

### 3 Rings

A ring is an abelian group with a multiplication. The situation is very similar to the integers  $\mathbb{Z}$ . We know that  $(\mathbb{Z}, +)$  is an abelian group, but at the same time we have multiplication as an additional composition. Rings were introduced by the German mathematician R. Dedekind (1831–1916), a student of Gauss, in connection with his studies of algebraic numbers, complex numbers that are roots of polynomials with integer coefficients. The definition of a ring appears in Dedekind's supplements to Dirichlet's book *Zahlentheorie* in the late nineteenth century. The theory of rings forms a wide framework useful in solving equations, computing with congruences, solving problems in number theory and exploring quantum mathematics. We will mostly deal with commutative rings (such as  $\mathbb{Z}$ ), for which factors can be interchanged.

Ideals are certain subgroups of commutative rings that satisfy one crucial property producing new (quotient) rings, just as normal subgroups give rise to new (quotient) groups. Ideals were originally born out of failed, but very clever, attempts to prove Fermat's last theorem. In order to understand the definitions and concepts of this chapter it is advisable to be extremely concrete. Each time you encounter a new definition or a new concept check it with your examples. The main examples in this chapter are the integers  $\mathbb{Z}$ , finite quotient rings  $\mathbb{Z}/n\mathbb{Z}$  of the integers, the Gaussian integers  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$  and  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ .

Using rings and ideals we will prove Fermat's famous two-square theorem: a prime number  $\equiv 1 \pmod{4}$  is the sum of two unique squares (e.g.  $13 = 2^2 + 3^2$ ). We will also show how computing the two squares given the prime number is related to quadratic residues and the Euclidean algorithm.

The first part of this chapter is a little on the heavy side concerning new concepts and definitions. Do not despair. None of them is really difficult. Make sure you study all examples intensively and link them to the concepts. Applications of the theory begin in subsection 3.5.5.

### 3.1 Definition

A *ring* is an abelian group  $(R, +)$  with an additional composition  $\cdot : R \times R \rightarrow R$  called multiplication. Multiplication satisfies the following for every  $x, y, z \in R$ :

- (i)  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ;
- (ii) there exists an element  $1 \in R$  such that  $1 \cdot x = x \cdot 1 = x$ ;
- (iii)  $x \cdot (y + z) = x \cdot y + x \cdot z$  and  $(y + z) \cdot x = y \cdot x + z \cdot x$ .

We will usually leave out  $\cdot$  in  $x \cdot y$  and simply write  $xy$ . The neutral element in the abelian group  $(R, +)$  is denoted  $0$ .

**Definition 3.1.1** Below we list some of the most important definitions concerning a ring  $R$ .

- (i) A subset  $S \subseteq R$  of a ring  $R$  is called a *subring* if  $S$  is a subgroup of  $(R, +)$ ,  $1 \in S$  and  $xy \in S$  if  $x, y \in S$ .
- (ii) An element  $x \in R \setminus \{0\}$  is called a *zero divisor* if there exists  $y \in R \setminus \{0\}$  such that  $xy = 0$  or  $yx = 0$ .
- (iii) An element  $x \in R$  is called a *unit* if there exists  $y \in R$  such that  $xy = yx = 1$ . In this case  $y$  is denoted  $x^{-1}$  and called the inverse of  $x$ . The set of units in  $R$  is denoted  $R^*$ .
- (iv)  $R$  is called *commutative* if  $xy = yx$  for every  $x, y \in R$ .

The multiplication in  $R$  makes  $R^*$  into a group. If  $R \neq \{0\}$  then  $0 \notin R^*$ . The group of units in a commutative ring  $R$  is an abelian group.

**Example 3.1.2** The integers  $\mathbb{Z}$  with addition and multiplication form in some sense the most natural commutative ring (later we will see that there is a unique ring homomorphism from  $\mathbb{Z}$  into any commutative ring). Notice that  $\mathbb{Z}^* = \{-1, 1\}$ . An example of a non-commutative ring is provided by the  $2 \times 2$  matrices

$$\text{Mat}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

with real entries. Here the addition is the usual addition of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix},$$

and the multiplication is the usual multiplication of matrices,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

The complex numbers  $\mathbb{C}$  form a ring containing the integers  $\mathbb{Z}$  as a subring. Again  $\mathbb{C}$  is a subring of the ring of quaternions  $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ , where addition is given component-wise and multiplication can be computed by the relations  $i^2 = j^2 = k^2 = ijk = -1$ . Using these relations one can deduce the composition table

$\cdot$	1	$i$	$j$	$k$
1	1	$i$	$j$	$k$
$i$	$i$	-1	$k$	$-j$
$j$	$j$	$-k$	-1	$i$
$k$	$k$	$j$	$-i$	-1

for the multiplication. So  $\mathbb{H}$  is a non-commutative ring with a highly intricate multiplication. Its discoverer, William R. Hamilton (1805–65) wrote

Tomorrow will be the fifteenth birthday of the Quaternions. They started into life, or light, full grown, on the 16th of October, 1843, as I was walking with Lady Hamilton in Dublin, and came up to Brougham Bridge. That is to say, I then and there felt the galvanic circuit of thought closed, and the sparks which fell from it were the fundamental equations between  $I$ ,  $J$  and  $K$ ; *exactly such* as I have used them ever since. I pulled out, on the spot, a pocketbook, which still exists, and made an entry, on which, *at the very moment*, I felt that it might be worth my while to expend the labour of at least ten (or it might be fifteen) years to come. But then it is fair to say that this was because I felt a problem to have been at that moment solved, an intellectual *want relieved*, which had *haunted* me for at least *fifteen years* before.

Even though non-commutative rings are extremely interesting, we shall limit ourselves to commutative rings in the rest of this book. So, from this point onwards a ring will always refer to a commutative ring.

The rational and complex numbers are both examples of rings  $R$  satisfying  $R^* = R \setminus \{0\}$ . A ring  $R$  with  $R^* = R \setminus \{0\}$  is called a *field*. If  $K \subseteq L$  are fields and  $K$  is a subring of  $L$  then  $K$  is called a *subfield* of  $L$  and  $L$  is called an *extension field* of  $K$ . A *domain* is a ring  $R \neq \{0\}$  with no zero divisors. Let us record the first basic properties about domains and fields.

**Proposition 3.1.3** *Let  $R$  be a domain and  $a, x, y \in R$ . If  $a \neq 0$  and  $ax = ay$  then  $x = y$ .*

*Proof.* If  $ax = ay$  then  $a(x - y) = 0$ . Since  $a \neq 0$ , this means that  $x - y = 0$ ; thus  $x = y$ .  $\square$

**Proposition 3.1.4** *Let  $F$  be a field. Then  $F$  is a domain.*

*Proof.* Suppose that  $x, y \in F$ ,  $x \neq 0$  and  $xy = 0$ . We must prove that  $y = 0$ . Since  $x \neq 0$ , there exists  $x^{-1} \in F$  such that  $x^{-1}x = 1$ . This means that  $0 = x^{-1}0 = x^{-1}(xy) = (x^{-1}x)y = y$ .  $\square$

The set of integers  $\mathbb{Z}$  is a subring of the rational numbers  $\mathbb{Q}$  with the usual addition and multiplication and  $\mathbb{Z}^* = \{1, -1\}$ . So  $\mathbb{Z}$  is a domain that is not a field. The ring of rational numbers  $\mathbb{Q}$  is a field, since every fraction  $a/b \neq 0$  can be inverted:  $(a/b)(b/a) = 1$ . The ring of rational numbers  $\mathbb{Q}$  is a subfield of the real numbers  $\mathbb{R}$  and the real numbers form a subfield of the complex numbers  $\mathbb{C}$  that is an extension field of  $\mathbb{R}$ .

**Example 3.1.5** Consider the subset

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

of  $\mathbb{C}$ . The usual rules,  $(a + bi) + (c + di) = (a + c) + (b + d)i$  and  $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ , for adding and multiplying complex numbers imply that  $\mathbb{Q}(i)$  is a subring of  $\mathbb{C}$ . If  $z = a + bi$  is a non-zero element of  $\mathbb{Q}(i)$  then

$$\frac{1}{z} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$

and it follows that  $\mathbb{Q}(i)$  is a field. It is an extension field of  $\mathbb{Q}$  and a subfield of  $\mathbb{C}$ . Recall that  $|z|^2 = z\bar{z}$ , where  $|z|$  is the modulus and  $\bar{z}$  the complex conjugate of  $z \in \mathbb{C}$ . We call  $|z|^2$  the norm of  $z \in \mathbb{C}$  and denote it  $N(z)$ . Notice that

$$N(z_1 z_2) = N(z_1)N(z_2) \quad (3.1)$$

for  $z_1, z_2 \in \mathbb{C}$ . If  $z = a + bi$  then  $N(z) = (a + bi)(a - bi) = a^2 + b^2$ . Inside  $\mathbb{Q}(i)$  we have the subring  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ , which is called the ring of *Gaussian integers*. Note that  $N(z) \in \mathbb{N}$  if  $z \in \mathbb{Z}[i]$ . The property (3.1) of  $N$  implies that an element  $z \in \mathbb{Z}[i]$  is a unit if and only if  $N(z) = 1$ : if  $z$  is a unit then there exists  $y \in \mathbb{Z}[i]$  such that  $zy = 1$ , and (3.1) gives  $1 = N(zy) = N(z)N(y)$ , so that  $N(z) = 1$ . However, if  $z = a + bi$  and  $N(z) = (a + bi)(a - bi) = a^2 + b^2 = 1$  then  $zy = 1$ , where  $y = a - bi \in \mathbb{Z}[i]$  and  $z$  is a unit. Using this characterization of the units one finds that  $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$ .

Prime numbers in  $\mathbb{Z}$  are not necessarily “prime numbers” in  $\mathbb{Z}[i]$ : for 5, for example, we have the factorization  $5 = (1 + 2i)(1 - 2i)$  in  $\mathbb{Z}[i]$ . We will have a good deal more to say about this phenomenon later in the chapter.

### 3.1.1 Ideals

An *ideal* in a ring  $R$  is a subgroup  $I$  of  $(R, +)$  such that  $\lambda x \in I$  for every  $\lambda \in R$  and  $x \in I$ . Notice that  $R$  itself is an ideal and that a given ideal  $I$  is the whole ring  $R$  if and only if  $1 \in I$  (see Exercise 3.4).

Let  $r_1, \dots, r_n \in R$ . Then the subset

$$\langle r_1, \dots, r_n \rangle = \{ \lambda_1 r_1 + \dots + \lambda_n r_n \mid \lambda_1, \dots, \lambda_n \in R \}$$

is an ideal in  $R$  (see Exercise 3.5). If  $I$  is an ideal in  $R$  and there exist  $r_1, \dots, r_n \in R$  such that  $I = \langle r_1, \dots, r_n \rangle$ , we say that  $I$  is (finitely) *generated* by  $r_1, \dots, r_n \in R$ . Notice that  $\langle r_1, \dots, r_n \rangle \subseteq I$  if  $r_1, \dots, r_n \in I$  (see Exercise 3.6).

**Remark 3.1.6** It also makes sense to talk about an ideal generated by infinitely many elements. One defines this as follows. Let  $M$  be any subset of  $R$ . Then the ideal generated by  $M$  is

$$\langle f \mid f \in M \rangle = \{ a_1 f_1 + \dots + a_n f_n \mid n \in \mathbb{N}, a_1, \dots, a_n \in R, f_1, \dots, f_n \in M \}.$$

**Remark 3.1.7** Let  $I$  and  $J$  be ideals in a ring  $R$ .

- (i) Then  $I \cap J$  and  $I + J = \{ i + j \mid i \in I, j \in J \}$  are also ideals in  $R$ .
- (ii) The product  $IJ$  of  $I$  and  $J$  is defined to be the ideal generated by  $\{ ij \mid i \in I, j \in J \}$  according to Remark 3.1.6. This has an obvious generalization to a finite number of ideals. Notice that  $IJ \subseteq I \cap J$ .

**Remark 3.1.8** An ideal in a field  $F$  is either  $\langle 0 \rangle$  or  $F$  itself. If  $I \neq \langle 0 \rangle$  is an ideal in  $F$  and  $a \in I \setminus \{0\}$  we can find  $b \in F$  such that  $ba = 1$ . By the definition of an ideal,  $1 = ba \in I$ . This implies that  $I = F$ .

An ideal  $I$  in  $R$  that can be generated by one element is called a *principal ideal*. In this case there exists  $d \in R$  such that  $I = \langle d \rangle$ .

**Definition 3.1.9** A domain in which every ideal is a principal ideal is called a *principal ideal domain*.

**Proposition 3.1.10** The ring  $\mathbb{Z}$  is a principal ideal domain.

*Proof.* A subgroup of  $\mathbb{Z}$  can be written  $d\mathbb{Z}$  for  $d \in \mathbb{Z}$  (see Proposition 2.2.3). This shows that every subgroup is a principal ideal. Since an ideal is in particular a subgroup this finishes the proof.  $\square$

Let us study ideals in the ring of Gaussian integers. We have already seen that the norm function  $N(a + bi) = a^2 + b^2$  plays a central role. In the following crucial result we use a special property of the norm function, which will be formalized later in the notion of a Euclidean domain.

**Theorem 3.1.11** *The ring of Gaussian integers  $\mathbb{Z}[i]$  is a principal ideal domain.*

*Proof.* Let  $I$  be a non-zero ideal in  $\mathbb{Z}[i]$ . Choose among the non-zero elements in  $I$  an element  $d = a + bi \in I$  such that  $N(d) = a^2 + b^2$  is minimal. Now suppose that  $z \in I$ ; then, computing in  $\mathbb{C}$  we get  $z/d = q_1 + q_2i$ , where  $q_1, q_2 \in \mathbb{Q}$ . A point in the complex plane is at most  $\sqrt{2}/2$  away from a point with integer real and imaginary parts (why?). Therefore we may choose an element  $q = c + di \in \mathbb{Z}[i]$  such that  $|z/d - q|^2 < 1$  or, using the norm given in Example 3.1.5,

$$N(z/d - q) < 1. \quad (3.2)$$

Multiplying both sides of (3.2) by  $N(d)$  we get  $N(z - qd) < N(d)$ , using (3.1). Since  $z - qd \in I$ , we must have that  $z = qd$  by the construction of  $d$ . Thus  $I \subseteq \langle d \rangle$ . The other inclusion holds since  $d \in I$ , so we have proved that  $I$  is a principal ideal.  $\square$

However, the ring  $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$  contains ideals that are not principal. This will be revealed later in this chapter.

## 3.2 Quotient rings

Let  $I$  be an ideal in a ring  $R$ . Then  $I$  is in particular a subgroup of the abelian group  $(R, +)$ , and the set  $R/I = \{[x] \mid x \in R\}$  of left cosets  $[x] = x + I$  of  $I$  with respect to  $+$  is an abelian group (recall that  $[x] = [y]$  if and only if  $x - y \in I$ ). We can make  $R/I$  into a ring in a very natural way by defining addition and multiplication as follows:

- (i)  $[x] + [y] = [x + y]$  for every  $[x], [y] \in R/I$ ,
- (ii)  $[x][y] = [xy]$  for every  $[x], [y] \in R/I$ .

It is built into the definition of an ideal that these operations are independent of the choice of the element in the left coset. Suppose that  $[x] = [x']$  and  $[y] = [y']$ . For the definition to be independent of the choice of element, we need that  $[x + y] = [x' + y']$  and  $[xy] = [x'y']$ . We already know that  $[x + y] = [x' + y']$ , since composition in the quotient group  $(R/I, +)$  is well defined. As  $xy - x'y' = x(y - y') + y'(x - x') \in I$ , it follows that  $xy - x'y' \in I$  and therefore that  $[xy] = [x'y']$ . Notice how all this is inspired by Proposition 1.3.4. The new ring  $R/I$  is called the quotient ring of  $R$  by  $I$  and has  $[0]$  and  $[1]$  playing the role of 0 and 1. Notice that  $[x] = 0$  in  $R/I$  if and only if  $x \in I$ .

### 3.2.1 Quotient rings of $\mathbb{Z}$

An ideal in  $\mathbb{Z}$  is a principal ideal  $\langle d \rangle$  generated by a natural number  $d$ . Two elements  $x, y \in \mathbb{Z}$  represent the same element  $[x] = [y]$  in  $\mathbb{Z}/d\mathbb{Z}$  if and only if  $x - y \in d\mathbb{Z}$  if and only if  $d \mid x - y$ . One way of thinking of the elements in  $\mathbb{Z}/d\mathbb{Z}$  is as represented by the remainders by division with  $d$ ,  $\{[0], [1], [2], [3], \dots, [d - 1]\}$ .

**Example 3.2.1** If  $d = 6$  then  $\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$ . Here we have  $[4] + [4] = [2]$  and  $[3][4] = [0]$ .

**Proposition 3.2.2** Suppose that  $d$  is a positive integer. Then the group of units  $(\mathbb{Z}/d\mathbb{Z})^*$  is an abelian group with  $\varphi(d)$  elements.

*Proof.* Let us check that a coset  $[x] = x + d\mathbb{Z}$  is a unit if and only if  $\gcd(x, d) = 1$ . If  $\gcd(x, d) = 1$  then we can find  $\lambda, \mu \in \mathbb{Z}$  such that  $\lambda x + \mu d = 1$ . Therefore  $[\lambda x + \mu d] = [\lambda x] + [\mu d] = [\lambda][x] = [1]$ , so that  $x$  is a unit. However, if  $[x]$  is a unit in  $\mathbb{Z}/d\mathbb{Z}$  then there exists an element  $[\lambda] \in \mathbb{Z}/d\mathbb{Z}$  such that  $[\lambda][x] = [\lambda x] = [1]$ . Thus  $\lambda x - 1 \in d\mathbb{Z}$  and we can find  $\mu \in \mathbb{Z}$  such that  $\lambda x - 1 = \mu d$ . This implies that  $\gcd(x, d) = 1$ .  $\square$

Notice the connection with subsection 2.3.2, where we constructed  $(\mathbb{Z}/d\mathbb{Z})^*$  without using the ring structure of  $\mathbb{Z}/d\mathbb{Z}$ .

**Proposition 3.2.3** Let  $n \in \mathbb{N}$ . Then  $\mathbb{Z}/n\mathbb{Z}$  is a field if and only if  $n$  is a prime number. If  $n$  is a composite number then  $\mathbb{Z}/n\mathbb{Z}$  is not a domain.

*Proof.* Assume that  $n > 0$ . By Proposition 3.2.2 we have  $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ . Since  $|\mathbb{Z}/n\mathbb{Z}| = n$ , this shows that  $\mathbb{Z}/n\mathbb{Z}$  is a field if and only if  $\varphi(n) = n - 1$ .

This last condition holds if and only if  $n$  is a prime number. If  $n$  is a composite number, we may write  $n = ab$ , where  $1 < a, b < n$ . This means that  $[a] \neq [0]$  and  $[b] \neq [0]$  in  $\mathbb{Z}/n\mathbb{Z}$ , but  $[a][b] = [n] = [0]$ , so that  $\mathbb{Z}/n\mathbb{Z}$  is not a domain.  $\square$

**Remark 3.2.4** What happens if  $n = 0$  in Proposition 3.2.3?

**Definition 3.2.5** The field  $\mathbb{Z}/p\mathbb{Z}$  is denoted  $\mathbb{F}_p$ , where  $p$  is a prime number.

### 3.2.2 Prime ideals

Suppose that  $I$  is an ideal in a ring  $R$ . When is the quotient ring  $R/I$  a domain? When is  $R/I$  a field? Suppose that  $R/I$  is a domain. Then  $R/I \neq 0$  and  $[x][y] = 0$  implies  $[x] = 0$  or  $[y] = 0$  for every  $[x], [y] \in R/I$ . In terms of the ideal  $I$  this means that

$$I \neq R \text{ and } xy \in I \text{ implies } x \in I \text{ or } y \in I$$

for every  $x, y \in R$ . An ideal satisfying this condition is called a *prime ideal*. Conversely, if  $I \subseteq R$  is a prime ideal then  $R/I$  is a domain (see Exercise 3.21). Thus we end up with the following proposition.

**Proposition 3.2.6** *An ideal  $I \subseteq R$  is a prime ideal if and only if  $R/I$  is a domain.*

### 3.2.3 Maximal ideals

Suppose that  $R/I$  is a field. This means that  $R/I \neq 0$  and that for every non-zero element  $[x] \in R/I$  there exists  $[y] \in R/I$  such that  $[x][y] = [xy] = [1]$ .

In terms of the ideal  $I$ , this means that for every  $x \notin I$  there exists  $y \in R$  such that  $xy - 1 \in I$ . Suppose that  $J$  is another ideal such that  $I \subseteq J \subseteq R$ . If  $x \in J \setminus I$  then we may find  $y \notin I$  such that  $xy - 1 \in I \subseteq J$ . But since  $xy$  is in  $J$  (as  $x \in J$ ) it follows that  $1 = -(xy - 1) + xy \in J$ . This means that  $J = R$ . We have proved that if  $R/I$  is a field then  $I$  is an ideal satisfying the following:

$$\text{if } I \subsetneq J \text{ then } J = R,$$

where  $J$  is an ideal of  $R$ . An ideal satisfying this condition is called a *maximal ideal* (maximal among the ideals properly contained in  $R$ ).



If  $I \subseteq R$  is a maximal ideal then  $R/I$  is a field. This can be seen as follows. If  $[x] \in R/I$  is a non-zero element then  $x \notin I$ . The subset  $I + Rx = \{i + rx \mid i \in I, r \in R\}$  is an ideal in  $R$ . Since  $I \subsetneq I + Rx$ , we must have that  $I + Rx = R$ . Therefore  $1 \in I + Rx$ . So we may write  $1 = m + rx$  for suitable  $m \in I, r \in R$ . Going to  $R/I$  we get  $[1] = [r][x]$ , so that  $[x]$  is a unit in  $R/I$ . We end up with the following proposition.

**Proposition 3.2.7** *An ideal  $I \subseteq R$  is a maximal ideal if and only if  $R/I$  is a field.*

**Remark 3.2.8** A maximal ideal is a prime ideal, because a field is a domain (Proposition 3.1.4).

**Example 3.2.9** The ring  $\mathbb{Z}$  is a principal ideal domain. This means that every ideal in  $\mathbb{Z}$  has the form  $\langle d \rangle = d\mathbb{Z}$  for some  $d \in \mathbb{Z}$ . Which of these are maximal? Suppose that  $p$  is a prime number and that  $\langle p \rangle = p\mathbb{Z}$  is contained in another ideal  $\langle d \rangle = d\mathbb{Z}$  in  $\mathbb{Z}$ . Then  $p \in \langle d \rangle$ . Therefore  $d$  divides  $p$  and so  $d = \pm 1$  or  $d = \pm p$ . This implies that  $\langle d \rangle = \mathbb{Z}$  or  $\langle d \rangle = p\mathbb{Z}$ , proving that  $\langle p \rangle$  is a maximal ideal. The ideal  $\langle 0 \rangle$  is a prime ideal that is not a maximal ideal. An ideal  $\langle m \rangle$  generated by a composite number  $m = ab$ , where  $a, b \neq \pm 1$  is not a prime ideal, since  $ab \in \langle m \rangle$  but  $a \notin \langle m \rangle$  and  $b \notin \langle m \rangle$ .

### 3.3 Ring homomorphisms

A map  $f : R \rightarrow S$  between two rings  $R$  and  $S$  is called a *ring homomorphism* if it is a group homomorphism from  $(R, +)$  to  $(S, +)$ ,  $f(xy) = f(x)f(y)$  for every  $x, y \in R$  and  $f(1) = 1$ . A bijective ring homomorphism is called a *ring isomorphism*. If  $R$  and  $S$  are rings and there exists a ring isomorphism  $f : R \rightarrow S$ , we say that  $R$  and  $S$  are isomorphic. This is denoted  $R \cong S$ .

**Example 3.3.1** The map  $R \rightarrow R/I$  given by  $r \mapsto [r]$  is a (surjective) ring homomorphism. This follows from the way we defined addition and multiplication in  $R/I$ .

The kernel  $\text{Ker } f = \{r \in R \mid f(r) = 0\} \subseteq R$  of  $f$  (as a group homomorphism) is an ideal of  $R$  and the image  $f(R)$  is a subring of  $S$  (see Exercise 3.11). The isomorphism theorem for rings follows almost immediately from the analogue for groups (see Theorem 2.5.1).

**Proposition 3.3.2** *Let  $R$  and  $S$  be rings and  $f : R \rightarrow S$  a ring homomorphism with kernel  $K = \text{Ker}(f)$ . Then*

$$\tilde{f} : R/K \rightarrow f(R)$$

*given by  $\tilde{f}(r + K) = f(r)$  is a well defined map and a ring isomorphism.*

*Proof.* We already know that  $\tilde{f}$  is a well defined map and an isomorphism of abelian groups by Theorem 2.5.1. It remains to check that it is a ring homomorphism. Clearly  $\tilde{f}(1 + K) = f(1) = 1$ . Since

$$\begin{aligned}\tilde{f}((x + K)(y + K)) &= \tilde{f}(xy + K) \\ &= f(xy) = f(x)f(y) \\ &= \tilde{f}(x + K)\tilde{f}(y + K)\end{aligned}$$

for  $x, y \in R$ , it follows that  $\tilde{f}$  is a ring homomorphism.  $\square$

### 3.3.1 The unique ring homomorphism from $\mathbb{Z}$

**Lemma 3.3.3** *For every ring  $R$ , there is a unique ring homomorphism  $f : \mathbb{Z} \rightarrow R$ .*

*Proof.* A ring homomorphism  $f : \mathbb{Z} \rightarrow R$  is in particular a group homomorphism  $f : (\mathbb{Z}, +) \rightarrow (R, +)$  with  $f(1) = 1$ . This last condition says that  $f = f_1$  in the notation of Section 2.6. So  $f$  is unique. We just need to show that  $f = f_1 : \mathbb{Z} \rightarrow R$  is a ring homomorphism. In other words we must show that  $f(mn) = f(m)f(n)$  for  $m, n \in \mathbb{Z}$ . We can assume that  $m, n > 0$ , since  $f(-m) = f((-1)m) = f(-1)f(m) = -f(m)$ . Now the result follows if  $x(y + z) = xy + xz$  ( $x, y, z \in R$ ) is applied successively: a sum of  $m$  copies of 1 multiplied by a sum of  $n$  copies of 1 is a sum of  $mn$  copies of 1 (here  $1 \in R$ ).  $\square$

**Remark 3.3.4** Let  $f : \mathbb{Z} \rightarrow R$  denote the unique ring homomorphism for a given ring  $R$ . For  $n \geq 0$ , one thinks of  $f(n)$  as

$$f(n) = 1 + 1 + \cdots + 1,$$

a sum of  $n$  copies of  $1 \in R$ . Given the unique ring homomorphism  $f : \mathbb{Z} \rightarrow R$  it makes sense to view integers as elements in any ring. When  $n \in \mathbb{Z}$  and we write  $n \in R$  we are referring to the element  $f(n)$  of  $R$ .

Let  $R$  be a ring. Let  $\text{ord}(1)$  denote the order of 1 in  $(R, +)$ . This turns out to be a fundamental invariant of  $R$ . If  $\text{ord}(1)$  is infinite then  $R$  is said to have *characteristic zero*. If  $\text{ord}(1)$  is finite  $R$  is said to have finite characteristic  $\text{ord}(1)$ . So the characteristic of  $R$  is  $n_1$ , where  $n_1 \in \mathbb{N}$  and  $n_1\mathbb{Z} = \text{Ker } f_1$  in the notation of Section 2.6. The characteristic of  $R$  is denoted  $\text{char } R$ . In the positive-characteristic case one usually thinks of  $\text{char } R$  as the smallest natural number  $n$  for which  $1 + \cdots + 1$  ( $n$  times)  $= 0$  in  $R$ .

The ring  $\mathbb{Z}$  of integers has characteristic zero. The same is true for  $\mathbb{Q}, \mathbb{R}$ . But  $\text{char } \mathbb{Z}/n\mathbb{Z} = n$  for  $n \in \mathbb{N}$ .

**Lemma 3.3.5** *Let  $R$  be a ring. Then there is an injective ring homomorphism*

$$\mathbb{Z}/n\mathbb{Z} \rightarrow R,$$

where  $n = \text{char } R$ .

*Proof.* Let  $f : \mathbb{Z} \rightarrow R$  be the unique ring homomorphism. Then  $f(\mathbb{Z}) = S$  is a subring of  $R$  and  $\text{Ker}(f) = n\mathbb{Z}$  for  $n = \text{char } R$ . The isomorphism theorem for rings (Proposition 3.3.2) says that we have a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \rightarrow S.$$

But this means that we have the desired injective ring homomorphism  $\mathbb{Z}/n\mathbb{Z} \rightarrow S \subseteq R$ .  $\square$

**Remark 3.3.6** In the situation of Lemma 3.3.5 we say that  $\mathbb{Z}/n\mathbb{Z}$  is contained in  $R$ , since it is isomorphic to a subring in  $R$ .

**Proposition 3.3.7** *Let  $R$  be a domain. Then  $\text{char } R$  is either zero or a prime number. If  $R$  is finite then  $R$  is a field and  $\text{char } R$  is a prime number.*

*Proof.* Let  $n = \text{char } R$ . We know that  $\mathbb{Z}/n\mathbb{Z}$  is a subring of  $R$  by Lemma 3.3.5. This means in particular that  $\mathbb{Z}/n\mathbb{Z}$  is a domain, being a subring of a domain. In this way  $n$  must be zero or a prime number by Proposition 3.2.3. If  $R$  is a finite domain then  $n > 0$  (if  $n = 0$ ,  $R$  would contain  $\mathbb{Z}$  as a subring) and  $n$  must be a prime number. A finite domain is a field (see Exercise 3.23).  $\square$

### 3.3.2 Freshman's Dream

The title of this subsection refers to certain beginners' mistakes in calculus exercises: for example, that the sine of a sum of two angles  $\sin(x + y)$  is equal

to  $\sin(x) + \sin(y)$  or that  $(x + y)^5$  is equal to  $x^5 + y^5$  for  $x, y \in \mathbb{R}$ . Of course, one has to insert intermediate terms coming from the binomial formula to evaluate  $(x + y)^5$ . Let us state a general version of the binomial formula.

**Lemma 3.3.8** *Let  $R$  be a ring and  $a, b$  two elements in  $R$ . Then*

$$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

for  $n \in \mathbb{N}$ .

*Proof.* This can be proved using induction. The case  $n = 1$  is clear. Assume that

$$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n;$$

then  $(a + b)^{n+1} = (a + b)^n(a + b)$ . Using  $ab = ba$  and

$$\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$$

for  $i = 1, \dots, n$ , the result follows.  $\square$

Notice that the binomial coefficients in Lemma 3.3.8 are considered as elements in the ring  $R$  through the unique ring homomorphism  $\mathbb{Z} \rightarrow R$ . We will keep using this convention. Now for the main insight, which looks innocent but is incredibly powerful.

**Theorem 3.3.9 (Freshman's Dream)** *Let  $R$  be a ring of prime characteristic  $p$ . Then*

$$(x + y)^{p^r} = x^{p^r} + y^{p^r}$$

for every  $x, y \in R$  and  $r \in \mathbb{N}$ .

*Proof.* Since  $\text{char } R = p$ , the kernel of the unique ring homomorphism  $\mathbb{Z} \rightarrow R$  is  $p\mathbb{Z}$ . As  $p$  divides the binomial coefficients

$$\binom{p}{1}, \quad \binom{p}{2}, \quad \dots, \quad \binom{p}{p-1},$$

by Exercise 1.30(i), it follows that  $\binom{p}{i} = 0$  in  $R$  when  $i = 1, \dots, p-1$ . Using Lemma 3.3.8, this shows that  $(x + y)^p = x^p + y^p$  in  $R$ . Now conclude by induction for  $r > 1$  that

$$(x + y)^{p^r} = ((x + y)^p)^{p^{r-1}} = (x^p + y^p)^{p^{r-1}} = (x^p)^{p^{r-1}} + (y^p)^{p^{r-1}} = x^{p^r} + y^{p^r}.$$

$\square$

Freshman's Dream is one of the most useful facts in algebra. Doing mathematics in a universe where this kind of linearity is possible is a dream come true. Already in the following chapter on polynomials, Freshman's Dream will become an indispensable tool especially in proving the law of quadratic reciprocity.

**Remark 3.3.10** Notice that if  $R$  is a ring of prime characteristic  $p$  then Theorem 3.3.9 shows that the map  $F : R \rightarrow R$  given by  $F(x) = x^p$  is a ring homomorphism. It is called the Frobenius map after G. Frobenius (1849–1917).

### 3.4 Fields of fractions

If  $R$  is a domain then there is a very natural field  $Q$  and an injective ring homomorphism  $R \rightarrow Q$ . In a precise sense one may say that  $Q$  is the “smallest” field containing  $R$ . The field  $Q$  consists of fractions with a numerator in  $R$  and a denominator in  $R \setminus \{0\}$ . The situation is practically identical with the situation  $R = \mathbb{Z}$  and  $Q = \mathbb{Q}$  and the construction the same as in Appendix A.2.2. We let  $M = R \times (R \setminus \{0\})$  and define  $Q = M/\sim$ , where  $(a, s) \sim (b, t)$  if and only if  $at = bs$ . As in Appendix A.2.2 we let  $\frac{a}{s}$  denote the equivalence class containing  $(a, s) \in M$ . Then

$$\frac{a}{s} \frac{b}{t} = \frac{ab}{st}, \quad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$

are well defined operations and they make  $Q$  into a ring, where

$$0 = \frac{0}{a} \quad \text{and} \quad 1 = \frac{a}{a}$$

for every  $a \in R \setminus \{0\}$ . Notice that  $Q$  is a field, since

$$\frac{a}{s} \neq 0$$

in  $Q$  means that  $a \neq 0$ . In this case

$$\frac{s}{a} \in Q \quad \text{and} \quad \frac{a}{s} \frac{s}{a} = \frac{as}{as} = 1$$

in  $Q$ . Furthermore,  $Q$  comes with an injective ring homomorphism  $i : R \rightarrow Q$  given by

$$i(a) = \frac{a}{1}.$$

The field  $Q$  is called the *field of fractions* of  $R$ . The following proposition states formally that it is the “smallest” field containing  $R$ .

**Proposition 3.4.1** *Let  $R$  be a domain with field of fractions  $Q$ , let  $L$  be a field and let  $\varphi : R \rightarrow L$  be an injective ring homomorphism. Then there exists a unique injective ring homomorphism  $\bar{\varphi} : Q \rightarrow L$  such that  $\bar{\varphi} \circ i = \varphi$ .*

*Proof.* If  $\bar{\varphi} \circ i = \varphi$  then we must have

$$1 = \bar{\varphi} \left( \frac{s}{1} \right) = \bar{\varphi} \left( \frac{s}{1} \right) \bar{\varphi} \left( \frac{1}{s} \right) = \varphi(s) \bar{\varphi} \left( \frac{1}{s} \right),$$

where  $s \in R \setminus \{0\}$ . So there is only one way of defining  $\bar{\varphi}$ , provided that  $\bar{\varphi} \circ i = \varphi$ :

$$\bar{\varphi} \left( \frac{a}{s} \right) = \bar{\varphi} \left( \frac{a}{1} \right) \bar{\varphi} \left( \frac{1}{s} \right) = \varphi(a) \varphi(s)^{-1}.$$

This is well defined: if

$$\frac{a}{s} = \frac{b}{t}$$

then  $at = bs$ . Therefore  $\varphi(a)\varphi(t) = \varphi(b)\varphi(s)$  and  $\varphi(a)\varphi(s)^{-1} = \varphi(b)\varphi(t)^{-1}$ . Let us prove that  $\bar{\varphi}$  really is a ring homomorphism. Proving that  $\bar{\varphi}$  preserves multiplication is left to the reader. Below we prove that  $\bar{\varphi}$  preserves addition:

$$\begin{aligned} \bar{\varphi} \left( \frac{a}{s} + \frac{b}{t} \right) &= \bar{\varphi} \left( \frac{at + bs}{st} \right) \\ &= (\varphi(a)\varphi(t) + \varphi(b)\varphi(s))\varphi(st)^{-1} \\ &= \varphi(a)\varphi(s)^{-1} + \varphi(b)\varphi(t)^{-1} \\ &= \bar{\varphi} \left( \frac{a}{s} \right) + \bar{\varphi} \left( \frac{b}{t} \right). \end{aligned}$$

To prove that  $\bar{\varphi}$  is injective it is enough to show that  $\text{Ker}(\bar{\varphi}) = \{0\}$ . Suppose that

$$\bar{\varphi} \left( \frac{a}{s} \right) = \varphi(a)\varphi(s)^{-1} = 0.$$

Then  $\varphi(a) = 0$  and therefore  $a = 0$  since  $\varphi$  is injective. This proves that

$$\frac{a}{s} = 0$$

and therefore that  $\text{Ker}(\bar{\varphi}) = \{0\}$ . □

**Corollary 3.4.2** *Let  $R$  be a domain contained in the field  $L$ . The smallest subfield in  $L$  containing  $R$  is*

$$K = \{as^{-1} \mid a \in R, s \in R \setminus \{0\}\}.$$

*The field of fractions of  $R$  is isomorphic to  $K$ .*

*Proof.* Let  $a, b \in R$  and  $s, t \in R \setminus \{0\}$ . Then  $(as^{-1})(bt^{-1}) = (ab)(ts)^{-1}$ ,  $as^{-1} + bt^{-1} = (at + bs)(ts)^{-1}$  and  $(as^{-1})^{-1} = sa^{-1}$  if  $a \neq 0$ . These formulas imply that  $K$  is a subfield of  $L$ . Any subfield of  $L$  containing  $R$  must contain  $as^{-1}$ , where  $a \in R$  and  $s \in R \setminus \{0\}$ . So  $K$  is the smallest subfield containing  $R$ . Let  $Q$  be the field of fractions of  $R$ . Then the unique injective ring homomorphism  $\bar{\varphi} : Q \rightarrow K$  of Proposition 3.4.1 is surjective, since it is given by

$$\bar{\varphi}\left(\frac{a}{s}\right) = as^{-1}$$

(notice that  $\varphi$  is the inclusion of  $R$  into  $L$ ). It is therefore an isomorphism and  $Q$  becomes isomorphic to  $K$ .  $\square$

**Example 3.4.3** The Gaussian integers  $\mathbb{Z}[i]$  form a domain whose field of fractions is isomorphic to  $\mathbb{Q}(i)$ . This follows from Corollary 3.4.2 and Example 3.1.5.

### 3.5 Unique factorization

What is the analogue of a prime number in a general commutative ring? Is there such a thing as unique factorization? Saying that a “general prime number” should be an element  $x$  that cannot be factored except for the factorization  $x = ab$ , where  $a$  or  $b$  is a unit, is not enough. The key property turns out to be the generalization of the fact that if a prime number divides a product of two numbers then it divides one of them (this is Lemma 1.8.3). A unique factorization domain is a domain like  $\mathbb{Z}$ , where every non-zero element has a unique factorization into prime elements. The main result in this section is that a principal ideal domain is a unique factorization domain (Theorem 3.5.7). The proof is not difficult once you recall how we proved unique factorization into prime numbers for  $\mathbb{Z}$  in Theorem 1.8.5. The only difference is in Lemma 3.5.5, which in a sense is an abstract version of Lemma 1.8.1. In the following we will assume that  $R$  is a domain.

### 3.5.1 Divisibility and greatest common divisor

Suppose that  $x, y \in R$ . If  $x = ry$  for some  $r \in R$ , we say that  $y$  is a *divisor* of  $x$ . This is denoted  $y \mid x$ . Notice that  $y \mid x$  if and only if  $\langle x \rangle \subseteq \langle y \rangle$ . If  $x = uy$ , where  $u \in R^*$ , then  $\langle x \rangle = \langle y \rangle$ . However, if  $\langle x \rangle = \langle y \rangle$  then  $x = ry$  and  $y = sx$  for some  $r, s \in R$ . Therefore  $x = r(sx) = (rs)x$ . Since  $R$  is a domain we conclude that  $rs = 1$  by Proposition 3.1.3 (if  $x \neq 0$ ). This means that  $r, s \in R^*$ . Thus,  $\langle x \rangle = \langle y \rangle$  implies that there exists  $u \in R^*$  such that  $x = uy$ . In this case we say that  $x$  and  $y$  are *associated elements* of  $R$ .

An element  $d \in R$  is a *greatest common divisor* of  $a, b \in R$  if  $d$  is a common divisor of  $a$  and  $b$  and every common divisor of  $a$  and  $b$  divides  $d$ . Notice how this generalizes the greatest common divisor definition for the integers (see Section 1.4).

Let  $R$  be a principal ideal domain. For every  $a, b \in R$  we know that there exists  $d \in R$  such that  $\langle a, b \rangle = \{xa + yb \mid x, y \in R\} = \langle d \rangle$ . We claim that  $d$  is a greatest common divisor of  $a$  and  $b$ . Clearly  $d$  is a common divisor of  $a$  and  $b$  since  $\langle a \rangle \subseteq \langle d \rangle$  and  $\langle b \rangle \subseteq \langle d \rangle$ . If  $e$  is a common divisor of  $a$  and  $b$  then  $\langle e \rangle \supseteq \langle a, b \rangle = \langle d \rangle$ . Thus  $e$  divides  $d$  and so  $d$  is a greatest common divisor of  $a$  and  $b$ .

### 3.5.2 Irreducible elements

An element  $r \in R \setminus R^*$  is called *irreducible* if  $r = ab$  for  $a, b \in R$  implies that either  $a$  or  $b$  is a unit. Thus if  $r$  is an irreducible element and  $u$  is a unit then  $ur$  is also an irreducible element. A non-zero element  $x \in R \setminus R^*$  is said to have a *factorization into irreducible elements* if there exist irreducible elements  $p_1, \dots, p_r \in R$  such that

$$x = p_1 \cdots p_r.$$

Now  $x$  is said to have *unique factorization into irreducible elements* if for any other irreducible factorization

$$x = q_1 \cdots q_s,$$

every  $p_i$  for  $i = 1, \dots, r$  divides  $q_j$  for some  $j = 1, \dots, s$  (this implies that  $p_i = uq_j$ , where  $u$  is a unit). In particular we have  $r = s$  by Proposition 3.1.3. A domain  $R$  such that every non-zero element in  $R \setminus R^*$  has unique factorization into irreducible elements is called a *unique factorization domain*.

**Example 3.5.1** The irreducible elements in the ring of integers are  $\pm p$ , where  $p$  is a prime number. So  $\mathbb{Z}$  is a unique factorization domain by Theorem 1.8.5.



We do not know yet whether the ring of Gaussian integers  $\mathbb{Z}[i]$  is a unique factorization domain. This will follow once we have proved that a principal ideal domain is a unique factorization domain.

### 3.5.3 Prime elements

A non-zero element  $p \in R \setminus R^*$  is called a *prime element* if  $p \mid xy$  for  $x, y \in R$  implies that  $p \mid x$  or  $p \mid y$ .

**Proposition 3.5.2** *A prime element is irreducible.*

*Proof.* Let  $p$  be a prime element. Suppose that  $p = ab$ . By definition of a prime element we can conclude that  $p \mid a$  or  $p \mid b$ . Suppose that  $p \mid a$ . Then we can write  $a = rp$  for some  $r \in R$ . This implies that  $p = rpb$ . Now Proposition 3.1.3 gives that  $b$  is a unit. Thus  $p$  is irreducible.  $\square$

**Proposition 3.5.3** *Let  $R$  be a ring for which every non-zero element  $x \in R \setminus R^*$  has a factorization into irreducible elements. Every irreducible element is a prime element in  $R$  if and only if  $R$  is a unique factorization domain.*

*Proof.* The “only if” part is identical to the proof of unique factorization for the integers (see Theorem 1.8.5). Suppose that  $x \in R$  is a non-zero element with two factorizations:

$$x = p_1 \cdots p_r = q_1 \cdots q_s.$$

Now fix an irreducible element  $p_i$  from the left hand side. Since  $p_i$  is a prime element dividing a product  $q_1 \cdots q_s$ , it must divide some  $q_j$  (see Remark 1.8.4). Let us prove the “if” part. Assume that  $R$  is a unique factorization domain and let  $p \in R$  be an irreducible element. Suppose that  $p \mid ab$ , where  $a, b \in R$ . We must prove that  $p \mid a$  or  $p \mid b$ . Assume that  $ab \neq 0$ . Then  $a$  and  $b$  have factorizations into irreducible elements. Because of unique factorization, one of these factorizations must contain an irreducible element divisible by  $p$ . This proves the “if” part.  $\square$

**Remark 3.5.4** The subset  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$  is a subring of  $\mathbb{C}$ . In  $\mathbb{Z}[\sqrt{-5}]$  we have two different factorizations of 6:

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

Both factorizations turn out to be irreducible, so that in this case the irreducible factorizations are not unique. Let us prove that 2 is an irreducible element of  $\mathbb{Z}[\sqrt{-5}]$  that is not a prime element. From the above we see that  $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ . But 2 does not divide either of these factors. Assume for example that  $2 \mid 1 + \sqrt{-5}$ . Then there exists  $z \in \mathbb{Z}[\sqrt{-5}]$  such that  $2z = 1 + \sqrt{-5}$ . But this would show that

$$z = \frac{1}{2} + \frac{1}{2}\sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}].$$

As in the case of the Gaussian integers (Example 3.1.5) the norm function  $N(z) = z\bar{z}$  gives a function  $N : \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{N}$  such that  $N(z_1 z_2) = N(z_1)N(z_2)$ , where  $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$ . If  $z = x + y\sqrt{-5}$  then  $N(x + y\sqrt{-5}) = (x + y\sqrt{-5})(x - y\sqrt{-5}) = x^2 + 5y^2$ . Again it is easy to show that  $z \in \mathbb{Z}[\sqrt{-5}]^*$  if and only if  $N(z) = 1$ . This gives that  $z = x + y\sqrt{-5}$  is a unit if and only if  $x = \pm 1$  and  $y = 0$ . To prove that 2 is an irreducible element, we assume that  $2 = ab$ , where  $a = x + y\sqrt{-5}$  and  $b = x' + y'\sqrt{-5}$ . The crucial point is now to use the norm function. This gives  $N(2) = 4 = N(a)N(b) = (x^2 + 5y^2)(x'^2 + 5y'^2)$ , where  $x, y, x', y' \in \mathbb{Z}$ . We must have  $y = y' = 0$  (why?), showing that one of  $a$  or  $b$  is a unit.

The following lemma is analogous to the statement that every non-zero integer is a product of prime numbers (Lemma 1.8.1).

**Lemma 3.5.5** *Let  $R$  be a principal ideal domain and  $r$  a non-zero element. Then  $r$  has an irreducible factorization.*

*Proof.* An increasing sequence (a chain) of principal ideals  $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$  in  $R$  must stabilize: there is a step  $N \in \mathbb{N}$  such that  $\langle a_i \rangle = \langle a_{i+1} \rangle = \cdots$  for  $i \geq N$ . This is proved using that the union

$$\bigcup_{i=1}^{\infty} \langle a_i \rangle$$

is an ideal  $I$  in  $R$  (see Exercise 3.9, where you are also asked to show that the union of two ideals is not necessarily an ideal). From this we get  $I = \langle d \rangle$ , for some  $d \in R$ , since every ideal in  $R$  is principal. By definition of union, we must have  $d \in \langle a_N \rangle$  for some  $N$ . Thus  $\langle d \rangle \subseteq \langle a_N \rangle$  showing that  $\langle a_i \rangle = \langle d \rangle$  for  $i \geq N$ .

Suppose that  $r \in R \setminus R^*$  is a non-zero element that is not a product of irreducible elements. Then  $r$  is not irreducible. So we can write  $r = r_1 s_1$  where  $r_1, s_1 \notin R^*$ . This means that  $\langle r \rangle \subsetneq \langle r_1 \rangle$  and  $\langle r \rangle \subsetneq \langle s_1 \rangle$ . If both  $r_1$  and  $s_1$  are

products of irreducible elements then so is  $r$ , contradicting our assumption. So, at least one of  $r_1$  and  $s_1$  is *not* a product of irreducible elements. Assume that  $r_1$  is not a product of irreducible elements. Again we can write  $r_1 = r_2 s_2$ , where  $r_2, s_2 \notin R^*$ ,  $\langle r_1 \rangle \subsetneq \langle r_2 \rangle$  and  $\langle r_1 \rangle \subsetneq \langle s_2 \rangle$ . We may assume that  $r_2$  is not a product of irreducible elements. Continuing in this way we obtain the infinite chain

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_2 \rangle \subsetneq \cdots,$$

where no  $r_i$  is a product of irreducible elements. This is a chain of ideals that does not stabilize, contradicting the first part of the proof. Thus every non-zero element  $r$  which is not a unit is a product of irreducible elements.  $\square$

**Proposition 3.5.6** *Suppose that  $R$  is a principal ideal domain that is not a field. An ideal  $\langle x \rangle \subseteq R$  is a maximal ideal if and only if  $x$  is an irreducible element in  $R$ .*

*Proof.* If  $x$  is irreducible in  $R$  and  $\langle x \rangle$  is contained in another ideal  $\langle y \rangle$  then  $x = ys$  for some  $s \in R$ . Since  $x$  is irreducible this implies that  $s$  or  $y$  is a unit. Thus  $\langle y \rangle = \langle x \rangle$  or  $\langle y \rangle = R$ , showing that  $\langle x \rangle$  is a maximal ideal. However, if  $\langle x \rangle$  is a maximal ideal and  $x = ys$  for some  $y, s \in R$  then one of  $y$  and  $s$  must be a unit. If not, then  $\langle x \rangle$  would be strictly contained in  $\langle y \rangle$  since  $s$  is not a unit. Since  $y$  is not a unit,  $\langle y \rangle$  must be strictly contained in  $R$  contradicting that  $\langle x \rangle$  is a maximal ideal.  $\square$

**Theorem 3.5.7** *A principal ideal domain  $R$  is a unique factorization domain.*

*Proof.* In Lemma 3.5.5 we proved that every non-zero element has an irreducible factorization. The only thing missing is to prove that such a factorization is unique. This is accomplished, using Proposition 3.5.3, by proving that the irreducible elements are prime. Let  $\pi \in R$  be an irreducible element such that  $\pi \mid ab$  and  $\pi \nmid a$ . We will prove that  $\pi \mid b$ . That  $\pi \nmid a$  implies  $a \notin \langle \pi \rangle$  and therefore  $\langle \pi, a \rangle \supsetneq \langle \pi \rangle$ . Since  $\langle \pi \rangle$  is a maximal ideal, by Proposition 3.5.6, it follows that  $\langle \pi, a \rangle = R = \langle 1 \rangle$ . So we can find  $x, y \in R$  such that  $x\pi + ya = 1$ . Now multiply both sides by  $b$  and get  $xb\pi + yab = b$ . Since  $\pi \mid ab$ , this shows that  $\pi \mid b$ . You should compare this to the proof of Corollary 1.5.10. They are practically identical except that here we have a more general framework.  $\square$

**Remark 3.5.8** The ring  $\mathbb{Z}[\sqrt{-5}]$  is not a principal ideal domain since 2 is an irreducible element that is not a prime element (see Remark 3.5.4). In fact we can explicitly give an example of an ideal  $I$  in  $\mathbb{Z}[\sqrt{-5}]$  that is not a principal

ideal. Let  $I = \langle 2, 1 + \sqrt{-5} \rangle$ . By explicit computation and a little rewriting one may prove that  $I = \{(2a + b) + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ . This implies that  $1 \notin I$ , so that  $I \neq R$ . Let us assume that  $I = \langle d \rangle$  for some  $d \in \mathbb{Z}[\sqrt{-5}]$ . Recall that  $N(x + y\sqrt{-5}) = x^2 + 5y^2$ , where  $x, y \in \mathbb{Z}$ . As  $d$  is not a unit, we get  $N(d) > 1$ . Since  $d$  divides every element of  $I$ , it must divide 2. Therefore  $N(d) \mid N(2) = 4$  and we must have  $N(d) = 4$ , since  $N(d) = 2$  is impossible. But  $N(d) = 4$  means that we can assume that  $d = 2$ . But  $1 + \sqrt{-5} \notin \langle 2 \rangle$ , since  $2 \nmid 1 + \sqrt{-5}$ . We have proved that  $\langle 2, 1 + \sqrt{-5} \rangle$  cannot be a principal ideal.

Suppose that we are given two elements  $a, b$  in a unique factorization domain. Suppose furthermore that we have found prime elements  $p_1, \dots, p_n$  such that

$$\begin{aligned} a &= p_1^{r_1} \cdots p_n^{r_n}, \\ b &= p_1^{s_1} \cdots p_n^{s_n}, \end{aligned}$$

where  $r_i, s_i \geq 0$ . Then a greatest common divisor (see subsection 3.5.1) of  $a$  and  $b$  is given by

$$c = p_1^{t_1} \cdots p_n^{t_n},$$

where  $t_i = \min(r_i, s_i)$ ; compare this with Remark 1.8.6. Usually it is very difficult (as for  $\mathbb{Z}$ ) to compute prime factorizations of elements effectively. So relying on prime factorizations for finding a greatest common divisor may be a slow process. The Euclidean algorithm is in general much faster, but it does not necessarily exist in domains more general than  $\mathbb{Z}$ . If it does, there is a special term for the domain, as follows.

### 3.5.4 Euclidean domains

A domain  $R$  is called Euclidean if there exists a Euclidean function  $N : R \setminus \{0\} \rightarrow \mathbb{N}$ . A Euclidean function satisfies that for every  $x \in R$ ,  $d \in R \setminus \{0\}$ , there exist  $q, r \in R$  such that

$$x = qd + r,$$

where either  $r = 0$  or  $N(r) < N(d)$ .

The ring of integers  $\mathbb{Z}$  carries the absolute value  $|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$  as a Euclidean function. Using Theorem 1.2.1 it is easy to verify that for every  $x \in \mathbb{Z}$ ,  $d \in \mathbb{Z} \setminus \{0\}$ , there exist  $q, r \in \mathbb{Z}$  such that

$$x = qd + r,$$

where  $r = 0$  or  $|r| < |d|$ . After having seen the proof of Theorem 3.1.11, the following proposition should come as no surprise.

**Proposition 3.5.9** *A Euclidean domain  $R$  is a principal ideal domain.*

*Proof.* Let  $I \subset R$  be a non-zero ideal in  $R$  and let  $x \in I$  be a non-zero element such that  $N(x)$  is minimal (compared with every  $N(y)$ , where  $y \in I \setminus \{0\}$ ). We claim that  $I = Rx$ . Suppose that  $y \in I$ . Then we may find  $q \in R$  such that

$$y = qx + r$$

where  $r = 0$  or  $N(r) < N(x)$ . But as  $r = y - qx \in I$ , we must have  $r = 0$  since  $N(x)$  is minimal among  $N(z)$ , where  $z$  runs through the non-zero elements of  $I$ . This means that  $y = qx$  and thus  $I = Rx$ .  $\square$

Recall the definition in subsection 3.5.1 of a greatest common divisor along with the description of it in a principal ideal domain. A greatest common divisor of two elements in a Euclidean domain  $R$  can be found using the Euclidean algorithm (hence the term Euclidean). Here is how this works. Let  $N : R \setminus \{0\} \rightarrow \mathbb{N}$  be a Euclidean function and suppose that  $a, b \in R$ . A greatest common divisor is a generator for the (principal) ideal  $\langle a, b \rangle$ .

If either  $a$  or  $b$  is zero, we are done. Suppose that both  $a$  and  $b$  are non-zero and that  $N(a) \geq N(b)$ . Then there exists  $q \in R$  such that  $a = qb + r$ , where either  $r = 0$  or  $N(r) < N(b)$ . We have  $\langle a, b \rangle = \langle b, r \rangle$  since  $r = a - qb \in \langle a, b \rangle$  and  $a = qb + r \in \langle b, r \rangle$ . Continue the procedure with  $a = b$  and  $b = r$  until one of  $a$  and  $b$  is zero. This will eventually happen, since we are strictly decreasing the maximum value of the norm function of  $a$  and  $b$  in each step. You should work out Exercise 3.29 to practice the Euclidean algorithm in the Gaussian integers with the norm function (you can do that before seeing the proof that  $\mathbb{Z}[i]$  with the norm function is a Euclidean domain).

**Remark 3.5.10** A principal ideal domain is not a Euclidean domain in general. The ring  $R = \mathbb{Z}[\xi] = \{x + y\xi \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$ , where  $\xi = (1 + \sqrt{-19})/2$ , is an example of a principal ideal domain that is not a Euclidean domain. One may prove that  $R$  cannot be a Euclidean domain using  $R^* = \{\pm 1\}$ . Proving that  $R$  is a principal ideal domain is more difficult.

We will see later that polynomial rings in one variable over a field are Euclidean domains (using the degree function). A nice fact is that the ring

of Gaussian integers is a Euclidean domain. This can actually be proved by drawing circles in the complex plane.

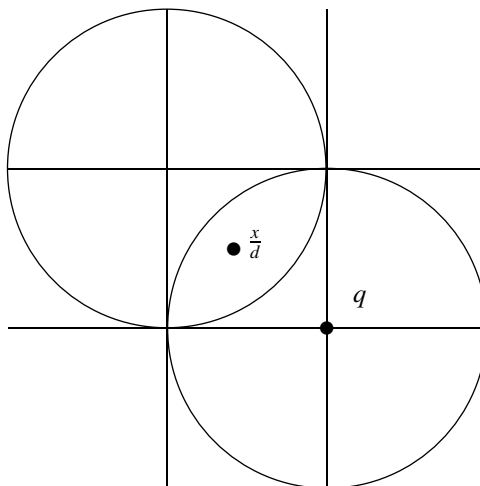
### 3.5.5 Fermat's two-square theorem

A beautiful result due to Fermat says that a prime number  $p \equiv 1 \pmod{4}$  is the sum of two unique squares (e.g.  $13 = 4 + 9$ ). We will prove this result using unique factorization in the ring of Gaussian integers  $\mathbb{Z}[i]$ . Recall the norm function  $N : \mathbb{Z}[i] \rightarrow \mathbb{N}$  given by  $N(a + bi) = (a + bi)(a - bi) = |a + bi|^2 = a^2 + b^2$ . This function is an invaluable tool in reasoning about Gaussian integers. Here is an example.

**Proposition 3.5.11** *Let  $\pi = a + bi \in \mathbb{Z}[i]$  be a Gaussian integer with  $N(\pi) = p$ , where  $p$  is a prime number. Then  $\pi$  is a prime element in  $\mathbb{Z}[i]$ .*

*Proof.* It suffices to check that  $\pi$  is an irreducible element by Theorems 3.1.11 and 3.5.7 and Proposition 3.5.3. Assume that  $\pi = ab$ . Then  $N(\pi) = N(a)N(b)$ . This means that  $N(a) = p$  or  $N(b) = p$ . If for example  $N(a) = p$  then  $N(b) = 1$  and  $b$  is a unit (see Example 3.1.5). So  $\pi$  is irreducible.  $\square$

We have indicated in the proof of Theorem 3.1.11 that  $\mathbb{Z}[i]$  is a Euclidean domain. Let us give some more details. Given  $x \in \mathbb{Z}[i]$  and  $d \in \mathbb{Z}[i] \setminus \{0\}$ , we can form  $x/d \in \mathbb{Q}[i]$ .



The above picture shows that we may find  $q = q_1 + iq_2 \in \mathbb{Z}[i]$  such that

$$\left| \frac{x}{d} - q \right|^2 < 1.$$

Multiplying both sides by  $N(d)$  and using  $N(ab) = N(a)N(b)$  we get  $N(x - qd) < N(d)$ , showing that  $\mathbb{Z}[i]$  is a Euclidean domain and hence a principal ideal domain and a unique factorization domain. Let us dig a little deeper into the prime elements in  $\mathbb{Z}[i]$ . We wish to prove that prime numbers congruent to 1 modulo 4 fail to be prime elements in  $\mathbb{Z}[i]$ . This agrees with the examples  $5 = (2 + i)(2 - i)$  and  $13 = (3 + 2i)(3 - 2i)$ . First, a classical result that deserves to be singled out:

**Lemma 3.5.12 (Lagrange)** *Let  $p$  be a prime number. If  $p \equiv 1 \pmod{4}$  then the congruence*

$$x^2 \equiv -1 \pmod{p}$$

*can be solved by  $x = (2n)!$  where  $p = 4n + 1$ .*

*Proof.* This is a consequence of Wilson's theorem, which says that  $(4n)! \equiv -1 \pmod{p}$  (see Exercise 1.29(ii)). Write  $(4n)!$  as

$$4n(4n-1) \cdots (4n-2n+1)2n(2n-1) \cdots 2 \cdot 1.$$

Since  $4n \equiv -1 \pmod{p}$ ,  $4n-1 \equiv -2 \pmod{p}$ ,  $\dots$ ,  $4n-2n+1 \equiv -2n \pmod{p}$  it follows that  $-1 \equiv (4n)! \equiv ((2n)!)^2$ . Thus  $x = (2n)!$  solves the congruence.  $\square$

**Remark 3.5.13** There is another proof of Lemma 3.5.12, which in a way is simpler. It also suggests an effective algorithm for computing a solution to the congruence  $x^2 \equiv -1 \pmod{p}$ . Suppose that  $a$  is a quadratic non-residue modulo  $p$  (see Section 1.11). Then we know by Theorem 1.11.4 that

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

So when  $p \equiv 1 \pmod{4}$ ,  $x = a^{(p-1)/4}$  (or its remainder  $[a^{(p-1)/4}]_p$ , which can be computed effectively using repeated squaring) is a solution to  $x^2 \equiv -1 \pmod{p}$ .

**Corollary 3.5.14** *A prime number  $p \equiv 1 \pmod{4}$  is not a prime element in  $\mathbb{Z}[i]$ .*

*Proof.* By Lemma 3.5.12 we can find an integer  $x$  such that  $x^2 \equiv -1 \pmod{p}$ . Then  $p \mid x^2 + 1 = (x + i)(x - i)$ . But  $p \nmid x + i$  and  $p \nmid x - i$ , since  $x/p + (1/p)i \notin \mathbb{Z}[i]$  and  $x/p - (1/p)i \notin \mathbb{Z}[i]$ . This shows that  $p$  is not a prime element in  $\mathbb{Z}[i]$ .  $\square$

Let us move on to prove Fermat's famous two-square theorem.

**Theorem 3.5.15 (Fermat)** *A prime number  $p \equiv 1 \pmod{4}$  is a sum of two uniquely determined squares.*

*Proof.* Assume that  $p = a^2 + b^2$  for some integers  $a, b \in \mathbb{Z}$ . Then  $x = a + bi$  is an element of  $\mathbb{Z}[i]$  with  $N(x) = p$ . So  $x$  is a prime element by Proposition 3.5.11. If  $p = c^2 + d^2$  for some other integers  $c, d \in \mathbb{Z}$  then  $p = (c + id)(c - id) = (a + bi)(a - bi)$  gives two irreducible factorizations of  $p$ . Now the uniqueness of the squares can be deduced from the fact that  $p$  has a unique irreducible factorization and  $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$ . For example, if  $c + di \mid a + bi$  then  $a + bi = u(c + di)$ , where  $u \in \mathbb{Z}[i]^*$ . The four units correspond to the following cases:  $c = a, d = b$ ;  $c = -a, d = -b$ ;  $c = b, d = -a$ ;  $c = -b, d = -a$ . These cases show that the squares are unique.

For the existence we need to prove that a prime number  $p \equiv 1 \pmod{4}$  is a sum of two squares. We know by Corollary 3.5.14 that  $p$  is not a prime element in  $\mathbb{Z}[i]$ . Let  $\pi = a + bi \in \mathbb{Z}[i]$  be a prime element such that  $p = \pi x$ , where  $x \in \mathbb{Z}[i]$ . Then  $x$  is not a unit (if  $x$  were a unit then  $p$  would be a prime element) and so  $N(x) > 1$ . This means that  $N(\pi) = p$ , since  $p^2 = N(p) = N(\pi)N(x)$ . But then  $N(\pi) = \pi\bar{\pi} = a^2 + b^2 = p$  and we have expressed  $p$  as a sum of two squares.  $\square$

### 3.5.6 The Euclidean algorithm strikes again

We have proved that every prime number  $p$  congruent to 1 modulo 4 is a sum of two squares. So far, trial and error has enabled us to guess identities like  $5 = 1^2 + 2^2$ ,  $13 = 3^2 + 2^2$ ,  $\dots$ . There is a beautiful algorithm (due to Cornacchia, based on a continued-fractions algorithm due to Serret and Hermite) for finding the two squares that sum up to  $p$ .

We will describe the algorithm but leave out the proof that it works (see [25] for the proof or do Exercise 3.40 (HOF) on your own – the title of this subsection is the title of [25]). The key point is to compute  $x \in \mathbb{N}$  such that  $x^2 \equiv -1 \pmod{p}$ . This can be done effectively using Remark 3.5.13. Pick a number  $a = 1, 2, \dots, p - 1$  at random. Since the numbers of quadratic residues



and quadratic non-residues modulo  $p$  are the same, the probability that  $a$  is a quadratic non-residue is  $1/2$ . If this is so then  $a^{(p-1)/2} \equiv -1$  and Remark 3.5.13 gives the solution. If not, try another random  $a$ . The probability of not having encountered a quadratic non-residue after  $n$  trials is  $(1/2)^n$ .

Suppose that  $x$  is a solution to the congruence  $x^2 \equiv -1 \pmod{p}$ . We may assume that  $0 < x < p/2$  (why?). Then use the Euclidean algorithm on  $p$  and  $x$ . The first two remainders  $a, b < \sqrt{p}$  satisfy  $p = a^2 + b^2$ . Here are some examples.

**Example 3.5.16** Let  $p = 41$ . Then  $x = 9$  satisfies  $x^2 \equiv -1 \pmod{p}$ . Let us apply the Euclidean algorithm to 41 and 9 (see Example 1.5.5).

$i$	-1	0	1	2	3	4
$r_i$	41	9	5	4	1	0
$q_i$			4	1	1	4
$a_i$	1	0	1	-1	2	-9
$b_i$	0	1	-4	5	-9	41

The first two remainders  $< \sqrt{41}$  are 5 and 4, and  $41 = 5^2 + 4^2$ .

**Example 3.5.17** Let  $p = 113$ . Then  $x = 15$  satisfies  $x^2 \equiv -1 \pmod{p}$ . Let us apply the Euclidean algorithm to 113 and 15:

$i$	-1	0	1	2	3	4
$r_i$	113	15	8	7	1	0
$q_i$			7	1	1	7
$a_i$	1	0	1	-1	2	-15
$b_i$	0	1	-7	8	-15	113

The first two remainders  $< \sqrt{113}$  are 8 and 7, and  $113 = 8^2 + 7^2$ .

There are many patterns in the above examples. If you look at the row with remainders then it appears backwards, up to a sign in the bottom row. Notice also that the algorithm seems to stop after an even number of steps  $n$  and that  $p \mid r_j^2 + r_{n-j-2}^2$  for  $j = -2, -1, 0, \dots, n$ . These facts and the complete proof that the algorithm works can be found in [25].

### 3.5.7 Prime numbers congruent to 1 modulo 4

Euclid proved that there are infinitely many prime numbers. His proof can be extended to the stronger statement that there are infinitely many prime numbers

congruent to 1 modulo 4. Here we show how the Gaussian integers help us in proving this statement.

**Lemma 3.5.18** *A prime number  $p \equiv 3 \pmod{4}$  is a prime element in  $\mathbb{Z}[i]$ .*

*Proof.* Let  $\pi = c + id \in \mathbb{Z}[i]$  be a prime element dividing  $p$ . Write this as  $p = \pi x$  for  $x \in \mathbb{Z}[i]$ . Then  $N(\pi)N(x) = N(p) = p^2$ . Thus  $N(\pi) = p$  or  $N(\pi) = p^2$ . If  $N(\pi) = \pi\bar{\pi} = c^2 + d^2 = p$  then  $p$  is the sum of two squares, but the sum of two squares is not congruent to 3 modulo 4 (see Exercise 3.32). So we must have  $N(\pi) = p^2$ . Therefore  $N(x) = 1$ ,  $x$  is a unit and  $p$  is a prime element, since it is a unit times a prime element.  $\square$

**Corollary 3.5.19** *If  $p$  is an odd prime number dividing  $x^2 + 1$  for some  $x \in \mathbb{Z}$  then  $p \equiv 1 \pmod{4}$ .*

*Proof.* Let  $p$  be a prime number dividing  $x^2 + 1$ . If  $p \equiv 3 \pmod{4}$  then  $p$  is a prime element in  $\mathbb{Z}[i]$ . Thus  $p \mid (x^2 + 1) = (x + i)(x - i)$ , but  $p$  does not divide either  $x + i$  or  $x - i$ . So we must have  $p \equiv 1 \pmod{4}$ .  $\square$

**Theorem 3.5.20** *There are infinitely many primes congruent to 1 modulo 4.*

*Proof.* Suppose there are only finitely many prime numbers  $q_1, \dots, q_s$  congruent to 1 modulo 4. Then form the number

$$N = (q_1 q_2 \cdots q_s)^2 + 1.$$

By Corollary 3.5.19,  $N$  is divisible by a prime  $p \equiv 1 \pmod{4}$ . But  $p \notin \{q_1, \dots, q_s\}$ , since  $q_i \nmid N$  for  $i = 1, \dots, s$ .  $\square$

**Remark 3.5.21** A celebrated result of Dirichlet (1805–59) states that an arithmetic progression

$$b, \quad b + a, \quad b + 2a, \quad b + 3a, \quad \dots$$

contains infinitely many primes if  $a$  and  $b$  are relatively prime. It is one of the truly deep theorems of number theory (we have just seen that the case  $b = 1$  and  $a = 4$  is not particularly easy). We will prove that there are infinitely many primes  $\equiv 1 \pmod{n}$  for every  $n \geq 2$  after having introduced cyclotomic polynomials in Chapter 4.

### 3.5.8 Fermat's last theorem

Suppose we wish to prove Fermat's last theorem (FLT) for  $n = 3$ :  $x^3 + y^3 = z^3$  has no solutions, assuming that  $x$ ,  $y$  and  $z$  are non-zero natural numbers. A very fruitful idea is to view the identity  $x^3 + y^3 = z^3$  in a ring containing not only the integers but also complex numbers! In fact putting  $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ , we have  $\omega^2 + \omega + 1 = 0$  and

$$x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y). \quad (3.3)$$

This factorization does not make sense in the ring  $\mathbb{Z}$ , but in the enlarged ring  $\mathbb{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbb{Z}\}$ .

One can prove that  $\mathbb{Z}[\omega]$  is a unique factorization domain. A further analysis [12] of the identity (3.3) in the ring  $\mathbb{Z}[\omega]$  (using the prime element  $1 - \omega$ ) proves FLT for  $n = 3$ . For any odd prime number  $p$  we have the factorization

$$x^p + y^p = (x + y)(x + \omega y) \cdots (x + \omega^{p-1} y)$$

in the ring  $\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} \mid a_0, \dots, a_{p-2} \in \mathbb{Z}\}$ , where  $\omega = e^{2\pi i/p}$ . In 1847 Lamé (1795–1870) announced to the French academy that he had proved FLT. His “proof” was based on the (wrong) assumption that  $\mathbb{Z}[\omega]$  is a unique factorization domain for all primes  $p$ . A letter from Kummer (1810–93) pointed out the mistake and introduced “ideal complex numbers” to restore unique factorization. Kummer proved the remarkable theorem that FLT holds for an odd prime number  $p$  if  $p$  does not divide the numerator of any of the Bernoulli numbers  $B_2, B_4, \dots, B_{p-3}$  (such a prime number is called regular). The Bernoulli numbers are given by the coefficients  $B_n$  in the power series expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$$

and can be computed using a variant of Newton's method ([5], Section 4.4). The first few Bernoulli numbers are

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \quad B_5 = 0, \quad B_6 = \frac{1}{42}.$$

Using Kummer's result we see that FLT holds for  $p = 3, 5, 7$ . The thirty-second Bernoulli number is

$$-\frac{7709321041217}{510}.$$

Since  $7709321041217 = 37 \cdot 683 \cdot 305065927$ , this shows that 37 is an irregular prime number (in fact the first). The Danish mathematician J. L. W. Jensen (1859–1925) [15] showed in 1915 that there are infinitely many irregular prime numbers. Analyzing irregular prime numbers, FLT was proved by S. Wagstaff for all  $n$  up to 125000 in 1978.

Kummer's insights led to an immense amount of important mathematics. FLT was finally proved in the early morning (EDST) of September 19, 1994 by the British mathematician Andrew Wiles of Princeton University. Wiles' proof [26] utilizes the most advanced techniques of modern mathematics and builds heavily on results obtained in the late twentieth century.

### 3.6 Exercises

1. Show that a zero divisor cannot be a unit.
2. We may view the complex numbers  $\mathbb{C}$  as the real plane  $\mathbb{R}^2$  with basis 1 and  $i$ . This means that the real plane as an abelian group can be equipped with a multiplication making it into a field. Can we extend this multiplication to obtain a ring multiplication on  $\mathbb{R}^3$ ? View  $\mathbb{R}^3$  as  $a + bi + cj$ , where  $a, b, c \in \mathbb{R}$ . Suppose that we have a multiplication on  $\mathbb{R}^3$ , making it into a ring, such that  $ii = i^2 = -1$ . Then  $ij = x + yi + zj$  for  $x, y, z \in \mathbb{R}$ . Multiply both sides of this equation by  $i$  to show that such a multiplication cannot exist (however, if you add one more dimension then you can obtain a multiplication, as we saw in Example 3.1.2).
3. Let  $R$  be a ring. Prove that  $0 \cdot x = 0$  and  $-x = (-1) \cdot x$  for every  $x \in R$ .
4. Prove that an ideal  $I$  in a ring  $R$  is the whole ring if and only if  $1 \in I$ .
5. Let  $R$  be a ring and  $r_1, \dots, r_n \in R$ . Prove that the subset  $\langle r_1, \dots, r_n \rangle = \{\lambda_1 r_1 + \dots + \lambda_n r_n \mid \lambda_1, \dots, \lambda_n \in R\}$  is an ideal in  $R$ .
6. Let  $I$  be an ideal in a ring  $R$ . Prove that  $\langle r_1, \dots, r_n \rangle \subseteq I$  if  $r_1, \dots, r_n \in I$ .
7. Let  $M$  be a subset of a ring  $R$ . Prove that  $\langle f \mid f \in M \rangle$  (see Remark 3.1.6) is an ideal.
8. Let  $I$  and  $J$  be ideals in the ring  $R$ .
  - (i) Prove that

$$I \cap J$$

is an ideal in  $R$ .

- (ii) Prove that

$$I + J = \{a + b \mid a \in I, b \in J\}$$

is an ideal in  $R$ .

(iii) Prove that

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid n \geq 1, a_i \in I, b_i \in J \right\}$$

is an ideal in  $R$ .

(iv) Prove that  $IJ \subseteq I \cap J$ . Give an example where  $IJ \subsetneq I \cap J$ .

(v) Is  $\{ab \mid a \in I, b \in J\}$  an ideal in  $R$ ?

9. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be an increasing sequence of ideals in a ring  $R$ . Prove that the union of the ideals is an ideal. Give an example of two ideals  $I$  and  $J$  such that  $I \cup J$  is not an ideal.

10. Let  $R$  be a ring with the property that every ideal  $I \subseteq R$  is finitely generated i.e. there are finitely many elements  $r_1, \dots, r_n \in R$  such that  $I = \langle r_1, \dots, r_n \rangle$  (such a ring is called *noetherian*).

(i) Prove that an increasing sequence (chain) of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

must stabilize, i.e. there is a natural number  $N$  such that

$$I_N = I_{N+1} = \cdots$$

(ii) Is an ideal  $J \neq R$  in a noetherian ring contained in a maximal ideal?

11. Prove that the kernel  $\text{Ker } f = \{r \in R \mid f(r) = 0\} \subseteq R$  of a ring homomorphism  $f : R \rightarrow S$  is an ideal of  $R$  and that the image  $f(R)$  is a subring of  $S$ .

12. (i) Find integers  $\lambda, \mu \in \mathbb{Z}$  such that

$$49\lambda + 13\mu = 1,$$

and show using this that the coset  $[13]$  is a unit in  $\mathbb{Z}/49\mathbb{Z}$ .

(ii) In the following  $R$  will denote  $\mathbb{Z}/p^l\mathbb{Z}$ , where  $p$  is a prime and  $l > 0$  a natural number. Show that  $R$  is not a domain if  $l > 1$ .

(iii) Show that the number of non-units in  $R$  is  $p^{l-1}$ .

(iv) Suppose that  $r^2 = r$  where  $r \in R$ . Show that  $r = [0]$  or  $r = [1]$ .

13. Show that the group of units  $\mathbb{Z}[i]^*$  in  $\mathbb{Z}[i]$  is isomorphic to  $\mathbb{Z}/4\mathbb{Z}$ .

14. Let  $\omega = e^{2\pi i/p}$ , where  $p \in \mathbb{N}$  and  $p > 1$ . Prove that

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} \mid a_0, \dots, a_{p-2} \in \mathbb{Z}\}$$

is a subring of  $\mathbb{C}$ .

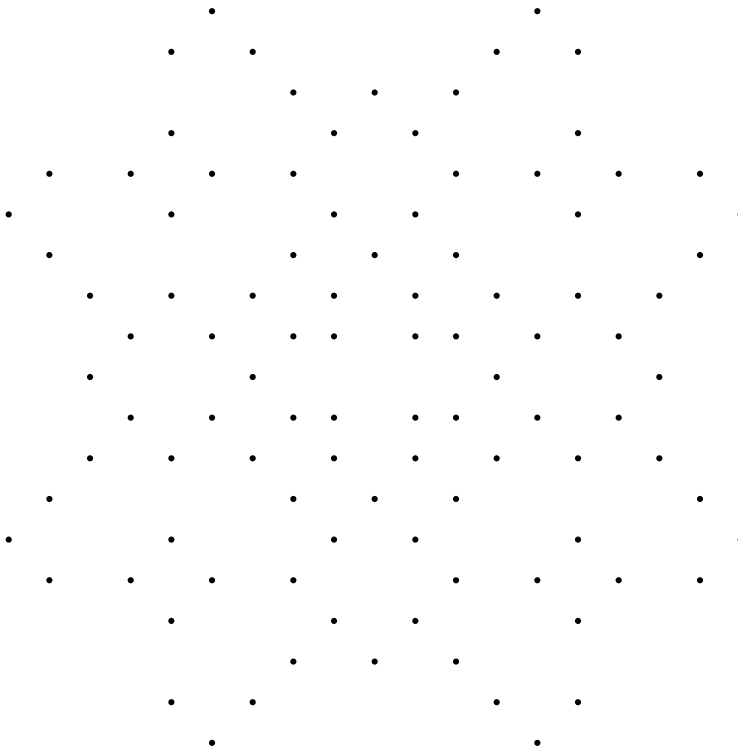
15. (i) Show that  $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$  is a subring of  $\mathbb{R}$ .  
 (ii) Show that  $\mathbb{Z}[\sqrt{2}]^*$  is infinite (hint: consider powers of  $1 + \sqrt{2}$ ).
16. Let  $R$  denote the ring  $\mathbb{Z}[i]/\langle 1 + 3i \rangle$ .  
 (i) Show that  $i - 3 \in \langle 1 + 3i \rangle$  and that  $[i] = [3]$  in  $R$ . Use this to prove that  $[10] = [0]$  in  $R$  and that  $[a + bi] = [a + 3b]$ , where  $a, b \in \mathbb{Z}$ .  
 (ii) Show that the unique ring homomorphism

$$\varphi : \mathbb{Z} \rightarrow R$$

is surjective.

- (iii) Show that  $1 + 3i$  is not a unit and that  $1 + 3i$  does not divide 2 and 5 in  $\mathbb{Z}[i]$ . Conclude that  $\text{Ker } \varphi = 10\mathbb{Z}$ .  
 (iv) Show that  $R \cong \mathbb{Z}/10\mathbb{Z}$ .
17. Let  $R$  be a commutative ring and let  $I, J$ , where  $I \subseteq J$ , be ideals in  $R$ .  
 (i) Show that  $\varphi : R/I \rightarrow R/J$  given by  $\varphi(x + I) = x + J$  is a well defined, surjective ring homomorphism.  
 (ii) Let  $R = \mathbb{Z}[i]$ . Consider  $n \in \mathbb{Z} \setminus \{0\}$  and the ideal  $I = Rn$  in  $R$ . Show that  $a + bi \in I$  if and only if  $n|a$  and  $n|b$ . Show that  $R/I$  is a finite ring.  
 (iii) Use the notation from (ii). Let  $J \neq 0$  be an ideal in  $R$ . Show that  $J \cap \mathbb{Z}$  is an ideal in  $\mathbb{Z}$  and that  $J \cap \mathbb{Z} \neq 0$ .  
 (iv) Use the notation from (ii) and (iii). Show that  $R/J$  is a finite ring.
18. Prove that a ring having characteristic zero contains a subring isomorphic to  $\mathbb{Z}$ .
19. Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Show that  $J = \text{Ker}(\varphi)$  is a prime ideal if  $S$  is a domain. Show that  $J$  is a maximal ideal if  $S$  is a field and  $\varphi$  is surjective.
20. Let  $I$  be an ideal in the ring  $R$  and let  $\pi : R \rightarrow R/I$  denote the canonical ring homomorphism.  
 (i) Let  $J \subseteq R/I$  be an ideal. Prove that  $\pi^{-1}(J)$  is an ideal containing  $I$ .  
 (ii) Let  $I' \supseteq I$  be an ideal containing  $I$ . Prove that  $\pi(I')$  is an ideal in  $R/I$ .  
 (iii) Prove that  $\pi$  and  $\pi^{-1}$  give a one to one correspondence, preserving  $\subseteq$ , between ideals in  $R$  containing  $I$  and ideals in  $R/I$ . Use this to prove that  $R/I$  is a field if and only if  $I$  is a maximal ideal.  
 (iv) List the (finitely many) ideals in  $\mathbb{Z}/24\mathbb{Z}$ .
21. Let  $R$  be a non-zero commutative ring. Prove that  $R/P$  is a domain if  $P$  is a prime ideal.
22. Let  $I$  and  $J$  be ideals and  $P$  a prime ideal of  $R$ . Prove that if  $IJ \subseteq P$  then  $I \subseteq P$  or  $J \subseteq P$ .

23. Prove that a finite domain  $F$  is a field (hint: consider  $x \in F \setminus \{0\}$  along with  $x^2, x^3, \dots$ ).
24. What is the fraction field of a field?
25. Prove that every ideal in the quotient ring  $R/I$  of a principal ideal domain  $R$  is principal. Give an example of a ring which is not a domain but for which every ideal is a principal ideal.
26. What are the units in  $\mathbb{Z}/8\mathbb{Z}$ ? Give an example of a ring  $R$  with an element  $x \neq 0, 1$  such that  $x^2 = x$ . Is  $R$  a domain? Suppose that every  $x \in R$  satisfies  $x^2 = x$ . Show that  $\text{char } R = 2$ .
27. Let  $f(z) = \bar{z}$  denote the conjugation map for a complex number  $z \in \mathbb{C}$ . Prove that  $f$  is a ring homomorphism  $\mathbb{Z}[i] \rightarrow \mathbb{Z}[i]$  and that  $f(\pi)$  is a prime element if  $\pi \in \mathbb{Z}[i]$  is a prime element.
28. Is the remainder  $r$  in the definition of a Euclidean domain unique?
29. Compute a greatest common divisor  $d$  of  $a = 4 + 5i$  and  $b = 7 + 8i$  in  $\mathbb{Z}[i]$  along with  $\lambda, \mu \in \mathbb{Z}[i]$  such that  $\lambda a + \mu b = d$ .
30. Let  $\mathbb{Z}[\omega] = \{x + \omega y \mid x, y \in \mathbb{Z}\}$ , where  $\omega^2 + \omega + 1 = 0$ . Let  $z = x + \omega y \in \mathbb{Z}[\omega]$  and let  $\bar{z}$  denote the complex conjugate of  $z$ .
  - (i) Prove that  $N(z) = z\bar{z} = x^2 - xy + y^2$  and that  $N(z_1 z_2) = N(z_1)N(z_2)$ . Show that  $z \in \mathbb{Z}[\omega]$  is a unit if and only if  $N(z) = 1$ .
  - (ii) Prove that  $z \in \mathbb{Z}[\omega]$  is irreducible if  $N(z)$  is a prime number.
  - (iii) Prove that  $\mathbb{Z}[\omega]$  is a Euclidean domain.
  - (iv) Prove that  $1 - \omega$  is a prime element in  $\mathbb{Z}[\omega]$ .
31. Is  $\mathbb{Z}[\sqrt{-3}] = \{x + y\sqrt{-3} \mid x, y \in \mathbb{Z}\}$  a Euclidean ring?
32. Prove that the square of a number is either  $\equiv 0 \pmod{4}$  or  $\equiv 1 \pmod{4}$ .
33. Let  $\pi$  denote a prime element in  $\mathbb{Z}[i]$  such that  $\pi \notin \mathbb{Z}, i\mathbb{Z}$ . Prove that  $N(\pi) = 2$  or  $N(\pi) = p$ , where  $p$  is a prime number  $\equiv 1 \pmod{4}$ . Give a complete classification of the prime elements in  $\mathbb{Z}[i]$  using the prime numbers in  $\mathbb{Z}$ .
34. Prove that there are infinitely many prime numbers  $\equiv 3 \pmod{4}$  by imitating the proof of Theorem 1.8.2 with  $N = 4p_1 \cdots p_n - 1$ .
35. How do you write 221 as a sum of two squares using that  $17 = 1^2 + 4^2$  and  $13 = 2^2 + 3^2$ ?
36. Show that 51 is not a sum of two squares.
37. Write 137 as a sum of two squares using the algorithm outlined in subsection 3.5.6.
38. How do the points shown in the following diagram relate to the Gaussian integers?



39. Let  $p$  be a prime number. Define

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{s} \in \mathbb{Q} \mid p \nmid s \right\} \subseteq \mathbb{Q}.$$

- (i) Prove that  $\mathbb{Z}$  is a subring of  $\mathbb{Z}_{(p)}$  and that  $\mathbb{Z}_{(p)}$  is a subring of  $\mathbb{Q}$ . Show that the field of fractions of  $\mathbb{Z}_{(p)}$  is isomorphic to  $\mathbb{Q}$ .
  - (ii) Find the units  $\mathbb{Z}_{(p)}^*$ .
  - (iii) Show that every non-zero element  $x \in \mathbb{Z}_{(p)}$  can be written uniquely as  $up^n$ , where  $u$  is a unit and  $n \geq 0$ .
  - (iv) Let  $I$  be a non-zero ideal of  $\mathbb{Z}_{(p)}$ . Show that  $I = \langle p^n \rangle$  for some  $n \geq 0$ .
  - (v) Show that  $\mathbb{Z}_{(p)}$  contains only one maximal ideal.
40. **(HOF)** Prove that the algorithm given in subsection 3.5.6 works without consulting [25].
41. **(HOF)** Let  $R = \mathbb{Z}[\xi] = \{x + y\xi \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$ , where  $\xi = (1 + \sqrt{-19})/2$ . Prove that  $R$  is a principal ideal domain that is not a Euclidean domain.