Chapter 2
A Crash Course in Ring Theory

2.1 Basic Definitions

In $\mathbb{Z}$ we can add, subtract, and multiply without restrictions, but we can't always divide. That is what makes questions of divisibility and factorization interesting. To do arithmetic in more general number systems, we abstract these basic properties of $\mathbb{Z}$ to get the definition of a ring.

2.1.1 Definition. *A* **ring** $(R, +, \cdot)$ *is a set* R *with two binary operations (usually termed addition and multiplication) satisfying the following three axioms:*

(a) $(R, +)$ *is an abelian group with identity element* 0_R.
(b) The operation $\cdot$ *is associative, commutative and has an identity* 1_R*, such that* $1_R \cdot a = a$*, for all* $a \in R$*;*
(c) Multiplication distributes over addition: for all $a, b, c \in R$*, we have* $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

A **subring** of R is a subset $S \subseteq R$ that contains 1_R and is closed under addition, additive inverses, and multiplication. This makes S a ring in its own right under the operations inherited from R, with $1_S = 1_R$. Unless confusion is possible, we'll drop the subscript and write 0 and 1 for 0_R and 1_R.

2.1.2 Definition. *A* **unit** *in* R *is an element* $a \in R$ *for which there exists a* $b \in R$ *such that* $ab = 1$.

The b in the Definition is unique and is called the multiplicative inverse of a, denoted a^{-1}. The set of all units is a group under multiplication, denoted $R^\times$.

2.1.3 Example. Let $R = \mathbb{Z}[\sqrt{2}]$. It's easy to see that $\varepsilon = 1 + \sqrt{2}$ is a unit in R:

$$-\mathrm{N}\varepsilon = \varepsilon(-\bar{\varepsilon}) = (1 + \sqrt{2})(-1 + \sqrt{2}) = 1.$$

M. Trifković, *Algebraic Theory of Quadratic Numbers*, Universitext,
DOI 10.1007/978-1-4614-7717-4_2, © Springer Science+Business Media New York 2013

We claim that the powers of ε are all distinct, and thus form an infinite set of units in $\mathbb{Z}[\sqrt{2}]$. Indeed, if $\varepsilon^k = \varepsilon^l$, then $\varepsilon^{k-l} = 1$. This can only be true if $k = l$: otherwise, ε would be one of the two real roots of 1, namely 1 or -1. □

Particularly simple and important are rings such as $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, in which we can divide by any nonzero element.

2.1.4 Definition. *A ring F is a* **field** *if every nonzero element is invertible, i.e., $F^\times = F \setminus 0$.*

The focus of this book will be fields of the form $\mathbb{Q}[\sqrt{D}]$.

Exercises

2.1.1. Decide which of the following are subrings of $\mathbb{C}$. Do you see a pattern?

(a) $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{2}}{2}$
(b) $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{3}}{2}$
(c) $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{5}}{2}$
(d) $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-7}}{2}$
(e) $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-11}}{2}$

2.1.2. Let R and S be rings. Show that componentwise addition and multiplication make $R \times S = \{(r, s) : r \in R, s \in S\}$ into a ring.

2.1.3. Prove that the ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n = p$, a prime. When we want to emphasize that we are considering $\mathbb{Z}/p\mathbb{Z}$ as a field, rather than merely an abelian group, we write $\mathbb{F}_p$ instead of $\mathbb{Z}/p\mathbb{Z}$.

2.1.4. Let R be a ring. For $n \in \mathbb{Z}$ and $a \in R$, we formally define the following intuitive operation: $n{\cdot}a = \underbrace{a + \cdots + a}_{n \text{ times}}$ if $n > 0$, $0{\cdot}a = 0_R$, and $n{\cdot}a = (-n){\cdot}(-a)$ if $n < 0$. We define the **characteristic of** R, denoted $\operatorname{char} R$, as follows. If $n \cdot 1_R \neq 0_R$ for all $n \in \mathbb{Z} \setminus 0$, we put $\operatorname{char} R = 0$. Otherwise, $\operatorname{char} R$ is the smallest positive integer n for which $n \cdot 1_R = 0$.

(a) Find the characteristics of the following rings: (a) $\mathbb{C}$; (b) $\mathbb{Z}/n\mathbb{Z}$; (c) $(\mathbb{Z}/n\mathbb{Z})[x]$; (d) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
(b) For a field F, prove that $\operatorname{char} F$ is 0 or a prime number.

2.1.5. Here we get to know a noncommutative ring that will make a cameo appearance in our investigations.

(a) For $k \in \mathbb{N}$, let $M_{k\times k}(\mathbb{Z})$ be the set of $k \times k$ matrices with entries in $\mathbb{Z}$, equipped with the usual matrix addition and multiplication. Show that $(M_{k\times k}(\mathbb{Z}), +, \cdot)$ satisfies all the ring axioms except the commutativity of multiplication.

(b) A unit in $M_{k\times k}(\mathbb{Z})$ is any a with a *two-sided* inverse: $ab = ba = 1$ for some $k \times k$ matrix b. Denote the unit group $M_{k\times k}(\mathbb{Z})^\times$ by $\mathrm{GL}_k(\mathbb{Z})$. Prove that

$$GL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, \quad ad - bc = \pm 1 \right\}.$$

(c) Find a necessary and sufficient condition for $a, b \in \mathbb{Z}$ to appear in the top row of a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in GL_2(\mathbb{Z})$.

2.2 Ideals, Homomorphisms, and Quotients

In Ch. 1 we hinted at the importance of ideals to arithmetic. Their role in ring theory is analogous to that of normal subgroups in group theory.

2.2.1 Definition. *Let R be a ring. An* **ideal** *$I \subseteq R$ is an additive subgroup that absorbs multiplication: if $a \in R$ and $x \in I$, then $ax \in I$.*

Most of the ideals in this book will be of the form $\mathbb{Z}\alpha + \mathbb{Z}\beta = \{m\alpha + n\beta : m, n \in \mathbb{Z}\}$ for some $\alpha, \beta \in \mathbb{C}$, termed generators.

2.2.2 Example. We will show that $I = \mathbb{Z} \cdot 7 + \mathbb{Z}(3 + \sqrt{-5})$ absorbs multiplication by $\mathbb{Z}[\sqrt{-5}]$. It suffices to check that $\sqrt{-5}I \subseteq I$, which we check on the generators:

$$\sqrt{-5} \cdot 7 = (-3) \cdot 7 + 7(3 + \sqrt{-5}) \in I$$
$$\sqrt{-5} \cdot (3 + \sqrt{-5}) = -5 + 3\sqrt{-5} = -2 \cdot 7 + 3(3 + \sqrt{-5}) \in I. \qquad \square$$

We're also interested in functions that respect the ring structure.

2.2.3 Definition. *Given rings R and S, a function $\varphi : R \to S$ is a* **ring homomorphism** *if it meets the following conditions for any $a, b \in R$:*

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$
(b) $\varphi(ab) = \varphi(a)\varphi(b)$
(c) $\varphi(1_R) = 1_S$

If φ is one-to-one and onto, it is called a **ring isomorphism**. If an isomorphism exists between two rings R and S, we say they are **isomorphic** and write $R \cong S$.

The notion of kernel links ideals and ring homomorphisms.

2.2.4 Definition. *The* **kernel** *of a ring homomorphism $\varphi : R \to S$ is*

$$\ker \varphi = \{a \in R : \varphi(a) = 0_S\}.$$

It's easy to check that $\ker\varphi$ is an ideal. It measures how far φ is from being injective, in the sense that φ is one-to-one if and only if $\ker\varphi = 0_R$. When φ is onto, we can reconstruct it from its kernel by means of the quotient ring construction.

Given a ring R and its ideal I, we define an equivalence relation $\sim$ on R by $a \sim b$ if $a - b \in I$. The equivalence class of $a \in R$ is the **coset** $a + I = \{a + x : r \in I\}$. The set of all cosets, i.e., the partition of R defined by $\sim$, is denoted by $R/I = \{a + I : a \in R\}$.

2.2.5 Proposition-Definition (Definition of a Quotient Ring)**.** *Let I be an ideal of a ring R. The expressions*

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = (ab) + I$$

are well-defined operations that make R/I into a ring.

The function $\pi : R \to R/I$ defined by $\pi(a) = a + I$ is a surjective ring homomorphism.

Proof. When we write an element of R/I as $a + I$, we are in fact choosing a representative of this coset, namely a. Any other $a' \in a + I$ would do, as $a' + I = a + I$. We need to check that the two operations, defined in terms of arbitrary coset representatives, in fact depend only on the cosets themselves.

We do this for multiplication, and leave the rest to you. If $a + I = a' + I$ and $b + I = b' + I$, we need to show that $ab + I = a'b' + I$. By the definition of cosets as equivalence classes, we have $a - a', b - b' \in I$. As I absorbs multiplication, we get, as desired, $ab - a'b' = a(b - b') + b'(a - a') \in I$. ■

2.2.6 Theorem (First Isomorphism Theorem for Rings)**.** *Let $\varphi : R \to S$ be a ring homomorphism. The assignment $a + \ker\varphi \mapsto \varphi(a)$ gives a well-defined ring isomorphism $\tilde{\varphi} : R/\ker\varphi \to \varphi(R)$ that satisfies $\varphi = \pi \circ \tilde{\varphi}$. We say that $\tilde{\varphi}$ is* **induced** *from φ.*

2.2.7 Example. Take $R = \mathbb{Z}$ and $I = 5\mathbb{Z}$. We usually think of $\mathbb{Z}/5\mathbb{Z}$ as the set $\{0, 1, 2, 3, 4\}$. To reduce $a \in \mathbb{Z}$ modulo 5, we find $5k \in 5\mathbb{Z}$ for which $a + 5k \in \{0, 1, 2, 3, 4\}$. □

This generalizes to computing an arbitrary quotient R/I. Since $a + I = a + x + I$ for all $x \in I$, we look for an $x \in I$ that makes $a + x$ as simple as possible. We often refer to $a + I$ as "a modulo I."

2.2.8 Example. It's not hard to check that $I = \mathbb{Z} \cdot 11 + \mathbb{Z}(4 - \sqrt{5})$ is an ideal of the ring $R = \mathbb{Z}[\sqrt{5}]$. Fix $a = k + l\sqrt{5} \in R$, and look for $x = m \cdot 11 + n(4 - \sqrt{5}) \in I$ for which

$$a + x = (k + 11m + 4n) + (l - n)\sqrt{5}$$

is as simple as possible. A natural choice would be to take $n = l$, so that $a + x$ is in fact in $\mathbb{Z}$. That integer changes by a multiple of 11 as we vary m. We pick

m so that $k+4l+11m \in \{0, 1, 2, \ldots, 10\}$. Thus, each coset has a representative in $\{0, 1, 2, \ldots, 10\}$, which strongly suggests (but doesn't prove!) that $R/I \cong \mathbb{Z}/11\mathbb{Z}$.

For a rigorous proof we use Thm. 2.2.6 and look for a surjective ring homomorphism $\varphi : R \to \mathbb{Z}/11\mathbb{Z}$ with kernel I. Any such homomorphism satisfies $\varphi(\sqrt{5})^2 = \varphi(5) = 5 \pmod{11}$. Since $4^2 \equiv 5 \pmod{11}$, we can easily check that $\varphi(x+y\sqrt{5}) = x+4y \pmod{11}$ is the desired ring homomorphism.

To illustrate, let's reduce $\alpha = 2 + 3\sqrt{5}$ modulo I. Here $k = 2, l = 3$, so $n = 3$ and $m = -1$: $(2 + 3\sqrt{5}) + ((-1) \cdot 11 + 3(4 - \sqrt{5})) = 3$. Thus, $\alpha \equiv 3 \pmod{I}$, which we also see from $\varphi(2 + 3\sqrt{5}) = 2 + 3 \cdot 4 \equiv 3 \pmod{11}$. □

2.2.9 Example. Now take $R = \mathbb{Z}[i], I = 3\mathbb{Z}[i] = \mathbb{Z} \cdot 3 + \mathbb{Z} \cdot 3i$. Take $a = k + li \in R$ and look for $x = 3m + 3ni \in I$ which makes

$$a + x = (k + 3m) + (l + 3n)i$$

as simple as possible. We can't always kill the imaginary part, but we can make it $0, 1$, or 2. We similarly adjust the real part to get

$$R/I \cong \{k + li : k, l \in \{0, 1, 2\}\},$$

at least as sets. In fact, $R/I \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, the isomorphism being induced, as in Thm. 2.2.6, by the homomorphism

$$\varphi : R \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \varphi(k + li) = (k \bmod 3, l \bmod 3). \qquad \square$$

In both examples, we're really only determining the additive group structure of the quotient R/I. Its multiplication is determined by the multiplication in R, as in Prop.-Def. 2.2.5. We will develop a systematic method for computing similar quotients in Sec. 3.4 .

Exercises

2.2.1. Let $X \subseteq R$ be an arbitrary subset. Prove that the smallest ideal containing X, called the ideal **generated** by X, is given by

$$\langle X \rangle = \left\{ \sum_{i=1}^{k} r_i x_i : k \in \mathbb{N}, r_i \in R, x_i \in X \right\}.$$

2.2.2. Let $R = \mathbb{Z}[\sqrt{19}]$ and put $I_b = \mathbb{Z} \cdot 5 + \mathbb{Z}(b + \sqrt{19})$ for $b \in \{0, 1, 2, 3, 4\}$. Which of the five I_b are ideals of R?

2.2.3. Find all values of $a \in \mathbb{N}$ for which $\mathbb{Z} \cdot a + \mathbb{Z}(9 + \sqrt{26})$ is an ideal of the ring $R = \mathbb{Z}[\sqrt{26}]$.

2.2.4. Let $\varphi : R \to S$ be a ring homomorphism. Show φ is injective if and only if $\ker \varphi = 0$.

2.2.5. Let R be a ring. Show that there is exactly one ring homomorphism $\varphi : \mathbb{Z} \to R$, and that $\operatorname{char} R$ (see Exer. 2.1.4) is the non-negative generator of the ideal $\ker \varphi$.

2.2.6. Let R be a ring with p elements, for p prime. Show that R is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

2.2.7.* Let R be a ring of prime characteristic p. Show that the function from R to itself given by $a \mapsto a^p$ is a ring homomorphism, called the **Frobenius endomorphism**.

2.2.8. Prove Prop.-Def. 2.2.5 and Thm. 2.2.6.

2.2.9. Let $\sigma\colon R \to S$ be a *surjective* ring homomorphism, and I be an ideal of R. Show that the assignment $a + I \mapsto (\sigma a) + \sigma(I)$ gives a well-defined ring homomorphism $\sigma \mod I\colon R/I \to S/\sigma(I)$.

2.2.10. Let I be an ideal of a ring R, and let $\pi : R \to R/I$ be the ring homomorphism from Prop.-Def. 2.2.5. Prove that the assignment $J \mapsto \pi^{-1}J$ gives a bijection between the set of ideals of R/I and the set of ideals of R containing I.

2.2.11. For both examples Ex. 2.2.8 and Ex. 2.2.9, check that φ is an onto ring homomorphism with kernel I. Find all other such homomorphisms.

2.2.12. In Ex. 2.2.9, we determined the additive group structure of $\mathbb{Z}[i]/3\mathbb{Z}[i]$. Write down its multiplication table, as determined by Prop.-Def. 2.2.5. (Since we know multiplication is commutative, you only need to fill in half the table.) What are the units in $\mathbb{Z}[i]/3\mathbb{Z}[i]$?

2.2.13. Given a ring R and a subset $I \subseteq R$ below, prove that I is an ideal. Then imitate Ex. 2.2.8 to guess the quotient R/I, prove your guess is correct using the first isomorphism Theorem 2.2.6, and finally reduce the given α modulo I:

(a) $R = \mathbb{Z}[\sqrt{22}],\ I = \mathbb{Z} \cdot 7 + \mathbb{Z}(1 + \sqrt{22}),\ \alpha = 5 - 4\sqrt{22}$
(b) $R = \mathbb{Z}[\sqrt{46}],\ I = \mathbb{Z} \cdot 23 + \mathbb{Z}\sqrt{46},\ \alpha = -15 + 29\sqrt{46}$

2.2.14. This is the first in a series of exercises that show how ideals resolve the failure of unique factorization of 6 in $\mathbb{Z}[\sqrt{-5}]$, Ex. 1.5.4, along the lines envisaged by Kummer.

(a) Show that the following sets are ideals of $\mathbb{Z}[\sqrt{-5}]$:

$$P_1 = \mathbb{Z} \cdot 2 + \mathbb{Z}(1 + \sqrt{-5}),$$
$$P_2 = \mathbb{Z} \cdot 3 + \mathbb{Z}(1 + \sqrt{-5}),$$
$$P_3 = \mathbb{Z} \cdot 3 + \mathbb{Z}(-1 + \sqrt{-5}).$$

(b) For any $X \subseteq \mathbb{C}$, we put $\bar{X} = \{\bar{z} : z \in X\}$. Show that $\bar{P_1} = P_1$ and $\bar{P_2} = P_3$.
(c) Compute the quotient $\mathbb{Z}[\sqrt{-5}]/P_i$ for $i = 1, 2, 3$. (Continued in Exer. 2.3.6.)

2.2.15. Let F be a field. List all ideals of F. Deduce that any ring homomorphism from F to a ring R is injective.

2.2.16. Let K be a subfield of L.

(a) Prove that L is a K-vector space.
(b) Let $f\colon L \to L$ be a ring homomorphism. Prove that f is a K-linear transformation if and only if $f(k) = k$ for all $k \in K$.
(c) Assume $\dim_K L < \infty$. Let $f\colon L \to L$ be a ring homomorphism fixing K pointwise as in part (b). Prove f is bijective, and therefore is a ring isomorphism.

2.2.17. Let F be a field with finitely many elements. By Exer. 2.1.4(b), $\operatorname{char} F = p$, a positive prime. Exer. 2.2.5 then defines a ring homomorphism $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$. Deduce from this, using Exer. 2.2.16, that F has p^n elements, for some n.

2.3 Principal Ideals

Divisibility in a general ring R is just as interesting as in $\mathbb{Z}$. For $a, b \in R$, we say that a **divides** b, written $a \mid b$, if $b = ac$ for some $c \in R$. If an ideal I of R contains a, then by the absorption property it must contain all elements divisible by a. In other words, $Ra \subseteq I$, where

$$Ra = \{ra : r \in R\}.$$

It's easy to check that Ra is itself an ideal, hence the smallest ideal containing a.

2.3.1 Definition. *An ideal I of R is a* **principal ideal** *if $I = Ra$ for some $a \in R$. Any such a is called a* **generator** *of I.*

If the ring R is fixed, we sometimes write $\langle a \rangle$ for Ra, in keeping with Exer. 2.2.1. When $R = \mathbb{Z}$ and the generator is a specific number, we follow tradition and write the generator on the left, e.g., $3\mathbb{Z}$ instead of $\mathbb{Z}3$.

2.3.2 Example. Let R be the ring $\mathbb{Z}[\sqrt{-5}]$. We claim that its ideal $I = \mathbb{Z} \cdot 7 + \mathbb{Z}(3 + \sqrt{-5})$ from Ex. 2.2.2 is not principal. If I had a generator α, we could find $\gamma, \delta \in R$ such that

$$7 = \gamma\alpha \text{ and } 3 + \sqrt{-5} = \delta\alpha.$$

Taking the norm, we get two multiplicative identities in $\mathbb{Z}$,

$$49 = \mathrm{N}\gamma \cdot \mathrm{N}\alpha \text{ and } 14 = \mathrm{N}\delta \cdot \mathrm{N}\alpha,$$

which imply $\mathrm{N}\alpha \mid \gcd(49, 14) = 7$. The equation $\mathrm{N}(x + y\sqrt{-5}) = x^2 + 5y^2 = 7$ has no solution in $\mathbb{Z}$, so $\mathrm{N}\alpha = 1$, α is a unit, and $I = R\alpha = R$. To arrive at

a contradiction, it suffices to show that $1 \notin I$. This is because the equation $1 = a \cdot 7 + b(3 + \sqrt{-5})$ has for its only solution $a = 1/7 \notin \mathbb{Z}$ and $b = 0$. □

The notion of a principal ideal is most useful when dealing with rings similar to $\mathbb{Z}$.

2.3.3 Definition. *A ring $\mathcal{D}$ is an* **integral domain** *if it has no zero-divisors: for all $a, b \in \mathcal{D}$ with $ab = 0$, we have $a = 0$ or $b = 0$.*

Integral domains are precisely the rings in which **cancellation** holds: for all $a, b, c \in \mathcal{D}$ with $a \neq 0$, $ab = ac$ implies $b = c$. Any subring of a field F is an integral domain: the equality $ab = ac$ remains valid in F, where we can cancel a by multiplying both sides by $a^{-1} \in F$. For an example of a ring that isn't an integral domain, consider $\mathbb{Z}/6\mathbb{Z}$: in it, $2 \cdot 3 = 0$, while $2 \neq 0$ and $3 \neq 0$.

You can easily check the following basic properties of principal ideals.

2.3.4 Proposition. *Let R be a ring and $a, b \in R$.*

(a) $Ra = R$ if and only if $a \in R^\times$.
(b) The following three statements are equivalent: (i) $a \mid b$; (ii) $b \in Ra$; (iii) $Rb \subseteq Ra$.
(c) Assume that R is an integral domain. Then $Ra = Rb$ if and only if $a = bu$, for some $u \in R^\times$.

2.3.5 Definition. *A* **principal ideal domain (PID)** *is an integral domain in which every ideal is principal.*

The prototypical PID is $\mathbb{Z}$. Other familiar PIDs include any field F, as well as its polynomial ring $F[x]$. In fact, all three satisfy the stronger property of having a version of the division algorithm.

2.3.6 Definition. *Let $\mathcal{D}$ be an integral domain. A* **Euclid size** *on $\mathcal{D}$ is a function $\nu : \mathcal{D} \setminus 0 \to \mathbb{Z}_{\geq 0}$ with the following property: for any $a, b \in \mathcal{D}, b \neq 0$, there exist $q, r \in \mathcal{D}$ such that $a = bq + r$, and either $r = 0$ or $\nu(r) < \nu(b)$. The integral domain $\mathcal{D}$ is called a* **Euclid domain** *if there exists a Euclid size on it.*[1]

2.3.7 Example. Here are the Euclid sizes for the three families of PIDs mentioned before Def. 2.3.6:

(a) $\nu : \mathbb{Z} \setminus 0 \to \mathbb{Z}_{\geq 0}, \quad \nu(n) = |n|$
(b) $\nu : F \setminus 0 \to \mathbb{Z}_{\geq 0}, \quad \nu(x) = 1$
(c) $\nu : F[x] \setminus 0 \to \mathbb{Z}_{\geq 0}, \quad \nu(f(x)) = \deg f(x)$

In the last example, the degree of the zero polynomial is not defined, which is why the general definition excludes 0 from the domain of ν. □

[1] This is slightly nonstandard terminology. A Euclid size is commonly termed a "Euclidean norm," and a ring equipped with one a "Euclidean domain/" We prefer the term "Euclid size" to avoid confusion with the field norm $N\alpha = \alpha\bar{\alpha}$.

The argument of Lemma 1.2.11 for $\mathbb{Z}[i]$ generalizes to show that an arbitrary Euclid domain is a PID. Indeed, the proofs of unique factorization in $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ all follow the following outline:

$$\text{Division algorithm} \Rightarrow \text{All ideals are principal} \Rightarrow \text{Euclid's algorithm} \Rightarrow \text{Euclid's lemma} \Rightarrow \text{Unique factorization.}$$

This train of thought proves unique factorization in both a Euclid domain and a PID; the Euclid domain merely boards it at the first stop (the division algorithm), the PID at the second. Since there are many more PIDs than Euclid domains, we will organize our study of arithmetic around the question, when is the ring of integers in a quadratic field a PID? For an example of a PID that can't be equipped with a Euclid size, see Exer. 2.3.9.

Exercises

2.3.1. Show $\mathcal{D}$ is an integral domain if and only if $ab = ac$ implies $b = c$ for all $a, b, c \in \mathcal{D}, a \neq 0$.

2.3.2. Prove Prop. 2.3.4

2.3.3.* For a nonsquare $D \in \mathbb{Z}$, prove that $\mathbb{Q}[\sqrt{D}] \cong \mathbb{Q}[x]/\langle x^2 - D\rangle$.

2.3.4. Put $\delta = \frac{1+\sqrt{-23}}{2}$ and $R = \mathbb{Z} + \mathbb{Z}\delta$.

(a) Prove that R is a ring.
(b) Prove that $I = \mathbb{Z} \cdot 3 + \mathbb{Z}(1 - \delta)$ is an ideal of R.
(c) Prove that I isn't principal.

2.3.5. Let $R = \mathbb{Z}[\sqrt{2}]$. Find $\alpha, \beta \in R$ for which $\langle 3 - 7\sqrt{2}\rangle = \mathbb{Z}\alpha + \mathbb{Z}\beta$.

2.3.6. Prove that the ideals P_1, P_2, P_3 from Exer. 2.2.14 are all nonprincipal. (Continued in Exer. 2.4.7.)

2.3.7. Show that the three functions of Ex. 2.3.7 are indeed Euclid size functions on their respective rings.

2.3.8. Let $\mathcal{D}$ be a Euclid domain with size function $\nu : \mathcal{D} \setminus 0 \to \mathbb{Z}_{\geq 0}$.

(a) One often additionally requires that $\nu(a) \leq \nu(ab)$ for all $a, b \in \mathcal{D} \setminus 0$, and calls such a ν a **strong Euclid size**. If $\mathcal{D}$ is a Euclid domain with size ν, show that the formula

$$\nu'(a) = \min\{\nu(ax) : x \in \mathcal{D} \setminus 0\}$$

defines a strong Euclid size on $\mathcal{D}$. We may therefore assume that every Euclid domain has a strong Euclid size without losing generality.
(b) Under that assumption, put $m = \min\{\nu(a) : a \in \mathcal{D} \setminus 0\}$. Describe the set of elements of smallest size, $\{u \in \mathcal{D} \setminus 0 : \nu(u) = m\}$.

2.3.9.* In this exercise, we show that $\mathcal{D} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is not a Euclid domain. We argue by contradiction, assuming that there is a strong Euclid size ν on $\mathcal{D}$.

(a) Find $\mathcal{D}^\times$.
(b) Show that 2 and 3 are irreducible in $\mathcal{D}$.
(c) Let $a \in \mathcal{D}$ have the second-smallest size, i.e., next-smallest after the m of Exer. 2.3.8(b). What does Exer. 2.3.8(b) tell you about the size of $\mathcal{D}/\mathcal{D}a$?
(d) Deduce a contradiction to (b) by showing that $a \mid 2$ or $a \mid 3$.

We will see in Ex. 5.4.3 that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID.

2.3.10. Let K be an arbitrary field. Use the division algorithm on $K[x]$ to show that a polynomial of degree d in $K[x]$ can have at most d roots in K.

2.3.11. Let K be a finite field. Since $K^\times$ is a finite abelian group, it is isomorphic to a product of cyclic groups,

$$K^\times \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}, \tag{2.3.8}$$

where the $d_i \in \mathbb{N}$ satisfy $d_r \mid d_{r-1} \mid \cdots \mid d_1$. We will show that $K^\times$ is cyclic by showing that $d_1 = |K^\times|$, and therefore $i = 1$.

Assume that $d_1 < |K^\times|$. Then by (2.3.8), we have that $x^{d_1} = 1$ for all $x \in K^\times$. Show that this contradicts Exer. 2.3.10

2.4 Operations on Ideals

We will extend various multiplicative notions from ring elements to ideals, much as Kummer envisaged for his ideal numbers. Our first definition is motivated by Prop. 2.3.4(b).

2.4.1 Definition. *Let I and J be ideals of a ring R. If $J \subseteq I$, we say that I* **divides** *J and write $I \mid J$. In the special case when $J = Ra$ is principal, we write $I \mid a$ for the equivalent statements $I \mid Ra$ and $a \in I$.*

"Divide and con(tain)" is a mnemonic to help you remember that $I \mid J$ is simply an alternative notation for $I \supseteq J$. The redundancy allows us to systematically translate statements about divisibility of numbers into conjectures about containment of ideals, which are usually easier to prove.

2.4.2 Example. Consider the transitivity of divisibility in $\mathbb{Z}$:

$$\text{If } a \mid b \text{ and } b \mid c, \text{then } a \mid c. \tag{2.4.3}$$

A plausible generalization to ideals I, J, K in a ring R would be:

$$\text{If } I \mid J \text{ and } J \mid K, \text{then } I \mid K. \tag{2.4.4}$$

This statement is merely *analogous* to the true statement (2.4.3). To prove it, we replace | with $\supseteq$, which reduces (2.4.4) to the usual transitivity of inclusion

$$\text{If } I \supseteq J \text{ and } J \supseteq K, \text{then } I \supseteq K.$$

For more examples, see Exer. 2.4.5. □

To extend the analogy between ideals and numbers, we define some multiplication-related operations on ideals in R.

2.4.5 Definition. *For two ideals I and J of R, we define the following sets, each of which is itself an ideal:*

$$\begin{aligned} I + J &= \{x + y : x \in I, y \in J\} \\ I \cap J &= \{x : x \in I \text{ and } x \in J\} \\ IJ &= \{\textstyle\sum_{i=1}^{m} x_i y_i : x_i \in I, y_i \in J\}. \end{aligned}$$

Remarks:

(a) The ideal $I + J$ is the smallest ideal containing both I and J. In the language of divisibility, it is the biggest ideal dividing both. We therefore think of $I + J$ as the greatest common divisor of I and J (and *not* as the analogue of addition of numbers).
(b) In particular, if $I + J = R$, we say that I and J are **relatively prime ideals**. This happens if and only if there exist $x \in I$ and $y \in J$ with $x + y = 1$.
(c) Similarly, we think of $I \cap J$ as the least common multiple of I and J.
(d) The definition of IJ is the least transparent of the lot. You might be tempted to define the product of I and J as the *set* of all products xy, where $x \in I$ and $y \in J$. Alas, this set is not closed under addition. As we defined it, IJ is the smallest ideal containing all products xy as x ranges over I and y over J.
(e) The definition of IJ extends ring multiplication to ideals, in the sense that $(Ra)(Rb) = R(ab)$.

2.4.6 Example. Let $R = \mathbb{Z}[\sqrt{19}]$. Check that the following are ideals in R:

$$I = \mathbb{Z} \cdot 2 + \mathbb{Z}(1 + \sqrt{19}), \quad J = \mathbb{Z} \cdot 3 + \mathbb{Z}(2 + \sqrt{19}).$$

By definition, IJ contains the four products of a generator of I with a generator of J:

$$\begin{aligned} 2 \cdot 3 &= 6 \\ 2 \cdot (2 + \sqrt{19}) &= 4 + 2\sqrt{19} \\ (1 + \sqrt{19}) \cdot 3 &= 3 + 3\sqrt{19} \\ (1 + \sqrt{19})(2 + \sqrt{19}) &= 21 + 3\sqrt{19}. \end{aligned} \tag{2.4.7}$$

A generic product $(a\cdot 2+b(1+\sqrt{19}))(c\cdot 3+d(2+\sqrt{19}))$ is a $\mathbb{Z}$-linear combination of the four elements above:

$$IJ = \{k\cdot 6 + l(3+3\sqrt{19}) + m(4+2\sqrt{19}) + n(21+3\sqrt{19}) : k,l,m,n \in \mathbb{Z}\}.$$

We would like to write IJ in the form $IJ = \mathbb{Z}a + \mathbb{Z}(b+\sqrt{19})$. To this end, look for relations among the generators listed in (2.4.7).

We observe that $-1+\sqrt{19} = (3+3\sqrt{19}) - (4+2\sqrt{19}) \in IJ$, and that the last three generators in (2.4.7) are $\mathbb{Z}$-linear combinations of 6 and $-1+\sqrt{19}$:

$$\begin{aligned} 3+3\sqrt{19} &= 6+3(-1+\sqrt{19}) \\ 4+2\sqrt{19} &= 6+2(-1+\sqrt{19}) \\ 21+3\sqrt{19} &= 4\cdot 6+3(-1+\sqrt{19}). \end{aligned}$$

We conclude that $IJ = \mathbb{Z}\cdot 6+\mathbb{Z}(-1+\sqrt{19})$. Similarly, one finds that $I+J = \{k\cdot 2+l(1+\sqrt{19})+m\cdot 3+n(2+\sqrt{19}) : k,l,m,n\in\mathbb{Z}\}$. In particular, $I+J$ contains $3-2=1$, so that $I+J=R$ and I and J are relatively prime. □

The procedure for finding relations among the generators in the example may seem ad hoc, but it is clearly pure linear algebra, which we will study in depth in Ch. 3.

Many results about division and congruences in $\mathbb{Z}$ turn out to be special cases of ideal-theoretic propositions. As an example, the Chinese remainder theorem in $\mathbb{Z}$ follows from the following general result.

2.4.8 Proposition (The Chinese Remainder Theorem)**.** *Let I and J be two relatively prime ideals of a ring R. Then*

$$R/IJ \cong R/I \times R/J.$$

The ring structure on the product is given by componentwise addition and multiplication.

Proof. Our only general tool for proving that two rings are isomorphic is the first isomorphism theorem (Thm. 2.2.6). It will imply the proposition once we construct a surjective homomorphism $\varphi\colon R \to R/I \times R/J$ with a kernel that is precisely IJ. The natural candidate is the homomorphism $\varphi(a) = (a+I, a+J)$.

In a much-used move, we deduce from $I+J=R$ that there exist $x\in I$ and $y\in J$ such that $x+y=1$. Pick any $a,b\in R$. As $bx+ay = bx+a(1-x) = b(1-y)+ay$, we find that

$$\varphi(bx+ay) = (a+x(b-a)+I, b+y(a-b)+J) = (a+I, b+J),$$

and φ is indeed onto.

Observe that $\varphi(a) = (a+I, a+J) = (I,J)$, the zero element in $R/I\times R/J$, if and only if $a\in I$ and $a\in J$. In brief, $\ker\varphi = I\cap J$, so the proposition will

be proved once we show that $I \cap J = IJ$. The inclusion $\supseteq$ holds in general. As for $\subseteq$, take any $a \in I \cap J$. Using the x and y as above, we see that

$$a = a \cdot 1 = a(x + y) = ax + ay \in IJ. \qquad \blacksquare$$

2.4.9 Example. Let's take $R = \mathbb{Z}$, $I = 12\mathbb{Z}$, and $J = 17\mathbb{Z}$. The two ideals are relatively prime, since

$$1 = \gcd(12, 17) = (-7) \cdot 12 + 5 \cdot 17 \in I + J. \tag{2.4.10}$$

The elementary version of the Chinese Remainder Theorem has two parts. The first part asserts that for any $r, s \in \mathbb{Z}$, there exists an $a \in \mathbb{Z}$ satisfying both congruences

$$a \equiv r \pmod{12} \text{ and } a \equiv s \pmod{17}. \tag{2.4.11}$$

That is just the restatement of the surjectivity of the homomorphism $\varphi(a) = (a \mod 12, a \mod 17)$ of Prop. 2.4.8. The second part, which claims that a is unique modulo $12 \cdot 17$, is equivalent to the injectivity of φ.

Solutions to the two particular systems,

$$\begin{aligned} a_{10} &\equiv 1 \pmod{12}, \quad a_{10} \equiv 0 \pmod{17}, \text{ and} \\ a_{01} &\equiv 0 \pmod{12}, \quad a_{01} \equiv 1 \pmod{17}, \end{aligned}$$

can be read off from the result of Euclid's Algorithm in (2.4.10): $a_{10} = 5 \cdot 17, a_{01} = -7 \cdot 12$. The solution to an arbitrary system of congruences (2.4.11) is then a linear combination of these two particular solutions: $a = ra_{10} + sa_{01} = 85r - 84s$. $\square$

Exercises

2.4.1. Check that the three operations of Def. 2.4.5 indeed produce ideals.

2.4.2.(a) Let I and J be ideals of R. Show that $I \cup J$ is an ideal of R if and only if either $I \subseteq J$ or $J \subseteq I$.

(b) Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain (finite or infinite) of ideals in R. Prove that $\cup_{n \geq 1} I_n$ is an ideal.

2.4.3. Let I, J, and K be ideals of a ring R. Prove the following identities:

(a) $I + J = J + I, IJ = JI$
(b) $(I + J) + K = I + (J + K), (IJ)K = I(JK)$
(c) $(I + J)K = IK + JK$
(d) $IR = RI = I$

(e) If $IJ = R$, then $I = J = R$. In other words, R is the only ideal with an inverse for ideal multiplication.
(f) If $I \subseteq J$, then $IK \subseteq JK$.

2.4.4. An ideal I of a ring R is **finitely generated** if $I = \langle X \rangle$ for a finite subset $X = \{x_1, \ldots, x_n\} \subseteq R$ (for notation, see Exer. 2.2.1). Prove that $I = Rx_1 + \cdots + Rx_n$.

2.4.5. Here is a list of true statements about the integers:

(a) $1 \mid a \mid 0$
(b) If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.
(c) If $a \mid c$ and $b \mid c$, then $\operatorname{lcm}(a, b) \mid c$.
(d) $a \mid b$ if and only if $b = ac$ for some $c \in \mathbb{Z}$.
(e) $ab = \operatorname{lcm}(a, b) \gcd(a, b)$
(f) A chain of divisors in $\mathbb{Z}$ is a sequence $a_1, a_2, \ldots \in \mathbb{Z}$ satisfying $a_2 \mid a_1, a_3 \mid a_2$, etc. Any chain of divisors stabilizes: there is an $n_0 \in \mathbb{N}$ such that $a_{n+1} = a_n$ for $n \geq n_0$.

Following Ex. 2.4.2, translate these statements into conjectures about ideals in a ring R, and state them in terms of both ideal divisibility and containment. If you like a challenge, decide which of the resulting conjectures are true (and give a proof), and which aren't (and give a counterexample).

2.4.6. Consider the ring $R = \mathbb{Z}[\sqrt{7}]$ and its two subsets

$$I = \mathbb{Z} \cdot 6 + \mathbb{Z}(2 + 2\sqrt{7}), \quad J = \mathbb{Z} \cdot 21 + \mathbb{Z}(7 + \sqrt{7}).$$

Check that both are ideals. Write the ideals $I + J$, IJ and $I \cap J$ as lattices of the form $\mathbb{Z}a + \mathbb{Z}(b + c\sqrt{7})$.

2.4.7. Recall the ideals P_1, P_2 and P_3 from Exer. 2.2.14. Denote by $\langle \alpha \rangle$ the principal ideal generated by $\alpha \in \mathbb{Z}[\sqrt{-5}]$. In the following diagram, check the vertical equalities by performing the indicated ideal multiplications:

$$\begin{array}{ccccccc} \langle 6 \rangle & = & \langle 2 \rangle & \cdot & \langle 3 \rangle & = \langle 1 + \sqrt{-5} \rangle & \cdot \langle 1 - \sqrt{-5} \rangle \\ \| & & \| & & \| & \| & \| \\ P_1^2 & \cdot & P_2 P_3 & = & P_1 P_2 & \cdot & P_1 P_3. \end{array}$$

These identities almost resolve the apparent failure of unique factorization of 6 in $\mathbb{Z}[\sqrt{-5}]$, following Kummer's program of Sec. 1.5. All that is left is to show that P_1, P_2, P_3 are "prime," which awaits in Exer. 2.5.5.

2.4.8. Let I, J, and K be ideals in the ring R. Assume that $I + J = R, I \mid K$ and $J \mid K$. Prove that $IJ \mid K$.

2.5 Prime and Maximal Ideals

Before we generalize unique factorization to ideals, we need to decide which among them are the right analog of prime numbers.

2.5.1 Definition. *An ideal M of R is* **maximal** *if $M \neq R$ and R is the only ideal strictly containing M.*

In other words, if I is an ideal with $M \subseteq I \subseteq R$, then either $I = M$ or $I = R$.

2.5.2 Definition. *An ideal P of R is* **prime** *if $P \neq R$ and if, for all $a, b \in R$, $ab \in P$ implies $a \in P$ or $b \in P$.*

In terms of ideal divisibility (Def. 2.4.1), an ideal $P \neq R$ is prime if, for all $a, b \in R$,

$$P \mid ab \text{ implies } P \mid a \text{ or } P \mid b.$$

Prime ideals thus satisfy a generalization (*à la* Kummer) of Euclid's lemma. By definition, R itself is neither a prime nor a maximal ideal.

2.5.3 Example. Let $p \in \mathbb{N}$ be prime. The following chain of implications shows that $\mathbb{Z}p$ is a prime ideal of $\mathbb{Z}$:

$$ab \in \mathbb{Z}p \quad \Rightarrow \quad p \mid ab \quad \Rightarrow \quad p \mid a \text{ or } p \mid b \quad \Rightarrow \quad a \in \mathbb{Z}p \text{ or } b \in \mathbb{Z}p.$$

In fact, $\mathbb{Z}p$ is also maximal. Suppose that an ideal $\mathbb{Z}a$ satisfies $\mathbb{Z}p \subsetneqq \mathbb{Z}a$, or, in elementary terms, $a \mid p$ and $a \neq p$. Since p is prime, a must be ± 1, so that $\mathbb{Z}a = \mathbb{Z}$, as required by Def. 2.5.1.

On the other hand, $\mathbb{Z} \cdot 6$ is not a prime ideal of $\mathbb{Z}$: $2 \cdot 3$ is in $\mathbb{Z} \cdot 6$, but neither 2 nor 3 is. □

The following pair of propositions characterizes maximal and prime ideals in terms of their quotients.

2.5.4 Proposition. *An ideal $P \subsetneqq R$ is prime if and only if R/P is an integral domain.*

Proof. In the diagram

$$\begin{array}{ccccc} (a+P)(b+P) = 0+P & \Rightarrow & (a+P = 0+P \text{ or } b+P = 0+P) \\ \Updownarrow & & \Updownarrow & & \Updownarrow \\ ab \in P & \Rightarrow & (a \in P & \text{or} & b \in P) \end{array}$$

the top row is the statement that R/P is an integral domain, while the bottom row asserts that P is a prime ideal. The two statements are equivalent since their constituents are, by the definition of the quotient ring R/P. ■

2.5.5 Proposition. *An ideal $M \subsetneqq R$ is maximal if and only if R/M is a field.*

Proof. Let $M \subsetneqq R$ be a maximal ideal and $a+M \in R/M$ a nonzero element. This means that $a \notin M$, so that we have a strict inclusion $M \subsetneqq M + Ra$. The maximality of M implies $M + Ra = R$, giving us an $m \in M$ and $b \in R$ such that $m + ba = 1$. Then

$$(b + M)(a + M) = ba + M = (1 - m) + M = 1 + M,$$

and $a+M$ has a multiplicative inverse, $b+M$. For the converse, simply reverse the argument. ■

2.5.6 Corollary. *Any maximal ideal is a prime ideal.*

Proof. If M is a maximal ideal of R, then R/M is a field. In particular, R/M is an integral domain, so that M is a prime ideal. ■

Conversely, when is a prime ideal maximal? The corollary to the following proposition gives a sufficient condition that will be satisfied in rings of quadratic integers.

2.5.7 Proposition. *Let $\mathcal{D}$ be a ring with finitely many elements. Then $\mathcal{D}$ is an integral domain if and only if $\mathcal{D}$ is a field.*

Proof. Assume that $\mathcal{D}$ is an integral domain and take $a \in \mathcal{D} \setminus 0$. Consider the homomorphism of additive groups $\mu_a : (\mathcal{D}, +) \to (\mathcal{D}, +)$ defined by $\mu_a(x) = ax$. As $\mathcal{D}$ is an integral domain, we find that

$$\ker \mu_a = \{x \in \mathcal{D} : ax = 0\} = 0.$$

This means that μ_a is injective and therefore also surjective, since $\mathcal{D}$ is finite. In particular, there exists a $b \in \mathcal{D}$ such that $\mu_a(b) = ab = 1$. Thus, each nonzero element of $\mathcal{D}$ is invertible, which makes $\mathcal{D}$ a field. The converse is trivial, as every field is an integral domain. ■

2.5.8 Corollary. *Let P be a prime ideal of a ring R. If R/P is finite, then P is a maximal ideal.*

As suggested in Ch. 1, we are shifting the focus of arithmetic from elements to ideals. It is nevertheless interesting that a direct generalization of prime numbers to elements of an arbitrary integral domain yields a somewhat more general notion than the requirement that Euclid's lemma be satisfied.

2.5.9 Definition. *Let $\mathcal{D}$ be an integral domain and $p \in \mathcal{D} \setminus \mathcal{D}^\times$.*

(a) p is **irreducible** *if, for all $a, b \in R$, $p = ab$ implies either $a \in \mathcal{D}^\times$ or $b \in \mathcal{D}^\times$.*

(b) p is a **prime element** *if, for all $a, b \in R$, $p \mid ab$ implies $p \mid a$ or $p \mid b$.*

Check the following basic consequences of the definition.

2.5.10 Proposition. *Let $\mathcal{D}$ be an integral domain.*

(a) An element $p \in \mathcal{D}$ is prime if and only if $\mathcal{D}p$ is a prime ideal.
(b) Any prime element of $\mathcal{D}$ is irreducible.

The converse of (b) is not generally true.

2.5.11 Example. We saw in Ex. 1.5.4 that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. It is, however, not a prime element of $\mathbb{Z}[\sqrt{-5}]$: $3 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, but 3 does not divide either factor. □

Exercises

2.5.1.* Let P be an ideal of a ring R. Show that P is a prime ideal if and only if the following analog of Euclid's lemma holds for any two ideals I and J of R:

$$P \mid IJ \text{ if and only if } P \mid I \text{ or } P \mid J.$$

2.5.2. Prove Prop. 2.5.10.

2.5.3. Prove that a ring R is an integral domain if and only if $\{0\}$ is a prime ideal of R.

2.5.4. In each example, decide whether I is a prime ideal of R. If it isn't, find a prime ideal $P \supseteq I$:

(a) $R = \mathbb{Z}[\sqrt{14}]$, $I = \mathbb{Z} \cdot 35 + \mathbb{Z}(7+\sqrt{14})$
(b) $R = \mathbb{Z}[\sqrt{-33}]$, $I = \mathbb{Z} \cdot 7 + \mathbb{Z}(4+\sqrt{-33})$
(c) $R = \mathbb{Z}[\frac{1+\sqrt{21}}{2}]$, $I = \mathbb{Z} \cdot 85 + \mathbb{Z}(9+\frac{1+\sqrt{21}}{2})$
(d) $R = \mathbb{Z}[\sqrt{35}]$, $I = \mathbb{Z} \cdot 1 + \mathbb{Z}(-5+\sqrt{35})$

2.5.5. To conclude the series of exercises on the factorization of 6 in $\mathbb{Z}[\sqrt{-5}]$, show that the ideals P_1, P_2, P_3 of Exer. 2.2.14 are all prime. Use your calculation from part (c) of that exercise.

2.5.6. Let R be a PID. Show that each nonzero prime ideal P of R is maximal.

2.5.7. Let $R = \mathbb{C}[x, y]$, the ring of polynomials in two variables with coefficients in $\mathbb{C}$. Show that $Rx + Ry$ is a maximal ideal, and that Rx is a prime ideal that isn't maximal.

2.5.8.* Prove that there are infinitely many prime ideals in $\mathbb{Z}[\sqrt{D}]$, for any $D \in \mathbb{Z}$ which isn't a complete square.

2.5.9. Let M be a maximal ideal of a ring R.

(a) Show that M is the *only* maximal ideal of R if and only if $R^\times = R \setminus M$. In that case, R is called a **local ring**.
(b) Show that R/M^n is a local ring with a unique maximal ideal that is M/M^n.

2.5.10. Let R be a local ring with maximal ideal M.

(a) Check that $1 + M^n$ is a subgroup of $R^\times$.
(b) Show that reduction modulo M defines a surjective group homomorphism $R^\times \to (R/M)^\times$ with kernel $1 + M$.
(c) Prove that $1 + m + M^{n+1} \mapsto m + M^{n+1}$ is an isomorphism between the multiplicative group $(1 + M^n)/(1 + M^{n+1})$ and the additive group M^n/M^{n+1}. Show that the latter group has the structure of an R/M-vector space.

Springer

http://www.springer.com/978-1-4614-7716-7

Algebraic Theory of Quadratic Numbers
Trifković, M.
2013, XI, 197 p. 29 illus., Softcover
ISBN: 978-1-4614-7716-7