i}) = -\boldsymbol{i}(1 + \boldsymbol{i})^2$;

  (ii) if $p \equiv 1 \pmod 4$ then $p = \boldsymbol{\pi}\bar{\boldsymbol{\pi}}$, where $\boldsymbol{\pi}$ is a prime;

  (iii) if $p \equiv 3 \pmod 4$ then p is prime in $\mathfrak{G}$.

(c) Every prime in $\mathfrak{G}$ can be written as a unit-multiple of the following primes

  (i) $1 + \boldsymbol{i}$;

  (ii) $\boldsymbol{\pi}$ or $\bar{\boldsymbol{\pi}}$ such that $\operatorname{Nm}(\boldsymbol{\pi}) = \boldsymbol{\pi}\bar{\boldsymbol{\pi}} = p \in \operatorname{Spec}(\mathbb{Z})$ and $p \equiv 1 \pmod 4$;

  (iii) $p \in \operatorname{Spec}(\mathbb{Z})$, where $p \equiv 3 \pmod 4$.

Note that $p \equiv 1 \pmod 4$ is equivalent to $p = 4k + 1$, for some $k \in \mathbb{Z}$ and $p \equiv 3 \pmod 4$ is equivalent to $p = 4k + 3$ (for some $k \in \mathbb{Z}$). Clearly there are no primes $p \geq 3$ satisfying $p \equiv 0, 2 \pmod 4$.

Proof. (a) To show that (i) implies (ii) we first note that $x = 1$ is a solution to the congruence when $p = 2$, so we can assume $p \neq 2$.

Since $p \neq 2$ the polynomial $t^{p-1} - 1$ can be factored

$$t^{p-1} - 1 = \big(t^{(p-1)/2} - 1\big)\big(t^{(p-1)/2} + 1\big).$$

A polynomial of degree d has at most d roots modulo p (why?).

Fermat's little theorem implies that $t^{p-1} - 1$ has $p - 1$ roots modulo p (namely, $\{1, 2, \ldots, p-1\}$). The polynomial $t^{(p-1)/2} - 1$ has at least one root ($t = 1$) and at most $(p-1)/2$. Hence the polynomial $t^{(p-1)/2} + 1$ has at least one root, say, a. In other words, $a^{(p-1)/2} = -1$. Since $p = 4k + 1$, $(p-1)/2 = 2k$, and so $a^{(p-1)/2} = a^{2k} = (a^k)^2 = -1$, which proves that (i) implies (ii).

That $x^2 \equiv -1 \pmod{p}$ is equivalent to $p \mid (x^2 + 1)$

$$p \mid (x^2 + 1) \iff p \mid (x - \boldsymbol{i})(x + \boldsymbol{i}).$$

If p is a prime in $\mathfrak{G}$, i.e., that $(p) \in \mathrm{Spec}(\mathfrak{G})$, we must have

$$p \mid (x - \boldsymbol{i}) \quad \text{or} \quad p \mid (x + \boldsymbol{i}).$$

Say, $p \mid (x - \boldsymbol{i})$. Then $x - \boldsymbol{i} = pc$ for some $c \in \mathfrak{G}$. Put $c = a + b\boldsymbol{i}$:

$$pc = p(a + b\boldsymbol{i}) = x - \boldsymbol{i} \quad \Longrightarrow \quad pb\boldsymbol{i} = -\boldsymbol{i} \iff pb = -1.$$

But since p is a prime in $\mathbb{Z}$, this is not possible. Hence p cannot be a prime in $\mathfrak{G}$ and so is composite.

Assume that $p = uv$ is decomposition of p in $\mathfrak{G}$. Then

$$\mathrm{Nm}(p) = \mathrm{Nm}(uv) = \mathrm{Nm}(u)\mathrm{Nm}(v) \iff p^2 = \mathrm{Nm}(u)\mathrm{Nm}(v).$$

Hence $\mathrm{Nm}(u) = \mathrm{Nm}(v) = p$. Otherwise one of $\mathrm{Nm}(u)$ and $\mathrm{Nm}(v)$ is 1 and, by corollary 12, this would imply that one of these is a unit. This is a contradiction to the assumption that p is a prime.

This means that, upon writing $u = a + b\boldsymbol{i}$,

$$p = \mathrm{Nm}(u) = a^2 + b^2.$$

Therefore p is a sum of squares and thus (ii) implies (iii).

Suppose now that $p = a^2 + b^2$, for some $a, b \in \mathbb{Z}$. Then we can factor p as

$$p = (a + b\boldsymbol{i})(a - b\boldsymbol{i}), \tag{5}$$

in other words, p is composite. Assume that $p \not\equiv 1 \pmod{4}$, i.e., $p \equiv 3 \pmod{4}$. This is then equivalent to $p = 4k + 3$ for some $k \in \mathbb{Z}$. It is easy to check that there is no way for $4k + 3$ to be a sum of two squares (try a and b with the different possible parities). Hence $p \equiv 1 \pmod{4}$ and this proves that (iii) implies (i), and so part (a) is proved.

(b) Part (i) is obvious. For part (ii) assume that $p \equiv 1 \pmod{4}$. Then p can be factored as in (5). Therefore, we need to prove that $\boldsymbol{\pi} = a + b\boldsymbol{i}$ and $\bar{\boldsymbol{\pi}} = a - b\boldsymbol{i}$ are primes. However, $\mathrm{Nm}(\boldsymbol{\pi}) = \mathrm{Nm}(\bar{\boldsymbol{\pi}}) = p$ and so theorem 11 implies that, indeed, both of these are primes. This also implies that if $p \equiv 3 \pmod{4}$ then p must be a prime in $\mathfrak{G}$, since otherwise we can factor into two conjugate prime elements by (ii).

(c) This a collection of theorems...

□

4 ▷ The field $\mathbb{Q}(\sqrt{d})$ and its ring of integers ◁

4.1 ◇ Definition ◇

Definition 11. Assume that the roots of the equation

$$y^2 + \alpha y + \beta = 0, \quad \alpha, \beta \in \mathbb{Z},$$

are non-rational. Let $\boldsymbol{\xi} \notin \mathbb{Q}$ be one of these. The two-dimensional $\mathbb{Q}$-vector space

$$\mathbb{Q}(\boldsymbol{\xi}) := \mathbb{Q} + \mathbb{Q} \cdot \boldsymbol{\xi} = \left\{ a + b\boldsymbol{\xi} \mid a, b \in \mathbb{Q} \right\}$$

is the **quadratic number field generated by** $\boldsymbol{\xi}$.

- The field $\mathbb{Q}(\boldsymbol{\xi})$ is a **quadratic field extension** of $\mathbb{Q}$ and we write $\mathbb{Q}(\boldsymbol{\xi})/\mathbb{Q}$ to denote this extension.
- The field is **imaginary** if $\boldsymbol{\xi}^2 < 0$ and **real** if $\boldsymbol{\xi}^2 > 0$.

When $\boldsymbol{\xi}$ is not necessary to make explicit we will often write K for $\mathbb{Q}(\boldsymbol{\xi})$.

The proof that $\mathbb{Q}(\boldsymbol{\xi})$ is indeed a field is left as an exercise.

Since

$$y^2 + \alpha x + \beta = \left(y + \frac{\alpha}{2}\right)^2 + \beta - \frac{\alpha^2}{4}$$

we can, by putting $z := y + \alpha/2$, assume that $\boldsymbol{\xi}$ is a solution to an equation on the form $y^2 = D$. In other words, we can assume that $\boldsymbol{\xi} = \sqrt{D}$ for some $D \in \mathbb{Z} \setminus \{0, 1\}$. Clearly, $D = \beta - \alpha^2/4$.

We will from now on always assume that $\boldsymbol{\xi} = \sqrt{D}$ for some square-free integer $D \neq 0, 1$.

Example 6. Clearly, when $\alpha = 0$ and $\beta = 1$, we get the field

$$\mathbb{Q}(\boldsymbol{i}) := \left\{ a + b\boldsymbol{i} \mid a, b \in \mathbb{Q} \right\}.$$

Observe that the Gaussian integers $\mathfrak{G} = \mathbb{Z}[\boldsymbol{i}]$ is a subring in $\mathbb{Q}(\boldsymbol{i})$.

Example 7. Put $\boldsymbol{\xi} = \sqrt{-3}$. Then $\mathbb{Q}(\boldsymbol{\xi})$ is an imaginary quadratic field.

The element

$$\boldsymbol{z} := \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\boldsymbol{\xi})$$

is a solution to the equation $y^2 + y + 1 = 0$. We have

$$\mathbb{Q}(\boldsymbol{z}) \subseteq \mathbb{Q}(\boldsymbol{\xi}).$$

A moment's thought will convince the reader that

$$\mathbb{Q}(\boldsymbol{z}) = \mathbb{Q}(\boldsymbol{\xi}).$$

Therefore, there can be many equations whose roots generate the same quadratic field.

There is a canonical automorphism

$$\mathsf{conj} : \mathbb{Q}(\boldsymbol{\xi}) \to \mathbb{Q}(\boldsymbol{\xi}), \quad a + b\boldsymbol{\xi} \;\mapsto\; a - b\boldsymbol{\xi}$$

on any quadratic field. This is an **involution**, meaning that $\mathsf{c}^2 = \mathrm{id}$. Therefore,

$$\mathsf{conj}^2(a + b\boldsymbol{\xi}) = \mathsf{conj}\big(\mathsf{conj}(a + b\boldsymbol{\xi})\big) = a + b\boldsymbol{\xi}.$$

As a consequence, the set $G := \{\mathrm{id}, \mathsf{conj}\}$ is a group, isomorphic to $\mathbb{Z}/2$, called the **Galois group** of the quadratic extension $\mathbb{Q}(\boldsymbol{\xi})/\mathbb{Q}$.

The element $\bar{\boldsymbol{z}} := \mathsf{conj}(\boldsymbol{z})$ is called the **conjugate** of $\boldsymbol{z} \in \mathbb{Q}(\boldsymbol{\xi})$.

4.2 ◇ The characteristic polynomial and the discriminant ◇

Let $\boldsymbol{z} = a + b\boldsymbol{\xi} \in \mathbb{Q}(\boldsymbol{\xi})$ be non-zero in order to avoid trivialities. The there is a unique (up to multiples) quadratic polynomial $P_{\boldsymbol{z}}(y) \in \mathbb{Q}[y]$ such that $P_{\boldsymbol{z}}(\boldsymbol{z}) = 0$. Indeed, remembering that $\boldsymbol{\xi}^2 = D$, this polynomial is

$$P_{\boldsymbol{z}}(y) = y^2 - 2ay + a^2 - b^2 D$$

as is easily checked. The polynomial $P_{\boldsymbol{z}}(y)$ is called the **characteristic polynomial** (or **minimal polynomial**) of $\boldsymbol{z}$.

A more conceptual definition is the following.

Definition 12. Let $\boldsymbol{z} \in \mathbb{Q}(\boldsymbol{\xi})$.

(i) Define $\mathrm{Tr}(\boldsymbol{z}) := \boldsymbol{z} + \bar{\boldsymbol{z}}$ and $\mathrm{N}(\boldsymbol{z}) := \boldsymbol{z}\bar{\boldsymbol{z}} = \boldsymbol{z} \cdot \mathsf{conj}(\boldsymbol{z})$, the **trace** and **norm** of $\boldsymbol{z}$, respectively. Then

$$P_{\boldsymbol{z}}(y) = y^2 - \mathrm{Tr}(\boldsymbol{z})y + \mathrm{N}(\boldsymbol{z}). \tag{6}$$

(ii) The **discriminant** of $\boldsymbol{z}$ is

$$\Delta(\boldsymbol{z}) := (\boldsymbol{z} - \bar{\boldsymbol{z}})^2 = \boldsymbol{z}^2 + \bar{\boldsymbol{z}}^2 - 2\mathrm{N}(\boldsymbol{z}) = 4b^2\mathrm{N}(\boldsymbol{z}).$$

Theorem 14. The norm and trace satisfy

$$\mathrm{Tr}(\boldsymbol{z}+\boldsymbol{w}) = \mathrm{Tr}(\boldsymbol{z}) + \mathrm{Tr}(\boldsymbol{w}), \quad \text{and} \quad \mathrm{N}(\boldsymbol{z}\boldsymbol{w}) = \mathrm{N}(\boldsymbol{z})\mathrm{N}(\boldsymbol{w}),$$

in other words, Tr is additive and N is multiplicative.

Proof. This is an easy exercise. □

Remark 2. Observe that following:

(i) $\mathrm{Tr}(\boldsymbol{z}), \mathrm{N}(\boldsymbol{z}) \in \mathbb{Q}$ (prove this!).

(ii) We are not claiming that N and Nm are somehow related. In fact, properties (ii) and (iii) in definition 9 are satisfied for N, but (i) is not always true. In fact, part (i) of definition 9 is true only for fields where where $D < 0$, i.e., for imaginary quadratic fields.

Theorem 15 (Cayley–Hamilton)**.** Viewing multiplication of $\boldsymbol{z}$ on the vector space $\mathbb{Q}(\boldsymbol{\xi})$ as a linear map, i.e.,

$$m_{\boldsymbol{z}} : \mathbb{Q}(\boldsymbol{\xi}) \to \mathbb{Q}(\boldsymbol{\xi}), \quad \boldsymbol{w} \longmapsto \boldsymbol{z}\cdot\boldsymbol{w},$$

then

$$P_{\boldsymbol{z}}(m_{\boldsymbol{z}}) = P_{\boldsymbol{z}}(\boldsymbol{z}) = 0.$$

Proof. Insert $\boldsymbol{z}$ into $P_{\boldsymbol{z}}$ and check that it becomes zero. □

4.3 ◇ Rings of integers ◇

Definition 13. Let $K = \mathbb{Q}(\boldsymbol{\xi})$ be a quadratic field. Then the **ring of (quadratic) integers** in K is the subring of K defined as

$$\begin{aligned}\mathfrak{O}_K &:= \Big\{\boldsymbol{z} \in \mathbb{Q}(\boldsymbol{\xi}) \;\Big|\; P(\boldsymbol{z}) = 0, \text{for some } \textit{monic } P(\boldsymbol{z}) \in \mathbb{Z}[y]_2\Big\} \\ &= \Big\{\boldsymbol{z} \in \mathbb{Q}(\boldsymbol{\xi}) \;\Big|\; \mathrm{Tr}(\boldsymbol{z}), \mathrm{N}(\boldsymbol{z}) \in \mathbb{Z}\Big\},\end{aligned}$$

where $\mathbb{Z}[y]_2$ denotes the set of all polynomial of degree two. That $\mathfrak{O}_K$ is indeed a ring follows from theorem 14 (check this!). The second equality follows from theorem 15.

Note that $\mathbb{Z} \subset \mathfrak{O}_K$ since every $a \in \mathbb{Z}$ is the solution to the equation $(y-a)^2 = 0$.

For an element $\boldsymbol{w} \in K = \mathbb{Q}(\boldsymbol{\xi})$, we put

$$\mathbb{Z}[\boldsymbol{w}] := \mathbb{Z} + \mathbb{Z}\boldsymbol{w} = \Big\{ a + b\boldsymbol{w} \mid a, b \in \mathbb{Z} \Big\}.$$

We now have the following explicit description of $\mathfrak{O}_K$.

Theorem 16. We have

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\boldsymbol{\xi}], & \text{if } D \equiv 2, 3 \,(\mathrm{mod}\, 4) \\ \mathbb{Z}\big[\frac{1+\boldsymbol{\xi}}{2}\big], & \text{if } D \equiv 1 \,(\mathrm{mod}\, 4). \end{cases}$$

Proof. Recall the assumption that D is square-free.

Clearly, both $\boldsymbol{\xi}$ and $(1 + \boldsymbol{\xi})/2$ lie in $\mathfrak{O}_K$ since they are solutions to the equations $y^2 - D = 0$ (in the first case) and $y^2 - y - (D-1)/4 = 0$ (in the second case), respectively. Hence,

$$\mathbb{Z}[\boldsymbol{\xi}] \subseteq \mathfrak{O}_K, \text{ for } D \equiv 2, 3 \,(\mathrm{mod}\, 4),$$

and

$$\mathbb{Z}\Big[\frac{1+\boldsymbol{\xi}}{2}\Big] \subseteq \mathfrak{O}_K, \text{ for } D \equiv 1 \,(\mathrm{mod}\, 4).$$

We thus have to prove the reverse inclusions.

Suppose $\boldsymbol{z} = a + b\boldsymbol{\xi} \in \mathfrak{O}_K$, for $a, b \in \mathbb{Q}$. We need to prove that we can take $a, b \in \mathbb{Z}$. Put $a = r/2$ and $b = m/n$, for some $r, m, n \in \mathbb{Z}$ where $\gcd(m, n) = 1$.

Then (check!)

$$\mathrm{N}(\boldsymbol{z}) = a^2 - b^2 D \iff 4m^2 D = n^2(r^2 - 4\mathrm{N}(\boldsymbol{z})).$$

This implies that

$$n^2 \mid 4m^2 D$$

and since $\gcd(m, n) = 1$ we must have that $n^2 \mid 4D$.

If n has a prime factor $p \geq 3$ then $p^2 \mid 4D$ gives a contradiction since D is square-free. Hence, n must be a power of 2, $n = 2^k$, implying that $2^{2k} \mid 4D$. There is at most one factor 2 in D since D is square-free, so k is either 0 or 1, showing that n is either 1 or 2. Therefore, we can write $b = m/2$ for some m.

Since $\mathrm{N}(\boldsymbol{z}) = a^2 - b^2 D \in \mathbb{Z}$, we find that

$$\frac{r^2}{4} - \frac{m^2 D}{4} = k \iff r^2 \equiv m^2 D \,(\mathrm{mod}\, 4). \tag{7}$$

Now, the congruence $D \equiv 2, 3 \,(\mathrm{mod}\, 4)$ is equivalent to $D = 4l + i$, where $i = 2, 3$. Putting this into (7), we find that r^2 and m^2 must both be congruent to zero modulo 4. Consequently, r and m are even. The assumption that $a = r/2$ and $b = m/2$ means that $a, b \in \mathbb{Z}$ and so $\boldsymbol{z} \in \mathbb{Z}[\boldsymbol{\xi}]$ when $D \equiv 2, 3 \,(\mathrm{mod}\, 4)$.

On the other, if $D \equiv 1 \,(\mathrm{mod}\, 4) \iff D = 4l + 1$, we get from (7) that $r^2 \equiv m^2 \,(\mathrm{mod}\, 4)$, implying that $r \equiv m \,(\mathrm{mod}\, 2)$. Hence, $r = m + 2s$ for some $s \in \mathbb{Z}$ and so

$$\boldsymbol{z} = a + b\boldsymbol{\xi} = \frac{r}{2} + \frac{m\boldsymbol{\xi}}{2} = \frac{m + 2s}{2} + \frac{m\boldsymbol{\xi}}{2} = s + m\frac{1 + \boldsymbol{\xi}}{2} \in \mathbb{Z}\Big[\frac{1+\boldsymbol{\xi}}{2}\Big],$$

completing the proof. □

Remark 3. It is probably advisable to issue a warning at this point. In the case where $D \equiv 1 \,(\mathrm{mod}\, 4)$ we see that $(1+\boldsymbol{\xi})/2 \in \mathfrak{O}_K$. This does *not* mean that $1/2 \in \mathfrak{O}_K$. Indeed, suppose we had $1/2 \in \mathfrak{O}_K$. Then there would exist $a, b \in \mathbb{Z}$ such that

$$\frac{1}{2} = a + b\frac{1+\boldsymbol{\xi}}{2} \iff 2a + b + b\boldsymbol{\xi} = 1.$$

Since there is no $\boldsymbol{\xi}$ on the right-hand side, we must have $b = 0$. However, this would imply that $2a = 1$, which is a contradiction to the fact that $a \in \mathbb{Z}$.

Definition 14. It is convenient to put

$$\boldsymbol{\lambda} := \begin{cases} \boldsymbol{\xi}, & \text{if } D \equiv 2, 3 \,(\mathrm{mod}\, 4) \\ \frac{1+\boldsymbol{\xi}}{2}, & \text{if } D \equiv 1 \,(\mathrm{mod}\, 4), \end{cases}$$

calling this the **universal generator** for $\mathfrak{O}_K$. Observe that

$$\mathbb{Q}(\boldsymbol{\lambda}) = \mathbb{Q}(\boldsymbol{\xi})$$

(ref. example 7).

We note

Lemma 6. The norm of the universal generator is given as

$$\mathrm{N}(\boldsymbol{\lambda}) := \begin{cases} D, & \text{if } D \equiv 2, 3 \,(\mathrm{mod}\, 4) \\ \frac{1-D}{4}, & \text{if } D \equiv 1 \,(\mathrm{mod}\, 4). \end{cases}$$

Definition 15. The **discriminant** of $\mathbb{Q}(\boldsymbol{\xi})$ (or $\mathfrak{O}_K$) is defined as

$$\Delta := \begin{cases} 4\boldsymbol{\lambda}, & \text{if } D \equiv 2, 3 \,(\mathrm{mod}\, 4) \\ \boldsymbol{\lambda}, & \text{if } D \equiv 1 \,(\mathrm{mod}\, 4). \end{cases}$$

It is now possible to unify the two cases in theorem 16 (check this!):

Corollary 17. We have

$$\mathfrak{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{\Delta + \sqrt{\Delta}}{2},$$

where Δ is the discriminant of $\mathfrak{O}_K$.

5 ▷ Ideal theory for quadratic fields ◁

There are several statements in this section that are left without proofs (at least for now). An interested reader can look up these in any book on algebraic number theory.

5.1 ◇ Modules, lattices and ideals ◇

Recall that a vector space V over a field k is an abelian group such that for every $\boldsymbol{u} \in V$ and $a \in k$, we have that $a\boldsymbol{u} \in V$. We will now generalise this by replacing k by an arbitrary commutative ring.

Definition 16. Let $\mathfrak{R}$ be a commutative ring and $M = (M, +)$ an abelian group. Then M is an **$\mathfrak{R}$-module**, or a **module over $\mathfrak{R}$** if the following axioms hold:

(M1) for all $r \in \mathfrak{R}$ and all $\boldsymbol{u} \in M$,

$$r\boldsymbol{u} \in M \quad \text{and} \quad \boldsymbol{u}r \in M;$$

(M2) for all $r \in \mathfrak{R}$ and all $\boldsymbol{u}, \boldsymbol{v} \in M$,

$$r(\boldsymbol{u} + \boldsymbol{v}) = r\boldsymbol{u} + r\boldsymbol{v}, \quad \text{and} \quad (\boldsymbol{u} + \boldsymbol{v})r = \boldsymbol{u}r + \boldsymbol{v}r;$$

(M3) for all $r, s \in \mathfrak{R}$ and all $\boldsymbol{u} \in M$,

$$(r + s)\boldsymbol{u} = r\boldsymbol{u} + s\boldsymbol{u};$$

(M4) for all $\boldsymbol{u} \in M$

$$1 \cdot \boldsymbol{u} = \boldsymbol{u} \cdot 1 = \boldsymbol{u}.$$

Clearly a vector space over k is a k-module. In addition, $\mathfrak{R}$ is itself an $\mathfrak{R}$-module. Here are a couple of less trivial example.

Example 8. Let $I \subseteq \mathfrak{R}$ be an ideal. Then I is an $\mathfrak{R}$-module. Indeed, an equivalent definition of an ideal is as a a subset of $\mathfrak{R}$ that is also an $\mathfrak{R}$-module. Recall that, if $1 \in I$, then $I = \mathfrak{R}$ and so we get the $\mathfrak{R}$ viewed as a module over itself.

Example 9. Once again, let $I \subset \mathfrak{R}$ be an ideal. Then $\mathfrak{R}/I$ is an $\mathfrak{R}$-module: let $m = r + I \in \mathfrak{R}/I$, and let $s \in \mathfrak{R}$. Then

$$s \cdot m = s(r + I) = sr + sI = sr + I \in \mathfrak{R}/I,$$

since I is an ideal. The verification that the other axioms are satisfied is left as an exercise for the reader.

For a concrete example, consider $\mathfrak{R} = k[y]$ and $I = (f(y))$. Recall that if $f(y)$ is irreducible, I is a prime ideal (and also maximal since $k[y]$ is a PID. (Hence, $\mathfrak{R}/I$ is a field extension of k.) It is important to observe that, for $P(y) \in k[y]$,

$$P(y) \longmapsto R(y) \in \mathfrak{R}/I, \quad P(y) = Q(y)f(y) + R(y) \quad \text{(division algorithm)}.$$

Hence $\deg(R(y)) < \deg(f(y))$.

This means that $P(y)$ acts on $q(y) + (f(y))$ as

$$P(y)\big(q(y) + (f(x))\big) = R(y)q(y) + (f(y)) = r(y) + (f(y)),$$

where $R(y)q(y) = r(y) + g(y)f(y)$ for some $g(y) \in k[y]$.

The above looks more complicated than it is. The only thing to remember is that when we multiply elements from $\mathfrak{R}$ with elements in $\mathfrak{R}/I$ we must reduce modulo I.

For instance, let $f(y) = y^2 + 11$ in $\mathfrak{R} = \mathbb{Q}[y]$. This gives that

$$\mathfrak{R}/(f(y)) = \mathbb{Q}[y]/(y^2 + 11) = \mathbb{Q}(\boldsymbol{\xi}), \quad \boldsymbol{\xi}^2 = -11,$$

i.e., $\mathfrak{R}/I$ is a quadratic field.

Now, let $P(y) \in \mathfrak{R}$ and let $r(\boldsymbol{\xi})$ be its reduction modulo $f(y) = y^2 + 11$ (i.e., the residue of $P(y)$ modulo $(y^2 + 11)$). Note that $y \mapsto \boldsymbol{\xi}$ under the reduction. Hence,

$$P(y) \cdot (a + b\boldsymbol{\xi}) = r(\boldsymbol{\xi})(a + b\boldsymbol{\xi}) = a' + b'\boldsymbol{\xi},$$

where we have killed all multiples of $f(y) = y^2 + 11$ (reducing modulo $f(y)$).

Suppose $P(y) = y^3 - 7y - 2$, then

$$\begin{aligned}(y^3 + 7y - 2) \cdot (5 - 3\boldsymbol{\xi}) &= (y \cdot y^2 + 3y^2 - 2) \cdot (5 - 3\boldsymbol{\xi}) \\ &= (\boldsymbol{\xi} \cdot 11 + 7\boldsymbol{\xi} - 2) \cdot (5 - 3\boldsymbol{\xi}) \\ &= (14\boldsymbol{\xi} - 2) \cdot (5 - 3\boldsymbol{\xi}) \\ &= 70\boldsymbol{\xi} - 42\boldsymbol{\xi}^2 - 10 + 6\boldsymbol{\xi} \\ &= -472 + 76\boldsymbol{\xi}.\end{aligned}$$

Observe that the equalities are taken modulo $y^2 + 11$.

The following example is important.

Example 10. Suppose $\mathfrak{R} = \mathbb{Z}$ and let $W := \{\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n\} \subset \mathbb{C}$. The **lattice** spanned by W is the $\mathbb{Z}$-module

$$\Lambda = \mathbb{Z}\boldsymbol{w}_1 + \mathbb{Z}\boldsymbol{w}_2 + \cdots + \mathbb{Z}\boldsymbol{w}_n.$$

This means that if $\boldsymbol{z} \in \Lambda$ then

$$\boldsymbol{z} = a_1\boldsymbol{w}_1 + a_2\boldsymbol{w}_2 + \cdots + a_n\boldsymbol{w}_n.$$

Note that $\Lambda \subset \mathbb{C}$.

Now, assume that $\mathfrak{R} = \mathfrak{O}_K = \mathbb{Z}[\boldsymbol{\lambda}]$ for K a quadratic number field. The $\mathbb{Z}$-module

$$\Lambda_{\boldsymbol{\lambda}} := \mathbb{Z} \cdot 1 + \mathbb{Z}\boldsymbol{\lambda} = \mathbb{Z} + \mathbb{Z}\boldsymbol{\lambda} \subset \mathbb{C}$$

is a lattice in $\mathbb{C}$. In addition, it is an $\mathfrak{O}_K$-module: for $\boldsymbol{z} = a + b\boldsymbol{\lambda} \in \mathfrak{O}_K$, we have

$$\boldsymbol{z}(u + v\boldsymbol{\lambda}) = (a + b\boldsymbol{\lambda})(u + v\boldsymbol{\lambda}) = au + bv\boldsymbol{\lambda}^2 + (av + bu)\boldsymbol{\lambda}.$$

Observe that this is essentially tautological. Recall that

$$\boldsymbol{\lambda}^2 = \begin{cases} D, & \text{if } D \equiv 2, 3 \pmod 4 \\ \boldsymbol{\lambda} + \frac{D-1}{4}, & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

so

$$\boldsymbol{z}(u + v\boldsymbol{\lambda}) = \begin{cases} au + bvD + (av + bu)\boldsymbol{\lambda}, & \text{if } D \equiv 2, 3 \pmod 4 \\ \left(au + \frac{bv(D-1)}{4}\right) + (av + bu + bv)\boldsymbol{\lambda}, & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

We won't prove the following two lemmas.

Lemma 7. Let Λ be a lattice

$$\Lambda = \mathbb{Z}\boldsymbol{z}_1 + \mathbb{Z}\boldsymbol{z}_2 \subseteq \mathfrak{O}_K = \mathbb{Z} + \mathbb{Z}\boldsymbol{\lambda}.$$

Then there are $n, m \in \mathbb{Z}_{\geq 1}$ and $a \in \mathbb{Z}$, such that

$$\Lambda \simeq \mathbb{Z}n + \mathbb{Z}(a + m\boldsymbol{\lambda})$$

as a lattice.

Lemma 8 (Ideals and lattices)**.** The lattice $\Lambda = \mathbb{Z}n + \mathbb{Z}(a + b\boldsymbol{\lambda})$ is an ideal if and only if

$$b \mid a, \quad b \mid n, \quad \text{and} \quad n \mid \big(b \cdot \mathrm{N}(m + \boldsymbol{\lambda})\big),$$

where m is the unique integer satisfying $a = mb$.

Observe that there can be non-principal ideals in $\mathfrak{O}_K$. Hence $\mathfrak{O}_K$ is not, in general, a PID.

If $\mathfrak{a} = \mathbb{Z}n + \mathbb{Z}(a + b\boldsymbol{\lambda})$ is an ideal we use the equivalent notations

$$\mathfrak{a} = \mathbb{Z}n + \mathbb{Z}(a + b\boldsymbol{\lambda}) \iff \mathfrak{a} = \big(n, a + b\boldsymbol{\lambda}\big).$$

Definition 17. Let $\mathtt{S}, \mathtt{T} \subset \mathfrak{R}$ be two subsets in a ring $\mathfrak{R}$. Then the product of $\mathtt{S}$ and $\mathtt{T}$ is defined as

$$\mathtt{S} \cdot \mathtt{T} := \Big\{ s_1t_1 + s_2t_2 + \cdots + s_nt_n \;\Big|\; s_i \in \mathtt{S},\, t_i \in \mathtt{T} \Big\} \subset \mathfrak{R}.$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, then so is $\mathfrak{a} \cdot \mathfrak{b}$ and, since both $\mathfrak{a}$ and $\mathfrak{b}$ are ideals,

$$\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a}, \quad \mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{b}.$$

The reader should convince him- herself of this.

Definition 18. Assume that $\mathfrak{a} \subset \mathfrak{O}_K$ is an ideal, then we define the **conjugate ideal** to be

$$\bar{\mathfrak{a}} := \big\{ \bar{a} \mid a \in \mathfrak{a} \big\}.$$

The **norm** of $\mathfrak{a}$ is defined as the ideal

$$\mathrm{N}(\mathfrak{a}) = \mathfrak{a} \cdot \bar{\mathfrak{a}}.$$

Observe that this is an ideal (ref. definition 17). Clearly, $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\bar{\mathfrak{a}})$, and if $\mathfrak{a} = (a)$, then

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}((a)) = (a)(\bar{a}) = (a)(a) = (a^2).$$

Lemma 9. The norm of $\mathfrak{a}$ is a principal ideal, $\mathrm{N}(\mathfrak{a}) = (a)$, $a \in \mathfrak{O}_K$. In addition,

$$\mathrm{N}(\mathfrak{a}) = \big(\#(\mathfrak{O}_K/\mathfrak{a})\big).$$

The last claim of lemma 9 is actually the general definition of the ideal norm. However, for quadratic fields this is equivalent to the one given in definition 18.

We will often be sloppy and write $\mathrm{N}(\mathfrak{a}) = a$.

5.2 ◇ Unique factorisation of ideals ◇

Theorem 18. Let $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{O}_K)$ be a prime ideal. Then there is a unique prime $p \in \mathrm{Spec}(\mathbb{Z})$ such that

$$\mathfrak{p} \mid (p), \text{ i.e., such that } (p) \subset \mathfrak{p}.$$

We will often write $\mathfrak{p} \mid p$ instead of $\mathfrak{p} \mid (p)$.

Proof. Factor $\mathrm{N}(\mathfrak{p}) = p_1 p_2 \cdots p_n$. Since $\mathrm{N}(\mathfrak{p}) = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ we see that

$$\mathfrak{p} \cdot \bar{\mathfrak{p}} = p_1 p_2 \cdots p_n \iff \mathfrak{p} \mid p_1 p_2 \cdots p_n \iff (p_1 p_2 \cdots p_n) \subset \mathfrak{p}.$$

There is no restriction in assuming that $n = 2$. Hence assume $p_1 p_2 \in \mathfrak{p}$, with $p_1 \neq p_2$.

Since $\mathfrak{p}$ is a prime ideal we have that $p_1 \in \mathfrak{p}$ or $p_2 \in \mathfrak{p}$. Suppose both p_1 and p_2 are in $\mathfrak{p}$. This implies that, for all $a, b \in \mathbb{Z}$, $ap_1 + bp_2 \in \mathfrak{p}$. However, $p_1 \neq p_2$ so $\gcd(p_1, p_2) = 1$ and by Bézout's identity there are $x, y \in \mathbb{Z}$ such that $xp_1 + yp_2 = 1$. Hence, $1 \in \mathfrak{p}$ which implies that $\mathfrak{p} = \mathfrak{O}_K$, which is a contradiction. □

From lemma 8 and theorem 18, we see that if $\mathfrak{p}$ is prime, then n in lemma 8 must be p where $\mathfrak{p} \mid p$.

Example 11. Let $K = \mathbb{Q}(\sqrt{-5})$. Theorem 16 implies that

$$\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}.$$

We can observe the factorisations

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}). \tag{8}$$

The factors here are all irreducible. Indeed, suppose, for instance $7 = ab$ for some $a, b \in \mathfrak{O}_K$. Then $\mathrm{N}(7) = \mathrm{N}(a)\mathrm{N}(b)$ implies that $\mathrm{N}(a) = \pm 7$. If $a = a_1 + a_2\sqrt{-5}$, we get $a_1^2 - 5a_2^2 = \pm 7$. This is easily seen to have no solution for $a_1, a_2 \in \mathbb{Z}$. Similarly, if $(1 + 2\sqrt{-5}) = ab$, we get

$$\mathrm{N}(1 + 2\sqrt{-5}) = \mathrm{N}(a)\mathrm{N}(b) \iff -19 = \mathrm{N}(a)\mathrm{N}(b).$$

However 19 is a prime so either $\mathrm{N}(a) = \pm 19$ and $\mathrm{N}(b) = \mp 1$ or vice versa. Just as above, these lead to equations that are not solvable over $\mathbb{Z}$.

As a consequence the factors in (8) are irreducible. They are also not associates since neither of the factors are invertible in $\mathfrak{O}_K$. Therefore the two factorisations in (8) are unique and so $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Even though it is not in general possible to uniquely factor *elements* it is always possible to factor *ideals*.

Theorem 19. Let $\mathfrak{a}$ be an ideal in $\mathfrak{O}_K$. Then there is *unique* set of primes

$$\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\} \subset \mathrm{Spec}(\mathfrak{O}_K)$$

such that

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

This theorem is proved in much greater generality in the last section.

A natural question is: how do we recognise the elements in $\mathrm{Spec}(\mathfrak{O}_K)$? We have already remarked that a necessary condition for

$$\mathfrak{p} = (n, a + b\boldsymbol{\lambda}) = \mathbb{Z}n + \mathbb{Z}(a + b\boldsymbol{\lambda})$$

to be prime, is that $n = p$ and that $b = \pm 1$ or $b = \pm p$ (cf. lemma (8)). Hence we can assume that $b = 1$ since

$$\mathfrak{p} = \mathbb{Z}n + \mathbb{Z}(a + b\boldsymbol{\lambda}) = b(\mathbb{Z}(n/b) + \mathbb{Z}(a/b + \boldsymbol{\lambda}))$$

(What on earth do I mean here???)

We will answer the above question fully in the next section.

6 ▷ Ramification and Quadratic Reciprocity ◁

Recall theorem 13, parts of which we restate and reformulate here for easy reference:

Theorem 20. Let $K = \mathbb{Q}(\boldsymbol{i})$. Since $-1 \equiv 3 \pmod 4$, we see that

$$\mathfrak{O}_K = \mathbb{Z}[\boldsymbol{i}] = \mathfrak{G}.$$

Let $p \in \mathrm{Spec}(\mathbb{Z})$.

(a) The following statements are equivalent:

(i) $p = 2$ or $p \equiv 1 \pmod 4$;
(ii) $y^2 \equiv -1 \pmod p$ has a solution;
(iii) $p = a^2 + b^2 = (a + b\boldsymbol{i})(a - b\boldsymbol{i}) \in \mathbb{Z}[\boldsymbol{i}]$.

(b) In addition,

(i) $2 = (1 + \boldsymbol{i})(1 - \boldsymbol{i}) = -\boldsymbol{i}(1 + \boldsymbol{i})^2$;
(ii) if $p \equiv 1 \pmod 4$ then $p = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p} \in \mathrm{Spec}(\mathbb{Z}[\boldsymbol{i}])$ is a prime;
(iii) if $p \equiv 3 \pmod 4$ then $p \in \mathrm{Spec}(\mathbb{Z}[\boldsymbol{i}])$.

We would like to generalise this to all quadratic number fields. The problem is that the proof of the above theorem hinged crucially on the property that $\mathbb{Z}[\boldsymbol{i}]$ is a Euclidean ring, a property that is very rare among the rings $\mathfrak{O}_K$.

First, note that the splitting behaviour of p in $\mathbb{Z}[\boldsymbol{i}]$ is connected to the solution of the equation $y^2 + 1 = 0$ in $\mathbb{F}_p$. Note also that $\Delta(\mathbb{Z}[\boldsymbol{i}]) = -4$. Hence, for $p \neq 2$, part (a) in the theorem can be reformulated as (check!)

$$p = (a + b\boldsymbol{i})(a - b\boldsymbol{i}) \iff \left(\frac{\Delta}{p}\right) = 1 \iff p \equiv 1 \pmod 4.$$

The aim now is to extend, as much as possible, these equivalences to all quadratic number fields.

6.1 ◇ Ramification ◇

Recall that, by convention, $(a/p) = 1$ is equivalent to $y^2 = a$ has two *distinct* solutions in $\mathbb{F}_p$. If $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{O}_K)$ then $\bar{\mathfrak{p}} \in \mathrm{Spec}(\mathfrak{O}_K)$.

Theorem 21. Let $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$ be a quadratic number field with ring of integers $\mathfrak{O}_K$ and $p \in \mathrm{Spec}(\mathbb{Z})$ an *odd* prime. Then,

(a)
$$\left(\frac{\Delta}{p}\right) = 1 \quad \Longrightarrow \quad p = \mathfrak{p}\bar{\mathfrak{p}}, \quad \text{for some } \mathfrak{p} \in \mathrm{Spec}(\mathfrak{O}_K),$$
with $\mathfrak{p} \neq \bar{\mathfrak{p}}$;

(b)
$$\left(\frac{\Delta}{p}\right) = -1 \quad \Longrightarrow \quad p \in \mathrm{Spec}(\mathfrak{O}_K),$$

(c) or, if $p \mid \Delta$, then $p = \mathfrak{p}^2$ for some $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{O}_K)$.

Observe that the three cases are mutually exclusive.

Definition 19. In the (distinct) cases in theorem 21 above, the prime p is said to be, respectively, **split** (or **unramified**), **inert** or **ramified** in $\mathfrak{O}_K$.

Proof. □

The following is a specialisation to quadratic number fields of a theorem due to Dedekind.

Theorem 22. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field with ring of integers $\mathfrak{O}_K$. Put $P(y) = y^2 - D$.

The reduction $\bar{P}(y)$ of $P(y)$ modulo p is either irreducible over $\mathbb{F}_p$ or factor into two (not necessarily unique) linear factors.

(a) If $p \neq 2$, then

(i) $\bar{P}(y)$ is irreducible over $\mathbb{F}_p$, implies that $p \in \mathrm{Spec}(\mathfrak{O}_K)$;

(ii) $\bar{P}(y) = (y + a)(y - a)$, implies
$$p = (p, a + \boldsymbol{\lambda})(p, a - \boldsymbol{\lambda}) = (\mathbb{Z}p + \mathbb{Z}(a + \boldsymbol{\lambda}))(\mathbb{Z}p + \mathbb{Z}(a - \boldsymbol{\lambda})),$$
and

(iii) $\bar{P}(y) = (y + a)^2$, implies that $p = (p, a + \boldsymbol{\lambda})^2$.

(b) If $p = 2$, then either $2 \in \mathrm{Spec}(\mathfrak{O}_K)$ or $2 = \mathfrak{p}^2$ for some $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{O}_K)$.

The theorem follows from theorem 21 and lemma 8.

The representations of the primes in theorem 22 are *not* unique. For instance, in $K = \mathbb{Q}(\sqrt{7})$, the ideals $(13, -8-3\sqrt{7}) = (13, 5+10\sqrt{7})$, since $-8 \equiv 5 \pmod{13}$ and $-3 \equiv 10 \pmod{13}$.

6.2 ◇ Quadratic Reciprocity, again ◇

6.3 ◇ Prime ideals and Spec($\mathfrak{O}_K$) ◇

6.4 ◇ The Zariski topology on Spec($\mathfrak{O}_K$) ◇

6.5 ◇ Fractional and invertible ideals ◇

Definition 20. A **fractional ideal** Λ is an $\mathfrak{O}_K$-module on the form

$$\Lambda = \mathfrak{O}_K \boldsymbol{w}_1 + \mathfrak{O}_K \boldsymbol{w}_2 + \cdots + \mathfrak{O}_K \boldsymbol{w}_n \subset K, \quad \boldsymbol{w}_i \in K.$$

Observe that Λ need not be a subset of $\mathfrak{O}_K$. A fractional ideal inside $\mathfrak{O}_K$ is an ordinary ideal.

The **inverse** to Λ is the module

$$\Lambda^{-1} := \left\{ \boldsymbol{z} \in K \;\middle|\; \boldsymbol{z} \cdot \Lambda \subseteq \mathfrak{O}_K \right\} \subset K.$$

Note that (check this!)

$$\Lambda \cdot \Lambda^{-1} = (1) = \mathfrak{O}_K,$$

justifying the term "inverse".

If one needs to be very specific at some point one often use the term **integral ideal** for ideals in $\mathfrak{O}_K$.

It is not obvious that the definition of Λ^{-1} makes sense. In other words that Λ^{-1} is also a fractional ideal. For simplicity we will grant this as a fact.

6.6 ◇ The class group ◇

7 ▷ Number fields and relative field extensions ◁

Theorem 23. Let $\mathfrak{a}$ be an ideal in $\mathfrak{O}_K$. Then there is *unique* set of primes

$$\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\} \subset \operatorname{Spec}(\mathfrak{O}_K)$$

such that

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

Lemma 10. For every ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Lemma 11. Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$. Define

$$\mathfrak{p}^{-1} := \{a \in K \mid a \cdot \mathfrak{p} \subseteq \mathfrak{O}_K\}.$$

Then $\mathfrak{a} \cdot \mathfrak{p}^{-1} \neq \mathfrak{a}$ for every non-zero ideal $\mathfrak{a}$ in $\mathfrak{O}_K$. Notice that $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1}$ since $1 \in \mathfrak{p}^{-1}$.

Proof of Lemma 10. Let $\mathtt{S}$ be the set of all ideals such that the statement of the lemma does not hold, and assume that $\mathtt{S}$ is non-empty. Since $\mathfrak{O}_K$ is noetherian the set $\mathtt{S}$ must have a maximal element, $\mathfrak{a}$. Furthermore, $\mathfrak{a}$ cannot be a prime ideal so there are $b, c \in \mathfrak{O}_K$ such that $bc \in \mathfrak{a}$ but $b \notin \mathfrak{a}$, $c \notin \mathfrak{a}$. Clearly, $\mathfrak{a} \subset \mathfrak{a}+(b)$, $\mathfrak{a} \subset \mathfrak{a} + (c)$ and $(\mathfrak{a} + (b))(\mathfrak{a} + (c)) \subseteq \mathfrak{a}$. Since $\mathfrak{a}$ is maximal with respect to not containing a product of prime ideals, $\mathfrak{a} + (b)$ and $\mathfrak{a} + (c)$ do. But this together with $(\mathfrak{a} + (b))(\mathfrak{a} + (c)) \subseteq \mathfrak{a}$ implies that $\mathfrak{a}$ also does, a contradiction. □

Proof of Lemma 11. Let $a \in \mathfrak{p}$, $a \neq 0$. Then by the previous lemma there are primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$. We can assume that r is the smallest possible such that this is true. Then one of the $\mathfrak{p}_i$'s, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$ since if not, then we could choose $a_j \in \mathfrak{p} \setminus \mathfrak{p}_j$ with $a_1 \cdots a_r \in \mathfrak{p}$; but since $\mathfrak{p}$ is prime, $a_j \in \mathfrak{p}$, for some j, a contradiction. This implies that $\mathfrak{p}_1 = \mathfrak{p}$ since $\mathfrak{p}_1$ is maximal. We have that $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$, so there is a $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin a\mathfrak{O}_K$, i.e., $a^{-1}b \notin \mathfrak{O}_K$. However, we have that $b\mathfrak{p} \subseteq (a)$ so $a^{-1}b\mathfrak{p} \subseteq \mathfrak{O}_K$, implying that $a^{-1}b \in \mathfrak{p}^{-1}$, so $\mathfrak{p}^{-1} \neq \mathfrak{O}_K$.

Let $\mathfrak{a}$ be a non-zero ideal with generators $a_1, \ldots, a_n$ (since $\mathfrak{O}_K$ is noetherian every ideal is finitely generated, another standard fact of noetherian rings). Assume that $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{a}$. Then for every $b \in \mathfrak{p}^{-1}$ we have

$$ba_i = \sum_j A_{ij} a_j, \quad \text{where } A_{ij} \in \mathfrak{O}_K.$$

This is equivalent to

$$\begin{pmatrix} b - A_{11} & -A_{12} & \ldots & -A_{1n} \\ -A_{21} & b - A_{22} & \ldots & -A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -A_{n1} & -A_{n2} & \ldots & b - A_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \mathbf{0}.$$

Denote the square-matrix by W. By Cramer's rule we get

$$\det(W)a_1 = \det(W)a_2 = \cdots = \det(W)a_n = 0, \quad \Longrightarrow \quad \det(W) = 0.$$

Hence b is integral over $\mathfrak{O}_K$ (expand $\det(W)$); so $b \in \mathfrak{O}_K$ since $\mathfrak{O}_K$ is integrally closed, and thus $\mathfrak{p}^{-1} = \mathfrak{O}_K$, a contradiction. Therefore, $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$ and the proof is finished. □

Now we can prove Theorem 23.

Proof of Theorem 23. We begin by showing existence. Let $\mathtt{S}$ be the set of proper non-zero ideals that cannot be decomposed into prime ideals. The same argument as in the proof of Lemma 10 shows that there is a maximal element $\mathfrak{a} \in \mathtt{S}$. This ideal is not prime so is included in a prime (maximal) ideal[(c)] $\mathfrak{p}$.

[(c)] This is a fact from ring theory (following from Zorn's lemma): every ideal is contained in a maximal ideal.

We get

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K.$$

However, Lemma 11 shows that $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$ strictly. Since $\mathfrak{p}$ is maximal (notice that $\mathfrak{a}\mathfrak{p}^{-1}$ is an ideal for all non-zero ideals $\mathfrak{a}$) we must have that

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}_K.$$

Clearly, $\mathfrak{a} \neq \mathfrak{p}$ implies that $\mathfrak{a}\mathfrak{p} \neq \mathfrak{O}_K$, hence, taking into account the maximality of $\mathfrak{a}$ in $\mathtt{S}$ and $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$, the ideal $\mathfrak{a}\mathfrak{p}^{-1}$ admits a prime decomposition

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \quad \text{and then so does} \quad \mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n,$$

a contradiction.

To show uniqueness assume that $\mathfrak{a}$ can be decomposed as

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_m.$$

The definition of prime ideals can be re-phrased as

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p} \quad \Longleftrightarrow \quad \mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \text{ or } \mathfrak{p} \mid \mathfrak{b}.$$

Now, $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_m$ implies that $\mathfrak{p}_1 | \mathfrak{q}_i$ for some $1 \leq i \leq m$. Since $\mathfrak{p}_1$ is maximal, $\mathfrak{p}_1 = \mathfrak{q}_i$. Hence, multiplying with $\mathfrak{p}_1^{-1}$ and using that $\mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathfrak{O}_K$, we can cancel $\mathfrak{p}_1 = \mathfrak{q}_i$. Continuing like this shows that $n = m$ and exactly one of the $\mathfrak{q}_j$'s correspond to a given $\mathfrak{p}_i$. The proof is finished. □