Algebra I:
Groups, Rings, & Arithmetic

Serban Raianu
California State University, Dominguez Hills

To my wife Andrea

Introduction

> "Young man, in mathematics you don't understand things. You just get used to them."
>
> John von Neumann

Algebra is the language of modern mathematics, so learning it can be frustrating and rewarding, just like learning a foreign language. If you have never tried to learn a foreign language as an adult imagine this: you are in a foreign country and you decided to learn the language. You bought a book with a CD and a TV. You already read the book and listened to the CD several times. You are watching the weatherman on TV, and you are sure he is saying some numbers, because the screen is full of them. Even though you can say and spell all numbers, you are not able to identify even a single one in what he is saying. Then you are watching the news and you see the prime minister on the screen. You know his name and you are sure the anchor must be saying his name but you could not identify the moment when she says it even if your life depended on it. Shortly put, you think you gave it your best effort but you don't understand anything. You feel like crying, and breaking the screen of your TV with your CD player. But you don't give up, and continue to work hard, read the book, listen to the CD, do the exercises, and watch TV. And one day, as if someone flipped a switch, your hard work pays off, and you are not only able to identify a temperature or a name, but you understand whole phrases. It feels like you are on top of the world.

In exactly the same way, when learning algebra, you will not be able to recognize for a while known terms in new contexts. Be prepared for this and keep trying, one day everything will click into place and its beauty will be revealed.

The other thing that makes studying algebra hard is developing an intuition when dealing with abstract notions, which can be hard. Acquiring it involves a lot of trial and error on concrete examples, which will need to be

kept in our minds as a substitute of the abstract notion until the intuition becomes reliable, and we can reason on the abstract notion itself. Think of trying to study dogs in general (or an abstract dog) when all you know is your own dog. You will probably make an assertion on the abstract dog based on your own dog that will be false (say your dog is a Siberian Husky, and your claim is that all dogs have eyes of different colors). Understanding that the assertion is false means finding an example of another dog for which the assertion is false (this is called a counterexample, say you discover your neighbor has a Standard Poodle with eyes of the same color). From now on, the role of the abstract dog in your mind is played by a list of two dogs: your dog, which is an example for which the assertion is true, and the new dog, the counterexample (note that for the assertion "all dogs have eyes of the same color", your dog is the counterexample and the neighbor's dog is the example; this assertion is also false). You continue working, making assertions, trying to find examples, trying to prove the assertions, trying to find counterexamples when you can't prove the assertions, and so on. The abstract "dogs" that we study in algebra are the sets, groups, rings, fields, and so on. Imagine now that the only ring you know is the ring of integers, $\mathbb{Z}$. When you think of an abstract ring, you think of $\mathbb{Z}$. Based on your knowledge of $\mathbb{Z}$, you claim that in an abstract ring the product of two nonzero elements is nonzero. Then you discover that in the ring $\mathbb{Z}_4$ you have $2 \cdot 2 = 0$. From now on, when you think of an abstract ring you think of $\mathbb{Z}$ or $\mathbb{Z}_4$. Now based on your knowledge of $\mathbb{Z}$ and $\mathbb{Z}_4$ you claim that in a ring multiplication is commutative. Then you discover that in the ring of two by two matrices, $M_2(\mathbb{Z})$, multiplication is not commutative. From now on, when you think of an abstract ring you think of $\mathbb{Z}$, $\mathbb{Z}_4$, or $M_2(\mathbb{Z})$. To see if a new assertion on an abstract ring is true or not, you will first test it on these three rings. The list we are developing is a list of examples and counterexamples. Imagine a successful algebra student as a construction worker with tools conveniently arranged all over the body: the tools are the examples and counterexamples that help build our understanding of the abstract notions.

Our initial examples, the "dogs" that we "own" (i.e. the concrete examples we are supposed to know) are the number sets together with their operations. We assume we know that all the properties of the addition and multiplication of numbers are true, we will not prove them, and we will use them when needed. Understanding how we can construct a number set starting from another is an important part of the study of algebra:
We consider first the natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

An equation of the type $m + x = n$ where $m, n \in \mathbb{N}$ might have a solution

in $\mathbb{N}$, like $1 + x = 2$, or not, like $2 + x = 1$. By adding the solutions of all these equations to $\mathbb{N}$ we obtain the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Trying to make sense of the negative numbers that were added to $\mathbb{N}$ is not hard: we can think of positive and negative temperatures, going left or right on a line, receiving and giving (money), and so on.
Now an equation of the type $mx = n$ where $m, n \in \mathbb{Z}$ might have a solution in $\mathbb{Z}$, like $1 \cdot x = 2$, or not, like $2x = 1$. By adding the solutions of all these equations to $\mathbb{Z}$ we obtain the rationals

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$$

Again, trying to understand what $\frac{1}{2}$ means is not hard, think of a half of a pie. In this course we will learn how to perform a general construction of this type (see the section on Rings of Fractions).
Now an equation of the type $x^2 = m$ where $m \in \mathbb{Q}$ might have solutions in $\mathbb{Q}$, like $x^2 = 1$, or not, like $x^2 = 2$. Adding to $\mathbb{Q}$ all solutions of these equations (and also other numbers) leads to the reals $\mathbb{R}$. Making sense of $\sqrt{2}$ again is not hard: the diagonal of a square with side 1 has length $\sqrt{2}$.
Consider now an equation of the type $x^2 = r$ where $r \in \mathbb{R}$. This equation might have solutions, like $x^2 = 1$, or not, like $x^2 = -1$. Adding to $\mathbb{R}$ the solutions of this last equation, call them i and $-i$, leads to the complex numbers

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

Making sense of i took some time. Trying $i = \sqrt{-1}$ is a risky idea, because this radical does not have the same properties as the one we know. Assuming it does can lead to

$$-1 = i^2 = \sqrt{-1}\sqrt{-1} = \sqrt{(-1)^2} = \sqrt{1} = 1,$$

and warns us that if we do that we have to unlearn the property of radicals saying that $\sqrt{a}\sqrt{b} = \sqrt{ab}$. Failure to understand i is illustrated by the letter i (for "imaginary") used (sometimes with a derogatory connotation) to denote it. Algebra helps describe i precisely: as we will see later in this course, i is "the coset of the indeterminate in the factor ring of the polynomial ring in one indeterminate X with real coefficients factored through the principal ideal generated by the polynomial $X^2 + 1$." Therefore, we will learn in this course that we can construct $\mathbb{C}$ like this:

$$\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1).$$

It may be interesting to note that we can no longer expand $\mathbb{C}$ by adding roots of polynomials with coefficients in $\mathbb{C}$: any polynomial of degree at least one with complex coefficients has a complex root in $\mathbb{C}$ (this is the famous Fundamental Theorem of Algebra and it says that $\mathbb{C}$ is algebraically closed).
There is yet another (fairly easy and convincing) justification for the "existence" of i, or at least of a model of it. We start with the matrix of the rotation of angle α about the origin in the plane:

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

If we replace now $\cos(\alpha)$ and $\sin(\alpha)$ by $a, b \in \mathbb{R}$, we get

$$\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\} = \left\{ a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}. \quad (1)$$

As we can easily check, we have

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (2)$$

so if we define addition and multiplication in the set described in (1) by extending multiplication of real numbers and/or matrices, we see that the elements of this set behave exactly like the complex numbers (note that $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = i$ from the solution to Exercise 1.4.5 xxvi)). According to (2), i may be seen as the rotation of 90° about the origin in the plane, and the equality $i^2 = -1$ can be read as "the rotation of 180° about the origin in the plane can be obtained by applying twice the rotation of 90°".
From a strictly algebraic point of view, the description of $\mathbb{C}$ as a factor ring is more valuable, because it uses a standard procedure for finding roots of polynomials. This course will expose mathematics majors to some other standard constructions and ideas of algebra. One of them is the principle according to which we try to describe various notions and constructions without referring to elements, but using only objects and maps (morphisms) between them. One of the benefits of this approach is that strong similarities between seemingly unrelated notions are revealed in this way, a typical example being the duality between the notions of injective and surjective functions. We will describe this similarity by saying that in the category of sets, a function is in(sur)jective if and only if is a mono(epi)morphism. A second benefit is that we can then easily move from sets (no operations) to groups (one operation) and to rings (two operations). In the course of this transition, we will see that the above characterization of injective functions

is easy to prove in all three cases, while the corresponding assertion for surjective functions goes from easy (for sets) to too-hard-to-be-proved-here (for groups), to not true (for rings). A third benefit (which will not be explored in this course) is that these notions and constructions can be also used for objects that are not built on sets.

Other standard constructions that students will learn in this course are the notions of factor set (factor group, factor ring), ring of fractions, ring of formal power series, and ring of polynomials. All these constructions satisfy certain "universal properties", which can be regarded as "apps" that are used to produce maps (or morphisms). The initial occurrence of a universal property is naturally explained by the attempt to describe a factor set using only sets and functions (and no elements), as mentioned above. The future math teachers will especially benefit from studying all these constructions, for example they will learn, among other things, the distinction between polynomials and polynomial functions, and a proof for the existence of the partial fractions decomposition that is used in calculus.

The book has three chapters with seven sections in each chapter, and so it contains enough material for a first one semester course in algebra. All exercises have detailed solutions at the end of each section (something I first saw in the books of D.G. Northcott, and really appreciated as a student). Needless to say, the students should try really hard to solve the exercises for as long as possible (at least a few days for each of them) before looking at the solution.

Every teacher's teaching style is the result of many interactions with the teacher's teachers, friends, colleagues, and students. Even though I am aware I risk leaving out names of people who heavily influenced my teaching, I will mention just a few of my teachers, T. Albu, P. Alger, I. Colojoară, G. Galbură, I.D. Ion, L. Panaitopol, N. Radu, M. Şabac, my advisor C. Năstăsescu, a few of my friends, A. Buium, M. Beattie, M. Cohen, S. Dăscălescu, D. Fischman, P. Ionescu, G. Jennings, C. Menini, D. Quinn, F. Van Oystaeyen, and my students at the University of Bucharest and California State University, Dominguez Hills.

Contents

Chapter 1

Groups

1.1 Sets and functions

No communication is possible without a common ground consisting of terms that everybody understands. In the absence of these terms it is not even possible to ask questions. One such primary notion, which we assume we all know, is the notion of a set. Sets consist of elements. We write that a is an element of the set A like this: $a \in A$. A set A is a subset of the set B if every element of A is also an element of B, and we write this as $A \subseteq B$. We denote by $\emptyset$ the empty set, the set with no elements. The set whose elements are $a_1, a_2, \ldots a_n$ will be denoted by $\{a_1, a_2, \ldots a_n\}$. The union of the sets A and B consists of the elements that belong to at least one of the sets:

$$A \cup B = \{a \mid a \in A \text{ or } a \in B\}.$$

The intersection of the sets A and B consists of the elements that belong to both sets:

$$A \cap B = \{a \mid a \in A \text{ and } a \in B\}.$$

Basic examples of sets include sets of numbers: the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$, the integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$, the rationals $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.

Assuming we all know something that we do not completely understand is risky. To see that this naive approach may lead to paradoxes consider the set of all sets and denote it by $\mathcal{S}$. Then let $M = \{X \in \mathcal{S} \mid X \notin X\}$, and we see that $M \in M$ if and only if M itself satisfies the condition in the definition of M, which is $M \notin M$. Paradoxes like this one have prompted various attempts to introduce sets by a list of axioms.

Once we know what a set is we can define ordered pairs of elements: (x, y) will mean the set $\{\{x, y\}, \{x\}\}$, i.e. x and y are the elements, order matters and x is the first element. Note that $\{1, 2\} = \{2, 1\}$ because the two sets have the same elements, but $(1, 2) \neq (2, 1)$ because the sets $\{\{1, 2\}, \{1\}\}$ and $\{\{1, 2\}, \{2\}\}$ do not have the same elements. The cartesian product of the sets A and B is defined by

$$A \times B = \{(a, b) \mid a \in A, \ \ b \in B\}$$

We can now give the definition of a function (or map):

Definition 1.1.1 *A function f defined on A with values in B (we write $f : A \longrightarrow B$ and we say that f is defined on A with values in B) consists of three sets: A, the domain; B, the codomain; and a subset G_f of $A \times B$, the graph, satisfying the property that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in G_f$. If $(a, b) \in G_f$ we write $b = f(a)$ and call it the image of a through f.*

Two functions are equal if all three pairs of sets in the definition are equal: the functions have the same domain, the same codomain, and the images of every element in the common domain through the two functions are also equal. If $f : A \longrightarrow B$ and $g : B \longrightarrow C$, then we can define the composition of the functions f and g by $g \circ f : A \longrightarrow C$, $(g \circ f)(a) = g(f(a))$ for all $a \in A$. Sometimes we write gf instead of $g \circ f$.

Exercise 1.1.2 *If $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$, prove that $(h \circ g) \circ f = h \circ (g \circ f)$. (We say that the composition of functions is associative.)*

If $f : A \longrightarrow B$ is a function, $C \subseteq A$ and $D \subseteq B$, we define the image of C through f as

$$f(C) = \{f(a) \mid a \in C\},$$

and the inverse image (or preimage) of D through f as

$$f^{-1}(D) = \{a \mid a \in A, \ \ f(a) \in D\}.$$

We call $f(A)$ the image of the function f and we denote it by $Im(f)$. Note that some authors use the range of f as a synonym for the image of f [14], while others use range instead of codomain [20].

Given any set A, the identity function of the set A, denoted Id_A or 1_A, is the function defined on A with values in A that sends each element $a \in A$ to itself: $Id_A : A \longrightarrow A$, $Id_A(a) = a$ for all $a \in A$. We now define some special classes of functions.

Definition 1.1.3 *We say that the function $f : A \longrightarrow B$ is injective (or one-to-one) if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$, or, equivalently, if $a_1 \neq a_2$ implies that $f(a_1) \neq f(a_2)$.*

Definition 1.1.4 *We say that the function $f : A \longrightarrow B$ is surjective (or onto) if for any element $b \in B$ there exists $a \in A$ such that $b = f(a)$, or, equivalently, if $Im(f) = B$.*

Definition 1.1.5 *A function that is both injective and surjective is called bijective.*

Exercise 1.1.6 *Give examples of functions that are:*
i) neither injective nor surjective
ii) injective but not surjective
iii) surjective but not injective
iv) bijective.

Exercise 1.1.7 *Let $f : A \longrightarrow B$ and assume that $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_n\}$. If f is injective or surjective, then f is bijective.*

Exercise 1.1.8 *Find a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ which is:*
i) injective but not surjective.
ii) surjective but not injective.

For the rest of this section we will assume that all sets are nonempty. Our next goal is to show that the notions of injective and surjective functions are really similar, which is something that we cannot see by comparing Definitions 1.1.3 and 1.1.4. A first step in this direction is the following:

Proposition 1.1.9 *Let $f : A \longrightarrow B$ be a function. Then the following assertions hold:*
i) f is injective if and only if there exists a function $g : B \longrightarrow A$ such that $g \circ f = Id_A$, i.e. f has a left inverse.
ii) f is surjective if and only if there exists a function $g : B \longrightarrow A$ such that $f \circ g = Id_B$, i.e. f has a right inverse.

Proof: i) Assume f is injective, and fix an element $a_0 \in A$. We define g as follows: if $b \in B$ is not in $Im(f)$, set $g(b) = a_0$. If $b \in Im(f)$, since f is injective there exists a unique $a \in A$ such that $b = f(a)$. In this case let $g(b) = a$. Then for each $a \in A$ we have that $g(f(a)) = a$, so $g \circ f = Id_A$. Conversely, if a function $g : B \longrightarrow A$ such that $g \circ f = Id_A$ exists, let $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$, and so $a_1 = a_2$.
ii) Assume f is surjective, and let $b \in B$. Then we choose an element $a \in A$ such that $f(a) = b$ (which exists because f is surjective) and we

let $g(b) = a$. Then $f(g(b)) = f(a) = b$, so $f \circ g = Id_B$. Conversely, if a function $g : B \longrightarrow A$ such that $f \circ g = Id_B$ exists, then for any $b \in B$ we have that $b = f(g(b))$, so $b \in Im(f)$ and thus f is surjective. ∎

Proposition 1.1.9 shows that injectivity and surjectivity are closely related, we can get one from the other by replacing "left" with "right" or the other way around. It also provides the following useful characterization of bijective functions:

Corollary 1.1.10 *A function $f : A \longrightarrow B$ is bijective if and only if it is invertible, i.e. there exists a function $g : B \longrightarrow A$ such that $f \circ g = Id_B$ and $g \circ f = Id_A$.*

Proof: If f is bijective, then by Proposition 1.1.9 it has a left inverse g_1 and a right inverse g_2. Then for any $b \in B$ we have that $g_1(b) = g_1(Id_B(b)) = g_1(f \circ g_2(b)) = (g_1 \circ f)(g_2(b)) = Id_A(g_2(b)) = g_2(b)$, so $g_1 = g_2$, and f is invertible. The converse follows immediately from Proposition 1.1.9. ∎

As seen in the proof above, a function cannot have more than one inverse: if the inverse exists it must be unique, and our notation for it will be f^{-1}. Note that this notation makes sense even if f is not invertible (the preimage of a subset above), but in case the function is invertible, the preimage of a subset is the image of that set through the inverse function, which justifies the notation.

Exercise 1.1.11 *Prove that the inverse of a bijective function is also bijective.*

Exercise 1.1.12 *Find a left inverse, a right inverse, or an inverse for each of the examples you gave in Exercises 1.1.6 and 1.1.8, or explain why they do not exist.*

Exercise 1.1.13 *For each of the following functions:*
a) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2$,
b) $g : [0, \infty) \longrightarrow \mathbb{R}$, $g(x) = x^2$,
c) $h : \mathbb{R} \longrightarrow [0, \infty)$, $h(x) = x^2$,
answer the following questions:
i) Does the function have a left inverse? Justify your answer, then find a left inverse if it exists.
ii) Does the function have a right inverse? Justify your answer, then find a right inverse if it exists.

We now investigate further how injectivity and surjectivity are related. It turns out that the two definitions can be stated only in terms of sets and

maps (without any reference to elements), and we can obtain one from the other simply by reversing the arrows. We say that they are dual notions. Doing things without reference to elements has the advantage that the same techniques and/or results may be used for objects that are not sets.

Proposition 1.1.14 *Let $f : A \longrightarrow B$ be a function. Then the following assertions hold:*
i) f is injective if and only if given any set X, and functions $g, h : X \longrightarrow A$ such that $f \circ g = f \circ h$, it follows that $g = h$.
ii) f is surjective if and only if given any set X, and functions $g, h : B \longrightarrow X$ such that $g \circ f = h \circ f$, it follows that $g = h$.

Proof: i) Assume that f is injective. Then by Proposition 1.1.9 f has a left inverse, and by composing the equality $f \circ g = f \circ h$ with that left inverse from the left gives $g = h$. Conversely, assume the condition in the statement holds, and let a_1 and a_2 elements of A such that $f(a_1) = f(a_2)$. Take $X = \{a_1, a_2\}$, and define $g, h : X \longrightarrow A$ by $g(a_1) = g(a_2) = a_1$, and $h(a_1) = h(a_2) = a_2$. Then $f \circ g = f \circ h$, and so $g = h$, thus $a_1 = a_2$.
ii) If f is surjective, composing the equality $g \circ f = h \circ f$ from the right with the right inverse that exists by Proposition 1.1.9 we get that $g = h$. Conversely, if the condition holds we assume that f is not surjective and look for a contradiction. Choose $b \in Im(f)$ and $x \in B$ but $x \notin Im(f)$. Then let $X = \{x, b\}$, and define g to be the constant function b. Now let h send all the elements of B to b, with the exception of x which is sent to x. It is clear that $g \neq h$ but $g \circ f = h \circ f =$ the constant function b, which is a contradiction. ∎

Exercise 1.1.15 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are injective functions, then $g \circ f$ is also injective. The assertion is also true if we replace "injective" by "surjective".*

Exercise 1.1.16 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions such that $g \circ f$ is injective, then f is injective.*

Exercise 1.1.17 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions such that $g \circ f$ is surjective, then g is surjective.*

Exercise 1.1.18 *If $f : A \longrightarrow B$ is a function, $C_1, C_2 \subseteq A$, $D_1, D_2 \subseteq B$, then:*
i) $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$.
ii) $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$. Give an example when the inclusion is strict, and prove that if f is injective equality holds.
iii) $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$.
iv) $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$.

Solutions to the Exercises on Section 1.1

Exercise 1.1.2 *If $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$, prove that $(h \circ g) \circ f = h \circ (g \circ f)$. (We say that the composition of functions is associative.)*
Solution: Both $(h \circ g) \circ f$ and $h \circ (g \circ f)$ have domain A and codomain D, so we only need to show that $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$ for all $a \in A$. If $a \in A$, then $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) = h((g \circ f)(a)) = (h \circ (g \circ f))(a)$.

Exercise 1.1.6 *Give examples of functions that are:*
i) neither injective nor surjective
ii) injective but not surjective
iii) surjective but not injective
iv) bijective.
Solution: i) $A = \{1, 2\}$, $f : A \longrightarrow A$, $f(1) = f(2) = 1$.
ii) $A = \{1\}$, $B = \{1, 2\}$, $f : A \longrightarrow B$, $f(1) = 1$.
iii) $A = \{1, 2\}$, $B = \{1\}$, $f : A \longrightarrow B$, $f(1) = f(2) = 1$.
iv) $A = \{1, 2\}$, $Id_A : A \longrightarrow A$.

Exercise 1.1.7 *Let $f : A \longrightarrow B$ and assume that $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_n\}$. If f is injective or surjective, then f is bijective.*
Solution: If f is injective, $Im(f)$ has n elements and is contained in B, which also has n elements, therefore $Im(f) = B$ and f is surjective. If f is surjective but not injective, $Im(f)$ has at most $n - 1$ elements, a contradiction.

Exercise 1.1.8 *Find a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ which is:*
i) injective but not surjective.
ii) surjective but not injective.
Solution: i) If $f(n) = 2n$ for all $n \in \mathbb{N}$, then f is injective but $1 \notin Im(f)$.
ii) Put $f(0) = 0$, and $f(n) = n - 1$ if $n \geq 1$, then f is surjective but $f(0) = f(1)$.

Exercise 1.1.11 *Prove that the inverse of a bijective function is also bijective.*
Solution: The inverse of a bijective function is invertible, and is therefore bijective by Corollary 1.1.10.

Exercise 1.1.12 *Find a left inverse, a right inverse, or an inverse for each of the examples you gave in Exercises 1.1.6 and 1.1.8, or explain why they do not exist.*
Solution: For Exercise 1.1.6:

i) $A = \{1, 2\}$, $f : A \longrightarrow A$, $f(1) = f(2) = 1$. Since f is neither injective nor surjective, f does not have a left or a right inverse.
ii) $A = \{1\}$, $B = \{1, 2\}$, $f : A \longrightarrow B$, $f(1) = 1$. Since f is injective but not surjective, f has a left inverse, but not a (right) inverse. A left inverse for f is $f' : B \longrightarrow A$, $f'(1) = f'(2) = 1$.
iii) $A = \{1, 2\}$, $B = \{1\}$, $f : A \longrightarrow B$, $f(1) = f(2) = 1$. Since f is surjective but not injective, f has a right inverse, but not a (left) inverse. A right inverse for f is $f' : B \longrightarrow A$, $f'(1) = 1$.
iv) $A = \{1, 2\}$, $Id_A : A \longrightarrow A$. Id_A is bijective and is its own inverse.
For Exercise 1.1.8:
i) If $f(n) = 2n$ for all $n \in \mathbb{N}$, then f is injective but $1 \notin Im(f)$. A left inverse for f is $f' : \mathbb{N} \longrightarrow \mathbb{N}$,

$$f'(n) = \begin{cases} k & \text{if } n = 2k \\ 0 & \text{if } n = 2k + 1 \end{cases}$$

ii) Put $f(0) = 0$, and $f(n) = n - 1$ if $n \geq 1$, then f is surjective but $f(0) = f(1)$. A right inverse for f is $f' : \mathbb{N} \longrightarrow \mathbb{N}$, $f'(n) = n + 1$.

Exercise 1.1.13 *For each of the following functions:*
a) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2$,
b) $g : [0, \infty) \longrightarrow \mathbb{R}$, $g(x) = x^2$,
c) $h : \mathbb{R} \longrightarrow [0, \infty)$, $h(x) = x^2$,
answer the following questions:
i) Does the function have a left inverse? Justify your answer, then find a left inverse if it exists.
ii) Does the function have a right inverse? Justify your answer, then find a right inverse if it exists.
Solution: a) f is neither injective ($f(1) = f(-1)$) nor surjective ($-1 \notin Im(f)$), so f has no left or right inverse.
b) g is injective, but not surjective, so g will have a left inverse but not a right inverse. A left inverse for g is $g' : \mathbb{R} \longrightarrow [0, \infty)$, $g'(x) = \sqrt{|x|}$.
c) h is surjective, but not injective, so h will have a right inverse but not a left inverse. A right inverse for h is $h' : [0, \infty) \longrightarrow \mathbb{R}$, $h'(x) = \sqrt{x}$.

Exercise 1.1.15 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are injective functions, then $g \circ f$ is also injective. The assertion is also true if we replace "injective" by "surjective".*
Solution: If f and g are injective, let f_1 and g_1 be left inverses of f and g, respectively. Thus $f_1 : B \longrightarrow A$, $g_1 : C \longrightarrow B$, $f_1 \circ f = Id_A$ and $g_1 \circ g = Id_B$. We have that $(f_1 \circ g_1) \circ (g \circ f) = f_1 \circ (g_1 \circ g) \circ f = f_1 \circ Id_B \circ f = f_1 \circ f = Id_A$, so $f_1 \circ g_1$ is a left inverse of $g \circ f$, and thus $g \circ f$ is injective. The proof for the case of surjective functions is similar.

Exercise 1.1.16 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions such that $g \circ f$ is injective, then f is injective.*
Solution: Let $e : C \longrightarrow A$ be a left inverse for $g \circ f$, i.e. $e \circ (g \circ f) = Id_A$. Then $e \circ g$ is a left inverse for f, so f is injective.

Exercise 1.1.17 *If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions such that $g \circ f$ is surjective, then g is surjective.*
Solution: Let $e : C \longrightarrow A$ be a right inverse for $g \circ f$, i.e. $(g \circ f) \circ e = Id_C$. Then $f \circ e$ is a right inverse for g, so g is surjective.

Exercise 1.1.18 *If $f : A \longrightarrow B$ is a function, $C_1, C_2 \subseteq A$, $D_1, D_2 \subseteq B$, then:*
i) $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$.
ii) $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$. Give an example when the inclusion is strict, and prove that if f is injective equality holds.
iii) $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$.
iv) $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$.
Solution: i) Let $b \in f(C_1 \cup C_2)$. Then $b = f(a)$, where $a \in C_1 \cup C_2$, i.e. $a \in C_1$ or $a \in C_2$. Then $b \in f(C_1)$ or $b \in f(C_2)$, so $b \in f(C_1) \cup f(C_2)$. Conversely, $f(C_1) \subseteq f(C_1) \cup f(C_2)$ and $f(C_2) \subseteq f(C_1) \cup f(C_2)$, so $f(C_1) \cup f(C_2) \subseteq f(C_1) \cup f(C_2)$.
ii) Let $b \in f(C_1 \cap C_2)$. Then $b = f(a)$, where $a \in C_1 \cap C_2$, i.e. $a \in C_1$ and $a \in C_2$. Then $b \in f(C_1)$ and $b \in f(C_2)$, so $b \in f(C_1) \cap f(C_2)$. Conversely, if $b \in f(C_1) \cap f(C_2)$, then $b = f(a_1)$, where $a_1 \in C_1$, and $b = f(a_2)$, where $a_2 \in C_2$. If f is injective, then we get that $a_1 = a_2$ so $b \in f(C_1) \cap f(C_2)$, and thus $f(C_1) \cap f(C_2) = f(C_1) \cap f(C_2)$. An example when the inclusion is strict is the following: $A = \{1, 2\}$, $B = \{1\}$, $f : A \longrightarrow B$, $f(1) = f(2) = 1$, $C_1 = \{1\}$, $C_2 = \{2\}$. Then $C_1 \cap C_2 = \emptyset$, so $f(C_1 \cap C_2) = \emptyset$, and $f(C_1) \cap f(C_2) = \{1\}$.
iii) We have that $a \in f^{-1}(D_1 \cup D_2)$ if and only if $f(a) \in D_1 \cup D_2$ if and only if $f(a) \in D_1$ or $f(a) \in D_2$ if and only if $a \in f^{-1}(D_1) \cup f^{-1}(D_2)$.
iv) We have that $a \in f^{-1}(D_1 \cap D_2)$ if and only if $f(a) \in D_1 \cap D_2$ if and only if $f(a) \in D_1$ and $f(a) \in D_2$ if and only if $a \in f^{-1}(D_1) \cap f^{-1}(D_2)$.

1.2 The integers

In this section we review the arithmetic properties of the integers. All letters in this section will represent integers. We will use the following

Well-Ordering Principle. Any nonempty set of nonnegative integers has a least element.

The first application of this principle is

Theorem 1.2.1 (The Division Algorithm) *If a and b are integers and $b \neq 0$, then there exist integers q and r such that $a = bq + r$ and $|r| < |b|$.*

Proof: We will find q and r satisfying the conditions, with $r \geq 0$. These q and r are usually called the quotient and remainder of a divided by b.
Consider the set $W = \{a - tb \geq 0 \mid t \in \mathbb{Z}\}$. It is easy to see that W is nonempty, just take $t = -|a|\, b$. By the well-ordering principle, W has a least element $r = a - qb$. We claim that $r < |b|$. Indeed, if $|b| \leq r$, then $r > r - |b| \geq 0$, and $r - |b| = a - qb - |b| = a - (q \pm 1)b \in W$, which contradicts the fact that r is the least element in W.
Finally, we remark that if $r \neq 0$, the pair $q + \frac{|b|}{b}$ and $r - |b|$ also satisfy the conditions. ∎

Theorem 1.2.1 has important practical consequences. For example it says that any integer has one of the forms $2k$ or $2k + 1$.

Definition 1.2.2 *Given integers a and b, we say that a divides b (or a is a factor of b, or b is a multiple of a, or b is divisible by a), and we write $a \mid b$, if there exists an integer c such that $b = ac$.*

Exercise 1.2.3 *Prove the following:*
i) $1 \mid a$ *for all* a.
ii) $a \mid 0$ *for all* a.
iii) If $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
iv) If $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
v) If $a \mid b$ *and* $a \mid c$, *then* $a \mid ub + vc$ *for all* u, v.
vi) If $a \mid 1$, *then* $a = \pm 1$.
vii) If $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$.

Exercise 1.2.4 *Prove that a product of three consecutive integers is divisible by 3.*

Definition 1.2.5 *Given integers a and b, we say that d is a* **greatest common divisor** *of a and b (we write $d = (a, b)$) if the following two conditions are satisfied:*

i) $d \mid a$ *and* $d \mid b$.
ii) if $c \mid a$ *and* $c \mid b$, *then* $c \mid d$.

It follows immediately from the definition that $a \mid b$ if and only if $a = (a, b)$.

Exercise 1.2.6 *If* $d_1 = (a, b)$ *and* $d_2 = (a, b)$, *then* $d_1 = \pm d_2$.

A second application of the well-ordering principle is the existence of a greatest common divisor:

Theorem 1.2.7 *Given integers* a *and* b, *a greatest common divisor of* a *and* b *exists.*

Proof: If $a = b = 0$, then $0 = (0, 0)$. If not both of a and b are 0, consider the set $W = \{ma + nb > 0 \mid m, n \in \mathbb{Z}\}$. $W \neq \emptyset$ because $a^2 + b^2 \in W$. By the well-ordering principle W has a least element $d = ua + vb$, and we show that $d = (a, b)$. We prove first that $d \mid a$. Indeed, if d does not divide a we use the division algorithm to find q and r such that $a = dq + r$, where $0 < r < d$. Now since $r = a - dq = a - (ua + vb) = (1 - u)a + (-v)b \in W$, this contradicts the fact that d is the least element in W. The proof of the fact that $d \mid b$ is identical. Finally, if $c \mid a$ and $c \mid b$, then $a = ce$ and $b = cf$. It follows that $d = ua + vb = uce + vcf = c(ue + vf)$, so $c \mid d$ and the proof is complete. ∎

From the proof of Theorem 1.2.7 we immediately obtain the following

Corollary 1.2.8 *Given integers* a *and* b, *if* $d = (a, b)$, *then there exist* u, v *such that* $d = ua + vb$. *(We say that* d *is a linear combination of* a *and* b.*)*

Exercise 1.2.9 *i) Show by giving an example that* u *and* v *in Corollary 1.2.8 are not unique.*
ii) Show by giving an example that $d = ua + vb$ *does not imply* $d = (a, b)$.

Proposition 1.2.10 (The Euclidean Algorithm)
i) If $a = bq + r$, *then* $(a, b) = (b, r)$.
ii) If a, b *are nonzero integers, consider the following chain of divisions:*
$| a | = q_0 \cdot |b| + r_0$, *where* $0 \leq r_0 < |b|$,
$|b| = q_1 \cdot r_0 + r_1$, *where* $0 \leq r_1 < r_0$,
$r_0 = q_2 \cdot r_1 + r_2$, *where* $0 \leq r_2 < r_1$,
...
$r_n = q_{n+2} \cdot r_{n+1} + r_{n+2}$, *where* $0 \leq r_{n+2} < r_{n+1}$,
...
Then $\{r_n\}$ *is a strictly decreasing chain of nonnegative integers, so one of them has to be 0. The last nonzero remainder in this chain is a greatest common divisor for* a *and* b.

Proof: i) Let $d = (a, b)$. We show that $d = (b, r)$. We clearly have that $d \mid b$, and since $d \mid a$, we also get that $d \mid a - qb = r$, so d is a common divisor of b and r. Now if $c \mid b$ and $c \mid r$, we have that $c \mid bq + r = a$, so $c \mid d$.
Conversely, if $d = (b, r)$, we show that $d = (a, b)$. We clearly have that $d \mid b$, and since $d \mid r$, we also get that $d \mid bq + r = a$, so d is a common divisor of a and b. Now if $c \mid a$ and $c \mid b$, then $c \mid a - bq = r$, so $c \mid d$.
ii) Assume that r_n is the last nonzero term of the sequence of remainders, so $r_{n+1} = 0$. Applying i) repeatedly we get that $(\mid a \mid, \mid b \mid) = (\mid b \mid, r_0) = (r_0, r_1) = \ldots = (r_n, r_{n+1}) = (r_n, 0) = r_n$, so $r_n = (a, b)$. ∎

Remark 1.2.11 *If we find $d = (a, b)$ using the Euclidean algorithm, we can use back substitution to write d as a linear combination of a and b.*

Exercise 1.2.12 *Use the Euclidean algorithm to find $(987, -345)$, then write it as a linear combination of 987 and -345.*

Definition 1.2.13 *We say that a and b are* **relatively prime** *if $1 = (a, b)$.*

Exercise 1.2.14 *i) Show that a and b are relatively prime if and only if $1 = ma + nb$ for some m and n.*
ii) If $0 \neq d = (a, b)$, $a = da_1$, $b = db_1$, show that $1 = (a_1, b_1)$.

Theorem 1.2.15 (Euclid's Lemma) *If $1 = (a, b)$, and $a \mid bc$, then $a \mid c$.*

Proof: Write $1 = ma+nb$, and $bc = ae$. Then $c = mac+nbc = mac+nae = a(mc + ne)$. ∎

Exercise 1.2.16 *If $1 = (a, b)$ and $1 = (a, c)$, then $1 = (a, bc)$.*

Exercise 1.2.17 *Show that if $a \mid c$, $b \mid c$, and $1 = (a, b)$, then $ab \mid c$. What happens if $1 \neq (a, b)$?*

Exercise 1.2.18 *Show that 6 divides $n^3 - n$.*

Definition 1.2.19 *An integer $p \neq 0$, $p \neq \pm 1$, is said to be* **prime** *if from $p \mid ab$ it follows that $p \mid a$ or $p \mid b$.*

Exercise 1.2.20 *Let $p \neq 0$, $p \neq \pm 1$. The following assertions are equivalent:*
i) p is prime.
ii) If $p = ab$, then one of a and b has the same absolute value as p.
iii) $d \mid p$ implies that $d = \pm 1$ or $d = \pm p$.

Exercise 1.2.21 *If p is prime, and $p \mid a_1 a_2 \ldots a_n$, then there exists i, $1 \leq i \leq n$ such that $p \mid a_i$.*

Exercise 1.2.22 *Show that any odd prime p is of the form $4n+1$ or $4n+3$ for some n.*

The following important result is another application of the well-ordering principle.

Theorem 1.2.23 (Fundamental Theorem of Arithmetic) *Any positive integer n, $n \neq 0$, can be factored as a product of primes.(This means that if $n \neq 1$, then $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where p_i is prime, $1 \leq i \leq k$.) Moreover, the factorization is unique if we disregard the order of the prime factors or their signs. (This means that if there exists another factorization $n = q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$, where q_j is prime, $1 \leq j \leq l$, then $k = l$ and for any i, $1 \leq i \leq k$ there exists a j, $1 \leq j \leq k$ such that $a_i = b_j$ and $p_i = \pm q_j$.)*

Proof: By fiat, 1 is the product of an empty set of primes.
Let $W = \{n \mid n > 1, n \text{ cannot be factored as in the statement}\}$. By the well-ordering principle, if W is nonempty, then W has a least element m. Since $m \in W$ we have that m is not prime, so we can write $m = ab$, where $1 < a, b < m$. Since m is the least element of W it follows that none of a and b are elements of W, so both of them have a factorization as in the statement. But replacing those factorizations in $m = ab$ we see that m has one such factorization, a contradiction. Now for the uniqueness part, assume that

$$p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$$

are two factorizations as products of primes, and we proceed by induction on the length of the factorization, which is the maximum of k and l. The case when the length is 1 is clear. Assume that the length is greater than 1 and the assertion is true for smaller lengths. Then $p_1 \mid q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$, and so p_1 divides one of the q_j. It follows that $p_1 = \pm q_j$, and after canceling p_1 we can apply the induction hypothesis. ∎

Exercise 1.2.24 *Why do we ask $p \neq 0$, $p \neq \pm 1$ in Definition 1.2.19?*

The following old result and its proof go back to Euclid.

Theorem 1.2.25 *There are infinitely many prime numbers.*

Proof: We assume that $p_1, p_2, \dots, p_n$ are all the prime numbers, and look for a contradiction. We let $n = 1 + p_1 p_2 \dots p_n$. Then $|p_1 p_2 \dots p_n| > 1$, so $n \neq 0$, $n \neq \pm 1$. By Theorem 1.2.23 there exists i, $1 \leq i \leq n$ such that $p_i \mid n$. Then $p_i \mid n - p_1 p_2 \dots p_n = 1$, a contradiction. ∎

Exercise 1.2.26 *Show that if p is prime, then $\sqrt{p}$ is irrational by proving that there are no integers a and b such that $a^2 = pb^2$.*

Exercise 1.2.27 *(P. Ionescu) Prove that it is not possible to draw an equilateral triangle on graph paper such that all vertices are at nodes of the grid.*

Solutions to the Exercises on Section 1.2

Exercise 1.2.3 *Prove the following:*
i) $1 \mid a$ *for all* a.
ii) $a \mid 0$ *for all* a.
iii) If $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
iv) If $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
v) If $a \mid b$ *and* $a \mid c$, *then* $a \mid ub + vc$ *for all* u, v.
vi) If $a \mid 1$, *then* $a = \pm 1$.
vii) If $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$.
Solution: i) $a = 1 \cdot a$.
ii) $0 = a \cdot 0$.
iii) We have that $b = ad$ and $c = be = ade$.
iv) We have that $b = ae$ and $d = cf$, so $bd = acef$.
v) We have $b = ad$ and $c = ae$, so $ub + vc = uad + vae = a(ud + ve)$.
vi) We have $1 = ab$, so $|a| = 1$.
vii) If both a and b are 0, the statement is clear. If one of them is not 0, the other one has to be different from 0 as well. In that case we have $b = au$ and $a = bv = auv$, so $1 = uv$.

Exercise 1.2.4 *Prove that a product of three consecutive integers is divisible by 3.*
Solution: A product of three consecutive integers has the form $n(n+1)(n+2)$. By Theorem 1.2.1 we have that $n = 3q$ or $n = 3q + 1$ or $n = 3q + 2$. If $n = 3q$, then $n(n+1)(n+2) = 3q(3q+1)(3q+2)$. If $n = 3q + 1$, then $n(n+1)(n+2) = (3q+1)(3q+2)(3q+3) = 3(3q+1)(3q+2)(q+1)$. If $n = 3q+2$, then $n(n+1)(n+2) = (3q+2)(3q+3)(3q+4) = 3(3q+2)(q+1)(3q+4)$.

Exercise 1.2.6 *If* $d_1 = (a, b)$ *and* $d_2 = (a, b)$, *then* $d_1 = \pm d_2$.
Solution: Since $d_1 = (a, b)$, $d_2 \mid a$, and $d_2 \mid b$, it follows that $d_2 \mid d_1$. Similarly, $d_1 \mid d_2$.

Exercise 1.2.9 *i) Show by giving an example that* u *and* v *in Corollary 1.2.8 are not unique.*
ii) Show by giving an example that $d = ua + vb$ *does not imply* $d = (a, b)$.
Solution: i) We have $1 = (2, 3)$, and $1 = 2 \cdot (-1) + 3 \cdot 1 = 2 \cdot 2 + 3 \cdot (-1)$.
ii) $2 = 1 \cdot 1 + 1 \cdot 1$.

Exercise 1.2.12 *Use the Euclidean algorithm to find* $(987, -345)$, *then write it as a linear combination of* 987 *and* -345.
Solution: Since $(987, -345) = (987, 345)$ we have:
$987 = 2 \cdot 345 + 297$, $0 \leq 297 < 345$
$345 = 1 \cdot 297 + 48$, $0 \leq 48 < 297$

$297 = 6 \cdot 48 + 9$, $0 \leq 9 < 48$
$48 = 5 \cdot 9 + 3$, $0 \leq 3 < 9$
$9 = 3 \cdot 3 + 0$. Then $3 = (987, 345)$, and $3 = 48 - 5 \cdot 9 = 48 - 5 \cdot (297 - 6 \cdot 48) = 31 \cdot 48 - 5 \cdot 297 = 31 \cdot (345 - 1 \cdot 297) - 5 \cdot 297 = 31 \cdot 345 - 36 \cdot 297 = 31 \cdot 345 - 36 \cdot (987 - 2 \cdot 345) = 103 \cdot 345 - 36 \cdot 987 = (-103) \cdot (-345) - 36 \cdot 987$.

Exercise 1.2.14 *i) Show that a and b are relatively prime if and only if $1 = ma + nb$ for some m and n.*
ii) If $0 \neq d = (a, b)$, $a = da_1$, $b = db_1$, show that $1 = (a_1, b_1)$.
Solution: i) If $1 = (a, b)$, then 1 is a linear combination of a and b by Corollary 1.2.8. Conversely, if $1 = ma + nb$, $d \mid a$ and $d \mid b$, it follows that $d \mid 1$.
ii) Write $d = au + bv = da_1u + db_1v$, divide by d, then apply i).

Exercise 1.2.16 *If $1 = (a, b)$ and $1 = (a, c)$, then $1 = (a, bc)$.*
Solution: Write $au + bv = 1$ and $as + ct = 1$. Then $1 = (au + bv)(as + ct) = a^2us + auct + bvas + bvct = a(aus + uct + bvs) + (bc)(vt)$.

Exercise 1.2.17 *Show that if $a \mid c$, $b \mid c$, and $1 = (a, b)$, then $ab \mid c$. What happens if $1 \neq (a, b)$?*
Solution: Let $c = ad$, $c = bf$, and $1 = au + bv$. Then $c = auc + bvc = aubf + bvad = (ab)(uf + vd)$. If $1 \neq (a, b)$ the assertion is false: $4 \mid 12$ and $6 \mid 12$, but 24 does not divide 12.

Exercise 1.2.18 *Show that 6 divides $n^3 - n$.*
Solution: We have that $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1) = (n - 1)n(n + 1)$, a product of three consecutive numbers, so by Exercise 1.2.4 $3 \mid n^3 - n$. Since similarly 2 divides a product of two consecutive numbers, we also have $2 \mid n^3 - n$. Since $1 = (2, 3)$, it follows from Exercise 1.2.17 that $6 \mid n^3 - n$.

Exercise 1.2.20 *Let $p \neq 0$, $p \neq \pm 1$. The following assertions are equivalent:*
i) p is prime.
ii) If $p = ab$, then one of a and b has the same absolute value as p.
iii) $d \mid p$ implies that $d = \pm 1$ or $d = \pm p$.
Solution: *i)* $\Rightarrow$ *ii)*. Since $p = ab$, it follows that $a \mid p$ and $b \mid p$, and also that $p \mid ab$. Since p is prime, it follows that $p \mid a$ or $p \mid b$. Therefore $a = \pm p$ or $b = \pm p$ by Exercise 1.2.3, *vii)*.
ii) $\Rightarrow$ *iii)*. Let $p = de$. It follows that $|d| = |p|$, in which case $d = \pm p$, or $|e| = |p|$, in which case $d = \pm 1$.
iii) $\Rightarrow$ *i)*. Let $p \mid ab$, and consider $d = (a, p)$. From the hypothesis it follows that either $d = \pm 1$, in which case $p \mid b$ by Euclid's lemma, or $d = \pm a$, which

means that $p \mid a$.

Exercise 1.2.21 *If p is prime, and $p \mid a_1 a_2 \dots a_n$, then there exists i, $1 \leq i \leq n$ such that $p \mid a_i$.*
Solution: We use induction on n. If $n = 1$ there is nothing to prove. If $n > 1$ and the assertion is true for numbers $< n$, we have $p \mid a_1 \cdot (a_2 \dots a_n)$, so either $p \mid a_1$ or $p \mid a_2 \dots a_n$ and we can apply the induction hypothesis.

Exercise 1.2.22 *Show that any odd prime p is of the form $4n+1$ or $4n+3$ for some n.*
Solution: By the division algorithm we have that $p = 4n$ or $p = 4n+1$ or $p = 4n+2 = 2(2n+1)$ or $p = 4n+3$. The first and third cases contradict either the fact that p is prime, or that p is odd, so the conclusion follows.

Exercise 1.2.24 *Why do we ask $p \neq 0$, $p \neq \pm 1$ in Definition 1.2.19?*
Solution: While it is true that 0 satisfies the definition of prime numbers, and ± 1 satisfy the equivalent conditions in Exercise 1.2.20, accepting any of these three numbers as prime would hurt the uniqueness of the decomposition as a product of prime numbers in the fundamental theorem of arithmetic (Theorem 1.2.23).

Exercise 1.2.26 *Show that if p is prime, then $\sqrt{p}$ is irrational by proving that there are no integers a and b such that $a^2 = pb^2$.*
Solution: Assume that such a and b exist, and look at the powers of p on both sides of the equality $a^2 = pb^2$. The power of p on the left is even, while the power of p on the right is odd, and this contradicts the uniqueness of the decomposition as a product of prime numbers in the fundamental theorem of arithmetic (Theorem 1.2.23).

Exercise 1.2.27 *(P. Ionescu) Prove that it is not possible to draw an equilateral triangle on graph paper such that all vertices are at nodes of the grid.*
Solution: Suppose such an equilateral triangle exists, and draw horizontal and vertical lines through the vertices of the triangle in order to inscribe it in a rectangle whose sides have integer lengths. This rectangle is the union of the equilateral triangle and two or three right triangles. Right triangles whose legs have integer lengths have rational areas (either an integer or half of an integer). Denote by l the side of the equilateral triangle. By the Pythagorean theorem, l^2 is an integer. It follows that the area of the triangle, which is $\frac{l^2\sqrt{3}}{4}$, is rational, so $\sqrt{3}$ is rational, a contradiction.

1.3 Equivalence relations and factor sets

In this section we start introducing one of the most fundamental concepts of modern mathematics: the notion of factor (or quotient) structure. We actually start with no structure at all, since in this section we only consider sets, but we will soon be looking at more and more structures when we consider factor groups or factor rings later on. We start with the following:

Definition 1.3.1 *If M is a set, a subset $\mathcal{R}$ of the cartesian product $M \times M$ is called a* (binary) relation *on M. We will write $x\mathcal{R}y$ if $(x, y) \in \mathcal{R}$, and we say that x is in the relation $\mathcal{R}$ with y.*

Definition 1.3.2 *A relation $\mathcal{E}$ on the set M is called an* equivalence relation *if it satisfies the following three properties for arbitrarily chosen $x, y, z \in M$:*
i) $x\mathcal{E}x$ (reflexivity).
ii) $x\mathcal{E}y \Rightarrow y\mathcal{E}x$ (symmetry).
iii) $x\mathcal{E}y$ and $y\mathcal{E}z \Rightarrow x\mathcal{E}z$ (transitivity).

We give some examples of equivalence relations, but we leave the verifications as an exercise:

Exercise 1.3.3 *Prove that the following relations are equivalence relations:*
i) On the set $\mathbb{Z}$: $a \equiv b \Leftrightarrow a = b$.
ii) On the set $\mathbb{Z}$: fix $n > 0$; then $a \equiv b \ (mod\ n) \Leftrightarrow n \mid a - b$. (This is called congruence modulo n.)
iii) On the set $\mathbb{Z}$: $a \sim_d b \Leftrightarrow a \mid b$ and $b \mid a$. (This is called association in divisibility.)
iv) On the set of points in the plane: fix a point C; then $A\mathcal{R}B \Leftrightarrow A$ and B are at the same distance from C.
v) Let M and N be sets and $f : M \longrightarrow N$ a function. Define the following relation on M: $x\mathcal{R}_f y \Leftrightarrow f(x) = f(y)$.

Definition 1.3.4 *Let $\mathcal{E}$ be an equivalence relation on the set M, and $x \in M$. We define the* equivalence class *of x relative to $\mathcal{E}$, by*

$$\hat{x}_{\mathcal{E}} = \{y \in M \mid x\mathcal{E}y\}.$$

If there is no danger of confusion we will omit the index and write $\hat{x} = \hat{x}_{\mathcal{E}}$. An equivalence class for $\mathcal{E}$ is the equivalence class of some element in M.

Exercise 1.3.5 *Describe the equivalence classes of the equivalence relations in Exercise 1.3.3.*

Exercise 1.3.6 *If $y \in \hat{x}$, then $\hat{x} = \hat{y}$.*

We now recall the definition of a partition of a set.

Definition 1.3.7 *Let M be a set. A family $\{M_i\}_{i\in I}$ of subsets of M is called a* partition *of M if the following conditions are satisfied:*
i) $M_i \neq \emptyset$ for all $i \in I$.
ii) The sets in the family are disjoint, i.e. $M_i \cap M_j = \emptyset$ if $i, j \in I$, $i \neq j$.
iii) The sets cover M, i.e. $M = \cup_{i\in I} M_i$ (This means that any element in M belongs to one of the M_i's).

Proposition 1.3.8 *The equivalence classes of an equivalence relation $\mathcal{E}$ on the set M form a partition of M.*

Proof: We need to check the three conditions in Definition 1.3.7.
i) An equivalence class is $\hat{x}$ for some $x \in M$, so $\hat{x} \neq \emptyset$ because $x \in \hat{x}$ by reflexivity.
ii) Two equivalence classes are either disjoint or they coincide. Indeed, if $\hat{x} \cap \hat{y} \neq \emptyset$, let $z \in \hat{x} \cap \hat{y}$, and then $\hat{x} = \hat{y} = \hat{z}$ by Exercise 1.3.6.
iii) If $x \in M$, then $x \in \hat{x}$ as remarked in i). ∎

Exercise 1.3.9 *Let M be a set, and $\{M_i\}_{i\in I}$ a partition of M. Define the following relation on M: $x\mathcal{R}y \Leftrightarrow$ there exists $i \in I$ such that $x, y \in M_i$. Then $\mathcal{R}$ is an equivalence relation.*

Proposition 1.3.10 *There exists a bijective correspondence between the set of equivalence classes on a set M and the set of partitions on M.*

Proof: We start with and equivalence relation $\mathcal{E}$ on M. We form the partition of M consisting of the equivalence classes of $\mathcal{E}$, then we associate the equivalence relation $\mathcal{R}$ as in Exercise 1.3.9. This means that $x\mathcal{R}y$ if and only if x, y belong to an equivalence class of $\mathcal{E}$, if and only if $x\mathcal{E}y$, so $\mathcal{R} = \mathcal{E}$ and we got back to $\mathcal{E}$.
Conversely, start with a partition $\{M_i\}_{i\in I}$ of M, and consider the equivalence relation $\mathcal{R}$ as in Exercise 1.3.9. Then the equivalence classes of $\mathcal{R}$ are the M_i's, since we can check that if $x \in M_i$, then $M_i = \hat{x}$. ∎

Definition 1.3.11 *If M is a set and $\mathcal{E}$ is an equivalence relation on M, the* factor set *(or* quotient set*) of M through $\mathcal{E}$ is the set of equivalence classes of $\mathcal{E}$ and is denoted by $M/\mathcal{E}$. If we select one element in each equivalence class and denote the set of all these elements by $\mathcal{S}$, then the factor set of M through $\mathcal{E}$ can be described as*

$$M/\mathcal{E} = \{\hat{x} \mid x \in \mathcal{S}\}.$$

$\mathcal{S}$ is called a complete system of representatives *for the equivalence classes of $\mathcal{E}$,*

Exercise 1.3.12 *Describe the factor sets in Exercise 1.3.3 and indicate a complete system of representatives for each one.*

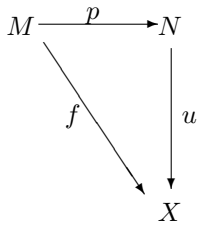
As we did in the case of injective and surjective functions, we will describe the notion of factor set in a way that does not make any reference to elements. We first give a second definition of a factor set, then show that the two definitions are equivalent.

Definition 1.3.13 *If M is a set, a factor set of M is a pair (N, p), where N is a set and $p : M \longrightarrow N$ is a surjective function.*

Example 1.3.14 *A factor set in the sense of Definition 1.3.11 is also a factor set in the sense of Definition 1.3.13, because the function $p : M \longrightarrow M/\mathcal{E}$, defined by $p(x) = \hat{x}$, is surjective (this function is called the canonical surjection).*

The following important result ensures that the two definitions of a factor set are actually the same:

Theorem 1.3.15 (The Universal Property of the Factor Set) *Let (N, p) be a factor set of the set M, let X be a set and $f : M \longrightarrow X$ a function.*
i) There exists a function $u : N \longrightarrow X$ such that $f = up$ (we say that f factors through p), which means that the diagram



is commutative, if and only if $\mathcal{R}_p \subseteq \mathcal{R}_f$ (i.e. $p(x_1) = p(x_2) \Rightarrow f(x_1) = f(x_2)$). If u exists, then it is unique.
If u as in i) exists, then:
ii) u is surjective if and only if f is surjective.
iii) u is injective if and only if $\mathcal{R}_p = \mathcal{R}_f$ (i.e. $p(x_1) = p(x_2) \Leftrightarrow f(x_1) = f(x_2)$).

Proof: i) Assume that a function u like in the statement exists, and let $x_1, x_2 \in M$ such that $p(x_1) = p(x_2)$. Then $f(x_1) = u(p(x_1)) = u(p(x_2) = f(x_2)$. Conversely, assume that $p(x_1) = p(x_2) \Rightarrow f(x_1) = f(x_2)$ and let $y \in N$. Since p is surjective, let $x \in M$ such that $p(x) = y$, and define

$u(y) = f(x)$. We need to show that the definition is correct, i.e. it does not depend on the choice of x. Indeed, if we have another $x_1 \in M$ such that $p(x_1) = y$, then $p(x) = p(x_1) = y$, so $f(x) = f(x_1)$, and the definition of $u(y)$ does not depend on x. Now if two functions u_1 and u_2 with the property that $u_1 p = u_2 p = f$ exist, we let $y \in N$. Again since p is surjective there exists $x \in M$ such that $p(x) = y$, and hence $u_1(y) = u_1(p(x)) = f(x) = u_2(p(x)) = u_2(y)$, so $u_1 = u_2$.
ii) If u is surjective, then $f = up$ is surjective because it is a composition of surjective functions (see Exercise 1.1.15). Conversely, if $f = up$ is surjective, then u is surjective by Exercise 1.1.17.
iii) If u is injective, let $f(x_1) = f(x_2)$. It follows that $u(p(x_1)) = u(p(x_2))$, and so $p(x_1) = p(x_2)$. Conversely, assume that $p(x_1) = p(x_2) \Leftrightarrow f(x_1) = f(x_2)$ and let $y_1, y_2 \in N$ such that $u(y_1) = u(y_2)$. Since p is surjective let $x_1, x_2 \in M$ such that $p(x_1) = y_1$ and $p(x_2) = y_2$. Then we have $f(x_1) = u(p(x_1)) = u(p(x_2)) = f(x_2)$. By the hypothesis we have that $p(x_1) = p(x_2)$, so $y_1 = y_2$ and u is injective. ∎

Corollary 1.3.16 *If (N_1, p_1) and (N_2, p_2) are two factor sets of M such that $\mathcal{R}_{p_1} = \mathcal{R}_{p_2}$, then there exists a bijective function $u : N_1 \longrightarrow N_2$ such that $up_1 = p_2$.*

Proof: Take $(N, p) = (N_1, p_1)$, $X = N_2$ and $f = p_2$ in Theorem 1.3.15, hence we find u as in the statement, which is bijective. We can actually only use i) in Theorem 1.3.15: also take $(N, p) = (N_2, p_2)$, $X = N_1$ and $f = p_1$, and find v, $vp_2 = p_1$. Then $uvp_1 = p_1$, and $vup_2 = p_2$, so $uv = Id_{N_1}$ and $vu = Id_{N_2}$ by uniqueness. ∎

Corollary 1.3.17 *If (N, p) is a factor set of M, then there exists a bijection $u : N \longrightarrow M/\mathcal{R}_p$ such that $u \circ p$ is the canonical surjection sending an element to its equivalence class.*

Proof: Take $(N_1, p_1) = (N, p)$ and $(N_2, p_2) = (M/\mathcal{R}_p, can)$, where $can : M \longrightarrow M/\mathcal{R}_p$, $can(x) = \hat{x}$. Then $can(x_1) = can(x_2)$ if and only if $x_1 \mathcal{R}_p x_2$ if and only if $p(x_1) = p(x_2)$, and we can apply Corollary 1.3.16. ∎

For a set M we will denote by $\mathcal{P}(M)$ the set of all subsets of M. If $M = \{x_1, x_2, \ldots, x_m\}$, then we write $card(M) = m$.

Exercise 1.3.18 *Let $M = \{x_1, x_2, \ldots, x_m\}$ and $N = \{y_1, y_2, \ldots, y_n\}$.*
i) If $A_1, A_2, \ldots, A_k \in \mathcal{P}(M)$, prove by induction on k that

$$card(A_1 \cup A_2 \cup \ldots \cup A_k) = \sum_{i=1}^{k} card(A_i) - \sum_{1 \leq i < j \leq k} card(A_i \cap A_j) +$$

$$+\ldots+(-1)^{k+1}card(\cap_{i=1}^{k}A_i)$$

(This is the inclusion-exclusion principle)
ii) The number of functions from M to N is n^m.
iii) $card(\mathcal{P}(M))=2^m$.
iv) If $m=n$, the number of bijective functions from M to N is $m!$.
v) If $m\leq n$, the number of injective functions from M to N is ${}_nP_m=\frac{n!}{(n-m)!}$.
vi) If $m\geq n$, the number of surjective functions from M to N is:

$$n^m-\binom{n}{1}(n-1)^m+\binom{n}{2}(n-2)^m+\ldots+(-1)^{n-1}\binom{n}{n-1},$$

where $\binom{n}{k}={}_nC_k=\frac{n!}{k!(n-k)!}$.
vii) Let $k\leq m$. The number of equivalence relations on M such that the factor set has k elements is:

$$E_{m,k}=\frac{1}{k!}(k^m-\binom{k}{1}(k-1)^{m-1}+\binom{k}{2}(k-2)^{m-2}+\ldots+(-1)^{k-1}\binom{k}{k-1}),$$

and so the number of equivalence relations on M is $E_{m,1}+E_{m,2}+\ldots+E_{m,m}$.

Exercise 1.3.19 *i) Let A be a set and $B\in\mathcal{P}(A)$. Define the following relation on $\mathcal{P}(A)$: if $X,Y\in\mathcal{P}(A)$, then $X\mathcal{R}Y$ if and only if $X\cap B=Y\cap B$. Show that $\mathcal{R}$ is an equivalence relation and there exists a bijection between the factor set $\mathcal{P}(A)/\mathcal{R}$ and $\mathcal{P}(B)$.*
ii) Let A and B be nonempty sets, and denote by B^A the set of functions from A to B. Choose $a\in A$, and define the following relation on B^A: $f\mathcal{R}g$ if and only if $f(a)=g(a)$. Show that $\mathcal{R}$ is an equivalence relation and there exists a bijection between the factor set $B^A/\mathcal{R}$ and B.
iii) With the same notation as in ii), let $C\in\mathcal{P}(A)$, and define the following relation on B^A: $f\mathcal{R}'g$ if and only if $f(x)=g(x)$ for all $x\in C$. Show that $\mathcal{R}'$ is an equivalence relation and there exists a bijection between the factor set $B^A/\mathcal{R}'$ and B^C.
iv) Show that i) and ii) can be obtained as particular cases of iii).

Exercise 1.3.20 *Show that the relation defined on $\mathbb{R}$ by $x\mathcal{R}y$ if and only if $x-y\in\mathbb{Z}$ is an equivalence relation, and there is a bijection between the factor set and a circle.*

Solutions to the Exercises on Section 1.3

Exercise 1.3.3 *Prove that the following relations are equivalence relations:*
i) On the set $\mathbb{Z}$*:* $a \equiv b \Leftrightarrow a = b$.
ii) On the set $\mathbb{Z}$*: fix* $n > 0$*; then* $a \equiv b \ (mod\ n) \Leftrightarrow n \mid a - b$*. (This is called congruence modulo* n*.)*
iii) On the set $\mathbb{Z}$*:* $a \sim_d b \Leftrightarrow a \mid b$ *and* $b \mid a$*. (This is called association in divisibility.)*
iv) On the set of points in the plane: fix a point C*; then* $A\mathcal{R}B \Leftrightarrow A$ *and* B *are at the same distance from* C*.*
v) Let M *and* N *be sets and* $f : M \longrightarrow N$ *a function. Define the following relation on* M*:* $x\mathcal{R}_f y \Leftrightarrow f(x) = f(y)$.
Solution: i) If $a \in \mathbb{Z}$, then $a = a$; if $a = b$, then $b = a$; if $a = b$ and $b = c$, then $a = c$.
ii) If $a \in \mathbb{Z}$, then $n \mid a - a = 0$; if $n \mid a - b$, then $n \mid b - a$; if $n \mid a - b$ and $n \mid b - c$, then $n \mid a - b + b - c = a - c$. (Note that i) is a particular case of ii)), we get it for $n = 0$. Also note that $a \equiv b \ (mod\ n)) \Leftrightarrow a$ and b have the same remainder when divided by n.)
iii) If $a \in \mathbb{Z}$, then $a \sim_d a$, because $a \mid a$; symmetry is clear; transitivity follows from the transitivity of divisibility, applied twice.
iv) Similar to i), because $A\mathcal{R}B \Leftrightarrow |AC| = |BC|$.
v) Similar to i) or iv).

Exercise 1.3.5 *Describe the equivalence classes of the equivalence relations in Exercise 1.3.3.*
Solution: i) If $a \in \mathbb{Z}$, then $\hat{a} = \{a\}$.
ii) If $a \in \mathbb{Z}$, then $\hat{a} = \{a + kn \mid k \in \mathbb{Z}\}$.
iii) If $a \in \mathbb{Z}$, then $\hat{a} = \{a, -a\}$.
iv) $\hat{A}$=circle with center C and radius $|AC|$.
v) If $x \in M$, then $\hat{x} = f^{-1}(f(x)) = f^{-1}(\{f(x)\})$.

Exercise 1.3.6 *If* $y \in \hat{x}$*, then* $\hat{x} = \hat{y}$.
Solution: If $y \in \hat{x}$, then $\hat{y} \subseteq \hat{x}$, by symmetry and transitivity. Also, $x \in \hat{y}$ by symmetry, so $\hat{x} = \hat{y}$.

Exercise 1.3.9 *Let* M *be a set, and* $\{M_i\}_{i \in I}$ *a partition of* M*. Define the following relation on* M*:* $x\mathcal{R}y \Leftrightarrow$ *there exists* $i \in I$ *such that* $x, y \in M_i$*. Then* $\mathcal{R}$ *is an equivalence relation.*
Solution: The reflexive property follows from the fact that any $x \in M$ belongs to one of the M_i's. Symmetry is clear, because the order of x and y in "$x, y \in M_i$" is not important. Now, if $x, y \in M_i$ and $y, z \in M_j$, then $y \in M_i \cap M_j$, so $i = j$.

Exercise 1.3.12 *Describe the factor sets in Exercise 1.3.3 and indicate a complete system of representatives for each one.*
Solution: i) The integers form a complete system of representatives, so the factor set is in a bijective correspondence with $\mathbb{Z}$.
ii) A complete system of representatives is the set of all positive remainders: $\{0, 1, \ldots, n-1\}$, so the factor set can be described as $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$ (We call $\mathbb{Z}_n$ "$\mathbb{Z}$ mod n", and if the context is clear, we can omit the hats). Indeed, for any $a \in \mathbb{Z}$ there exist q and r such that $a = nq + r$, $0 \leq r \leq n-1$ so $a \in \hat{r}$. Now, if $a \in \hat{i} \cap \hat{j}$, where $0 \leq i < j \leq n-1$, it follows that $n \mid j - i$, and since $0 \leq j - i \leq n-1$ it follows that $j - i = 0$, or $i = j$.
iii) The factor set is $\{\hat{n} \mid n \in \mathbb{Z}, \hat{n} = \{-n, n\}\}$. A complete system of representatives is $\mathbb{N}$.
iv) The factor set is the set of all circles centered at C. A complete system of representatives is a ray (half line) starting at C.
v) The factor set is the set of all fibers of f (i.e. preimages of images of elements of M). A complete set of representatives is selected by choosing one element x in each fiber $f^{-1}(y)$, where $y \in Im(f) = f(M)$. Therefore, any complete system of representatives is in a bijective correspondence with $Im(f) = f(M)$.

Exercise 1.3.18 *Let $M = \{x_1, x_2, \ldots, x_m\}$ and $N = \{y_1, y_2, \ldots, y_n\}$.*
i) If $A_1, A_2, \ldots, A_k \in \mathcal{P}(M)$, prove by induction on k that

$$card(A_1 \cup A_2 \cup \ldots \cup A_k) = \sum_{i=1}^{k} card(A_i) - \sum_{1 \leq i < j \leq k} card(A_i \cap A_j) +$$

$$+ \ldots + (-1)^{k+1} card(\cap_{i=1}^{k} A_i)$$

(This is the inclusion-exclusion principle)
ii) The number of functions from M to N is n^m.
iii) $card(\mathcal{P}(M)) = 2^m$.
iv) If $m = n$, the number of bijective functions from M to N is $m!$.
v) If $m \leq n$, the number of injective functions from M to N is ${}_nP_m = \frac{n!}{(n-m)!}$.
vi) If $m \geq n$, the number of surjective functions from M to N is:

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m + \ldots + (-1)^{n-1}\binom{n}{n-1},$$

where $\binom{n}{k} = {}_nC_k = \frac{n!}{k!(n-k)!}$.
vii) Let $k \leq m$. The number of equivalence relations on M such that the

factor set has k elements is:

$$E_{m,k} = \frac{1}{k!}(k^m - \binom{k}{1}(k-1)^{m-1} + \binom{k}{2}(k-2)^{m-2} + \ldots + (-1)^{k-1}\binom{k}{k-1}),$$

and so the number of equivalence relations on M is $E_{m,1}+E_{m,2}+\ldots+E_{m,m}$.
Solution: i) For $k = 2$ the assertion is clear, just note that when you add the number of elements of A_1 and A_2, the elements in the intersection are counted twice. Assume now that $k > 2$ and the assertion is true for $k-1$ sets. Then we have

$$(A_1 \cup A_2 \cup \ldots \cup A_{k-1}) \cap A_k = \cup_{i<k}(A_i \cap A_k),$$

so applying the case $k = 2$ we get

$$card(A_1 \cup A_2 \cup \ldots \cup A_k) = card(A_1 \cup A_2 \cup \ldots \cup A_{k-1}) + card(A_k) -$$

$$-card(\cup_{i<k}(A_i \cap A_k)),$$

and we can apply the induction hypothesis and regroup the terms to get the assertion for k.
ii) We use induction on m. If $m = 1$, then M has one element, and it is clear that there are exactly n functions form M to N. If we assume that there are n^{m-1} functions from $\{x_1, \ldots, x_{m-1}\}$ to N, then each function from M to N can be obtained by extending one of those functions by defining it on x_m. Since this can be done in n ways, it follows that there are $n^{m-1} \cdot n = n^m$ functions from M to N.
iii) The function $\phi : \mathcal{P}(M) \longrightarrow \{0,1\}^M$, defined by

$$\phi(X)(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{if } x \notin X \end{cases}$$

which is called the characteristic function of the subset X, is a bijection, with inverse $\psi : \{0,1\}^M \longrightarrow \mathcal{P}(M)$, defined by $\psi(f) = f^{-1}(1)$. Then the assertion follows from ii).
iv) To define a bijection from M to N, we can give it any value at x_1, then x_2 can be sent to any of the remaining $m-1$ values, and so on, until the value at x_m will be the only element of Y left available. So there are $m \cdot (m-1) \cdot \ldots \cdot 1 = m!$ bijective functions from M to N.
v) There is a bijection between the set in injective functions from M to N and the set of ordered subsets with m elements of N. Since there are $\binom{n}{m} = {}_nC_m = \dfrac{n!}{m!(n-m)!}$ subsets of N with m elements, and each set can be ordered in $m!$ ways by iv), the number of injective functions from M to N is $m! \cdot {}_nC_m = {}_nP_m$.

vi) Let us denote by A_i the set of functions from M to N which do not take the value y_i. The set of functions that are not surjective is $A_1 \cup A_2 \cup \ldots \cup A_n$, so the number of surjective functions is $n^m - card(A_1 \cup A_2 \cup \ldots \cup A_n)$. But A_i is the set of functions from M to the set $N \setminus \{y_i\} = \{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n\}$, so $card(A_i) = (n-1)^m$, and therefore $\sum_{i=1}^n card(A_i) = n(n-1)^m$. Similarly, $A_i \cap A_j$ is the set of functions from M to $N \setminus \{y_i, y_j\}$, and so $card(A_i \cap A_j) = (n-2)^m$, and so $\sum_{i<j} card(A_i \cap A_j) = \binom{n}{2}(n-2)^m$, and so on. Note that $A_1 \cap A_2 \cap \ldots \cap A_n = \emptyset$.
vi) By Proposition 1.3.10 we need to count the partitions of M into k subsets. Each partition defines a surjection from M to the set $\{1, 2, \ldots, k\}$, defined by ordering the sets in the partition and sending each element of M to the index of the set in the partition that contains it. Since ordering the sets in the partition can be done in $k!$ different ways, it follows that the number of partitions of M into k subsets is the number of surjective functions from M to $\{1, 2, \ldots, k\}$ divided by $k!$.

Exercise 1.3.19 *i) Let A be a set and $B \in \mathcal{P}(A)$. Define the following relation on $\mathcal{P}(A)$: if $X, Y \in \mathcal{P}(A)$, then $X \mathcal{R} Y$ if and only if $X \cap B = Y \cap B$. Show that $\mathcal{R}$ is an equivalence relation and there exists a bijection between the factor set $\mathcal{P}(A)/\mathcal{R}$ and $\mathcal{P}(B)$.*
ii) Let A and B be nonempty sets, and denote by B^A the set of functions from A to B. Choose $a \in A$, and define the following relation on B^A: $f \mathcal{R} g$ if and only if $f(a) = g(a)$. Show that $\mathcal{R}$ is an equivalence relation and there exists a bijection between the factor set $B^A/\mathcal{R}$ and B.
iii) With the same notation as in ii), let $C \in \mathcal{P}(A)$, and define the following relation on B^A: $f \mathcal{R}' g$ if and only if $f(x) = g(x)$ for all $x \in C$. Show that $\mathcal{R}'$ is an equivalence relation and there exists a bijection between the factor set $B^A/\mathcal{R}'$ and B^C.
iv) Show that i) and ii) can be obtained as particular cases of iii).
Solution: i) Let $f : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$, $f(X) = X \cap B$. Then f is surjective, $\mathcal{R} = \mathcal{R}_f$ is an equivalence relation by Exercise 1.3.3, v), and we can use Corollary 1.3.16 for $M = \mathcal{P}(A)$, $N_1 = \mathcal{P}(A)/\mathcal{R}$, $p_1 = can$, $N_2 = \mathcal{P}(B)$, $p_2 = f$.
ii) Let $F : B^A \longrightarrow B$, $F(f) = f(a)$. Then F is surjective, $\mathcal{R} = \mathcal{R}_F$ is an equivalence relation by Exercise 1.3.3, v), and we can use Corollary 1.3.16 for $M = B^A$, $N_1 = B^A/\mathcal{R}$, $p_1 = can$, $N_2 = B$, $p_2 = F$.
iii) Let $F : B^A \longrightarrow B^C$, $F(f) =$ the restriction of f to C. Then F is surjective, $\mathcal{R} = \mathcal{R}_F$ is an equivalence relation by Exercise 1.3.3, v), and we can use Corollary 1.3.16 for $M = B^A$, $N_1 = B^A/\mathcal{R}$, $p_1 = can$, $N_2 = B^C$, $p_2 = F$.
iv) We can get ii) from iii) by taking $C = \{a\}$, and i) from iii) by taking $B = \{0, 1\}$, $A = A$ and $B = C$, and using the bijection between subsets

and characteristic functions defined in the solution of Exercise 1.3.18, iii).

Exercise 1.3.20 *Show that the relation defined on* $\mathbb{R}$ *by* $x\mathcal{R}y$ *if and only if* $x - y \in \mathbb{Z}$ *is an equivalence relation, and there is a bijection between the factor set and a circle.*

Solution: Let C denote the unit circle centered at the origin, and define $f : \mathbb{R} \longrightarrow C$ by $f(x) = (\cos(2\pi(x - [x])), \sin(2\pi(x - [x])))$, where $[x]$ is the greatest integer less than or equal to x. Then $0 \leq x - [x] < 1$, and so $(x-[x])-(y-[y]) \in \mathbb{Z}$ if and only if $(x-[x])-(y-[y]) = 0$, i.e. $x-y \in \mathbb{Z}$, thus $\mathcal{R} = \mathcal{R}_f$, and we can use Corollary 1.3.16 for $M = \mathbb{R}$, $N_1 = \mathbb{R}/\mathcal{R}$, $p_1 = can$, $N_2 = C$, $p_2 = f$.

1.4 Groups and morphisms of groups

Definition 1.4.1 *A* binary operation *on the set M is a function $\cdot : M \times M \longrightarrow M$, $\cdot(x, y) = xy$.*

Definition 1.4.2 *A set G, together with a binary operation $\cdot$ on G, denoted by $(G, \cdot)$, is called a* group *if the following conditions are satisfied:*
G1) the operation is associative, i.e. $x(yz) = (xy)z$ for all $x, y, z \in G$.
G2) the operation has an identity element, i.e. there exists an element $e \in G$ such that $ex = xe = x$ for all $x \in G$.
G3) every element in G has a symmetric element, i.e. for any $x \in G$ there exists an element $x' \in G$ such that $xx' = x'x = e$.
If the following condition is also satisfied:
G4) the operation is commutative, i.e. $xy = yx$ for all $x, y \in G$,
then the group is said to be abelian *(or* commutative*).*

As we can see in the above definition, our notation for a generic group operation will be multiplicative, i.e. a generic group will be denoted by $(G, \cdot)$, (or simply G if it is clear what the operation is) where the operation $\cdot : G \times G \longrightarrow G$, $\cdot(a, b) = ab$ is not necessarily the multiplication.

Exercise 1.4.3 *Write the definition of the group in additive notation, i.e. rewrite Definition 1.4.2 for $(G, +)$, where $+ : G \times G \longrightarrow G$, $+(x, y) = x + y$.*

Exercise 1.4.4 *i) If e_1 and e_2 are identity elements in a group, i.e. they both satisfy condition G2) in Definition 1.4.2, then prove that $e_1 = e_2$. This means that the identity element in a group is unique. Our notation for it will be 1_G if the notation for the operation of the group is multiplicative, and 0_G if the notation for the operation of the group is additive.*
ii) Show that the symmetric element of an element x in a group G is unique, i.e. if x' and x'' both satisfy the condition in Definition 1.4.2, G3), then $x' = x''$. If the notation is multiplicative, we will call the symmetric element of x the inverse *of x and we will denote it by x^{-1}. If the notation is additive, we will call the symmetric element of x* the opposite *of x and we will denote it by $-x$.*
iii) Prove that if in a group G we have $xy = xz$, it follows that $y = z$ (this is called the cancelation law).

Exercise 1.4.5 *Which of the following are groups:*
i) $(\mathbb{N}, +)$, the set of natural numbers, the operation is the addition of natural numbers.
ii) $(\mathbb{N}, \cdot)$, the set of natural numbers, the operation is the multiplication of natural numbers.
iii) $(\mathbb{Z}, +)$, the set of integers, the operation is the addition of integers.

iv) $(\mathbb{Z}, \cdot)$*, the set of integers, the operation is the multiplication of integers.*
v) $(\mathbb{Q}, +)$*, the set of rational numbers, the operation is the addition of rational numbers.*
vi) $(\mathbb{Q}, \cdot)$*, the set of rational numbers, the operation is the multiplication of rational numbers.*
vii) $(\mathbb{R}, +)$*, the set of real numbers, the operation is the addition of real numbers.*
viii) $(\mathbb{R}, \cdot)$*, the set of real numbers, the operation is the multiplication of real numbers.*
ix) $(\mathbb{C}, +)$*, the set of complex numbers, the operation is the addition of complex numbers.*
x) $(\mathbb{C}, \cdot)$*, the set of complex numbers, the operation is the multiplication of complex numbers.*
xi) $(\mathbb{N}^*, \cdot)$*, the set of nonzero natural numbers, the operation is the multiplication of natural numbers.*
xii) $(\mathbb{Z}^*, \cdot)$*, the set of nonzero integers, the operation is the multiplication of integers.*
xiii) $(\mathbb{Q}^*, \cdot)$*, the set of nonzero rational numbers, the operation is the multiplication of rational numbers.*
xiv) $(\mathbb{R}^*, \cdot)$*, the set of nonzero real numbers, the operation is the multiplication of real numbers.*
xv) $(\mathbb{C}^*, \cdot)$*, the set of nonzero complex numbers, the operation is the multiplication of complex numbers.*
xvi) $((0, \infty), \cdot)$*, the interval* $(0, \infty)$*, the operation is the multiplication of real numbers.*
xvii) $((-\infty, 0), \cdot)$*, the interval* $(-\infty, 0)$*, the operation is the multiplication of real numbers.*
xviii) $(S(M), \circ)$*,* $S(M) = \{f : M \longrightarrow M \mid f \text{ is bijective}\}$ *and* $\circ$ *is the composition of functions. We will denote* $S_n = S(\{1, 2, \ldots, n\})$*.*
xix) $(G^M, \cdot)$*, where* $(G, \cdot)$ *is a group,* M *is a set,* G^M *is the set of functions defined on* M *with values in* G*, and* $(f \cdot g)(x) = f(x)g(x)$ *for* $f, g \in G^M$*,* $x \in G$*.*
xx) $(GL_2(\mathbb{C}), \cdot)$*, where*

$$GL_2(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{C}, ad - bc \neq 0 \right\}$$

and $\cdot$ *is the multiplication of matrices.*
xxi) $(\{1, -1\}, \cdot)$*.*
xxii) $(\{1, -1\}, +)$*.*
xxiii) $(\{0\}, +)$*.*
xxiv) $(\{1\}, \cdot)$*.*
xxv) $(\{0\}, \cdot)$*.*

xxvi) $(Q_8, \cdot)$*, where* $\cdot$ *is the multiplication of matrices, and* Q_8 *is the following subset of* $M_2(\mathbb{C})$*:*

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}.$$

xxvii) $(\mathcal{P}(M), *)$*, where* M *is a set, and* $A * B = \{x \in M \mid x \in A \cup B, x \notin A \cap B\}$*.*

We are now going to define two operations on the set $\mathbb{Z}_n$ (see Exercise 1.3.12, ii)). In order to do that we will need the following:

Exercise 1.4.6 *Let* $n > 0$ *be an integer, and assume that* $a \equiv b \ (mod\ n)$ *and* $c \equiv d \ (mod\ n)$*. Then:*
i) $a + c \equiv b + d \ (mod\ n)$*.*
ii) $ac \equiv bd \ (mod\ n)$*.*

The previous exercise shows that we can talk about the sum and product of elements in $\mathbb{Z}_n$: if $\hat{a}, \hat{b} \in \mathbb{Z}_n$, define

$$\hat{a} + \hat{b} = \widehat{a + b},$$

and

$$\hat{a}\hat{b} = \widehat{ab}.$$

Exercise 1.4.7 *Which of the following sets are groups:*
i) $(\mathbb{Z}_n, +)$*.*
ii) $(\mathbb{Z}_n, \cdot)$*.*
iii) $(\mathbf{U}_n, \cdot)$*, where* $\mathbf{U}_n = \{\hat{a} \in \mathbb{Z}_n \mid 1 = (a, n)\}$*.*
iv) $(\mathbf{U}_n, +)$*.*

Exercise 1.4.8 *Let* G_1 *and* G_2 *be groups, and define the following operation on the cartesian product* $G_1 \times G_2$*:* $(x, y) \cdot (x', y') = (xx', yy')$*, where* $x, x' \in G_1$ *and* $y, y' \in G_2$*. Show that* $G_1 \times G_2$ *is a group with this operation (it is called the* direct product *of the groups* G_1 *and* G_2*).*

Definition 1.4.9 *If* G *and* G' *are groups, a function* $f : G \longrightarrow G'$ *is called a* group morphism *if* f *preserves the group operation, i.e.* $f(xy) = f(x)f(y)$ *for all* $x, y \in G$*. The morphism* f *is said to be an injective morphism if the function* f *is injective. Similarly, if the function* f *is surjective, we say that* f *is a surjective morphism. A group morphism* $f : G \longrightarrow G'$ *is*

called an isomorphism *if there exists a group morphism* $f' : G' \longrightarrow G$ *such that* $f \circ f' = Id_{G'}$ *and* $f' \circ f = Id_G$*; we then say that the groups* G *and* G' *are* isomorphic*, and we write* $G \simeq G'$*. A morphism from* G *to* G *is called an* endomorphism *of* G*, and an isomorphism from* G *to* G *is called an* automorphism *of* G*.*

The following properties of group morphisms are left as exercises:

Exercise 1.4.10 *Let* $f : G \longrightarrow G'$ *and* $g : G' \longrightarrow G''$ *be group morphisms. Then:*
i) $f(1_G) = 1_{G'}$*.*
ii) For $x \in G$*, we have* $f(x^{-1}) = f(x)^{-1}$*.*
iii) gf *is a group morphism.*
iv) f *is an isomorphism if and only if* f *is bijective.*

Exercise 1.4.11 *Which of the following maps are group morphisms? For each of them decide if they are injective, surjective, or an isomorphism. If a morphism is an isomorphism, find the inverse.*
i) $Id_G : G \longrightarrow G$*.*
ii) $i : \mathbb{Z} \longrightarrow \mathbb{Q}$*,* $i(x) = x/1$ *for* $x \in \mathbb{Z}$*.*
iii) If $x \in G$*,* $f_x : G \longrightarrow G$*,* $f_x(g) = xgx^{-1}$ *for all* $g \in G$*.*
iv) G *is a group,* M *is a nonempty set,* G^M *is as in Exercise 1.4.5, xix), and* $\varphi : G \longrightarrow G^M$*,* $\varphi(g)(x) = g$ *for all* $x \in M$*.*
v) $\ln : (0, \infty) \longrightarrow \mathbb{R}$*.*
vi) $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$*,* $f(\hat{a}(mod\ 4)) = \hat{a}(mod\ 2)$*.*
vii) $g : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$*,* $g(\hat{a}(mod\ 2)) = \hat{a}(mod\ 4)$*.*
viii) $p_1 : G_1 \times G_2 \longrightarrow G_1$*,* $p_1(x, y) = x$*.*

Exercise 1.4.12 *If* $\varphi : M \longrightarrow N$ *is a bijection, show that* $S(M) \simeq S(N)$ *(see Exercise 1.4.5, xviii)). In particular, if* M *has* n *elements, then* $M \simeq S_n$*.*

Exercise 1.4.13 *Write all the elements of* S_3 *and find the inverse of each element.*

Solutions to the Exercises on Section 1.4

Exercise 1.4.3 *Write the definition of the group in additive notation, i.e. rewrite Definition 1.4.2 for $(G,+)$, where $+ : G\times G \longrightarrow G$, $+(x,y) = x+y$.*
Solution: G1) $x+(y+z) = (x+y)+z$ for all $x,y,z \in G$.
G2) there exists an element $e \in G$ such that $e+x = x+e = x$ for all $x \in G$.
G3) for any $x \in G$ there exists an element $x' \in G$ such that $x+x' = x'+x = e$.
G is abelian if the following condition is also satisfied:
G4) $x+y = y+x$ for all $x,y \in G$

Exercise 1.4.4 *i) If e_1 and e_2 are identity elements in a group, i.e. they both satisfy condition G2) in Definition 1.4.2, then prove that $e_1 = e_2$. This means that the identity element in a group is unique. Our notation for it will be 1_G if the notation for the operation of the group is multiplicative, and 0_G if the notation for the operation of the group is additive.*
ii) Show that the symmetric element of an element x in a group G is unique, i.e. if x' and x'' both satisfy the condition in Definition 1.4.2, G3), then $x' = x''$. If the notation is multiplicative, we will call the symmetric element of x the inverse *of x and we will denote it by x^{-1}. If the notation is additive, we will call the symmetric element of x* the opposite *of x and we will denote it by $-x$.*
iii) Prove that if in a group G we have $xy = xz$, it follows that $y = z$ (this is called the cancelation law).
Solution: i) Taking $x = e_2$ in G2) for e_1 we get: $e_1e_2 = e_2e_1 = e_2$. Taking $x = e_1$ in G2) for e_2 we get: $e_2e_1 = e_1e_2 = e_1$. Comparing the two we get $e_1e_2 = e_2e_1 = e_2 = e_1$.
ii) Since $xx' = 1_G$, it follows that $x''xx' = x''$, and since $x''x = 1_G$, we get that $x' = x''$.
iii) If $xy = xz$, then $x^{-1}xy = x^{-1}xz$, so $y = z$.

Exercise 1.4.5 *Which of the following are groups:*
i) $(\mathbb{N},+)$, the set of natural numbers, the operation is the addition of natural numbers.
ii) $(\mathbb{N},\cdot)$, the set of natural numbers, the operation is the multiplication of natural numbers.
iii) $(\mathbb{Z},+)$, the set of integers, the operation is the addition of integers.
iv) $(\mathbb{Z},\cdot)$, the set of integers, the operation is the multiplication of integers.
v) $(\mathbb{Q},+)$, the set of rational numbers, the operation is the addition of rational numbers.
vi) $(\mathbb{Q},\cdot)$, the set of rational numbers, the operation is the multiplication of rational numbers.
vii) $(\mathbb{R},+)$, the set of real numbers, the operation is the addition of real

numbers.
viii) $(\mathbb{R}, \cdot)$*, the set of real numbers, the operation is the multiplication of real numbers.*
ix) $(\mathbb{C}, +)$*, the set of complex numbers, the operation is the addition of complex numbers.*
x) $(\mathbb{C}, \cdot)$*, the set of complex numbers, the operation is the multiplication of complex numbers.*
xi) $(\mathbb{N}^*, \cdot)$*, the set of nonzero natural numbers, the operation is the multiplication of natural numbers.*
xii) $(\mathbb{Z}^*, \cdot)$*, the set of nonzero integers, the operation is the multiplication of integers.*
xiii) $(\mathbb{Q}^*, \cdot)$*, the set of nonzero rational numbers, the operation is the multiplication of rational numbers.*
xiv) $(\mathbb{R}^*, \cdot)$*, the set of nonzero real numbers, the operation is the multiplication of real numbers.*
xv) $(\mathbb{C}^*, \cdot)$*, the set of nonzero complex numbers, the operation is the multiplication of complex numbers.*
xvi) $((0, \infty), \cdot)$*, the interval* $(0, \infty)$*, the operation is the multiplication of real numbers.*
xvii) $((-\infty, 0), \cdot)$*, the interval* $(-\infty, 0)$*, the operation is the multiplication of real numbers.*
xviii) $(S(M), \circ)$*,* $S(M) = \{f : M \longrightarrow M \mid f \text{ is bijective}\}$ *and* $\circ$ *is the composition of functions. We will denote* $S_n = S(\{1, 2, \ldots, n\})$*.*
xix) $(G^M, \cdot)$*, where* $(G, \cdot)$ *is a group,* M *is a set,* G^M *is the set of functions defined on* M *with values in* G*, and* $(f \cdot g)(x) = f(x)g(x)$ *for* $f, g \in G^M$*,* $x \in G$*.*
xx) $(GL_2(\mathbb{C}), \cdot)$*, where*

$$GL_2(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{C}, ad - bc \neq 0 \right\}$$

and $\cdot$ *is the multiplication of matrices.*
xxi) $(\{1, -1\}, \cdot)$*.*
xxii) $(\{1, -1\}, +)$*.*
xxiii) $(\{0\}, +)$*.*
xxiv) $(\{1\}, \cdot)$*.*
xxv) $(\{0\}, \cdot)$*.*
xxvi) $(Q_8, \cdot)$*, where* $\cdot$ *is the multiplication of matrices, and* Q_8 *is the following subset of* $M_2(\mathbb{C})$*:*

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \right.$$

$$\left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}.$$

xxvii) $(\mathcal{P}(M), *)$*, where* M *is a set, and* $A * B = \{x \in M \mid x \in A \cup B, x \notin A \cap B\}$.

Solution: i) No, G3) is not satisfied: $x + 1 \neq 0$ for all $x \in \mathbb{N}$.
ii) No, G3) is not satisfied: $x \cdot 0 \neq 1$ for all $x \in \mathbb{N}$.
iii) $(\mathbb{Z}, +)$ is an abelian group: the sum of two integers is an integer; addition is associative and commutative; 0 is the identity element; the opposite of $x \in \mathbb{Z}$ is $-x$.
iv) No, G3) is not satisfied: $x \cdot 0 \neq 1$ for all $x \in \mathbb{Z}$.
v) $(\mathbb{Q}, +)$ is an abelian group: the sum of two rational numbers is a rational number; addition is associative and commutative; 0 is the identity element; the opposite of $x \in \mathbb{Q}$ is $-x$.
vi) No, G3) is not satisfied: $x \cdot 0 \neq 1$ for all $x \in \mathbb{Q}$.
vii) $(\mathbb{R}, +)$ is an abelian group: the sum of two real numbers is a real number; addition is associative; 0 is the identity element; the opposite of $x \in \mathbb{R}$ is $-x$.
viii) No, G3) is not satisfied: $x \cdot 0 \neq 1$ for all $x \in \mathbb{R}$.
ix) $(\mathbb{C}, +)$ is an abelian group: the sum of two complex numbers is a complex number; addition is associative and commutative; 0 is the identity element; the opposite of $x \in \mathbb{C}$ is $-x$.
x) No, G3) is not satisfied: $x \cdot 0 \neq 1$ for all $x \in \mathbb{C}$.
xi) No, G3) is not satisfied: $x \cdot 2 \neq 1$ for all $x \in \mathbb{N}^*$.
xii) No, G3) is not satisfied: $x \cdot 2 \neq 1$ for all $x \in \mathbb{Z}^*$.
xiii) $(\mathbb{Q}^*, \cdot)$ is an abelian group: the product of two nonzero rational numbers is a nonzero rational number; multiplication is associative and commutative; 1 is the identity element; the inverse of $x \in \mathbb{Q}^*$ is $1/x$.
xiv) $(\mathbb{R}^*, \cdot)$ is an abelian group: the product of two nonzero real numbers is a nonzero real number; multiplication is associative and commutative; 1 is the identity element; the inverse of $x \in \mathbb{R}^*$ is $1/x$.
xv) $(\mathbb{C}^*, \cdot)$ is an abelian group: the product of two nonzero complex numbers is a nonzero complex number; multiplication is associative and commutative; 1 is the identity element; the inverse of $a + bi \in \mathbb{C}^*$ is

$$\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

xvi) $((0, \infty), \cdot)$ is an abelian group: the product of two positive real numbers is a positive real number; multiplication is associative and commutative; 1 is the identity element; the inverse of $x \in (0, \infty)$ is $1/x$.
xvii) No, $\cdot$ is not an operation on $(-\infty, 0)$, because $(-1) \cdot (-1) \notin (-\infty, 0)$.
xviii) $(S(M), \circ)$ is a group. The composition of two bijective functions is bijective; composition of functions is associative; the identity element is

Id_M; a bijective function is invertible. $S(M)$ is not necessarily abelian: S_2 is abelian, but S_3 is not: the transpositions (12) and (13) do not commute (see Exercise 1.4.13).
xix) $(G^M, \cdot)$ is a group, and it is abelian if G is abelian. It is clear that $f \cdot g \in G^M$. The operation on G^M is associative because the operation on G is associative. The identity element is the constant function $1 : M \longrightarrow G$, $1(x) = 1_G$ for all $x \in M$. The inverse of $f \in G^M$ is $f^{-1} : M \longrightarrow G$, $f^{-1}(x) = f(x)^{-1}$ for $x \in M$.
xx) $(GL_2(\mathbb{C}), \cdot)$ is a nonabelian group. Recall that multiplication of matrices is defined as

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

and it is associative. The identity element is

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

and the inverse of a matrix is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}.$$

$GL_2(\mathbb{C})$ is nonabelian because

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$$

xxi) $(\{1, -1\}, \cdot)$ is an abelian group.
xxii) $(\{1, -1\}, +)$ is not a group because $1 + 1 \notin \{1, -1\}$.
xxiii) $(\{0\}, +)$ is an abelian group.
xxiv) $(\{1\}, \cdot)$ is an abelian group.
xxv) $(\{0\}, \cdot)$ is an abelian group.
xxvi) $(Q_8, \cdot)$ is a nonabelian group, called the quaternion group. If we denote

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad -1 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad i = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad -i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$j = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad -j = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \quad k = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \quad -k = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

then we can check that $i^2 = j^2 = k^2 = ijk = -1$, and we can use these relations to check that $\cdot$ is an operation on Q_8. Q_8 is not abelian because $ij \neq ji$.
xxvii) $(\mathcal{P}(M), *)$ is an abelian group. If $A, B, C \in \mathcal{P}(M)$, then both $A * (B * C)$ and $(A * B) * C$ are equal to the set

$$\{x \in M \mid x \in A \cup B \cup C, x \notin (A \cap B) \cup (A \cap C) \cup (B \cap C)\},$$

so $*$ is associative. The identity element is $\emptyset$ and the symmetric of the set A is A itself.

Exercise 1.4.6 *Let $n > 0$ be an integer, and assume that $a \equiv b \ (mod\ n)$ and $c \equiv d \ (mod\ n)$. Then:*
i) $a + c \equiv b + d \ (mod\ n)$.
ii) $ac \equiv bd \ (mod\ n)$.
Solution: i) Since $n \mid a - b$ and $n \mid c - d$, let k, l be integers such that $a - b = kn$ and $c - d = ln$. Then $a - b + c - d = (k + l)n$, so $n \mid a + c - (b + d)$.
ii) With the notation of i), we have $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckn + bln = n(ck + bl)$, so $n \mid ac - bd$.

Exercise 1.4.7 *Which of the following sets are groups:*
i) $(\mathbb{Z}_n, +)$.
ii) $(\mathbb{Z}_n, \cdot)$.
iii) $(\mathbf{U}_n, \cdot)$, where $\mathbf{U}_n = \{\hat{a} \in \mathbb{Z}_n \mid 1 = (a, n)\}$.
iv) $(\mathbf{U}_n, +)$.
Solution: i) $(\mathbb{Z}_n, +)$ is an abelian group. By Exercise 1.4.6 we have that $+$ is an operation, and it is associative and commutative because addition of the integers is so. The identity element is $\hat{0}$, and the opposite of $\hat{a}$ is $\widehat{n - a}$.
ii) $(\mathbb{Z}_n, \cdot)$ is not a group if $n \neq 1$, because G3) is not satisfied, $\hat{0} \cdot \hat{a} = \hat{0} \neq \hat{1}$ for all a.
iii) $(\mathbf{U}_n, \cdot)$ is an abelian group, because $\cdot$ is associative and commutative, and $\hat{1}$ is the identity element. If $1 = (a, n)$, then $1 = au + nv$, so $\hat{1} = \widehat{au + nv} = \hat{a}\hat{u} + \hat{n}\hat{v} = \hat{a}\hat{u}$, so the inverse of $\hat{a}$ is $\hat{u}$.
iv) We clearly have that $\hat{1} \in \mathbf{U}_n$, but if we add n copies of $\hat{1}$ we get $\hat{0} \notin \mathbf{U}_n$, so $+$ is not an operation on $\mathbf{U}_n$.

Exercise 1.4.8 *Let G_1 and G_2 be groups, and define the following operation on the cartesian product $G_1 \times G_2$: $(x, y) \cdot (x', y') = (xx', yy')$, where $x, x' \in G_1$ and $y, y' \in G_2$. Show that $G_1 \times G_2$ is a group with this operation (it is called the* direct product *of the groups G_1 and G_2).*
Solution: It is clear that $\cdot$ is an operation and it is associative. The identity element is $(1_{G_1}, 1_{G_2})$, and the inverse of (x_1, x_2) is (x_1^{-1}, x_2^{-1}).

Exercise 1.4.10 *Let $f : G \longrightarrow G'$ and $g : G' \longrightarrow G''$ be group morphisms. Then:*
i) $f(1_G) = 1_{G'}$.
ii) For $x \in G$, we have $f(x^{-1}) = f(x)^{-1}$.
iii) gf is a group morphism.
iv) f is an isomorphism if and only if f is bijective.
Solution: i) $1_G \cdot 1_G = 1_G$, so $f(1_G \cdot 1_G) = f(1_G)$, or $f(1_G)f(1_G) = f(1_G) = f(1_G)1_{G'}$, and the assertion follows from the cancelation law.
ii) We have that $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_G) = 1_{G'}$, so the assertion follows by multiplying both sides of this equality by $f(x)^{-1}$.
iii) $gf(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y))$.
iv) We have to prove that if the morphism f is bijective, then its inverse f^{-1} is also a morphism. We have $f^{-1}(x'y') = f^{-1}(f(f^{-1}(x'))f(f^{-1}(y'))) = f^{-1}(f(f^{-1}(x')f^{-1}(y'))) = f^{-1}f(f^{-1}(x')f^{-1}(y')) = f^{-1}(x')f^{-1}(y')$.

Exercise 1.4.11 *Which of the following maps are group morphisms? For each of them decide if they are injective, surjective, or an isomorphism. If a morphism is an isomorphism, find the inverse.*
i) $Id_G : G \longrightarrow G$.
ii) $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, $i(x) = x/1$ for $x \in \mathbb{Z}$.
iii) If $x \in G$, $f_x : G \longrightarrow G$, $f_x(g) = xgx^{-1}$ for all $g \in G$.
iv) G is a group, M is a nonempty set, G^M is as in Exercise 1.4.5, xix), and $\varphi : G \longrightarrow G^M$, $\varphi(g)(x) = g$ for all $x \in M$.
v) $\ln : (0, \infty) \longrightarrow \mathbb{R}$.
vi) $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$, $f(\hat{a}(mod\ 4)) = \hat{a}(mod\ 2)$.
vii) $g : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$, $g(\hat{a}(mod\ 2)) = \hat{a}(mod\ 4)$.
viii) $p_1 : G_1 \times G_2 \longrightarrow G_1$, $p_1(x, y) = x$.
Solution: i) it is an isomorphism, and it is its own inverse.
ii) this is an injective morphism.
iii) $f_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = f_x(g)f_x(h)$. It is an isomorphism, and the inverse of f_x is $f_{x^{-1}}$.
iv) We have $\varphi(gh)(x) = gh = \varphi(g)\varphi(h)(x)$ for all $x \in M$, so φ is a group morphism. It is injective, because if $\varphi(g) = \varphi(h)$, then $\varphi(g)(x) = \varphi(h)(x)$ for all $x \in M$, so $g = h$.
v) We have $\ln(xy) = \ln(x) + \ln(y)$, so ln is a group morphism. Since ln is bijective, with inverse the exponential function, ln is an isomorphism.
vi) Let us check that f is correctly defined: if $\hat{a}(mod\ 4) = \hat{b}(mod\ 4)$, then $4 \mid a - b$, so $2 \mid a - b$ and hence $\hat{a}(mod\ 2) = \hat{b}(mod\ 2)$, or $f(\hat{a}(mod\ 4)) = f(\hat{b}(mod\ 4))$, and f is correctly defined. By the definition of addition mod 4 or mod 2, f is a group morphism which is clearly surjective.
vii) g is not correctly defined: $\hat{1}(mod\ 2) = \hat{3}(mod\ 2)$, but $\hat{1}(mod\ 4) \neq \hat{3}(mod\ 4)$).

viii) We have $p_1((x,y)(x',y')) = p_1(xx',yy') = xx' = p_1(x,y)p_1(x',y')$, so p_1 is a group morphism. It is clearly surjective, because if $x \in G_1$, then $x = p_1(x, 1_{G_2})$.

Exercise 1.4.12 *If $\varphi : M \longrightarrow N$ is a bijection, show that $S(M) \simeq S(N)$ (see Exercise 1.4.5, xviii)). In particular, if M has n elements, then $M \simeq S_n$.*
Solution: Define $\psi : S(M) \longrightarrow S(N)$ by $\psi(f) = \varphi f \varphi^{-1}$ for $f \in S(M)$. It is easy to check that ψ is a morphism and that its inverse is $\psi^{-1} : S(N) \longrightarrow S(M)$, $\psi^{-1}(g) = \varphi^{-1} g \varphi$.

Exercise 1.4.13 *Write all the elements of S_3 and find the inverse of each element.*
Solution: We will write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

if $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. We will also write this as $\sigma = (123)$ (the *cycle* $(a_1 a_2 \dots a_k)$ in S_n is the function that sends a_i to a_{i+1} for $i = 1, \dots, k-1$, and a_k to a_1, and leaves all the other elements unchanged; the set $\{a_1, a_2, \dots, a_k\}$ is called the *orbit* of the cycle, and k is called its length). With this notation we have

$$S_3 = \{Id, (12), (13), (23), (123), (132)\}.$$

Each of $Id, (12), (13), (23)$ is its own inverse, and the inverse of (123) is (132). Note that S_3 is not abelian because $(12)(13) = (132)$ and $(13)(12) = (123)$.

1.5 Subgroups and normal subgroups

We know that both $(\mathbb{R}^*, \cdot)$ and $((0,\infty), \cdot)$ are groups. This means that the operation of the group $(\mathbb{R}^*, \cdot)$ restricted to the subset $(0,\infty)$ is also an operation, and it satisfies the axioms in the definition of a group. We say that the operation of the group $(\mathbb{R}^*, \cdot)$ induces a group structure on the subset $(0,\infty)$, or that $(0,\infty)$ is a subgroup of $\mathbb{R}^*$. In general we have the following:

Definition 1.5.1 *Let G be a group, and H a nonempty subset of G. Then H is called a* subgroup *of G if the operation on G induces an operation on H such that H together with the induced operation forms a group. If H is a subgroup of G we write $H \leq G$.*

Trivial examples of subgroups in any group G are the so called improper subgroups $\{1_G\}$ and G itself. When checking that a certain nonempty subset H of a group G is a subgroup we need to check three conditions:
SG1) If $x, y \in H$, then $xy \in H$. This means that the operation on G induces an operation on H. (If this is true, we say that H is closed, or stable, under the operation of G.)
Associativity is a gimme, because we know it holds for elements of G, and all elements of H are also elements of G.
SG2) $1_G \in H$. This comes from condition G2) in the definition of a group applied to H: if e is an identity element of H, then $ee = e$ in H, and when we consider this equality in G and multiply both sides by e^{-1} we get that $e = 1_G$.
SG3) If $x \in H$, then $x^{-1} \in H$. Because of $G2$, any inverse of x in H will be an inverse of x in G, so the assertion is true because of the uniqueness of the inverse.

Proposition 1.5.2 *Let G be a group and $\emptyset \neq H \subseteq G$. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $x^{-1}y \in H$.

Proof: i) $\Rightarrow$ ii). Let $x, y \in H$. By SG3) we have $x^{-1} \in H$, and by SG1) we get $x^{-1}y \in H$.
ii) $\Rightarrow$ i). We first check SG2). Let $x \in H$, then by ii) $x^{-1}x = 1_G \in H$. Now for $x \in H$ we can use ii) for x and 1_G to get $x^{-1}1_G = x^{-1} \in H$, so SG3) also holds. Finally, if $x, y \in H$, then $xy = (x^{-1})^{-1}y \in H$ by SG3) and ii), so SG1) holds too. ∎

Exercise 1.5.3 *Write in additive notation conditions SG1), SG2), SG3), and Proposition 1.5.2.*

Exercise 1.5.4 *Let G be a group and $\emptyset \neq H \subseteq G$. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $xy^{-1} \in H$.

If $\emptyset \neq H \subseteq G$ is a finite subset, it is a lot easier to check that $H \leq G$:

Proposition 1.5.5 *Let G be a group and $\emptyset \neq H \subseteq G$ a finite subset. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $xy \in H$.

Proof: We only prove ii) $\Rightarrow$ i), because the converse is obvious. Let $x \in H$, and consider the function $\varphi : H \longrightarrow H$, defined by $\varphi(y) = xy$ for $y \in H$. Then φ takes values in H because of ii), and it is injective because of the cancelation law in G. Since H is finite, it follows that φ is also surjective, so there exists $x' \in H$ such that $\varphi(x') = x$. This means $xx' = x$, and after considering this equality in G and multiplying both sides on the left by x^{-1}, we get that $x' = 1_G$, so we checked SG2). We now use again the fact that φ is surjective, so there exists $x'' \in H$ such that $\varphi(x'') = 1_G$. This means $xx'' = 1_G$, and after considering this equality in G and multiplying both sides on the left by x^{-1}, we get that $x'' = x^{-1}$, so we also checked SG3). ∎

Exercise 1.5.6 *Which of the following subsets are subgroups:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) $\mathbb{N} \subseteq \mathbb{Z}$.
iii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iv) $\{0, 2, 4\} \subseteq \mathbb{Z}_5$.
v) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
vi) $\{Id, (12)\} \subseteq S_3$.
vii) $\{Id, (12), (13)\} \subseteq S_3$.
viii) $\{Id, (123)\} \subseteq S_3$.
ix) $\{Id, (123), (132)\} \subseteq S_3$.
x) $O(2) = \{A \in GL_2(\mathbb{R}) \mid A^{-1} = A^t\} \subseteq GL_2(\mathbb{R})$ (see Exercise 1.4.5, xx)).
xi) $SO(2) = \{A \in O(2) \mid det(A) = 1\} \subseteq O(2)$
xii) $\{1, -1, i, -i\} \subseteq Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, the quaternion group, see Exercise 1.4.5, xxvi).
xiii) $H \cap K$, where $H, K \leq G$.
xiv) $H \cup K$, where $H, K \leq G$.

We now show that all the subgroups of $\mathbb{Z}$ look like the one in Exercise 1.5.6 iii).

Proposition 1.5.7 *If $H \leq \mathbb{Z}$, then there exists $n \in \mathbb{Z}$ such that $H = n\mathbb{Z}$.*

Proof: If $H = \{0\}$ we take $n = 0$. If $H \neq \{0\}$, we consider the set $W = \{x \in H \mid x > 0\}$. Then if $0 \neq x \in H$, then we also have $-x \in H$ and so $W \neq \emptyset$. By the well-ordering principle, W has a smallest element n. Since H is a subgroup and $n \in H$, it is clear that $n\mathbb{Z} \subseteq H$. Conversely, if $m \in H$, we write $m = qn + r$, where $0 \leq n$. Since $r = m - nq \in H$ it follows that $r = 0$ because otherwise we get a contradiction with the fact that n is the least element in W, and so $m = nq \in n\mathbb{Z}$. ∎

Exercise 1.5.8 *Let $f : G \longrightarrow G'$ be a morphism of groups. Then:*
i) $f(G) \leq G'$ (we denote $f(G)$ by $Im(f)$ and call it the image of f).
ii) $f^{-1}(1_{G'}) \leq G$ (we denote $f^{-1}(1_{G'})$ by $Ker(f)$ and call it the kernel of f).
iii) If $H \leq G$, then $f(H) \leq G'$.
iv) If $H' \leq G'$, then $f^{-1}(H') \leq G$.
v) f is surjective $\Leftrightarrow Im(f) = G'$.
vi) f is injective $\Leftrightarrow Ker(f) = \{1_G\}$.

The following result is a version for groups of Proposition 1.1.14:

Proposition 1.5.9 *Let $f : G \longrightarrow G'$ be a group morphism. Then the following assertions hold:*
i) f is injective if and only if given any group X, and group morphisms $g, h : X \longrightarrow G$ such that $f \circ g = f \circ h$, it follows that $g = h$.
ii) f is surjective if and only if given any group X, and group morphisms $g, h : G' \longrightarrow X$ such that $g \circ f = h \circ f$, it follows that $g = h$.

Proof: We will only prove i), because ii) is very hard to prove (it is easy to see, of course, that if f is surjective, then the condition in ii) holds, the other implication is hard). We already know from Proposition 1.1.14 i) that if f is injective, then the condition is satisfied, because groups are sets, and group morphisms are functions. We now assume that f is not injective, and therefore $Ker(f) \neq \{1_G\}$ by Exercise 1.5.8 vi). Choose $X = Ker(f)$ and take $g : X \longrightarrow G$ to be the inclusion, and $h : X \longrightarrow G$ to be the constant function sending all elements of X to 1_G. It is clear that $fg = fh$, but $g \neq h$ because there is an $x \in X$, $x \neq 1$, so $g(x) \neq h(x)$, and the proof is complete. ∎

Let now G be a group, and E a subset of G. There exists a smallest subgroup of G that contains all the elements of E, it is the intersection of all the subgroups containing E. Such subgroups clearly exist, since G contains E. We call it the subgroup generated by the set E. It is clear that the subgroup generated by $\emptyset$ is $\{1_G\}$. If the group is generated by a set with one element, the group is called cyclic. A description of the subgroup generated by a set is given in the following:

Proposition 1.5.10 *Let E be a subset of the group G. The subgroup H generated by E consists of all finite products of elements of E or inverses of elements of E.*

Proof: Let H' the set of all finite products of elements of E or inverses of elements of E. Since H is a subgroup that contains E, it is clear that $H' \subseteq H$. Since H is the smallest subgroup that contains E, in order to prove the inclusion $H \subseteq H'$ it is enough to prove that H' is a subgroup that contains E. It is clear that H' contains E, and that if $x, y \in H'$, then $x^{-1}y \in H'$, which proves the claim. ∎

If $H, K \leq G$, the subgroup generated by $H \cup K$ will be denoted by HK (or $H + K$ in additive notation). By the previous result, if G is a cyclic group generated by the element a, then we have

$$G = \{a^k \mid k \in \mathbb{Z}\},$$

where

$$a^k = \begin{cases} \text{the product of } k \text{ copies of } a & \text{if } k > 0 \\ 1_G & \text{if } k = 0 \\ \text{the product of } -k \text{ copies of } a^{-1} & \text{if } k < 0 \end{cases}$$

In additive notation, if G is a cyclic group generated by the element a, then we have

$$G = \{ka \mid k \in \mathbb{Z}\},$$

where

$$ka = \begin{cases} \text{the sum of } k \text{ copies of } a & \text{if } k > 0 \\ 0_G & \text{if } k = 0 \\ \text{the sum of } -k \text{ copies of } -a & \text{if } k < 0 \end{cases}$$

Example 1.5.11 *It is clear that $\mathbb{Z}$ is cyclic (it is generated by 1 or -1), and $n\mathbb{Z}$ is also cyclic for any n (it is generated by n or $-n$). Then $\mathbb{Z}_n$ is cyclic, generated by 1. Since all cyclic groups are clearly abelian, S_3 is not cyclic. It can also be checked that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian but not cyclic.*

We now introduce an important class of subgroups.

Definition 1.5.12 *Let G be a group and $H \leq G$. We will say that H is a* normal *subgroup of G (and we will write $H \trianglelefteq G$) if for any $x \in G$ and $h \in H$ we have $xhx^{-1} \in H$.*

If we denote $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$, the condition in the definition above becomes $xHx^{-1} \subseteq H$ for all $x \in G$ (we can also use $\leq$ instead of

$\subseteq$, since xHx^{-1} is a subgroup of G, hence of H if it is contained in it). It is clear that the trivial subgroups $\{1_G\}$ and G are normal, and also that any subgroup of an abelian group is normal. Here are some examples and counterexamples.

Exercise 1.5.13 *Which of the following subsets are normal subgroups:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iii) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
iv) $\{Id, (12)\} \subseteq S_3$.
v) $\{Id, (123), (132)\} \subseteq S_3$.
vi) $O(2) = \{A \in GL_2(\mathbb{R}) \mid A^{-1} = A^t\} \subseteq GL_2(\mathbb{R})$ *(see Exercise 1.4.5, xx)).*
vii) $SO(2) = \{A \in O(2) \mid det(A) = 1\} \subseteq O(2)$
viii) $\{1, -1, i, -i\} \subseteq Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$*, the quaternion group, see Exercise 1.4.5, xxvi).*

We end this section with the study of the behavior of normal groups through group morphisms.

Proposition 1.5.14 *Let* $f : G \longrightarrow G'$ *be a group morphism. Then the following assertions hold:*
i) If $H' \trianglelefteq G'$*, then* $f^{-1}(H') \trianglelefteq G$.
ii) If f *is surjective and* $H \trianglelefteq G$*, then* $f(H) \trianglelefteq G'$.

Proof: i) We know from Exercise 1.5.8 iv) that $f^{-1}(H') \leq G$. Let $x \in G$ and $h \in f^{-1}(H')$. We know that $f(h) \in H'$ and we want to prove that $f(xhx^{-1}) \in H'$. We have $f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)f(h)f(x)^{-1} \in H'$, because $H' \trianglelefteq G'$.
ii) We know from Exercise 1.5.8 iii) that $f(H) \leq G'$. Let $x' \in G'$ and $h' \in f(H)$. Then $h' = f(h)$ for some $h \in H$, and since f is surjective, $x' = f(x)$ for some $x \in G$. We then have $x'h'x'^{-1} = f(x)f(h)f(x)^{-1} = f(x)f(h)f(x^{-1}) = f(xhx^{-1}) \in f(H)$, since $H \trianglelefteq G$. ∎

Exercise 1.5.15 *Give an example to show that the assertion in Proposition 1.5.14 ii) is not true if* f *is not surjective.*

Corollary 1.5.16 *Let* $f : G \longrightarrow G'$ *be a surjective group morphism. There exists a bijective correspondence between the subgroups of* G' *and the subgroups of* G *which contain* $Ker(f)$*. This correspondence induces a bijective correspondence between the normal subgroups of* G' *and the normal subgroups of* G *which contain* $Ker(f)$*.*

Proof: Let $H' \leq G'$. Then $f^{-1}(H') \leq G$ and $Ker(f) = f^{-1}(1_G) \subseteq f^{-1}(H')$. If $H \leq G$ and $Ker(f) \subseteq H$, then $f(H) \leq G'$. We prove first that

$$f(f^{-1}(H')) = H' \tag{1.1}$$

Let $h' \in H'$. Since f is surjective, $h' = f(h)$ for some $h \in G$. Since it is clear that $h \in f^{-1}(H')$ this shows that $H' \subseteq f(f^{-1}(H'))$. Conversely, let $h' \in f(f^{-1}(H'))$. Then $h' = f(h)$, where $h \in f^{-1}(H')$. But this means $f(h) \in H'$, so $h' \in H'$.
We now prove

$$f^{-1}(f(H)) = H \tag{1.2}$$

Indeed, if $h \in f^{-1}(f(H))$, then $f(h) \in f(H)$, so $f(h) = f(h_1)$, where $h_1 \in H$. Then $hh_1^{-1} \in Ker(f) \subseteq H$, so $h \in H$. Conversely, if $h \in H$, then $f(h) \in f(H)$, and so clearly $h \in f^{-1}(f(H))$.
By (1.1) and (1.2) we see that the correspondences defined above are bijections inverse to each other. The statement about normal subgroups follows from Proposition 1.5.14. ∎

Exercise 1.5.17 *Show that any subgroup of $\mathbb{Z}_n$ is generated by an element $\hat{d}$, where $d \mid n$.*

Solutions to the Exercises on Section 1.5

Exercise 1.5.3 *Write in additive notation conditions SG1), SG2), SG3), and Proposition 1.5.2.*
Solution: SG1) If $x, y \in H$, then $x + y \in H$.
SG2) $0_G \in H$.
SG3) If $x \in H$, then $-x \in H$.

Exercise 1.5.4 *Let G be a group and $\emptyset \neq H \subseteq G$. Then the following assertions are equivalent:*
i) $H \leq G$.
ii) If $x, y \in H$, then $xy^{-1} \in H$.
Solution: i) $\Rightarrow$ ii). Let $x, y \in H$. By SG3) we have $y^{-1} \in H$, and by SG1) we get $xy^{-1} \in H$.
ii) $\Rightarrow$ i). We first check SG2). Let $x \in H$, then by ii) $xx^{-1} = 1_G \in H$. Now for $x \in H$ we can use ii) for x and 1_G to get $1_G x^{-1} = x^{-1} \in H$, so SG3) also holds. Finally, if $x, y \in H$, then $xy = x(y^{-1})^{-1} \in H$ by SG3) and ii), so SG1) holds too.

Exercise 1.5.6 *Which of the following subsets are subgroups:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) $\mathbb{N} \subseteq \mathbb{Z}$.
iii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iv) $\{0, 2, 4\} \subseteq \mathbb{Z}_5$.
v) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
vi) $\{Id, (12)\} \subseteq S_3$.
vii) $\{Id, (12), (13)\} \subseteq S_3$.
viii) $\{Id, (123)\} \subseteq S_3$.
ix) $\{Id, (123), (132)\} \subseteq S_3$.
x) $O(2) = \{A \in GL_2(\mathbb{R}) \mid A^{-1} = A^t\} \subseteq GL_2(\mathbb{R})$ (see Exercise 1.4.5, xx)).
xi) $SO(2) = \{A \in O(2) \mid det(A) = 1\} \subseteq O(2)$
xii) $\{1, -1, i, -i\} \subseteq Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, the quaternion group, see Exercise 1.4.5, xxvi).
xiii) $H \cap K$, where $H, K \leq G$.
xiv) $H \cup K$, where $H, K \leq G$.
Solution: i) $\mathbb{Z} \leq \mathbb{Q}$, because $0 \in \mathbb{Z}$, and $n - m \in \mathbb{Z}$ for all integers m, n.
ii) Not a subgroup, $1 - 2 \notin \mathbb{N}$.
iii) $n\mathbb{Z} \leq \mathbb{Z}$, because $0 = n \cdot 0 \in n\mathbb{Z}$, and if $k, k' \in \mathbb{Z}$, then

$$nk - nk' = n(k - k') \in n\mathbb{Z}.$$

iv) Not a subgroup, $2 + 4 = 1 \notin \{0, 2, 4\}$.

v) $\{0,2,4\} \leq \mathbb{Z}_6$, because $\{0,2,4\}$ is closed under $+$:

$$2+2=4, \;\; 2+4=0, \;\; 4+4=2.$$

vi) $\{Id,(12)\} \leq S_3$, because $(12)(12) = Id$.
vii) Not a subgroup, $(12)(13) = (132) \notin \{Id,(12),(13)\}$.
viii) Not a subgroup, $(123)(123) = (132) \notin \{Id,(123)\}$.
ix) $\{Id,(123),(132)\} \leq S_3$, because $(123)(123) = (132)$ and $(132)(132) = (123)$.
x) $O(2) \leq GL_2(\mathbb{R})$, because $I_2 \in O(2)$, and if $A, B \in O(2)$, then

$$(A^{-1}B)^{-1} = B^{-1}A = B^t(A^t)^t = (A^tB)^t = (A^{-1}B)^t.$$

xi) $SO(2) \leq O(2)$, because $I_2 \in SO(2)$, and if $A, B \in SO(2)$, then $det(A^{-1}B) = det(A^tB) = det(A^t)det(B) = det(A)det(B) = 1$.
xii) $\{1,-1,i,-i\} \leq Q_8$, because

$$x \in \{1,-1,i,-i\} \Rightarrow -x \in \{1,-1,i,-i\},$$

so we only have to check that $i^2 = -1$.
xiii) Clearly $H \cap K \neq \emptyset$, because $1_G \in H \cap K$. If $x, y \in H \cap K$, then $x, y \in H$ and $x, y \in K$, so $x^{-1}y \in H$ and $x^{-1}y \in K$, so $x^{-1}y \in H \cap K$. Note that the same proof works for the intersection of an arbitrary family of subgroups, not just two subgroups.
xiv) If one of H or K is contained in the other one, then the union is equal to the larger of the two, and it is therefore a subgroup. Now if $H \not\subseteq K$ and $K \not\subseteq H$ we show that $H \cup K$ is not a subgroup. Indeed, let $x \in H$, $x \notin K$, $y \in K$, and $y \notin H$. Then $xy \notin H \cup K$, because if $xy \in H$ it follows that $y = x^{-1}xy \in H$, and if $xy \in K$, then $x = xyy^{-1} \in K$.

Exercise 1.5.8 *Let $f : G \longrightarrow G'$ be a morphism of groups. Then:*
i) $f(G) \leq G'$ (we denote $f(G)$ by $Im(f)$ and call it the image of f).
ii) $f^{-1}(1_{G'}) \leq G$ (we denote

$$Ker(f) = f^{-1}(1_{G'})$$

and call it the kernel of f).
iii) If $H \leq G$, then $f(H) \leq G'$.
iv) If $H' \leq G'$, then $f^{-1}(H') \leq G$.
v) f is surjective $\Leftrightarrow Im(f) = G'$.
vi) f is injective $\Leftrightarrow Ker(f) = \{1_G\}$.
Solution: i) $1_{G'} = f(1_G) \in f(G)$, and if $x', y' \in f(G)$, then $x' = f(x)$ and $y' = f(y)$, so $x'^{-1}y' = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y) \in f(G)$.
ii) $1_G \in f^{-1}(1_{G'})$, and if $x, y \in f^{-1}(1_{G'})$, then $f(x^{-1}y) = f(x)^{-1}f(y) =$

$= 1_{G'}$.
iii) $1_{G'} = f(1_G) \in f(H)$, and if $x', y' \in f(H)$, then $x' = f(x)$ and $y' = f(y)$ for some $x, y \in H$, so $x^{-1}y \in H$ and $x'^{-1}y' = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y) \in f(H)$.
iv) $1_G \in f^{-1}(H')$, and if $x, y \in f^{-1}(H')$, then $f(x), f(y) \in H'$, and $f(x^{-1}y) = f(x)^{-1}f(y) = H'$.
v) is obvious.
vi) Assume that f is injective, and let $x \in Ker(f)$. Then $f(x) = f(1_G) = 1_{G'}$, so $x = 1_G$. Conversely, we assume now that $Ker(f) = \{1_G\}$ and we prove that f is injective. Let $x, y \in G$ such that $f(x) = f(y)$. Then $f(x)f(y)^{-1} = 1_{G'}$, so $f(xy^{-1}) = 1_{G'}$, i.e. $xy^{-1} \in Ker(f) = \{1_G\}$. Therefore $xy^{-1} = 1_G$, so $x = y$.

Exercise 1.5.13 *Which of the following subsets are normal subgroups:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iii) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
iv) $\{Id, (12)\} \subseteq S_3$.
v) $\{Id, (123), (132)\} \subseteq S_3$.
vi) $O(2) = \{A \in GL_2(\mathbb{R}) \mid A^{-1} = A^t\} \subseteq GL_2(\mathbb{R})$ *(see Exercise 1.4.5, xx)).*
vii) $SO(2) = \{A \in O(2) \mid det(A) = 1\} \subseteq O(2)$
viii) $\{1, -1, i, -i\} \subseteq Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$*, the quaternion group, see Exercise 1.4.5, xxvi).*
Solution: i), ii), iii). The subsets are subgroups of abelian groups by Exercise 1.5.6, so they are normal subgroups.
iv) No, because $(13)(12)(13) = (23) \notin \{Id, (12)\}$.
v) $\{Id, (123), (132)\} \trianglelefteq S_3$, because we can check that

$$(12)(123)(12) = (13)(123)(13) = (23)(123)(23) = (132)$$

and

$$(12)(132)(12) = (13)(132)(13) = (23)(132)(23) = (123).$$

vi) No, because

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix} \notin O(2)$$

vii) The map $\varphi : O(2) \longrightarrow \{1, -1\}$ defined by $\varphi(A) = det(A)$ is a group morphism, and $Ker(\varphi) = SO(2)$, so $SO(2) \trianglelefteq O(2)$.
viii) $\{1, -1, i, -i\} \trianglelefteq Q_8$. Since $x \in \{1, -1, i, -i\} \Rightarrow -x \in \{1, -1, i, -i\}$, we only need to check that $ii(-i) = i \in \{1, -1, i, -i\}$, $ji(-j) = -i \in \{1, -1, i, -i\}$, and $ki(-k) = -i \in \{1, -1, i, -i\}$, so $\{1, -1, i, -i\} \trianglelefteq Q_8$.

Exercise 1.5.15 *Give an example to show that the assertion in Proposition 1.5.14 ii) is not true if f is not surjective.*
Solution: Let $i : \{Id, (12)\} \longrightarrow S_3$ denote the inclusion. Then i is a group morphism because $\{Id, (12)\} \leq S_3$, $\{Id, (12)\} \trianglelefteq \{Id, (12)\}$, but $\{Id, (12)\}$ is not normal in S_3 by Exercise 1.5.13 iv).

Exercise 1.5.17 *Show that any subgroup of $\mathbb{Z}_n$ is generated by an element $\hat{d}$, where $d \mid n$.*
Solution: The map $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $f(a) = \hat{a}$ is a surjective group morphism, so by Corollary 1.5.16 there exists a bijective correspondence between the subgroups of $\mathbb{Z}_n$ and the subgroups of $\mathbb{Z}$ that contain $Ker(f) = n\mathbb{Z}$. Now $a\mathbb{Z} \subseteq b\mathbb{Z} \Leftrightarrow a \in b\mathbb{Z} \Leftrightarrow b \mid a$. Therefore, a subgroup of $\mathbb{Z}_n$ is $f(d\mathbb{Z})$ for some $d \mid n$.

1.6 Factor groups

Let G be a group and $H \leq G$. We define two relations on G:

$$x \equiv_l y \ (mod\ H) \Longleftrightarrow x^{-1}y \in H,$$

and

$$x \equiv_r y \ (mod\ H) \Longleftrightarrow xy^{-1} \in H.$$

Proposition 1.6.1 *$\equiv_l \ (mod\ H)$ is an equivalence relation on G.*

Proof: If $x \in G$, then $x^{-1}x = 1_G \in H$, so the relation is reflexive. If $x^{-1}y \in H$, then $(x^{-1}y)^{-1} = y^{-1}x \in H$, so the relation is symmetric. Now if $x^{-1}y \in H$ and $y^{-1}z \in H$, then $x^{-1}z = x^{-1}yy^{-1}z \in H$, so the relation is transitive. ∎

Exercise 1.6.2 *$\equiv_r \ (mod\ H)$ is an equivalence relation on G.*

Proposition 1.6.3 *Let G be a group, $H \leq G$ and $x \in G$. Denote by $\hat{x}$ the equivalence class of x with respect to the equivalence relation $\equiv_l \ (mod\ H)$. Then $\hat{x} = xH = \{xh \mid h \in H\}$. We will call xH the* left coset *of x relative to H.*

Proof: We have that

$$\begin{aligned} \hat{x} &= \{y \in G \mid x \equiv_l y \ (mod\ H)\} \\ &= \{y \in G \mid x^{-1}y \in H\} \\ &= \{y \in G \mid x^{-1}y = h,\ h \in H\} \\ &= \{y \in G \mid y = xh,\ h \in H\} \\ &= \{xh \in G \mid h \in H\} = xH. \end{aligned}$$

∎

Exercise 1.6.4 *Let G be a group, $H \leq G$ and $x \in G$. Denote by $\hat{x}$ the equivalence class of x with respect to the equivalence relation $\equiv_r \ (mod\ H)$. Then $\hat{x} = Hx = \{hx \mid h \in H\}$. We will call Hx the* right coset *of x relative to H.*

Proposition 1.6.5 *The map*

$$\varphi : G/\equiv_l (mod\ H) \longrightarrow G/\equiv_r (mod\ H),$$

defined by $\varphi(xH) = Hx^{-1}$, is a bijection.

Proof: We first need to show that φ is well defined. Indeed, if $xH = yH$, then $x^{-1}y \in H$, so $(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} \in H$, and hence $Hy^{-1} = Hx^{-1}$. Now define $\psi : G/\equiv_r (mod\ H) \longrightarrow G/\equiv_l (mod\ H)$ by $\psi(Hx) = x^{-1}H$. The fact that ψ is well defined is checked as above. It is clear that $\varphi(\psi(Hx)) = Hx$ and $\psi(\varphi(xH)) = xH$ for all $x \in G$, so φ and ψ are bijections inverse to each other. ∎

We will now see why the notion of normal subgroup is so important.

Theorem 1.6.6 *Let G be a group and $H \leq G$. The following assertions are equivalent:*
i) H is a normal subgroup.
ii) The two equivalence relations defined by H coincide: for $x, y \in G$ we have

$$x \equiv_l y\ (mod\, H) \Longleftrightarrow x \equiv_r y\ (mod\, H).$$

Proof: i) ⇒ ii). Assume that $H \trianglelefteq G$ and $x^{-1}y \in H$. Then $x(x^{-1}y)x^{-1} \in H$, so $yx^{-1} \in H$, and therefore $xy^{-1} \in H$. The fact that $xy^{-1} \in H \Rightarrow x^{-1}y \in H$ is proved similarly.
ii) ⇒ i). Let $x \in G$ and $h \in H$. We want to prove that $xhx^{-1} \in H$. We know that $xH = Hx$, so $xh = h_1x$ for some $h_1 \in H$. It follows that $xhx^{-1} = h_1xx^{-1} = h_1 \in H$, and the proof is complete. ∎

If $H \trianglelefteq G$ it follows from Theorem 1.6.6 that the factor sets with respect to the two identical equivalence relations defined by H coincide. Our notation for this factor set will be G/H.
Recall from Exercise 1.3.3 v) that a function f defined on a set M also defines an equivalence relation $\mathcal{R}_f$ on M. We now consider the analog situation for groups.

Proposition 1.6.7 *Let $f : G \longrightarrow G'$ be a morphism of groups. Then $\mathcal{R}_f$ coincides with the equivalence relation defined by the normal subgroup $Ker(f)$ on G.*

Proof: For $x, y \in G$, we have that $x\mathcal{R}_f y$ if and only if $f(x) = f(y)$ if and only if $f(x)f(y)^{-1} = 1_{G'}$ if and only if $f(x)f(y^{-1}) = 1_{G'}$ if and only if $f(xy^{-1}) = 1_{G'}$ if and only if $xy^{-1} \in Ker(f)$. ∎

Proposition 1.6.8 *If $H \trianglelefteq G$, G/H is a group, and the canonical surjection from G to G/H is a group morphism.*

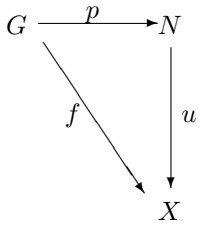
Proof: We have that $can : G \longrightarrow G/H$ sends $x \in G$ to $Hx = xH$. We define the operation on G/H by $(xH)(yH) = (xy)H$. We check that the operation is well defined. Let $x'H = xH$ and $y'H = yH$. Then $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}h_1y' = y^{-1}y'h_2$ for some $h_1, h_2 \in H$.

Therefore $(xy)^{-1}(x'y') \in H$, and so $(xy)H = (x'y')H$.
It is easy to see that G/H is a group with this operation, and the definition ensures that *can* is a morphism of groups. Note that the inverse of xH in G/H is $x^{-1}H$, and $1_{G/H} = H$. ∎

Definition 1.6.9 *The group G/H defined in Proposition 1.6.8 is called the* factor group *of the group G relative to the normal subgroup H.*

As in the case of factor sets, we can define the factor group without any reference to elements: we will say that a factor group of the group G is a pair (N, p), where N is a group and $p : G \longrightarrow N$ is a surjective group morphism. Again as in the case of sets, it turns out that the two definitions are equivalent. One implication follows from Proposition 1.6.7. The other one follows from a result similar to Theorem 1.3.15:

Theorem 1.6.10 (The Universal Property of the Factor Group) *Let (N, p) be a factor group of the group G, let X be a group and $f : G \longrightarrow X$ a group morphism.*
i) There exists a group morphism $u : N \longrightarrow X$ such that $f = up$, which means that the diagram



is commutative, if and only if $Ker(p) \subseteq Ker(f)$. If u exists, then it is unique.
If u as in i) exists, then:
ii) u is surjective if and only if f is surjective.
iii) u is injective if and only if $Ker(p) = Ker(f)$.

Proof: Using Theorem 1.3.15 and Proposition 1.6.7 we see that the only thing left to prove is that if a function u as in the statement exists, then it is a group morphism. Let $x', y' \in N$, and $x, y \in G$ such that $p(x) = x'$ and $p(y) = y'$. Then $u(x'y') = u(p(x)p(y)) = u(p(xy)) = f(xy) = f(x)f(y) = u(p(x))u(p(y)) = u(x')u(y')$. ∎

Corollary 1.6.11 *If (N_1, p_1) and (N_2, p_2) are two factor groups of G such that $Ker(p_1) = Ker(p_2)$, then there exists an isomorphism $u : N_1 \longrightarrow N_2$ such that $up_1 = p_2$.*

Proof: Take $(N,p)=(N_1,p_1)$, $X=N_2$ and $f=p_2$ in Theorem 1.6.10. ∎

Corollary 1.6.12 *If (N,p) is a factor group of G, then there exists an isomorphism $u:N\longrightarrow G/Ker(p)$ such that $u\circ p$ is the canonical surjection.*

Proof: Take $(N_1,p_1)=(N,p)$ and $(N_2,p_2)=(G/Ker(p),can)$, where $can:G\longrightarrow G/Ker(p)$, $can(x)=xKer(p)$. Then $Ker(can)=Ker(p)$ and we can apply Corollary 1.6.11. ∎

Corollary 1.6.13 (The First Isomorphism Theorem for Groups) *Let $f:G\longrightarrow G'$ be a group morphism. Then*

$$G/Ker(f)\simeq Im(f).$$

Proof: Use Corollary 1.6.12 for $(Im(f),f)$. ∎

Corollary 1.6.14 (The Second Isomorphism Theorem for Groups) *Let $H,K\leq G$ be such that H is a normal subgroup of HK, the subgroup of G generated by H and K. Then $H\cap K$ is a normal subgroup of K, and*

$$K/H\cap K\simeq HK/H.$$

Proof: Define $f:K\longrightarrow HK/H$ to be the composition of the inclusion $i:K\subseteq HK$ with the canonical surjection $can:HK\longrightarrow HK/H$, $f=can\circ i$. We have that f is surjective, because for any element $\alpha\in HK/H$ we have that $\alpha=can(x_1y_1x_2y_2\dots x_ny_n)$, where $x_i\in H$ and $y_i\in K$. But then $\alpha=can(x_1)can(y_1)can(x_2)can(y_2)\dots can(x_n)can(y_n)=can(y_1)can(y_2)\dots can(y_n)=can(y_1y_2\dots y_n)$, because $can(x_i)=H$. If we prove that $Ker(f)=H\cap K$ the assertion will follow from Corollary 1.6.13. It is clear that $H\cap K\subseteq Kerf(f)$. Let now $y\in Ker(f)$. It follows that $y\in K$ and $can(y)=H$, so $y\in H$. Therefore $y\in H\cap K$ and the proof is complete. ∎

Corollary 1.6.15 (The Third Isomorphism Theorem for Groups) *Let G be a group and $H\leq N$ two normal subgroups of G. Then*

$$(G/H)/(N/H)\simeq G/N.$$

Proof: Define $f:G/H\longrightarrow G/N$ by $f(xH)=xN$. We have that f is well defined, because if $x^{-1}y\in H$ it follows that $x^{-1}y\in N$, since $H\subseteq N$. It is clear that f is surjective and $Ker(f)=N/H$, so the result follows from Corollary 1.6.13. ∎

Exercise 1.6.16 *Any cyclic group is isomorphic to a $\mathbb{Z}_n$.*

Exercise 1.6.17 *Prove the following isomorphisms:*
i) $\mathbb{Z}_8/\{0,4\} \simeq \mathbb{Z}_4$.
ii) $S_3/\{Id,(123),(132)\} \simeq \mathbb{Z}_2$.
iii) $Q_8/\{1,-1,i,-i\} \simeq \mathbb{Z}_2$, *where* $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ *is the quaternion group from Exercise 1.4.5, xxvi).*
iv) $Q_8/\{1,-1\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, *where* $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ *is the quaternion group from Exercise 1.4.5, xxvi).*

We end this section by mentioning another way of introducing factor groups. Instead of starting with a group G and a normal subgroup of G, we start with an equivalence relation $\mathcal{R}$ on the set G which is compatible with the group operation, i.e. we can multiply relations: if $x_1\mathcal{R}y_1$ and $x_2\mathcal{R}y_2$, then $x_1y_1\mathcal{R}x_2y_2$. The fact that then the factor set $G/\mathcal{R}$ becomes a group such that the canonical surjection is a group morphism follows from the fact that $x\mathcal{R}y$ if and only if x and y are congruent modulo the normal subgroup $C_1 = \{h \in G \mid h\mathcal{R}1\}$.

Solutions to the Exercises on Section 1.6

Exercise 1.6.2 $\equiv_r \ (mod\ H)$ *is an equivalence relation on* G.
Solution: If $x \in G$, then $xx^{-1} = 1_G \in H$, so the relation is reflexive. If $xy^{-1} \in H$, then $(xy^{-1})^{-1} = yx^{-1} \in H$, so the relation is symmetric. Now if $xy^{-1} \in H$ and $yz^{-1} \in H$, then $xz^{-1} = xy^{-1}yz^{-1} \in H$, so the relation is transitive.

Exercise 1.6.4 *Let* G *be a group,* $H \leq G$ *and* $x \in G$. *Denote by* $\hat{x}$ *the equivalence class of* x *with respect to the equivalence relation* $\equiv_r \ (mod\ H)$. *Then* $\hat{x} = Hx = \{hx \mid h \in H\}$. *We will call* Hx *the* right coset *of* x *relative to* H.
Solution: We have that

$$\begin{aligned} \hat{x} &= \{y \in G \mid y \equiv_r x\ (mod\ H)\} \\ &= \{y \in G \mid yx^{-1} \in H\} \\ &= \{y \in G \mid yx^{-1} = h,\ h \in H\} \\ &= \{y \in G \mid y = hx,\ h \in H\} \\ &= \{hx \in G \mid h \in H\} = Hx. \end{aligned}$$

Exercise 1.6.16 *Any cyclic group is isomorphic to a* $\mathbb{Z}_n$.
Solution: If G is cyclic, then

$$G =< a >= \{a^k \mid k \in \mathbb{Z}\},$$

and it is easy to check that the function

$$f : \mathbb{Z} \longrightarrow G, \ \ f(k) = a^k,$$

is a surjective group morphism. Consequently, $G \simeq \mathbb{Z}/Ker(f)$ by Corollary 1.6.13.

Exercise 1.6.17 *Prove the following isomorphisms:*
i) $\mathbb{Z}_8/\{0,4\} \simeq \mathbb{Z}_4$.
ii) $S_3/\{Id, (123), (132)\} \simeq \mathbb{Z}_2$.
iii) $Q_8/\{1,-1,i,-i\} \simeq \mathbb{Z}_2$, *where* $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ *is the quaternion group from Exercise 1.4.5, xxvi).*
iv) $Q_8/\{1,-1\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, *where* $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ *is the quaternion group from Exercise 1.4.5, xxvi).*
Solution: i) Define $f : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_4$ by $f(0) = f(4) = 0$, $f(1) = f(5) = 1$, $f(2) = f(6) = 2$, and $f(3) = f(7) = 3$. Then f is a surjective group morphism, and $Ker(f) = \{0,4\}$, so we can apply Corollary 1.6.13.
ii) Define $f : S_3 \longrightarrow \mathbb{Z}_2$ by $f((12)) = f((13)) = f((23)) = 1$, and $f(Id) =$

$f((123)) = f((132)) = 0$. Then f is a surjective group morphism, and $Ker(f) = \{Id, (123), (132)\}$, hence we can apply Corollary 1.6.13.
iii) Define $f : Q_8 \longrightarrow \mathbb{Z}_2$ by $f(1) = f(-1) = f(i) = f(-i) = 0$ and $f(j) = f(-j) = f(k) = f(-k) = 1$. Then f is a surjective group morphism, and $Ker(f) = \{1, -1, i, -i\}$, thus we can apply Corollary 1.6.13.
iv) Define $f : Q_8 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ by $f(1) = f(-1) = (0, 0)$, $f(i) = f(-i) = (1, 0)$, $f(j) = f(-j) = (0, 1)$, and $f(k) = f(-k) = (1, 1)$. Then f is a surjective group morphism, and $Ker(f) = \{1, -1\}$, so we can apply Corollary 1.6.13.

1.7 Finite groups and the Lagrange theorem

A finite group is a group G such that the set G is finite.

Definition 1.7.1 *Let G be a group. The* order *of the group G, if G is finite, is equal to the number of elements of G. If G has n elements, we will write $|G| = n$. If G is infinite we say that G has infinite order, and we write $|G| = \infty$.*

We saw in Proposition 1.6.5 that the set of left cosets of a group relative to a subgroup is in a bijection with the set of right cosets. This allows us to give the following:

Definition 1.7.2 *Let G be a group, and $H \leq G$. The* index *of H in G, is equal to the number of left (or right) cosets of G relative to H, if there are finitely many such cosets. If there are n cosets, we will write $|G : H| = n$. If there are infinitely many cosets we say that H has infinite index in G, and we write $|G : H| = \infty$. Note that if $H \trianglelefteq G$, then the order of the factor group G/H coincides with the index of H in G: $|G/H| = |G : H|$.*

It is clear that any subgroup of a finite group is finite and has finite index. An infinite group can have finite subgroups ($\{1, -1\} \leq (0, \infty)$), or subgroups of finite index ($|\mathbb{Z} : n\mathbb{Z}| = n$ if $n > 0$).

Exercise 1.7.3 *A subgroup of index two is normal.*

Theorem 1.7.4 *Let G be a finite group, and $H \leq G$. Then*

$$|G| = |H|\,|G : H|\,.$$

Proof: G is equal to the union of the left cosets relative to H, and the cosets are disjoint, so the order of G is equal to the sum of elements of the left cosets. In each left coset xH there are $|H|$ elements, because the function $\varphi : H \longrightarrow xH$, $\varphi(h) = hx$ is bijective (it is clearly surjective, and it is also injective by the cancelation law). On the other hand, there are exactly $|G : H|$ cosets, so the result follows. ∎

Corollary 1.7.5 *The order of a subgroup of a finite group divides the order of the group.*

Definition 1.7.6 *Let G be a group and $a \in G$. The* order *of a is the order of $< a >$, the cyclic subgroup generated by a (recall that $< a >= \{a^k \mid k \in \mathbb{Z}\}$). We write $|a| = |< a >|$.*

Exercise 1.7.7 *Let G be a finite group and $a \in G$. Then:*
i) the order of a divides the order of G.
ii) $|a| = 1$ if and only if $a = 1_G$.
iii) $|a| = \left|a^{-1}\right|$.

Exercise 1.7.8 *Find the orders of all the elements of the group:*
i) $\mathbb{Z}_4$.
ii) $\mathbb{Z}_2 \times \mathbb{Z}_2$.
iii) $\mathbb{Z}_6$.
iv) S_3.
v) The quaternion group Q_8.

Proposition 1.7.9 *Let $a \in G$, $|a| = n$. Then n is the smallest element of the set $\{m \in \mathbb{N} \mid a^m = 1_G\}$.*

Proof: Since $|a| = n$, it follows that $< a >= \{1_G, a, a^2, \ldots, a^{n-1}\}$ has n elements, i.e. the elements $1_G, a, a^2, \ldots, a^{n-1}$ are distinct, so in particular $a^k \neq 1_G$ if $0 < k < n$. Since we know that $a^n \in < a >$, it follows that $a^n = 1_G$, and the assertion is proved. ∎

Exercise 1.7.10 *Let $a \in G$, $|a| = n$. If $a^m = 1_G$, then $n \mid m$.*

Exercise 1.7.11 *If $|G| = n$ and $a \in G$, then $a^n = 1_G$.*

Exercise 1.7.12 *Any group of prime order is cyclic.*

Proposition 1.7.13 *A group of order 6 is isomorphic to $\mathbb{Z}_6$ or S_3.*

Proof: If G is cyclic, then G is isomorphic to $\mathbb{Z}_6$. If G is not cyclic, there are no elements of order 6, so all elements different from 1_G have order 2 or 3. If all elements have order 2, and we pick two such elements, x and y, then xy also has order 2, so $xyxy = 1_G$, and multiplying this equality by x on the left and y on the right we get $yx = xy$. It follows that $\{1_G, x, y, xy\} \leq G$, so by the Lagrange theorem $4 \mid 6$, a contradiction. It follows that there exists an element $\theta \in G$ of order 3. Then $H = \{1_G, \theta, \theta^2\}$ has index 2, so it is normal. We prove that any element z in the complement of H has order 2. Indeed, $z^2 \in H$ (G/H has order 2), and if $z^2 = \theta$ or $z^2 = \theta^2$ we get that the order of z is 3 or 6. Since G is not cyclic, the order cannot be 6. If the order is 3 and $z^2 = \theta^2$, then $\theta^2 z = 1_G$, so $z = \theta$, a contradiction. Similarly, if $z^2 = \theta$ we get $z = \theta^2$, a contradiction. In conclusion, the order of z is 2. Let now $\tau \in G$, $\tau \notin H$. Then we know that the elements $\tau, \tau\theta, \tau\theta^2$ are distinct and not in H, so they all have order 2 and $G = \{1_G, \theta, \theta^2, \tau, \tau\theta, \tau\theta^2\}$. We have $\theta\tau = (\theta^2)^{-1}\tau^{-1} = (\tau\theta^2)^{-1} = \tau\theta^2$, and $\theta^2\tau = \theta^{-1}\tau^{-1} = (\tau\theta)^{-1} = \tau\theta$, and we can check that the group morphism $\varphi : S_3 \longrightarrow G$, $\varphi((12)) = \tau$ and $\varphi((123)) = \theta$ is an isomorphism. ∎

Exercise 1.7.14 *Prove that a group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

We now recall the definition of a least common multiple of two integers. (Note that the definition can be extended to any number of integers.)

Definition 1.7.15 *If a and b are integers, we say that m is a least common multiple of a and b (and we write $m = [a, b]$) if the following conditions hold:*
i) $a \mid m$ and $b \mid m$.
ii) If $a \mid n$ and $b \mid n$, then $m \mid n$.

Exercise 1.7.16 *If a and b are integers, then $ab = (a, b)[a, b]$ (this means that if not both of a and b are 0, then $[a, b] = ab/(a, b)$.)*

Proposition 1.7.17 *Let $a, b \in G$, $|a| = m$, $|b| = n$, and $ab = ba$. Then*
i) if $1 = (m, n)$, then $|ab| = mn$.
ii) is it true that $|ab| = [m, n]$?

Proof: i) Let $k = |ab|$. It is clear that $(ab)^{mn} = a^{mn}b^{mn} = 1_G$, so $k \mid mn$ by Exercise 1.7.10. Now since $(ab)^k = a^k b^k = 1_G$, then $(ab)^{nk} = a^{nk}b^{nk} = a^{nk} = 1_G$. Then by Exercise 1.7.10 we get that $m \mid nk$, and since $1 = (m, n)$ we have $m \mid k$ by Euclid's lemma. Similarly, $n \mid k$, and hence $mn = [m, n] \mid k$, so $mn = k$.
ii) Take $|a| = m > 1$, and $b = a^{-1}$. By Exercise 1.7.7 iii), $|b| = m$. Then $ab = ba = 1_G$ has order $1 \neq [m, m] = m$, so the answer is no. ∎

Exercise 1.7.18 *Give an example to show that the conclusion of Proposition 1.7.17 i) is not true if $ab \neq ba$.*

Exercise 1.7.19 *Show that:*
i) $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm} \Leftrightarrow 1 = (m, n)$.
ii) $n\mathbb{Z} \cap m\mathbb{Z} = [m, n]\mathbb{Z}$.
iii) $n\mathbb{Z} + m\mathbb{Z} = (m, n)\mathbb{Z}$.

Exercise 1.7.20 *Let $(a_1 a_2 \dots a_k) \in S_n$ be a cycle of length k. Show that $|(a_1 a_2 \dots a_k)| = k$.*

Exercise 1.7.20 provides a quick way to find the order of a permutation in S_n. We first write the permutation as a product of disjoint cycles, then, since disjoint cycles commute, we find the order of the permutation as the least common multiple of the lengths of those cycles.

Exercise 1.7.21 *Find the order of*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 5 & 8 & 1 & 2 & 10 & 7 & 9 & 4 \end{pmatrix} \in S_{10}.$$

We now define the signature of a permutation. For any $\sigma \in S_n$, define

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

If $\sigma, \tau \in S_n$ we have

$$\varepsilon(\sigma\tau) = \prod_{1 \leq i < j \leq n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} =$$

$$= \prod_{1 \leq i < j \leq n} \frac{\tau(i) - \tau(j)}{i - j} \cdot \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \varepsilon(\sigma)\varepsilon(\tau).$$

Therefore

$$\varepsilon : S_n \longrightarrow \{1, -1\}$$

is a group morphism. This morphism is surjective, the identity is sent to one, and any transposition is sent to -1. The permutations in the kernel of this morphism (denoted by A_n and called the *alternating group*) are called *even*, and the other ones are called *odd*. To see why they are called even and odd, consider a cycle in S_n of length k, and write it as a product of transpositions like this:

$$(i_1 i_2 \dots i_k) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2).$$

Therefore any even (odd) permutation can be written as a product of an even (odd) number of transpositions. In particular, a cycle is even if and only if it has odd length.

The next important result is Cayley's theorem. It says that any group is isomorphic to a permutation group (i.e. a subgroup of a symmetric group $S(M)$, see Exercise 1.4.5, xviii)), and we leave the proof as an exercise.

Exercise 1.7.22 *Let G be a group. Prove that the map $\varphi : G \longrightarrow S(G)$ sending $x \in G$ to $\varphi(x) : G \longrightarrow G$, $\varphi(x)(g) = xg$ is an injective morphism of groups.*

Historically, the first studied groups were groups of permutations (of solutions of polynomial equations). Groups also arise naturally as symmetries of various geometric objects. The group of symmetries of a plane figure consist of all the transformations applied to a cutout of that figure after we take it out of a board before putting it back in the hole. It is clear that the options that we have before putting the cutout back are rotations, or flips, or combinations of these. We call these transformations symmetries, and the operation is composition. Let us look at a few examples.

We start with the symmetries of a rectangle. Once we cut the rectangle from a board and we take it out, we have the following options before we put it back in: do nothing, just put it back, we denote this by I. Rotate the rectangle by π (left or right, it's the same transformation), we denote this by R. Flip it upside down, we denote this by F. Twist it left to right or right to left, we call this T. Combining all these gives the following table for this group

$$\begin{array}{cccccc} \circ & I & R & F & T \\ I & I & R & F & T \\ R & R & I & T & F \\ F & F & T & I & R \\ T & T & F & R & I \end{array}$$

This group is called the Klein Four Group, is usually denoted by V_4 and is easily seen to be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Something really ineresting happens if we repeat the experiment with the rectangle, but this time attach a ribbon to the center of the rectangle and hold the other end, without twisting it. If we just take out the rectangle and put it back in without doing anything, we get 1, as before. However, if we rotate the rectangle by 2π before putting it back in, we get a new transformation, denoted by -1, in which the rectangle is exactly as in the initial position, but the ribbon has a full twist. The surprising thing is that it does not matter if the twist is on the left or on the right (we are allowed to move the rectangle and the end of the ribbon as long as we don't twist them). This is the famous Dirac belt trick, or the Balinese candle-dance trick (look them up in YouTube), which says that two twists in the ribbon are the same as no twist. In order to convince ourselves that this is true, put two twists (4π) in the ribbon, move your hand holding the ribbon closer to the rectangle (without twisting) until a loop is formed, then ask a friend to grab the rectangle and move it through the loop (again, without twisting). Now pull your hand holding the ribbon away and watch the twists disappear (if you look at the ribbon before pulling you will get a better uderstanding of the Balinese candle-dance trick). Now let's check that a left twist is the same as a right twist. Start with a left twist, then add (temporarily) another left twist. Perform the Dirac belt trick to make all twists disappear. Finally, we need to undo the left twist that we put in, and this is done by performing a right twist. Now let's see what other transformations we can get. Rotating the rectangle by π clockwise adds half a twist to the ribbon with the right side of the ribbon up. We denote this by i. Rotating the rectangle by π counterclockwise adds half a twist to the ribbon with the left side of the ribbon up. We denote this by $-i$. Flipping the rectangle such that the ribbon is on top is denoted by j, and flipping it such that the ribbon is on the bottom is denoted by $-j$. Finally,

twisting the rectangle to the right puts a half twist on the ribbon (right side up), and we denote this by k, while twisting the rectangle to the left puts a half twist on the ribbon (left side up), and we denote this by $-k$. As you have probably guessed the group of symmetries of this "tethered" rectangle is the quaternion group Q_8 (see Exercise 1.4.5, xxvi)). We just check that composition by -1 is what it should be. For example, adding a full left twist to a left half twist is equivalent to a right half twist. To see this, add a temporary left half twist to get two twists, make the twists disappear, then undo the left half twist by adding a right half twist.

We find now the group of symmetries of an equilateral triangle, which is called the dihedral group D_3. If we denote by 1 the identity transformation (does nothing), by θ the counterclockwise rotation of $\frac{2\pi}{3}$ about the center of the triangle, and by τ the flip along one of the heights of the triangle, then we can check that

$$D_3 = \{1, \theta, \theta^2, \tau, \theta\tau, \theta^2\tau\},$$

$\theta^3 = \tau^2 = 1$, $\tau\theta = \theta^2\tau$, so $D_3 \simeq S_3$ as in the proof of Proposition 1.7.13. Another way to see this is to mark the vertices of the cutout and the vertices of the hole by $\cdot$, $\cdot\cdot$, and $\cdots$ (we use these rather than 1, 2, and 3 so that they can be read from the other side as well), and note that the transformations of the triangle correspond in fact to the permutations of the vertices.

The group of transformations of a square, which is called the dihedral group D_4, is obtained as follows: we denote by θ the counterclockwise rotation of $\frac{\pi}{2}$ about the center of the square, and by τ the flip along one of the perpendiculars from the center to one of the sides, then we can check that

$$D_4 = \{1, \theta, \theta^2, \theta^3, \tau, \theta\tau, \theta^2\tau, \theta^3\tau\},$$

$\theta^4 = \tau^2 = 1$, $\tau\theta = \theta^3\tau$.

The group of transformations of a regular polygon with n sides, which is called the dihedral group D_n, is obtained as follows: we denote by θ the counterclockwise rotation of $\frac{2\pi}{n}$ about the center of the polygon, and by τ the flip along one of the perpendiculars from the center to one of the sides, then we can check that

$$D_n = \{1, \theta, \theta^2, \ldots, \theta^{n-1}, \tau, \theta\tau, \theta^2\tau, \ldots, \theta^{n-1}\tau\},$$

$\theta^n = \tau^2 = 1$, $\tau\theta = \theta^{n-1}\tau$.

Solutions to the Exercises on Section 1.7

Exercise 1.7.3 *A subgroup of index two is normal.*
Solution: Let $H \leq G$, $|G : H| = 2$. The left cosets of G relative to H are H and xH for some $x \in G$, while the right cosets are H and Hx. But $Hx = xH = G \setminus H$, so $H \trianglelefteq G$.

Exercise 1.7.7 *Let G be a finite group and $a \in G$. Then:*
i) the order of a divides the order of G.
ii) $|a| = 1$ if and only if $a = 1_G$.
iii) $|a| = \left|a^{-1}\right|$.
Solution: i) The order of a is the order of the subgroup generated by a, so the assertion follows from the Lagrange theorem.
ii) The subgroup generated by a is equal to $\{1_G\}$ if and only if $a = 1_G$.
iii) $a^k = 1_G \Leftrightarrow (a^{-1})^k = 1_G$.

Exercise 1.7.8 *Find the orders of all the elements of the group:*
i) $\mathbb{Z}_4$.
ii) $\mathbb{Z}_2 \times \mathbb{Z}_2$.
iii) $\mathbb{Z}_6$.
iv) S_3.
v) The quaternion group Q_8.
Solution: The order of the identity element in a group is 1, so we will ignore the identity element in all cases.
i) The order of 1 and 3 is 4, and the order of 2 is 2.
ii) All elements different from $(0, 0)$ have order 2.
iii) The order of 1 and 5 is 6, the order of 2 and 4 is 3, and the order of 3 is 2.
iv) The order of $(12), (13)$, and (23) is 2, and the order of (123) and (132) is 3.
v) The order of -1 is 2, and the order of $i, -i, j, -j, k$, and $-k$ is 4.

Exercise 1.7.10 *Let $a \in G$, $|a| = n$. If $a^m = 1_G$, then $n \mid m$.*
Solution: By the division algorithm we have $m = qn+r$, where $0 \leq r < n$. If $r \neq 0$, then $a^m = a^{nq+r} = (a^n)^q a^r = a^r = 1_G$, and this contradicts Proposition 1.7.9. In conclusion $r = 0$, or $n \mid m$.

Exercise 1.7.11 *If $|G| = n$ and $a \in G$, then $a^n = 1_G$.*
Solution: Since G is finite, the order of a is also finite, and by Exercise 1.7.7 i), $n = k\,|a|$. Then $a^n = (a^{|a|})^k = 1_G^k = 1_G$.

Exercise 1.7.12 *Any group of prime order is cyclic.*
Solution: Let $a \in G$, $a \neq 1_G$. Then $|a| \neq 1$ and it divides the order of G.

Since the order of G is prime, it follows that $|a| = |G|$, or $< a >= G$.

Exercise 1.7.14 *Prove that a group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*
Solution: Let G be a group of order 4. If there exists an element of order 4, then the group is cyclic, hence isomorphic to $\mathbb{Z}_4$. If there are no elements of order 4, then all elements different from 1_G have order 2. Let x, y be two distinct such elements. Then the elements $1_G, x, y, xy$ are distinct, and hence $G = \{1_G, x, y, xy\}$. Then the map $f : G \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$, defined by $f(1_G) = (0,0)$, $f(x) = (1,0)$, $f(y) = (0,1)$, and $f(xy) = (1,1)$ is an isomorphism.

Exercise 1.7.16 *If a and b are integers, then $ab = (a,b)[a,b]$ (this means that if not both of a and b are 0, then $[a,b] = ab/(a,b)$.)*
Solution: It is clear that $[0,0] = (0,0) = 0$. Now if a and b are not both 0, let $d = (a,b)$. We have that $d \mid a \mid ab$, so $ab = md$. We show that $m = [a,b]$. We have that $a = da_1$ and $b = db_1$. Therefore, $da_1db_1 = md$, hence $a_1db_1 = a_1b = ab_1 = m$, i.e. m is a multiple of a and b. Now if $a \mid n$ and $b \mid n$, it follows that $n = aa_2$ and $n = bb_2$, so $na_1 = ba_1b_2 = mb_2$, and $nb_1 = ab_1a_2 = ma_2$. Let u, v be such that $1 = ua_1 + vb_1$. Then $n = n(ua_1 + vb_1) = umb_2 + vma_2 = m(ub_2 + va_2)$.

Exercise 1.7.18 *Give an example to show that the conclusion of Proposition 1.7.17 i) is not true if $ab \neq ba$.*
Solution: The order of (12) in S_3 is 2, and the order of (123) is 3, but the order of (12)(123) = (23) is 2.

Exercise 1.7.19 *Show that:*
i) $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm} \Leftrightarrow 1 = (m,n)$.
ii) $n\mathbb{Z} \cap m\mathbb{Z} = [m,n]\mathbb{Z}$.
iii) $n\mathbb{Z} + m\mathbb{Z} = (m,n)\mathbb{Z}$.
Solution: i) If $1 = (m,n)$, the order of $(1,0)$ is n, the order of $(0,1)$ is m, and $(1,0)$ and $(0,1)$ commute, so the order of $(1,1)$ is $[n,m] = nm$, i.e. $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic of order nm, hence isomorphic to $\mathbb{Z}_{nm}$. Conversely, if $1 \neq (m,n)$, then there is a least common multiple $k = [m,n]$ such that $0 < k < nm$. For any $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m$, we have $k(a,b) = (0,0)$, so there are no elements of order nm in $\mathbb{Z}_n \times \mathbb{Z}_m$.
The right to left implication is known as the **Chinese Remainder Theorem**, and is usually given in this form: if $1 = (m,n)$, then the system of two congruences $x \equiv a \pmod m$ and $x \equiv b \pmod n$ has a solution. A constructive proof of this statement goes like this: since $1 = (m,n)$ we have $1 = m(m^{-1})_{(mod\, n)} + n(n^{-1})_{(mod\, m)}$. A solution to the first congruence is of the form $mt + a$, and we find t by asking it to

also be a solution to the second congruence: $mt + a \equiv b \pmod{n}$, so $t = (m^{-1})_{(mod\ n)}(b-a)$, and a solution to the system will be congruent to $m(m^{-1})_{(mod\ n)}(b-a) + a \pmod{mn}$. Collecting terms in a and b and replacing $1 - m(m^{-1})_{(mod\ n)} = n(n^{-1})_{(mod\ m)}$ produces the more symmetric system solution $n(n^{-1})_{(mod\ m)}a + m(m^{-1})_{(mod\ n)}b \pmod{mn}$.
ii) Let $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$. We will show that $k = [m,n]$. Obviously $k\mathbb{Z} \subseteq n\mathbb{Z}$ and $k\mathbb{Z} \subseteq m\mathbb{Z}$, so $n \mid k$ and $m \mid k$. Now if $n \mid l$ and $m \mid l$, then $l\mathbb{Z} \subseteq n\mathbb{Z}$ and $l\mathbb{Z} \subseteq m\mathbb{Z}$, so $l\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$, so $k \mid l$.
iii) Let $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. We show that $d = (a,b)$. Since $n\mathbb{Z} \subseteq d\mathbb{Z}$ and $m\mathbb{Z} \subseteq d\mathbb{Z}$, it follows that $d \mid n$ and $d \mid m$. Now if $s \mid n$ and $s \mid m$, it follows that s divides any linear combination of n and m, in particular $s \mid d$.

Exercise 1.7.20 *Let $(a_1a_2\dots a_k) \in S_n$ be a cycle of length k. Show that $|(a_1a_2\dots a_k)| = k$.*
Solution: Let $\sigma = (a_1a_2\dots a_k)$. Then $\sigma^2(a_1) = a_3$, $\sigma^3(a_1) = a_4$, $\dots$ $\sigma^{k-1}(a_1) = a_k$, and $\sigma^k = Id$.

Exercise 1.7.21 *Find the order of*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 5 & 8 & 1 & 2 & 10 & 7 & 9 & 4 \end{pmatrix} \in S_{10}.$$

Solution: We have that $\sigma = (135)(26)(487\,10)$, so $|\sigma| = [3,2,4] = 12$.

Exercise 1.7.22 *Let G be a group. Prove that the map $\varphi : G \longrightarrow S(G)$ sending $x \in G$ to $\varphi(x) : G \longrightarrow G$, $\varphi(x)(g) = xg$ is an injective morphism of groups.*
Solution: First we have that $\varphi(xy)(g) = (xy)g = x(yg) = \varphi(x)(yg) = \varphi(x)(\varphi(y)(g)) = \varphi(x)\varphi(y)(g)$ for all $g \in G$, so $\varphi(xy) = \varphi(x)\varphi(y)$, i.e. φ is a group morphism. Now if $x \in Ker(\varphi)$, it follows that $\varphi(x) = Id_G$, in particular $\varphi(x)(1_G) = x1_G = 1_G$. Therefore $x = 1_G$, i.e. $Ker(\varphi) = \{1_G\}$, so φ is injective.

Chapter 2

Rings

2.1 Rings and morphisms of rings

In this section we continue the process started in Section 1.4: there we started with a set and considered an operation on that set. Now we are starting with a group and consider a second operation on it.

Definition 2.1.1 *A* ring *is a set R with at least two elements, 0_R and 1_R, and two operations, $+$ and $\cdot$, called* addition *and* multiplication*, such that the following conditions hold:*
i) $(R,+)$ is an abelian group with identity element 0_R.
ii) Multiplication is associative and has identity element 1_R. This means that for all $a,b,c \in R$ we have:

$$a(bc) = (ab)c \text{ and } a1_R = 1_R a = a.$$

iii) Multiplication is distributive with respect to addition, i.e. for all $a,b,c \in R$ we have:

$$a(b+c) = ab + ac \text{ and } (a+b)c = ac + bc.$$

If multiplication is commutative, we say that the ring is commutative.

Exercise 2.1.2 *Let $(R,+,\cdot)$ be a ring. Then the following hold:*
i) $a0_R = 0_R a = 0_R$ for all $a \in R$.
ii) Rule of signs: $a(-b) = (-a)b = -ab$, and $(-a)(-b) = ab$.
iii) $a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n$ and $(b_1 + b_2 + \ldots + b_n)a = b_1 a + b_2 a + \ldots + b_n a$ for all $n \geq 2$ and $a, b_1, b_2, \ldots, b_n \in R$.
iv) Newton's binomial formula: If R is commutative, then for all $a,b \in R$ and $n \geq 1$ we have

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + b^n.$$

Definition 2.1.3 *An element a in a ring R is called* invertible *(or a* unit*), if it has an inverse with respect to multiplication, i.e. there exists $a' \in R$ such that $aa' = a'a = 1_R$. The inverse of a unit $a \in R$ is unique (see Exercise 1.4.4 ii)) and will be denoted by a^{-1}. The set of units of the ring R will be denoted by $U(R)$.*
An element a in a ring R is called a left zero divisor *if there exists $b \in R$, $b \neq 0_R$, such that $ab = 0_R$. Similarly, a will be a* right zero divisor *if there exists $b \in R$, $b \neq 0_R$, such that $ba = 0_R$.*

Exercise 2.1.4 *Let $(R, +, \cdot)$ be a ring. Then:*
i) 0_R is a zero divisor (left and right).
ii) if $a \in R$ is a unit, a is not a zero divisor (left or right).
iii) if $a \in R$ is a zero divisor, a is not a unit.
iv) $(U(R), \cdot)$ is a group.

Definition 2.1.5 *A commutative ring F is called a* field *if any non-zero element of R is a unit (i.e. $U(F) = F^* = F \setminus \{0_F\}$). A commutative ring D is called a* domain *if D has no zero divisors other than 0_D.*

Exercise 2.1.6 *Show that any field is a domain.*

We give now some examples of rings, but leave the verification as an exercise.

Exercise 2.1.7 *Show that the following are rings. Which ones are commutative? Which ones are domains? Which ones are fields?*
i) $(\mathbb{Z}, +, \cdot)$.
ii) $(\mathbb{Q}, +, \cdot)$.
iii) $(\mathbb{R}, +, \cdot)$.
iv) $(\mathbb{C}, +, \cdot)$.
v) The set of 2×2 matrices with real entries, together with the addition and multiplication of matrices: $(M_2(\mathbb{R}), +, \cdot)$.
vi) $(C[0,1], +, \cdot)$, *where*

$$C[0,1] = \{f : [0,1] \longrightarrow \mathbb{R} \mid \ f \text{ is continuous}\},$$

$$(f+g)(x) = f(x) + g(x),\ (fg)(x) = f(x)g(x),\ f, g \in C[0,1],\ x \in [0,1].$$

vii) $(\mathbb{Z}_2, +, \cdot)$.
viii) $(\mathbb{Z}_4, +, \cdot)$.
ix) $(\mathbb{Z}_n, +, \cdot)$.
x) $(End(G), +, \cdot)$, *where* $(G, +)$ *is an abelian group,*

$$End(G) = \{f : G \longrightarrow G \mid f \text{ is a group morphism}\},$$

$$(f+g)(x) = f(x) + g(x),\ (fg)(x) = (f \circ g)(x),\ f, g \in End(G),\ x \in G.$$

xi) $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$, *with componentwise addition and multiplication defined by using distributivity and the relations between* i, j, k.
xii) If $F_4 = \{0, 1, a, b\}$ *is a field, write the addition and multiplication tables of* F_4.

Exercise 2.1.8 *Give an example of a domain that is not a field.*

Exercise 2.1.9 *If* R *is a ring and* $a, b \in R$, *then*
i) if $ab = 0_R$, *does it follow that* $ba = 0_R$?
ii) if $ab = 1_R$, *does it follow that* $ba = 1_R$?
iii) (Jacobson-Kaplansky) if $ab = 1_R$ *and* $ba \neq 1_R$, *then the set of left inverses of* b, $\mathcal{L} = \{c \in R \mid cb = 1\}$, *is infinite.*

Definition 2.1.10 *Let* R *and* R' *be rings, and* $f : R \longrightarrow R'$. *We say that* f *is a* ring morphism *if the following hold:*
i) f *is a group morphism, i.e.* $f(x + y) = f(x) + f(y)$ *for all* $x, y \in R$.
ii) $f(xy) = f(x)f(y)$ *for all* $x, y \in R$.
iii) $f(1_R) = 1_{R'}$.
The morphism f *is said to be an injective morphism if the function* f *is injective. Similarly, if the function* f *is surjective, we say that* f *is a surjective morphism. A ring morphism* $f : R \longrightarrow R'$ *is called an* isomorphism *if there exists a ring morphism* $f' : R' \longrightarrow R$ *such that* $f \circ f' = Id_{R'}$ *and* $f' \circ f = Id_R$; *we then say that the rings* R *and* R' *are* isomorphic, *and we write* $R \simeq R'$. *A morphism from* R *to* R *is called an* endomorphism *of* R, *and an isomorphism from* R *to* R *is called an* automorphism *of* R.

We remark that since f is a group morphism, it is automatic that $f(0_R) = 0_{R'}$ (see Exercise 1.4.10 i)). For ring morphisms we have to ask that $f(1_R) = 1_{R'}$, because it does not follow from the other two conditions. Indeed, the constant map 0_R from R to R satisfies i) and ii) from Definition 2.1.10, but not iii).

Exercise 2.1.11 *Let* R_1 *and* R_2 *be rings, and define the following operations on the cartesian product* $R_1 \times R_2$: $(x, y) + (x', y') = (x + x', y + y')$ *and* $(x, y) \cdot (x', y') = (xx', yy')$, *where* $x, x' \in R_1$ *and* $y, y' \in R_2$. *Show that* $R_1 \times R_2$ *is a ring with these operations (it is called the* direct product *of the rings* R_1 *and* R_2*).*

The following properties of ring morphisms are left as exercises:

Exercise 2.1.12 *Let $f : R \longrightarrow R'$ and $g : R' \longrightarrow R''$ be ring morphisms. Then:*
i) if $x \in U(R)$, then $f(x) \in U(R')$, and we have $f(x^{-1}) = f(x)^{-1}$.
ii) gf is a ring morphism.
iii) f is an isomorphism if and only if f is bijective.

Exercise 2.1.13 *Which of the following maps are ring morphisms? For each of them decide if they are injective, surjective, or an isomorphism. If a morphism is an isomorphism, find the inverse.*
i) $Id_R : R \longrightarrow R$.
ii) $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, $i(x) = x/1$ for $x \in \mathbb{Z}$.
iii) If $x \in U(R)$, $f_x : R \longrightarrow R$, $f_x(y) = xyx^{-1}$ for all $y \in R$.
iv) $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$, $f(\hat{a}(mod\ 4)) = \hat{a}(mod\ 2)$.
v) $g : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$, $g(\hat{a}(mod\ 2)) = \hat{a}(mod\ 4)$.
vi) $p_1 : R_1 \times R_2 \longrightarrow R_1$, $p_1(x, y) = x$.

Solutions to the Exercises on Section 2.1

Exercise 2.1.2 *Let $(R,+,\cdot)$ be a ring. Then the following hold:*
i) $a0_R = 0_R a = 0_R$ for all $a \in R$.
ii) Rule of signs: $a(-b) = (-a)b = -ab$, and $(-a)(-b) = ab$.
iii) $a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n$ and $(b_1 + b_2 + \ldots + b_n)a = b_1a + b_2a + \ldots + b_na$ for all $n \geq 2$ and $a, b_1, b_2, \ldots, b_n \in R$.
iv) Newton's binomial formula: If R is commutative, then for all $a, b \in R$ and $n \geq 1$ we have

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + b^n.$$

Solution: i) $a0_R = a(0_R + 0_R) = a0_R + a0_R$, and after adding $-a0_R$ to both sides we get $a0_R = 0_R$. The equality $0_R a = 0_R$ is proved similarly.
ii) $0_R = a0_R = a(b-b) = ab + a(-b)$, so $a(-b) = -ab$. The proof of $(-a)b = -ab$ is similar. Now $(-a)(-b) = (-(-a))b = ab$.
iii) Use induction on n. For $n = 2$ we have $a(b_1+b_2) = ab_1+ab_2$ which is the distributivity law. If the assertion is true for n, then $a(b_1+\ldots+b_n+b_{n+1}) = a(b_1 + \ldots + b_n) + ab_{n+1} = ab_1 + \ldots + ab_n + ab_{n+1}$.
iv) We use induction on n. For $n = 1$ the assertion is clear. Now assume the assertion is true for n and compute $(a+b)^{n+1} = (a+b)^n(a+b) = a^{n+1} + \binom{n}{1}a^n b + \binom{n}{2}a^{n-1}b^2 + \ldots + \binom{n}{n-1}a^2b^{n-1} + ab^n + a^n b + \binom{n}{1}a^{n-1}b^2 + \binom{n}{2}a^{n-2}b^3 + \ldots + \binom{n}{n-1}ab^n + b^{n+1}$. The assertion follows after collecting like terms and using $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ for all $1 \leq k \leq n$, which may be verified directly.

Exercise 2.1.4 *Let $(R,+,\cdot)$ be a ring. Then:*
i) 0_R is a zero divisor (left and right).
ii) if $a \in R$ is a unit, a is not a zero divisor (left or right).
iii) if $a \in R$ is a zero divisor, a is not a unit.
iv) $(U(R),\cdot)$ is a group.
Solution: i) $0_R 1_R = 1_R 0_R = 0_R$.
ii) Assume that a is a unit, and let $ab = 0_R$. After multiplying by a^{-1} on the left, we get $b = 0_R$. Similarly, if $ba = 0_R$, then $b = 0_R$.
iii) is logically equivalent to ii).
iv) Multiplication is associative, $1_R \in U(R)$, and all elements in U have inverses.

Exercise 2.1.6 *Show that any field is a domain.*
Solution: Let F be a field. We need to show that if $ab = 0_F$, then $a = 0_F$

or $b = 0_F$. Let $ab = 0_F$ and $a \neq 0_F$. Then a^{-1} exists, and after multiplying by it on the left we get $b = 0_F$.

Exercise 2.1.7 *Show that the following are rings. Which ones are commutative? Which ones are domains? Which ones are fields?*
i) $(\mathbb{Z}, +, \cdot)$.
ii) $(\mathbb{Q}, +, \cdot)$.
iii) $(\mathbb{R}, +, \cdot)$.
iv) $(\mathbb{C}, +, \cdot)$.
v) The set of 2×2 *matrices with real entries, together with the addition and multiplication of matrices:* $(M_2(\mathbb{R}), +, \cdot)$.
vi) $(C[0,1], +, \cdot)$, *where*

$$C[0,1] = \{f : [0,1] \longrightarrow \mathbb{R} \mid \ f \text{ is continuous}\},$$

$$(f+g)(x) = f(x) + g(x),\ (fg)(x) = f(x)g(x),\ f, g \in C[0,1],\ x \in [0,1].$$

vii) $(\mathbb{Z}_2, +, \cdot)$.
viii) $(\mathbb{Z}_4, +, \cdot)$.
ix) $(\mathbb{Z}_n, +, \cdot)$.
x) $(End(G), +, \cdot)$, *where* $(G, +)$ *is an abelian group,*

$$End(G) = \{f : G \longrightarrow G \mid f \text{ is a group morphism}\},$$

$$(f+g)(x) = f(x) + g(x),\ (fg)(x) = (f \circ g)(x),\ f, g \in End(G),\ x \in G.$$

xi) $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$, *with componentwise addition and multiplication defined by using distributivity and the relations between* i, j, k.
xii) If $F_4 = \{0, 1, a, b\}$ *is a field, write the addition and multiplication tables of* F_4.
Solution: i) $\mathbb{Z}$ is a domain, but not a field, since 2 does not have an inverse in $\mathbb{Z}$.
ii), iii), iv) are fields.
v) $M_2(\mathbb{R})$ is a ring, but it is not commutative and it has zero divisors, because

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

vi) $C[0,1]$ is a commutative ring and it has zero divisors, since $fg = 0$, where

$$f(x) = \begin{cases} 0.5 - x & \text{if } 0 \leq x \leq 0.5 \\ 0 & \text{if } 0.5 < x \leq 1 \end{cases} \quad g(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq 0.5 \\ 0.5 - x & \text{if } 0.5 < x \leq 1 \end{cases}$$

vii) $\mathbb{Z}_2$ is a field.
viii) $\mathbb{Z}_4$ is a commutative ring, and it has zero divisors since $2 \cdot 2 = 0$.
ix) $\mathbb{Z}_p$ is a field if p is prime. Indeed, if $0 < a < p$, then $1 = (a, p)$, so $1 = au + pv$, and therefore the coset of u is the inverse of a in $\mathbb{Z}_p$. If n is not prime, then $n = kl$, $1 < k, l < n$ so in $\mathbb{Z}_n$ we have $k, l \neq 0$ and $kl = 0$.
x) $End(G)$ is a ring. If G is the group $\mathbb{Z}^{\mathbb{N}}$ like in Exercise 1.4.5 xix), i.e.

$$\mathbb{Z}^{\mathbb{N}} = \{(a_0, a_1, a_2, \ldots) \mid a_i \in \mathbb{Z}\}$$

and the operation is the componentwise addition, then we have the following elements $p, l, r \in End(G)$:

$$p(a_0, a_1, a_2, \ldots) = (a_0, 0, 0, \ldots)\ r(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, \ldots).$$

We then have that $p, r \neq 0$ but $pr = 0$ and $rp \neq 0$, so in general $End(G)$ is not commutative and it has zero divisors.
xi) $\mathbb{H}$ is a ring in which all nonzero elements are units, and is not commutative. Such a ring is called a division ring. For example, the inverse of $a + bi + cj + dk \neq 0$ is

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

The elements of $\mathbb{H}$ are called quaternions and $\mathbb{H}$ is called the ring of real quaternions. We can represent quaternions as matrices in $M_2(\mathbb{C})$ by using the matrix representations of 1, i, j, and k as in the solution to Exercise 1.4.5, xxvi):

$$a + bi + cj + dk = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} + c \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} + d \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} =$$

$$= \begin{bmatrix} a - di & -b + ci \\ b + ci & a + di \end{bmatrix}.$$

We can also construct $\mathbb{H}$ using $\mathbb{C}$ in the same way we constructed $\mathbb{C}$ using $\mathbb{R}$:

$$a + bi + cj + dk = a + bi + cj + dij = a + bi + (c + di)j.$$

xii) The elements 1, $1 + 1$, $1 + a$ and $1 + b$ are distinct, so

$$\{1, 1 + 1, 1 + a, 1 + b\} = F_4.$$

Therefore

$$1 + 1 + 1 + 1 + a + 1 + b = 1 + a + b,$$

and after adding to both sides the opposite of $1+a+b$ we get $1+1+1+1 = 0$. But

$$1 + 1 + 1 + 1 = (1 + 1)(1 + 1) = (1 + 1)^2 = 0,$$

so $1+1=0$. It follows that $a+a=b+b=0$. Now $a+b$ cannot be 0, because after adding a to both sides we would get $a=b$; it cannot be a or b because we would get that either $b=0$ or $a=0$, so it has to be that $a+b=1$. In conclusion, the addidion table of F_4 is

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Now ab cannot be 0, a, or b, so $ab=1$. Then a^2 cannot be 0, 1, or a, so we must have $a^2=b$, and, similarly, $b^2=a$. In conclusion, the multiplication table of F_4 is

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Exercise 2.1.8 *Give an example of a domain that is not a field.*
Solution: The ring of integers $\mathbb{Z}$.

Exercise 2.1.9 *If R is a ring and $a,b\in R$, then*
i) if $ab=0_R$, does it follow that $ba=0_R$?
ii) if $ab=1_R$, does it follow that $ba=1_R$?
iii) (Jacobson-Kaplansky) if $ab=1_R$ and $ba\neq 1_R$, then the set of left inverses of b, $\mathcal{L}=\{c\in R\mid cb=1\}$, is infinite.
Solution: i) See the solution of Exercise 2.1.7 v).
ii) With the notation in the solution of Exercise 2.1.7 x), also let $l\in End(G)$, $l(a_0,a_1,a_2,\ldots)=(a_1,a_2,\ldots)$. Then $lr=1$ and $rl\neq 1$. We also remark that this provides another example for i): r is a right zero divisor because $pr=0$, but it is not a left zero divisor because it has a left inverse.
iii) (Bitzer) Define $f:\mathcal{L}\longrightarrow\mathcal{L}$, $f(c)=bc-1+a$, where $1=1_R$. We show that f is injective but not surjective, and therefore $\mathcal{L}$ is infinite by Exercise 1.1.7. We first show that f is injective: if $bc-1+a=bc'-1+a$, then $bc=bc'$, so $c=c'$ after multiplying on the left by a. Now, if there is a c such that $f(c)=bc-1+a=a$, it follows that $bc=1$, so $c=a$, which contradicts the fact that $ba\neq 1$. In conclusion, there is no c such that $f(c)=a$, i.e. f is not surjective.

Exercise 2.1.11 *Let R_1 and R_2 be rings, and define the following operations on the cartesian product $R_1\times R_2$: $(x,y)+(x',y')=(x+x',y+y')$*

and $(x,y)\cdot(x',y')=(xx',yy')$*, where* $x,x'\in R_1$ *and* $y,y'\in R_2$*. Show that* $R_1\times R_2$ *is a ring with these operations (it is called the* direct product *of the rings* R_1 *and* R_2*).*
Solution: We already know that R_1 and R_2 is an abelian group with addition. Distributivity follows from the distributivity in R_1 and R_2, and the identity element is $(1_{R_1},1_{R_2})$.

Exercise 2.1.12 *Let* $f:R\longrightarrow R'$ *and* $g:R'\longrightarrow R''$ *be ring morphisms. Then:*
i) if $x\in U(R)$*, then* $f(x)\in U(R')$*, and we have* $f(x^{-1})=f(x)^{-1}$*.*
ii) gf *is a ring morphism.*
iii) f *is an isomorphism if and only if* f *is bijective.*
Solution: i) We have that $1_{R'}=f(1_R)=f(xx^{-1})=f(x)f(x^{-1})$.
ii) and iii). We already know from Exercise 1.4.10 iii) and iv) that addition is preserved. The proof for multiplication is identical.

Exercise 2.1.13 *Which of the following maps are ring morphisms? For each of them decide if they are injective, surjective, or an isomorphism. If a morphism is an isomorphism, find the inverse.*
i) $Id_R:R\longrightarrow R$*.*
ii) $i:\mathbb{Z}\longrightarrow\mathbb{Q}$*,* $i(x)=x/1$ *for* $x\in\mathbb{Z}$*.*
iii) If $x\in U(R)$*,* $f_x:R\longrightarrow R$*,* $f_x(y)=xyx^{-1}$ *for all* $y\in R$*.*
iv) $f:\mathbb{Z}_4\longrightarrow\mathbb{Z}_2$*,* $f(\hat{a}(mod\ 4))=\hat{a}(mod\ 2)$*.*
v) $g:\mathbb{Z}_2\longrightarrow\mathbb{Z}_4$*,* $g(\hat{a}(mod\ 2))=\hat{a}(mod\ 4)$*.*
vi) $p_1:R_1\times R_2\longrightarrow R_1$*,* $p_1(x,y)=x$*.*
Solution: i) It is an isomorphism, equal to its own inverse.
ii) It is an injective ring morphism.
iii) It is an isomorphism, with inverse $f_{x^{-1}}$. The fact that the multiplication or the identity element are preserved follows like in the case of groups (see Exercise 1.4.11 iii)). In order to show that f_x preserves the addition, use left and right distributivity.
iv) f is a surjective group morphism by Exercise 1.4.11 vi). It is also a ring morphism by the definition of multiplication for congruence classes.
v) g is not well defined, see Exercise 1.4.11 vii).
vi) p_1 is a surjective group morphism by Exercise 1.4.11 viii). It is also a ring morphism by the definition of multiplication in the direct product ring.

2.2 Subrings and ideals

In this section we introduce two notions that are the analogs for rings of the notions of subgroup and normal subgroup. We begin by the following:

Definition 2.2.1 *Let R be a ring, and S a nonempty subset of R. Then S is called a* subring *of R if the operations on R induce on S a ring structure.*

A trivial example of a subring in any ring R is R itself. When checking that a certain subset S of a ring R is a subring we need to check three conditions:
SR1) If $x, y \in S$, then $x - y \in S$.
SR2) $1_R \in S$.
SR3) If $x, y \in S$, then $xy \in S$.
Note that SR2) ensures that S is not empty, and SR1) says that S is a subgroup of R. In conclusion, a subring of a ring is a subgroup that contains the identity and is closed under multiplication.

Exercise 2.2.2 *Which of the following subsets are subrings:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) $\mathbb{Q} \subseteq \mathbb{R}$.
iii) $\mathbb{R} \subseteq \mathbb{C}$.
iv) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
v) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
vi) the intersection of a family of subrings of a ring R.
vii) $D(0,1) = \{f \in C[0,1] \mid f$ *differentiable on* $(0,1)\} \subseteq C[0,1]$.

Exercise 2.2.3 *Let $f : R \longrightarrow R'$ be a morphism of rings. Then:*
i) $f(R)$ is a subring of R' (as in the case of groups, we denote $f(R)$ by $Im(f)$ and call it the image of f).
ii) is $f^{-1}(0_{R'})$ a subring of R? (as in the case of groups, we denote $f^{-1}(0_{R'})$ by $Ker(f)$ and call it the kernel of f).
iii) If S is a subring of R, then $f(S)$ is a subring of R'.
iv) If S' is a subring of R', then $f^{-1}(S')$ is a subring of R.
v) f is surjective $\Leftrightarrow Im(f) = R'$.
vi) f is injective $\Leftrightarrow Ker(f) = \{0_R\}$.

We now introduce an important notion that plays the same role for rings that normal subgroups play for groups.

Definition 2.2.4 *Let R be a ring and I a nonempty subset of R. We will say that I is a* left ideal *of R if I is a subgroup of R and it is closed under left multiples. This means that the following conditions are satisfied:*

LI1) for any $x, y \in I$ we have $x - y \in I$.
LI2) for any $x \in I$ and $r \in R$ we have $rx \in I$.
We will say that I is a right ideal *of R if I is a subgroup of R and it is closed under right multiples. This means that the following conditions are satisfied:*
RI1) for any $x, y \in I$ we have $x - y \in I$.
RI2) for any $x \in I$ and $r \in R$ we have $xr \in I$.
An ideal that is both a left and a right ideal is called two-sided*. Properties LI2) and RI2) are called absorption properties.*

Trivial examples of two-sided ideals in any ring R are $\{0_R\}$ and R itself. An ideal different from R is called *proper*.

Exercise 2.2.5 *i) A subring of R that is also an ideal (left or right) has to be equal to R.*
ii) In general, the ideal I of R is equal to $R \Leftrightarrow I$ contains a unit.

Exercise 2.2.6 *Let F be a commutative ring. The following assertions are equivalent:*
i) F is a field.
ii) The only ideals of F are $\{0_F\}$ and F.

Here are some examples.

Exercise 2.2.7 *Which of the following subsets are ideals:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iii) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
iv) $J \subseteq M_2(\mathbb{R})$, where

$$J = \left\{ \left[\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right] \middle| \ a, b \in \mathbb{R} \right\}$$

v) $K \subseteq M_2(\mathbb{R})$, where

$$K = \left\{ \left[\begin{array}{cc} a & 0 \\ b & 0 \end{array} \right] \middle| \ a, b \in \mathbb{R} \right\}$$

vi) the intersection of a family of ideals (left, right, or two-sided) of a ring R.

Exercise 2.2.8 *Let R be a commutative ring, and $x_1, x_2, \ldots, x_n \in R$. Then*

$$I = Rx_1 + Rx_2 + \ldots + Rx_n = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \mid a_i \in R, 1 \leq i \leq n\}$$

is an ideal of R, called the ideal generated *by* $x_1, x_2, \ldots, x_n$. *If* $n = 1$, Rx_1 *is called the* principal ideal *generated by* x_1.

Definition 2.2.9 *A domain in which all ideals are principal is called a* Principal Ideal Domain *(or PID).*

Exercise 2.2.10 *Show that* $\mathbb{Z}$ *is a PID.*

We end this section with the study of the behavior of ideals through ring morphisms.

Proposition 2.2.11 *Let* $f : R \longrightarrow R'$ *be a ring morphism. Then the following assertions hold:*
i) If I' *is a left ideal of* R', *then* $f^{-1}(I')$ *is a left ideal of* R, *and the same is true if we replace "left" by "right" or "two-sided".*
ii) If f *is surjective and* I *is a left ideal of* R, *then* $f(I)$ *is a left ideal of* R', *and the same is true if we replace "left" by "right" or "two-sided".*
iii) $Ker(f)$ *is a two-sided ideal of* R.

Proof: i) We know from Exercise 1.5.8 iv) that $f^{-1}(I') \leq R$. Let $r \in R$ and $x \in f^{-1}(I')$. We know that $f(x) \in I'$ and we want to prove that $f(rx) \in I'$. We have $f(rx) = f(r)f(x) \in I'$, because I' is a left ideal of R'. The proof of the other two assertions is similar.
ii) We know from Exercise 1.5.8 iii) that $f(I) \leq R'$. Let $r' \in R'$ and $x' \in f(I)$. Then $x' = f(x)$ for some $x \in I$, and since f is surjective, $r' = f(r)$ for some $r \in R$. We then have $r'x' = f(r)f(x) = f(rx) \in f(I)$, since I is a left ideal of R. The proof of the other two assertions is similar.
iii) follows from i), because $\{0_{R'}\}$ is a two-sided ideal of R'. ∎

Exercise 2.2.12 *Give an example to show that the assertion in Proposition 2.2.11 ii) is not true if* f *is not surjective.*

Corollary 2.2.13 *Let* $f : R \longrightarrow R'$ *be a surjective ring morphism. There exists a bijective correspondence between the left ideals of* R' *and the left ideals of* R *which contain* $Ker(f)$, *and the assertion remains true if we replace "left" by "right" or "two-sided".*

Proof: By Corollary 1.5.16 there exists a bijective correspondence between the subgroups of R' and the subgroups of R which contain $Ker(f)$, so it is enough to show that that correspondence maps ideals to ideals. Let I' be a left ideal of R'. Then $f^{-1}(I')$ is a left ideal of R and $Ker(f) = f^{-1}(0_{R'}) \subseteq f^{-1}(I')$. If I is a left ideal of R and $Ker(f) \subseteq I$, then $f(I)$ is a left ideal of R'. The proof of the other two assertions is similar. ∎

Exercise 2.2.14 *Show that any ideal of* $\mathbb{Z}_n$ *is principal.*

Solutions to the Exercises on Section 2.2

Exercise 2.2.2 *Which of the following subsets are subrings:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) $\mathbb{Q} \subseteq \mathbb{R}$.
iii) $\mathbb{R} \subseteq \mathbb{C}$.
iv) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
v) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
vi) the intersection of a family of subrings of a ring R.
vii) $D(0,1) = \{f \in C[0,1] \mid f$ *differentiable on* $(0,1)\} \subseteq C[0,1]$.
Solution: i), ii) and iii) are all subrings.
iv) is not always a subring, because $1 \notin n\mathbb{Z}$ unless $n = \pm 1$.
v) not a subring, it does not contain 1.
vi) if $\{S_i\}_{i \in I}$ is a family of subrings of R, then $S = \cap_{i \in I} S_i$ is a subring. If $x, y \in S$, then $x, y \in S_i$ for all $i \in I$, so $x + y, xy \in S_i$ for all $i \in I$, therefore $x + y, xy \in S$. Since $1 \in S_i$ for all $i \in I$, it follows that $1 \in S$.
vii) is a subring, the constant function 1 is differentiable, and the sum and product of two differentiable functions are differentiable.

Exercise 2.2.3 *Let* $f : R \longrightarrow R'$ *be a morphism of rings. Then:*
i) $f(R)$ *is a subring of* R' *(as in the case of groups, we denote* $f(R)$ *by* $Im(f)$ *and call it the image of* f*).*
ii) is $f^{-1}(0_{R'})$ *a subring of* R*? (as in the case of groups, we denote* $f^{-1}(0_{R'})$ *by* $Ker(f)$ *and call it the kernel of* f*).*
iii) If S *is a subring of* R*, then* $f(S)$ *is a subring of* R'*.*
iv) If S' *is a subring of* R'*, then* $f^{-1}(S')$ *is a subring of* R*.*
v) f *is surjective* $\Leftrightarrow Im(f) = R'$*.*
vi) f *is injective* $\Leftrightarrow Ker(f) = \{0_R\}$*.*
Solution: i) is a subring. We know that $Im(f)$ is a subgroup of R'. We have that $1_{R'} = f(1_R) \in Im(f)$, and if $x', y' \in Im(f)$, then $x' = f(x)$ and $y' = f(y)$, and so $x'y' = f(x)f(y) = f(xy) \in Im(f)$.
ii) not a subring, $1_R \notin Ker(f)$.
iii) is a subring, the proof is similar to i).
iv) is a subring, we have $1_R \in f^{-1}(S')$. Then if $x, y \in f^{-1}(S')$, so $f(x+y) = f(x) + f(y) \in S'$, and $f(xy) = f(x)f(y) \in S'$, thus $x + y, xy \in f^{-1}(S')$.
v) is just the definition of surjectivity.
vi) follows from Exercise 1.5.8 vi), because f is in particular a morphism of groups.

Exercise 2.2.5 *i) A subring of* R *that is also an ideal (left or right) has to be equal to* R*.*
ii) In general, the ideal I *of* R *is equal to* $R \Leftrightarrow I$ *contains a unit.*
Solution: i) If $1_R \in I$, then any $r \in R$ will be in I, since it can be written

as $r = r1_R$ or $r = 1_R r$, so $I = R$.
ii) If $I = R$, then $1_R \in I$ is a unit. Conversely, if $x \in I$ is a unit, then $1_R = xx^{-1} = x^{-1}x$, so $1_R \in I$, thus $I = R$ by i).

Exercise 2.2.6 *Let F be a commutative ring. The following assertions are equivalent:*
i) F is a field.
ii) The only ideals of F are $\{0_F\}$ and F.
Solution: i) $\Rightarrow$ ii). Let $I \neq \{0_F\}$ be an ideal of F. Choose $x \in I$, $x \neq 0_F$. Since F is a field, x is a unit, so $I = F$ by Exercise 2.2.5 ii).
ii) $\Rightarrow$ i). Let $x \in F$, $x \neq 0_F$. Then $Rx = \{rx \mid r \in R\} \neq \{0_F\}$ is an ideal, so it has to be equal to F, thus $1_F = rx$ for some $r \in F$, i.e. x is a unit.

Exercise 2.2.7 *Which of the following subsets are ideals:*
i) $\mathbb{Z} \subseteq \mathbb{Q}$.
ii) If $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
iii) $\{0, 2, 4\} \subseteq \mathbb{Z}_6$.
iv) $J \subseteq M_2(\mathbb{R})$, where

$$J = \left\{ \left[\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right] \middle| \ a, b \in \mathbb{R} \right\}$$

v) $K \subseteq M_2(\mathbb{R})$, where

$$K = \left\{ \left[\begin{array}{cc} a & 0 \\ b & 0 \end{array} \right] \middle| \ a, b \in \mathbb{R} \right\}$$

vi) the intersection of a family of ideals (left, right, or two sided) of a ring R.
Solution: i) not an ideal, $1 \in \mathbb{Z}$ but $\mathbb{Z} \neq \mathbb{Q}$.
ii) We have $0 = n0 \in n\mathbb{Z}$. If $x, y \in n\mathbb{Z}$, then $x = nk$ and $y = nm$, so $x - y = nk - nm = n(k - m) \in n\mathbb{Z}$. Now if $l \in \mathbb{Z}$, then $lx = l(nk) = n(lk) \in n\mathbb{Z}$, so $n\mathbb{Z}$ is an ideal.
iii) We have $\{0, 2, 4\} = 2\mathbb{Z}_6 = \{2a \mid a \in \mathbb{Z}_6\} = \{2\cdot 0, 2\cdot 1, 2\cdot 2, 2\cdot 3, 2\cdot 4, 2\cdot 5\}$, and the verification that this is an ideal of $\mathbb{Z}_6$ is similar to ii).
iv) J is clearly a subgroup. We have

$$\left[\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right] \left[\begin{array}{cc} c & d \\ e & f \end{array} \right] = \left[\begin{array}{cc} ac + be & ad + bf \\ 0 & 0 \end{array} \right] \in J,$$

and

$$\left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] \left[\begin{array}{cc} 1 & 1 \\ 0 & 0 \end{array} \right] = \left[\begin{array}{cc} 0 & 0 \\ 1 & 1 \end{array} \right] \notin J,$$

so J is a right ideal but not a left ideal.
v) K is clearly a subgroup. We have

$$\left[\begin{array}{cc} c & d \\ e & f \end{array}\right]\left[\begin{array}{cc} a & 0 \\ b & 0 \end{array}\right]=\left[\begin{array}{cc} ca+db & 0 \\ da+fb & 0 \end{array}\right]\in K,$$

and

$$\left[\begin{array}{cc} 1 & 0 \\ 1 & 0 \end{array}\right]\left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right]=\left[\begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array}\right]\notin K,$$

so K is a left ideal but not a right ideal.

Exercise 2.2.8 *Let R be a commutative ring, and $x_1, x_2, \ldots, x_n \in R$. Then*

$$I = Rx_1 + Rx_2 + \ldots + Rx_n = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \mid a_i \in R, 1 \leq i \leq n\}$$

is an ideal of R, called the ideal generated *by $x_1, x_2, \ldots, x_n$. If $n = 1$, Rx_1 is called the* principal ideal *generated by x_1.*
Solution: We have $0_R = 0_Rx_1 + 0_Rx_2 + \ldots + 0_Rx_n \in I$, and

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n - (b_1x_1 + b_2x_2 + \ldots + b_nx_n) =$$

$$= (a_1 - b_1)x_1 + (a_2 - b_2)x_2 + \ldots + (a_n - b_n)x_n \in I.$$

If $r \in R$, then

$$r(a_1x_1 + a_2x_2 + \ldots + a_nx_n) = (ra_1)x_1 + (ra_2)x_2 + \ldots + (ra_n)x_n \in I,$$

so I is an ideal.

Exercise 2.2.10 *Show that $\mathbb{Z}$ is a PID.*
Solution: First, $\mathbb{Z}$ is a domain, because it is commutative, and $mn \neq 0$ if $m \neq 0$ and $n \neq 0$. Then by Proposition 1.5.7 all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, and by Exercise 2.2.7 these are ideals. In conclusion, all ideals of $\mathbb{Z}$ are principal.

Exercise 2.2.12 *Give an example to show that the assertion in Proposition 2.2.11 ii) is not true if f is not surjective.*
Solution: Consider the inclusion $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$.

Exercise 2.2.14 *Show that any ideal of $\mathbb{Z}_n$ is principal.*
Solution: Let I be an ideal of $\mathbb{Z}_n$. Then I is a subgroup of $\mathbb{Z}_n$, so by Corollary 1.5.16 we have that I is the image through the canonical surjection of a subgroup of $\mathbb{Z}$ which contains $n\mathbb{Z}$, i.e. $I = can(d\mathbb{Z}) = \hat{d}\mathbb{Z}_n$, where $d \mid n$. But $\hat{d}\mathbb{Z}_n$ is the principal ideal generated by $\hat{d}$, so I is principal. (We could also use Exercise 1.5.17 and the fact that if $m \in \mathbb{Z}$, then $m\widehat{d} = \widehat{md} = \widehat{m}\widehat{d}$).

2.3 Factor rings

Let G be a group and $H \trianglelefteq G$. Recall that this means that $xH = Hx$ for all $x \in G$, or, equivalently, that the two congruences modulo H, left and right, coincide:

$$x \equiv y(mod\ H) \Leftrightarrow xy^{-1} \in H \Leftrightarrow x^{-1}y \in H.$$

This also meant that congruence modulo H is compatible with the group operation, i.e. we can multiply congruences: if $x \equiv y(mod\ H)$ and $z \equiv w(mod\ H)$, then $xz \equiv yw(mod\ H)$, because $zw^{-1} = h \in H$, $xh = h_1x$ for some $h_1 \in H$, and $xy^{-1} = h_2 \in H$, so $xz(yw)^{-1} = xzw^{-1}y^{-1} = xhy^{-1} = h_1xy^{-1} = h_1h_2 \in H$. This is equivalent to the fact that multiplication of congruence classes (or cosets) relative to H is well defined, or the canonical surjection from G to G/H is a group morphism.
Let now R be a ring and I a two-sided ideal of R. In particular, I is a subgroup of the abelian group R (under addition), so I is a normal subgroup of R. In conclusion, we can introduce a group structure on the factor group R/I like this:

$$(x + I) + (y + I) = (x + y) + I,\ \ x, y \in R,$$

so R/I is a group under the addition defined above, and the canonical surjection $can : R \longrightarrow R/I$ is a surjective group morphism. The zero element of this group is $0_{R/I} = 0 + I = I$. The fact that I is a two-sided ideal allows us to define multiplication on R/I like this:

$$(x + I)(y + I) = xy + I,\ \ x, y \in R.$$

In order to show that this multiplication is well defined, we need to show that if $x - x' \in I$ and $y - y' \in I$, then $xy - x'y' \in I$. Now $xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + (x - x')y' \in I$, because both $x(y - y')$ and $(x - x')y'$ belong to I (note that both left and right absorption properties were used). In this way R/I becomes a ring with identity $1_{R/I} = 1 + I$. The fact that the ring axioms are verified follows from the definition of the operations and the fact that R is a ring. For example left distributivity is checked as follows:

$$\begin{aligned}(x + I)((y + I) + (z + I)) &= (x + I)(y + z + I)\\ &= x(y + z) + I\\ &= xy + xz + I\\ &= (xy + I) + (xz + I)\\ &= (x + I)(y + I) + (x + I)(z + I).\end{aligned}$$

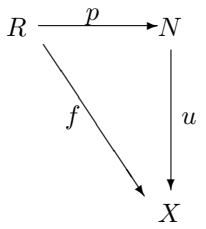
Definition 2.3.1 *If R is a ring, and I is a two-sided ideal of R, the ring R/I constructed above is called the* factor ring *of R relative to I.*

As in the case of sets or groups, we can define factor rings without any reference to elements:

Definition 2.3.2 *A factor ring of the ring R is a pair (N, p), where N is a ring, and $p : R \longrightarrow N$ is a surjective ring morphism.*

Since $can : R \longrightarrow R/I$ is a surjective ring morphism, a factor ring in the sense of Definition 2.3.1 is also a factor ring in the sense of Definition 2.3.2. The fact that the two definitions are equivalent will follow, as in the case of sets or groups, from a universal property.

Theorem 2.3.3 (The Universal Property of the Factor Ring) *Let (N, p) be a factor ring of the ring R, let X be a ring and $f : R \longrightarrow X$ a ring morphism.*
i) There exists a ring morphism $u : N \longrightarrow X$ such that $f = up$, which means that the diagram



is commutative, if and only if $Ker(p) \subseteq Ker(f)$. If u exists, then it is unique.
If u as in i) exists, then:
ii) u is surjective if and only if f is surjective.
iii) u is injective if and only if $Ker(p) = Ker(f)$.

Using Theorem 1.6.10 we see that the only thing left to prove is that if a group morphism u as in the statement exists, then it is a ring morphism. Since f is a ring morphism, the proof is identical to the one of Theorem 1.6.10.

Exercise 2.3.4 *Prove Theorem 2.3.3.*

Corollary 2.3.5 *If (N_1, p_1) and (N_2, p_2) are two factor rings of R such that $Ker(p_1) = Ker(p_2)$, then there exists an isomorphism $u : N_1 \longrightarrow N_2$ such that $up_1 = p_2$.*

Exercise 2.3.6 *Prove Corollary 2.3.5.*

Corollary 2.3.7 *If (N, p) is a factor ring of R, then there exists an isomorphism $u : N \longrightarrow R/Ker(p)$ such that $u \circ p$ is the canonical surjection.*

Exercise 2.3.8 *Prove Corollary 2.3.7.*

Corollary 2.3.9 (The First Isomorphism Theorem for Rings) *Let $f : R \longrightarrow R'$ be a ring morphism. Then*

$$R/Ker(f) \simeq Im(f).$$

Exercise 2.3.10 *Prove Corollary 2.3.9.*

Read again Corollary 2.2.13 and its proof before attempting the following:

Exercise 2.3.11 *There is a bijective correspondence between the ideals of the factor ring R/I and the ideals of R that contain I.*

Corollary 2.3.12 (The Second Isomorphism Theorem for Rings) *Let R be a ring and let $I \subseteq J$ be two-sided ideals of R. Then*

$$(R/I)/(J/I) \simeq R/J.$$

Exercise 2.3.13 *Prove Corollary 2.3.12.*

Exercise 2.3.14 *Any factor ring of $\mathbb{Z}$ is isomorphic to a $\mathbb{Z}_n$ for some integer $n \geq 0$.*

Exercise 2.3.15 *i) Prove that $\mathbb{Z}_3$ is isomorphic to a factor ring of $\mathbb{Z}_9$.*
ii) If $d \mid n$ are positive integers, prove that $\mathbb{Z}_d$ is isomorphic to a factor ring of $\mathbb{Z}_n$.

Exercise 2.3.16 *Let $n > 0$ be an integer.*
i) Describe the units of the ring $\mathbb{Z}_n$.
ii) Describe the zero divisors of the ring $\mathbb{Z}_n$.
iii) (Euler's Theorem) If a is an integer and $1 = (a, n)$, then $a^{\varphi(n)} \equiv 1(mod\ n)$, where $\varphi(n)$ is the Euler function, $\varphi(0) = 0$, $\varphi(1) = 1$, and if $m > 1$, $\varphi(m) =$ number of natural numbers relatively prime to m and less than m.
iv) Show that $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ as rings $\Leftrightarrow 1 = (n, m)$.
v) φ is multiplicative, i.e. $\varphi(nm) = \varphi(n)\varphi(m)$ if $1 = (n, m)$.

vi) $\varphi(p^k) = p^k - p^{k-1}$.
vii) If $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ *and* p_i *are distinct primes,* $1 \leq i \leq s$, *then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_s}\right).$$

viii) (Fermat's Little Theorem) If p *is a positive prime and* a *is an integer, then* $a^p \equiv a(mod\ p)$.

The result in the following exercise is known as Wilson's Theorem.

Exercise 2.3.17 *An integer* $p > 1$ *is prime if and only if* $(p-1)! \equiv -1(mod\ p)$.

As we did at the end of Section 1.6, we mention another way of introducing factor rings. Instead of starting with a group R and a two-sided ideal of R, we start with an equivalence relation $\mathcal{R}$ on the set R which is compatible with the ring operations, i.e. we can add and multiply relations: if $x_1 \mathcal{R} y_1$ and $x_2 \mathcal{R} y_2$, then $x_1 + y_1 \mathcal{R} x_2 + y_2$ and $x_1 y_1 \mathcal{R} x_2 y_2$, and moreover 1 and 0 are not equivalent. The fact that then the factor set $R/\mathcal{R}$ becomes a ring such that the canonical surjection is a ring morphism follows from the fact that $x \mathcal{R} y$ if and only if x and y are congruent modulo the two-sided ideal $C_0 = \{a \in R \mid a \mathcal{R} 0\}$.

Solutions to the Exercises on Section 2.3

Exercise 2.3.4 *Prove Theorem 2.3.3.*
Solution: We know that if u exists, then it is a morphism of additive groups. We have that $u(1_N) = u(p(1_R)) = f(1_R) = 1_X$. Then let $x', y' \in N$, and $x, y \in R$ such that $p(x) = x'$ and $p(y) = y'$. It follows that $u(x'y') = u(p(x)p(y)) = u(p(xy)) = f(xy) = f(x)f(y) = u(p(x))u(p(y)) = u(x')u(y')$.

Exercise 2.3.6 *Prove Corollary 2.3.5.*
Solution: Take $(N, p) = (N_1, p_1)$, $X = N_2$ and $f = p_2$ in Theorem 2.3.3.

Exercise 2.3.8 *Prove Corollary 2.3.7.*
Solution: Take $(N_1, p_1) = (N, p)$ and $(N_2, p_2) = (R/Ker(p), can)$, where $can : R \longrightarrow R/Ker(p)$, $can(x) = x + Ker(p)$. Then $Ker(can) = Ker(p)$ and we can apply Corollary 2.3.5.

Exercise 2.3.10 *Prove Corollary 2.3.9.*
Solution: Use Corollary 2.3.7 for $(Im(f), f)$.

Exercise 2.3.11 *There is a bijective correspondence between the ideals of the factor ring R/I and the ideals of R that contain I.*
Solution: Apply Corollary 2.2.13 for $can : R \longrightarrow R/I$ and note that $Ker(can) = I$.

Exercise 2.3.13 *Prove Corollary 2.3.12.*
Solution: Define $f : R/I \longrightarrow R/J$ by $f(x + I) = x + J$. We have that f is well defined, because if $x - y \in I$ it follows that $x - y \in J$, since $I \subseteq J$. It is clear that f is surjective and $Ker(f) = J/I$, so the result follows from Corollary 2.3.9.

Exercise 2.3.14 *Any factor ring of $\mathbb{Z}$ is isomorphic to a $\mathbb{Z}_n$ for some integer $n \geq 0$.*
Solution: By Exercise 2.2.10, any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Exercise 2.3.15 *i) Prove that $\mathbb{Z}_3$ is isomorphic to a factor ring of $\mathbb{Z}_9$.*
ii) If $d \mid n$ are positive integers, prove that $\mathbb{Z}_d$ is isomorphic to a factor ring of $\mathbb{Z}_n$.
Solution: i) Define $f : \mathbb{Z}_9 \longrightarrow \mathbb{Z}_3$ by $f(\hat{a}(mod\ 9)) = \hat{a}(mod\ 3)$. Since $3 \mid 9$, f is a well defined surjective ring morphism. Then $\mathbb{Z}_9/Ker(f) \simeq \mathbb{Z}_3$ by Theorem 2.3.9. Note that $Ker(f) = \{0, 3, 6\} = 3\mathbb{Z}_9$.
ii) Define $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_d$ by $f(\hat{a}(mod\ n)) = \hat{a}(mod\ d)$. Since $d \mid n$, f is a well defined surjective ring morphism. Then $\mathbb{Z}_n/Ker(f) \simeq \mathbb{Z}_d$ by Theorem

2.3.9. Note that $Ker(f) = d\mathbb{Z}_n$.

Exercise 2.3.16 *Let $n > 0$ be an integer.*
i) Describe the units of the ring $\mathbb{Z}_n$.
ii) Describe the zero divisors of the ring $\mathbb{Z}_n$.
iii) (Euler's Theorem) If a is an integer and $1 = (a, n)$, then $a^{\varphi(n)} \equiv 1(mod\ n)$, where $\varphi(n)$ is the Euler function, $\varphi(0) = 0$, $\varphi(1) = 1$, and if $m > 1$, $\varphi(m) =$ number of natural numbers relatively prime to m and less than m.
iv) Show that $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ as rings $\Leftrightarrow 1 = (n, m)$.
v) φ is multiplicative, i.e. $\varphi(nm) = \varphi(n)\varphi(m)$ if $1 = (n, m)$.
vi) $\varphi(p^k) = p^k - p^{k-1}$.
vii) If $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ and p_i are distinct primes, $1 \leq i \leq s$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_s}\right).$$

viii) (Fermat's Little Theorem) If p is a positive prime and a is an integer, then $a^p \equiv a(mod\ p)$.
Solution: i) (See Exercise 1.4.7 iii)). The units of $\mathbb{Z}_n$ are denoted by $\mathbf{U}_n$, they consist of those $a \in \mathbb{Z}_n$ with the property that $1 = (a, n)$, and they form an abelian group under multiplication. We have that $a \in \mathbb{Z}_n$ is a unit if and only if $au = 1$ for some u, if and only if $n \mid 1 - au$ if and only if $1 - au = nv$ for some v, if and only if $1 = au + nv$ if and only if $1 = (a, n)$.
ii) If $a \in \mathbb{Z}_n$ is not a unit, then it is a zero divisor. Indeed, if $a \in \mathbb{Z}_n$ is not a zero divisor, then the map $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $f(b) = ab$ is injective, because if $ab_1 = ab_2$, then $a(b_1 - b_2) = 0$, so $b_1 - b_2 = 0$, or $b_1 = b_2$. Since $\mathbb{Z}_n$ is finite, f is also surjective, so there exists a b such that $ab = 1$, i.e. a is a unit. Consequently, by Exercise 2.1.4 iii), the zero divisors in $\mathbb{Z}_n$ are precisely the non-units: $\{a \in \mathbb{Z}_n \mid 1 \neq (a, n)\}$.
iii) By i), the order of the group $\mathbf{U}_n$ is $\varphi(n) = |\mathbf{U}_n|$. If $1 = (a, n)$, then $\hat{a}$ is an element of the group, hence its order divides the order of the group, i.e. $\varphi(n)$, by Exercise 1.7.7 i), and the result follows.
iv) If $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ as rings, they are also isomorphic as groups, so $1 = (n, m)$ by Exercise 1.7.19 i). Conversely, if $1 = (n, m)$, then the map $f : \mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$, $f(\hat{a}(mod\, nm)) = (\hat{a}(mod\, n), \hat{a}(mod\, m))$ is an injective ring morphism, hence an isomorphism (both sets have the same number of elements).
v) Let $1 = (n, m)$. By iv) and the definition of multiplication in the direct product, we have that $\mathbf{U}_n \times \mathbf{U}_m \simeq \mathbf{U}_{nm}$. The left hand side has $\varphi(n)\varphi(m)$, and the right hand side has $\varphi(nm)$ elements, so the result follows.
vi) We count how many numbers between 1 and p^k are not relativley prime

to p^k. These numbers are $p, 2p, 3p, p^{k-1}p = p^k$, so there are p^{k-1} of them. The rest, i.e. $p^k - p^{k-1}$, are relatively prime to p^k.
vii) Since the p_i are distinct primes, we apply v) $k-1$ times and we get $\varphi(p_1^{k_1}p_2^{k_2}\dots p_s^{k_s}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}\dots p_s^{k_s}) = \dots = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\dots\varphi(p_s^{k_s})$. Then by vi) we get $\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\dots(p_s^{k_s} - p_s^{k_s-1}) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_s}\right)$.
viii) We need to show that $p \mid a^p - a = a(a^{p-1}-1)$. This is obviously true if p divides a. If p does not divide a, use iii) for $n = p$ to obtain that p divides $a^{p-1} - 1$.

Exercise 2.3.17 *An integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 (mod\ p)$.*
Solution: If $p = 2$ the assertion is clear. If p is an odd prime, $\mathbf{U}_p = \{1, 2, \dots, p-1\}$. If $a \in \mathbf{U}_p$ is equal to its own inverse, then $p \mid a^2 - 1 = (a+1)(a-1)$, so $a = p-1$, or $a = 1$. Therefore, in the product $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$, each element appears with its inverse (with the exception of 1 and $p-1$, which are their own inverses. Therefore, $(p-1)! = 1 \cdot 1 \cdot 1 \cdots 1 \cdot (p-1)$ in $\mathbb{Z}_p$, or $(p-1)! \equiv -1 (\text{mod } p)$.
Conversely, if $(p-1)! \equiv -1 (\text{mod } p)$, it follows that p is not divisible by any prime less than $p-1$, so p is prime.

2.4 Prime and maximal ideals

From now on, all rings will be commutative.

Definition 2.4.1 *An ideal P of the commutative ring R is said to be* prime *if $P \neq R$ and $ab \in P$ implies that $a \in P$ or $b \in P$.*

Exercise 2.4.2 *Show that $\{0_R\}$ is a prime ideal if and only if R is a domain.*

Exercise 2.4.3 *i) Show that $\{0\}$ is a prime ideal of $\mathbb{Z}$.*
ii) Show that if $P \neq \{0\}$ is a prime ideal of $\mathbb{Z}$, then $P = p\mathbb{Z}$, where p is prime.

We now investigate how prime ideals behave relative to ring morphisms.

Proposition 2.4.4 *Let $f : R \longrightarrow R'$ be a ring morphism (recall that all rings are commutative).*
i) If P' is a prime ideal of R', then $P = f^{-1}(P')$ is a prime ideal of R.
ii) If f is surjective, and P is a prime ideal of R such that $Ker(f) \subseteq P$, then $P' = f(P)$ is a prime ideal of R'.

Proof: i) We first remark that $P \neq R$, because $1_R \notin P = f^{-1}(P')$ ($f(1_R) = 1_{R'} \notin P'$). We know that P is an ideal of R by Proposition 2.2.11 i). Let now $ab \in P$. Then $f(ab) = f(a)f(b) \in P'$, and since P' is prime, we have that $f(a) \in P'$ or $f(b) \in P'$. So we have $a \in P$ or $b \in P$.
ii) We know that P' is an ideal of R' by Proposition 2.2.11 ii). Moreover, $P' \neq R'$, because if $1_{R'} \in P'$, then there exists $x \in P$ such that $f(x) = f(1_R) = 1_{R'}$. But then $x - 1 \in Ker(f) \subseteq P$, so $1_R \in P$, a contradiction. Let now $a'b' \in P'$. Then $a' = f(a)$ and $b' = f(b)$, where $a, b \in R$, and $f(a)f(b) = f(ab) \in P'$. This means that $f(ab) = f(x)$ for some $x \in P$. But then $ab - x \in P$, so $ab \in P$. It follows that $a \in P$ or $b \in P$, i.e. $a' = f(a) \in f(P) = P'$, or $b' = f(b) \in f(P) = P'$. ∎

Exercise 2.4.5 *Give examples to show that Proposition 2.4.4 ii) fails if either f is not surjective, or P does not contain $Ker(f)$.*

Corollary 2.4.6 *The following are equivalent for an ideal P of R:*
i) P is prime.
ii) R/P is a domain.

Proof: Use Proposition 2.4.4 for $can : R \longrightarrow R/P$, $can(x) = x + P$, $P = Ker(can)$, and $P' = \{0_{R/P}\}$. ∎

Exercise 2.4.7 *Prove Corollary 2.4.6 using the definition of a prime ideal.*

Exercise 2.4.8 *Show that a prime ideal of $\mathbb{Z}_n$ is of the form $p\mathbb{Z}_n$, where $p \in \mathbb{Z}$ is a prime divisor of n.*

Definition 2.4.9 *An ideal M of the commutative ring R is said to be* maximal *if $M \neq R$ and for any ideal I of R such that $M \subseteq I \subseteq R$ it follows that $I = M$ or $I = R$.*

Exercise 2.4.10 *Show that $\{0_R\}$ is a maximal ideal if and only if R is a field.*

Proposition 2.4.11 *Let $f : R \longrightarrow R'$ be a surjective ring morphism (recall that all rings are commutative).*
i) If M' is a maximal ideal of R', then $M = f^{-1}(M')$ is a maximal ideal of R.
ii) If M is a maximal ideal of R such that $Ker(f) \subseteq M$, then $M' = f(M)$ is a maximal ideal of R'.

Proof: Recall from Corollary 2.2.13 that there is a bijective correspondence between the ideals of R' and the ideals of R that contain $Ker(f)$. Since this correspondence preserves inclusions, the result follows. ∎

Use Proposition 2.4.11 to prove the following:

Exercise 2.4.12 *The following are equivalent for an ideal M of R:*
i) M is maximal.
ii) R/M is a field.

Exercise 2.4.13 *Prove Exercise 2.4.12 using the definition of a maximal ideal.*

Exercise 2.4.14 *M is a maximal ideal of $\mathbb{Z}$ if and only if $M = p\mathbb{Z}$, where p is prime.*

Exercise 2.4.15 *i) Show that if M is a maximal ideal of R, then M is prime.*
ii) Give an example of a prime ideal that is not maximal.

Exercise 2.4.16 *i) Find the maximal ideals of $\mathbb{Z}_n$.*
ii) Can you find a prime ideal in $\mathbb{Z}_n$ that is not maximal?

Exercise 2.4.17 *Any proper ideal of $\mathbb{Z}$ is contained in a maximal ideal of $\mathbb{Z}$.*

The assertion of Exercise 2.4.17 remains true if we replace $\mathbb{Z}$ by a commutative ring R, but we will not prove this.

Solutions to the Exercises on Section 2.4

Exercise 2.4.2 *Show that* $\{0_R\}$ *is a prime ideal if and only if* R *is a domain.*
Solution: R is a domain if and only if $ab = 0_R$ implies $a = 0_R$ or $b = 0_R$, i.e. $\{0_R\}$ is a prime ideal.

Exercise 2.4.3 *i) Show that* $\{0\}$ *is a prime ideal of* $\mathbb{Z}$.
ii) Show that if $P \neq \{0\}$ *is a prime ideal of* $\mathbb{Z}$, *then* $P = p\mathbb{Z}$, *where* p *is prime.*
Solution: i) $\mathbb{Z}$ is a domain.
ii) If $p\mathbb{Z}$, $p \neq 0$, is a prime ideal, then $p\mathbb{Z} \neq \mathbb{Z}$, i.e. $p \neq \pm 1$. Now $p\mathbb{Z}$ is a prime ideal $\Leftrightarrow$ if $ab \in p\mathbb{Z}$ then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z} \Leftrightarrow$ if $p \mid ab$ then $p \mid a$ or $p \mid b$, so p is prime.

Exercise 2.4.5 *Give examples to show that Proposition 2.4.4 ii) fails if either* f *is not surjective, or* P *does not contain* $Ker(f)$.
Solution: Consider first the inclusion of $\mathbb{Z}$ in $\mathbb{Q}$. Then $2\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, but it is not even an ideal of $\mathbb{Q}$. Now look at $can : \mathbb{Z} \longrightarrow \mathbb{Z}_2$, which is a surjective ring morphism. Then $3\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, it does not contain $Ker(can) = 2\mathbb{Z}$, and $can(3\mathbb{Z}) = \mathbb{Z}_2$, so it is not a prime ideal.

Exercise 2.4.7 *Prove Corollary 2.4.6 using the definition of a prime ideal.*
Solution: By Exercise 2.4.2, R/P is a domain $\Leftrightarrow \{0_{R/P}\}$ is a prime ideal $\Leftrightarrow (a+P)(b+P) = P$ implies $a + P = P$ or $b + P = P \Leftrightarrow ab \in P$ implies $a \in P$ or $b \in P \Leftrightarrow P$ is a prime ideal.

Exercise 2.4.8 *Show that a prime ideal of* $\mathbb{Z}_n$ *is of the form* $p\mathbb{Z}_n$, *where* $p \in \mathbb{Z}$ *is a prime divisor of* n.
Solution: The prime ideals of $\mathbb{Z}_n$ are images through the canonical surjection $can : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ of prime ideals of $\mathbb{Z}$ that contain $Ker(can) = n\mathbb{Z}$, i.e. $p\mathbb{Z}$, where $p \mid n$ and p is prime. Then $can(p\mathbb{Z}) = p\mathbb{Z}_n$.

Exercise 2.4.10 *Show that* $\{0_R\}$ *is a maximal ideal if and only if* R *is a field.*
Solution: R is a field $\Leftrightarrow \{0_R\}$ and R are the only ideals of $R \Leftrightarrow \{0_R\}$ is a maximal ideal.

Exercise 2.4.12 *The following are equivalent for an ideal* M *of* R:
i) M *is maximal.*
ii) R/M *is a field.*
Solution: Let $can : R \longrightarrow R/M$ denote the canonical surjection.
i) $\Rightarrow$ ii). We have that $M = Ker(can)$, so if M is maximal we get that $can(M) = \{M\} = \{0_{R/M}\}$ is also maximal, i.e. R/M is a field.

ii) $\Rightarrow$ i). If R/M is a field, then $\{0_{R/M}\}$ is maximal, so $M = Ker(can)$ is maximal.

Exercise 2.4.13 *Prove Exercise 2.4.12 using the definition of a maximal ideal.*
Solution: i) $\Rightarrow$ ii). If M is maximal, let $x + M \in R/M$, $x + M \neq 0_{R/M}$, i.e. $x \notin M$. Then $I = M + xR = \{a + xr \mid a \in M, r \in R\}$ is an ideal of R that strictly contains M (because $x \in I$ and $x \notin M$). Since M is maximal, we have $I = R$, so $1 = a + xr$ for some $m \in M$ and $r \in R$. Then $(x + M)(r + M) = xr + M = 1 + M$, so $x + M$ is a unit.
ii) $\Rightarrow$ i). Let $M \subseteq I \subseteq R$, and assume $M \neq I$. Let $x \in I$, $x \notin M$. Since R/M is a field, $x + M$ has an inverse $r + M$, i.e. $xr + M = 1 + M$, or $1 - xr \in M \subseteq I$. Then $1 - xr = b \in I$, so $1 = xr + b \in I$, i.e. $I = R$.

Exercise 2.4.14 *M is a maximal ideal of $\mathbb{Z}$ if and only if $M = p\mathbb{Z}$, where p is prime.*
Solution: The ideal $M = p\mathbb{Z}$ is maximal if and only if $p \neq \pm 1$ and if $p\mathbb{Z} \subseteq d\mathbb{Z} \subseteq \mathbb{Z}$ then $d\mathbb{Z} = p\mathbb{Z}$ or $d\mathbb{Z} = \mathbb{Z}$, if and only if $d \neq 0$, $d \neq \pm 1$, and if $d \mid p$, then $d = \pm p$ or $d = \pm 1$, if and only if p is prime by Exercise 1.2.20 iii).

Exercise 2.4.15 *i) Show that if M is a maximal ideal of R, then M is prime.*
ii) Give an example of a prime ideal that is not maximal.
Solution: i) If M is maximal, then R/M is a field, hence a domain, so M is prime.
ii) The ideal $\{0\}$ of $\mathbb{Z}$ is prime because $\mathbb{Z}$ is a domain, but not maximal, because $\mathbb{Z}$ is not a field.

Exercise 2.4.16 *i) Find the maximal ideals of $\mathbb{Z}_n$.*
ii) Can you find a prime ideal in $\mathbb{Z}_n$ that is not maximal?
Solution: We assume that $n > 1$.
i) will follow from ii).
ii) No, by Exercise 2.4.8 a prime ideal of $\mathbb{Z}_n$ is of the form $p\mathbb{Z}_n = p\mathbb{Z}/n\mathbb{Z}$, so $\mathbb{Z}_n/p\mathbb{Z}_n = (\mathbb{Z}/n\mathbb{Z})/(p\mathbb{Z}/n\mathbb{Z}$, which is isomorphic to $\mathbb{Z}_p$ by Corollary 2.3.12. Therefore all prime ideals of $\mathbb{Z}_n$ are maximal.

Exercise 2.4.17 *Any proper ideal of $\mathbb{Z}$ is contained in a maximal ideal of $\mathbb{Z}$.*
Solution: Any integer $n \neq \pm 1$ has a prime divisor p, so $n\mathbb{Z} \subseteq p\mathbb{Z}$.

2.5 Rings of fractions

Recall that all rings considered here are commutative.

Definition 2.5.1 *Let R be a commutative ring, and $S \subseteq R$. We say that S is a* multiplicative subset *if the following conditions are satisfied:*
MS1) $1_R \in S$.
MS2) if $s, t \in S$, *then* $st \in S$.
MS3) S *does not contain any zero divisors.*

Exercise 2.5.2 *i) If P is a prime ideal of R, show that $R \setminus P$ has properties MS1) and MS2).*
ii) If R is a domain and P is a prime ideal of R, then $R \setminus P$ is a multiplicative set.
iii) If R is a domain, show that $S = R^* = \{r \in R \mid r \neq 0_R\}$ is a multiplicative set.
iv) If $f \in R$ is not a zero divisor, then $S = \{f^k \mid k \in \mathbb{N}\}$ is a multiplicative set.
v) If R is a commutative ring, the set $S = \{s \in R \mid s$ is not a zero divisor$\}$ is a multiplicative subset.
vi) Is $\{1, 3, 5\} \subseteq \mathbb{Z}_6$ a multiplicative set?
vii) Is $\{1, 3, 5, 7\} \subseteq \mathbb{Z}_8$ a multiplicative set?

Lemma 2.5.3 *Let R be a commutative ring and S a multiplicative subset in R. The relation on $R \times S$ defined by*

$$(a, s) \sim (b, t) \Leftrightarrow at = bs$$

is an equivalence relation.

Proof: The relation is clearly reflexive, i.e. for any $(a, s) \in R \times S$ we have $(a, s) \sim (a, s)$, since $as = as$. If $(a, s) \sim (b, t)$, then $at = bs$, so $bs = at$, and therefore $(b, t) \sim (a, s)$, i.e. the relation is symmetric. Finally, if $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$, then $at = bs$ and $bu = ct$. Multiplying the first equality by u and the second one by s, we get $atu = bsu$, and $bsu = cts$. Consequently, we get $atu = cts$, so $t(au - cs) = 0_R$. Since $t \in S$ is not a zero divisor, we get $au = cs$, i.e. $(a, s) = (c, u)$, so the relation is transitive, and the proof is complete. ∎

The equivalence class of the element $(a, s) \in R \times S$ will be denoted by $\frac{a}{s}$ and called a *fraction*. The element a will be called the *numerator* of the fraction $\frac{a}{s}$, and the element s will be called the denominator of the fraction $\frac{a}{s}$. We remark that if we allow zero divisors in S, then the relation defined

in Lemma 2.5.3 is not an equivalence relation, because it is not transitive. To see this, assume that $a \in S$ and $b \in R$, $b \neq 0_R$ such that $ab = 0_R$. Then we have

$$\frac{b}{1_R} = \frac{ab}{a} = \frac{0_R}{a} = \frac{0_R}{1_R},$$

since it is easy to check each equality, however $\frac{b}{1_R} \neq \frac{0_R}{1_R}$, because $b \neq 0_R$. It is possible to allow zero divisors in S by changing the definition of the equivalence relation on $R \times S$, but we will not do this here.

Proposition 2.5.4 *Let R be a commutative ring, S a multiplicative subset in R, and denote by*

$$S^{-1}R = \frac{R \times S}{\sim} = \left\{ \frac{a}{s} \;\middle|\; (a, s) \in R \times S \right\}$$

the factor set of the set $R \times S$ relative to the equivalence relation $\sim$. Then $S^{-1}R$ becomes a commutative ring with the following operations:

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

and

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Moreover, the map

$$\varphi_S : R \longrightarrow S^{-1}R, \;\; \varphi(a) = \frac{a}{1_R}$$

is an injective ring morphism that sends each $s \in S$ to a unit in $S^{-1}R$. We will call φ_S the canonical injection.

Proof: We first need to show that the two operations are well defined, i.e. the definitions do not depend on the representatives chosen. This means that if $\frac{a}{s} = \frac{a'}{s'}$ and $\frac{b}{t} = \frac{b'}{t'}$, we need to prove that

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'},$$

and

$$\frac{ab}{st} = \frac{a'b'}{s't'}.$$

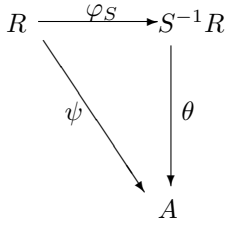
In order to prove the first equality, we need to show that $(at + bs)s't' = (a't'+b's')st$. We know that $as' = a's$ and $bt' = b't$, so, after multiplying the

first by tt' and the second by ss', we get $ats't' = a't'st$ and $bss't' = b's'st$, which can be added to obtain the desired equality.
In order to prove the second equality, we need to show that $abs't' = a'b'st$, which can be obtained by multiplying $as' = a's$ and $bt' = b't$.
It may be immediately checked that the addition of fractions defined above is associative and commutative. Then we have that $0_{S^{-1}R} = \frac{0_R}{1_R} = \frac{0_R}{s}$ for any $s \in S$, and the opposite of $\frac{a}{s}$ is $\frac{-a}{s}$, so $S^{-1}R$ is an abelian group with $+$.
The multiplication of fractions is obviously associative and commutative, and $1_{S^{-1}R} = \frac{1_R}{1_R} = \frac{s}{s}$ for any $s \in S$. Distributivity is also easy to check, so $S^{-1}R$ is a commutative ring.
It is obvious that φ_S is a ring morphism, and if $\frac{a}{1_R} = \frac{0_R}{1_R}$, then $a = 0_R$, i.e. $Ker(\varphi_S) = \{0_R\}$, so φ_S is injective.
Finally, if $s \in S$, then $\varphi(s) = \frac{s}{1_R}$ is a unit with inverse $(\varphi(s))^{-1} = \frac{1_R}{s}$. ∎

Definition 2.5.5 *We will call the pair $(S^{-1}R, \varphi_S)$, defined in Proposition 2.5.4, the* ring of fractions *of R relative to S (or with denominators in S).*

The ring of fractions has the following universal property:

Theorem 2.5.6 (The Universal Property of the Ring of Fractions) *Let R be a commutative ring, S a multiplicative subset in R, and $(S^{-1}R, \varphi_S)$ the ring of fractions of the ring R with denominators in S. Then for any commutative ring A, and any ring morphism $\psi : R \longrightarrow A$, with the property that $\psi(s)$ is a unit in A for any $s \in S$, there exists a unique ring morphism $\theta : S^{-1}R \longrightarrow A$ such that $\psi = \theta\varphi_S$, which means that the diagram*



is commutative.

Proof: Define $\theta\left(\frac{a}{s}\right) = \psi(a)\psi(s)^{-1}$. The definition is correct, because if $\frac{a}{s} = \frac{a'}{s'}$, then $as' = a's$, so $\psi(as') = \psi(a's)$, or $\psi(a)\psi(s') = \psi(a')\psi(s)$, and

so, after multiplying by $\psi(s)^{-1}\psi(s')^{-1}$ we get $\psi(a)\psi(s)^{-1} = \psi(a')\psi(s')^{-1}$. We check that θ is a ring morphism:

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

$$\begin{aligned}
\theta\left(\frac{a}{s}\cdot\frac{b}{t}\right) &= \theta\left(\frac{ab}{st}\right) \\
&= \psi(ab)\psi(st)^{-1} \\
&= \psi(a)\psi(b)\psi(s)^{-1}\psi(t)^{-1} \\
&= \psi(a)\psi(s)^{-1}\psi(b)\psi(t)^{-1} \\
&= \theta\left(\frac{a}{s}\right)\theta\left(\frac{b}{t}\right),
\end{aligned}$$

and

$$\theta\left(\frac{1_R}{1_R}\right) = \psi(1_R)\psi(1_R)^{-1} = 1_X 1_X = 1_X.$$

We have that

$$\theta(\varphi_S(a)) = \theta\left(\frac{a}{1_R}\right) = \psi(a)\psi(1_R)^{-1} = \psi(a)1_X = \psi(a),$$

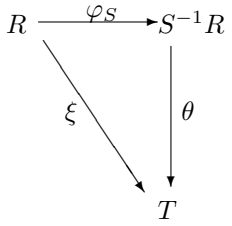
so $\psi = \theta\varphi_S$.
We now show that θ is unique. If θ' is another morphism with the property that $\psi = \theta'\varphi_S$, we have

$$\begin{aligned}
\theta'\left(\frac{a}{s}\right) &= \theta'\left(\frac{a}{1_R}\right)\theta'\left(\frac{1_R}{s}\right) \\
&= \theta'\left(\frac{a}{1_R}\right)\theta'\left(\frac{s}{1_R}\right)^{-1} \\
&= \theta'(\varphi_S(a))\theta'(\varphi_S(s))^{-1} \\
&= \psi(a)\psi(s)^{-1} \\
&= \theta\left(\frac{a}{s}\right).
\end{aligned}$$

∎

The following corollary says that the ring of fractions is unique, up to an isomorphism, among the rings satisfying the same universal property.

Corollary 2.5.7 *If the pair (T, ξ), where $\xi : R \longrightarrow T$ sends the elements of S to units in T, satisfies the universal property in Theorem 2.5.6, then there exists an isomorphism $\theta : S^{-1}R \longrightarrow T$ such that $\theta\varphi_S = \xi$, i.e. the diagram*



is commutative.

Proof: By the universal property for $(S^{-1}R, \varphi_S)$ there exists a ring morphism $\theta : S^{-1}R \longrightarrow T$ such that $\theta\varphi_S = \xi$, and by the universal property for (T, ξ) there exists a ring morphism $\theta' : T \longrightarrow S^{-1}R$ such that $\theta'\xi = \varphi_S$. It follows that $\theta'\theta\varphi_S = \theta'\xi = \varphi_S$, and $\theta\theta'\xi = \theta\varphi_S = \xi$. Since we also have that $Id_{S^{-1}R}\varphi_S = \varphi_S$ and $Id_T\xi = \xi$, by the uniqueness of the morphism in the universal property we get that $\theta\theta' = Id_T$ and $\theta'\theta = Id_{S^{-1}R}$, i.e. θ and θ' are isomorphisms inverse to each other. ∎

Definition 2.5.8 *If R is a domain, P is a prime ideal of R, and $S = R\backslash P$, the ring of fractions $(S^{-1}R, \varphi_S)$ is denoted by (R_P, φ_P), and is called the* localization *of R at the prime ideal P.*

We will refer to the ring of fractions $(S^{-1}R, \varphi_S)$ simply as $S^{-1}R$, with the understanding that it always comes with the injective ring morphism $\varphi_S : R \longrightarrow S^{-1}R$, $\varphi(a) = \dfrac{a}{1_R}$.

Definition 2.5.9 *If S is the multiplicative subset of Exercise 2.5.2 v), then we will call the ring of fractions $S^{-1}R$ the* total ring of fractions *of the ring R.*

Exercise 2.5.10 *Show that the total ring of fractions of a domain R is a field, called the* field of fractions *of the domain R. Because of Definition 2.5.8, the field of fractions of the domain R is sometimes denoted by $R_{\{0_R\}}$.*

Exercise 2.5.11 *If S is the multiplicative subset of Exercise 2.5.2 vii), show that $S^{-1}\mathbb{Z}_8 \simeq \mathbb{Z}_8$.*

Exercise 2.5.12 *If S consists of units of R, show that $S^{-1}R \simeq R$.*

Exercise 2.5.13 *i) If I is an ideal of R, show that*

$$I^e = \left\{ \frac{a}{s} \middle| a \in I \right\}$$

is an ideal of $S^{-1}R$.
ii) If J is an ideal of $S^{-1}R$, show that

$$J^c = \varphi_S^{-1}(J) = \{a \in R \mid \varphi_S(a) = \frac{a}{1_R} \in J\}$$

is an ideal of R, and $J = J^{ce}$.
iii) Show that there is a bijective correspondence between the prime ideals of $S^{-1}R$ and the prime ideals of R that are disjoint from S.
iv) Show that if I is not prime we can have $I \cap S = \emptyset$ and $I \neq I^{ec}$.
v) Show that a ring of fractions of a domain is also a domain.
vi) Find the maximal ideals of R_P, where R is a domain and P is prime.

We now show that when constructing a ring of fractions, we can maximize the set of denominators, i.e. the multiplicative set S, in the sense that we can assume that all divisors of elements in S are also in S.

Definition 2.5.14 *We say that the multiplicative subset S is* saturated *if from $ST \in S$ it follows that both s and t are in S. This means that for any $t \in S$ and $s \mid t$ we get that $s \in S$.*

Exercise 2.5.15 *Let S be a multiplicative set in the ring R. Then:*
i)

$$S_{sat} = \{s \in R \mid \exists t \in S, \ \ s \mid t\}$$

is a saturated multiplicative set containing S, and $S^{-1}R \simeq S_{sat}^{-1}R$.
ii) If $S = \{1\}$, then $S_{sat} = U(R)$.
iii) If P is a prime ideal in the domain R, and $S = R \setminus P$ (see Exercise 2.5.2 ii)), then $S = S_{sat}$.

Now we see that the condition $1 \in S$ in Definition 2.5.1 could have been replaced by the weaker condition that S is non-empty. In that case, we could have defined the canonical injection by $\varphi(a) = \frac{as}{s}$ for $s \in S$ and check that the definition does not depend on the element s.

We now extend the definition of a maximal ideal as follows: if Γ is a set of ideals of the ring R, we say that $M \in \Gamma$ is *maximal in* Γ if it is not

properly contained in any other ideal in Γ. A maximal ideal in the set of all proper ideals of R is a maximal ideal in the sense of Definition 2.4.9. One way to show that maximal ideals in $\Gamma \neq \emptyset$ exist is to use Zorn's Lemma, which says that if for any non-empty chain of ideals $\{I_i\}_{i\in\Lambda}$ (this means that for any $i, j \in \Lambda$ we either have $I_i \subseteq I_j$ or $I_j \subseteq I_i$) there exists a $J \in \Gamma$ such that $I_i \subseteq J\ \forall i \in \Lambda$, then Γ has at least one maximal element.

We illustrate the use of Zorn's Lemma with the following result, due to Krull. This is a device that produces prime ideals starting with multiplicative subsets.

Proposition 2.5.16 *Let S be a multiplicative subset in the commutative ring R, and I an ideal of R such that $I \cap S = \emptyset$. Then the set*

$$\Gamma = \{J \text{ ideal of } R \mid \ I \subseteq J,\ \ J \cap S = \emptyset\}$$

has maximal elements, which are prime ideals of R.

Proof: We use Zorn's Lemma. We have that $I \in \Gamma$, so $\Gamma \neq \emptyset$. If $\{I_i\}_{i\in\Lambda}$ is a chain in Γ, then $J = \cup_{i\in\Lambda} I_i$ is an ideal of R, and

$$J \cap S = (\cup_{i\in\Lambda} I_i) \cap S = \cup_{i\in\Lambda}(I_i \cap S) = \emptyset,$$

which shows that $J \in \Gamma$. Since it is clear that $I_i \subseteq J\ \forall i \in \Lambda$, then Γ has at least one maximal element P.

We show that P is a prime ideal. It is clear that $P \neq R$ because $1 \notin P$. If we now take $x, y \in R$ such that $x \notin P$ and $y \notin P$, we have that $P \subsetneq P + xR$, and so $P + xR \neq \emptyset$. Similarly, $P \subsetneq P + yR$, and so $P + yR \neq \emptyset$. Let $s = p_1 + xa_1$ and $t = p_2 + ya_2$, where $s, t \in S$ and $p_1, p_2 \in P$. Then

$$st = (p_1 + xa_1)(p_2 + ya_2) \in P,$$

because after expanding, the first three products have a factor in P and the last one is a multiple of xy. We have thus found an element $st \in P \cap S$, a contradiction. ∎

Exercise 2.5.17 *Show that any saturated multiplicative subset is the complement of a union of prime ideals.*

Solutions to the Exercises on Section 2.5

Exercise 2.5.2 *i) If P is a prime ideal of R, show that $R \setminus P$ has properties MS1) and MS2).*
ii) If R is a domain and P is a prime ideal of R, then $R \setminus P$ is a multiplicative set.
iii) If R is a domain, show that $S = R^* = \{r \in R \mid r \neq 0_R\}$ is a multiplicative set.
iv) If $f \in R$ is not a zero divisor, then $S = \{f^k \mid k \in \mathbb{N}\}$ is a multiplicative set.
v) If R is a commutative ring, the set $S = \{s \in R \mid s$ is not a zero divisor$\}$ is a multiplicative subset.
vi) Is $\{1, 3, 5\} \subseteq \mathbb{Z}_6$ a multiplicative set?
vii) Is $\{1, 3, 5, 7\} \subseteq \mathbb{Z}_8$ a multiplicative set?
Solution: i) $1_R \notin P$ because $P \neq R$. If $a \notin P$ and $b \notin P$, then $ab \notin P$ by the definition of a prime ideal.
ii) follows from i) and the fact that there are no zero divisors in R.
iii) follows from ii), because $\{0_R\}$ is a prime ideal in R.
iv) $1_R = f^0 \in S$. If $k, l \in \mathbb{N}$, then $f^k f^l = f^{k+l} \in S$. If $f^k a = f f^{k-1} a = 0_R$, then $f^{k-1} a = 0_R$ since f is not a zero divisor, and we can continue until we get $a = 0_R$.
v) 1_R is not a zero divisor. It is clear that if a, b are not zero divisors, then ab is not a zero divisor.
vi) No, 3 is a zero divisor.
vii) Yes, this is actually the set of units in $\mathbb{Z}_8$.

Exercise 2.5.10 *Show that the total ring of fractions of a domain R is a field, called the* field of fractions *of the domain R. Because of Definition 2.5.8, the field of fractions of the domain R is sometimes denoted by $R_{\{0_R\}}$.*
Solution: If $\frac{a}{b} \neq \frac{0_R}{1_R}$, it follows that $a \neq 0_R$, so $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Exercise 2.5.11 *If S is the multiplicative subset of Exercise 2.5.2 vii), show that $S^{-1}\mathbb{Z}_8 \simeq \mathbb{Z}_8$.*
Solution: S consists of units of $\mathbb{Z}_8$, see the solution to Exercise 2.5.12 below.

Exercise 2.5.12 *If S consists of units of R, show that $S^{-1}R \simeq R$.*
Solution: Both (R, Id_R) and $(S^{-1}R, \varphi_S)$ satisfy the same universal property, so the assertion follows from Corollary 2.5.7.
This can also be proved without using the universal property: we will prove that the injective ring morphism $\varphi_S : R \longrightarrow S^{-1}R$, $\varphi_S(r) = \frac{r}{1_R}$, is

an isomorphism. To do this it is enough to prove that it is surjective. Let $\frac{r}{s} \in S^{-1}R$. Then $\varphi_S(rs^{-1}) = \frac{rs^{-1}}{1_R} = \frac{r}{s}$, because $rs^{-1}s = r1_R$.

Exercise 2.5.13 *i) If I is an ideal of R, show that*

$$I^e = \left\{ \frac{a}{s} \middle| a \in I \right\}$$

is an ideal of $S^{-1}R$.
ii) If J is an ideal of $S^{-1}R$, show that

$$J^c = \varphi_S^{-1}(J) = \{a \in R \mid \varphi_S(a) = \frac{a}{1_R} \in J\}$$

is an ideal of R, and $J = J^{ce}$.
iii) Show that there is a bijective correspondence between the prime ideals of $S^{-1}R$ and the prime ideals of R that are disjoint from S.
iv) Show that if I is not prime we can have $I \cap S = \emptyset$ and $I \neq I^{ec}$.
v) Show that a ring of fractions of a domain is also a domain.
vi) Find the maximal ideals of R_P, where R is a domain and P is prime.

Solution: i) It is clear that $\frac{0_R}{1_R} \in I^e$. Now if $\frac{a}{s}, \frac{b}{t} \in I^e$, then

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \in I^e,$$

because $at+bs \in I$. Finally, if $\frac{a}{s} \in I^e$ and $\frac{r}{t} \in S^{-1}R$, then $\frac{a}{s} \cdot \frac{r}{t} = \frac{ar}{st} \in I^e$, because $ar \in I$.
ii) The first assertion follows from Proposition 2.2.11.
We now prove

$$J = J^{ce}. \tag{2.1}$$

If $\frac{a}{s} \in J$, then $\frac{s}{1_R} \cdot \frac{a}{s} = \frac{a}{1_R} \in J$, so $a \in J^c$, and therefore $\frac{a}{s} \in J^{ce}$. Conversely, if $\frac{a}{s} \in J^{ce}$, then $a \in J^c$, and so $\frac{a}{1_R} \in J$. But then $\frac{a}{s} = \frac{a}{1_R} \cdot \frac{1_R}{s} \in J$.
iii) If P is a prime ideal of R and $P \cap S = \emptyset$, then

$$P^e = \left\{ \frac{a}{s} \middle| a \in P \right\}$$

is a proper ideal of $S^{-1}R$. Indeed, if $\frac{1_R}{1_R} = \frac{a}{s} \in P^e$, then $a = s \in P \cap S$, a contradiction. Note that if $s \in P \cap S$, then $P^e = S^{-1}R$, because P^e contains the unit $\frac{s}{1_R}$ (we say that in this case P "explodes" in $S^{-1}R$). P^e

is a prime ideal, because if $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in P^e$, then $ab \in P$, so $a \in P$ or $b \in P$, i.e. $\frac{a}{s} \in P^e$ or $\frac{b}{t} \in P^e$.
Now if Q is a prime ideal of $S^{-1}R$,

$$Q^c = \varphi_S^{-1}(Q) = \{a \in R \mid \varphi_S(a) = \frac{a}{1_R} \in Q\}$$

satisfies $Q^c \cap S = \emptyset$, because the images of elements in S through φ_S are units in $S^{-1}R$. By Proposition 2.4.4 i), Q^c is a prime ideal of R.
If P is a prime ideal of R and $P \cap S = \emptyset$, then we have that

$$P^{ec} = P, \tag{2.2}$$

because $a \in P \Rightarrow \frac{a}{1_R} \in P^e$. Conversely, if $\frac{a}{1_R} \in P^e$, then $\frac{a}{1_R} = \frac{b}{s} \in P^e$, where $b \in P$ and $s \in S$. Then $as = b \in P$, and since $s \notin P$, we have that $a \in P$.
Now (2.2) and (2.1) show that $P \mapsto P^e$ and $Q \mapsto Q^c$ are bijections inverse to each other.
iv) Take $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, and $S = \{1, 2, 4, 8, \ldots, 2^n, \ldots\}$. Then $I \cap S = \emptyset$ and $3 \in I^{ec}$, because $\frac{3}{1} = \frac{6}{2} \in I^e$, but $3 \notin I$.
v) We know that $\{0_R\}$ is a prime ideal of R, so by i) $\{0_R\}^e$ is also prime.
vi) The bijective correspondences in i) preserve inclusions, so all prime ideals in R_P are contained in P^e. Indeed, if P_1 is a prime ideal of R such that $P_1 \cap (R \setminus P) = \emptyset$, i.e. $P_1 \subseteq P$, then $P_1^e \subseteq P^e$. If P_1^e is maximal, then $P_1^e = P^e$. In conclusion, R_P has only one maximal ideal (we say it is a "local" ring), namely P^e, which is also denoted by P_P.

Exercise 2.5.15 *Let S be a multiplicative set in the ring R. Then:*
i)

$$S_{sat} = \{s \in R \mid \exists t \in S, \ \ s \mid t\}$$

is a saturated multiplicative set containing S, and $S^{-1}R \simeq S_{sat}^{-1}R$.
ii) If $S = \{1\}$, then $S_{sat} = U(R)$.
iii) If P is a prime ideal in the domain R, and $S = R \setminus P$ (see Exercise 2.5.2 ii)), then $S = S_{sat}$.
Solution: i) Let $s_1, s_2 \in S_{sat}$, and $t_1, t_2 \in S$ such that $s_1 \mid t_1$ and $s_2 \mid t_2$. Then $s_1 s_2 \mid t_1 t_2 \in S$. If $s \in S_{sat}$ is a zero divisor, and $s \mid t \in S$, then t is also a zero divisor, a contradiction.
Let now $\varphi : R \longrightarrow S^{-1}R$ and $\varphi' : R \longrightarrow S_{sat}^{-1}R$ denote the canonical injections. Since $S \subseteq S_{sat}$, by Theorem 2.5.6 there exists a ring morphism $\theta : S^{-1}R \longrightarrow S_{sat}^{-1}R$, $\theta(\frac{a}{t}) = \frac{a}{t}$. Since θ is clearly injective, let $\frac{a}{s} \in S_{sat}^{-1}R$,

and $t \in S$, $t = sr$. Then $\theta(\frac{ar}{sr}) = \frac{ar}{sr} = \frac{a}{s}$, so θ is also surjective.
ii) If $u \in U(R)$, then $v \mid u$ if and only if $v \in U(R)$.
iii) $ab \notin P$ if and only if $a \notin P$ and $b \notin P$.

Exercise 2.5.17 *Show that any saturated multiplicative subset is the complement of a union of prime ideals.*
Solution: We need to show that any $x \notin S$ belongs to a prime disjoint from S. If $x \notin S$, then $xR \cap S = \emptyset$, because S is saturated. If we take $I = xR$ in Proposition 2.5.16, we get that x belongs to a maximal element, which is a prime ideal disjoint from S.

2.6 Polynomial rings

Recall that all rings are commutative, even if the constructions in this section may be performed without this condition. If R is a ring, we recall that $R^{\mathbb{N}}$ is the set of all functions from $\mathbb{N}$ to R. If f is such a function, we can refer to it as a sequence: $f = (a_0, a_1, \ldots, a_n, \ldots)$, where $a_n = f(n)$ for all $n \in \mathbb{N}$. Since $(R, +)$ is an abelian group, we recall from Exercise 1.4.5 xix) that $R^{\mathbb{N}}$ is an abelian group with the following operation. If $f = (a_0, a_1, \ldots, a_n, \ldots)$ and $g = (b_0, b_1, \ldots, b_n, \ldots)$, then

$$f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots).$$

Also recall that the zero element is $(0_R, 0_R, \ldots)$, and the opposite of the function $(a_0, a_1, \ldots)$ is $(-a_0, -a_1, \ldots)$. We will introduce a new operation on $R^{\mathbb{N}}$.

Proposition 2.6.1 *If $f = (a_0, a_1, \ldots, a_n, \ldots)$ and $g = (b_0, b_1, \ldots, b_n, \ldots)$, then*

$$fg = (c_0, c_1, \ldots, c_n, \ldots), \;\; c_n = \sum_{i+j=n} a_i b_j, \;\; n \in \mathbb{N}$$

is commutative, associative, distributive with respect to addition, and has identity element $(1_R, 0_R, 0_R, \ldots)$.

Proof: This multiplication is obviously commutative, because the multiplication in R is commutative. Let

$$h = (c_0, c_1, \ldots), \; (fg)h = (d_0, d_1, \ldots, d_n, \ldots),$$

and

$$f(gh) = (e_0, e_1, \ldots, e_n, \ldots).$$

We have

$$\begin{aligned} d_n &= \sum_{k+l=n} (\sum_{i+j=k} a_i b_j) c_l \\ &= \sum_{k+l=n} \sum_{i+j=k} (a_i b_j) c_l \\ &= \sum_{i+j+l=n} (a_i b_j) c_l \\ &= \sum_{i+j+l=n} a_i (b_j c_l) \\ &= \sum_{i+k=n} \sum_{j+l=k} a_i (b_j c_l) \\ &= \sum_{i+k=n} a_i (\sum_{j+l=k} b_j c_l) \\ &= e_n \end{aligned}$$

for all $n \in \mathbb{N}$, so the multiplication is associative. Now

$$\begin{aligned} f(g+h) &= (a_0(b_0+c_0), \ldots, \sum_{i+j=n} a_i(b_j+c_j), \ldots) \\ &= (a_0b_0 + a_0c_0, \ldots, \sum_{i+j=n} a_ib_j + \sum_{i+j=n} a_ic_j, \ldots) \\ &= fg + fh, \end{aligned}$$

so multiplication is distributive with respect to addition.
It is easy to see that $(1_R, 0_R, 0_R, \ldots)$ is the identity element for multiplication (writing the element on position j as $\delta_{0,j}$ will make this even easier). ∎

Definition 2.6.2 *$(R^{\mathbb{N}}, +, \cdot)$ is a commutative ring. If we denote*

$$X = (0_R, 1_R, 0_R, \ldots) \tag{2.3}$$

(i.e. $X : \mathbb{N} \longrightarrow R$ is the function that sends 1 to 1_R and all the other natural numbers to 0_R), then we can check that

$$X^n = (0_R, \ldots, 0_R, 1_R, 0_R, \ldots), \quad n \text{ times } 0_R \text{ in the beginning},$$

and an element $f = (a_0, a_1, \ldots, a_n, \ldots)$ can be written as

$$f = \sum_{i=0}^{\infty} a_i X^i,$$

where $X^0 = 1_R$. *We will call* f *a* formal series *(or formal power series), and the elements* a_i *the* coefficients *of the series* f. *We call* a_0 *the* free term *or the* constant term *of* f. *We will denote*

$$R[[X]] = R^{\mathbb{N}},$$

and we will call it the ring of formal series in one indeterminate with coefficients in R. *We will call the injective ring morphism*

$$\varphi : R \longrightarrow R[[X]], \;\; \varphi(a) = (a, 0_R, \ldots)$$

the canonical injection.

Exercise 2.6.3 *Check that the canonical injection*

$$\varphi : R \longrightarrow R[[X]], \;\; \varphi(a) = (a, 0_R, \ldots)$$

is an injective ring morphism.

Remark 2.6.4 *Note that it does not make much sense to call* X *a "variable" (even though you might see it called this way in some texts), because it does not vary, it does not take any values. In fact,* X *is a function defined on* $\mathbb{N}$ *with values in* R, *and its definition is given in (2.3).*

Definition 2.6.5 *A formal series with only finitely many nonzero coefficients is called a* polynomial. *The sum and product of two polynomials are also polynomials, so the polynomials form a subring of* $R[[X]]$, *denoted by* $R[X]$. *It is clear that the canonical injection* φ *takes values in* $R[X]$. *If we identify* 0_R *by* $\varphi(0_R)$ *and* 1_R *by* $\varphi(1_R)$, *then* $0_{R[X]} = 0_R$ *and* $1_{R[X]} = 1_R$. *We call* $R[X]$ *the* polynomial ring in one indeterminate with coefficients in R. *Note that* $R[X]$ *always comes with* $\varphi : R \longrightarrow R[X]$, *which gives a way of regarding elements of* R *as polynomials (called* constants*).*

Exercise 2.6.6 *Check that* $R[X]$ *is a subring of* $R[[X]]$.

A polynomial $f \in R[X]$ may be written uniquely as

$$f = a_0 + a_1 X + a_2 X^2 + \ldots a_n X^n,$$

where $a_i X^i = \varphi(a_i) X^i = (0_R, \ldots, 0_R, a_i, 0_R, \ldots)$, i times 0_R in the beginning.

Exercise 2.6.7 *Why are the coefficients of a polynomial unique?*

A polynomial of the form aX^i is called a *monomial*. A formal series is a formal sum of monomials, and a polynomial is a (finite) sum of monomials.

Definition 2.6.8 *If $f \in R[X]$, $f \neq 0_R$, then f may be written uniquely as*

$$f = a_0 + a_1X + a_2X^2 + \dots a_nX^n,\ a_n \neq 0_R.$$

We call n the degree *of f, and we write $deg(f) = n$ (in this case a_n is called the* leading coefficient *of f). Note that the zero polynomial does not have a degree.*

Exercise 2.6.9 *Let $f, g \in R[X]$, $f, g \neq 0_R$. Then, if $f + g$ and fg are nonzero, we have:*
i) $deg(f + g) \leq max\{deg(f), deg(g)\}$. Give an example when we have $=$ and an example when we have $<$.
ii) $deg(fg) \leq deg(f) + deg(g)$. Give an example when we have $=$ and an example when we have $<$.

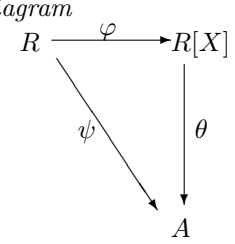
Exercise 2.6.10 *i) Show that $f \in R[X]$ is a zero divisor if and only if there exists $a \in R$, $a \neq 0_R$ such that $af = 0_R$.*
ii) Find the zero divisors of degree 2 in $\mathbb{Z}_6[X]$.
iii) If R is a domain, then $R[X]$ is a domain.

Exercise 2.6.11 *An element $a \in R$ is called* nilpotent *if there exists $n \in \mathbb{N}$ such that $a^n = 0_R$.*
i) Show that the set of nilpotent elements in R is an ideal, called the nilradical *of R, and denoted by $\mathcal{N}(R)$.*
ii) Find the nilpotent elements in $\mathbb{Z}_{12}$.
iii) Show that $f \in R[X]$ is nilpotent if and only if all its coefficients are nilpotent.
iv) Find the nilpotents of degree 1 in $\mathbb{Z}_{12}[X]$.

Exercise 2.6.12 *i) Show that if u is a unit and x is nilpotent, then $u + x$ is a unit.*
ii) Show that $f \in R[X]$ is a unit if and only the constant term a_0 is a unit in R and the other coefficients are nilpotent.
iii) Find the units of degree 1 in $\mathbb{Z}_{12}[X]$.
iv) If R is a domain, the units in $R[X]$ are the units in R.
v) If F is a field, the units in $F[X]$ are the nonzero constants.

Like the factor set, the factor group, the factor ring, and the ring of fractions, the polynomial ring also satisfies a universal property.

Theorem 2.6.13 *Let R be a commutative ring, $R[X]$ the polynomial ring, and $\varphi : R \longrightarrow R[X]$ the canonical injection. Then for any commutative ring A, any ring morphism $\psi : R \longrightarrow A$, and any $x \in A$, there exists a unique ring morphism $\theta : R[X] \longrightarrow A$ such that $\theta(X) = x$ and $\theta\varphi = \psi$, i.e. such that the diagram*



is commutative.

Exercise 2.6.14 *Prove Theorem 2.6.13.*
(Hint: If $f \in R[X]$, $f = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} \varphi(a_i) X^i$, put $\theta(f) = \sum_{i=0}^{n} \psi(a_i) x^i$.)

The universal property may be used to produce new examples of rings. If we take $R = \mathbb{Z}$, $A = \mathbb{C}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ the inclusion, and $x = i$, we denote $Im(\theta)$ by $\mathbb{Z}[i]$, and call it the ring of Gauss integers. Using the fact that $i^2 = -1$, we have

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Now take $R = \mathbb{Z}$, $A = \mathbb{C}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ the inclusion, and $x = i\sqrt{3}$. We denote $Im(\theta)$ by $\mathbb{Z}[i\sqrt{3}]$. Using the fact that $(i\sqrt{3})^2 = -3$, we have

$$\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}.$$

If we take $R = \mathbb{Z}$, $A = \mathbb{R}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{R}$ the inclusion, and $x = \sqrt{2}$, we denote $Im(\theta)$ by $\mathbb{Z}[\sqrt{2}]$. Using the fact that $(\sqrt{2})^2 = 2$, we have

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Exercise 2.6.15 *Show that $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{3}]$, and $\mathbb{Z}[\sqrt{2}]$ are domains, and that their fields of fractions are (in order):*

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

$$\mathbb{Q}(i\sqrt{3}) = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Q}\},$$

and

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

The following result is a partial version for rings of Proposition 1.1.14 and Proposition 1.5.9:

Proposition 2.6.16 *Let $f : R \longrightarrow R'$ be a morphism of commutative rings. Then the following assertions hold:*
i) f is injective if and only if given any commutative ring A, and ring morphisms $g, h : A \longrightarrow R$ such that $fg = fh$, it follows that $g = h$.
ii) If f is surjective, then given any commutative ring A, and ring morphisms $g, h : R' \longrightarrow A$ such that $gf = hf$, it follows that $g = h$.

Proof: i) If f is injective, the condition holds by Proposition 1.1.14 or Proposition 1.5.9. Conversely, assume that the condition holds and $x_1, x_2 \in R$ are distinct elements such that $f(x_1) = f(x_2)$. We take $A = R[X]$, and use Theorem 2.6.13 to find ring morphisms $g, h : R[X] \longrightarrow R$ such that $g(X) = x_1$ and $h(X) = x_2$. Then $g \neq h$, but $fg = fh$, a contradiction.
ii) If f is surjective, the condition holds by Proposition 1.1.14 or Proposition 1.5.9. ∎

Remark 2.6.17 *The converse of Proposition 2.6.16 ii) is false, because the inclusion $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ satisfies the condition, but is not surjective. Indeed, if A is a commutative ring, and $g, h : \mathbb{Q} \longrightarrow A$ such that $gf = hf$, let $\frac{a}{b} \in \mathbb{Q}$. Then*

$$\begin{aligned}
g\left(\frac{a}{b}\right) &= g\left(\frac{a}{1} \cdot \frac{1}{b}\right) \\
&= g\left(\frac{a}{1}\left(\frac{b}{1}\right)^{-1}\right) \\
&= g\left(\frac{a}{1}\right) g\left(\left(\frac{b}{1}\right)^{-1}\right) \\
&= gf(a)gf(b)^{-1} \\
&= hf(a)hf(b)^{-1} \\
&= h\left(\frac{a}{1}\right) h\left(\left(\frac{b}{1}\right)^{-1}\right) \\
&= h\left(\frac{a}{1}\left(\frac{b}{1}\right)^{-1}\right) \\
&= h\left(\frac{a}{1} \cdot \frac{1}{b}\right) \\
&= h\left(\frac{a}{b}\right),
\end{aligned}$$

so $g = h$.

Another application of the universal property is the definition of a polynomial function. If $a \in R$, by the universal property there exists a ring morphism $\theta : R[X] \longrightarrow R$ such that $\theta(X) = a$. If $f \in R[X]$, we will denote $\theta(f)$ by $f(a)$ (when we do this we say that we specialize X to a). In this way, the polynomial f defines a function $\tilde{f} : R \longrightarrow R$, $\tilde{f}(x) = f(x)$ for $x \in R$. If $f = a_0 + a_1X + a_2X^2 + \ldots a_nX^n$, we have that

$$\tilde{f}(x) = f(x) = a_0 + a_1x + a_2x^2 + \ldots a_nx^n.$$

Note that in this notation, x is a variable, it can be any element of R. For polynomial functions, unlike polynomials, it is no longer true that if $\tilde{f} = 0_R$ (the constant function 0_R) then all coefficients are also equal to zero. An example is the polynomial function associated to the polynomial $f = X^2 + X \in \mathbb{Z}_2[X]$. The associated function is $\tilde{f} : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$, $\tilde{f}(x) = x^2 + x$ for $x \in \mathbb{Z}_2$. Then $\tilde{f}(0) = 0^2 + 0 = 0$, and $\tilde{f}(1) = 1^2 + 1 = 1 + 1 = 0$, so $\tilde{f} = 0$, even though $f \neq 0$. As we will see later (look after Exercise 3.3.9), this cannot happen if R is an infinite domain. Note that in general f is a function from $\mathbb{N}$ to R, while $\tilde{f}$ is a function from R to R (or from A to A, where A is a ring to which we have a ring morphism from R). Sometimes the polynomial functions are called simply polynomials. For example, the "polynomials" studied in high school are in fact polynomial functions.

Exercise 2.6.18 *Let I be an ideal of R. We denote by $IR[X]$ the ideal of $R[X]$ generated by the set I:*

$$IR[X] = \{a_1f_1 + \ldots + a_kf_k \mid k \geq 1, a_i \in I, f_i \in R[X], 1 \leq i \leq k\}.$$

i) Show that $IR[X]$ is an ideal of $R[X]$.
ii) Show that $R[X]/(IR[X]) \simeq (R/I)[X]$.
iii) If P is a prime ideal of R, show that $PR[X]$ is a prime ideal of $R[X]$.

Exercise 2.6.19 *Let R be a commutative ring, $h \in R$ not a zero divisor, and $S = \{1, h, h^2, \ldots\}$. Then*

$$S^{-1}R \simeq R[X]/((hX - 1_R)R[X]),$$

where $(hX - 1_R)R[X]$ denotes the principal ideal of $R[X]$ generated by $hX - 1_R$:

$$(hX - 1_R)R[X] = \{(hX - 1_R)f \mid f \in R[X]\}.$$

Definition 2.6.20 *If F is a field, the field of fractions of the domain $F[X]$ is denoted by $F(X)$ and is called the* field of rational fractions in one indeterminate with coefficients in F.

Exercise 2.6.21 *Show that the field of fractions of the domain* $\mathbb{Z}[X]$ *is* $\mathbb{Q}(X)$.

Solutions to the Exercises on Section 2.6

Exercise 2.6.3 *Check that the canonical injection*

$$\varphi : R \longrightarrow R[[X]], \;\; \varphi(a) = (a, 0_R, \ldots)$$

is an injective ring morphism.
Solution: We have $\varphi(a+b) = (a+b, 0_R, \ldots) = (a, 0_R, \ldots) + (b, 0_R, \ldots) = \varphi(a) + \varphi(b)$, and $\varphi(ab) = (ab, 0_R, \ldots) = (a, 0_R, \ldots)(b, 0_R, \ldots) = \varphi(a)\varphi(b)$. It is also clear that $\varphi(1_R) = (1_R, 0_R, \ldots) = 1_{R[[X]]}$, and $Ker(\varphi) = \{0_R\}$, so φ is injective.

Exercise 2.6.6 *Check that $R[X]$ is a subring of $R[[X]]$.*
Solution: Clearly $(1_R, 0_R, \ldots) \in R[X]$. If $f, g \in R[X]$, assume that the coefficients of X^k in f and g are zero for $k \geq n$. Then the coefficient of X^k in $f+g$ is zero for $k \geq n$, and the coefficient of X^k in fg is zero for $k \geq 2n$.

Exercise 2.6.7 *Why are the coefficients of a polynomial unique?*
Solution: A polynomial is a function defined on $\mathbb{N}$ with values in the ring R. The coefficients of the polynomial are the values of the function.

Exercise 2.6.9 *Let $f, g \in R[X]$, $f, g \neq 0_R$. Then, if $f+g$ and fg are nonzero, we have:*
i) $deg(f+g) \leq max\{deg(f), deg(g)\}$. Give an example when we have $=$ and an example when we have $<$.
ii) $deg(fg) \leq deg(f) + deg(g)$. Give an example when we have $=$ and an example when we have $<$.
Solution: Let $f = a_0 + a_1X + \ldots + a_nX^n$, and $g = b_0 + b_1X + \ldots + b_mX^m$, where a_n, b_m are nonzero.
i) The coefficient of X^k in $f+g$ is equal to $a_k + b_k$, so if $k > max\{n, m\}$ it is zero. If $f = X, g = 1 \in \mathbb{R}[X]$, then $f+g = X+1$ has degree $1 = max\{1, 0\}$. If $f = -X + 1, g = X \in \mathbb{Z}_2[X]$, then $f + g = 1$ has degree $0 < max\{1, 1\}$.
ii) The coefficient of X^k in fg is equal to $\sum_{i+j=k} a_ib_j$, so if $k > n + m$ it is zero. If $f = X, g = 1 \in \mathbb{R}[X]$, then $fg = X$ has degree $1 = 1 + 0$. If $f = 2X + 1, g = 2X \in \mathbb{Z}_4[X]$, then $fg = 2X$ has degree $1 < 1 + 1$.

Exercise 2.6.10 *i) Show that $f \in R[X]$ is a zero divisor if and only if there exists $a \in R$, $a \neq 0_R$ such that $af = 0_R$.*
ii) Find the zero divisors of degree 2 in $\mathbb{Z}_6[X]$.
iii) If R is a domain, then $R[X]$ is a domain.
Solution: i) (Scott) Let $f = a_0 + a_1X + \ldots + a_nX^n$. Assume that $fg = 0_R$, $g \neq 0_R$, $deg(g) = m$ and m is the least possible. If $g = b_0 + b_1X + \ldots + b_mX^m$, then $a_nb_m = 0_R$, and since $f(a_ng) = 0_R$ it follows that $a_ng = 0_R$

by the minimality of m. We now write $0_R = fg = a_nX^ng + a_{n-1}X^{n-1}g + \ldots + a_1Xg + a_0g$, and since $a_ng = 0_R$, we get $a_{n-1}b_m = 0_R$, and so again $a_{n-1}g = 0_R$ by the minimality of m. We continue until we get $a_ig = 0_R$ for $i = 0, \ldots, n$, which means $b_mf = 0_R$, i.e. $m = 0$. The converse implication is obvious.
ii) If $f = aX^2 + bX + c \in \mathbb{Z}_6$, $a \neq 0$, is a zero divisor, by i), there is a $d \neq 0$ in $\mathbb{Z}_6$ such that $ad = bd = cd = 0$. If $d = 2$ or $d = 4$, we have that $a = 3$, b is 0 or 3, and c is 0 or 3, so in this case we have $1 \cdot 2 \cdot 2 = 4$ polynomials: $3X^2$,$3X^2+3$, $3X^2+3X$, and $3X^2+3X+3$. If $d = 3$ we have that a is 2 or 4, b is 0 or 2 or 4, and c is 0 or 2 or 4, so in this case we have $2\cdot3\cdot3 = 18$ polynomials: $2X^2$, $2X^2+2$, $2X^2+4$, $2X^2+2X$, $2X^2+2X+2$, $2X^2+2X+4$, $2X^2+4X$, $2X^2+4X+2$, $2X^2+4X+4$, $4X^2$, $4X^2+2$, $4X^2+4$, $4X^2+2X$, $4X^2+2X+2$, $4X^2+2X+4$, $4X^2+4X$, $4X^2+4X+2$, and $4X^2+4X+4$.
iii) This is easy, it does not require the use of i): if f and g are nonzero polynomials, $a_n \neq 0_R$ and $b_m \neq 0_R$ are their respective leading coefficients, then $a_nb_m \neq 0_R$ is the leading coefficient of fg.

Exercise 2.6.11 *An element $a \in R$ is called* nilpotent *if there exists $n \in \mathbb{N}$ such that $a^n = 0_R$.*
i) Show that the set of nilpotent elements in R is an ideal, called the nilradical *of R, and denoted by $\mathcal{N}(R)$.*
ii) Find the nilpotent elements in $\mathbb{Z}_{12}$.
iii) Show that $f \in R[X]$ is nilpotent if and only if all its coefficients are nilpotent.
iv) Find the nilpotents of degree 1 in $\mathbb{Z}_{12}[X]$.
Solution: i) It is clear that 0_R is nilpotent, and if $a^n = 0_R$, then $(ax)^n = a^nx^n = 0_R$ for any $x \in R$. If $a^n = 0_R$ and $b^m = 0_R$, then by Exercise 2.1.2 iv) we have that $(a+b)^k = 0_R$ for any $k > n+m$.
ii) It is easy to see that if $a \in \mathbb{Z}_{12}$ is nilpotent, then a has to be divisible by both 2 and 3, so 6 and 0 are the only nilpotent elements in $\mathbb{Z}_{12}$.
iii) Let $f = a_0 + a_1X + \ldots + a_nX^n$. Assume that $a_i \in \mathcal{N}(R) \subseteq \mathcal{N}(R[X])$ for $0 \leq i \leq n$. Then $a_iX^i \in \mathcal{N}(R[X])$, so $f = \sum_{i=0}^{n} a_iX^i \in \mathcal{N}(R[X])$. Conversely, assume $f \in \mathcal{N}(R[X])$, $f^k = 0_R$. Then the leading coefficient of f^k is $a_n^k = 0_R$. So $a_n \in \mathcal{N}(R) \subseteq \mathcal{N}(R[X])$, and therefore $a_nX^n \in \mathcal{N}(R[X])$. Thus $f - a_nX^n \in \mathcal{N}(R[X])$, and we can continue until we get $a_0 \in \mathcal{N}(R)$.
iv) By iii), a nilpotent polynomial of degree 1 in $\mathbb{Z}_{12}[X]$ is of the form $aX + b$, where a, b are nilpotent and $a \neq 0$. By ii) we get that $a = 6$ and $b = 0$ or $b = 6$. In conclusion, there are two nilpotent polynomials of degree 1 in $\mathbb{Z}_{12}[X]$: $6X$ and $6X + 6$.

Exercise 2.6.12 *i) Show that if u is a unit and x is nilpotent, then $u+x$ is a unit.*
ii) Show that $f \in R[X]$ is a unit if and only the constant term a_0 is a unit in R and the other coefficients are nilpotent.
iii) Find the units of degree 1 in $\mathbb{Z}_{12}[X]$.
iv) If R is a domain, the units in $R[X]$ are the units in R.
v) If F is a field, the units in $F[X]$ are the nonzero constants.
Solution: i) Since $u+x = u(1+u^{-1}x)$ and $u^{-1}x$ is nilpotent, we can assume $u = 1$. If $x^n = 0$, then $1 = 1-(-x)^n = (1+x)(1-x+\ldots+(-x)^{n-1})$ so $1+x$ is a unit.
ii) Let $f = a_0 + a_1X + \ldots + a_nX^n$. Assume that $a_0 \in U(R)$ and $a_i \in \mathcal{N}(R)$ for $1 \leq i \leq n$. We have that $a_iX^i \in \mathcal{N}(R[X])$ and $a_0 \in U(R) \subseteq U(R[X])$, so by i) $f \in U(R[X])$. Conversely, let $g = b_0 + b_1X + \ldots + b_mX^m$, $fg = 1_R$. We have $a_0b_0 = 1_R$, so $a_0 \in U(R)$. Then $a_nb_m = 0_R$ and $a_nb_{m-1} + a_{n_1}b_m = 0_R$. Multiplying the second equality by a_n and using the first, we get $a_n^2b_{m-1} = 0_R$. We continue until we get $a_n^{m+1}b_0 = 0_R$, and since b_0 is a unit we get that a_n is nilpotent. Now a_nX^n is also nilpotent, so $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} = f - a_nX^n$ is a unit by i). We continue as before until we get that $a_{n-1}, \ldots, a_1$ are nilpotent.
iii) By ii), a unit of degree 1 is of the form $aX + b$, where $b \in \mathbf{U}_{12} = \{1, 5, 7, 11\}$ and $a \neq 0$ is nilpotent, i.e. $a = 6$. In conclusion, there are four units of degree one in $\mathbb{Z}_{12}[X]$: $6X+1$, $6X+5$, $6X+7$, and $6X+11$.
iv) A domain does not have any nilpotent elements different from zero.
v) The units in a field are all nonzero elements.

Exercise 2.6.14 *Prove Theorem 2.6.13.*
(Hint: If $f \in R[X]$, $f = \sum_{i=0}^{n} a_iX^i = \sum_{i=0}^{n} \varphi(a_i)X^i$, put $\theta(f) = \sum_{i=0}^{n} \psi(a_i)x^i$.)
Solution: We check that the map θ defined in the hint is a ring morphism that takes X to x and satisfies $\theta\varphi = \psi$. First, $\theta(\varphi(a)) = \psi(a)$ for $a \in R$, so $\theta\varphi = \psi$ and in particular $\theta(1_R) = 1_A$. If $g \in R[X]$, $g = \sum_{i=0}^{n} b_iX^i = \sum_{i=0}^{n} \varphi(b_i)X^i$ (here n is actually the maximum of $deg(f)$ and $deg(g)$, and we complete with zero coefficients the polynomial of smaller degree), then

$$\theta(f+g) = \sum_{i=0}^{n} \psi(a_i+b_i)x^i = \sum_{i=0}^{n} (\psi(a_i)+\psi(b_i))x^i = \theta(f) + \theta(g),$$

and

$$\theta(fg) = \sum_{i=0}^{2n} \psi(\sum_{j+k=i} a_j b_k) x^i = \sum_{i=0}^{2n} \sum_{j+k=i} \psi(a_j)\psi(b_k)x^i = \theta(f)\theta(g).$$

To prove uniqueness, let θ' be a ring morphism that takes X to x and satisfies $\theta'\varphi = \psi$. Then

$$\theta'(f) = \theta'(\sum_{i=0}^{n} \varphi(a_i)X^i) = \sum_{i=0}^{n} \theta'\varphi(a_i)\theta'(X)^i = \sum_{i=0}^{n} \psi(a_i)x^i = \theta(f).$$

Exercise 2.6.15 *Show that $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{3}]$, and $\mathbb{Z}[\sqrt{2}]$ are domains, and that their fields of fractions are (in order):*

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

$$\mathbb{Q}(i\sqrt{3}) = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Q}\},$$

and

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Solution: $\mathbb{Z}[i]$ and $\mathbb{Z}[i\sqrt{3}]$ are subrings of $\mathbb{C}$, and $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$, so they are all domains (a subring of a field is a domain).
If $a + bi \in \mathbb{Z}[i]$, we denote by $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. We have $a + bi = 0 \Leftrightarrow N(a + bi) = 0 \Leftrightarrow a = b = 0$ (because if $b \neq 0$, then $i = ab^{-1} \in \mathbb{Q}$, a contradiction). If we denote by K the field of fractions of $\mathbb{Z}[i]$, then we have

$$\begin{aligned}
K &= \left\{ \frac{a+bi}{c+di} \middle| c + di \neq 0 \right\} \\
&= \left\{ \frac{(a+bi)(c-di)}{(c+di)(c-di)} \middle| c + di \neq 0 \right\} \\
&= \left\{ \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} \middle| c + di \neq 0 \right\} \\
&= \left\{ \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i \middle| c^2 + d^2 \neq 0 \right\} \\
&= \{a + bi \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(i)
\end{aligned}$$

If $a + bi \in \mathbb{Z}[i\sqrt{3}]$, we denote by $N(a + bi\sqrt{3}) = (a + bi\sqrt{3})(a - bi\sqrt{3}) = a^2 + 3b^2$. We have $a + bi\sqrt{3} = 0 \Leftrightarrow N(a + bi\sqrt{3}) = 0 \Leftrightarrow a = b = 0$ (because

if $b \neq 0$, then $i\sqrt{3} = ab^{-1} \in \mathbb{Q}$, a contradiction). If we denote by K the field of fractions of $\mathbb{Z}[i\sqrt{3}]$, then we have

$$\begin{aligned} K &= \left\{ \frac{a+bi\sqrt{3}}{c+di\sqrt{3}} \middle| c+di\sqrt{3} \neq 0 \right\} \\ &= \left\{ \frac{(a+bi\sqrt{3})(c-di\sqrt{3})}{(c+di\sqrt{3})(c-di\sqrt{3})} \middle| c+di\sqrt{3} \neq 0 \right\} \\ &= \left\{ \frac{(ac+bd)+(bc-ad)i\sqrt{3}}{c^2+3d^2} \middle| c+di\sqrt{3} \neq 0 \right\} \\ &= \left\{ \frac{ac+bd}{c^2+3d^2} + \frac{bc-ad}{c^2+3d^2} i\sqrt{3} \middle| c^2+3d^2 \neq 0 \right\} \\ &= \{a+bi\sqrt{3} \mid a,b \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{3}) \end{aligned}$$

If $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, we denote by $N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2-2b^2$. We have $a+b\sqrt{2}=0 \Leftrightarrow N(a+b\sqrt{2})=0 \Leftrightarrow a=b=0$ (because if $b \neq 0$, then $\sqrt{2} = -ab^{-1} \in \mathbb{Q}$, a contradiction). If we denote by K the field of fractions of $\mathbb{Z}[\sqrt{2}]$, then we have

$$\begin{aligned} K &= \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \middle| c+d\sqrt{2} \neq 0 \right\} \\ &= \left\{ \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})} \middle| c+d\sqrt{2} \neq 0 \right\} \\ &= \left\{ \frac{(ac+bd)+(bc-ad)\sqrt{2}}{c^2-2d^2} \middle| c+d\sqrt{2} \neq 0 \right\} \\ &= \left\{ \frac{ac+bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} \middle| c^2-2d^2 \neq 0 \right\} \\ &= \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}) \end{aligned}$$

Exercise 2.6.18 *Let I be an ideal of R. We denote by $IR[X]$ the ideal of $R[X]$ generated by the set I:*

$$IR[X] = \{a_1f_1 + \ldots + a_kf_k \mid k \geq 1, a_i \in I, f_i \in R[X], 1 \leq i \leq k\}.$$

i) Show that $IR[X]$ is an ideal of $R[X]$.
ii) Show that $R[X]/(IR[X]) \simeq (R/I)[X]$.
iii) If P is a prime ideal of R, show that $PR[X]$ is a prime ideal of $R[X]$.
Solution: i) See Exercise 2.2.8.

ii) We have that $f \in IR[X] \Leftrightarrow$ all coefficients of f are in I. Let $\theta : R[X] \longrightarrow (R/I)[X]$ be the ring morphism (from the universal property of polynomial rings) that sends X to X. If $f \in R[X]$, $f = \sum_{i=0}^{n} a_i X^i$, $\theta(f) = \sum_{i=0}^{n} (a_i + I)X^i$. It is clear that θ is surjective, and $f \in Ker(\theta) \Leftrightarrow f \in IR[X]$. The result follows from Corollary 2.3.9.
iii) P is prime $\Rightarrow R/P$ is a domain $\Rightarrow (R/P)[X]$ is a domain $\Rightarrow PR[X]$ is prime.

Exercise 2.6.19 *Let R be a commutative ring, $h \in R$ not a zero divisor, and $S = \{1, h, h^2, \ldots\}$. Then*

$$S^{-1}R \simeq R[X]/((hX - 1_R)R[X]),$$

where $(hX - 1_R)R[X]$ denotes the principal ideal of $R[X]$ generated by $hX - 1_R$:

$$(hX - 1_R)R[X] = \{(hX - 1_R)f \mid f \in R[X]\}.$$

Solution: Let θ be the ring morphism (from the universal property of polynomial rings) $\theta : R[X] \longrightarrow S^{-1}R$, $\theta(X) = \frac{1_R}{h}$. It is clear that θ is surjective, since $\frac{a}{h^n} = \theta(aX^n)$. It is also clear that $(Xh - 1_R) \subseteq Ker(\theta)$. Let now $f \in Ker(\theta)$, $f = \sum_{i=0}^{n} a_i X^i$. It follows that $a_0 h^n + a_1 h^{n-1} + \ldots + a_{n-1}h + a_n = 0_R$. Then $fh^n = fh^n - (a_0 h^n + a_1 h^{n-1} + \ldots + a_{n-1}h + a_n) = (Xh - 1_R)g$, where $g = \sum_{i=0}^{n-1} b_i X^i \in R[X]$. We identify coefficients in $fh^n = (Xh - 1_R)g$ starting with the free term, and we get $a_0 h^n = -b_0$, i.e. $b_0 = -h^n a_0$. Then $a_1 h^n = -a_0 h^{n+1} - b_1$, so $b_1 = h^n c_1$ for some $c_1 \in R$. We continue and find that $b_i = h^n c_i$ for $0 \leq i \leq n-1$, i.e. $g = h^n e$. We get $h^n(f - (Xh - 1_R)e) = 0_R$. Since h is not a zero divisor in R, it follows that h^n is not a zero divisor in R, hence in $R[X]$, and so $f = (Xh - 1_R)e \in (Xh - 1_R)$. We proved that $Ker(\theta) = (Xh - 1_R)$, and the assertion follows from Corollary 2.3.9.

Exercise 2.6.21 *Show that the field of fractions of the domain $\mathbb{Z}[X]$ is $\mathbb{Q}(X)$.*
Solution: The field of fractions of $\mathbb{Z}[X]$ is clearly contained in $\mathbb{Q}(X)$. To check the reverse inclusion, take $\frac{f}{g}$, where $f, g \in \mathbb{Q}[X]$, $g \neq 0$, and write

$\frac{f}{g} = \frac{mf}{mg}$, where m is a common multiple of all denominators of coefficients of f and g.

2.7 Symmetric polynomials

Recall that all rings in sight are commutative. We start this section by considering polynomials in more than one indeterminate. It should be clear (after thinking about it for a moment), that the letter we used to denote the indeterminate does not matter. In other words, if R is a commutative ring, then the polynomial ring in one indeterminate with coefficients in R can be denoted by $R[X]$ or $R[Y]$, which actually represent the same object: the set of functions of finite support from $\mathbb{N}$ to R, which becomes a ring with the operations defined in Definition 2.6.5. Alternatively, we can show that $R[X]$ and $R[Y]$ are isomorphic using Theorem 2.6.13: the isomorphism is the unique ring morphism from $R[X]$ to $R[Y]$ which acts as the identity on R and sends X to Y. If we start now with the commutative ring R, form the polynomial ring $R[X]$ in one indeterminate with coefficients in R, then form the polynomial ring in one indeterminate with coefficients in $R[X]$, $R[X][Y]$, is it clear that this is the same thing (or at least isomorphic to) $R[Y][X]$? If this is clear, then we will denote this ring by $R[X,Y]$ and we will call it the ring of polynomials in two indeterminates with coefficients in R. If this is not clear, we can define recurrently the ring of polynomials in n indeterminates with coefficients in R by using induction and the next result:

Proposition 2.7.1 *If $R \simeq S$ as rings, then $R[X] \simeq S[X]$ as rings.*

Exercise 2.7.2 *Prove Proposition 2.7.1.*

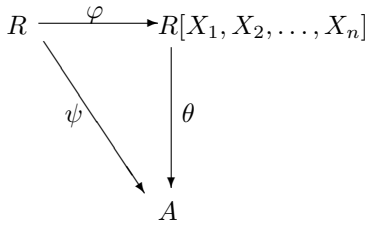
Definition 2.7.3 *We can now use induction and Proposition 2.7.1 in order to define the polynomial ring in n indeterminates with coefficients in R as:*

$$R[X_1, X_2, \ldots, X_n] = R[X_1, X_2, \ldots, X_{n-1}][X_n],$$

for $n > 1$. We denote by $\varphi : R \longrightarrow R[X_1, X_2, \ldots, X_n]$ the composition of the n canonical injections, and we also call it the canonical injection.

The ring of polynomials in n indeterminates with coefficients in R satisfies the following universal property, which can be proved using induction on n and Theorem 2.6.13:

Theorem 2.7.4 *Let R be a commutative ring, $R[X_1, X_2, \ldots, X_n]$ the polynomial ring in n indeterminates with coefficients in R, and $\varphi : R \longrightarrow R[X_1, X_2, \ldots, X_n]$ the canonical injection. Then for any commutative ring A, any ring morphism $\psi : R \longrightarrow A$, and elements $x_i \in A$, $1 \leq i \leq n$, there exists a unique ring morphism $\theta : R[X_1, X_2, \ldots, X_n] \longrightarrow A$ such that $\theta(X_i) = x_i$, $1 \leq i \leq n$, and $\theta\varphi = \psi$, i.e. such that the diagram*



is commutative.

Definition 2.7.5 *We call* $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n} \in R[X_1, X_2, \dots, X_n]$ *a* monomial*, and the natural number* $k_1 + k_2 + \dots + k_n$ *its* degree*.*

It can be shown that a polynomial $f \in R[X_1, X_2, \dots, X_n]$ can be written uniquely as a sum of monomials. The maximum degree of these monomials is called the *degree* of f and is denoted by $deg(f)$.

Definition 2.7.6 *A polynomial* $f \in R[X_1, X_2, \dots, X_n]$ *is called* homogeneous *if all monomials in the decomposition of* f *as a sum of monomials have the same degree (which has to be* $deg(f)$*).*

We now define symmetric polynomials.

Exercise 2.7.7 *If* R *is a ring, the set*

$$Aut(R) = \{f : R \longrightarrow R \mid f \text{ is a ring isomorphism}\}$$

is a group under the composition of functions.

Definition 2.7.8 *We say that the group* G acts as automorphisms *on the ring* R *if there exists a group morphism* $G \longrightarrow Aut(R)$*, which is called an* action *of* G *on* R*. If this is the case, the image of* $g \in G$ *through the action will send the element* $a \in R$ *to* $a^g \in R$*, and we denote by*

$$R^G = \{a \in R \mid a^g = a,\ \forall g \in G\}.$$

Exercise 2.7.9 *If the group* G *acts on the ring* R *as automorphisms,* R^G *is a subring of* R*. (We call it the* ring of invariants*).*

We can use Theorem 2.7.4 to define an action of the symmetric group S_n on the polynomial ring $R[X_1, X_2, \dots, X_n]$. We do this as follows: after we fix $\sigma \in S_n$, we take in Theorem 2.7.4 $A = R[X_1, X_2, \dots, X_n]$, $f = \varphi$, and $x_i = X_{\sigma(i)}$ for $1 \leq i \leq n$. We obtain a θ_σ that defines the action by $f^\sigma = \theta_\sigma(f)$.

Definition 2.7.10 *The elements of* $R[X_1, X_2, \dots, X_n]^{S_n}$ *are called* symmetric polynomials*.*

The following symmetric polynomials are called the *fundamental symmetric polynomials*:

$$s_1 = X_1 + X_2 + \ldots + X_n$$
$$s_2 = X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n$$
$$s_3 = X_1X_2X_3 + X_1X_2X_4 + \ldots + X_{n-2}X_{n-1}X_n$$
$$\vdots$$
$$s_{n-1} = X_1X_2\ldots X_{n-1} + X_1X_2\ldots X_{n-2}X_n + \ldots X_2X_3\ldots X_n$$
$$s_n = X_1X_2\ldots X_n$$

We note that the fundamental symmetric polynomials are homogeneous, and $deg(s_k) = k$, $1 \leq k \leq n$.

We prove now the fundamental theorem of symmetric polynomials:

Theorem 2.7.11 *Every symmetric polynomial $f \in R[X_1, X_2, \ldots, X_n]^{S_n}$ can be written uniquely as a polynomial of the fundamental symmetric polynomials, i.e. there exists a unique $g \in R[X_1, X_2, \ldots, X_n]$ such that $f = g(s_1, s_2, \ldots, s_n)$.*

Proof: Note that $g(s_1, s_2, \ldots, s_n) = \theta(g)$, where $\theta : R[X_1, X_2, \ldots, X_n] \longrightarrow R[X_1, X_2, \ldots, X_n]$ is the unique ring morphism (obtained from Theorem 2.7.4) that is the identity on R and sends X_k to s_k, $1 \leq k \leq n$. In terms of θ, the two assertions of the theorem are:
i) θ is injective.
ii) $Im(\theta) = R[X_1, X_2, \ldots, X_n]^{S_n}$.
We define the lexicographical order on $\mathbb{N}^n$ as follows: we say that

$$(k_1, k_2, \ldots, k_n) > (l_1, l_2, \ldots, l_n)$$

if $k_i > l_i$ for the first i for which they differ.

We first prove i). Let $f \in Ker(\theta)$, $f \neq 0$. It follows that f is a finite sum of monomials, of which at least one is not 0. To each of these monomials, which are of the form $aX_1^{k_1}X_2^{k_2}\ldots X_n^{k_n}$, we associate the element

$$(k_1 + k_2 + \ldots + k_n, k_2 + k_3 + \ldots + k_n, \ldots, k_{n-1} + k_n, k_n) \in \mathbb{N}^n,$$

which we also use to denote the greatest such element in the lexicographical order. Then, in the polynomial $\theta(f) = f(s_1, s_2, \ldots, s_n)$, the nonzero monomial $aX_1^{k_1+k_2+\ldots+k_n}X_2^{k_2+k_3+\ldots+k_n}\ldots X_n^{k_n}$ has the greatest associated n-tuple in the lexicographical order and so it will not cancel with any other monomial. In other words, $\theta(f) \neq 0$, and we proved i).

Now we prove ii). It is enough to assume that f is a homogeneous symmetric polynomial, as its homogeneous components also have to be

symmetric. After proving ii) for the homogeneous components of f we can take the sum of the g-s as the final g for f. We write f as a sum of monomials of the form $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$, and we pick the monomial with the property that $(k_1, k_2, \dots, k_n) \in \mathbb{N}^n$ is the greatest in the lexicographical order. It is clear that we have that $k_1 \geq k_2 \geq \dots \geq k_n$, because f is symmetric, and if $k_i < k_{i+1}$, then the monomial $aX_1^{k_1}X_2^{k_2}\dots X_i^{k_{i+1}}X_{i+1}^{k_1}\dots X_n^{k_n}$ has

$$(k_1, k_2, \dots, k_{i+1}, k_i, \dots, k_n) > (k_1, k_2, \dots, k_i, k_{i+1}, \dots, k_n).$$

Then we consider the polynomial $f - as_1^{k_1-k_2}s_2^{k_2-k_3}\dots s_n^{k_n}$. This is also a symmetric polynomial, of the same degree as f (if it's not 0), and in it the monomial with the greatest n-tuple in the lexicographical order cancelled. We repeat the procedure, which will end after a finite number of steps, and we get that our g is the sum of the monomials $aX_1^{k_1-k_2}X_2^{k_2-k_3}\dots X_n^{k_n}$ considered in each step. ∎

The proof of Theorem 2.7.11 provides an algorithm that we can use to write a symmetric polynomial as a polynomial of the fundamental symmetric polynomials. We show how this works by writing $f = X_1^4 + X_2^4 + X_1^2X_2 + X_1X_2^2$ as a polynomial g of the fundamental symmetric polynomials $s_1 = X_1 + X_2$ and $s_2 = X_1X_2$.

We have that f is a sum of two homogeneous polynomials, $f = f_1 + f_2$, where $f_1 = X_1^4 + X_2^4$, and $f_2 = X_1^2X_2 + X_1X_2^2$.

We first write f_1, which is homogeneous of degree 4, as a polynomial of s_1 and s_2. The greatest pair in the lexicographical order in $\mathbb{N}^2$ is $(4, 0)$. We write all pairs (k_1, k_2) with $k_1 \geq k_2$ and $k_1 + k_2 = 4$. They are:

$$(4, 0) > (3, 1) > (2, 2).$$

Then there exist integers A, B such that

$$f_1 - s_1^4 - As_1^{3-1}s_2^1 - Bs_1^{2-2}s_2^2 = 0.$$

In order to find A, B we plug in values for X_1 and X_2, and solve the linear system with two unknowns and two equations:

X_1	X_2	s_1	s_2	f_1	$f_1 - s_1^4 - As_1^2s_2 - Bs_2^2 = 0$
1	1	2	1	2	$-14 - 4A - B = 0$
2	1	3	2	17	$-64 - 18A - 4B = 0$

We solve the system and find $A = -4$ and $B = 2$. Therefore, we have that

$$f_1 = g_1(s_1, s_2) = s_1^4 - 4s_1^2s_2 + 2s_2^2,$$

so $g_1 = X_1^4 - 4X_1^2X_2 + 2X_2^2$.

We now write f_2, which is homogeneous of degree 3, as a polynomial of s_1 and s_2. The greatest pair in the lexicographical order in $\mathbb{N}^2$ is $(2,1)$. Since there are no other pairs (k_1,k_2) with $k_1 \geq k_2$ and $k_1+k_2=3$ such that $(2,1)>(k_1,k_2)$, it follows that $f_2=g_2(s_1,s_2)=s_1s_2$, and $g_2=X_1X_2$.

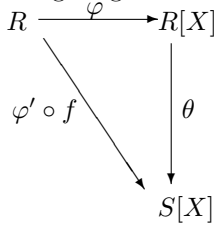
In conclusion, $f=g(s_1,s_2)=s_1^4-4s_1^2s_2+2s_2^2+s_1s_2$, so $g=g_1+g_2X_1^4-4X_1^2X_2+2X_2^2+X_1X_2$.

Exercise 2.7.12 *Write each of the following polynomials as a polynomial of the fundamental symmetric polynomials.*

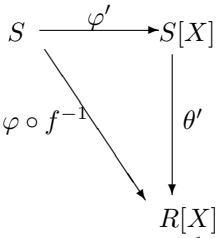
i) $(X_1^2+X_2^2)(X_1^2+X_3^2)(X_2^2+X_3^2)$
ii) $X_1^2X_2+X_1X_2^2+X_1^2X_3+X_1X_3^2+X_2^2X_3+X_2X_3^2$
iii) $(X_1+X_2+X_3)(X_1^2+X_2^2+X_3^2)$
iv) $X_1^4+X_2^4+X_3^4-4(X_1^2X_2X_3+X_1X_2^2X_3+X_1X_2X_3^2)$

Solutions to the Exercises on Section 2.7

Exercise 2.7.2 *Prove Proposition 2.7.1.*
Solution: Suppose $f : R \longrightarrow S$ is a ring isomorphism, and denote by $\varphi : R \longrightarrow R[X]$ and $\varphi' : S \longrightarrow S[X]$ the canonical injections. We let θ denote the ring morphism sending X to X obtained by applying Theorem 2.6.13 to the following diagram:



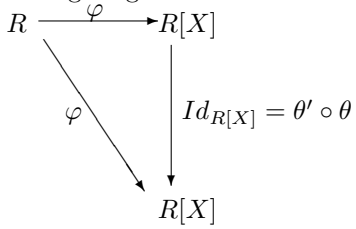
We have that $\theta \circ \varphi = \varphi' \circ f$. Now we let θ' denote the ring morphism sending X to X obtained by applying Theorem 2.6.13 to the following diagram:



We have that $\theta' \circ \varphi' = \varphi \circ f^{-1}$, and therefore

$$\begin{aligned} \theta' \circ \theta \circ \varphi &= \theta' \circ \varphi' \circ f \\ &= \varphi \circ f^{-1} \circ f \\ &= \varphi, \end{aligned}$$

so $Id_{R[X]} = \theta' \circ \theta$ by the uniqueness of the morphism in Theorem 2.6.13 applied to the following diagram.



The fact that $Id_{R[X]} = \theta \circ \theta'$ is proved similarly.

Exercise 2.7.7 *If R is a ring, the set*

$$Aut(R) = \{f : R\ R | f \text{ is a ring isomorphism}\}$$

is a group under the composition of functions.
Solution: The composition of two ring isomorphisms is a ring isomorphism, composition of functions is associative, Id_R is a ring isomorphism, and the inverse of a ring isomorphism is also a ring isomorphism. Note that the group $Aut(R)$ is not necessarily abelian if R is commutative.

Exercise 2.7.9 *If the group G acts on the ring R as automorphisms, R^G is a subring of R. (We call it the* ring of invariants*).*
Solution: It is clear that $1_R \in R^G$, because every ring morphism sends the identity to the identity. Then, if $a, b \in R^G$, we have that $(a-b)^g = a^g - b^g = a - b$, and $(ab)^g = a^g b^g = ab$.

Exercise 2.7.12 *Write each of the following polynomials as a polynomial of the fundamental symmetric polynomials.*

i) $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$
ii) $X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2$
iii) $(X_1 + X_2 + X_3)(X_1^2 + X_2^2 + X_3^2)$
iv) $X_1^4 + X_2^4 + X_3^4 - 4(X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2)$
Solution: We only give a detailed solution for i), then give the answers for ii), iii), and iv).

i)We have to write $f = (X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$, which is homogeneous of degree 6, as a polynomial of s_1, s_2, and s_3. The greatest triple in the lexicographical order in $\mathbb{N}^3$ is $(4, 2, 0)$. We write all pairs (k_1, k_2, k_3) with $k_1 \geq k_2 \geq k_3$ and $k_1 + k_2 + k_3 = 6$. They are:

$$(4, 2, 0) > (4, 1, 1) > (3, 3, 0) > (3, 2, 1) > (2, 2, 2).$$

Then there exist integers A, B, C, D such that

$$f - s_1^2s_2^2 - As_1^3s_3 - Bs_2^3 - Cs_1s_2s_3 - Ds_3^2 = 0. \tag{2.4}$$

In order to find A, B, C, D we plug in values for X_1, X_2, and X_3, and solve the linear system with four unknowns and four equations:

X_1	X_2	X_3	s_1	s_2	s_3	f	(2.4)
1	1	0	2	1	0	2	$-2 - B = 0$
2	-1	-1	0	-3	2	50	$50 + 27B - 4D = 0$
1	-2	-2	-3	0	4	200	$200 + 108A - 16D = 0$
1	-1	-1	-1	-1	1	8	$7 + A + B - C - D = 0$

We solve the system and find $A = -2$, $B = -2$, $C = 4$, and $D = -1$. Therefore, we have that

$$f = g_1(s_1, s_2) = s_1^2 s_2^2 - 2s_1^3 s_3 - 2s_2^3 + 4s_1 s_2 s_3 - s_3^2.$$

ii) $s_1 s_2 - 3s_3$
iii) $s_1^3 - 2s_1 s_2$
iv) $s_1^4 - 4s_1^2 s_2 + 2s_2^2$

Chapter 3

Arithmetic in rings

3.1 Divisibility

From now on we assume that all rings are domains. The following definition is inspired by Definition 1.2.2:

Definition 3.1.1 *Given a domain R, and $a, b \in R$, we say that a divides b (or a is a factor of b, or b is a multiple of a, or b is divisible by a) if there exists $c \in R$ such that $b = ac$. If $a \mid b$ and $b \mid a$, we say that a and b are associated in divisibility, and we write $a \sim_d b$.*

Compare the following exercise to Exercise 1.2.3:

Exercise 3.1.2 *Prove the following:*
i) $1_R \mid a$ *for all* $a \in R$.
ii) $a \mid 0_R$ *for all* $a \in R$.
iii) If $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
iv) If $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
v) If $a \mid b$ *and* $a \mid c$, *then* $a \mid ub + vc$ *for all* $u, v \in R$.
vi) $a \mid 1_R$ *if and only if* $a \in U(R)$.
vii) If $a \sim_d b$, *then* $a = ub$ *for some* $u \in U(R)$.

Definition 3.1.3 *Given a domain R, and $a, b \in R$, we say that $d \in R$ is a* **greatest common divisor** *of a and b (we write $d = (a, b)$) if the following two conditions are satisfied:*
i) $d \mid a$ *and* $d \mid b$.
ii) if $c \mid a$ *and* $c \mid b$, *then* $c \mid d$.

It is clear that $(a, 0_R) = a$ for all $a \in R$, in particular $(0_R, 0_R) = 0_R$.

Exercise 3.1.4 *If $d_1 = (a, b)$ and $d_2 = (a, b)$, then $d_1 \sim_d d_2$, i.e. $d_1 = ud_2$ for some $u \in U(R)$.*

The following definition is inspired by Definition 1.7.15:

Definition 3.1.5 *If R is a domain and $a, b \in R$, we say that m is a* **least common multiple of** *a* **and** *b (and we write $m = [a, b]$) if the following conditions hold:*
i) $a \mid m$ and $b \mid m$.
ii) If $a \mid n$ and $b \mid n$, then $m \mid n$.

It is clear that $[a, 0_R] = 0_R$ for all $a \in R$, in particular $[0_R, 0_R] = 0_R$.

Exercise 3.1.6 *If $m_1 = [a, b]$ and $m_2 = [a, b]$, then $m_1 \sim_d m_2$, i.e. $m_1 = um_2$ for some $u \in U(R)$.*

Compare the following to ii) and iii) of Exercise 1.7.19.

Exercise 3.1.7 *i) If the ideal generated by a and b is principal, generated by d, then $d = (a, b)$.*
ii) If the intersection of the principal ideals generated by a and b is principal, generated by m, then $m = [a, b]$.

The next result shows that the existence of a least common multiple implies the existence of a greatest common divisor, and that if both a least common multiple and a greatest common divisor exist, they are connected as we expect them to be (see Exercise 1.7.16):

Proposition 3.1.8 *If R is a domain, $a, b \in R$,and $[a, b]$ exists, then (a, b) also exists, and we have $ab = (a, b)[a, b]$. (Note that since the greatest common divisor and the least common multiple are not unique, this equality simply means that there exist a greatest common divisor and a least common multiple of a and b whose product is ab.)*

Proof: We can assume that both a and b are nonzero. Let $m = [a, b]$. Since ab is a common multiple of a and b, it follows that $m \mid ab$, so there exists a $d \in R$ such that $dm = ab$.

We show that $d = (a, b)$. We have that $m = a'a$, and so $da'a = ab$, so $d \mid b$ because $a \neq 0_R$. Similarly $d \mid a$.

Now let $c \mid a$ and $c \mid b$. We have that $a = ca_1$ and $b = db_1$. Since ca_1b_1 is a common multiple of a and b, it follows that $m \mid ca_1b_1$, and so $ca_1b_1 = mu$ for some $u \in R$. Therefore we get that $dca_1b_1 = dmu = abu = ca_1cb_1u$, and since $ca_1b_1 \neq 0_R$, we get that $d = cu$, i.e. we proved that $d = (a, b)$. ∎

We now show that two elements having a greatest common divisor do not necessarily have a least common multiple. We will produce two different examples of such pairs, in the two domains described in the following:

Exercise 3.1.9 *i) The set*

$$\mathbb{Z} + X^2\mathbb{Z}[X] = \{a_0 + a_2X^2 + a_3X^3 + \ldots + a_nX^n \mid n \geq 2, a_i \in \mathbb{Z}\}$$

is a subring of the polynomial ring $\mathbb{Z}[X]$, and so it is a domain with the usual addition and multiplication of polynomials.
ii) The set

$$\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$, and so it is a domain.
iii) The function $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$, defined by $N(a+bi\sqrt{5}) = a^2+5b^2$, has the property $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[i\sqrt{5}]$.
iv) $U(\mathbb{Z}[i\sqrt{5}]) = \{-1, 1\}$.

Proposition 3.1.10 *It is possible that two elements have a greatest common divisor, but their least common multiple does not exist.*

Proof: Consider first the elements X^2 and X^3 in $\mathbb{Z} + X^2\mathbb{Z}[X]$, which have a greatest common divisor, namely $1 = (X^2, X^3)$, because they are only divisible by ± 1 and themselves. If they had a least common multiple, by Proposition 3.1.8 we must have $X^2X^3 = X^5 = [X^2, X^3]$. But $X^6 = X^4X^2 = X^3X^3$ is a common multiple, and $X^5 \nmid X^6$. So $[X^2, X^3]$ does not exist. Note that this example shows that Corollary 1.2.8 is not true if we replace $\mathbb{Z}$ with an arbitrary domain: it is clear that no linear combination of X^2 and X^3 will be equal to 1.

Consider now the elements 3 and $1 + i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$. Since no $x \in \mathbb{Z}[i\sqrt{5}]$ can have either $N(x) = 2$ or $N(x) = 3$, it follows that $1 = (3, 1 + i\sqrt{5})$. If $[3, 1 + i\sqrt{5}]$ exists, it has to be $3(1 + i\sqrt{5})$ by Proposition 3.1.8, so $N(3(1 + i\sqrt{5})) = N(3)N(1 + i\sqrt{5}) = 54$. But $6 = 3 \cdot 2 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ is a common multiple, and $6 \nmid 3(1 + i\sqrt{5})$ because $N(6) = 36 \nmid 54$. ∎

Proposition 3.1.11 *If R is a domain, and $a, b, c \in R$, $c \neq 0_R$, have the property that (ac, bc) exists, then (a, b) also exists and $(ac, bc) = (a, b)c$.*

Proof: Let $d = (ac, bc)$. Since c is a common divisor of ac and bc, it follows that $c \mid d$, or $d = cd'$ for some $d' \in R$. We show that $d' = (a, b)$. Since $d'c \mid ac$, $d'c \mid bc$, and $c \neq 0_R$, it follows that $d' \mid a$ and $d' \mid b$. Now if $e \mid a$ and $e \mid b$, it follows that $ec \mod ac$ and $ec \mid bc$, so $ec \mid d = d'c$, therefore $e \mid d'$. ∎

Exercise 3.1.12 *Assume that a and b are not both 0 and $d = (a, b)$. Let $a = da'$ and $b = db'$. Prove that $1_R = (a', b')$.*

The next result shows that the greatest common divisor of two elements might not exist, so Theorem 1.2.7 does not remain true if we try to replace $\mathbb{Z}$ by an arbitrary domain.

Proposition 3.1.13 *It is possible that two elements have a greatest common divisor, but their products with the same element of the domain R do not have a greatest common divisor.*

Proof: As seen in the proof of Proposition 3.1.10, we have that $1 = (X^2, X^3)$ in $\mathbb{Z} + X^2\mathbb{Z}[X]$. If we multiply both of them by X^3, and we assume that (X^5, X^6) exists, it should be X^3 by Proposition 3.1.11. However, X^2 is a common divisor of $X^5 = X^2X^3$ and $X^6 = x^2X^4$, but $X^2 \nmid X^3$. So X^5 and X^6 do not have a greatest common divisor.

Again, we also give an example in $\mathbb{Z}[i\sqrt{5}]$. We have seen in the proof of Proposition 3.1.10 that $1 = (3, 1 + i\sqrt{5})$. If we multiply both of them by $1 - i\sqrt{5}$, and we assume that $(3(1 - i\sqrt{5}), 6)$ exists, it should be $1 - i\sqrt{5}$ by Proposition 3.1.11. However, 3 is a common divisor of $3(1 - i\sqrt{5})$ and 6, but $3 \nmid 1 - i\sqrt{5}$, because $N(3) = 9 \nmid 6 = N(1 - i\sqrt{5})$. So $3(1 - i\sqrt{5})$ and 6 do not have a greatest common divisor. ∎

Definition 3.1.14 *A domain R is called a* **GCD-domain** *if every two elements in R have a greatest common divisor.*

Exercise 3.1.15 *Give two examples of GCD-domains, and two examples of domains which are not GCD-domains.*

Proposition 3.1.10 says that "locally", the existence of a greatest common divisor does not imply the existence of a least common multiple. Here's what happens "globally":

Exercise 3.1.16 *The following assertions are equivalent:*
i) R is a GCD-domain.
ii) Every two elements in R have a least common multiple.

Exercise 3.1.17 *Is the Euclid Lemma (see Theorem 1.2.15) true in any domain? Prove that the Euclid Lemma holds in a GCD-domain.*

Exercise 3.1.18 *(See Exercise 1.2.16.) If $1_R = (a, b)$ and $1_R = (a, c)$, then is it true that $1_R = (a, bc)$ in any domain R? What if R is a GCD-domain?*

Exercise 3.1.19 *(See Exercise 1.2.17.) If $a \mid c$, $b \mid c$, and $1_R = (a, b)$, then is it true that $ab \mid c$ in any domain R? What if R is a GCD-domain?*

Solutions to the Exercises on Section 3.1

Exercise 3.1.2 *Prove the following:*
i) $1_R \mid a$ *for all* $a \in R$.
ii) $a \mid 0_R$ *for all* $a \in R$.
iii) If $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
iv) If $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
v) If $a \mid b$ *and* $a \mid c$, *then* $a \mid ub + vc$ *for all* $u, v \in R$.
vi) $a \mid 1_R$ *if and only if* $a \in U(R)$.
vii) If $a \mid b$ *and* $b \mid a$, *then* $a = ub$ *for some* $u \in U(R)$.
Solution: i) $a = 1_R \cdot a$.
ii) $0_R = a \cdot 0_R$.
iii) We have that $b = ad$ and $c = be = ade$.
iv) We have that $b = ae$ and $d = cf$, so $bd = acef$.
v) We have $b = ad$ and $c = ae$, so $ub + vc = uad + vae = a(ud + ve)$.
vi) We have $1_R = ab$ if and only if $a \in U(R)$.
vii) If both a and b are 0_R, the statement is clear. If one of them is not 0_R, the other one has to be different from 0_R as well. In that case we have $b = au$ and $a = bv = auv$, so $1_R = uv$ because R is a domain and $a \neq 0_R$.

Exercise 3.1.4 *If* $d_1 = (a, b)$ *and* $d_2 = (a, b)$, *then* $d_1 \sim_d d_2$, *i.e.* $d_1 = ud_2$ *for some* $u \in U(R)$.
Solution: Since $d_1 = (a, b)$, $d_2 \mid a$, and $d_2 \mid b$, it follows that $d_2 \mid d_1$. Similarly, $d_1 \mid d_2$, and we use Exercise 3.1.2 vii).

Exercise 3.1.6 *If* $m_1 = [a, b]$ *and* $m_2 = [a, b]$, *then* $m_1 \sim_d m_2$, *i.e.* $m_1 = um_2$ *for some* $u \in U(R)$.
Solution: Since $m_1 = [a, b]$, $a \mid m_2$, and $b \mid m_2$, it follows that $m_1 \mid m_2$. Similarly, $m_2 \mid m_1$, and we use Exercise 3.1.2 vii).

Exercise 3.1.7 *i) If the ideal generated by* a *and* b *is principal, generated by* d, *then* $d = (a, b)$.
ii) If the intersection of the principal ideals generated by a *and* b *is principal, generated by* m, *then* $m = [a, b]$.
Solution: i) Since $a, b \in dR$, d is a common divisor for a and b. If $c \mid a$ and $c \mid b$, then $c \mid d$, which is a linear combination of a and b.
ii) Since $m \in aR \cap bR$, m is a common multiple of a and b. If n is another common multiple, $n \in aR \cap bR = mR$, so $m \mid n$.

Exercise 3.1.9 *i) The set*

$$\mathbb{Z} + X^2\mathbb{Z}[X] = \{a_0 + a_2X^2 + a_3X^3 + \ldots + a_nX^n \mid n \geq 2, a_i \in \mathbb{Z}\}$$

is a subring of the polynomial ring $\mathbb{Z}[X]$, *and so it is a domain with the*

usual addition and multiplication of polynomials.
ii) The set

$$\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$*, and so it is a domain.*
iii) The function $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$*, defined by* $N(a+bi\sqrt{5}) = a^2+5b^2$*, has the property* $N(xy) = N(x)N(y)$ *for all* $x, y \in \mathbb{Z}[i\sqrt{5}]$*.*
iv) $U(\mathbb{Z}[i\sqrt{5}]) = \{-1, 1\}$*.*
Solution: i) is clear.
ii) Take $R = \mathbb{Z}$, $A = \mathbb{C}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ the inclusion, and $x = i\sqrt{5}$ in Theorem 2.6.13. We see that $Im(\theta) = \mathbb{Z}[i\sqrt{5}]$ using the fact that $(i\sqrt{5})^2 = -5$.
iii) If $x = a + bi\sqrt{5}$ and $y = c + di\sqrt{5}$, we have $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$.
iv) The only integer solutions of the equation $a^2 + 5b^2 = 1$ are $a = \pm 1$ and $b = 0$.

Exercise 3.1.12 *Assume that* a *and* b *are not both 0 and* $d = (a, b)$*. Let* $a = da'$ *and* $b = db'$*. Prove that* $1_R = (a', b')$*.*
Solution: Use Proposition 3.1.11.

Exercise 3.1.15 *Give two examples of GCD-domains, and two examples of domains which are not GCD-domains.*
Solution: $\mathbb{Z}$ is a *GCD*-domain by Theorem 1.2.7. Every field is a *GCD*-domain because the greatest common divisor of two elements is 0 if both elements are 0, and 1 if not.

The domains $\mathbb{Z} + X^2\mathbb{Z}[X]$ and $\mathbb{Z}[i\sqrt{5}]$ in Exercise 3.1.9 are not *GCD*-domains by Proposition 3.1.13.

Exercise 3.1.16 *The following assertions are equivalent:*
i) R *is a GCD-domain.*
ii) Every two elements in R *have a least common multiple.*
Solution: ii) $\Rightarrow$ i) follows from Proposition 3.1.8.
i) $\Rightarrow$ ii). Let $a, b \in R$ and assume that they are not 0. We let $d = (a, b)$, and since $a \mid ab$ it follows that $d \mid ab$, or $ab = dm$ for some $m \in R$. We show that $m = [a, b]$. We have that $a = da'$ and $b = db'$. Then $da'b = dm$, so $b \mid m$. Similarly we get that $a \mid m$. Assume now that $a \mid n$ and $b \mid n$. Then $ab \mid nb$ and $ab \mid na$, so $md = ab \mid (na, nb) = n(a, b) = nd$, and therefore $m \mid n$. (Note that this proof is different from the one in Exercise 1.7.16, which does not work in this case.)

Exercise 3.1.17 *Is the Euclid Lemma (see Theorem 1.2.15) true in any domain? Prove that the Euclid Lemma holds in a GCD-domain.*
Solution: No, take $a = X^2$, $b = c = X^3$ in $\mathbb{Z} + X^2\mathbb{Z}[X]$. Then $a \mid bc$,

$1_R = (a, b)$, but $a \nmid c$. If R is a GCD-domain, let $a \mid bc$ and $1_R = (a, b)$. Then, since $a \mid ac$, we have that $a \mid (ac, bc) = (a, b)c = c$.

Exercise 3.1.18 *(See Exercise 1.2.16.) If $1_R = (a, b)$ and $1_R = (a, c)$, then is it true that $1_R = (a, bc)$ in any domain R? What if R is a GCD-domain?*
Solution: No, take $a = X^2$ and $b = c = X^3$ in $\mathbb{Z} + X^2\mathbb{Z}[X]$. Then $1_R = (a, b) = (a, c)$ but $1_R \neq (a, bc)$. If R is a GCD-domain, let $d \mid a$ and $d \mid bc$. Then $(d, b) = 1_R$, and by the Euclid Lemma we get that $d \mid c$. Therefore $d \mid 1_R$ and we are done.

Exercise 3.1.19 *(See Exercise 1.2.17.) If $a \mid c$, $b \mid c$, and $1_R = (a, b)$, then is it true that $ab \mid c$ in any domain R? What if R is a GCD-domain?*
Solution: No, $a = X^2$, $b = X^3$, and $c = X^6$ in $\mathbb{Z} + X^2\mathbb{Z}[X]$. Then $a \mid c$, $b \mid c$, and $1_R = (a, b)$, but $ab \nmid c$. If R is a GCD-domain, let $a \mid c$, $b \mid c$, and $1_R = (a, b)$. Then $ab \mid bc$ and $ab \mid ac$, so $ab \mid (ac, bc) = (a, b)c = c$.

3.2 Prime and irreducible elements

We continue to assume that all rings are domains. The following definition generalizes Definition 1.2.19.

Definition 3.2.1 *Let R be a domain. Then an element $p \neq 0_R$, $p \notin U(R)$, is said to be* **prime** *if from $p \mid ab$ it follows that $p \mid a$ or $p \mid b$.*

Examples of prime elements in $\mathbb{Z}$ are therefore the prime numbers. In the ring $\mathbb{Z} + X^2\mathbb{Z}[X]$ (see Exercise 3.1.9), the element X^2 is not prime, because it divides $X^3X^3 = X^6 = X^2X^4$ but it does not divide X^3. In the ring $\mathbb{Z}[i\sqrt{5}]$, the element 2 is not prime, since it divides $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, but it does not divide either of $1 + i\sqrt{5}$ and $1 - i\sqrt{5}$, because $N(2) = 4 \nmid 6 = N(1 + i\sqrt{5}) = N(1 - i\sqrt{5})$.

Exercise 3.2.2 *If p is prime, and $p \mid a_1a_2 \dots a_n$, then there exists i, $1 \leq i \leq n$ such that $p \mid a_i$.*

Proposition 3.2.3 *The following assertions are equivalent for $p \neq 0_R$, $p \notin U(R)$:*
i) p is prime.
ii) The principal ideal generated by p, pR, is a prime ideal.

Proof: We have that $pR \neq R$, and pR s prime if and only if $ab \in pR$ implies $a \in pR$ or $b \in pR$, i.e. $p \mid ab$ implies $p \mid a$ or $p \mid b$. ∎

Combining Proposition 3.2.3 with Corollary 2.4.6 we get

Corollary 3.2.4 *If $p \neq 0_R$, $p \notin U(R)$, then p is prime if and only if R/pR is a domain.*

Exercise 3.2.5 *If R is a domain, then X is a prime element in the polynomial ring $R[X]$.*

Proposition 3.2.6 *Let $p \in R$ be a prime element. Then p is a prime element in the polynomial ring $R[X]$.*

Proof: We clearly have that $p \neq 0_R$ and $p \notin U(R[X]) = U(R)$ (see Exercise 2.6.12 iv)). By Proposition 3.2.3 we have that pR is a prime ideal, and so $pR[X]$ is a prime ideal by Exercise 2.6.18 iii), which shows that p is prime in $R[X]$, again by Proposition 3.2.3.

We are now going to give a direct proof, using the definition of prime elements. Assume that $p \mid fg$, where $f, g \in R[X]$,

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n, \quad g = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m.$$

If $p \nmid f$ and $p \nmid g$, let k and l be the smallest with the property that $p \nmid a_k$ and $p \nmid b_l$. But then p does not divide the coefficient of X^{k+l} in fg, which is

$$\sum_{i+j=k+l; i\neq k; j\neq l} a_i b_j + a_k b_l,$$

because in each of the terms of the sum one of the factors is divisible by p and $p \nmid a_k b_l$. In conclusion $p \nmid fg$, which is a contradiction. ∎

Exercise 3.2.7 *Let p be a prime element in R, and S a multiplicative set on R such that $pR \cap S = \emptyset$. Then $\frac{p}{1_R}$ is a prime element in $S^{-1}R$.*

Exercise 3.2.8 *Let R and T be domains, $f : R \longrightarrow T$ a ring morphism, and $p \in R$, $q \in T$ such that $f(p) = q$.*
i) If p is prime, is q prime?
ii) If q is prime, is p prime?

The following definition generalizes condition iii) in Exercise 1.2.20 (usually taken as a definition for prime numbers).

Definition 3.2.9 *Let R be a domain. Then an element $q \neq 0_R$, $q \notin U(R)$, is said to be* **irreducible** *if from $d \mid q$ it follows that $d \sim_d 1_R$ or $d \sim_d q$.*

The connection between prime and irreducible is given by the following

Proposition 3.2.10 *Any prime element is irreducible, but there are irreducible elements that are not prime.*

Proof: Assume that $p \in R$ is prime, and let $d \mid p$. It follows that $p = ds$, so $p \mid ds$. Since p is prime, it follows that $p \mid d$ or $p \mid s$. If $p \mid d$ we have $d \sim_d p$. If $p \mid s$, write $s = pu$, and observe that $p = dpu$. Since $p \neq 0_R$, we get $1_R = du$, or $d \sim_d 1_R$, which ends the proof.

Now $X^2 \in \mathbb{Z} + X^2\mathbb{Z}[X]$ is irreducible, but not prime, and $2 \in \mathbb{Z}[i\sqrt{5}]$ is also irreducible but not prime (see examples after Definition 3.2.1). ∎

Proposition 3.2.11 *In a GCD-domain, the notions of prime and irreducible coincide.*

Proof: Let $q \in R$ be irreducible. We have to show that q is prime, so we assume that $q \mid ab$. If $q \mid a$, we are done. If $q \nmid a$, then we must have that $1_R = (q, a)$ because q is irreducible, so we can apply Euclid Lemma (see Exercise 3.1.17) to get that $q \mid b$. ∎

Proposition 3.2.12 *Let $q \in R$ be irreducible. Then q is irreducible in the polynomial ring $R[X]$.*

Proof: Since R is a domain, the units in $R[X]$ are precisely the units in R by Exercise 2.6.12 iv). Therefore, $q \neq 0_R$ and $q \notin U(R[X])$. Since R is a domain, the divisors of q in $R[X]$ have to be polynomials of degree 0, i.e. nonzero elements of R, so these are the same as the divisors of q in R and we are done. ∎

Exercise 3.2.13 *Let p be an irreducible element in R, and S a multiplicative set on R such that $pR \cap S = \emptyset$. Is $\frac{p}{1_R}$ an irreducible element in $S^{-1}R$?*

Exercise 3.2.14 *Let R and T be domains, $f : R \longrightarrow T$ a ring morphism, and $p \in R$, $q \in T$ such that $f(p) = q$.*
i) If p is irreducible, is q irreducible?
ii) If q is irreducible, is p irreducible?

The following exercise should be compared to Exercise 3.1.9

Exercise 3.2.15 *i) The set*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$, and so it is a domain (its elements are called Gaussian integers).
ii) The function $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, defined by $N(a + bi) = a^2 + b^2$, has the property $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[i]$.
iii) $U(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$.

The following exercises look at prime and irreducible elements in $\mathbb{Z}[i]$. We will see soon, in Corollary 3.3.16, that these are in fact the same.

Exercise 3.2.16 *Let $x = a + bi \in \mathbb{Z}[i]$, $N(x) = 2$. Then*
i) x is irreducible.
ii) $x \in \{1 + i, -1 - i, 1 - i, -1 + i\}$.
iii) $x \sim_d 1 + i$.
iv) $x \mid y$ if and only if $N(y)$ is even.
v) x is prime.

Exercise 3.2.17 *Let $x = a+bi \in \mathbb{Z}[i]$, $N(x) = p$, where p is an odd prime. Then*
i) x is irreducible.
ii) $p \equiv 1 \pmod 4$.

Exercise 3.2.18 *If $\pi \in \mathbb{Z}[i]$ is prime, then one of the following assertions hold:*
i) $\pi \sim_d 1 + i$,
ii) $\pi \sim_d p$, where $p \in \mathbb{Z}$ is a prime congruent to 3 (mod 4),
iii) $N(\pi) = q$, $q \in \mathbb{Z}$ is a prime congruent to 1 (mod 4).

If we can prove that any π satisfying ii) and iii) from Exercise 3.2.18 is prime, then we found all primes in $\mathbb{Z}[i]$. We already know that an element satisfying iii) is irreducible (see Exercise 3.2.17), and the following exercise shows that an element satisfying ii) is irreducible, so everything will follow from Corollary 3.3.16.

Exercise 3.2.19 *Any $p \in \mathbb{Z}$, a prime congruent to 3 (mod 4), is an irreducible element in $\mathbb{Z}[i]$. Prove that there are infinitely many such primes.*

Exercise 3.2.20 *If $x, y \in \mathbb{Z}[i]$, $N(x) = N(y)$, does it follow that $x \sim_d y$?*

Solutions to the Exercises on Section 3.2

Exercise 3.2.2 *If p is prime, and $p \mid a_1 a_2 \dots a_n$, then there exists i, $1 \leq i \leq n$ such that $p \mid a_i$.*
Solution: Same as the solution to Exercise 1.2.21.

Exercise 3.2.5 *If R is a domain, then X is a prime element in the polynomial ring $R[X]$.*
Solution: $R[X]/XR[X] \simeq R$.

Exercise 3.2.7 *Let p be a prime element in R, and S a multiplicative set on R such that $pR \cap S = \emptyset$. Then $\frac{p}{1_R}$ is a prime element in $S^{-1}R$.*
Solution: We will omit the index R when writing 0 and 1. We first see that $\frac{p}{1} \neq \frac{0}{1}$ because $p \neq 0$, and $\frac{p}{1}$ is not a unit, because if $\frac{p}{1} \cdot \frac{a}{s} = \frac{1}{1}$, then $pa = s \in pR \cap S$, a contradiction.

Now, if $\frac{p}{1} \mid \frac{a}{s} \cdot \frac{b}{t}$, it follows that $\frac{ab}{st} = \frac{p}{1} \cdot \frac{c}{r}$, so $pcst = abr$, and since p can't divide r, it follows that $p \mid a$ or $p \mid b$. If say $p \mid a$, then $a = pu$, so $\frac{a}{s} = \frac{p}{1} \cdot \frac{u}{s}$, i.e. $\frac{p}{1} \mid \frac{a}{s}$, which ends the proof that $\frac{p}{1}$ is prime in $S^{-1}R$.

Exercise 3.2.8 *Let R and T be domains, $f : R \longrightarrow T$ a ring morphism, and $p \in R$, $q \in T$ such that $f(p) = q$.*
i) If p is prime, is q prime?
ii) If q is prime, is p prime?
Solution: i) No, take $R = \mathbb{Z}$, $T = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$, f the inclusion, and $p = q = 2$. We have that 2 is prime in $\mathbb{Z}$, but $2 = (1+i)(1-i) \in \mathbb{Z}[i]$.
ii) No, take $R = \mathbb{Z}$, $S = \{2^k \mid k \in \mathbb{N}\}$, $T = S^{-1}\mathbb{Z}$, f the canonical injection, $p = 6$, $q = \frac{6}{1}$. Then q is prime: if $\frac{6}{1} \cdot \frac{a}{2^k} = \frac{b}{2^m} \cdot \frac{c}{2^n}$, then $3 \mid b$ or $3 \mid c$, which means that $\frac{6}{1} \mid \frac{b}{2^m}$ or $\frac{6}{1} \mid \frac{c}{2^n}$.

Exercise 3.2.13 *Let p be an irreducible element in R, and S a multiplicative set on R such that $pR \cap S = \emptyset$. Is $\frac{p}{1_R}$ an irreducible element in $S^{-1}R$?*
Solution: No, let $R = \mathbb{Z}[i\sqrt{5}]$, $p = 3$, $S = \{2^k \mid k \in \mathbb{N}\}$. Then 3 is irreducible, because there are no elements of norm 3, but

$$\frac{3}{1} = \frac{1+i\sqrt{5}}{1} \cdot \frac{1-i\sqrt{5}}{2}.$$

We show that $\frac{1+i\sqrt{5}}{1}$ is not a unit. If $\frac{1+i\sqrt{5}}{1} \cdot \frac{a+bi\sqrt{5}}{2^k} = \frac{1}{1}$, then $2^k = a - 5b + (a+b)i\sqrt{5}$, so $a = -b$, and $2^k = 6a$, a contradiction.
We show that $\frac{3}{1} \nmid \frac{1+i\sqrt{5}}{1}$. If $\frac{1+i\sqrt{5}}{1} = \frac{3}{1} \cdot \frac{a+bi\sqrt{5}}{2^k}$, then $2^k(1+i\sqrt{5}) = 3(a+bi\sqrt{5})$, and it follows that $N(2^k(1+i\sqrt{5})) = 2^{2k} \cdot 6$ is divisible by 9, a contradiction.

Exercise 3.2.14 *Let R and T be domains, $f : R \longrightarrow T$ a ring morphism,*

and $p \in R$, $q \in T$ such that $f(p) = q$.
i) If p is irreducible, is q irreducible?
ii) If q is irreducible, is p irreducible?
Solution: No to both, see the solution to Exercise 3.2.8.

Exercise 3.2.15 *i) The set*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$, and so it is a domain (its elements are called Gaussian integers).
ii) The function $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, defined by $N(a + bi) = a^2 + b^2$, has the property $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[i]$.
iii) $U(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$.
Solution: i) Take $R = \mathbb{Z}$, $A = \mathbb{C}$, $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ the inclusion, and $x = i$ in Theorem 2.6.13. We see that $Im(\theta) = \mathbb{Z}[i]$ using the fact that $i^2 = -1$.
ii) See Exercise 3.1.9, iii).
iii) The only integer solutions of the equation $a^2 + b^2 = 1$ are $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$.

Exercise 3.2.16 *Let $x = a + bi \in \mathbb{Z}[i]$, $N(x) = 2$. Then*
i) x is irreducible.
ii) $x \in \{1 + i, -1 - i, 1 - i, -1 + i\}$.
iii) $x \sim_d 1 + i$.
iv) $x \mid y$ if and only if $N(y)$ is even.
v) x is prime.
Solution: i) If $x = yz$, then $2 = N(y)N(z)$, so either $N(y) = 1$ or $N(z) = 1$.
ii) The solutions of $a^2 + b^2 = 2$ are $a = \pm 1$ and $b = \pm 1$, so $x \in \{1 + i, -1 - i, 1 - i, -1 + i\}$.
iii) $-1 - i = (-1)(1 + i)$, $1 - i = (-i)(1 + i)$, $-1 + i = i(1 + i)$.
iv) If $x \mid y$, then $N(x) = 2 \mid N(y)$. Conversely, if $y = c+di$, $N(y) = c^2+d^2 = 2k$, it follows that c and d are both odd or both even, so both $c + d$ and $c - d$ are even. Then, if we put $c + di = (1 + i)(u + vi) = u - v + (u + v)i$, we can solve for u and v: $u = \frac{c+d}{2} \in \mathbb{Z}$, and $v = \frac{d-c}{2} \in \mathbb{Z}$.
v) This will follow from Corollary 3.3.16, but we give a direct proof. If $x \mid yz$, then $N(y)N(z)$ is even, so one of them has to be even, and we can use iv).

Exercise 3.2.17 *Let $x = a+bi \in \mathbb{Z}[i]$, $N(x) = p$, where p is an odd prime. Then*
i) x is irreducible.
ii) $p \equiv 1 \pmod 4$.

Solution: i) Same as Exercise 3.2.16 i).
ii) We have that p has to be congruent to 1 or 3 (mod 4). But $a^2 + b^2$ can only be congruent to 0,1, or 2 (mod4).

Exercise 3.2.18 *If $\pi \in \mathbb{Z}[i]$ is prime, then one of the following assertions hold:*
i) $\pi \sim_d 1 + i$,
ii) $\pi \sim_d p$, where $p \in \mathbb{Z}$ is a prime congruent to 3 (mod 4),
iii) $N(\pi) = q$, $q \in \mathbb{Z}$ is a prime congruent to 1 (mod 4).
Solution: $N(\pi) \neq 1$, so $N(\pi) = \pi\overline{\pi}$ can be written as a product of integer primes by Theorem 1.2.23:

$$\pi\overline{\pi} = p_1 p_2 \dots p_k.$$

If $k = 1$, i) or iii) hold by Exercises 3.2.16 and 3.2.17.
If $k \geq 2$, then π divides one of these primes, say $\pi \mid p_1$, or $p_1 = \pi x$. Then

$$N(p_1) = p_1^2 = N(\pi)N(x) = p_1 p_2 \dots p_k N(x),$$

so in this case we see that $k = 2$, $p_1 = p_2 = p$, and $N(x) = 1$, i.e. $\pi \sim_d p$. We clearly have that $p_1 \neq 2$, because $2 = (1+i)(1-i)$ is not prime. In order to finish the proof we have to show that p is not congruent to 1 (mod 4). Indeed, if this was the case, then we have an even number of congruences

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\dots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p} \end{aligned}$$

so if we denote $a = \frac{p-1}{2}!$, and we use Wilson's Theorem (see Exercise 2.3.17), we get that $(p-1)! \equiv a^2 \equiv -1 \pmod{p}$, i.e. $p \mid a^2+1 = (a+i)(a-i)$, and since clearly p does not divide either of $a + i$ and $a - i$, we get a contradiction. Therefore, p is congruent to 3 (mod 4).

Exercise 3.2.19 *Any $p \in \mathbb{Z}$, a prime congruent to 3 (mod 4), is an irreducible element in $\mathbb{Z}[i]$. Prove that there are infinitely many such primes.*
Solution: If $p = xy$, where $x, y \in \mathbb{Z}$. Then $p^2 = N(x)N(y)$, and the only way to avoid that one of $N(x)$ and $N(y)$ is 1 is to have both of them equal to p. But that is not possible by Exercise 3.2.17 ii).

For the second part, assume that there are only finitely many primes of the form $4k + 3$, call them $p_1, p_2, \dots, p_k$. The number $4p_1p_2 \cdots p_k - 1$ has to be divisible by one of $p_1, p_2, \dots, p_k$, because otherwise it would have remainder 1 modulo 4. But this is clearly false, so the proof is complete.

Exercise 3.2.20 *If $x, y \in \mathbb{Z}[i]$, $N(x) = N(y)$, does it follow that $x \sim_d y$?*
Solution: No, take $x = 2 + i$ and $y = 2 - i$. By Exercise 3.2.15 iii), the associates of x are $\{2 + i, -2 - i, -1 + 2i, 1 - 2i\} \not\ni y$.

3.3 Euclidean domains

We continue to assume that all rings are domains. The following definition is inspired by Theorem 1.2.1:

Definition 3.3.1 *A domain R is called* Euclidean *if there exists a function $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$ for which the Division Algorithm holds, i.e. if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ and $r = 0$ or $\varphi(r) < \varphi(b)$. The elements q qnd r are called a quotient and a remainder for a divided by b.*

By Theorem 1.2.1, $\mathbb{Z}$ is Euclidean, the function $\varphi : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ is defined by $\varphi(n) = |n|$. We noticed in the proof of Theorem 1.2.1 that there are generally two pairs of quotients and remainders for a division in $\mathbb{Z}$.

Exercise 3.3.2 *If we ask the remainder r in Theorem 1.2.1 to satisfy $r \geq 0$, then the quotient and remainder, the q and the r from the statement of the theorem are unique.*

Exercise 3.3.3 *If K is a field, show that K is Euclidian.*

The following result shows that if K is a field, then the polynomial ring $K[X]$ and the formal series ring $K[[X]]$ are Euclidian, with functions $\varphi : K[X] \setminus \{0\} \longrightarrow \mathbb{N}$ defined by $\varphi(f) = \deg(f)$, and $\psi : K[[X]] \setminus \{0\} \longrightarrow \mathbb{N}$ defined by $\psi(f) = \text{ord}(f) =$ the smallest power of X appearing in f:

Theorem 3.3.4 *i) Let K be a field, and $f, g \in K[X]$, $g \neq 0$. There exist $q, r \in K[X]$ such that $f = qg + r$, where $r = 0$ or $\deg(r) < \deg(g)$.*
ii) Let K be a field, and $f, g \in K[[X]]$, $g \neq 0$. There exist $q, r \in K[[X]]$ such that $f = qg + r$, where $r = 0$ or $\text{ord}(r) < \text{ord}(g)$.

Proof: i) The proof is similar to the one of Theorem 1.2.1. If $g \mid f$, then $f = qg$ for some $q \in K[X]$, and we take $r = 0$. If $g \nmid f$ (note that this implies that $f \neq 0$), we let $W = \{\deg(f - eg) \mid e \in K[X]\}$. By the well-ordering principle, we let $r = f - qg$ such that $\deg(r)$ is a least element of W. We want to show that $\deg(r) < \deg(g)$. If $\deg(r) = \deg(f - qg) = n \geq m = \deg(g)$, we write $r = f - qg = aX^n + a_{n-1}X^{n-1} + \ldots$ and $g = bX^m + b_{m-1}X^{m-1} + \ldots$. Then $f - qg - ab^{-1}X^{n-m}g$ has degree less than $\deg(r)$, a contradiction.
ii) The proof is identical to the proof of i), except we write $r = f - qg = aX^n + a_{n+1}X^{n+1} + \ldots$ and $g = bX^m + b_{m+1}X^{m+1} + \ldots$, and we replace degree by order everywhere.
We remark that the proofs of i) and ii) above are exactly the long division algorithms for polynomials and power series as you have seen them in beginning algebra and calculus. ∎

Remark 3.3.5 *We remark that the conclusion of Theorem 3.3.4 remains true for polynomials with coefficients in an arbitrary domain if the leading coefficient of g is a unit.*

Exercise 3.3.6 *Show that q and r from the statement of Theorem 3.3.4 are unique.*

Corollary 3.3.7 (Bézout's Little Theorem) *Let R be a domain, and $a \in R$. For any $f \in R[X]$, the remainder of f when divided by $X-a$ is $f(a)$ (the value of the polynomial function defined by f at $a \in R$). Consequently, $X - a \mid f$ if and only if $f(a) = 0$ (we say that a is a* root *of f).*

Proof: By Theorem 3.3.4 and Remark 3.3.5, we have that $f = (X-a)q+r$, where $r \in R$. After specializing X at a we get that $f(a) = r$. ∎

Exercise 3.3.8 (Rational Root Theorem) *If $\frac{a}{b} \in \mathbb{Q}$, $(a, b) = 1$, is a root of*

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X],$$

then $a \mid a_0$ and $b \mid a_n$.

Exercise 3.3.9 *If R is a domain and $f \in R[X]$ is a non-zero polynomial, then f has at most n roots, where $n = \deg(f)$. Is this true if R is not a domain?*

The previous exercise shows that if R is an infinite domain, we cannot have two different polynomials defining the same polynomial function. Indeed, the difference of the two polynomials would then have infinitely many roots, which is not possible, the number of roots is bounded by the degree. This is the reason why we can get away with identifying polynomials with polynomial functions in high school mathematics.

Exercise 3.3.10 *Let $p \in \mathbb{Z}$ be prime. Use the polynomial $(X-1)\cdots(X-p+1) - X^{p-1} + 1 \in \mathbb{Z}_p[X]$ to give another proof for Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$ (see Exercise 2.3.17).*

You might find other definitions for Euclidean domains in the literature. One of the most commonly used definitions requires that the function φ in Definition 3.3.1 additionally satisfies the condition

$$\text{If } a \text{ and } b \text{ are non-zero, and } a \mid b \text{ then } \varphi(a) \leq \varphi(b). \tag{3.1}$$

We will see in the next section (Proposition 3.4.6) that these two definitions are equivalent.

Another definition requires the function φ in Definition 3.3.1 to be multiplicative, i.e. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R \setminus \{0\}$. It is clear that if φ

is multiplicative, then it satisfies condition (3.1). Looking at our examples of Euclidean domains, we see that the functions we considered for $\mathbb{Z}$, a field K, and $\mathbb{Z}[i]$ (see Theorem 3.3.11 below) are all multiplicative. The only one that are not are $\varphi(f) = \deg(f)$, where K is a field and $f \in K[X] \setminus \{0\}$ and $\psi(f) = \text{ord}(f)$, where K is a field and $f \in K[[X]] \setminus \{0\}$. However, they can be replaced by $\varphi'(f) = 2^{\deg(f)}$ and $\psi'(f) = 2^{\text{ord}(f)}$, which are multiplicative. For a very long time it has been an open question whether any Euclidean domain has a multiplicative function. An example of an Euclidean domain for which this is not true was given in [10].

We now show that the ring of Gaussian integers, $\mathbb{Z}[i]$, is an Euclidean domain. Recall from Exercise 2.6.15 that its field of fractions is $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

Theorem 3.3.11 *i) $\mathbb{Z}[i]$ is Euclidean with respect to $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $N(a+bi) = a^2 + b^2$, if and only if $\forall z \in \mathbb{Q}(i)$ $\exists q \in \mathbb{Z}[i]$ such that $N(z-q) < 1$.*
ii) $\mathbb{Z}[i]$ is Euclidean with respect to $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $N(a+bi) = a^2 + b^2$.

Proof: i) Assume that $\mathbb{Z}[i]$ is Euclidean, and let $z = \frac{\alpha}{\beta} \in \mathbb{Q}(i)$, $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ such that $\alpha = \beta q + r$ and $N(r) < N(\beta)$ (this is because $N(r) = 0$ iff $r = 0$).Then we have

$$N(z-q) = N\left(\frac{\alpha}{\beta} - q\right) = N\left(\frac{\beta q + r}{\beta} - q\right) = N\left(\frac{r}{\beta}\right) = \frac{N(r)}{N(\beta)} < 1. \quad (3.2)$$

Conversely, let $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Let $z = \frac{\alpha}{\beta}$ and $q \in \mathbb{Z}[i]$ be such that $N(z-q) < 1$, and let $r = \alpha - \beta q$. Then (3.2) holds and we are done.
ii) If $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, then $\frac{\alpha}{\beta} \in \mathbb{Q}(i)$ is inside one of the squares of the lattice determined in the plane by $\mathbb{Z}[i]$. Any vertex of this square that is within a unit distance from $\frac{\alpha}{\beta}$ is a possible quotient according to i). In Figure 3.1, each of the nine regions displays the number of possible quotients when $\frac{\alpha}{\beta}$ is in that region. For each quotient q we find a remainder by putting $r = \alpha - \beta q$. We see that there are at least two and at most four possibilities, depending on the region that contains $\frac{\alpha}{\beta}$. ∎

Remark 3.3.12 *We have seen that for integers we have in general two pairs of quotients and remainders, but if we ask the reminder to be non-negative, then the quotient and remainder are unique. The quotient and remainder are also unique for polynomials with coefficients in a field, but in the case of Gaussian integers there is no way choose the quotient and remainder in order to make them unique.*

Theorem 3.3.13 *An Euclidean domain is a GCD-domain.*

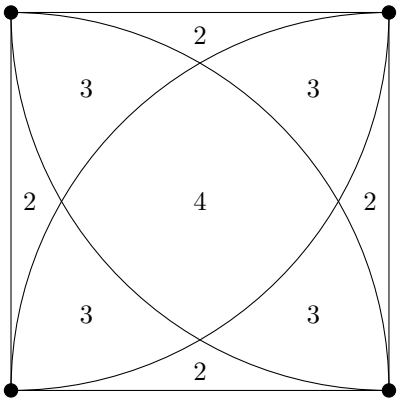


Figure 3.1: Number of quotient and remainder pairs in $\mathbb{Z}[i]$

Proof: The proof is identical to the proof of Theorem 1.2.7. Given elements a and b in an Euclidean domain R with function φ, we need to show that a greatest common divisor of a and b exists. If one of a and b is 0, then the other one is their greatest common divisor. So we assume that both of a and b are not 0, and we consider the set $W = \{\varphi(ma + nb) \mid m, n \in R, ma + nb \neq 0\}$. $W \neq \emptyset$ because we can pick $m = 1$ and $n = 0$. By the well-ordering principle W has a least element $\varphi(d) = \varphi(ua + vb)$, and we show that $d = (a, b)$. We prove first that $d \mid a$. Indeed, if d does not divide a we use the division algorithm to find q and r such that $a = dq + r$, where $\varphi(r) < \varphi(d)$. Now since $r = a - dq = a - (ua + vb) = (1 - u)a + (-v)b \in W$, this contradicts the fact that $\varphi(d)$ is the least element in W. The proof of the fact that $d \mid b$ is identical. Finally, if $c \mid a$ and $c \mid b$, then $a = ce$ and $b = cf$. It follows that $d = ua + vb = uce + vcf = c(ue + vf)$, so $c \mid d$ and the proof is complete. ∎

Exercise 3.3.14 *Find all possible quotients and remainders when dividing* $1 + 2i$ *by* $3 + 4i$ *in* $\mathbb{Z}[i]$.

From the proof of Theorem 3.3.13 we immediately obtain the following

Corollary 3.3.15 *In an Euclidean domain, the greatest common divisors of two elements is a linear combination of them (i.e. if* $d = (a, b)$, $\exists u, v \in R$ *such that* $d = au + bv$*).*

Corollary 3.3.16 *In an Euclidean ring, an element is prime if and only if it is irreducible.*

Proof: Proposition 3.2.11. ∎

The proof of the next result is identical to the one of Proposition 1.2.10, and since even the notation is the same, we will omit it.

Proposition 3.3.17 (The Euclidean Algorithm in Euclidean Domains)
In an Euclidean domain R with function φ we have the following:
i) If $a = bq + r$, then $(a, b) = (b, r)$.
ii) If a, b are nonzero, consider the following chain of divisions:
$a = q_0 b + r_0$, *where* $r_0 = 0$ *or* $\varphi(r_0) < \varphi(b)$,
$b = q_1 r_0 + r_1$, *where* $r_1 = 0$ *or* $\varphi(r_1) < \varphi(r_0)$,
$r_0 = q_2 r_1 + r_2$, *where* $r_2 = 0$ *or* $\varphi(r_2) < \varphi(r_1)$,
...
$r_n = q_{n+2} r_{n+1} + r_{n+2}$, *where* $r_{n+2} = 0$ *or* $\varphi(r_{n+2}) < \varphi(r_{n+1})$,
...
Then $\{\varphi(r_n)\}$ is a strictly decreasing chain of nonnegative integers, so one of the r's has to be 0. The last nonzero remainder in this chain is a greatest common divisor for a and b.

Remark 3.3.18 *If we find $d = (a, b)$ using the Euclidean algorithm, we can use back substitution to write d as a linear combination of a and b.*

Exercise 3.3.19 *Use the Euclidean algorithm to find $(4-3i, 2+i)$ in $\mathbb{Z}[i]$, then write it as a linear combination of $4 - 3i$ and $2 + i$.*

Exercise 3.3.20 *Use the Euclidean algorithm to find $(X^5 + X^4 + 2X + 2, X^2 + 3X + 2)$ in $\mathbb{Q}[X]$, then write it as a linear combination of $X^5 + X^4 + 2X + 2$ and $X^2 + 3X + 2$.*

Remark 3.3.21 *The greatest common divisor of two elements is generally not unique, any element associated in divisibility with it will also be a greatest common divisor. In $\mathbb{Z}$ we can make the greatest common divisor unique by requiring it to be positive. We can make the greatest common divisor of two polynomials with coefficients in a field unique if we require it to be monic (i.e. to have leading coefficient 1). For Gaussian integers we have no option for making the greatest common divisor unique.*

Solutions to the Exercises on Section 3.3

Exercise 3.3.2 *If we ask the remainder r in Theorem 1.2.1 to satisfy $r \geq 0$, then the quotient and remainder, the q and the r from the statement of the theorem are unique.*
Solution: Assume that $a = bq_1 + r_1 = bq_2 + r_2$, where $0 \leq r_1, r_2 < b$. Then $b(q_1 - q_2) = r_2 - r_1$, i.e. $b \mid r_2 - r_1$. Since $|\, r_2 - r_1 \,| < b$, it follows that $r_1 = r_2$, so $bq_1 = bq_2$, and since $b \neq 0$ we get that $q_1 = q_2$.

Exercise 3.3.3 *If K is a field, show that K is Euclidian.*
Solution: Define $\varphi : K \setminus \{0\} \longrightarrow \mathbb{N}$ by $\varphi(a) = 1$ for all $a \in K \setminus \{0\}$. Then for all $a, b \in K$, $b \neq 0$, we get $q = ab^{-1}$ and $r = 0$.

Exercise 3.3.6 *Show that q and r from the statement of Theorem 3.3.4 are unique.*
Solution: Assume $f = q_1 g + r_1 = q_2 g + r_2$. If $r_1 \neq r_2$, then $g(q_1 - q_2) = r_2 - r_1$, and $deg(g) < deg(r_2 - r_1)$, a contradiction. It follows that $r_1 = r_2$, so $q_1 = q_2$ as well, because $K[X]$ is a domain and $g \neq 0$. For the formal series case, just replace degree by order.

Exercise 3.3.8 *If $\frac{a}{b} \in \mathbb{Q}$, $(a, b) = 1$, is a root of*

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X],$$

then $a \mid a_0$ and $b \mid a_n$.
Solution: Write

$$a_n \left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \ldots + a_1 \left(\frac{a}{b}\right) + a_0 = 0,$$

so after multiplying both sides by b^n we get

$$a_n a^n + a_{n-1} a^{n-1} b + \ldots + a_1 a b^{n-1} + a_0 b^n = 0.$$

Therefore

$$a(a_n a^{n-1} + a_{n-1} a^{n-2} b + \ldots + a_1 b^{n-1}) = -a_0 b^n,$$

so by Euclid's Lemma (Theorem 1.2.15) we get that $a \mid a_0$. Then

$$b(a_{n-1} a^{n-1} + \ldots + a_1 a b^{n-2} + a_0 b^{n-1}) = -a_n a^n,$$

so $b \mid a_n$.

Exercise 3.3.9 *If R is a domain and $f \in R[X]$ is a non-zero polynomial, then f has at most n roots, where $n = deg(f)$. Is this true if R is not a*

domain?
Solution: Induction on n. If $n = 0$, then $0 \neq f \in R$, so f has no roots. If $n \geq 1$ and f has a root a, then $f = (X - a)g$, where $deg(g) = n - 1$ by Corollary 3.3.7. By the induction hypothesis g has at most $n - 1$ roots, so f has at most $n - 1 + 1 = n$ roots.

The assertion is false if R is not a domain, the polynomial $2X \in \mathbb{Z}_4[X]$ has degree one and two roots, 0 and 2.

Exercise 3.3.10 *Let $p \in \mathbb{Z}$ be prime. Use the polynomial $f = (X - 1)\cdots(X - p + 1) - X^{p-1} + 1 \in \mathbb{Z}_p[X]$ to give another proof for Wilson's Theorem: $(p - 1)! \equiv -1$ (mod p) (see Exercise 2.3.17).*
Solution: Assume $p > 2$. By Fermat's Little Theorem (Exercise 2.3.16 viii)), f has roots 1, 2, $\ldots, p - 1$. Since it has degree at most $p - 2$, by Exercise 3.3.9 it follows that $f = 0$. Specializing X at 0 gives $(p-1)! \equiv -1 \pmod{p}$.

Exercise 3.3.14 *Find all possible quotients and remainders when dividing $1 + 2i$ by $3 + 4i$ in $\mathbb{Z}[i]$.*
Solution: Since $N(3+4i) = 25 > 5 = N(1+2i)$, we can choose $q_1 = 0$ and $r_1 = 1 + 2i$. We now find the other quotients and remainders. We compute

$$z = \frac{1+2i}{3+4i} = \frac{(1+2i)(3-4i)}{25} = \frac{11+2i}{25} = \frac{11}{25} + \frac{2}{25}i.$$

We see that z is inside the square with vertices 0, 1, i, and $1 + i$. We compute

$$N(z-1) = \left(\frac{11}{25} - 1\right)^2 + \left(\frac{2}{25}\right)^2 = \frac{196}{625} + \frac{4}{625} = \frac{200}{625} < 1,$$

$$N(z-i) = \left(\frac{11}{25}\right)^2 + \left(\frac{2}{25} - 1\right)^2 = \frac{121}{625} + \frac{529}{625} = \frac{650}{625} > 1,$$

$$N(z-(1+i)) = \left(\frac{11}{25} - 1\right)^2 + \left(\frac{2}{25} - 1\right)^2 = \frac{196}{625} + \frac{529}{625} = \frac{725}{625} > 1.$$

There is only one other possible quotient, $q_2 = 1$, and remainder $r_2 = 1 + 2i - (3 + 4i) = -2 - 2i$.

Exercise 3.3.19 *Use the Euclidean algorithm to find $(4+3i, 2+i)$ in $\mathbb{Z}[i]$, then write it as a linear combination of $4 + 3i$ and $2 + i$.*
Solution: We compute

$$z_1 = \frac{4+3i}{2+i} = \frac{(4+3i)(2-i)}{5} = \frac{11+2i}{5} = \frac{11}{5} + \frac{2}{5}i.$$

We have that z_1 is inside the square with vertices 2, 3, $3+i$, and $2+i$. We only need one quotient and one remainder, and we see that $N(z_1-2) = \frac{1}{25}+\frac{4}{25} = \frac{5}{25} < 1$, so we write

$$4+3i = (2+i)\cdot 2 + i.$$

Since i is a unit, we have that $1 = (4+3i, 2+i)$, and since $i = 4+3i+(-2)(2+i)$, we get that

$$1 = (-i)(4+3i) + (2i)(2+i).$$

Exercise 3.3.20 *Use the Euclidean algorithm to find* (X^5+X^4+2X+2, X^2+3X+2) *in* $\mathbb{Q}[X]$*, then write it as a linear combination of* X^5+X^4+2X+2 *and* X^2+3X+2.
Solution: We first divide X^5+X^4+2X+2 by X^2+3X+2:

$$\begin{array}{r|l}
X^2+3X+2 & X^3-2X^2+4X-8 \\
\hline
X^5+X^4 \qquad\qquad +2X+2 & \\
-X^5-3X^4-2X^3 & \\
\hline
-2X^4-2X^3 & \\
2X^4+6X^3+4X^2 & \\
\hline
4X^3+4X^2+2X & \\
-4X^3-12X^2-8X & \\
\hline
-8X^2-6X+2 & \\
8X^2+24X+16 & \\
\hline
18X+18 &
\end{array}$$

so we have

$$X^5+X^4+2X+2 = (X^2+3X+2)(X^3-2X^2+4X-8)+18(X+1),$$

Then we divide X^2+3X+2 by $18X+18$:

$$\begin{array}{r|l}
18X+18 & \frac{1}{18}X+\frac{1}{9} \\
\hline
X^2+3X+2 & \\
-X^2-X & \\
\hline
2X+2 & \\
-2X-2 & \\
\hline
0 &
\end{array}$$

Since 18 is a unit, we have that $X+1 = (X^5+X^4+2X+2, X^2+3X+2)$, and

$$X+1 = \frac{1}{18}(X^5+X^4+2X+2)+(-\frac{1}{18}X^3+\frac{1}{9}X^2-\frac{2}{9}X+\frac{4}{9})(X^2+3X+2).$$

3.4 Principal Ideal Domains

Recall from Definition 2.2.9 that a domain R is said to be a *principal ideal domain* (PID for short) if every ideal of R is principal, i.e. is generated by one element.

Exercise 3.4.1 *Show that*
i) a field is a PID.
ii) $\mathbb{Z}$ is a PID.
iii) $\mathbb{Z}[X]$ is not a PID by proving that the ideal generated by 2 and X is not principal.

We now extend Exercise 2.2.10 (whose proof is actually the proof of Proposition 1.5.7) to Euclidean domains.

Theorem 3.4.2 *Any Euclidean domain is a PID.*

Proof: Let R be a Euclidean domain with function φ, and let I be an ideal of R. If $I = \{0\}$, I is generated by 0. If $I \neq \{0\}$, let

$$W = \{\varphi(a) \mid a \in I, a \neq 0\}.$$

By the well-ordering principle, let $b \in I$, $b \neq 0$, such that $\varphi(b)$ is the least element in W. We show that $I = bR$. It is clear that $bR \subseteq I$, because $b \in I$. If $a \in I$, let $q, r \in R$ such that $a = bq + r$, and $r = 0$ or $\varphi(r) < \varphi(b)$. Since $r = a - bq \in I$, the latter would contradict the fact that $\varphi(b)$ is the least element of W, so we get that $r = 0$ and the proof is complete. ∎

Exercise 3.4.3 *Show that*
i) $\mathbb{Z}[i]$ and $K[X]$, where K is a field, are PIDs.
ii) If R is a domain, then $R[X]$ is a PID if and only if R is a field.

Exercise 3.4.4 *Show that a PID is a GCD-domain.*

Exercise 3.4.5 *Is $\mathbb{Z}[i\sqrt{5}]$ a PID?*

We can now prove the equivalence of the two definitions for Euclidean domains promised at the end of the previous section.

Proposition 3.4.6 *Let R be an Euclidian ring with function $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$, and define $\varphi' : R \setminus \{0\} \longrightarrow \mathbb{N}$ by*

$$\varphi'(a) = \inf\{\varphi(b) \mid b \sim_d a\}.$$

Then R is an Euclidean ring with φ', and φ' also satisfies (3.1).

Proof: We show first that R is Euclidean with φ'. Let $a, b \in R$, $b \neq 0$, and let $b' \sim_d b$ be such that $\varphi'(b) = \varphi(b')$. Then let $q, r \in R$ such that $a = b'q + r$ and $r = 0$ or $\varphi(r) < \varphi(b')$. We have that $b' = bu$ for some $u \in U(R)$, so $a = buq + r$. Then, if $r \neq 0$, we have $\varphi'(r) \leq \varphi(r) < \varphi(b') = \varphi'(b)$.
We now prove that φ' satisfies (3.1). Let $a \mid b$ be non-zero elements in R, which means that $b \in aR$. By the proof of Theorem 3.4.2, it follows that $aR = cR$, where c has the property that $\phi'(c)$ is the smallest of all $\phi'(x)$, $x \in aR$. In particular, $\phi'(c) \leq \phi'(b)$. On the other hand, $a \sim_d c$, so $\phi'(c) = \phi'(a)$, and the proof is complete. ∎

Theorem 3.4.7 *Let R be a PID, $a \in R$, $a \neq 0$, $a \notin U(R)$. Then a can be written as a finite product of prime elements.*

Proof: Since PIDs are GCD-domains, any irreducible is prime, so we show that a is a finite product of irreducibles. If a is not a product of irreducibles, we can write $a = a_1 a'$, where $a_1, a' \notin U(R)$, and a_1 is not a product of irreducibles. Then $a_1 = a_2 a''$, where $a_2, a'' \notin U(R)$, and a_2 is not a product of irreducibles. We keep going and we get the following strictly ascending chain of principal ideals of R:

$$a_1 R \subset a_2 R \subset a_3 R \subset \dots .$$

But $I = \cup_{i \geq 1} a_i R$ is an ideal of R (because every element in I has to belong to one of the ideals in the chain, and therefore any two elements in I belong to one of the ideals in the chain), so $I = aR$ for some a. Now a has to belong to some $a_n R$, so the chain has to stabilize after that, a contradiction. ∎

Proposition 3.4.8 *Let R be a PID but not a field. Then M is a maximal ideal of R if and only iff it is generated by an irreducible element.*

Proof: Let $M = qR$ be an ideal of R, and assume that $d \mid q$. Then $M = qR \subseteq dR \subseteq R$. Since $qR = dR$ if and only if $d \sim_d q$ and $dR = R$ if and only if $d \in U(R)$, the assertion follows. ∎

Exercise 3.4.9 *Use Proposition 3.4.8 to give another proof of the fact that in a PID any irreducible is prime.*

Exercise 3.4.10 *Let*

$$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{ a + b\frac{1+i\sqrt{19}}{2} \middle| a, b \in \mathbb{Z} \right\}.$$

Prove that:
i) $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is a subring of $\mathbb{C}$, and therefore it is a domain.

ii) $N : \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \longrightarrow \mathbb{N}$, *defined by* $N\left(a + b\frac{1+i\sqrt{19}}{2}\right) = a^2 + ab + 5b^2$ *is multiplicative.*
iii) The field of fractions of $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *is*

$$\mathbb{Q}[i\sqrt{19}] = \{a + bi\sqrt{19} \mid a, b \in \mathbb{Q}\}.$$

iv) $U\left(\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]\right) = \{1, -1\}$.

Proposition 3.4.11 $R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *is a PID but is not Euclidean.*

Proof: Assume first that R is Euclidean with function φ, and let $b \notin \{0, \pm 1\}$ such that $\varphi(b)$ is the smallest (such a b exists by the well-ordering principle). Then for any a we have that $a = bq + r$, where $r \in \{0, \pm 1\}$, and so R/bR is isomorphic to $\mathbb{Z}_2$ or $\mathbb{Z}_3$. Now

$$\left(\frac{1 + i\sqrt{19}}{2}\right)^2 - \frac{1 + i\sqrt{19}}{2} = \frac{1 + i\sqrt{19}}{2} \cdot \frac{-1 + i\sqrt{19}}{2} = -5,$$

so if we put $\alpha = \frac{1+i\sqrt{19}}{2}$, we have that $\alpha^2 - \alpha + 5 = 0$, and if we denote by $\overline{\alpha}$ the coset of α in R/bR, we have that $\overline{\alpha}^2 - \overline{\alpha} + \overline{5} = \overline{0}$. However, no elements in $\mathbb{Z}_2$ or $\mathbb{Z}_3$ satisfy this, and therefore R is not Euclidean.

We now show that R is a PID using R.A. Wilson's proof from [41]. Let I be a non-zero ideal of R, and let $b \in I$, $b \neq 0$, such that $N(b)$ is the smallest possible (such a b exists by the well-ordering principle). We will show that $I = bR$. If this is not true, we choose $a \in I \setminus bR$ and we try to contradict the minimality of $N(b)$ by finding $u, v \in R$ such that $0 < N(ua - vb) < N(b)$, or $0 < N\left(u\frac{a}{b} - v\right) < 1$.

Since we can add any element of R to $\frac{a}{b}$ (and thus replace a by a plus something in bR), we can assume that the imaginary part of $\frac{a}{b} = x + iy$ is between $\pm\frac{\sqrt{19}}{4}$ by adding to it integer multiples of $i\frac{\sqrt{19}}{2}$.

Now if $-\frac{\sqrt{3}}{2} < y < \frac{\sqrt{3}}{2}$, then $N\left(\frac{a}{b} - k\right) < 1$, where k is the closest integer to x. Note that $a - kb \neq 0$ because $a \notin I$.

Now we assume that $\frac{\sqrt{3}}{2} < y < \frac{\sqrt{19}}{4}$, hence the imaginary part of $2\frac{a}{b} - \frac{1+i\sqrt{19}}{2}$ lies between $\sqrt{3} - \frac{\sqrt{19}}{2}$ and 0. But $3\sqrt{3} > \sqrt{19}$, so $\frac{\sqrt{3}}{2} > \frac{\sqrt{19}}{2} - \sqrt{3} > 0$, and we have that $N(2\frac{a}{b} - \frac{1+i\sqrt{19}}{2} - l) < 1$, where l is the closest integer to $2x - \frac{1}{2}$.

The only way this will not work is if $2\frac{a}{b} - \frac{1+i\sqrt{19}}{2} - l = 0$, which means that $2\frac{a}{b} \in R$. Remembering that $|y| \leq \frac{\sqrt{19}}{4}$, this means that we can assume

that $y = \frac{\sqrt{19}}{4}$. After adding integers to $\frac{a}{b}$ we can assume that $\frac{a}{b} = \frac{\pm 1 + i\sqrt{19}}{4}$, so if we take $u = \frac{\mp 1 + i\sqrt{19}}{2}$ and $v = -2$ we have that

$$0 < N\left(u\frac{a}{b} - v\right) = N\left(\frac{(i\sqrt{19}+1)(i\sqrt{19}-1)}{8} + 2\right) = \frac{1}{4} < 1,$$

and the proof is complete. ∎

Solutions to the Exercises on Section 3.4

Exercise 3.4.1 *Show that*
i) a field is a PID.
ii) $\mathbb{Z}$ is a PID.
iii) $\mathbb{Z}[X]$ is not a PID by showing that the ideal generated by 2 and X is not principal.
Solution: i) The only ideals are $\{0\}$ and the field itself.
ii) This is Exercise 2.2.10.
iii) Assume that $2\mathbb{Z}[X] + X\mathbb{Z}[X] = d\mathbb{Z}[X]$ for some $d \in \mathbb{Z}[X]$. Since $2 \in d\mathbb{Z}[X]$ it follows that $deg(d) = 0$, and since $X \in d\mathbb{Z}[X]$ it follows that $d = \pm 1$, so we get $1 = 2f + Xg$ for some $f, g \in \mathbb{Z}[X]$. If we specialize X to 0, we see that $2 \mid 1$ in $\mathbb{Z}$, a contradiction.

Exercise 3.4.3 *Show that*
i) $\mathbb{Z}[i]$ and $K[X]$, where K is a field, are PIDs.
ii) If R is a domain, then $R[X]$ is a PID if and only if R is a field.
Solution: i) Follows from Theorems 3.3.4, 3.3.11, and 3.4.2.
ii) If R is a field, the assertion follows from i). If a is non-zero and a non-unit, then as in the solution to Exercise 3.4.1 iii) we get that $1 = af + Xg$, so the constant term of the right hand side is 1. This is a contradiction, because the constant term of the right hand side is 0 or a.

Exercise 3.4.4 *Show that a PID is a GCD-domain.*
Solution: See Exercise 3.1.7

Exercise 3.4.5 *Is $\mathbb{Z}[i\sqrt{5}]$ a PID?*
Solution: No, see the proof of Proposition 3.1.13, which shows that $\mathbb{Z}[i\sqrt{5}]$ is not a GCD-domain.

Exercise 3.4.9 *Use Proposition 3.4.8 to give another proof of the fact that in a PID any irreducible is prime.*
Solution: Let q be an irreducible. By Proposition 3.4.8, qR is maximal, so it is prime. Then q is prime by Proposition 3.2.3.

Exercise 3.4.10 *Let*

$$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a + b\frac{1+i\sqrt{19}}{2}\middle| a, b \in \mathbb{Z}\right\}.$$

Prove that:
i) $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is a subring of $\mathbb{C}$, and therefore it is a domain.
ii) $N : \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \longrightarrow \mathbb{N}$, defined by $N\left(a + b\frac{1+i\sqrt{19}}{2}\right) = a^2 + ab + 5b^2$ is

multiplicative.
iii) The field of fractions of $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *is*

$$\mathbb{Q}[i\sqrt{19}] = \{a + bi\sqrt{19} \mid a, b \in \mathbb{Q}\}.$$

iv) $U\left(\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]\right) = \{1, -1\}$.
Solution: i) The only thing we need to check is closure under multiplication, the rest are obvious. We compute

$$\left(a + b\frac{1+i\sqrt{19}}{2}\right)\left(c + d\frac{1+i\sqrt{19}}{2}\right) = ac - 5bd + (bc + ad + bd)\frac{1+i\sqrt{19}}{2}$$

ii) We have

$$\left(a + b\frac{1+i\sqrt{19}}{2}\right)\left(\overline{a + b\frac{1+i\sqrt{19}}{2}}\right) = a^2 + ab + 5b^2.$$

iii) We denote by K the field of fractions of $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$. We have

$$\frac{a + b\frac{1+i\sqrt{19}}{2}}{c + d\frac{1+i\sqrt{19}}{2}} = \frac{2ac + 10bd + bc + ad}{2(c^2 + cd + 5d^2} + \frac{bc - ad}{2(c^2 + ad + 5d^2)}i\sqrt{19},$$

so $K \subseteq \mathbb{Q}[i\sqrt{19}]$. Conversely,

$$\frac{a}{b} + \frac{c}{d}i\sqrt{19} = \frac{bc - 2ad + 2bc\frac{1+i\sqrt{19}}{2}}{2bd},$$

so $\mathbb{Q}[i\sqrt{19}] \subseteq K$ as well.
iv) If $u = a + b\frac{1+i\sqrt{19}}{2}$ is a unit, by ii) we have that $a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 = 1$. It follows that $b = 0$ and $a = \pm 1$.

3.5 Unique Factorization Domains

In this section we study domains in which the analog of the Fundamental Theorem of Arithmetic (see Theorem 1.2.23) holds. We note first that the uniqueness part is true in any domain:

Exercise 3.5.1 *Let R be a domain, and assume that $p_1, p_2, \ldots, p_n$, and $q_1, q_2, \ldots q_m$ are prime elements of R such that*

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

Then $n = m$ and each of the p_i is associated in divisiblity to one of the q_j.

Definition 3.5.2 *A domain R is called a* Unique Factorization Domain *(UFD for short), if any non-zero element which is not a unit can be writtem as a finite product of prime elements.*

Exercise 3.5.3 *A PID is a UFD.*

Exercise 3.5.4 *In a UFD, any irreducible is prime.*

If R is an UFD, and we pick one representative in each class of elements associated in divisibility with a prime, we obtain a family of primes $\{p_i\}_{i\in I}$ such that any $a \in R$, $a \neq 0$ can be written as

$$a = u \prod_{i\in I} p_i^{k_i}, \tag{3.3}$$

where $u \in U(R)$ and only a finite number of $k_i \in \mathbb{N}$ are non-zero. This decomposition is then unique, i.e. if we also have that

$$a = v \prod_{i\in I} p_i^{n_i},$$

with the same properties as (3.3), then $u = v$ and $k_i = n_i \ \forall i \in I$.

Exercise 3.5.5 *Let R be a UFD. If $a, b \in R \setminus \{0\}$ have factorizations as in (3.3)*

$$a = u \prod_{i\in I} p_i^{m_i}, \quad b = v \prod_{i\in I} p_i^{n_i}.$$

Show that:
i) If $d = \prod_{i\in I} p_i^{k_i}$, where $k_i = \min\{m_i, n_i\}$, then $d = (a, b)$.
ii) If $m = \prod_{i\in I} p_i^{l_i}$, where $l_i = \max\{m_i, n_i\}$, then $m = [a, b]$.
iii) R is a GCD-domain.
iv) If $a, b_1, b_2, \ldots, b_n \in R$ satisfy $1 = (a, b_i)$ for $1 \leq i \leq n$, then $1 = (a, b_1 b_2 \cdots b_n)$.

The following result lists several characterizations of UFDs.

Theorem 3.5.6 *The following assertions are equivalent for a domain R:*
i) R is a UFD.
ii) Every non-zero non-unit element of R can be written as a finite product of irreducibles, and any irreducible is prime.
iii) Every non-zero non-unit element of R can be written as a finite product of irreducibles, and the factorization is unique modulo the order of factors and association in divisibility.
iv) R is a GCD-domain and every non-zero non-unit element of R can be written as a finite product of irreducibles.

Proof: i) $\Leftrightarrow$ ii) follows from Exercise 3.5.4.
i) $\Leftrightarrow$ iv) follows from Exercise 3.5.5.
ii) $\Rightarrow$ iii) is clear.
iii) $\Rightarrow$ ii). Assume that iii) holds, let q be an irreducible, and assume that $q \mid ab$, i.e. $ab = qq'$. By the uniqueness of the factorization we get that $q \mid a$ or $q \mid b$, i.e. q is prime and the proof is complete. ∎

Definition 3.5.7 *If R is a UFD and $f \in R[X]$, the* content *of f, denoted by $c(f)$, is the greatest common divisor of all coefficients of f. We say that f is* primitive *if $c(f) = 1$ (this means that there is no prime element in R that divides all coefficients of f). It is clear that if $f \in R[X]$, then we can write $f = c(f)f_1$, where $f_1 \in R[X]$ is primitive.*

Exercise 3.5.8 *Let R be a UFD, and $f, g \in R[X]$. Then:*
i) If $c(f) = c(g) = 1$, then $c(fg) = 1$ (i.e. the product of primitive polynomials is primitive).
ii) In general, $c(fg) \sim_d c(f)c(g)$.
iii) If $a \in R$, $a \neq 0$, g is primitive, and $g \mid af$, then $g \mid f$.
iv) If both f and g are primitive and $af = bg$, $a, b \in R \setminus \{0\}$, then $f \sim_d g$.

From Exercise 2.6.12 v) we get that if F is a field, then $f \in F[X]$ is irreducible if and only if we cannot write $f = gh$, where $deg(g), deg(h) < deg(f)$.

Exercise 3.5.9 *Let F be a field, and $f \in F[X]$. Prove the following assertions:*
i) If $deg(f) = 1$, then f is irreducible.
ii) If $deg(f)$ is 2 or 3, then f is irreducible if and only if f has no roots.
iii) $F[X]/(X - a)F[X] \simeq F$.
iv) If $a, b \in F$, $a \neq b$, then $1 = (X - a, X - b)$.

Proposition 3.5.10 *Let R be a UFD and K its field of fractions. The following assertions are equivalent for $f \in R[X]$ with $deg(f) \geq 1$:*

i) f is irreducible in $R[X]$.
ii) f is primitive and irreducible in $K[X]$.

Proof: i) $\Rightarrow$ ii). It is clear that f is primitive. If $f = gh$, with $g, h \in K[X]$, $deg(g), deg(h) < deg(f)$, we can multiply both sides by a, which is the product of all denominators of coefficients of g and h, and get $af = g_1 h_1$, $g_1, h_1 \in R[X]$, $deg(g_1), deg(h_1) < deg(f)$. Then $af = c(g_1)g_2 h_1$, and by Exercise 3.5.8 iii) we get that $g_2 \mid f$, a contradiction.
ii) $\Rightarrow$ i) is clear. ∎

Proposition 3.5.11 *If R is a UFD, then any irreducible polynomial in $R[X]$ is prime.*

Proof: If $deg(f) = 0$, then f is irreducible in R, hence prime in R, and so it is prime in $R[X]$ by Proposition 3.2.6. If $deg(f) \geq 1$, then f is primitive. Assume that $f \mid gh$ in $R[X]$. Since f is irreducible in $K[X]$ by Proposition 3.5.10 (K is the ring of fractions of R), then it is prime, so let us assume that $g = ff_1$ for some $f_1 \in K[X]$. If we let $a \in R$, $a \neq 0$, be such that $af_1 \in R[X]$, then we get that $f \mid ag$ in $R[X]$, so $f \mid g$ in $R[X]$ by Exercise 3.5.8 iii). ∎

Theorem 3.5.12 (Gauss) *If R is a UFD, then $R[X]$ is a UFD.*

Proof: We use Theorem 3.5.6 ii). By Proposition 3.5.11, it is enough to show that any non-zero non-unit $f \in R[X]$ can be written as a finite product of irreducibles. We use induction on $deg(f)$. If $deg(f) = 0$, then $f \in R$ is a finite product of primes in R, which are primes in $R[X]$, and therefore irreducible. If $deg(f) \geq 1$ we can write $f = c(f)f_1$, where f_1 is primitive, so we can assume that f is primitive. If f is not irreducible, then $f = gh$, where $deg(g), deg(h) < deg(f)$. By the induction hypothesis, booth g and h are finite products of irreducibles, and therefore so is f. ∎

Corollary 3.5.13 *If R is a UFD, then $R[X_1, X_2, \ldots, X_n]$ is a UFD for $n \geq 1$.*

We end this section with some irreducibility criteria for polynomials with integer coefficients. If $p \in \mathbb{Z}$ is a prime number and $f \in \mathbb{Z}[X]$, we will denote by $\overline{f} \in \mathbb{Z}_p[X]$ the image of f via the ring morphism from $\mathbb{Z}[X]$ to $\mathbb{Z}_p[X]$ that sends X to X and each integer to its coset modulo p (see Theorem 2.6.13).

Theorem 3.5.14 (Schönemann's Criterion) *Let $f = g^n + ph$, where $g, h \in \mathbb{Z}[X]$, $p \in \mathbb{Z}$ is prime, $\overline{g} \in \mathbb{Z}_p[X]$ is irreducible, and $\overline{g} \nmid \overline{h}$ in $\mathbb{Z}_p[X]$. Then f is irreducible in $\mathbb{Q}[X]$.*

Proof: Assume that $f = f_1 f_2$, where $deg(f_1), deg(f_2) < deg(f)$, and $f_1, f_2 \in \mathbb{Q}[X]$. We can assume that $f_1, f_2 \in \mathbb{Z}[X]$, because we can write $f = \frac{a}{b} f' f''$, where $1 = (a, b)$ and $f', f'' \in \mathbb{Z}[X]$ are primitive. Then $bc(f) = a$, so $\frac{a}{b} \in \mathbb{Z}$. Now $\overline{g}^n = \overline{f} = \overline{f_1 f_2}$, and since $\overline{g}$ is irreducible we get that $\overline{f_1} = \overline{g}^k$ and $\overline{f_2} = \overline{g}^{n-k}$, where $k, n-k \geq 1$. Then $f_1 = g^k + ph_1$, and $f_2 = g^{n-k} + ph_2$, so $f = g^n + ph = (g^k + ph_1)(g^{n-k} + ph_2) = g^n + ph_1 g^{n-k} + ph_2 g^k + p^2 h_1 h_2$. It follows that $h = h_1 g^{n-k} + h_2 g^k + ph_1 h_2$, so $\overline{g} \mid \overline{h}$, a contradiction. ∎

Corollary 3.5.15 (Eisenstein's Criterion) *Let*

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X],$$

and $p \in \mathbb{Z}$ a prime such that $p \nmid a_n$, $p \mid a_0$, $p \mid a_1$, $\ldots$ $p \mid a_{n-1}$, and $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[X]$.

Proof: We can multiply f by an integer such that $a_n = a^n$, where $a \equiv 1 \pmod{p}$. Then we can write $f = (aX)^n + pg$, $\overline{a}X = X$ is irreducible in $\mathbb{Z}_p[X]$, and $X \nmid \overline{g}$ in $\mathbb{Z}_p[X]$ because $p^2 \nmid a_0$. The assertion then follows from Theorem 3.5.14. ∎

Exercise 3.5.16 *Let $p \in \mathbb{Z}$ be a prime. Use Eisenstein's Criterion to show that $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible in $\mathbb{Q}[X]$ (since it is primitive it will also be irreducible in $\mathbb{Z}[X]$). Can you also use Schönemann's Criterion?*

Exercise 3.5.17 *Show that for each $n \geq 1$ there exists an irreducible polynomial of degree n in $\mathbb{Z}[X]$.*

Proposition 3.5.18 (The Reduction Criterion) *Let $f \in \mathbb{Z}[X]$. If $\overline{f}$ is irreducible in $\mathbb{Z}_p[X]$ and $deg(f) = deg(\overline{f})$, then f is irreducible in $\mathbb{Q}[X]$.*

Proof: If $f = gh$, where $deg(g), deg(h) < deg(f)$, then $\overline{f} = \overline{g}\overline{h}$, and since $deg(\overline{g}) \leq deg(g)$ and $deg(\overline{h}) \leq deg(h)$, we have $deg(\overline{g}), deg(\overline{h}) < deg(f) = deg(\overline{f})$, a contradiction. ∎

An application of Proposition 3.5.18 is the following

Proposition 3.5.19 *If p is a prime number, and $p \nmid a$, then the Artin-Schreier polynomial $X^p - X + a \in \mathbb{Z}[X]$ is irreducible.*

Proof: We use Proposition 3.5.18 and prove that $X^p - X + \overline{a} \in \mathbb{Z}_p[X]$ is irreducible. If it is not, let $f \mid X^p - X + \overline{a}$, f irreducible, and $1 \leq deg(f) \leq p - 1$.

We have the following possibilities:

Case 1. $f(X) \neq f(X+\overline{a})$. In this case we have that $f(X+i\overline{a}) \neq f(X+j\overline{a})$ for all $0 \leq i \neq j \leq p-1$. Indeed, if $f(X+i\overline{a}) = f(X+j\overline{a})$ for some $i \neq j$, it follows, after replacing X by $X - i\overline{a}$, that $f(X) = f(X+k\overline{a})$, where $1 = (k,p)$, so $hk + np = 1$. We then get that $f(X) = f(X+hk\overline{a}) = f(X+\overline{a}-np\overline{a}) = f(X+\overline{a})$, a contradiction. We now write $X^p - X + \overline{a} = f(X)g(X)$, and we get that for $i \in \{0,1,\ldots,p-1\}$:

$$X^p - X + \overline{a} = (X+i\overline{a})^p - X - i\overline{a} + \overline{a} = f(X+i\overline{a})g(X+i\overline{a}),$$

where we used Fermat's Little Theorem (Exercise 2.3.16 viii)). It follows that $X^p - X + \overline{a}$ is divisible by p different polynomials, so each of them has degree one. Since $X^p - X + \overline{a}$ has no roots in $\mathbb{Z}_p$, this is a contradiction.

Case 2. $f(X) = f(X+\overline{a})$. In this case we have $f(X) = f(X+i\overline{a})$ for all $0 \leq i \leq p-1$. Let $g(X) = f(X) - f(0)$, which has degree at most $p-1$. We have that $g(0) = f(0) - f(0) = 0$, and $g(i\overline{a}) = f(i\overline{a}) - f(0) = f(0) - f(0) = 0$ for all $0 \leq i \leq p-1$. Then g has p roots, so $g = 0$, which means that $f(X) = f(0)$, which contradicts $1 \leq deg(f) \leq p-1$. ∎

Exercise 3.5.20 *For a domain R, the following assertions are equivalent:*
i) R is a UFD.
ii) Any non-zero prime ideal of R contains a prime element.

Proposition 3.5.21 (Nagata) *Let R be a domain with the property that every ascending chain of principal ideals of R:*

$$a_1R \subseteq a_2R \subseteq a_3R \subseteq \ldots$$

stabilizes. If S is a multiplicative subset whose elements are products of primes, and $S^{-1}R$ is UFD, then R is UFD.

Proof: Assume that the elements in S are products of prime elements from $\{p_i\}_{i\in I}$. Let $P \neq \{0\}$ be a prime ideal of R. If $P \cap S \neq \emptyset$, then P contains a prime. Assume this is not true. We therefore have that $P \cap S = \emptyset$, and by Exercise 2.5.13 i) we get that $S^{-1}P = \{\frac{p}{s} \mid p \in P, s \in S\}$ is a prime ideal of $S^{-1}R$. It follows that $S^{-1}P$ contains a prime $\frac{p}{s}$ in $S^{-1}R$, and therefore $\frac{p}{1} \in S^{-1}P$ and $\frac{p}{1}$ is prime in $S^{-1}R$. Let $p \mid ab$. It follows that $\frac{p}{1} \mid \frac{a}{1}$ or $\frac{p}{1} \mid \frac{b}{1}$. If $\frac{p}{1} \mid \frac{a}{1}$, then $ap_1p_2\cdots p_k = pc$. If none of the p_i divides p, then all $p_i \mid c$ and so $p \mid a$. If $p_i \mid p$, then $p = a_ip_i$. If some $p_j \mid p_i$, we have $a_i = a_{i+1}p_j$, and so on. We get the ascending chain of principal ideals of R:

$$pR \subseteq a_i \subseteq a_{i+1}R \subseteq a_{i+2}R \subseteq \ldots,$$

which stabilizes at a_jR. Then we can replace p by a_j, since $\frac{a_j}{1} \in S^{-1}R$ is still prime, and we are done. ∎

Exercise 3.5.22 *Let p be a prime element in the domain R, and $S = \{1, p, p^2, p^3, \ldots\}$. If $S^{-1}R$ is UFD, then R is UFD.*

Solutions to the Exercises on Section 3.5

Exercise 3.5.1 *Let R be a domain, and assume that $p_1, p_2, \ldots, p_n$, and $q_1, q_2, \ldots q_m$ are prime elements of R such that*

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

Then $n = m$ and each of the p_i is associated in divisiblity to one of the q_j.
Solution: This is identical to the proof of uniqueness in Theorem 1.2.23. Assume that $n > m$ and look for a contradiction. We have that $p_1 \mid q_1 q_2 \cdots q_m$, so we can assume that $p_1 \mid q_1$. Since q_1 is prime, it is irreducible, so $p_1 \sim_d q_1$. Then, since R is a domain, we can cancel p_1 from both sides, and continue until we cancel p_1 through p_m. But then p_{m+1} divides a unit and it therefore has to be a unit, a contradiction.

Exercise 3.5.3 *A PID is a UFD.*
Solution: This follows from Theorem 3.4.7.

Exercise 3.5.4 *In a UFD, any irreducible is prime.*
Solution: Let $q \in R$ be an irreducible. Since $q \neq 0$ and $q \notin U(R)$, q has to be divisible by a prime, so it has to be associated in divisibility with it.

Exercise 3.5.5 *Let R be a UFD. If $a, b \in R \setminus \{0\}$ have factorizations as in (3.3)*

$$a = u \prod_{i \in I} p_i^{m_i}, \quad b = v \prod_{i \in I} p_i^{n_i}.$$

Show that:
i) If $d = \prod_{i \in I} p_i^{k_i}$, where $k_i = \min\{m_i, n_i\}$, then $d = (a, b)$.
ii) If $m = \prod_{i \in I} p_i^{l_i}$, where $l_i = \max\{m_i, n_i\}$, then $m = [a, b]$.
iii) R is a GCD-domain.
iv) If $a, b_1, b_2, \ldots, b_n \in R$ satisfy $1 = (a, b_i)$ for $1 \leq i \leq n$, then $1 = (a, b_1 b_2 \cdots b_n)$.
Solution: i) As in the solution to Exercise 3.5.1, we get that $\prod_{i \in I} p_i^{r_i} \mid \prod_{i \in I} p_i^{t_i}$ if and only if $r_i \leq t_i$, $\forall i \in I$.
ii) $[a, b] = ab/(a, b)$.
iii) If one of a or b is 0, then (a, b) is the other one.
iv) By iii) we can use induction and Exercise 3.1.18, but we can also prove this by showing that no prime p can divide a and $b_1 b_2 \cdots b_n$. Indeed, such a prime would have to divide a b_i, and so it would have to divide $(a, b_i) = 1$, a contradiction.

Exercise 3.5.8 *Let R be a UFD, and $f, g \in R[X]$. Then:*
i) If $c(f) = c(g) = 1$, then $c(fg) = 1$ (i.e. the product of primitive polynomials is primitive).

ii) In general, $c(fg) \sim_d c(f)c(g)$.
iii) If $a \in R$, $a \neq 0$, g *is primitive, and* $g \mid af$, *then* $g \mid f$.
iv) If both f *and* g *are primitive and* $af = bg$, $a, b \in R \setminus \{0\}$, *then* $f \sim_d g$.
Solution: i) follows from Proposition 3.2.6: if $p \in R$ is a prime element and $p \mid fg$, then $p \mid f$ of $p \mid g$.
ii) We write $f = c(f)f_1$ and $g = c(g)g_1$, where f_1, g_1 are primitive. Then $fg = c(f)c(g)f_1g_1$, and so $c(fg) \sim_d c(f)c(g)c(f_1g_1) \sim_d c(f)c(g)$, by i).
iii) There is an $h \in R[X]$ such that $af = hg$. Then by ii) we get that $ac(f) = c(h)$, so we can write $h = ac(f)h'$, and so $af = ac(f)h'g$, and after canceling the a we get that $g \mid f$.
iv) follows from iii).

Exercise 3.5.9 *Let* F *be a field, and* $f \in F[X]$. *Prove the following assertions:*
i) If $deg(f) = 1$, *then* f *is irreducible.*
ii) If $deg(f)$ *is 2 or 3, then* f *is irreducible if and only if* f *has no roots.*
iii) $F[X]/(X - a)F[X] \simeq F$.
iv) If $a, b \in F$, $a \neq b$, *then* $1 = (X - a, X - b)$.
Solution: i) 1 cannot be written as the sum of two positive integers.
ii) If 2 or 3 is written as the sum of two positive integers, one of them has to be 1. If f is divisible by the degree 1 polynomial $aX - b$, then ba^{-1} is a root of f by Corollary 3.3.7.
iii) Let $\phi : F[X] \longrightarrow F$ be the ring morphism from Theorem 2.6.13 sending X to a. By Corollary 3.3.7, $Ker(\varphi) = (X - a)F[X]$, and we can use Corollary 2.3.9.
iv) The Euclidean algorithm for $X - a$ and $X - b$ has one step: $X - a = (X - b) \cdot 1 + (b - a)$.

Exercise 3.5.16 *Let* $p \in \mathbb{Z}$ *be a prime. Use Eisenstein's Criterion to show that* $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ *is irreducible in* $\mathbb{Q}[X]$ *(since it is primitive it will also be irreducible in* $\mathbb{Z}[X]$*). Can you also use Schönemann's Criterion?*
Solution: It is clear that $f(X)$ is irreducible if and only if $f(X+1)$ is irreducible. But $f(X)) = \frac{X^p-1}{X-1}$, so $f(X+1) = \dfrac{(X+1)^p - 1}{X} = \displaystyle\sum_{k=1}^{p} \binom{p}{k} X^k$, and since $p \mid \binom{p}{k}$ for $k = 1, \ldots, p-1$, the leading coefficient is 1, and the free term is p, we can use Theorem 3.5.14.

In order to apply Schönemann's Criterion, observe that $p \mid (X-1)^p - X^p + 1$, so $(X-1)^p - (X^p - 1) = -p(X-1)g$ for some $g \in \mathbb{Z}[X]$. Then $f(X) = \frac{X^p-1}{X-1} = (X-1)^{p-1} + pg$, from where we can see that $p \nmid 1 = g(1)$, i.e. $X - 1 \nmid g$ in $\mathbb{Z}_p[X]$.

Exercise 3.5.17 *Show that for each $n \geq 1$ there exists an irreducible polynomial of degree n in $\mathbb{Z}[X]$.*
Solution: Apply Theorem 3.5.14 to the primitive polynomial $X^n - 2$ for $p = 2$.

Exercise 3.5.20 *For a domain R, the following assertions are equivalent:*
i) R is a UFD.
ii) Any non-zero prime ideal of R contains a prime element.
Solution: i) $\Rightarrow$ ii). Let P be a non-zero prime ideal, and $0 \neq x \in P$. By Definition 3.5.2, x is a product of primes, so P will have to contain one of them.
ii) $\Rightarrow$ i). Let

$$S = \{p_1 p_2 \cdots p_k \mid p_i \text{ are prime elements in } R\}.$$

As in the solution to Exercise 3.5.1, S is saturated: if $ab = p_1 p_2 \cdots p_k$, then, after renaming the primes, $a = up_1 p_2 \cdots p_i$ and $b = vp_{i+1} p_{i+2} \cdots p_k$, where $uv = 1$. If $a \neq 0$ and $a \notin U(R)$, such that $a \notin S$, then $aR \cap S = \emptyset$ because S is saturated. But by Proposition 2.5.16, a belongs to a prime P disjoint from S, and this is a contradiction (the hypothesis ensures that no primes are disjoint from S).

Exercise 3.5.22 *Let p be a prime element in the domain R, and $S = \{1, p, p^2, p^3, \ldots\}$. If $S^{-1}R$ is UFD, then R is UFD.*
Solution: Let P be a non-zero prime ideal of R. We can assume $P \cap S = \emptyset$, so $S^{-1}P$ contains a prime element $\frac{q}{1} \in S^{-1}R$. We can assume $p \nmid q$. If $q \mid ab$, then $\frac{q}{1} \mid \frac{a}{1} \cdot \frac{b}{1}$, so let's say $\frac{q}{1} \mid \frac{a}{1}$. This means that $ap^k = qc$ for some k and c, and since $p \nmid q$ we get that $p^k \mid c$, so $q \mid a$ and we are done.

3.6 Roots of polynomials

We start this section with a warm-up: finding relations between the roots of a polynomial and its coefficients. They extend the well-known formulas for the sum and the product of the roots of a quadratic equation.

Proposition 3.6.1 (Vieta's Formulas) *Let R be a domain, and $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in R[X]$ a polynomial of degree n. If $x_1, x_2, \ldots, x_n$ are roots of f in a domain T that contains R as a subring, then*

$$f = a_n(X - x_1)(X - x_2)\cdots(X - x_n)$$

and

$$a_n\left(\sum_{1\leq i_1<i_2<\ldots i_k\leq n} x_{i_1}x_{i_2}\cdots x_{i_k}\right) = (-1)^k a_{n-k},\ \ k \in \{1, 2, \ldots n\}$$

Proof: The first equality is obtained by applying Bézout's Theorem (Corollary 3.3.7) n times, to get $f = g(X - x_1)(X - x_2)\cdots(X - x_n)$ for some $g \in T[X]$. It follows that $\deg(g) = 0$, and $g = a_n$ by identifying the coefficients of X^n on the left and the right. The other n equalities follow by identifying the other n pairs of coefficients. ∎

Exercise 3.6.2 *If x_1, x_2, x_3 are the roots of $X^3 - 3X^2 + 1 \in \mathbb{Z}[X]$, find $x_1^4 + x_2^4 + x_3^4 - 4(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$.*

Finding roots of polynomials, i.e. solving polynomial equations, is a very old sport. The following result shows that in this sport you can easily score if you enlarge the goal.

Proposition 3.6.3 *Let K be a field and $f \in K[X]$, $\deg(f) = n \geq 1$. Then there exists a field L that contains K as a subfield (such an L is called a* field extension *of K) such that f has n (not necessarily distinct) roots in L.*

Proof: Induction on n. If $n = 1$, it is clear that f has a root in K, so in this case we can take $L = K$. We now assume that $n > 1$ and the assertion is true for polynomials of degree at most $n - 1$. Since $K[X]$ is a UFD, we let f_1 be irreducible in $K[X]$ such that $f = f_1f_2$. Since $K[X]$ is a PID, the ideal generated by f_1 is maximal, so $L_1 = K[X]/(f_1K[X])$ is a field. Since the composition of the canonical injection $K \longrightarrow K[X]$ with the canonical surjection $K[X] \longrightarrow K[X]/(f_1K[X])$ is injective (what is its kernel?), we can identify K with its image through it, and assume that L_1 is an extension of K. If we denote the coset of X modulo $f_1K[X]$ by $\overline{X}$,

it is clear that $x_1 = \overline{X}$ is a root of f_1, and hence a root of f. By Bézout's Theorem (Corollary 3.3.7), we can write $f = (X - x_1)g$, where $g \in L_1[X]$ and $\deg(g) = n - 1$. By the induction hypothesis there exists an extension L of L_1 which contains $n - 1$ roots for g, and if we add x_1 to this set, we find n roots of f in L. ∎

We use Proposition 3.6.3 to extend $\mathbb{R}$ to $\mathbb{C}$ as described in the introduction.

Corollary 3.6.4 *Consider the polynomial $X^2 + 1 \in \mathbb{R}[X]$. Then:*
i) There exists L an extension of $\mathbb{R}$ such that $X^2 + 1$ has both roots in L.
ii) $L \simeq \mathbb{C}$.

Proof: i) Since $X^2 + 1$ is irreducible in $\mathbb{R}[X]$ (it has no roots in $\mathbb{R}$), $L = \mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$ is a field that we may assume is an extension of $\mathbb{R}$. X^2+1 has both roots in L, they are $\overline{X}$ and $-\overline{X}$ (where $\overline{X}$ denotes again the coset of X modulo $(X^2+1)\mathbb{R}[X]$). By the division algorithm, the elements of $L = \mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$ can be written as $\overline{(X^2+1)q + a + bX} = a + b\overline{X}$, where $q \in \mathbb{R}[X]$ and $a, b \in \mathbb{R}$.
ii) The map from L to $\mathbb{C}$ sending $a + b\overline{X}$ to $a + bi$ is an isomorphism. ∎

Note that Corollary 3.6.4 gives the description of the complex number i announced in the introduction: i is "the coset of the indeterminate in the factor ring of the polynomial ring in one indeterminate X with real coefficients factored through the principal ideal generated by the polynomial $X^2 + 1$", and therefore $\mathbb{C}$ can be constructed as $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1) = \mathbb{R}[X]/(X^2 + 1)\mathbb{R}[X]$. Next, as it was also mentioned in the introduction, we see that we cannot extend $\mathbb{C}$ to a larger field by adding solutions to polynomial equations with complex coefficients. This is the next result, which says that $\mathbb{C}$ is algebraically closed. All known proofs of this result use results from outside algebra. The proof presented here, essentially due to Lagrange, keeps those to a minimum. A very spectacular proof uses Liouville's Theorem from complex analysis. If you did not take a complex analysis class yet, it might be an excellent idea to do that next. If this is not possible, an acceptable alternative could be reading George Cain's book [9].

Theorem 3.6.5 (The Fundamental Theorem of Algebra) *Any polynomial $f \in \mathbb{C}[X]$, $\deg(f) \geq 1$, has a root in $\mathbb{C}$.*

Proof: First, assume that $f \in \mathbb{R}[X]$ and $n = \deg(f) = 2^k m$, where m is odd. We prove by induction on k that f has a root in $\mathbb{C}$.
If $k = 0$, then, if we also denote by f the real polynomial function defined by f, we have that $\lim_{x\to\infty} f(x)f(-x) = -\infty$ since n is odd, so f has a real

zero because it has the intermediate value property. We also note that a quadratic polynomial with complex coefficients has two complex roots, by the fact that each complex number has a square root and the quadratic formula.

We assume now that $k > 0$ and the assertion is true for the maximum power of 2 dividing $n = \deg(f)$ less than or equal to $k-1$. By Proposition 3.6.3 there exists a field L, an extension of $\mathbb{C}$, such that f has roots $x_1, x_2, \ldots, x_n \in L$. For $a \in \mathbb{R}$, consider the elements

$$u_{ij}^a = x_i x_j + a(x_i + x_j) \in L,$$

and the polynomial

$$g_a = \prod_{1 \leq i < j \leq n} (X - u_{ij}^a) \in L[X],$$

which has degree $\frac{n(n+1)}{2}$, which is divisible by 2^{k-1} but not by 2^k. The coefficients of g_a are symmetric polynomials of the u_{ij}^a, and therefore also symmetric polynomials of $x_1, x_2, \ldots, x_n$, so by Theorem 2.7.11 and Proposition 3.6.1 $g_a \in \mathbb{R}[X]$. By the induction hypothesis, g_a has a complex root, and this is true for all $a \in \mathbb{R}$. Since $\mathbb{R}$ is infinite and the set of pairs $1 \leq i < j \leq n$ is finite, there exist $a, b \in \mathbb{R}$, $a \neq b$, and i, j, $1 \leq i < j \leq n$, such that $u_{ij}^a, u_{ij}^b \in \mathbb{C}$. But then

$$u_{ij}^a - u_{ij}^b = (a-b)(x_i + x_j) \in \mathbb{C},$$

and so $x_i + x_j \in \mathbb{C}$, and therefore $x_i x_j \in \mathbb{C}$ as well. It follows that x_i and x_j are the roots of a quadratic polynomial with complex coefficients, and therefore they are complex numbers.

Assume now that $f \in \mathbb{C}[X]$, $f = a_0 + a_1 X + \ldots + a_n X^n$, and let $\overline{f}$ be the polynomial whose coefficients are the complex conjugates of the coefficients of f:

$$\overline{f} = \overline{a_0} + \overline{a_1} X + \ldots + \overline{a_n} X^n.$$

Then each coefficient of $f\overline{f}$ is equal to its complex conjugate, i.e. $f\overline{f} \in \mathbb{R}[X]$, so it has a complex root z. But then $f(z)\overline{f}(z) = f(z)\overline{f(\overline{z})} = 0$, and so either z is a root of f, or z is a root of $\overline{f}$, i.e. $\overline{z}$ is a root of f, and the proof is complete. ∎

We have seen in Exercise 3.5.17 that in $\mathbb{Q}[X]$ there are irreducible polynomials of any degree ≥ 1.

Exercise 3.6.6 *i) Prove that an irreducible polynomial in $\mathbb{C}[X]$ has degree 1.*
ii) Prove that an irreducible polynomial in $\mathbb{R}[X]$ has degree 1 or degree 2 and no real roots.

We will now prove a theorem that you used in Mrs. Turner's 3^{rd} grade calculus class: the Partial Fractions Decomposition Theorem. Remember that Mrs. Turner told you that even though you are using this theorem in calculus, the proof actually uses arithmetic in polynomial rings.

Theorem 3.6.7 *Let $f, g \in \mathbb{R}[X]$, $\deg(f) < \deg(g)$ and $(f, g) = 1$. If g factors as a product of irreducible polynomials like this:*

$$g = (X - a_1)^{k_1} \cdots (X - a_m)^{k_m} \cdot$$

$$\cdot (X^2 + b_1 X + c_1)^{l_1} \cdots (X^2 + b_n X + c_n)^{l_n},$$

then there exist real numbers A_j^i, B_j^i, C_j^i such that

$$\frac{f}{g} = \frac{A_1^1}{X - a_1} + \cdots + \frac{A_{k_1}^1}{(X - a_1)^{k_1}} + \cdots +$$

$$+ \frac{B_1^n X + C_1^n}{X^2 + b_n X + c_n} + \cdots + \frac{B_{l_n}^n X + C_{l_n}^n}{(X^2 + b_n X + c_n)^{l_n}}.$$

Proof: We start with a rational fraction $\frac{f}{g_1 g_2}$, where $f, g_1, g_2 \in \mathbb{R}[X]$ are pairwise relatively prime and $\deg(f) < \deg(g_1 g_2)$. We will find $f_1, f_2 \in \mathbb{R}[X]$ such that $\deg(f_1) < \deg(g_1)$, $\deg(f_1) < \deg(g_1)$, and

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}.$$

Since $(g_1, g_2) = 1$, there exist $h_1, h_2 \in \mathbb{R}[X]$ such that

$$f = h_1 g_1 + h_2 g_2 \tag{3.4}$$

Using the division algorithm in $\mathbb{R}[X]$ we can write

$$h_2 = q g_1 + f_1, \quad \text{where } \deg(f_1) < \deg(g_1). \tag{3.5}$$

Using (3.5) in (3.4), distributing g_2, factoring out g_1, and denoting $f_2 = h_1 + q g_2$, we get

$$f = f_1 g_2 + f_2 g_1,$$

and so

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}.$$

The only thing left to prove is that $\deg(f_2) < \deg(g_2)$. We assume that $\deg(f_2) \geq \deg(g_2)$, and look for a contradiction. Then we have

$$\deg(f_2 g_1) \geq \deg(g_1 g_2) > \deg(f_1 g_2),$$

and so

$$\deg(f) = \deg(f_2 g_1) \geq \deg(g_1 g_2),$$

wich contradicts the hypotesis.

Now we use what we just proved for $g_1 = p^k$, $p \in \mathbb{R}[X]$ irreducible (and therefore of degree 1 or 2 by Exercise 3.6.6 ii)), and $g = g_1 g_2$ such that $p \nmid g_2$. We get

$$\frac{f}{p^k g_2} = \frac{f_1}{p^k} + \frac{f_2}{g_2},$$

where $\deg(f_1) < k \deg(p)$, and $\deg(f_2) < \deg(g_2)$. We now use repeatedly the divison algorithm to get

$$\begin{aligned}
\frac{f_1}{p^k} &= \frac{q_1 p + r_1}{p^k} \\
&= \frac{r_1}{p^k} + \frac{q_1}{p^{k-1}} \\
&= \frac{r_1}{p^k} + \frac{q_2 p + r_2}{p^{k-1}} \\
&= \frac{r_1}{p^k} + \frac{r_2}{p^{k-1}} + \frac{q_2}{p^{k-2}} \\
&\cdots \\
&= \frac{r_1}{p^k} + \frac{r_2}{p^{k-1}} + \ldots + \frac{r_{k-2}}{p^3} + \frac{q_{k-2}}{p^2} \\
&= \frac{r_1}{p^k} + \frac{r_2}{p^{k-1}} + \ldots + \frac{r_{k-2}}{p^3} + \frac{r_{k-1}}{p^2} + \frac{q_{k-1}}{p}.
\end{aligned}$$

If $\deg(p) = 1$, then $r_1, r_2, \ldots, r_{k-1}, q_{k-1} \in \mathbb{R}$, and if $\deg(p) = 2$, then $r_1, r_2, \ldots, r_{k-1}, q_{k-1} \in \mathbb{R}[X]$ all have degree at most one. We continue working on $\dfrac{f_2}{g_2}$ in a similar way until we exhaust all powers of irreducibles that divide g. ∎

If you were wondering when you will learn what "algebraically closed" means, the wait is over.

Definition 3.6.8 *If K is a field, an element α in a field extension of K is said to be* algebraic *over K if α is the root of a polynomial in $K[X]$. If any algebraic element over K is in K, we say that K is* algebraically closed. *A complex number which is algebraic over $\mathbb{Q}$ is called an* algebraic number.

Exercise 3.6.9 *Which of the fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are algebraically closed?*

Theorem 3.6.10 (Weak form of Hilbert's Nullstellensatz over $\mathbb{C}$) *If M is a maximal ideal of the polynomial ring $\mathbb{C}[X_1, X_2, \ldots, X_n]$, then*

$$\mathbb{C} = \mathbb{C}[X_1, X_2, \ldots, X_n]/M.$$

Proof: (Kaplansky) If $\mathbb{C} \subsetneq \mathbb{C}[X_1, X_2, \ldots, X_n]/M$, then

$$\exists t \in \mathbb{C}[X_1, X_2, \ldots, X_n]/M$$

transcendental over $\mathbb{C}$, because $\mathbb{C}$ is algebraically closed. The family

$$\left\{ \frac{1}{t-\alpha} \right\}_{\alpha \in \mathbb{C}}$$

is linearly independent, because the top of any non-trivial linear combination equal to 0 produces a polynomial with complex coefficients which has t as a root. This contadicts the fact that $\mathbb{C}[X_1, X_2, \ldots, X_n]/M$ is spanned by the cosets of the monomials, which is a countable set. ∎

Exercise 3.6.11 *i) Show that if K is a field and $a_1, a_2, \ldots, a_n \in K$, then the ideal generated by $X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n$ is maximal in $K[X_1, X_2, \ldots, X_n]$.*
ii) If M is a maximal ideal of $\mathbb{C}[X_1, X_2, \ldots, X_n]$, then M is generated by $X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n$, for some $a_1, a_2, \ldots, a_n \in \mathbb{C}$.

Exercise 3.6.12 *Let K be a field, and α an algebraic element over K. Then α is a root for a unique monic polynomial $Irr(\alpha, K)$, which divides any polynomial in $K[X]$ that has α as a root. $Irr(\alpha, K)$ is called the* minimal polynomial *of α over K. The* degree *of α is* $\deg(Irr(\alpha, K))$. *(Hint: start by choosing a polynomial with the lowest degree among all polynomials in $K[X]$ that have α as a root.)*

Definition 3.6.13 *Let R be a domain. An element of a domain that contains R as a subring is called* integral *over R if it is the root of a monic polynomial in $R[X]$. If any element in the field of fractions of R which is integral over R is in R, then R is said to be* integrally closed. *An algebraic number that is integral over $\mathbb{Z}$ is called an* algebraic integer. *Since the word "algebraic" in "algebraic integer" is sometimes omitted, the elements of $\mathbb{Z}$ are also called* rational integers *in order to avoid confusion.*

Real numbers that are not algebraic numbers are called *transcendental*. It may be proved that e and π are transcendental. The number i is obviously an algebraic integer.

Exercise 3.6.14 *Prove that $\mathbb{Z}$ is integrally closed.*

Exercise 3.6.15 *i) Give an example of an algebraic integer that is not a rational integer.*
ii) Give an example of an algebraic number that is not an algebraic integer.

Exercise 3.6.16 *If α is an algebraic integer, then $Irr(\alpha, K) \in \mathbb{Z}[X]$.*

Theorem 3.6.17 *Let R be a domain, K its field of fractions, and $n \in \mathbb{N}$, $n \geq 1$. Assume that $\alpha, \theta_1, \theta_2, \ldots, \theta_n$, are elements in an extension of K such that $\theta_1, \theta_2, \ldots, \theta_n$ are not all zero and the following equalities are satisfied:*

$$\alpha\theta_i = a_{i1}\theta_1 + a_{i2}\theta_2 + \ldots + a_{in}\theta_n, \quad i = 1, 2, \ldots, n, \tag{3.6}$$

where the n^2 coefficients $a_{ij} \in K$. Then α is algebraic over K. Moreover, if $a_{ij} \in R$ for all $1 \leq i, j \leq n$, then α is integral over R.

Proof: We use a result from linear algebra (see e.g. [35]): since the homogeneous system (3.6) has a non-trivial solution, its determinant has to be zero:

$$\begin{vmatrix} \alpha - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \alpha - a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} & \cdots & \alpha - a_{nn} \end{vmatrix} = 0$$

After expanding the determinant we get $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$, where the b_k are sums of products of the elements $-a_{ij}$. Hence $b_k \in K$, and $b_k \in R$ if $a_{ij} \in R$. ∎

Corollary 3.6.18 *Let R be a domain, and K its field of fractions. If α and β are algebraic over K, then $\alpha + \beta$ and $\alpha\beta$ are algebraic over K. If α and β are integral over R, then $\alpha + \beta$ and $\alpha\beta$ are algebraic over R. Therefore, the elements algebraic over K in a field extension L of K form a field, called the* algebraic closure *of K in L, and the elements integral over R in a domain T that contains R as a subring form a ring, called the* integral closure *of R in T.*

Proof: Assume that α and β satisfy

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0,$$

$$\beta^r + b_{r-1}\beta^{r-1} + \cdots + b_1\beta + b_0 = 0,$$

where $a_i, b_j \in K$. Let $n = mr$, and define $\theta_1, \theta_2, \ldots, \theta_n$ as the elements

$$\begin{array}{ccccc} 1, & \alpha, & \alpha^2, & \cdots, & \alpha^{m-1}, \\ \beta, & \alpha\beta, & \alpha^2\beta, & \cdots, & \alpha^{m-1}\beta, \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \beta^{r-1}, & \alpha\beta^{r-1}, & \alpha^2\beta^{r-1}, & \cdots, & \alpha^{m-1}\beta^{r-1}, \end{array}$$

in any order. Thus $\theta_1, \theta_2, \ldots, \theta_n$ are the elements $\alpha^s\beta^t$, where $0 \leq s \leq m-1$ and $0 \leq t \leq r-1$. Hence, for any i we have

$$\alpha\theta_i = \alpha^{s+1}\beta^t = \begin{cases} \text{some } \theta_k & \text{if } s+1 \leq m-1 \\ (-a_{m-1}\alpha^{m-1} - \cdots - a_1\alpha - a_0)\beta^t & \text{if } s+1 = m \end{cases}$$

Therefore we can find $h_{i1}, h_{i2}, \ldots, h_{in} \in K$ such that

$$\alpha\theta_i = h_{i1}\theta_1 + h_{i2}\theta_2 + \ldots + h_{in}\theta_n.$$

Similarly, we find $k_{i1}, k_{i2}, \ldots, k_{in} \in K$ such that

$$\beta\theta_i = k_{i1}\theta_1 + k_{i2}\theta_2 + \ldots + k_{in}\theta_n,$$

and so

$$(\alpha+\beta)\theta_i = (h_{i1}+k_{i1})\theta_1 + (h_{i2}+k_{i2})\theta_2 + \ldots + (h_{in}+k_{in})\theta_n,$$

which are of the form (3.6), and so $\alpha+\beta$ is algebraic over K. Moreover, if α and β are integral over R, then $a_i, b_i, h_{ij}, k_{ij} \in R$, and $\alpha+\beta$ is integral over R.
Now we have

$$\begin{aligned} (\alpha\beta)\theta_i &= \alpha(\sum_j k_{ij}\theta_j) \\ &= \sum_j k_{ij}\alpha\theta_j \\ &= \sum_j k_{ij}\sum_l h_{jl}\theta_l \\ &= \sum_l (\sum_j k_{ij}h_{jl})\theta_l, \end{aligned}$$

and we can apply again Theorem 3.6.17 to conclude that $\alpha\beta$ is algebraic over K, and that it is integral over R if α and β are.
The only other things left that are worth proving are the following:
If α is algebraic over K, $\alpha \neq 0$, and $Irr(\alpha, K) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$, then $a_0 \neq 0$ and

$$a_0(\alpha^{-1})^m + a_1(\alpha^{-1})^{m-1} + \cdots + a_{m-1}\alpha^{-1} + 1 = 0,$$

so α^{-1} is algebraic over K (note that if α is integral over R, α^{-1} is not integral over R if $a_0 \notin U(R)$).
If α satisfies

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0,$$

then $-\alpha$ satisfies

$$\alpha^m - a_{m-1}\alpha^{m-1} + \cdots + (-1)^{m-1}a_1\alpha + (-1)^m a_0 = 0.$$

∎

Corollary 3.6.19 *The algebraic numbers form a field, and the algebraic integers form a ring. We will denote the ring of algebraic integers by* $\mathbb{A}$.

Exercise 3.6.20 *Let* $d \in \mathbb{Z} \setminus \{0, \pm 1\}$ *be square-free, i.e.* $p \nmid d\ \forall p \in \mathbb{Z}$ *a prime number. Then*

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

is a field.

Definition 3.6.21 $\mathbb{Q}(\sqrt{d})$*, as in Exercise 3.6.20, is called a* quadratic field*. The ring of algebraic integers in a quadratic field will be called a* ring of quadratic integers*.*

Exercise 3.6.22 *Let* $\mathbb{Q}(\sqrt{d})$ *be a quadratic field, and denote by* A *the ring of algebraic integers in* $\mathbb{Q}(\sqrt{d})$ *(see Corollary 3.6.18). If* $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$*, we denote by*

$$Tr(z) = z + \overline{z} = 2a, \text{ and } N(z) = z\overline{z} = a^2 - b^2 d.$$

Prove that:
i) $A = \{z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \mid Tr(z), N(z) \in \mathbb{Z}\}$.
ii) $z \in A \Leftrightarrow u = 2a \in \mathbb{Z}$, $v = 2b \in \mathbb{Z}$, $u^2 - v^2 d \equiv 0$ *(mod 4).*
iii) If $z_1 = a_1 + b_1\sqrt{d}, z_2 = a_2 + b_2\sqrt{d} \in A$, *then* $2(a_1a_2 + b_1b_2d) \in \mathbb{Z}$.

Theorem 3.6.23 *Let* $\mathbb{Q}(\sqrt{d})$ *be a quadratic field, and* A *its ring of integers. Then*

$$A = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 (mod\ 4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 1 (mod\ 4) \end{cases}$$

Proof: If $z = a + b\sqrt{d} \in A$ and $d \equiv 2 (\text{mod } 4)$ we have

$$\begin{array}{cccccc} u & even & odd & even & odd & \\ v & even & even & odd & odd & \\ u^2 - 2v^2 & \equiv 0 & \equiv 1 & \equiv 2 & \equiv 3 & (\text{mod } 4) \end{array}$$

and if $d \equiv 2 (\text{mod } 4)$, we have

$$\begin{array}{cccccc} u & even & odd & even & odd & \\ v & even & even & odd & odd & \\ u^2 + v^2 & \equiv 0 & \equiv 1 & \equiv 1 & \equiv 2 & (\text{mod } 4) \end{array}$$

so if $d \equiv 2, 3 \pmod 4$ $u = 2a$ and $v = 2b$ are both even, so both a and b are in $\mathbb{Z}$.

If $d \equiv 1 (\text{mod } 4)$, we have

$$\begin{array}{cccccc} u & even & odd & even & odd & \\ v & even & even & odd & odd & \\ u^2 - v^2 & \equiv 0 & \equiv 1 & \equiv 3 & \equiv 0 & (\text{mod } 4) \end{array}$$

so in this case

$$A = \left\{ \frac{u}{2} + \frac{v}{2} d \;\middle|\; u, v \in \mathbb{Z} \text{ have the same parity} \right\}.$$

We need to show that

$$A = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2} \right].$$

For $\supseteq$, $a + b\frac{1+\sqrt{d}}{2} = \frac{2a+b}{2} + \frac{b}{2}\sqrt{d}$.
For $\subseteq$ we have, if $u = 2a$ and $v = 2b$, that $a + b\sqrt{d} = a - b + 2b\frac{1+\sqrt{d}}{2}$.
If $u = 2a + 1$ and $v = 2b + 1$, then

$$\frac{2a+1}{2} + \frac{2b+1}{2}\sqrt{d} =$$

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

$$= a - b + (2b+1)\frac{1+\sqrt{d}}{2},$$

and the proof is complete. ∎

Exercise 3.6.24 *i) Let $R \subseteq T \subseteq T'$, where R, T, and T' are domains. Then:*
i) If $\gamma \in T'$ is a root of

$$X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0 \in T[X],$$

and b_i are integral over R, for each $i = 0, 1, \ldots, n-1$, then γ is integral over R.
ii) If K is the field containing the field of fractions of R, and T is the integral closure of R in K, then T is integrally closed. In particular, a ring of quadratic integers and the ring of algebraic integers are integrally closed.

The quadratic field $\mathbb{Q}(\sqrt{d})$ is called real if $d > 0$, and imaginary if $d < 0$. One of the most important questions about quadratic fields was to determine for which values of d the ring of integers A is a PID. For imaginary quadratic fields, Gauss found in 1801 that this is true if

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163,$$

and conjectured that there are only finitely many such values of d. Heilbronn and Linfoot proved in 1934 that there are no more than 10 negative values of d for which this happens, alnd thus gave an affirmative answer to Gauss's conjecture. Then a theorem of Baker, Heegner, and Stark (which had various proofs, from the early 1950s to the late 1960s) established that the nine values found by Gauss are in fact the only ones.
For the same question in the case of real quadratic fields almost nothing is known. Gauss conjectured that there are infinitely many real quadratic fields for which the ring of integers is a PID.

For us, Theorem 3.6.23 gives new information about two rings that we studied. We showed in Proposition 3.1.10 that $\mathbb{Z}[i\sqrt{5}]$ is not a GCD-domain, and therefore it is not a UFD. We now know that $\mathbb{Z}[i\sqrt{5}]$ is not integrally closed, because the ring of integers of the quadratic field $\mathbb{Q}(i\sqrt{5})$ is $\mathbb{Z}\left[\frac{1+i\sqrt{5}}{2}\right] \supsetneq \mathbb{Z}[i\sqrt{5}]$. In order to show that $\mathbb{Z}[i\sqrt{5}]$ is not a UFD we can use the following:

Exercise 3.6.25 *If R is a UFD or a GCD-domain, then R is integrally closed.*

We proved in Proposition 3.4.11 that $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is a PID. Now we see from Theorem 3.6.23 that this is a ring of quadratic integers. It is actually one of the rings on Gauss's list of nine PIDs.

Solutions to the Exercises on Section 3.6

Exercise 3.6.2 *If x_1, x_2, x_3 are the roots of $X^3 - 3X^2 + 1 \in \mathbb{Z}[X]$, find $x_1^4 + x_2^4 + x_3^4 - 4(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)$.*
Solution: The expressions on the left of the n Vieta's Formulas in Proposition 3.6.1 are obtained by specializing the indeterminates $X_1, X_2, \dots X_n$ at $x_1, x_2, \dots, x_n$ in the fundamental symmetric polynomials $s_1, s_2, \dots s_n$. We will use the same notation for them:

$$s_1 = x_1 + x_2 + x_3 = -(-3),$$

$$s_2 = x_1x_2 + x_1x_3 + x_2x_3 = 0,$$

$$s_3 = x_1x_2x_3 = -1.$$

Then we write, as in Exercise 2.7.12 iv), $x_1^4+x_2^4+x_3^4-4(x_1^2x_2x_3+x_1x_2^2x_3+x_1x_2x_3^2) = s_1^4 - 4s_1^2s_2 + 2s_2^2 = 81$.

Exercise 3.6.6 *i) Prove that an irreducible polynomial in $\mathbb{C}[X]$ has degree 1.*
ii) Prove that an irreducible polynomial in $\mathbb{R}[X]$ has degree 1 or degree 2 and no real roots.
Solution: i) If $f \in \mathbb{C}[X]$ is irreducible, then $deg(f) \geq 1$, so by Theorem 3.6.5 f has a root $z \in \mathbb{C}$. By Corollary 3.3.7 $f = (X - z)g$, and since f is irreducible we get that $deg(g) = 0$, so $deg(f) = 1$.
ii) By the proof of Theorem 3.6.5, f has a complex root z. If $z \in \mathbb{R}$, then f has $deg(f) = 1$ as in the solution for i). If $z \notin \mathbb{R}$, then the complex conjugate $\overline{z}$ is also a root of f and $z \neq \overline{z}$. Then $f = (X-z)(X-\overline{z})g$, where $(X - z)(X - \overline{z}), g \in \mathbb{R}[X]$, and, as above, we get that $deg(g) = 0$ and so $deg(f) = 2$.

Exercise 3.6.9 *Which of the fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are algebraically closed?*
Solution: We have that i is an algebraic number, it's the root of $X^2 + 1 \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$, but $i \notin \mathbb{R}$, so $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed. By Theorem 3.6.5 and induction on the degree, any polynomial in $\mathbb{C}[X]$ of degree at least 1 factors as a product of polynomials of degree 1, so all of its roots are in $\mathbb{C}$, i.e. $\mathbb{C}$ is algebraically closed.

Exercise 3.6.11 *i) Show that if K is a field and $a_1, a_2, \dots, a_n \in K$, then the ideal generated by $X_1 - a_1, X_2 - a_2, \dots, X_n - a_n$ is maximal in $K[X_1, X_2, \dots, X_n]$.*
ii) If M is a maximal ideal of $\mathbb{C}[X_1, X_2, \dots, X_n]$, then M is generated by $X_1 - a_1, X_2 - a_2, \dots, X_n - a_n$, for some $a_1, a_2, \dots, a_n \in \mathbb{C}$.
Solution: i) Let $\varphi : K[X_1, X_2, \dots, X_n] \longrightarrow K$ be the ring morphism sending X_i to a_i, $1 \leq i \leq n$, obtained from Theorem 2.7.4. Using Corollary

3.3.7, we can write any $f \in K[X_1, X_2, \ldots, X_n]$ as $f = (X_1 - a_1)q_1 + r_1$, then $r_1 = (X_2 - a_2)q_2 + r_2$, and so on until we get

$$f = (X_1 - a_1)q_1 + (X_2 - a_2)q_2 + \ldots + (X_n - a_n)q_n + r_n,$$

where $\varphi(f) = r_n \in K$. From this we get that $Ker(\varphi)$ is generated by $X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n$, and $\varphi : K[X_1, X_2, \ldots, X_n]/Ker(\varphi) \simeq K$, because φ is surjective.

ii) By Theorem 3.6.10 we get that there exists an $a_i \in \mathbb{C}$ such that $X_i - a_i \in M$, $1 \leq i \leq n$, so M contains the ideal generated by $X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n$, and so it has to be equal to it by i).

Exercise 3.6.12 *Let K be a field, and α an algebraic element over K. Then α is a root for a unique monic polynomial $Irr(\alpha, K)$, which divides any polynomial in $K[X]$ that has α as a root. $Irr(\alpha, K)$ is called the* minimal polynomial *of α over K. The* degree *of α is $deg(Irr(\alpha, K))$. (Hint: start by choosing a polynomial with the lowest degree among all polynomials in $K[X]$ that have α as a root.)*
Solution: By the well-ordering principle we choose a polynomial f with minimal degree among all polynomials in $K[X]$ that have α as a root. If $g \in K[X]$ and $g(\alpha) = 0$, we write $g = qf + r$, where $r = 0$ or $deg(r) < deg(f)$. Since $r(\alpha) = 0$, we have that $r = 0$, otherwise the minimality of $deg(f)$ would be contradicted. It follows that any polynomial that has α as a root and has the same degree as f is associated in divisibility with f, i.e. it is equal to af for some $a \in K$, $a \neq 0$. There is only one monic polynomial associated in divisibility with f, and that is $Irr(\alpha, K)$.

Exercise 3.6.14 *Prove that $\mathbb{Z}$ is integrally closed.*
Solution: The claim is that any rational algebraic integer is a rational integer. Let $\frac{a}{b} \in \mathbb{Q}$, $(a, b) = 1$, be an algebraic integer. Then $\frac{a}{b}$ satisfies

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \ldots + a_1\frac{a}{b} + a_0 = 0,$$

where $a_i \in \mathbb{Z}$, $0 \leq i \leq n-1$. After chasing away denominators we get

$$a^n + ba_{n-1}a^{n-1} + \ldots + b^{n-1}a_1a + b^n a_0 = 0,$$

so $b \mid a^n$, and therefore $b = \pm 1$.

Exercise 3.6.15 *i) Give an example of an algebraic integer that is not a rational integer.*
ii) Give an example of an algebraic number that is not an algebraic integer.
Solution: i) $\sqrt{2}$ is a root of $X^2 - 2$ but it is not rational (see Exercise

1.2.26).
ii) $\frac{1}{2} \in \mathbb{Q}$ is the root of $2X-1$, but it is not an algebraic integer, because $\frac{1}{2} \notin \mathbb{Z}$.

Exercise 3.6.16 *If α is an algebraic integer, then $Irr(\alpha, K) \in \mathbb{Z}[X]$.*
Solution: We know that $f = Irr(\alpha, K) \in \mathbb{Q}[X]$, and $f \mid g$, where $g \in \mathbb{Z}[X]$ is monic, hence primitive. Let c be the smallest integer such that $cf \in \mathbb{Z}[X]$. Then cf has to be primitive, because if the prime p divides all its coefficients, then it divides its leading term, which is c, so $\frac{c}{p} \in \mathbb{Z}$ has the property that $\frac{c}{p}f \in \mathbb{Z}[X]$, which contradicts the minimality of c. Similarly, if d is the smallest integer such that $dh \in \mathbb{Z}[X]$, then dh is primitive. It follows by Exercise 3.5.8 ii) that $(cd)g = (cf)(dh)h$ is primitive, so $cd = \pm 1$, from which we get that both c and d are ± 1, i.e. $f, h \in \mathbb{Z}[X]$.

Exercise 3.6.20 *Let $d \in \mathbb{Z} \setminus \{0, \pm 1\}$ be square-free, i.e. $p \nmid d$ $\forall p \in \mathbb{Z}$ a prime number. Then*

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

is a field.
Solution: We first remark that by Exercise 1.2.26 we have that $\sqrt{d} \notin \mathbb{Q}$, and so $0 = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ if and only if $0 = a - b\sqrt{d}$ if and only if $a = b = 0$. It is easy to check that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$. If $0 \neq a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, then, as remarked realier,

$$(a + b\sqrt{d})(a + b\sqrt{d}) = a^2 - b^2 d \neq 0,$$

and it is easy to check that the inverse of $a + b\sqrt{d}$ is

$$(a + b\sqrt{d})^{-1} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d}.$$

Exercise 3.6.22 *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic field, and denote by A the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ (see Corollary 3.6.18). If $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we denote by*

$$Tr(z) = z + \overline{z} = 2a, \text{ and } N(z) = z\overline{z} = a^2 - b^2 d.$$

Prove that:
i) $A = \{z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \mid Tr(z), N(z) \in \mathbb{Z}\}$.
ii) $z \in A \Leftrightarrow u = 2a \in \mathbb{Z}$, $v = 2b \in \mathbb{Z}$, $u^2 - v^2 d \equiv 0 \pmod 4$.
iii) If $z_1 = a_1 + b_1\sqrt{d}, z_2 = a_2 + b_2\sqrt{d} \in A$, then $2(a_1 a_2 + b_1 b_2 d) \in \mathbb{Z}$.
Solution: i) $\supseteq$. Let $z \in \mathbb{Q}(\sqrt{d})$ such that $Tr(z), N(z) \in \mathbb{Z}$. Then z is a root of $X^2 - Tr(z)X + N(z) \in \mathbb{Z}[X]$, so z is integral over $\mathbb{Z}$, and therefore

an algebraic integer.
$\supseteq$. If $z \in A$, then z is an algebraic number. If $z \in \mathbb{Q}$, then $z \in \mathbb{Z}$ by Exercise 3.6.14, so clearly $Tr(z) = 2z, N(z) = z^2 \in \mathbb{Z}$. If $z \notin \mathbb{Q}$, then $Irr(z, \mathbb{Q}) = (X - z)(X - \overline{z}) = X^2 - Tr(z)X + N(z)$, and by Exercise 3.6.16 we get that $Irr(z, \mathbb{Q}) = X^2 - Tr(z)X + N(z) \in \mathbb{Z}[X]$, i.e. $Tr(z), N(z) \in \mathbb{Z}$.

ii) $\Rightarrow$. If $z \in A$, then by i) $N(z) = a^2 - b^2 d \in \mathbb{Z}$, so $4a^2 - 4b^2 d \in 4\mathbb{Z}$, i.e. $u^2 - v^2 d \equiv 0 \pmod 4$. Now also by i) $Tr(z) = 2a = u \in \mathbb{Z}$, so $dv^2 \in \mathbb{Z}$. Let $v = \frac{m}{n}$, $(m, n) = 1$. Then $dm^2 = n^2 k$, and so if a prime p divides n, it has to divide d, a contradiction. Thus $v \in \mathbb{Z}$ as well.
$\Leftarrow$. We have $Tr(z) = 2a \in \mathbb{Z}$, and

$$N(z) = a^2 - b^2 d = \left(\frac{u}{2}\right)^2 - \left(\frac{v}{2}\right)^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z},$$

so by i) $z \in A$.

iii) If $a + b\sqrt{d} \in A$, and $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$. If $a \notin \mathbb{Z}$, then $b \notin \mathbb{Z}$ and $2 \nmid d$. Indeed, if $b \in \mathbb{Z}$, then $a \in \mathbb{Z}$, a contradiction. So $b \notin \mathbb{Z}$. If $d = 2k$, then $(2a)^2 - (2b)^2 2k \in 4\mathbb{Z}$, so $(2a)^2 - (2b)^2 2k = 4l$, or $(2a)^2 = 4l + 2k(2b)^2 = 2(2l + k(2b)^2)$, i.e. $2 \mid (2a)^2$, hence $2 \mid 2a$, which contradicts $a \notin \mathbb{Z}$.
Now if one of $a_1, a_2 \in \mathbb{Z}$, this is clear. If none of them are integers, each of a_1, a_2, b_1, b_2 can be written as an odd number over 2, and since d is odd this is also clear.

Exercise 3.6.24 *i) Let $R \subseteq T \subseteq T'$, where R, T, and T' are domains. Then:*
i) If $\gamma \in T'$ is a root of

$$X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0 \in T[X],$$

and b_i are integral over R, for each $i = 0, 1, \ldots, n-1$, then γ is integral over R.
ii) If K is the field containing the field of fractions of R, and T is the integral closure of R in K, then T is integrally closed. In particular, a ring of quadratic integers and the ring of algebraic integers are integrally closed.
Solution: (C.D. Popescu) We know that for each $i \in \{0, 1, \ldots, n-1\}$, b_i is the root of a monic polynomial $f_i \in R[X]$, $\deg(f_i) = k_i$. We denote for $i \in \{0, 1, \ldots, n-1\}$ by

$$\alpha_{i,1} = b_i, \alpha_{i,2}, \ldots, \alpha_{i,k_i}$$

the roots of f_i in some field extension of K (see Proposition 3.6.3). We form the polynomial

$$f = \prod_{1 \le j_i \le k_i, 0 \le i \le n-1} (X^n + \alpha_{n-1,j_{n-1}} X^{n-1} + \ldots + \alpha_{1,j_1} X + \alpha_{0,j_0}),$$

which is a monic polynomial, has γ as a root, and its coefficients are symmetric polynomials in $\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,k_i}$ for each $i = 0, 1, \ldots, n-1$. By Vieta's Formulas (Proposition 3.6.1), each fundamental symmetric polynomial in $\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,k_i}$ is in R, so after applying the Fundamental Theorem of Symmetric Polynomials (Theorem 2.7.11) n times, we get that $f \in R[X]$.
ii) follows from i).

Exercise 3.6.25 *If R is a UFD or a GCD-domain, then R is integrally closed..*
Solution: Assume first that R is a UFD. If $\frac{a}{s}$, $(a, s) = 1$, satisfies

$$\frac{a^n}{s^n} + a_{n-1}\frac{a^{n-1}}{s^{n-1}} + \cdots + a_1\frac{a}{s} + a_0 = 0,$$

then

$$a^n + a_{n-1}sa^{n-1} + \cdots + a_1 s^{n-1}a + a_0 s^n = 0,$$

and so $s \mid a^n$. Now if a prime $p \mid s$, it follows that $p \mid a$, a contradiction. So $s \in U(R)$, i.e. $\frac{a}{s} \in R$.

In case R is a GCD-domain the proof is the same, with the exception that at the end, instead of using prime elements we use the implication $(a, s) = 1$ implies $(a^n, s) = 1$, which follows from Exercise 3.1.18.

3.7 Permanence of arithmetical properties

We start this section by putting together all the implications between the arithmetic properties studied in this chapter.

Proposition 3.7.1 *i) If R is Euclidean, then R is a PID.*
ii) $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is a PID but not Euclidean.

Proof: i) Theorem 3.4.2.
ii) Proposition 3.4.11. ∎

Proposition 3.7.2 *i) If R is a PID, then R is a UFD.*
ii) $\mathbb{Z}[X]$ is a UFD but not a PID.

Proof: i) Exercise 3.5.3.
ii) Exercise 3.4.1 iii). ∎

Proposition 3.7.3 *i) If R is a UFD, then R is a GCD-domain.*
ii) $\mathbb{A}$ is a GCD-domain but not a UFD.

Proof: i) Exercise 3.5.5 iii).
ii) The fact that $\mathbb{A}$ is a GCD-domain follows from [25, Theorem 102]. It is not a UFD because

$$2 = \sqrt{2}\sqrt{2} = \sqrt{2}\sqrt[4]{2}\sqrt[4]{2} = \sqrt{2}\sqrt[4]{2}\sqrt[8]{2}\sqrt[8]{2} = \sqrt{2}\sqrt[4]{2}\sqrt[8]{2}\sqrt[16]{2}\sqrt[16]{2} = \dots$$

and we can continue indefinitely. ∎

Proposition 3.7.4 *i) If R is a GCD-domain, then R is integrally closed.*
ii) $\mathbb{Z}[i\sqrt{5}]$ is integrally closed but not a GCD-domain.

Proof: i) Exercise 3.6.25.
ii) $\mathbb{Z}[i\sqrt{5}]$ is integrally closed because it is a ring of integers (see Theorem 3.6.23 and Exercise 3.6.24 ii)), but it is not a GCD-domain by Exercise 3.1.15. ∎

In the following table we list the answers the following questions: If the domain R has property $\mathcal{P}$, is it true that any subring T of R or a domain T that contains R as a subring also has property $\mathcal{P}$? If P is a prime ideal of R, does the factor ring R/P also have property $\mathcal{P}$? Here property $\mathcal{P}$ is one of the following: Euclidean, PID, UFD, GCD-domain, integrally closed.

R	$T \subseteq R$	$T \supseteq R$	R/P
Euclidean	no 3.7.5	no 3.7.10	yes 3.7.15
PID	no 3.7.6	no 3.7.11	yes 3.7.16
UFD	no 3.7.7	no 3.7.12	no 3.7.17
$GCD-$domain	no 3.7.8	no 3.7.13	no 3.7.18
integrally closed	no 3.7.9	no 3.7.14	no 3.7.19

Exercise 3.7.5 *Find an example of an Euclidean ring R and a subring T of R that is not Euclidean.*

Exercise 3.7.6 *Find an example of a PID R and a subring T of R that is not a PID.*

Exercise 3.7.7 *Find an example of a UFD R and a subring T of R that is not a UFD.*

Exercise 3.7.8 *Find an example of a GCD-domain R and a subring T of R that is not a GCD-domain.*

Exercise 3.7.9 *Find an example of an integrally closed domain R and a subring T of R that is not integrally closed.*

Exercise 3.7.10 *Find an example of an Euclidean ring R and a domain T containing R as a subring that is not Euclidean.*

Exercise 3.7.11 *Find an example of a PID R and a domain T containing R that is not a PID.*

Exercise 3.7.12 *Find an example of a UFD R and a domain T containing R that is not a UFD.*

Exercise 3.7.13 *Find an example of a GCD-domain R and a domain T containing R that is not a GCD-domain.*

Exercise 3.7.14 *Find an example of an integrally closed domain R and a domain T containing R that is not integrally closed.*

Exercise 3.7.15 *If R is Euclidean and P is a prime ideal of R, prove that R/P is Euclidean.*

Exercise 3.7.16 *If R is a PID and P is a prime ideal of R, prove that R/P is a PID.*

Exercise 3.7.17 *Give an example of a UFD R, and P a prime ideal of R, such that R/P is not a UFD.*

Exercise 3.7.18 *Give an example of a GCD-domain R, and P a prime ideal of R, such that R/P is not a GCD-domain.*

Exercise 3.7.19 *Give an example of R which is integrally closed, and P a prime ideal of R, such that R/P is not integrally closed.*

In the following table we list the answers the following questions: If the domain R has property $\mathcal{P}$, is it true that any ring of fractions of R, the polynomial (and the formal power series) ring in one indeterminate over R also has property $\mathcal{P}$? Here property $\mathcal{P}$ is one of the following: Euclidean, PID, UFD, GCD-domain, integrally closed.

R	$S^{-1}R$	$R[X]$	$R[[X]]$
Euclidean	yes 3.7.20	no 3.4.1	no 3.7.30
PID	yes 3.7.21	no 3.4.1	no 3.7.30
UFD	yes 3.7.22	yes 3.5.12	no 3.7.31
$GCD-$domain	yes 3.7.23	yes 3.7.25	no 3.7.32
integrally closed	yes 3.7.24	yes 3.7.26	no 3.7.33

Exercise 3.7.20 *If R is Euclidean and S is a multiplicative subset, then $S^{-1}R$ is Euclidean.*

Exercise 3.7.21 *If R is a PID and S is a multiplicative subset, then $S^{-1}R$ is a PID.*

Exercise 3.7.22 *If R is a UFD and S is a multiplicative subset, then $S^{-1}R$ is a UFD.*

Exercise 3.7.23 *If R is a GCD-domain and S is a multiplicative subset, then $S^{-1}R$ is a GCD-domain.*

Exercise 3.7.24 *If R is integrally closed and S is a multiplicative subset, then $S^{-1}R$ is integrally closed.*

Theorem 3.7.25 *If R is a GCD-domain, then $R[X]$ is a GD-domain.*

Proof: See [16, p.176] or [17]. ∎

Theorem 3.7.26 *If R is integrally closed, then $R[X]$ is integrally closed.*

Proof: See [7, V, § 1, Cor. 1 to Prop. 13, p. 312]. ∎

Remark 3.7.27 *The notion of integrally closed can be defined for rings that are not necessarily domains. In that case, Theorem 3.7.26 is no longer true, see [32].*

Theorem 3.7.28 *If R is a PID, then $R[[X]]$ is a UFD.*

Proof: Denote by $\varphi : R[[X]] \longrightarrow R$ the surjective ring morphism sending a formal series to its free term. We will use Exercise 3.5.20 and prove that any prime ideal P of $R[[X]]$ contains a prime element. If $X \in P$ we are

done, because $R[[X]]/XR[[X]] \simeq R$ is a domain. If $X \notin P$, we denote by $P^* = \varphi(P)$, which is an ideal in R. Since R is a PID, there exists $a \in R$ such that $P^* = Ra$. Let $f \in P$ be such that $a = \varphi(f)$. We will show that f is a prime element in $R[[X]]$ by proving that $P = fR[[X]]$ and using Proposition 3.2.3.
Since $f \in P$, it is clear that $fR[[X]] \subseteq P$. Conversely, let $g = b_0 + b_1X + b_2X^2 + \ldots \in P$. Since $b_0 \in P^* = \varphi(P)$, then $b_0 \in P^*$, so there exists $c_0 \in R$ such that $b_0 = c_0a$. It follows that $g - c_0f = Xg_1 \in P$, and since $X \notin P$, it follows that $g_1 \in P$. As before, there exists a $c_1 \in R$ such that $g_1 - c_1f = Xg_2$. It follows that

$$g = c_0f + X(c_1f + Xg_2) = (c_0 + c_1X)f + X^2g_2.$$

Since $g_2 \in P$, we choose $c_2 \in R$ such that $g_2 - c_2f = Xg_3$, and so

$$g = (c_0 + c_1X + c_2X^2)f + X^3g_3.$$

We continue and find elements $c_o, c_1, \ldots, c_n, \ldots$ and if we let $h = c_0 + c_1X + c_2X^2 + \ldots$, we get that $g = hf$, which ends the proof. ∎

Corollary 3.7.29 *If K is a field, then $K[[X,Y]]$ is a UFD.*

Proof: We have that $K[[X,Y]] = K[[X]][[Y]]$ and $K[[X]]$ is a PID because it is Euclidean by Theorem 3.3.4. Then we apply Theorem 3.7.28. ∎

Remark 3.7.30 *If K is a field, then $K[[X,Y]]$ is not a PID (and therefore not Euclidean). Indeed, if $K[[X,Y]]$ is a PID, it follows that 1 is a linear combination of X and Y, which is a contradiction (a linear combination of X and Y has no free term).*

Remark 3.7.31 *If R is a UFD, it does not follow that $R[[X]]$ is a UFD, see [42].*

Remark 3.7.32 *If R is a GCD-domain, it does not follow that $R[[X]]$ is a GCD-domain, see [2].*

Remark 3.7.33 *If R is integrally closed, it does not follow that $R[[X]]$ is integrally closed, see [39] and [45].*

Solutions to the Exercises on Section 3.7

Exercise 3.7.5 *Find an example of an Euclidean ring R and a subring T of R that is not Euclidean.*
Solution: Let $R = \mathbb{Q}(i\sqrt{5})$, and $T = \mathbb{Z}[i\sqrt{5}]$. R is Euclidean because it is a field, and T is not Euclidean because it is not integrally closed.

Exercise 3.7.6 *Find an example of a PID R and a subring T of R that is not a PID.*
Solution: Same example as in the solution to Exercise 3.7.5, just replace "Euclidean" by "PID".

Exercise 3.7.7 *Find an example of a UFD R and a subring T of R that is not a UFD.*
Solution: Same example as in the solution to Exercise 3.7.5, just replace "Euclidean" by "UFD".

Exercise 3.7.8 *Find an example of a GCD-domain R and a subring T of R that is not a GCD-domain.*
Solution: Same example as in the solution to Exercise 3.7.5, just replace "Euclidean" by "GCD-domain".

Exercise 3.7.9 *Find an example of an integrally closed domain R and a subring T of R that is not integrally closed.*
Solution: Same example as in the solution to Exercise 3.7.5, just replace the first "Euclidean" by "integrally closed", then delete "is not Euclidean because it".

Exercise 3.7.10 *Find an example of an Euclidean ring R and a domain T containing R as a subring that is not Euclidean.*
Solution: Let $R = \mathbb{Z}$, and $T = \mathbb{Z}[i\sqrt{5}]$. R is Euclidean, and T is not Euclidean because it is not integrally closed.

Exercise 3.7.11 *Find an example of a PID R and a domain T containing R that is not a PID.*
Solution: Same example as in the solution to Exercise 3.7.10, just replace "Euclidean" by "PID".

Exercise 3.7.12 *Find an example of a UFD R and a domain T containing R that is not a UFD.*
Solution: Same example as in the solution to Exercise 3.7.10, just replace "Euclidean" by "UFD".

Exercise 3.7.13 *Find an example of a GCD-domain R and a domain T*

containing R that is not a GCD-domain.
Solution: Same example as the one in the solution to Exercise 3.7.10, just replace "Euclidean" by "GCD-domain".

Exercise 3.7.14 *Find an example of an integrally closed domain R and a domain T containing R that is not integrally closed.*
Solution: Same example as in the solution to Exercise 3.7.10, just replace the first "Euclidean" by "integrally closed", then delete "is not Euclidean because it".

Exercise 3.7.15 *If R is Euclidean and P is a prime ideal of R, prove that R/P is Euclidean.*
Solution: If $P = \{0\}$ this is clear. If $P \neq \{0\}$, since R is a PID we have that P is generated by a prime element, which is irreducible, so P is maximal, i.e. R/P is a field.

Exercise 3.7.16 *If R is a PID and P is a prime ideal of R, prove that R/P is a PID.*
Solution: Same as the solution to Exercise 3.7.15.

Exercise 3.7.17 *Give an example of a UFD R, and P a prime ideal of R, such that R/P is not a UFD.*
Solution: Let $R = \mathbb{Z}[X]$ and P the ideal generated by the irreducible polynomial $X^2 + 5$. Then $R/P \simeq \mathbb{Z}[i\sqrt{5}]$. Indeed, let $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i\sqrt{5}]$ be the ring morphism that sends X to $i\sqrt{5}$ obtained from Theorem 2.6.13. Since φ is clearly surjective, we only have to show that $Ker(\varphi) = P$. One way to see this is that if $f \in Ker(\varphi)$, then $Irr(i\sqrt{5}, \mathbb{Q}) = X^2 + 5 \mid f$. Another way is to notice that if $f(i\sqrt{5}) = 0$, then also $f(-i\sqrt{5}) = 0$, and so f is divisible by $(X - i\sqrt{5})(X + i\sqrt{5}) = X^2 + 5$.

Exercise 3.7.18 *Give an example of a GCD-domain R, and P a prime ideal of R, such that R/P is not a GCD-domain.*
Solution: Same as the solution to Exercise 3.7.17.

Exercise 3.7.19 *Give an example of R which is integrally closed, and P a prime ideal of R, such that R/P is not integrally closed.*
Solution: Same as the solution to Exercise 3.7.17.

Exercise 3.7.20 *If R is Euclidean and S is a multiplicative subset, then $S^{-1}R$ is Euclidean.*
Solution: $S^{-1}R$ is a domain, because it is a subring of the field of fractions of the domain R. We denote by φ the Euclidean function on $R \setminus \{0\}$, and we define

$$\psi : S^{-1}R \longrightarrow \mathbb{N}$$

by

$$\psi\left(\frac{a}{s}\right) = \min\left\{\varphi(a') \middle| \frac{a}{s} = \frac{a'}{s'}\right\}.$$

Let $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$, $\frac{b}{t} \neq 0$, $\frac{b}{t} = \frac{b'}{t'}$, $\psi(\frac{b}{t}) = \varphi(b')$. Since R is Euclidean, there exist $q, r \in R$ such that

$$a = qb' + r, \quad \text{where } r = 0 \text{ or } \varphi(r) < \varphi(b').$$

Then

$$\frac{a}{s} = \frac{qt'}{s} \cdot \frac{b'}{t'} + \frac{r}{s},$$

and, if $r \neq 0$,

$$\psi\left(\frac{r}{s}\right) \leq \varphi(r) < \varphi(b') = \psi\left(\frac{b}{t}\right).$$

Exercise 3.7.21 *If R is a PID and S is a multiplicative subset, then $S^{-1}R$ is a PID.*
Solution: Let J be an ideal of $S^{-1}R$. Then by (2.1) we have that

$$J = J^{ce} = \left\{\frac{a}{s} \middle| a \in J^c, s \in S\right\}.$$

Now $J^c = xR$ for some $x \in J^c$, and so $\frac{x}{1}$ is a generator for J, i.e. any $\frac{a}{s} \in J = J^{ce}$ can be written as

$$\frac{a}{s} = \frac{xr}{s} = \frac{x}{1} \cdot \frac{r}{s}.$$

Exercise 3.7.22 *If R is a UFD and S is a multiplicative subset, then $S^{-1}R$ is a UFD.*
Solution: Let $\frac{a}{s}$ be a non-zero non-unit in $S_{-1}R$. Then

$$a = p_1 p_2 \cdots p_r p_{r+1} \cdots p_n,$$

where all p_i are prime elements in R, $p_1, \ldots, p_r$ divide elements in S, $p_{r+1}, \ldots, p_n$ do not divide elements in S, and $r < n$. Then

$$\frac{a}{s} = \frac{p_1 \cdots p_r}{s} \cdot \frac{p_{r+1}}{1} \cdots \frac{p_n}{1},$$

where $\frac{p_1 \cdots p_r}{s} \in U(S^{-1}R)$, and $\frac{p_{r+1}}{1}, \ldots, \frac{p_n}{1}$ are prime in $S^{-1}R$ by Exercise 3.2.7.

Exercise 3.7.23 *If R is a GCD-domain and S is a multiplicative subset, then $S^{-1}R$ is a GCD-domain.*

Solution: We can assume that S is saturated. If $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$, and $d = (a, b)$, where a and b are relatively prime to all elements of S, we want to show that $\frac{d}{1} = (\frac{a}{s}, \frac{b}{t}) = (\frac{a}{1}, \frac{b}{1})$. If $\frac{c}{1} \mid \frac{a}{1}$, and $\frac{c}{1} \mid \frac{b}{1}$, and c is relatively prime to all elements of S, we want to prove that $\frac{c}{1} \mid \frac{d}{1}$. We get $\frac{a}{1} = \frac{c}{1} \cdot \frac{e}{r}$, and $\frac{b}{1} = \frac{c}{1} \cdot \frac{f}{v}$, for some $e, f \in R$ and $r, v \in S$. It follows that $c \mid arv$ and $c \mid brv$, so $c \mid (arv, brv) = drv$. Since $(c, rv) = 1$, it follows that $c \mid d$, and therefore $\frac{c}{1} \mid \frac{d}{1}$.

Exercise 3.7.24 *If R is integrally closed and S is a multiplicative subset, then $S^{-1}R$ is integrally closed.*
Solution: We denote by K the field of fractions of R and we note that $S^{-1}R \subseteq K$. If $\frac{a}{s} \in K$ is integral over $S^{-1}R$, we want to find $a' \in R$ and $t \in S$ such that $\frac{a}{s} = \frac{a'}{t}$. There exist $\frac{a_o}{s_0}, \frac{a_1}{s_1}, \ldots, \frac{a_{n-1}}{s_{n-1}} \in S^{-1}R$ such that

$$\left(\frac{a}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{a}{s}\right)^{n-1} + \ldots + \frac{a_1}{s_1} \cdot \frac{a}{s} + \frac{a_0}{s_0} = 0. \tag{3.7}$$

If we denote $t = s_0 s_1 \cdots s_{n-1} \in S$, we have, after multiplying (3.7) by t^n, that

$$\left(\frac{at}{s}\right)^n + a'_{n-1}\left(\frac{at}{s}\right)^{n-1} + \ldots + a'_1 \cdot \frac{at}{s} + a'_0 = 0,$$

for some $a'_0, a'_1, \ldots, a'_{n-1} \in R$. Therefore $\frac{at}{s} = \frac{a'}{1}$ for some $a' \in R$, so $\frac{a}{s} = \frac{a'}{t} \in S^{-1}R$.

Index

Bibliography

[1] T. Albu, I.D. Ion, *Capitole de teoria algebrică a numerelor* (in Romanian) Editura Academiei Republicii Socialiste Romnia, Bucharest, 1984.

[2] D.D. Anderson, B.G. Kang, M.H. Park, GCD domains and power series rings, *Comm. Algebra* **30** (2002), 5955–5960.

[3] M. Artin, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[4] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[5] C. Băeţica, C. Boboc, S. Dăscălescu, G. Mincu, *Probleme de Algebră* (in Romanian), Editura Universităţii din Bucureşti, 2008.

[6] W.A. Bogley, D. Pengelley, How can symmetries of a rectangle, tethered up to homotopy, provide a physical model for the quaternion group? Generalizations?, talk at JMM 2019, video of the talk available online at the following URL: `https://quaternionnews.commons.gc.cuny.edu/archive-2019-jmm-ams-special-session-on-quaternions/`

[7] N. Bourbaki, *Commutative Algebra*, Chapters 1–7, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.

[8] N. Bourbaki, it Algebra I, Chapters 1–3, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.

[9] G. Cain, *Complex Analysis*, available online at the URL: `https://people.math.gatech.edu/~cain/winter99/complex.html`

[10] C.J. Conidis, P.P. Nielsen, V. Tombs, Transfinitely valued Euclidean domains have arbitrary indecomposable order type, *Comm. Algebra*, **47** (2019), 1105–1113.

[11] D.A. Cox, Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, *Amer. Math. Monthly* **118** (2011), 3–21.

[12] J. Dieudonné, *Topics in local algebra*, Edited and supplemented by Mario Borelli, Notre Dame Mathematical Lectures, No. 10, University of Notre Dame Press, Notre Dame, Ind. 1967.

[13] T. Dumitrescu, *Algebra* I (in Romanian), Editura Universităţii din Bucureşti, 2006.

[14] D.S. Dummit, R.M. Foote, *Abstract algebra*, Third edition, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[15] R. Gilmer, *Multiplicative ideal theory*, Pure and Applied Mathematics, No. 12, Marcel Dekker, Inc., New York, 1972.

[16] R. Gilmer, *Commutative semigroup rings*, University of Chicago Press, 1984.

[17] B. Haible, Gauss' Lemma without Primes, available online at the URL: `https://www.haible.de/bruno/papers/math/algebra/gcdgauss/`

[18] I.N. Herstein, *Abstract algebra*, Macmillan Publishing Company, New York, 1986.

[19] I.N. Herstein, *Topics in algebra*, Second edition, Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975.

[20] T.W. Hungerford, *Abstract Algebra: An Introduction* 2nd Edition, Cengage Learning, 1996.

[21] I.D. Ion, N. Radu, *Algebra* (in Romanian), Editura Didactică şi Pedagogică, Bucureşti, 1991.

[22] I.D. Ion, N. Radu, C. Niţă, D. Popescu, *Probleme de Algebră* (in Romanian), Editura Didactică şi Pedagogică, Bucureşti, 1981.

[23] P. Ionescu, Tre Esempi "Vissuti" (in Italian), preprint.

[24] N. Jacobson, *Basic Algebra* I and II, second edition, W.H. Freeman, San Francisco, 1985-1989.

[25] I. Kaplansky, *Commutative Rings*, Allyn and Bacon, Inc., Boston, Mass. 1970.

[26] I. Kaplansky, Commutative Rings, Conference on Commutative Algebra (Univ. Kansas, Lawrence, Kan., 1972), pp. 153–166, *Lecture Notes in Math.*, Vol. 311, Springer, Berlin, 1973.

[27] I. Kaplansky, *Infinite abelian groups* Revised edition, The University of Michigan Press, Ann Arbor, Mich. 1969.

[28] I. Kaplansky, *Fields and rings*, The University of Chicago Press, Chicago, Ill.-London, 1969.

[29] T.Y. Lam, *A First Course in Noncommutative Rings*, GTM 131, Springer-Verlag New York, 1991.

[30] T.Y. Lam, *Lectures on Modules and Rings*, GTM 189, Springer-Verlag New York, 1999.

[31] T.Y. Lam, *Exercises in Classical Ring Theory*, Problem Books in Mathematics, Springer-Verlag New York, 1995.

[32] T.G. Lucas, Characterizing when $R[X]$ is integrally closed, *Proc. Amer. Math. Soc.* **105** (1989), 861–867.

[33] G. Marasingha, The Partial Fraction Algorithm, available online at the URL: `http://marasingha.org/mathspages/partialfrac/html/node2.html`

[34] H. Matsumura, *Commutative Algebra*, W.A. Benjamin, Inc., New York, 1970.

[35] K. Matthews, *Elementary Linear Algebra*, available online at the URL: `http://www.numbertheory.org/book/`

[36] M. Nagata, *Local rings*, Interscience Tracts in Pure and Applied Mathematics, No. 13, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[37] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele Algebrei* (in Romanian), Editura Academiei Republicii Socialiste România, 1986.

[38] D.G. Northcott, *A first course of homological algebra*, Cambridge University Press, London, 1973.

[39] J. Ohm, Some counterexamples related to integral closure in D[[x]], *Trans. Amer. Math. Soc.* **122** (1966), 321–333, also available online at the URL: `https://www.ams.org/journals/tran/1966-122-02/S0002-9947-1966-0202753-9/S0002-9947-1966-0202753-9.pdf`

[40] J. Ohm, A matrix approach to zero-divisors in R[x], *Amer. Math. Monthly* **114** (2007), 444–450.

[41] R.A. Wilson, An elementary proof that not all principal ideal domains are Euclidean domains, *Math. Gaz.* **101** (2017), 289–293.

[42] P. Samuel, On unique factorization domains, *Illinois J. Math.* **5** (1961), 1–17.

[43] B.A. Sethuraman, *A Gentle Introduction to Abstract Algebra*, available online at the URL: `http://www.csun.edu/~asethura/GIAAFILES/GIAAMain.html`

[44] W.R. Scott, Divisors of zero in polynomial rings, *Amer. Math. Monthly* **61** (1954), 336.

[45] A. Seidenberg, Derivations and integral closure, *Pacific J. Math.*, **16** (1966), 167–173, also available online at the URL: `https://msp.org/pjm/1966/16-1/pjm-v16-n1-p16-p.pdf`

[46] M. Staley, Understanding quaternions and the Dirac belt trick, *European J. Phys.* **31** (2010), 467–478.

[47] W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, A Computational Approach, UTM Springer, 2008, also available at the URL: `https://wstein.org/ent/`

[48] M. Steinberger, *Algebra*, available online at the URL: `http://wayback.archive-it.org/3308/20181021041749/https://www.albany.edu/~mark/teach.htm`

[49] B.L. van der Waerden, *Algebra* Vol 1 & 2, Frederick Ungar Publishing Co., New York, 1970.

[50] B.L. van der Waerden, *A history of algebra. From al-Khwārizmī to Emmy Noether*, Springer-Verlag, Berlin, 1985.

[51] K. Yeats, Partial Fractions, available online at the URL:
`https://people.math.sfu.ca/~kya17/teaching/math343/3-343.pdf`