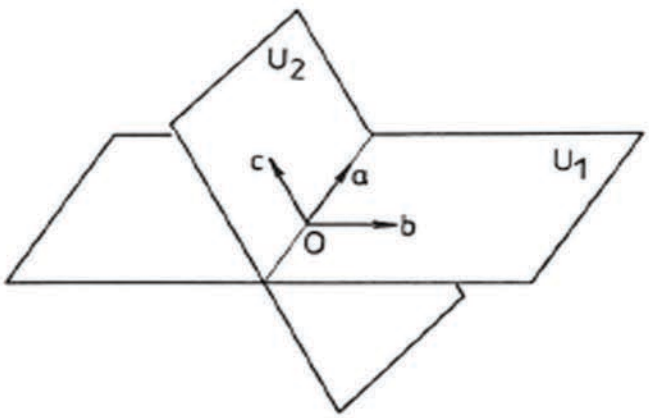
Abstract Algebra with Applications

IN TWO VOLUMES

Volume II

RINGS AND FIELDS



Karlheinz Spindler

Abstract Algebra with Applications

IN TWO VOLUMES

Volume II

Abstract Algebra with Applications

IN TWO VOLUMES

Volume II

RINGS AND FIELDS

Karlheinz Spindler

Darmstadt, Germany

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an informa business

Library of Congress Cataloging-in-Publication Data

Spindler, Karlheinz
Abstract algebra with applications / Karlheinz Spindler.
p. cm.
Includes bibliographical references and index.
Contents: v. 1. Vector spaces and groups -- v. 2. Rings and fields.
ISBN 0-8247-9144-4 (v. 1). -- ISBN 0-8247-9159-2 (v. 2)
1. Algebra, Abstract. I. Title.
QA162.S66 1994
512'.02--dc20 93-32090
CIP

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Current printing (last digit):
10 9 8 7 6 5 4 3 2 1

Meinen Eltern
in Liebe und Dankbarkeit

Preface

THIS volume continues the discussion of abstract algebra and its applications which was begun in Volume I with the treatment of linear algebra and group theory and is now carried on by studying rings and fields. The required set-theoretical background can be found in the Appendix to Volume I; moreover, references to Volume I are given for all facts from linear algebra and group theory which are needed in this volume.† Thus the two volumes together form a self-contained algebra text.

All comments concerning the objectives and the style of this textbook given in the preface of Volume I hold for Volume II as well. This means that I tried to write a text which

- enhances understanding by giving many examples and informal comments;
- offers many exercises which allow the students to check their understanding of the new material and to apply it to concrete problems;
- can be used for an individual self-study program and for reading courses;
- tries to reveal general underlying ideas which guide the students through the technical discussion of the material; and
- also presents the connections between algebra and other mathematical disciplines, thereby demonstrating the pervasive power of algebraic techniques and enabling the students to put the different algebraic theories into a more general framework.

The discussion of rings emphasizes those two topics from which the abstract-structural theory of rings has evolved and by which the introduction of many important concepts is motivated; namely, number theory and algebraic geometry. Ring theory is thereby shown to be rooted in both arithmetic and geometry in the same way in which the theory of vector spaces was traced back to both arithmetical and geometrical considerations in Volume I. Thus the Cartesian program of merging algebra and geometry is extended from linear equations and affine geometry to arbitrary polynomial equations and algebraic geometry. Field theory is presented in two blocks. First, there are three sections dealing with basic properties of algebraic and transcendental field extensions, normality and separability, as these topics are needed in the more advanced sections on ring theory. Second, Galois theory is discussed in some detail. In a short epilogue it is shown that Galois theory and Lie theory can be traced back to the same underlying fundamental idea, namely that of revealing symmetries in the solution set of an equation (be it an algebraic equation or a differential equation) by employing the mathematical concept of a group.

As was already stated in the preface to the first volume, I am greatly indebted to my doctoral thesis advisor, Karl Heinrich Hofmann; my colleagues with whom I have collaborated in preparing lectures and lab sessions in algebra and geometry, namely Benno Artmann, Jürgen Bokowski, Joachim Hilgert, Martin Petschke and Christian Terp; and, above all, to my family for their steadfast support, both practical and moral.

Karlheinz Spindler

† References to Volume I include the Roman number I. For example, (I.23.1) refers to item (23.1) in section 23 of Volume I, whereas (23.1) refers to item (23.1) in section 23 of the current volume.

Contents†

Volume I

† Headings below section titles refer to topics covered, much like an index, rather than to discrete subsections.

Volume II

1. Introduction: The Art of Doing Arithmetic

RECALL arithmetical problems that you learned to tackle earlier on in your education: solving linear equations $ax + b = 0$ and quadratic equations $ax^2 + bx + c = 0$, factoring terms like $a^2 - b^2 = (a + b)(a - b)$ or $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$, finding product expansions like $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$, and so on. All these problems involve the two basic operations of addition and multiplication, and arithmetic can be characterized as the art of handling these two operations. For example, the quadratic equation $ax^2 + bx + c = 0$ is essentially solved by simply rewriting it in the form $a(x + \frac{b}{2a})^2 + c - \frac{b^2}{4a} = 0$ or $(x + \frac{b}{2a})^2 = \frac{b^2 - 4ac}{4a^2}$.

When we talk about doing arithmetic, we usually have in mind the set of integers or the set of rational numbers; when it comes to taking roots also the domains of real or complex numbers. But there are other domains where we can do arithmetic; for example, we can add and multiply functions or matrices. We have to be careful, though, because multiplication in these other domains need not be commutative; for example, there are matrices A, B with $AB \neq BA$ and therefore $A^2 - B^2 \neq (A + B)(A - B)$. Another interesting example of objects that can be added and multiplied are the residue classes introduced in (I.20.14). In this chapter, we want to systematically study domains on which two operations, called addition and multiplication, are defined; these domains are called rings. One main source of ring theory is number theory, and we will see how number-theoretical problems stimulated the development of ring theory.†

Why is it that number theory (which is primarily concerned with the properties of natural numbers or integers) should stimulate the investigation of the arithmetical properties of more general domains? The answer is that quite often properties of domains other than the set of integers yield number-theoretical results about the integers themselves. Let us consider a prominent example for this phenomenon, an example which creates a link between the well-known arithmetic of integers and arithmetic in a more "abstract" domain and hence can serve as an "appetizer" for a general theory of rings.

In July 1801, after five years of work, Carl Friedrich Gauss (1777-1855) completed a book entitled *Disquisitiones Arithmeticae* which was, upon publication and ever after, considered as one of the greatest works in the theory of numbers. Why did this book attract such an attention that, for example, Dirichlet carried the French translation with him wherever he went and even slept with the book under his pillow? Even though there were many new things in the book (the first proof of the quadratic reciprocity law, the complete determination of those regular polygons that can be constructed with ruler and compass, extensive studies of binary quadratic forms, primitive roots, and so on), one of Gauss's greatest achievements in this book was the indication of a new way of looking at well-known facts in number theory. Indeed, let us see how Gauss begins his *Disquisitiones Arithmeticae*. After a dedication to his prince, duke Karl Wilhelm Ferdinand of Brunswick and Luneburg, and a short preface, Gauss starts his work with the following phrases: "If a number a divides the difference of two numbers b, c then b and c are called *congruent with respect to* a, otherwise *incongruent*; we call this a the *modulus*. Each of the numbers b, c is called a *residue* of the other in the first case, a *non-*

† The other main source of ring theory is algebraic geometry which will be discussed in a separate section later.

residue of the other in the second case."† In other words, Gauss starts his work with the introduction of the residue classes that we encountered in (I.20.14). Let us consider several examples in which the study of residue classes yields number-theoretical results or facilitates computations in the domain of integers.

(1.1) Example. *If the natural numbers a and n are relatively prime, then $a^{\varphi(n)}-1$ is divible by n* **(Euler's Theorem)**; *here φ denotes Euler's φ-function. In the special case that $n = p$ is a prime this says that $a^{p-1} - 1$ is divisible by p for all $a \in \mathbb{N}$* **(Fermat's Theorem).**

Proof. The multiplicative group $\mathbb{Z}_n^\times$ has $\varphi(n)$ elements, and the residue class $[a]$ of a modulo n is an element of this group because a is relatively prime to n. Hence $[a]^{\varphi(n)} = [1]$ by Lagrange's theorem. But this is the claim. ∎

(1.2) Example. *Let $a_n a_{n-1} \cdots a_1 a_0$ be the decimal representation of a natural number x. Then the following* **divisibility rules** *hold.*

(a) *x leaves the same remainder when divided by* 2(5) *as its last digit a_0.*

(b) *x leaves the same remainder when divided by* 3(9) *as its digit sum $a_0 + a_1 + \cdots + a_{n-1} + a_n$.*

(c) *x leaves the same remainder when divided by* 11 *as its alternating digit sum $a_0 - a_1 + a_2 - a_3 + - \cdots$.*

(d) *x leaves the same remainder when divided by* 7(11,13) *as the number $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - + \cdots$.*

(e) *x leaves the same remainder when divided by* 37 *as the number $a_2 a_1 a_0 + a_5 a_4 a_3 + a_8 a_7 a_6 + \cdots$.*

Proof. To say that $a_n a_{n-1} \cdots a_1 a_0$ is the decimal representation of x is tantamount to saying $x = \sum_{k=0}^{n} a_k 10^k$.

(a) Let $x' = a_0$. Since $10 = 2 \cdot 5$ we have $10 \equiv 0$ modulo 2 and modulo 5. Therefore, $x - x' = \sum_{k=1}^{n} a_k 10^k \equiv 0 \bmod 2(5)$, which is the claim.

(b) Let $x' = a_0 + a_1 + \cdots + a_{n-1} + a_n$. Since $10 \equiv 1$ modulo 3 and modulo 9, we have $x - x' = \sum_{k=0}^{n} a_k 10^k - \sum_{k=0}^{n} a_k = \sum_{k=0}^{n} a_k (10^k - 1) \equiv 0 \bmod 3(9)$, which is the claim.

(c) Let $x' = a_0 - a_1 + a_2 - + \cdots = \sum_{k=0}^{n} (-1)^k a_k$. Since $10 \equiv -1$ modulo 11, we have $x - x' = \sum_{k=0}^{n} a_k 10^k - \sum_{k=0}^{n} (-1)^k a_k = \sum_{k=0}^{n} a_k \left(10^k - (-1)^k\right) \equiv 0 \bmod 11$, which is the claim.

(d) Let $x' = a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - + \cdots = \sum_{k=0}^{\infty} (-1)^k (a_{3k} + 10 a_{3k+1} + 100 a_{3k+2})$ where we set $a_k := 0$ for $k > n$. Since $7 \cdot 11 \cdot 13 = 1001$ we have $1000 \equiv -1$ modulo 7, 11 and 13. Therefore,

---

† Gauss, like his great models Leibniz and Newton, wrote in Latin; the original text is as follows: "Si numerus a numerorum b, c differentiam metitur, b et c *secundum a congrui* dicuntur, sin minus, *incongrui*: ipsum a *modulum* appellamus. Uterque numerorum b, c priori in casu alterius *residuum*, in posteriori vero *nonresiduum* vocatur."

$$x - x' = \sum_{k=0}^{\infty} 10^{3k}(a_{3k} + 10a_{3k+1} + 100a_{3k+2}) - \sum_{k=0}^{n}(-1)^k(a_{3k} + 10a_{3k+1} + 100a_{3k+2})$$
$$= \sum_{k=0}^{\infty}(1000^k - (-1)^k)(a_{3k} + 10a_{3k+1} + 100a_{3k+2}) \equiv 0$$

mod 7(11, 13), which is the claim.

(e) Let $x' = a_2a_1a_0 + a_5a_4a_3 + a_8a_7a_6 + \cdots = \sum_{k=0}^{\infty}(a_{3k} + 10a_{3k+1} + 100a_{3k+2})$ where we again set $a_k := 0$ for $k > n$. Since $27 \cdot 37 = 999$ we have $1000 \equiv 1$ modulo 37. Therefore, $x - x' = \sum_{k=0}^{\infty} 10^{3k}(a_{3k} + 10a_{3k+1} + 100a_{3k+2}) - \sum_{k=0}^{n}(a_{3k} + 10a_{3k+1} + 100a_{3k+2}) = \sum_{k=0}^{\infty}(1000^k - 1)(a_{3k} + 10a_{3k+1} + 100a_{3k+2}) \equiv 0 \bmod 37$, which is the claim. ∎

(1.3) Example. *If we add up the squares of four consecutive numbers we can never obtain a square.*

Proof. Suppose $x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 = y^2$, i.e., $4x^2 + 12x + 14 = y^2$. Modulo 4, this reads $[2] = [y]^2$. But in $\mathbb{Z}_4$ we have $[0]^2 = [2]^2 = [0]$ and $[1]^2 = [3]^2 = [1]$; hence [2] is not a square in $\mathbb{Z}_4$. This is the desired contradiction. ∎

(1.4) Example. *What are the last two digits of the number* 7^{99999}*?*

Solution. We want to find the residue class of 7^{99999} modulo 100. Now in $\mathbb{Z}_{100}$ we have $[7]^4 = [49^2] = [2401] = [1]$; therefore, $[7]^{99999} = [7]^3 = [343] = [43]$. Hence the two last digits are 43. ∎

(1.5) Example. *What remainder is left if* 3^{100} *is divided by* 34*?*

Solution. We want to find the residue class of 3^{100} modulo 34. By Euler's theorem (see (1.1)) we have $[3]^{16} = [1]$ in $\mathbb{Z}_{34}$ because $\varphi(34) = 16$; hence $[3]^{100} = [3]^{16 \cdot 6 + 4} = [3]^4 = [81] = [13]$. Hence the remainder is 13. ∎

(1.6) Example. *Show that there are no integers* x *and* y *such that* $x^2 - 13y^2 = 275$.

Solution. If $x^2 - 13y^2 = 275$ then $[x]^2 = [275] = [2]$ in $\mathbb{Z}_{13}$. But in $\mathbb{Z}_{13}$ we have

$$[0]^2 = [0], \quad [\pm 1]^2 = [1], \quad [\pm 2]^2 = [4], \quad [\pm 3]^2 = [9],$$
$$[\pm 4]^2 = [3], \quad [\pm 5]^2 = [12], \quad [\pm 6]^2 = [10];$$

hence the equation $[x]^2 = [2]$ has no solution in $\mathbb{Z}_{13}$. ∎

(1.7) Example. *Pierre de Fermat (1601-1665) claimed in 1640 that all numbers of the form* $2^{2^n}+1$ $(n \in \mathbb{N}_0)$ *are primes, but he admitted that he did not know a proof. For* $n = 0, 1, 2, 3, 4$ *Fermat's claim is true, because* $3, 5, 17, 257$ *and* 65537 *are primes. However, the great Swiss mathematician Leonhard Euler (1707-1783) proved in 1732 that* $2^{32}+1$ *is divisible by* 641. *Check this fact!*

Solution. We have $2^4 + 5^4 = 16 + 625 = 641$ and $5 \cdot 2^7 = 5 \cdot 128 = 640$; modulo 641 these equations become

$$[5]^4 \;=\; -[2]^4 \qquad \text{and} \qquad [5]\cdot[2]^7 \;=\; [-1] \qquad \text{in } \mathbb{Z}_{641}\,.$$

Taking the fourth power of the second equation and plugging in the first we obtain $[1] = [5]^4[2]^{28} = -[2]^4[2]^{28} = -[2]^{32}$. But this means $[2^{32}+1] = [0]$ which is exactly the claim. ∎

(1.8) Example. *If* $p \in \mathbb{N}$ *is a prime number, then* $(p-1)!+1$ *is divisible by* p **(Wilson's Theorem).** *Conversely, if* $(n-1)!+1$ *is divisible by* n, *then* n *is a prime number.*

Proof. Let p be a prime. In the multiplicative group $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$, no element $[x] \neq [\pm 1]$ is its own inverse, because $[x]^2 = [1]$ implies $[0] = [x^2-1] = [x-1]\cdot[x+1]$ and hence $[x-1] = [0]$ or $[x+1] = [0]$ in $\mathbb{Z}_p$. Thus the elements of $\mathbb{Z}_p^\times$ other than $\pm[1]$ arise in pairs (ξ, ξ^{-1}). This implies

$$[(p-1)!] \;=\; [1]\cdot[2]\cdot[3]\cdots[p-1] \;=\; \prod_{\xi\in\mathbb{Z}_p^\times} \xi \;=\; [1]\cdot[-1] \;=\; [-1]$$

which is the claim. (Note that the argument also holds if $p = 2$; in this case $[1] = [-1]$.) Conversely, suppose that $(n-1)!+1$ is divisible by n, say $1\cdot 2\cdot 3\cdots(n-1)+1 = k\cdot n$. Obviously, none of the numbers $1, 2, \ldots, n-1$ divides the left-hand side of this equation, hence none of them divides n. This shows that n is prime. ∎

(1.9) Example. *Let* p *be a prime number of the form* $4n+1$. *Then there is a natural number* x *such that* x^2+1 *is divisible by* p.

Proof. We claim that $x := 1\cdot 2\cdots\frac{p-1}{2}$ has the desired property. Indeed, since $\frac{p-1}{2} = 2n$ is even, we also have $x = (-1)(-2)\cdots(-\frac{p-1}{2})$; therefore, in $\mathbb{Z}_p$ the following equation holds:

$$\begin{aligned}[x^2] \;&=\; \underbrace{[-1]}_{=[p-1]}\cdot\underbrace{[-2]}_{=[p-2]}\cdots\underbrace{[-\frac{p-1}{2}]}_{=[\frac{p+1}{2}]}\cdot[1]\cdot[2]\cdots[\frac{p-1}{2}] \\ &=\; [1]\cdot[2]\cdots[p-1] \;=\; [(p-1)!] \;=\; [-1]\end{aligned}$$

where the last equation is just Wilson's theorem (see (1.8)). ∎

(1.10) Example. *No natural number of the form $4n+3$ can be written as a sum of two squares.*

Proof. Suppose $4n+3 = x^2+y^2$. Modulo 4, this reads $[3] = [x]^2 + [y]^2$. But in $\mathbb{Z}_4$ we have $[0]^2 = [2]^2 = [0]$ and $[1]^2 = [3]^2 = [1]$; hence $[3]$ is not the sum of two squares in $\mathbb{Z}_4$. ∎

THESE examples show that the arithmetic of residue classes can yield results about the integers that could be obtained in a straightforward manner only by very tedious calculations. It should be noted that in some of the above examples this simplification was achieved due to the fact that the transition to residue classes translated a problem involving addition and multiplication into a purely multiplicative problem.† In (1.1) the statement that $a^{\varphi(n)}-1$ is divisible by n was translated into the purely multiplicative statement $[a]^{\varphi(n)} = [1]$ in $\mathbb{Z}_n$. Similarly, in (1.7) the statement that $2^{32}+1$ is divisible by 641 was rewritten as $[2]^{32} = [-1]$ in $\mathbb{Z}_{641}$, and in (1.8) the statement that $(p-1)!+1$ is divisible by p was rewritten as $[(p-1)!] = [-1]$ in $\mathbb{Z}_p$. Finally, in (1.6) the equation $x^2-13y^2 = 275$ became $[x]^2 = [2]$ in $\mathbb{Z}_{13}$. But in other problems the use of residue classes (though it gives us some information) does not yield the solution. For example, how should we find all integer solutions of equations like $x^2-3y^2 = 1$ or $y^2+4 = x^3$? Note that these two equations can be rewritten in a purely multiplicative way if we allow ourselves to use irrational and even complex numbers; namely, we can write $(x+y\sqrt{3})(x-y\sqrt{3}) = 1$ and $(y+2i)(y-2i) = x^3$. Since we are only interested in integer solutions we are lead to studying the domains $\mathbb{Z}+\mathbb{Z}\sqrt{3} := \{x+y\sqrt{3} \mid x,y \in \mathbb{Z}\}$ and $\mathbb{Z}+2i\mathbb{Z} := \{x+2iy \mid x,y \in \mathbb{Z}\}$. Similarly, a bold (and partly successful!) attempt to solve Fermat's problem is by introducing the number $\varepsilon := e^{2\pi i/n}$ which allows one to rewrite the equation $x^n+y^n = z^n$ in the purely multiplicative form

$$z^n \;=\; x^n+y^n \;=\; (x+y)(x+\varepsilon y)(x+\varepsilon^2 y)\cdots(x+\varepsilon^{n-1}y)\;.$$

The price we pay for this approach is that we cannot limit our study solely to integers; we want to do arithmetic in a larger domain containing the integers but also the number ε. (See problem 18 below.)

THUS even from the viewpoint of a "pure" number theorist it seems rewarding to do arithmetic in domains other than the integers. It will be the purpose of this chapter to study these domains.

---

† As a matter of fact, it is a characteristic feature of some of the hardest problems in number theory that they intertwine the additive and the multiplicative structure of the number system. The most famous (and most notorious) example is Fermat's Last Theorem, stating that the equation $x^n+y^n = z^n$ has no solution (x,y,z) in the natural numbers for any given exponent $n \geq 3$. Another example is Goldbach's Conjecture that every even natural number $n \geq 4$ can be written as a sum of two primes (where a prime is a number with the simplest possible multiplicative structure, namely a number $p \in \mathbb{N}$ whose only divisors in $\mathbb{N}$ are 1 and p itself). Also, it is not known whether there is only a finite number of primes p such that $p+2$ is also a prime; i.e., whether there is only a finite number of *twin primes* like $(3,5)$, $(5,7)$, $(11,13)$ or $(17,19)$.

Exercises

Problem 1. (a) Find the remainder of 2^{47} modulo 30, of 3^{47} modulo 23, of 3^{200} modulo 13, of 94^{200} modulo 13 and of 12^{100} modulo 34.

(b) Find the last digits of $3^{597}, 943^{597}$, 7^{123}, 987^{123} and 689^{1287}.

(c) Find the last two digits of 2^{400} and 3^{400}.

(d) Find the remainder of the division $2^{1,000,000} : 77$.

(e) What is the remainder if 4^{1000} is divided by 17?

Problem 2. A "magician" asks his audience to choose a number $N < 1000$ and to tell him the remainders r_7, r_{11} and r_{13} of this number modulo 7, 11 and 13. Without any further information, he is able to determine the number N. How does he do that?

Hint. Prove that $715r_7 + 364r_{11} + 924r_{13}$ is congruent to N modulo 1001.

Problem 3. (a) Show that $143^6 + 91^{10} + 77^{12} - 1$ is divisible by 1001.

(b) Show that $2222^{5555} + 5555^{2222}$ is divisible by 7.

(c) Show that $3n^5 + 5n^3 + 7n$ is divisible by 15 whenever $n \in \mathbb{Z}$.

(d) Show that $x^9 - 6x^7 + 9x^5 - 4x^3$ is divisible by 8640 for all $x \in \mathbb{Z}$.

Problem 4. (a) Show that the following congruences do not have solutions.

$$x^2 \equiv 3 \pmod 4, \quad y^2 \equiv 12 \pmod{16}, \quad z^2 \equiv 4444 \pmod{10^4}$$

(b) Show that the sum of the squares of three subsequent natural numbers is never a square itself.

(c) Show that none of the following equations has integer solutions.

$$x^2+y^2+z^2 = 8n+7,\ x^2+y^2 = 4a+3,\ x^2-y^2 = 4b+2,\ x^2-3y^n = 2,\ x^2-17m = 855$$

(d) Show that none of the numbers 11, 111, 1111, 11111,... is a square.

Hint. Consider these numbers modulo 4.

Problem 5. (a) Show that the equations $15x^2 - 7y^2 = 9$ and $x^2 + 3xy - 2y^2 = 122$ do not possess integer solutions.

(b) Find all integer solutions of the equations $5x^2 + 2xy + 2y^2 = 26$ and $x^2 + xy - 2y^2 = 10$.

(c) Show that if a, b, c are integers with $a^2 + b^2 = c^2$ then at least one of these three numbers is divisible by 3.

Problem 6. (a) Show that $x^n - 1$ is divisible by $x - 1$ for any $x \in \mathbb{Z}$ and $n \in \mathbb{N}$.

(b) Let $n \in \mathbb{N}$. Show that $6 \mid n^3 - n$, $30 \mid n^5 - n$, $42 \mid n^7 - n$, $8190 \mid n^{13} - n$, $510 \mid n^{17} - n$, $798 \mid n^{19} - n$, $330 \mid n^{21} - n$ and $383838 \mid n^{37} - n$.

Problem 7. Suppose that $n \in \mathbb{N}$ is odd. Show that $n^2 - 1$ is divisible by 8 and that $n^8 - 1$ is divisible by 32. Can you generalize?

Problem 8. Find all natural numbers n such that $2^n - 1$ is divisible by 31.

Problem 9. Let m and n be natural numbers with $n \geq 2$. Show that $2^m + 1$ is not divisible by $2^n - 1$.

Problem 10. (a) Suppose $m, n \in \mathbb{N}$ are either both even or both odd. Show that $a^m - a^n$ is divisible by 3 for any $a \in \mathbb{Z}$.

(b) Let $p > 3$ be a prime. Show that $a^p - a$ and $a^p b - b^p a$ are divisible by $6p$ for all $a, b \in \mathbb{Z}$.

Problem 11. Let p be a prime number.

(a) Show that $a \equiv 1$ modulo p implies that $a^{p^k} \equiv 1$ modulo p^{k+1} for all $k \in \mathbb{N}_0$.

(b) Show that $a \equiv b \,(\mathrm{mod}\, p^m)$ implies $a^p \equiv b^p \,(\mathrm{mod}\, p^{m+1})$.

Problem 12. (a) Let $p \neq 2, 5$ be a prime number. Show that p divides infinitely many of the numbers $1, 11, 111, 1111, 11111, \ldots$.

Hint.

$$9 \cdot \underbrace{11\ldots1}_{n} = 10^n - 1 .$$

(b) Let S be the set of all natural numbers whose decimal expansions have no digits other than 0 and 1. Show that S is multiplicatively closed, i.e., that if $s_1, s_2 \in S$ then $s_1 s_2 \in S$.

(c) Let $n \in \mathbb{N}$ and $k \in \{1, 2, 3, \ldots, 9\}$. Show that there is a multiple of n whose only digits (in the decimal expansion) are 0 and k.

Hint. It is enough to treat the case $k = 1$ (why?). Note that $10^n - 10$ is a multiple of n which has the form $9s = 1$ with $s \in S$. Now argue that there is an element $x \in \mathbb{N}$ with $9x = 11\ldots1 \in S$.

(d) Show that a natural number divides some number of the form $999\ldots9$ if and only if the last digit of n is $1, 3, 7$ or 9.

Problem 13. Let $p > 3$ be a prime number. Write

$$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}, \quad \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} = \frac{c}{d} \text{ and } \frac{1}{1^3} + \frac{1}{2^3} + \cdots + \frac{1}{(p-1)^3} = \frac{e}{f}$$

with $a, b, c, d \in \mathbb{N}$. Show that the numerators a, c and e are all divisible by p. Can you even show that a is divisible by p^2?

Hint. Consider the elements $\sum_{k=1}^{p-1} [k]^{-1}$, $\sum_{k=1}^{p-1} [k]^{-2}$ and $\sum_{k=1}^{p-1} [k]^{-3}$ in $\mathbb{Z}_p$ and use the formulas

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \quad \text{and} \quad \sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} .$$

Problem 14. (a) Show that if $p \neq 2$ is a prime then $(p-2)!-1$ and $(p-3)!-\frac{1}{2}(p-1)$ are divisible by p.

(b) For $n = 100, 99, 98, 97, 96$ find the remainder of $n!$ when divided by 101.

(c) For $n = 102, 101, 100, 99, 98$ find the remainder of $n!$ when divided by 103.

(d) Let p be an odd prime. Show that $1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{1}{2}(p+1)}$ modulo p.

(e) The fact that n is a prime if and only if $(n-1)! + 1$ is divisible by n can be considered as a criterion to check the primality of a given natural number. Can you imagine why this is not a very practical criterion?

Problem 15. Find a single congruence which is equivalent to the two congruences $x \equiv 1 \,(\mathrm{mod}\, 4)$ and $x \equiv 2 \,(\mathrm{mod}\, 3)$, i.e., find a congruence whose solutions are exactly those numbers which simultaneously solve the two given congruences.

Problem 16. Solve the equations $x^2 = x$ and $x^3 = x$ in $\mathbb{Z}_6$, in $\mathbb{Z}_{30}$ and in $\mathbb{Z}_q$ where q is the power of an odd prime.

Problem 17. Let p be an odd prime. We denote by $S_p := \{x^2 \mid x \in \mathbb{Z}_p\}$ the set of all squares in $\mathbb{Z}_p$ and by $N_p := \mathbb{Z}_p \setminus S_p$ the set of all non-squares.

(a) Show that $|S_p| = \frac{p+1}{2}$ and conclude that exactly half of the elements in $\mathbb{Z}_p^\times$ are squares.

(b) Show that if $u \in N_p$ then $N_p = uS_p \setminus \{0\}$ and prove the inclusions $Q_p Q_p \subseteq Q_p$, $Q_p N_p \subseteq N_p$ and $N_p N_p \subseteq Q_p$. (Thus the nonzero squares form a subgroup of $(\mathbb{Z}_p^\times, \cdot)$ of index 2.)

(c) Show that for any three elements $a, b, c \in \mathbb{Z}_p^\times$ there are elements $x, y \in \mathbb{Z}_p$ such that $ax^2 + by^2 = c$.

Hint. Use part (a) to show that the sets $\{ax^2 \mid x \in \mathbb{Z}_p\}$ and $\{c - by^2 \mid y \in \mathbb{Z}_p\}$ both have cardinality $(p+1)/2$ and hence have a nonempty intersection.

(d) Show that every element of $\mathbb{Z}_p$ can be written as the sum of two squares.

Problem 18. Let $\varepsilon := e^{2\pi i/3}$ and let $R := \mathbb{Z} + \mathbb{Z}\varepsilon + \mathbb{Z}\varepsilon^2$ be the set of all complex numbers $a + b\varepsilon + c\varepsilon^2$ with $a, b, c \in \mathbb{Z}$. Show that sums and products of elements of R lie again in R.

Problem 19. Suppose that p is a prime of the form $p = 2q + 1$ where q is odd. Using Wilson's theorem, show that $q! \equiv \pm 1$ modulo p.

Problem 20. (a) Show that for each element $x \in \mathbb{Z}_{19}^\times$ there is a number $n \in \mathbb{N}$ such that $x = [2]^n$.

(b) Show that the function

$$\begin{array}{rccc} \log : & \mathbb{Z}_{19}^\times & \to & \mathbb{Z}_{18} \\ & [2]^n & \mapsto & n \end{array}$$

is well-defined and has the property that $\log(xy) = \log x + \log y$, $\log(x/y) = \log x - \log y$ and $\log x^r = r \log x$ for all $x, y \in \mathbb{Z}_{19}^\times$ and all $r \in \mathbb{Z}$.

(c) List the values of this function, i.e., create a "logarithm table" for $\mathbb{Z}_{19}^\times$ and use this table to determine 30^{14} modulo 19 and 25^{11} modulo 19.

Problem 21. (a) Show that $3x \equiv 4\,(5)$ if and only if $x \equiv 3\,(5)$.

Hint. 3 has a multiplicative inverse modulo 5.

(b) Find a number n such that $8x \equiv 15\,(21)$ if and only if $x \equiv n\,(21)$.

(c) Show that $42x \equiv 259\,(847)$ if and only if $6x \equiv 49\,(121)$.

Problem 22. (a) Show that $3x + 5y$ is divisible by 19 if and only if $13x + 9y$ is.

Hint. We have to show that $3x = -5y$ in $\mathbb{Z}_{19}$ if and only if $13x = -9y$ in $\mathbb{Z}_{19}$. Now 3 and 13 are invertible in $\mathbb{Z}_{19}$.

(b) Find a natural number n such that $2x - 3y$ is divisible by 13 if and only if $5x + ny$ is.

Problem 23. The number $\star\star\star,398,246$ is divisible by $31\star$. Find the missing digits.

Problem 24. Show that the product of four consecutive natural numbers is neither a square nor a cube.

Problem 25. Show that among any 10 consecutive natural numbers there is at least one that is relatively prime to each of the others.

Problem 26. Let $x, y, z \in \mathbb{Z}$.

(a) Show that if $x^3 + y^3 - z^3$ is divisible by 9 then at least one of the numbers x, y, z is divisible by 3.

(b) Show that if $x^5 + y^5 - z^5$ is divisible by 25 then at least one of the numbers x, y, z is divisible by 5.

Problem 27. Show that if n is a square-free natural number then $x^{\varphi(n)+1} - x$ is divisible by n for all $x \in \mathbb{Z}$.

2. Rings and ring homomorphisms

ARITHMETIC is the art of manipulating terms by the basic operations of addition, subtraction and multiplication and also division whenever possible. This art can be practised in different domains; we can not only occupy ourselves with integers or rational numbers, but also with polynomials, matrices or other objects. In all these domains, the used operations satisfy certain arithmetic laws which we usually use without thinking. Now we will axiomatize the notions of addition and multiplication; namely, we will define a ring as a set with two arithmetic operations, called addition and multiplication, which satisfy certain rules (the "arithmetic laws"). This definition will turn out to be "weak" enough to include a variety of diverse examples, but "strong" enough to allow interesting conclusions and non-trivial applications. As guiding examples, we should keep in mind the set $\mathbb{Z}$ of all integers, the set $\mathbb{Z}[x]$ of all polynomials with integer coefficients and the set $\mathbb{Z}^{n\times n}$ of all $n \times n$-matrices with integer entries; each endowed with the usual addition and multiplication.

(2.1) Definitions. (a) *A* **ring** $(R,+,\cdot)$ *is a set* R *with two binary operations*

$$\begin{array}{ccc} R\times R & \to & R \\ (x,y) & \mapsto & x+y \end{array} \quad \textit{and} \quad \begin{array}{ccc} R\times R & \to & R \\ (x,y) & \mapsto & xy \end{array},$$

called addition and multiplication, such that the following conditions hold.

(1) $(R,+)$ *is an abelian group,*

(2) $(xy)z = x(yz)$ *for all* x,y,z (associative law for the multiplication in R),

(3) $x(y+z) = xy + xz$ *and* $(x+y)z = xz + yz$ *for all* x,y,z (distributive laws).

(b) *A ring* R *is called a* **commutative ring** *if*

$$xy = yx \qquad \textit{for all } x,y \in R\,.$$

(c) *A ring* R *is called a* **ring with identity** *or a* **unital ring** *if there is an element* $1 \neq 0$ *in* R *with*

$$r\cdot 1 = 1\cdot r = r \qquad \textit{for all } r \in R\,.$$

WE note that if a ring R possesses an identity element, then this element is uniquely determined; see the argument given in (I.20.3)(a). The condition $1 \neq 0$ serves to exclude the trivial ring $\{0\}$.

It is clear that not all the familiar arithmetic rules which are valid for the integers will hold in arbitrary rings; for example, the formula $a^2 - b^2 = (a+b)(a-b)$ relies on the commutativity of the multiplication and is therefore not true in noncommutative rings. However, some formulas are immediate consequences of the ring axioms and therefore valid in every ring.

(2.2) Proposition. *Let* R *be a ring and* $a,b \in R$. *Then*

$$a\cdot 0 = 0\cdot a = 0\,, \quad (-a)b = a(-b) = -ab\,, \quad (-a)(-b) = ab\,.$$

In particular, if R has an identity element 1 then $a(-1) = (-1)a = -a$.

Proof. We have $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0$. Adding $-(a \cdot 0)$ to both sides yields $a \cdot 0 = 0$. Similarly $0 \cdot a = 0$. Also, $(-a)b + ab = \big((-a) + a\big)b = 0 \cdot b = 0$ so that $(-a)b$ is indeed the additive inverse of ab, i.e., $(-a)b = -ab$. Similarly $a(-b) = -ab$. Finally, $(-a)(-b) = -a(-b) = -(-ab) = ab$. ∎

LET $(R, +, \cdot)$ be a ring. Then $(R, +)$ is an abelian group; therefore we can adopt the notation $m \cdot x$ for $m \in \mathbb{Z}$ and $x \in R$ which was introduced after definition (I.25.9).

If R has an identity element 1 we might encounter the phenomenon that the elements $1, 1 + 1, 1 + 1 + 1, \ldots$ are not all pairwise distinct because we might have $1 + 1 + \cdots + 1 = 0$ for a certain number of summands. For example, in $\mathbb{Z}_n$ we have $n \cdot 1 = 0$. To describe this phenomenon, we give the following definition.

(2.3) Definition. *Let R be a ring with identity element 1. The* **characteristic** $\operatorname{char} R$ *of R is defined as the smallest number $n \in \mathbb{N}$ such that $n \cdot 1 = 0$; if there is no such number we say that* $\operatorname{char} R = 0$.

BEFORE we turn to examples let us give one further definition.

(2.4) Definition. *Let $(R, +, \cdot)$ be a ring. A subset $U \subseteq R$ is called a* **subring** *of R if $(U, +, \cdot)$ is itself a ring. We write $U \leq R$ to express that U is a subring of R and also call $(R : U)$ a* **ring extension.** *If in this situation R has an identity element 1_R such that $1_R \in U$ then we call $(R : U)$ a* **unital ring extension.**

CLEARLY, U is a subring of R if and only if $0 \in U$ and if $x, y \in U$ implies that $-x \in U$, $x + y \in U$ and $xy \in U$. Moreover, if $(R : U)$ is a unital ring extension, then clearly 1_R is an identity element of U. On the other hand, it is possible that a ring extension $(R : U)$ is not unital even though both R and U possess an identity element. (See problem 16 below.)

(2.5) Examples. (a) With the usual addition and multiplication, all the sets in the chain

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

are commutative rings with identity, each a subring of all of its successors. For any $n \in \mathbb{Z}$, the set $n\mathbb{Z}$ of all multiples of n is a subring of $\mathbb{Z}$. Note that $n\mathbb{Z}$ has no identity unless $n = \pm 1$.

(b) Let $n \in \mathbb{Z} \setminus \{0, 1\}$ be square-free; i.e., $|n|$ is not divisible by the square of a natural number other than 1. Then let $\sqrt{n} := \begin{cases} \sqrt{n}, & \text{if } n > 0; \\ i\sqrt{|n|}, & \text{if } n < 0. \end{cases}$ Then

$$\mathbb{Z}[\sqrt{n}] \;:=\; \mathbb{Z} + \mathbb{Z}\sqrt{n} \;=\; \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$$

is a ring (with addition and multiplication inherited from $\mathbb{C}$), obviously the smallest subring of $\mathbb{C}$ containing $\sqrt{n}$.

(c) Fix a natural number n and consider the set $\mathbb{Z}_n$ of all residue classes modulo n as introduced in (I.20.14) in the group theory chapter. We saw in (I.20.14) that an addition and a multiplication on $\mathbb{Z}_n$ can be defined by

$$[x] + [y] := [x+y] \qquad \text{and} \qquad [x] \cdot [y] := [xy] .$$

It is easy to see that $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with identity element [1].

(d) The set $\mathbb{Z}[x]$ of all polynomials with integer coefficients, endowed with the usual addition and multiplication, is a commutative ring with identity. The same holds true for $\mathbb{Z}[x,y]$, the set of all polynomials in two variables x, y with coefficients in $\mathbb{Z}$.

(e) The set $K^{n\times n}$ of all $n \times n$-matrices with entries in the field K is a ring with identity which is not commutative for all $n \geq 2$. The set of all upper triangular matrices is a subring of $K^{n\times n}$.

(f) The set

$$\mathbb{H} := \{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C}\} \subseteq \mathbb{C}^{2\times 2}$$

is a subring of $\mathbb{C}^{2\times 2}$, called the ring of **quaternions**. (Compare with problem 19 in section [I.21] and with problem 32 in section [I.23].) Writing

$$\mathbf{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

we have

$$\mathbb{H} = \{a\mathbf{1} + bI + cJ + dK \mid a, b, c, d \in \mathbb{R}\} .$$

(g) Let $(A, +)$ be an arbitrary abelian group. Then A can be made into a commutative ring by defining $x \cdot y := 0$ for all $x, y \in A$; this multiplication is called the **trivial multiplication** on A.

(h) If $(U_i)_{i\in I}$ is a family of subrings of R, then the intersection $\bigcap_{i\in I} U_i$ and the sum

$$\sum_{i\in I} U_i := \{u_{i_1} + \cdots + u_{i_n} \mid n \in \mathbb{N},\ i_1, \ldots, i_n \in I,\ u_{i_k} \in U_{i_k}\}$$

are also subrings of R.

(i) An arbitrary ring R has its **center** $C(R) := \{x \in R \mid xy = yx \text{ for all } y \in R\}$ as a subring.

(j) If R is a subring of S and if $s_1, \ldots, s_n$ are elements of S, then the intersection of all subrings of S containing R and $s_1, \ldots, s_n$ is again a subring of S; it is denoted by $R[s_1, \ldots, s_n]$. † Obviously, $R[s_1, \ldots, s_n]$ is the smallest subring of R containing R and the elements $s_1, \ldots, s_n$; we say that $R[s_1, \ldots, s_n]$ is obtained from R by **adjoining** the elements $s_1, \ldots, s_n$.

IN the sequel we want to show how we can construct many new examples of rings from known rings.

(2.6) Example: Formal power series. Let R be an arbitrary ring. A **formal power series** over R is an expression

$$(\star) \qquad a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots =: \sum_{k=0}^{\infty} a_k x^k$$

† This notation was used in part (b) already.

where the coefficients a_k are elements of R and where x is a "symbol", an "indeterminate" or a "variable". This is too vague to be a good definition. Therefore, let us define a power series over R simply as a sequence

$$(\star\star) \qquad (a_0,\ a_1,\ a_2,\ a_3,\ \cdots)$$

of elements in R. Then $(\star)$ is just a different notation for $(\star\star)$, and the powers of the mysterious object x are merely used to label the positions in the sequence. The advantage of notation $(\star)$ becomes clear when we want to make the set of all power series over R into a ring. In notation $(\star\star)$, we define addition and multiplication by

$$(a_0,\ a_1,\ a_2,\ a_3,\ \cdots) + (b_0,\ b_1,\ b_2,\ b_3,\ \cdots) := (a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ a_3+a_3,\ \cdots)$$

and

$$\begin{aligned} &(a_0,\ a_1,\ a_2,\ a_3,\ \cdots)(b_0,\ b_1,\ b_2,\ b_3,\ \cdots) \\ :=&(a_0b_0,\ a_0b_1+a_1b_0,\ a_0b_2+a_1b_1+a_2b_0,\ a_0b_3+a_1b_2+a_2b_1+a_3b_0,\ \cdots) \\ =&\Big(\sum_{i+j=0} a_ib_j,\ \sum_{i+j=1} a_ib_j,\ \sum_{i+j=2} a_ib_j,\ \sum_{i+j=3} a_ib_j,\ \ldots\Big)\ . \end{aligned}$$

The definition for the multiplication might seem unintelligible at first, but becomes clear if one multiplies two "expressions" $a_0+a_1x+a_2x^2+\cdots$ and $b_0+b_1x+b_2x^2+\cdots$ with each other, using the normal arithmetic rules and not worrying too much about what the "symbol" x actually is. The ring of all formal power series over R is denoted by $R[[x]]$.

Observe that for any two ring elements $r, s \in R$ we have

$$\begin{aligned} (r,0,0,\cdots) + (s,0,0,\cdots) &= (r+s,0,0,\cdots) \qquad \text{and} \\ (r,0,0,\cdots) \cdot (s,0,0,\cdots) &= (rs,0,0,\cdots)\ . \end{aligned}$$

This shows that if we identify $r \in R$ with $(r,0,0,\cdots) \in R[x]$, we can consider R as a subring of $R[x]$. In notation $(\star)$ this just means that we view ring elements as "constant power series".

Clearly, $R[[x]]$ is commutative if and only if R is.

(2.7) Example: Polynomials. If R is any ring, then a **(formal) polynomial** over R is a formal power series with only a finite number of nonzero coefficients, i.e., an expression

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\ .$$

The set of all polynomials over R is denoted by $R[x]$ and is clearly a subring of $R[[x]]$. Again, we can identify R with the subring of all "constant" polynomials in $R[x]$.

Now suppose that R has an identity element 1. Then if we write

$$x := (0,\ 1,\ 0,\ 0,\ 0,\ \ldots) \in R[x]$$

it is easy to verify that

$$x^2 = (0,\ 0,\ 1,\ 0,\ 0,\ \ldots)\ ,\quad x^3 = (0,\ 0,\ 0,\ 1,\ 0,\ \ldots)\ ,\qquad \text{and so on.}$$

Formally defining $x^0 := (1,0,0,0,0,\ldots)$ we see that

$$\begin{aligned}&(a_0,\ a_1,\ a_2,\ \ldots,\ a_n,\ 0,\ 0,\ \ldots)\\ &= a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\end{aligned}$$

under the canonical identification of ring elements with constant polynomials. Hence the notation $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ for a polynomial is completely justified; the "symbol" x is no longer a mysterious object, but a well-defined element of $R[x]$. Similarly, the power series $\sum_{k=0}^{\infty} a_kx^k$ is the unique power series which coincides in the first n coefficients with the well-defined polynomial $a_0+a_1x+\cdots+a_nx^n$, for all $n \in \mathbb{N}_0$. Note however that we do not develop a notion of convergence that would allow us to talk about infinite sums.

IN a similar fashion we can define power series and polynomials in more than one variable.

(2.8) Example: Power series and polynomials in more than one variable. Let X be an arbitrary non-empty set. For the sake of convenience we choose an indexing $X = \{x_i \mid i \in I\}$ with $0 \notin I$. Then a formal power series over R in the (commuting) variables x_i $(i \in I)$ is an expression

$$a_0 + \sum_{i\in I} a_ix_i + \sum_{i,j\in I} a_{ij}x_ix_j + \sum_{i,j,k\in I} a_{ijk}x_ix_jx_k + \cdots$$

where the coefficients are elements of R and where in each of the sums occurring in this expression only finitely many of the coefficients are different from zero. More formally, we define the power series ring $R[[X]] = R[[(x_i)_{i\in I}]]$ as the set of all sequences

$$\left(a_0\ ,\ (a_i)_{i\in I}\ ,\ (a_{ij})_{i,j\in I}\ ,\ (a_{ijk})_{i,j,k\in I}\ ,\ \ldots\right)$$

where $a_0, a_i, a_{ij}, \ldots \in R$ and where each array $(a_{i_1i_2\ldots i_n})_{i_1,i_2,\ldots,i_n\in I}$ occurring in this sequence has only a finite number of nonzero members. The addition in $R[[X]]$ is defined by

$$\begin{aligned}&\left(a_0,\ (a_i)_i,\ (a_{ij})_{i,j},\ (a_{ijk})_{i,j,k},\ \ldots\right) + \left(b_0,\ (b_i)_i,\ (b_{ij})_{i,j},\ (b_{ijk})_{i,j,k},\ \ldots\right) =\\ &\left(a_0+b_0,\ (a_i+b_i)_i,\ (a_{ij}+b_{ij})_{i,j},\ (a_{ijk}+b_{ijk})_{i,j,k},\ \ldots\right),\end{aligned}$$

the multiplication by

$$\begin{aligned}&\left(a_0,\ (a_i)_i,\ (a_{ij})_{i,j},\ (a_{ijk})_{i,j,k},\ \ldots\right) \cdot \left(b_0,\ (b_i)_i,\ (b_{ij})_{i,j},\ (b_{ijk})_{i,j,k},\ \ldots\right) =\\ &\left(a_0b_0,\ \sum_i(a_0b_i+a_ib_0),\ \sum_{i,j}(a_0b_{ij}+a_ib_j+a_{ij}b_0),\ \sum_{i,j,k}(a_0b_{ijk}+a_ib_{jk}+a_{ij}b_k+a_{ijk}b_0),\ \ldots\right).\end{aligned}$$

As above, a polynomial is a power series with only a finite number of nonzero coefficients. The set of all polynomials over R in the variables $(x_i)_{i\in I}$ is denoted by $R[(x_i)_{i\in I}]$ and forms a subring of $R[[(x_i)_{i\in I}]]$. Again, R can be identified as the subring of all constant polynomials.

IN a concrete setting, the above formulas look much less complicated than in their general form. For example, in $\mathbb{Z}[x,y,z]$, the ring of polynomials in 3 variables x, y and z, we have

$$(x^2y^5 - y)(x^3 - x^2 + xyz) \;=\; x^5y^5 - x^3y - x^4y^6 - x^2y^2 + x^3y^6z - xy^2z \;,$$

and so on.

THE next example is the most important example of a non-commutative ring.

(2.9) Example: Matrix rings. Let R be a ring. Then the set $R^{n\times n}$ of all $n \times n$-matrices with coefficients in R is again a ring if we use the usual operations

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{n1}+b_{n1} & \cdots & a_{nn}+b_{nn} \end{pmatrix}$$

and

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} := \sum_{k=1}^{n} \begin{pmatrix} a_{1k}b_{k1} & \cdots & a_{1k}b_{kn} \\ \vdots & & \vdots \\ a_{nk}b_{k1} & \cdots & a_{nk}b_{kn} \end{pmatrix} .$$

If R has an identity element 1, then

$$\mathbf{1} := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

is an identity element of R. If $n \geq 2$, then the ring $R^{n\times n}$ is commutative if and only if the multiplication on R is trivial, i.e., if $xy = 0$ for all $x, y \in R$. Indeed, if there are two elements $x, y \in R$ with $xy \neq 0$, then

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & xy \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} .$$

DEPENDING on the context, there are different ways in which rings of functions can arise. Let us look at three examples.

(2.10) Example: Rings of functions with pointwise multiplication. Let R be a ring and $X \neq \emptyset$ be an arbitrary set. Then the set

$$R^X \;:=\; \{f : X \to R\}$$

of all functions from X to R is a ring with the argumentwise operations

$$(f+g)(x) \;:=\; f(x)+g(x) \qquad \text{and} \qquad (fg)(x) \;:=\; f(x)g(x) \;.$$

Clearly, R^X is commutative if and only if R is.

If X is not just a set, but has an additional structure, then we can single out subrings of R^X consisting of functions with special properties. For example, if X is a topological space, then the set $C(X)$ of all real-valued continuous functions on X is a subring of $X^{\mathbb{R}}$.

(2.11) Example: Rings of functions with composition multiplication. If $(A,+)$ is an abelian group, then

$$A^A \;=\; \{f : A \to A\}$$

is a ring with the operations

$$(f+g)(a) \;:=\; f(a)+g(a) \qquad \text{and} \qquad (f\circ g)(a) \;:=\; f\big(g(a)\big)\;.$$

The subset

$$\operatorname{End} A \;:=\; \{f : A \to A \mid f(a+b) = f(a)+f(b) \text{ for all } a,b \in A\}$$

is a subring of $(A^A,+,\circ)$, called the **endomorphism ring** of A.

NOTE that if R is a ring, then we can make R^R into a ring in two different ways, with the pointwise multiplication as in (2.10) or with the composition multiplication as in (2.11). In this case it is important to write down a ring as a triplet (either $(R^R,+,\cdot)$ or $(R^R,+,\circ)$) to make clear what operations are used.

ON some spaces of functions a third type of multiplication can be defined, which is called convolution.

(2.12) Example: Convolution rings. We do not want to give the most general definition of a convolution ring, but instead consider some examples.

The set $C(\mathbb{R}^n)$ of all continuous functions on $\mathbb{R}^n$ or the set $L^2(\mathbb{R}^n)$ of all square-integrable functions on $\mathbb{R}^n$ can be made into a ring with the operations

$$(f+g)(x) \;:=\; f(x)+g(x) \qquad \text{and} \qquad (f\star g)(x) \;:=\; \int_{\mathbb{R}^n} f(x-y)g(y)\,\mathrm{d}\,y\;.$$

For $C[0,\infty)$ we can define a modified version of these operations, namely

$$(f+g)(x) \;:=\; f(x)+g(x) \qquad \text{and} \qquad (f\star g)(x) \;:=\; \int_0^x f(x-t)g(t)\,\mathrm{d}\,t\;.$$

In both cases it is easy to check that the convolution product $\star$ is commutative.

Note that the multiplication of power series is given by a similar pattern. If we identify a power series $(a_0,a_1,a_2,\ldots)$ over R with the function $a : \mathbb{N}_0 \to R$ given by $a(n) = a_n$, then multiplication of power series corresponds to convolution of functions:

$$(a\star b)(n) \;=\; \sum_{k=0}^{n} a(n-k)b(k)\;.$$

LET us now see how new rings can be constructed from a given family of rings.

(2.13) Example: Direct product and direct sum. The **direct product** of a family $(R_i)_{i\in I}$ of rings is defined as

$$\prod_{i\in I} R_i \;:=\; \{r : I \to \bigcup_{i\in I} R_i \mid r(i) \in R_i\} \;.$$

This is a ring if we define the operations argumentwise, i.e., by

$$(r+s)(i) \;:=\; r(i)+s(i) \quad \text{and} \qquad (rs)(i) \;:=\; r(i)s(i) \;.$$

This means that $\prod_{i\in I} R_i$ is a subring of $(\bigcup_{i\in I} R_i)^I$.

Sometimes it is convenient to write the elements of $\prod_{i\in I} R_i$ as tuples $(r_i)_{i\in I}$; addition and multiplication are then understood componentwise:

$$(r_i)_{i\in I} + (s_i)_{i\in I} \;:=\; (r_i+s_i)_{i\in I} \qquad \text{and} \qquad (r_i)_{i\in I}(s_i)_{i\in I} \;:=\; (r_is_i)_{i\in I}$$

It is easy to see that $\prod_{i\in I} R_i$ is commutative if and only if all the rings R_i are.

The **direct sum** of a family $(R_i)_{i\in I}$ is the subring of $\prod_{i\in I} R_i$ which consists of all elements r such that $r_i = 0$ for almost all indices i, i.e., $r_i \neq 0$ for only a finite number of indices i. So

$$\bigoplus_{i\in I} R_i \;:=\; \{(r_i)_{i\in I} \mid r_i = 0 \text{ for almost all } i \in I\} \;.$$

For a finite family of rings, we also introduce the notation

$$\prod_{i=1}^{n} R_i \;:=\; R_1 \times \cdots \times R_n \qquad \text{and} \qquad \bigoplus_{i=1}^{n} R_i \;:=\; R_1 \oplus \cdots \oplus R_n \;;$$

clearly, the direct sum and the direct product coincide in this case.

WE have introduced rings as sets with a certain algebraic structure, and we have seen many examples of rings. Now – as we saw already in our investigation of groups – the study of sets with a certain algebraic structure includes a study of those functions between these sets that preserve the algebraic structure. In the case of rings, this leads to the notion of a ring homomorphism. Since the situation is completely analogous to the group case, we can proceed faster than we did there.

(2.14) Definitions. (a) *A mapping $f : R \to S$ between two rings is called a* **ring homomorphism** *if*

$$f(0) \;=\; 0 \;, \quad f(a+b) \;=\; f(a)+f(b) \quad \textit{and} \quad f(ab) \;=\; f(a)f(b) \;\textit{for all } a,b \in R \;.$$

The **kernel** $\ker f$ *and the* **image** $\operatorname{im} f = f(R)$ *are defined by*

$$\ker f \;:=\; \{a \in R \mid f(a) = 0\} \qquad \textit{and} \qquad \operatorname{im} f \;:=\; \{f(a) \mid a \in A\} \;.$$

(b) *A bijective ring homomorphism f is called a* **ring isomorphism**; *in this case f^{-1} is also a ring isomorphism. We say that two rings R and S are* **isomorphic** *and write $R \cong S$ if there is a ring isomorphism $f : R \to S$.*

(c) *An injective ring homomorphism $f : R \to S$ is called an* **embedding**.

AN isomorphism $f : R \to S$ can be thought of as a simple renaming of the elements in R; we call an element $f(r)$ instead of r but nothing else changes. This means that R and S are in some sense simply two realizations of the same ring. Similarly, if an embedding $f : R \to S$ is given we can identify R with its image $f(R)$ and thus treat R as a subring of S. We did this already when we considered R as a subring of $R[x]$ or $R[[x]]$ by identifying a ring element $r \in R$ with the constant polynomial r.

LET us summarize the basic properties of ring homomorphisms.

(2.15) Lemma. *Let $f : R \to S$ be a ring homomorphism.*

(a) *If U is a subring of R, then $f(U)$ is a subring of S. If V is a subring of S, then $f^{-1}(V)$ is a subring of R.*

(b) *If R is commutative, then so is $f(R)$. If R has an identity element 1 and f is not the zero mapping, then $f(R)$ has an identity element, namely $f(1)$.*

(c) $\ker f$ *is a subring of R, and* $\operatorname{im} f$ *is a subring of S.*

Proof. (a) Let U be a subring of R. Then $0_S = f(0_R) \in f(U)$. Let $u_1, u_2 \in U$. Then $f(u_1) + f(u_2) = f(u_1 + u_2) \in f(U)$, $-f(u_1) = f(-u_1) \in f(U)$ and $f(u_1)f(u_2) = f(u_1u_2) \in f(U)$. So $f(U) + f(U) \subseteq f(U), -f(U) \subseteq f(U)$ and $f(U)f(U) \subseteq f(U)$. This shows that $f(U)$ is a subring of S.

Now let V be a subring of S. Then $0_R \in f^{-1}(V)$ because $f(0_R) = 0_S \in V$. Let $u_1, u_2 \in f^{-1}(V)$, i.e., $f(u_1), f(u_2) \in V$. Then $f(u_1+u_2) = f(u_1)+f(u_2) \subseteq V+V \subseteq V$ so that $u_1 + u_2 \in f^{-1}(V)$. Similarly, $-u_1$ and u_1u_2 belong to $f^{-1}(V)$. This shows that $f^{-1}(V)$ is a subring of R.

(b) If $ab = ba$, then $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$. Let R have an identity element 1 and let $f \not\equiv 0$. Then there is an element $r_0 \in R$ with $0 \neq f(r_0) = f(r_0 \cdot 1) = f(r_0)f(1)$ which implies $f(1) \neq 0$. Moreover, $f(1)f(r) = f(r)f(1) = f(r)$ for all $r \in R$.

(c) $\ker f = f^{-1}(\{0\})$ is a subring of R and $\operatorname{im} f = f(R)$ is a subring of S due to part (a). ∎

(2.16) Examples. (a) If R is any ring the mapping $x \mapsto -x$, i.e., multiplication by -1, is an automorphism.

(b) The complex conjugation $z \mapsto \overline{z}$ defines a ring isomorphism $f : \mathbb{C} \to \mathbb{C}$.

(c) If n is a square-free number then the mapping $\mathbb{Z} + \mathbb{Z}\sqrt{n} \to \mathbb{Z} + \mathbb{Z}\sqrt{n}$ given by $a + b\sqrt{n} \mapsto a - b\sqrt{n}$ is an automorphism.

(d) If $d \mid m$ then we can define a mapping $f : \mathbb{Z}_m \to \mathbb{Z}_d$ by $f([x]_m) = [x]_d$. This mapping is a surjective ring homomorphism.

(e) The mapping $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ given by $[a]_{mn} \mapsto ([a]_m, [a]_n)$ is a well-defined homomorphism. It is easy to see that this mapping is injective (and hence an isomorphism) if and only if m and n are relatively prime. Consequently, if $n = p_1^{r_1} \cdots p_k^{r_k}$ then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$.

(f) If R is any ring and $r \in R$ an element of R, then the mapping $f : \mathbb{Z} \to R$ given by $f(m) = m \cdot r$ is a ring homomorphism.

(g) For a ring R and a set X, let R^X be the ring of all functions $f : X \to R$ with the pointwise operations. Then for any $x_0 \in X$ the **evaluation map**

$$\begin{array}{ccc} R^X & \to & R \\ f & \mapsto & f(x_0) \end{array}$$

is a homomorphism. This mapping is obtained by simply "plugging in" the argument x_0 into any given function f.

(h) Let R be a ring and $\varphi \in R[x]$ be a fixed polynomial. Then an endomorphism $\Phi : R[x] \to R[x]$ is defined by $f(x) \mapsto f\big(\varphi(x)\big)$, i.e., by

$$\Phi(a_0 + a_1 x + \cdots + a_n x^n) \;:=\; a_0 + a_1\varphi(x) + \cdots + a_n\varphi(x)^n \;.$$

Thus "plugging in" $\varphi(x)$ for x respects addition and multiplication.

(i) Given a set X and a ring R we can consider the ring R^X of all mappings $f : X \to R$ with the pointwise operations. Then for any subset $Y \subseteq X$ the **restriction map**

$$\begin{array}{ccc} R^X & \to & R^Y \\ f & \mapsto & f|_Y \end{array}$$

is a ring homomorphism.

(j) Let R be a commutative ring. If $\operatorname{char} R$ is a prime number p then the mapping $f : R \to R$ given by $f(x) = x^p$ is a homomorphism. This stems from the facts that $(xy)^p = x^p y^p$ (due to the commutativity of R) and $(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k = x^p + y^p$ (due to the property that $\binom{p}{k}$ is divisible by $p = \operatorname{char} R$ for $1 \le k \le p-1$). One calls $f : R \to R$ the **Frobenius homomorphism** of the ring R.

Exercises

Problem 1. (a) Let x, y be elements of a ring R such that $xy = yx$. Show that

$$(x+y)^n \;=\; x^n \;+\; \sum_{k=1}^{n-1} \binom{n}{k} x^{n-k}y^k \;+\; y^n$$

for all $n \in \mathbb{N}$. (If R has an identity element 1, we formally define $x^0 := 1$ for all $x \in R$; then the above equation becomes $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$.)

(b) Show that if R is a commutative ring of prime characteristic $\operatorname{char} R = p$, then $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for all $x, y \in R$ and all $n \in \mathbb{N}$.

(c) Let R be a commutative ring with identity. Prove the polynomial formula

$$(x_1 + x_2 + \cdots + x_n)^m \;=\; \sum_{\substack{m_1,\ldots,m_n \geq 0,\\ m_1+\cdots+m_n = m}} \frac{m!}{m_1!m_2!\cdots m_n!} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$$

where $x_1, \ldots, x_n \in R$ and $x^0 := 1$. **Hint.** Use induction on m.

Problem 2. Suppose the set R is equipped with two binary operations $+$ and $\cdot$ such that $(R,+)$ is a group, $(R,\cdot)$ is a semigroup with identity element 1, and $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$ for all $x, y, z \in R$. Conclude that $(R,+,\cdot)$ is a ring, i.e., show that the operation $+$ is necessarily commutative.

Hint. Calculate $(a+b)(1+1)$ in two ways, using both distributive laws.

Problem 3. Show that the following sets are subrings of $\mathbb{C}$.

(a) $R := \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \text{ is not divisible by } p\}$ where $p \in \mathbb{N}$ is a prime number.

(b) $S := \mathbb{Z} + \mathbb{Z}\varepsilon + \mathbb{Z}\varepsilon^2 + \cdots + \mathbb{Z}\varepsilon^{n-1}$ where $\varepsilon := e^{2\pi i/n}$.

Problem 4. (a) Let R be a ring and let S be an arbitrary set. Suppose that there is a bijection $f : R \to S$. Show that then S can be made into a ring (which is isomorphic to R) by defining

$$s_1 + s_2 := f\big(f^{-1}(s_1) + f^{-1}(s_2)\big) \qquad \text{and} \qquad s_1 \cdot s_2 := f\big(f^{-1}(s_1) \cdot f^{-1}(s_2)\big)\,.$$

(b) Given a ring $(R,+,\cdot)$ with identity, define new operations $\oplus$ and $\odot$ on R by $a \oplus b := a + b - 1$ and $a \odot b := a + b - ab$. Show that the zero element of $(R,+,\cdot)$ becomes the identity element of $(R,\oplus,\odot)$ and vice versa.

Problem 5. (a) Let R be a ring whose additive group $(R,+)$ is cyclic. Show that R is commutative.

(b) Let R be a finite ring with p elements where p is a prime number. Show that $R \cong \mathbb{Z}_p$ or $xy = 0$ for all $x, y \in R$.

Problem 6. Let $S = \{a, b, c, d\}$ be a set with 4 elements. Show that S can be made into a non-commutative ring by defining addition and multiplication as follows.

$$\begin{array}{c|cccc} + & a & b & c & d \\ \hline a & a & b & c & d \\ b & b & a & d & c \\ c & c & d & a & b \\ d & d & c & b & a \end{array} \qquad \begin{array}{c|cccc} \cdot & a & b & c & d \\ \hline a & a & a & a & a \\ b & a & a & b & b \\ c & a & a & c & c \\ d & a & a & d & d \end{array}$$

Hint. Consider the matrices $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ with coefficients in $\mathbb{Z}_2$.

Problem 7. Let R be a commutative ring with identity element 1 and let $R^{\mathbb{N}}$ be the set of all mappings $f : \mathbb{N} \to R$. Define two operations on $R^{\mathbb{N}}$ by

$$(f+g)(n) := f(n) + g(n), \quad (f \star g)(n) := \sum_{xy=n} f(x)g(y)$$

where the sum in the definition of the convolution product $\star$ runs over all pairs $(x, y) \in \mathbb{N} \times \mathbb{N}$ with $xy = n$.

(a) Show that $(R^{\mathbb{N}}, +, \star)$ is a commutative ring which possesses an identity element δ, namely

$$\delta(x) := \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \neq 1. \end{cases}$$

(b) A function $f \in R^{\mathbb{N}}$ is called **multiplicative** if $f(mn) = f(m)f(n)$ whenever $m, n \in \mathbb{N}$ are relatively prime. Show that the set of all multiplicative functions is a subring of $R^{\mathbb{N}}$.

(c) Define the **Möbius function** $\mu : \mathbb{N} \to R$ by

$$\mu(n) := \begin{cases} 1, & \text{if } n = 1; \\ (-1)^r, & \text{if } n = p_1 \cdots p_r \text{ with } r \text{ distinct prime factors;} \\ 0, & \text{if } n \text{ has a multiple prime factor.} \end{cases}$$

Show that μ is multiplicative and verify $\mu \star 1 = \delta$ where 1 denotes the constant function with the value 1.

(d) Suppose f and F are elements of $R^{\mathbb{N}}$. Show that $F = \mu \star f$ if and only if $f = \mu \star F$.

(e) Given $f \in R^{\mathbb{N}}$, let $F(n) := \sum_{d|n} f(d)$. Show that f can be reconstructed from F via

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) \quad \textbf{(Möbius inversion formula).}$$

Problem 8. Define functions $\sigma, \tau : \mathbb{N} \to \mathbb{Z}$ by

$\tau(n)$:= number of divisors of n ;

$\sigma(n)$:= sum of the divisors of n ;

$\varphi(n)$:= number of natural numbers less than n which are coprime with n .

(Note that φ is Euler's function introduced in (I.21.12) already.)

(a) Show that τ, σ and φ are multiplicative functions which satisfy the equations $\tau = 1 \star 1$, $\sigma = 1 \star \mathrm{id}_{\mathbb{N}}$ and $\varphi = \mu \star \mathrm{id}_{\mathbb{N}}$.

(b) Show that if $n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ is the prime factorization of a natural number n then

$$\begin{aligned} \tau(n) &= (r_1+1)(r_2+1)\cdots(r_m+1)\,, \\ \sigma(n) &= \frac{p_1^{r_1+1}-1}{p_1-1}\,\frac{p_2^{r_2+1}-1}{p_2-1}\cdots\frac{p_m^{r_m+1}-1}{p_m-1}\,, \\ \varphi(n) &= (p_1^{r_1}-p_1^{r_1-1})(p_2^{r_2}-p_2^{r_2-1})\cdots(p_m^{r_m}-p_m^{r_m-1})\,. \end{aligned}$$

(c) A natural number n is called **perfect** if it equals the sum of its proper divisors, i.e., if $\sigma(n) = 2n$. Show that if p is a prime number of the form $p = 2^{s+1} - 1$ then the number $n := 2^s p$ is perfect. Find some examples of perfect numbers!

(d) Show that φ takes each of its values only a finite number of times and that $\varphi(n)$ is even for all $n > 2$. Moreover, show that if $d \mid n$ then $\varphi(d) \mid \varphi(n)$.

Problem 9. (a) Let R be a ring with identity such that $x^3 = x$ for all $x \in R$. Show that $6 \cdot x = 0$ and $xy = yx$ for all $x, y \in R$.

(b) Let R be a ring with identity such that $x^4 = x$ for all $x \in R$. Show that R is commutative.

Problem 10. Let R be a ring.

(a) Show that a ring structure on $R \times R$ is given by

$$(a,b) + (c,d) := (a+c, b+d) \qquad \text{and} \qquad (a,b) \cdot (c,d) := (ac, ad+bc)\,.$$

(b) Let $R \times R$ be the ring with addition and multiplication as in (a). Show that

$$f : \begin{array}{ccc} R \times R & \to & R^{2\times 2} \\ (a,b) & \mapsto & \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \end{array}$$

is a ring homomorphism.

(c) Can you use the mapping f given in (b) to prove (a) without the need to check all the ring axioms?

Problem 11. Let R be a commutative ring with identity. Its "complexification" is defined as $R \times R$ with the operations

$$(a,b) + (c,d) := (a+c, c+d) \quad \text{and} \quad (a,b)(c,d) := (ac - bd, ad + bc)\,.$$

Considering R is a subring of $R \times R$ via $a \mapsto (a,0)$ and writing $i := (0,1)$, we can express each element of $R \times R$ in the form $a + ib$ with $a, b \in R$ where $i^2 = -1 \in R$. This explains the name "complexification" and the notation $R + iR$ for this ring.

Show that

$$f : \begin{array}{ccc} R + iR & \to & R^{2\times 2} \\ a + ib & \mapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array}$$

is a ring homomorphism.

Problem 12. Consider the ring $R = K^{n\times n}$ where K is a field.
(a) Find the center of R.
(b) Let U be the subring of R generated by all symmetric matrices. Show that $U = R$.

Problem 13. Let R be a ring and $X \subseteq R$. The **centralizer** of X in R is

$$C(X) := \{a \in R \mid ax = xa \text{ for all } x \in X\} .$$

(a) Show that $C(X)$ is a subring of R.
(b) Show that $X_1 \subseteq X_2$ implies $C(X_1) \supseteq C(X_2)$.
(c) Show that $X \subseteq C\big(C(X)\big)$ and $C(X) = C\Big(C\big(C(X)\big)\Big)$.
(d) Let $R = \mathbb{R}^{2\times 2}$ and $X := \{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R}\}$. Find $C(X)$.
(e) Find $C(X)$ where $X := \{\mathrm{diag}(1,2)\} \subseteq \mathbb{R}^{2\times 2}$.

Problem 14. Let R be a ring and $X \subseteq R$. The **(left) annihilator** of X in R is

$$A(X) := \{a \in R \mid ax = 0 \text{ for all } x \in X\} .$$

(a) Show that $A(X)$ is a subring of R.
(b) Show that $X_1 \subseteq X_2$ implies $A(X_1) \supseteq A(X_2)$.
(c) Show that if R is commutative then $X \subseteq A\big(A(X)\big)$ and $A(X) = A\Big(A\big(A(X)\big)\Big)$.
(d) Let $R = \mathbb{R}^{2\times 2}$ and $X := \{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R}\}$. Find $A(X)$.
(e) Find $A(X)$ where $X := \{\mathrm{diag}(1,2)\} \subseteq \mathbb{R}^{2\times 2}$.

Problem 15. (a) Let $f : R \to S$ be a ring homomorphism. Show that if R has an identity element 1, then $f(1)$ is an identity element for $f(R)$, but it may happen that S does not possess an identity element.
(b) Let $R = \{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R}\}$ and $S := \mathbb{R}^{2\times 2}$. Show that both R and S have an identity element, but that the inclusion mapping $f : R \to S$ does *not* satisfy $f(1_R) = 1_S$.

Problem 16. (a) Clearly, $\mathbb{Z}$ is a ring with identity. Find a subring of $\mathbb{Z}$ which has no identity element.

(b) Clearly, $\mathbb{Z}_6$ is a ring with identity. Show that the subring $U := \{[0],[2],[4]\}$ of R also has an identity element, but that the identity element of U is not the same as the identity element of $\mathbb{Z}_6$.

Remark. This phenomenon is further investigated in the next problem. Also compare with problem 15(b).

(c) Define a ring R and a subring $U \leq R$ as follows:

$$R := \{\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R}\}\,, \qquad U := \{\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid a \in \mathbb{R}\}\,.$$

Show that R does not possess an identity element, but U does.

Problem 17. Let U be a subring of $R := \mathbb{Z}_n$. Show that the following conditions are equivalent:

(a) U has an identity element;

(b) there is an element $u \in R$ with $u^2 = u$ and $U = Ru\,(= \mathbb{Z} \cdot u)$.

Problem 18. Let $(R_i)_{i\in I}$ be a family of rings. Under what circumstances do the direct product $\prod_{i\in I} R_i$ and the direct sum $\bigoplus_{i\in I} R_i$ possess an identity element?

Problem 19. (a) Let $R = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a,b \in \mathbb{R}\}$, considered as a subring of $\mathbb{R}^{2\times 2}$. Show that R has no identity element but that each element of the form $e = \begin{pmatrix} 1 & \star \\ 0 & 0 \end{pmatrix}$ is a **left-identity**, i.e., satisfies $ex = x$ for all $x \in R$.

(b) Let R be a ring with a *unique* element $e \neq 0$ such that $ex = x$ for all $x \in R$. Show that e is an identity element.

Hint. Calculate $(xe - x + e)y = y$ for $x, y \in R$.

Problem 20. Let R be a ring.

(a) Define operations on $\mathbb{Z} \times R$ as follows:

$$(m,x) + (n,y) := (m+n, x+y)\,, \quad (m,x)(n,y) := (mn, n\cdot x + m \cdot y + xy)\,.$$

Show that $\mathbb{Z} \times R$ is a ring of characteristic 0 with identity element $(1,0)$ which is commutative if and only if R is. Show that the mapping $x \mapsto (0,x)$ defines an embedding of R into $\mathbb{Z} \times R$. (This shows that every ring can be embedded into a unitary ring.)

(b) Show that if R has the property that $k \cdot x = 0$ for all $x \in x$ then we can do part (a) with $\mathbb{Z}_k \times R$ instead of $\mathbb{Z} \times R$ so that R can be embedded in a unitary ring of characteristic k.

Problem 21. Show that every ring $(R, +, \cdot)$ can be embedded into the endomorphism ring of an abelian group.

Hint. Show that if R has an identity element then

$$\begin{array}{ccc} R & \to & \mathrm{End}(R,+) \\ a & \mapsto & l_a \end{array}$$

is an embedding where $l_a : R \to R$ denotes the left-translation $x \mapsto ax$. For the general case, use problem 20.

Problem 22. Let $f : R \to S$ be a ring homomorphism.
(a) Show that a ring homomorphism $F : R[x] \to S[x]$ is defined by

$$F(a_0 + a_1 x + \cdots + a_n x^n) \;:=\; f(a_0) + f(a_1)x + \cdots + f(a_n)x^n \;.$$

How are $\ker F$ and $\operatorname{im} F$ related to $\ker f$ and $\operatorname{im} f$?
(b) Show that a ring homomorphism $F : R^{n\times n} \to S^{n\times n}$ is defined by

$$F\big((a_{ij})_{i,j}\big) \;:=\; \big(f(a_{ij})\big)_{i,j} \;.$$

How are $\ker F$ and $\operatorname{im} F$ related to $\ker f$ and $\operatorname{im} f$?

Problem 23. (a) Let R be a commutative ring. Show that the translation $l_a : R \to R$ given by $x \mapsto ax$ is a ring homomorphism if and only if $a^2 = a$.
(b) Find all endomorphisms of $\mathbb{Z}_q$ where q is a prime power.
(c) Find all endomorphisms of the rings $\mathbb{Z}, \mathbb{Z}^n, \mathbb{Q}, \mathbb{Q}[\sqrt{7}]$ and $\mathbb{Q}[\sqrt[3]{2}]$.

Problem 24. Show that the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are not isomorphic.

Problem 25. (a) Show that the only ring homomorphisms $f : \mathbb{Q} \to \mathbb{Q}$ are the zero mapping and the identity.
(b) Show that the only ring homomorphisms $f : \mathbb{R} \to \mathbb{R}$ are the zero mapping and the identity.
(c) Find a ring homomorphism $f : \mathbb{C} \to \mathbb{C}$ which is neither zero nor the identity.

Problem 26. (a) Show that there is a surjective ring homomorphism $f : \mathbb{Z}_m \to \mathbb{Z}_n$ if and only if $n \mid m$.
(b) Show that there is an injective ring homomorphism $f : \mathbb{Z}_m \to \mathbb{Z}_n$ if and only if $m \mid n$ and n/m is relatively prime with m.
(c) Show that if $m \in \mathbb{Z}_n^\times$ then the mapping $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $[k] \mapsto [mk]$ is a bijection.

Problem 27. Let $\{p_1, p_2, p_3, \ldots\}$ the set of all prime numbers.
(a) Show that for each number N the canonical map $\mathbb{Z} \to \prod_{k=1}^{N} \mathbb{Z}_{p_k}$ is surjective but not injective.
(b) Show that the canonical map $\mathbb{Z} \to \prod_{k=1}^{\infty} \mathbb{Z}_{p_k}$ is injective but not surjective.

Problem 28. Consider the ring $\mathbb{H}$ of quaternions.

(a) Recall that the conjugation of quaternions is defined by $\overline{a+bi+cj+dk} = a-bi-cj-dk$. Compute $x\bar{x}$ and $\bar{x}x$ where $x = a+bi+cj+dk$. Is conjugation a ring homomorphism?

(b) Find all the solutions of the equation $x^2 = x$ in $\mathbb{H}$.

(c) Find all the solutions of the equation $x^2 + 1 = 0$ in $\mathbb{H}$.

Problem 29. Let $f : R \to S$ be a mapping between rings such that for any two elements $x, y \in R$ the following conditions hold:

(1) $f(x+y) = f(x) + f(y)$;

(2) $f(xy) = f(x)f(y)$ or $f(xy) = f(y)f(x)$.

Show that f is a ring homomorphism or else $f(xy) = f(y)f(x)$ for all $x, y \in R$.

Hint. For all $x \in R$, consider the sets $U_x = \{y \in R \mid f(xy) = f(x)f(y)\}$ and $V_x = \{y \in R \mid f(xy) = f(y)f(x)\}$.

Problem 30. (a) Find all solutions of the equation $x^2 = x$ in $\mathbb{Z}_{10}$, $\mathbb{Z}_{20}$ and $\mathbb{Z}_{30}$.

(b) Find all solutions of the equation $x^2 = x$ in $\mathbb{Z}_{p^k}$ where p is a prime.

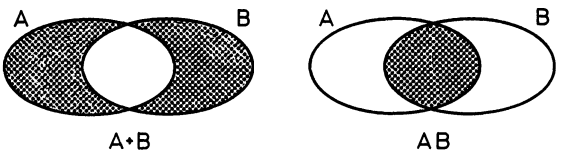
Problem 31. An element x in a ring R is called an **idempotent** if $x^2 = x$. A ring R is called a **Boolean ring** if every element of R is an idempotent.

(a) Show that $\mathbb{Z}_2$ is a Boolean ring.

(b) Let $X \neq 0$ be an arbitrary set. Show that the set $\mathbb{Z}_2^X$ of all mappings $f : X \to \mathbb{Z}_2$ is a Boolean ring if addition and multiplication are defined argumentwise.

(c) Let X be an arbitrary set and $\mathcal{P}(X)$ its power set, i.e., the set of all subsets of X. Show that $\mathcal{P}(X)$ becomes a Boolean ring if we define addition and multiplication by

$$A + B := (A \setminus B) \cup (B \setminus A) \quad \text{and} \quad A \cdot B := A \cap B .$$



What is the zero element in $(\mathcal{P}(X), +, \cdot)$? Does $\mathcal{P}(X)$ possess an identity element? If X has n elements, how many solutions does the equation $x^2 = x$ have in $\mathcal{P}(X)$?

Hint. Consider the mapping $\mathfrak{P}(X) \to \mathbb{Z}_2^X$ which assigns to each subset $A \subseteq X$ its characteristic function χ_A which is defined by

$$\chi_A(x) := \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{if } x \notin A. \end{cases}$$

(d) Let R be an arbitrary commutative ring and let B be the set of all idempotents in R. Define an addition and a multiplication on B by letting $x \oplus y := x + y - 2xy$ and $x \odot y := xy$. Show that $(B, \oplus, \odot)$ is a Boolean ring.

Problem 32. Let R be a Boolean ring.
(a) Show that $xy + yx = 0$ for all $x, y \in R$.
(b) Show that $x + x = 0$ for all $x \in R$. (Hence if $R \neq \{0\}$ then $\operatorname{char} R = 2$.)
(c) Show that R is commutative.

Problem 33. Show that every Boolean ring without identity can be embedded into a Boolean ring with identity.

Problem 34. A Boolean algebra is a set B together with two binary operations $\wedge$ and $\vee$ on B, two distinguished elements 0 and 1 in B and a self-mapping $x \mapsto \overline{x}$ † such that for all elements $x, y, z \in B$ the following rules:
(1) $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ (commutative laws);
(2) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ (distributive laws);
(3) $x \vee 0 = x$ and $x \wedge 1 = x$ (so that 0 and 1 are neutral elements);
(4) $x \wedge \overline{x} = 0$ and $x \vee \overline{x} = 1$.
(To get some intuition for these axioms see problem 35 for examples.)
(a) Prove that if B is a Boolean algebra and if $x, y, z \in B$ then the following conditions hold:
(5) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$ (associative laws);
(6) $\overline{x \wedge y} = \overline{x} \vee \overline{y}$ and $\overline{x \vee y} = \overline{x} \wedge \overline{y}$ (de Morgan's laws);
(7) $x \wedge x = x$ and $x \vee x = x$ (idempotency laws);
(8) $x \wedge 0 = 0$ and $x \vee 1 = 1$;
(9) $\overline{0} = 1$ and $\overline{1} = 0$;
(10) $\overline{\overline{x}} = x$.
(b) Show that every algebraic identity in a Boolean algebra remains true if one exchanges $\vee$ and $\wedge$ and also exchanges 0 and 1 in this identity.
(c) Let R be a Boolean ring with identity. Show that R becomes a Boolean algebra if we define meet, join and complement by

$$x \wedge y := xy\,, \quad x \vee y := x + y + xy\,, \quad \overline{x} = 1 + x\,.$$

(d) Let R be a Boolean algebra. Show that R becomes a Boolean ring if we define addition and multiplication by

$$x + y := (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \quad \text{and} \quad xy := x \wedge y\,.$$

Problem 35. In each of the following examples, a set R with two operations $\vee$ and $\wedge$, two distinguished elements 0 and 1 and a self-mapping $x \mapsto \overline{x}$ is given. Decide in each case which of the properties (1) through (10) in problem 34 are satisfied.
(a) Let $R = \{0, 1\}$ be a set with two elements and the following operations.

$$\begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \qquad \begin{array}{l} \overline{0} = 1 \\ \overline{1} = 0 \end{array}$$

† If $x, y \in B$ then $x \wedge y$ and $x \vee y$ are called the **meet** and the **join** of x and y, respectively; moreover, one calls $\overline{x}$ the **complement** of x.

(b) Let $R = \{0, 1, a, b\}$ be a set with four elements and the following operations.

$$\begin{array}{c|cccc} \vee & 0 & 1 & a & b \\ \hline 0 & 0 & 1 & a & b \\ 1 & 1 & 1 & 1 & 1 \\ a & a & 1 & a & 1 \\ b & b & 1 & 1 & b \end{array} \qquad \begin{array}{c|cccc} \wedge & 0 & 1 & a & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & a & b \\ a & 0 & a & a & 0 \\ b & 0 & b & 0 & b \end{array} \qquad \begin{array}{l} \overline{0} = 1 \\ \overline{1} = 0 \\ \overline{a} = b \\ \overline{b} = a \end{array}$$

(c) Let R be the interval $[0,1]$ and define $x \vee y := \max(x,y)$, $x \wedge y := \min(x,y)$ and $\overline{x} := 1 - x$.

(d) Let N be a given natural number and let R be the set of divisors of N. The special elements $\mathbf{0}$ and $\mathbf{1}$ in R are defined by $\mathbf{0} := 1$ and $\mathbf{1} := N$. Moreover, let $m \vee n := \mathrm{lcm}(m,n)$ and $m \wedge n := \gcd(m,n)$. Finally, $\overline{m} := N/m$.

(e) Let X be a nonempty set and let $R = \mathfrak{P}(X)$ be the power set of X with the operations $A \vee B := A \cup B$, $A \wedge B := A \cap B$ and $\overline{A} := X \setminus A$.

Problem 36. In his work "Investigations of the laws of thought" (1854) the British mathematician George Boole (1815-1864) laid the foundations for an algebraic treatment of logic. In this problem some ideas and consequences of Boole's work are outlined. Let X be a nonempty set.

(a) For any statement A about elements of X we let $T(A) := 1$ if A is true and $T(A) := 0$ if A is false. (This defines a **truth function** on any set of statements about elements of X.) For simplicity we write $T(A) = a$, $T(B) = b$, and so on. Show that

$$T(A \text{ and } B) \;=\; a + b - ab \quad \text{and} \quad T(A \text{ or } B) \;=\; ab$$

for all statements A and B where addition and multiplication are in $\mathbb{Z}_2$. As an example of how the use of T allows one to reduce logical problems to algebraic equations, show that exactly one of four statements A, B, C, D is false (the other three being true) if and only if $abcd = 0$ and $abc + abd + acd + bcd = 1$.

(b) For an element A of an electrical circuit with exactly one entrance and one exit let $T(A) := 1$ if current can flow from the entrace to the exit and $T(A) := 0$ otherwise. (For example, if A is just a piece of wire then $T(A) = 1$ whereas if A is a piece of wire which is disconnected by an open switch then $T(A) = 0$.) For simplicity we write $T(A) = a$, $T(B) = b$, and so on. Denote by $A \vee B$ the parallel connection and by $A \wedge B$ the series connection of A and B. Show that $T(A \vee B) = a + b - ab$ and $T(A \wedge B) = ab$ where addition and multiplication are in $\mathbb{Z}_2$. Find a connection to part (a) and discuss its implications for the possibility of processing information on a digital computer.

(c) Let $\mathfrak{S}(X)$ be all sentential formulas in one variable which become either true or false if an element $x \in X$ is plugged in for the variable. (Typical examples are "x is taller than 6 feet" or "y has brown hair and blue eyes".) We identify two such formulas if for each $x \in X$ they are either both true or both false. Show that $\mathfrak{S}(X)$ is a Boolean algebra if we define meet, join and complement by

$$A \vee B \;:=\; A \text{ or } B\,, \quad A \wedge B \;:=\; A \text{ and } B\,, \quad \overline{A} \;:=\; \neg A \;:=\; \text{not } A\,.$$

(d) Let $\mathfrak{P}(X)$ be equipped with the structure of a Boolean algebra as in part (e) of problem 35. Define a mapping $\theta : \mathfrak{S}(X) \to \mathfrak{P}(X)$ by $\theta(A) := \{x \in X \mid \text{statement } A \text{ is true for element } x\}$. Show that θ is a bijection which respects the Boolean structures on $\mathfrak{P}(X)$ and $\mathfrak{S}(X)$.

3. Integral domains and fields

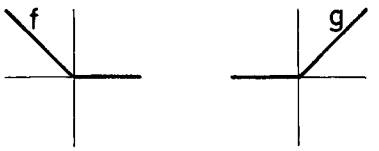
IT is clear that the arithmetic in an arbitrary ring can differ substantially from the well-known arithmetic in the ring of integers. One example is the possible non-commutativity of multiplication. But even in commutative rings unfamiliar phenomena can occur. We will point out these phenomena and then define a class of rings in which they cannot occur. These rings then resemble the integers much more than arbitrary rings which has the consequence that a reasonable theory of divisibility can be established. Let us start by considering special elements that can occur in a ring.

(3.1) Definitions. *Let R be a ring.*

(a) *An element $r \neq 0$ in R is called a* **zero-divisor** *if there is an element $s \neq 0$ such that $rs = 0$ or $sr = 0$.*

(b) *An element $r \in R$ is called* **nilpotent** *if $r^n = 0$ for some $n \geq 1$; clearly, a nonzero nilpotent element is a zero-divisor.*

(3.2) Examples. (a) In $C[-1,1]$, the two functions f and g sketched below are zero-divisors because $f \neq 0$, $g \neq 0$, but $fg = 0$. However, the ring $C[-1,1]$ possesses no nilpotent elements other than 0; if f^n is the zero-function for some $n \geq 1$ then f itself must be the zero-function.



(b) Let $R \neq \{0\}$ be an arbitrary ring. Pick an element $a \neq 0$ in R. Then

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{but} \quad \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{in } R^{2\times 2}.$$

Hence the ring $R^{2\times 2}$ possesses nonzero nilpotent elements.

(c) Suppose m is not divisible by n, but that m and n have a proper common factor a. Then $[m]$ is a zero-divisor in $\mathbb{Z}_n$. Indeed, let $m = xa$ and $n = ya$ where y is a proper factor of n. Then $[m] \neq [0]$ and $[y] \neq [0]$ in $\mathbb{Z}_n$, but $[m]\cdot[y] = [my] = [nx] = [0]$.

(d) Every direct product of two nonzero rings R and S has zero-divisors. In fact, if $r \in R \setminus \{0\}$ and $s \in S \setminus \{0\}$ then $(r,0)(0,s) = (0,0)$.

(e) The sum of two commuting nilpotent elements x and y in a ring is nilpotent again. In fact, if $x^m = 0$ and $y^n = 0$ then

$$(x+y)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} \underbrace{x^k}_{\substack{=0 \text{ if} \\ k \geq m}} \underbrace{y^{m+n-1-k}}_{\substack{=0 \text{ if} \\ k < m}} = 0 .$$

(f) Let R be a commutative ring. Then a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is nilpotent in $R[x]$ if and only if the coefficients $a_0, \ldots, a_n$ are nilpotent in R. In fact, if $a_0, \ldots, a_n$ are nilpotent in R then the polynomials $f_i(x) := a_ix^i$ are clearly nilpotent in $R[x]$, and hence $f = f_0 + f_1 + \cdots + f_n$ is nilpotent as a sum of commuting nilpotent elements. Let us show conversely by induction on n that if $a_0 + a_1x + \cdots + a_nx^n$ is nilpotent in $R[x]$ then $a_0, \ldots, a_n$ are nilpotent in R. If $f^N = 0$ then $a_0^N = 0$ because a_0^N is the first coefficient of f^N; this shows that a_0 is nilpotent. Let $g(x) := a_1 + a_2x + \cdots + a_nx^{n-1}$; then $xg(x) = f(x) + (-a_0)$ is nilpotent as the sum of two commuting nilpotent elements which entails that g is nilpotent. But then $a_1, \ldots, a_n$ are nilpotent by induction hypothesis.

LET us see what it means for a ring to be free of zero-divisors.

(3.3) Proposition. *Let R be a ring. Then the following conditions are equivalent.*
(a) *R has no zero-divisors.*
(b) *The following* **cancellation rules** *hold:*

$$ax = ay,\ a \neq 0 \implies x = y\ ; \qquad xa = ya,\ a \neq 0 \implies x = y\ .$$

(c) *For any given elements $a \in R \setminus \{0\}$ and $b \in R$ each of the equations $ax = b$ and $ya = b$ has at most one solution x or y.*

Proof. Clearly, (c) is simply a restatement of (b); hence it is enough to show the equivalence of (a) and (b). Suppose (a) holds. Then if $a \neq 0$ and $ax = ay$ or $xa = ya$, i.e., $a(x - y) = 0$ or $(x - y)a = 0$, we must have $x = y$; otherwise a and $x - y$ would be zero-divisors. Suppose conversely that (b) holds, but that nevertheless $ab = 0$ with $a \neq 0$ and $b \neq 0$. Then the equation $ax = 0$ has two solutions, namely $x = 0$ and $x = b$, contradicting (b). ∎

(3.4) Proposition. *Let R be a ring with identity and let $n := \operatorname{char} R$ be its characteristic. If R has no zero-divisors then n is zero or a prime number.*

Proof. Suppose that $n = n_1n_2$ is a composite number. Using the fact that $m \mapsto m \cdot 1$ is a ring homomorphism from $\mathbb{Z}$ into R, we have $0 = (n_1n_2) \cdot 1 = (n_1 \cdot 1)(n_2 \cdot 1)$. The assumption that R has no zero-divisors implies that $n_1 \cdot 1 = 0$ or $n_2 \cdot 1 = 0$ contradicting the fact that n is the *smallest* number k with $k \cdot 1 = 0$. ∎

IN a ring with identity there is another special class of elements, namely those which possess an inverse.

(3.5) Definition. *Let R be a ring with identity element* 1. *An element $r \in R$ is called* **invertible** *or a* **unit** *in R if there is an element $s \in R$ such that $rs = sr = 1$.*† *This element s is uniquely determined*†† *and denoted by $s = r^{-1}$. It is easy to check that*

$$R^\times := \{r \in R \mid r \text{ is invertible}\}$$

is a group under multiplication; it is called the **group of units** *of R.*

(3.6) Examples. (a) Clearly,

$$\boxed{\mathbb{Z}^\times = \{1, -1\}\,.}$$

(b) For all $n \in \mathbb{N}$ we have

$$\boxed{\mathbb{Z}_n^\times = \{[m] \mid m \text{ is coprime with } n\}\,.}$$

Here the inclusion $\subseteq$ is clear because of (3.2)(c) since a zero-divisor cannot be a unit. The converse inclusion was established in (I.20.14).

(c) Let $R = \mathbb{Z} + \mathbb{Z}\sqrt{n}$ where $n \in \mathbb{Z} \setminus \{0, 1\}$ is square-free. To find the units of R we introduce the **norm** $N : \mathbb{Q} + \mathbb{Q}\sqrt{n} \to \mathbb{Q} + \mathbb{Q}\sqrt{n}$ by

$$N(x + y\sqrt{n}) := x^2 - ny^2\,;$$

note that if $x, y \in \mathbb{Z}$ then $N(x + y\sqrt{n}) \in \mathbb{Z}$. If we define the **conjugation mapping** of $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ by $\overline{x + y\sqrt{n}} := x - y\sqrt{n}$, we can write

$$N(a) = a\overline{a}\,.$$

Note that $\overline{a + b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\,\overline{b}$ so that

$$N(ab) = ab\overline{ab} = ab\overline{a}\,\overline{b} = a\overline{a}b\overline{b} = N(a)N(b)\,.$$

Now we are ready to show that

$$\boxed{\begin{aligned}(\mathbb{Z} + \mathbb{Z}\sqrt{n})^\times &= \{x + y\sqrt{n} \mid x, y \in \mathbb{Z},\, x^2 - ny^2 = \pm 1\} \\ &= \{a \in \mathbb{Z} + \mathbb{Z}\sqrt{n} \mid N(a) = \pm 1\}\,.\end{aligned}}$$

Indeed, if $a \in R$ is a unit then there is an element $b \in R$ with $ab = 1$ which implies $1 = N(1) = N(ab) = N(a)N(b)$. Since $N(a)$ and $N(b)$ are integers, this is only possible if $N(a) = N(b) = \pm 1$. Suppose conversely that $N(a) = \pm 1$, i.e., $a\overline{a} = \pm 1$. Then clearly $\pm\overline{a}$ is an inverse of a.

---

† Equivalently, we could define r to be a unit if there are elements $s_1, s_2 \in R$ such that $s_1 r = r s_2 = 1$ for then s_1 and s_2 have to be equal. Indeed, $s_1 = s_1 \cdot 1 = s_1(rs_2) = (s_1 r)s_2 = 1 \cdot s_2 = s_2$.

†† If s and s' are inverse to r, then $s = s \cdot 1 = s(rs') = (sr)s' = 1 \cdot s' = s'$.

(d) Let R be a commutative ring with 1. As in (I.7.5) we can introduce the determinant $\det : R^{n\times n} \to R$. Then

$$\boxed{(R^{n\times n})^\times = \{A \in R^{n\times n} \mid \det A \in R^\times\}\,.}$$

For example, a matrix with integer entries has an inverse with integer entries if and only if its determinant is ± 1.

To prove this claim, assume first that $A \in (R^{n\times n})^\times$. Then there is a matrix $B \in R^{n\times n}$ such that $AB = BA = 1$. But this implies $(\det A)(\det B) = (\det B)(\det A) = 1$ so that $\det A \in R^\times$. Suppose conversely that $\det A \in R^\times$. Then Cramer's rule gives $A(\operatorname{adj} A) = (\operatorname{adj} A)A = (\det A)1$ so that $(\det A)^{-1}(\operatorname{adj} A)$ is inverse to A.

(e) Let R be a ring with 1 which has no zero-divisors. Then

$$\boxed{R[x]^\times = R^\times}$$

where we consider R as a subring of $R[x]$. To check this claim, suppose first that $r \in R^\times$. Let $s = r^{-1}$ in R. Then s (considered as a constant polynomial) is also inverse to r in $R[x]$. Conversely, let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]^\times$ with $a_n \neq 0$ and let $g(x) = b_0 + b_1x + \cdots + b_mx^m$ be the inverse of f where $b_m \neq 0$. Then

$$1 = f(x)g(x) = a_0b_0 + \cdots + a_nb_m\,x^{n+m}$$

where $a_nb_m \neq 0$ because R has no zero-divisors. We conclude that $n = m = 0$ and $a_0b_0 = 1$. Also, $1 = g(x)f(x) = b_0a_0$ so that $b_0 = a_0^{-1}$.

(f) Let R be a commutative ring with identity. Then

$$\boxed{R[x]^\times = \{a_0 + a_1x + \cdots + a_nx^n \mid a_0 \in R^\times,\, a_1, \ldots, a_n \text{ nilpotent in } R\}\,.}$$

Let us show the inclusion $\supseteq$ first. If $a_0 \in R^\times$ and if $a_1, \ldots, a_n$ are nilpotent then $g(x) := a_1x + \cdots + a_nx^n$ is nilpotent by (3.2)(f); hence $f(x) = a_0 + g(x)$ is a sum of a unit and a nilpotent element and therefore a unit. (See problem 3 below.) Let us now prove the converse inclusion $\subseteq$. If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is a unit in $R[x]$ then clearly a_0 is a unit in R; without loss of generality we may assume that $a_0 = 1$. Letting $g(x) := -(a_1 + a_2x + \cdots + a_nx^{n-1})$ we have $f(x) = 1 - xg(x)$, and the inverse of f can be written in the form $1 + xh(x)$. Then $1 = \big(1 - xg(x)\big)\big(1 + xh(x)\big) = 1 - xg(x) + xh(x) - x^2g(x)h(x)$ which implies that $h = g + xgh$. Substituting the left-hand side of this equation into the right-hand side we find that $h = g + xg(g + xgh) = g + xg^2 + x^2g^2h$. Repeating this substitution we find that

$$h = g + xg^2 + x^2g^3 + \cdots + x^{N-1}g^N + x^Ng^Nh$$

for all $N \in \mathbb{N}$. If we had $g^N \neq 0$ for all N this would produce arbitrarily high powers of x on the right-hand side which is, of course, impossible. Thus g is nilpotent so that $f(x) = a_0 + xg(x)$ is a sum of a unit and a nilpotent element and hence is a unit.

(g) Let R be a ring with 1. Then

$$\boxed{R[[x]]^\times = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots \mid a_0 \in R^\times\}\,.}$$

Let us prove this claim. If $f(x) = \sum_{k=0}^{\infty} a_k x^k$ has an inverse $g(x) = \sum_{k=0}^{\infty} b_k x^k$, then $1 = f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots$ and $1 = g(x)f(x) = b_0a_0 + (b_0a_1 + b_1a_0)x + \cdots$. This implies $a_0b_0 = b_0a_0 = 1$ so that $a_0 \in R^\times$. Conversely, let $a_0 \in R^\times$. The power series $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ satisfies $fg = 1$ if and only if

$$a_0b_0 = 1, \quad a_0b_1 + a_1b_0 = 0, \quad \ldots, \quad a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = 0, \quad \ldots$$

But the fact that a_0^{-1} exists allows us to solve these equations successively for b_0, b_1, b_2 and so on; this shows that $g \in R[[x]]$ with $fg = 1$ exists. Similarly, we find $h \in R[[x]]$ with $hf = 1$. But then $h = h \cdot 1 = h(fg) = (hf)g = 1 \cdot g = g$ so that $g = f^{-1}$.

(h) Let $\mathbb{H}$ be the ring of quaternions. Then

$$\boxed{\mathbb{H}^\times = \mathbb{H} \setminus \{0\}}$$

which means that every nonzero quaternion is invertible. This follows easily from the identity

$$\det \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = |a|^2 + |b|^2 .$$

(i) Let $\operatorname{End} A$ be the endomorphism ring of the abelian group $(A, +)$ as defined in (2.11). Then

$$\boxed{(\operatorname{End} A)^\times = \operatorname{Aut} A}$$

where $\operatorname{Aut} A$ denotes the automorphism group of A.

LET us study in some more detail the units of the rings $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ since these rings are of considerable importance in number theory. In fact, the determination of the units is essentially a number-theoretical problem. This determination is very easy if $n < 0$, but for positive values of n we need the following non-trivial result.

(3.7) Theorem. *Let $n \in \mathbb{N}$ be a natural number which is not a square.*

(a) *For any given $c \in \mathbb{N}$ there are $x, y \in \mathbb{N}$ with $0 < |x - y\sqrt{n}| < 1/c \leq 1/y$.*

(b) *There are infinitely many pairs $(x, y) \in \mathbb{N}^2$ such that $0 < |x - y\sqrt{n}| < \frac{1}{y}$; each such pair satisfies $|x^2 - ny^2| < 1 + 2\sqrt{n}$.*

(c) *The equation $x^2 - ny^2 = 1$* **(Pell's equation)**† *has a nontrivial solution $(x, y) \neq (1, 0)$ in $\mathbb{N}^2$.*

Proof. (a) For any $x \in \mathbb{R}$ we denote by $[x]$ the largest integer smaller than x. Given $c \in \mathbb{N}$, the numbers $k\sqrt{n} - [k\sqrt{n}]$ $(0 \leq k \leq c)$ are irrational except for $k = 0$; hence each of these numbers lies in one of the intervals $[0, \frac{1}{c}), (\frac{1}{c}, \frac{2}{c}), (\frac{2}{c}, \frac{3}{c}), \ldots, (\frac{c-1}{c}, 1)$. Since we have $c+1$ possibilities for k, but only c intervals, there are at least two different values $k_1 < k_2$ for k such that both $k_1\sqrt{n} - [k_1\sqrt{n}]$ and $k_2\sqrt{n} - [k_2\sqrt{n}]$ lie in the same interval. Then

$$\begin{aligned} \frac{1}{c} &> |(k_2\sqrt{n} - [k_2\sqrt{n}]) - (k_1\sqrt{n} - [k_1\sqrt{n}])| \\ &= |(\underbrace{k_2 - k_1}_{=: y \in \mathbb{N}})\sqrt{n} - (\underbrace{[k_2\sqrt{n}] - [k_1\sqrt{n}]}_{=: x \in \mathbb{N}})| = |x - y\sqrt{n}| ; \end{aligned}$$

† Named after John Pell (1611-1685).

Note that $x > 0$ because $n \geq 2$. Since $0 < y = k_2 - k_1 \leq k_2 \leq c$ we have $1/c \leq 1/y$ so that the desired inequality holds.

(b) Choose $c_1 \in \mathbb{N}$ and then $x_1, y_1 \in \mathbb{N}$ such that $0 < |x_1 - y_1\sqrt{n}| < 1/c_1 \leq 1/y_1$ as in (a). Then pick $c_2 \in \mathbb{N}$ so large that $1/c_2 < |x_1 - y_1\sqrt{n}|$ and choose x_2, y_2 according to part (a). Continuing in this fashion, we obtain an infinite sequence

$$\frac{1}{c_1} > |x_1 - y_1\sqrt{n}| > \frac{1}{c_2} > |x_2 - y_2\sqrt{n}| > \frac{1}{c_3} > |x_3 - y_3\sqrt{n}| > \cdots$$

where the pairs (x_i, y_i) have the desired property. Furthermore, if $|x - y\sqrt{n}| < 1/y$ then $|x + y\sqrt{n}| \leq |x - y\sqrt{n}| + |2y\sqrt{n}| < (1/y) + 2y\sqrt{n}$ by the triangle inequality and hence

$$|x^2 - ny^2| = |x - y\sqrt{n}|\,|x + y\sqrt{n}| < \frac{1}{y}\left(\frac{1}{y} + 2y\sqrt{n}\right) = \frac{1}{y^2} + 2\sqrt{n} \leq 1 + 2\sqrt{n}\,.$$

(c) Due to (b), there must be a natural number $r < 1 + 2\sqrt{n}$ which has an infinite number of representations as $r = |x^2 - ny^2|$ with $x, y \in \mathbb{N}$. Hence for at least one number $\varepsilon \in \{\pm 1\}$ there are infinitely many pairs (x, y) with $x^2 - ny^2 = \varepsilon r$. Since there is only a finite number of remainders modulo r, we can find two different solutions (x_1, y_1) and (x_2, y_2) such that $x_1 \equiv x_2$ and $y_1 \equiv y_2$ modulo r. Then

$$\alpha := \frac{x_1x_2 - ny_1y_2}{r} \in \mathbb{Z} \quad \text{and} \quad \beta := \frac{x_2y_1 - x_1y_2}{r} \in \mathbb{Z}$$

satisfy

$$(1)\quad (x_1 + y_1\sqrt{n})(x_2 - y_2\sqrt{n}) = (x_1x_2 - ny_1y_2) + (y_1x_2 - x_1y_2)\sqrt{n} = r(\alpha + \beta\sqrt{n})\,.$$

We apply the conjugation mapping $z \mapsto \overline{z}$ of $\mathbb{Q} + \mathbb{Q}\sqrt{n}$ to this equation and obtain

$$(2)\qquad (x_1 - y_1\sqrt{n})(x_2 + y_2\sqrt{n}) = r(\alpha - \beta\sqrt{n})\,.$$

Multiplying (1) and (2), we obtain

$$r^2(\alpha^2 - n\beta^2) = (x_1^2 - ny_1^2)(x_2^2 - ny_2^2) = (\varepsilon r)(\varepsilon r) = \varepsilon^2 r^2 = r^2$$

so that $\alpha^2 - n\beta^2 = 1$. This shows that $(|\alpha|, |\beta|)$ is a solution of Pell's equation. It remains to show that it is not the trivial solution. Suppose $\beta = 0$; then $x_1/x_2 = y_1/y_2 =: \kappa > 0$ so that $\varepsilon r = x_1^2 - ny_1^2 = \kappa^2(x_2^2 - ny_2^2) = \kappa^2\varepsilon r$ which implies $\kappa^2 = 1$, hence $\kappa = 1$ contradicting the fact that $(x_1, y_1) \neq (x_2, y_2)$. This contradiction shows that $\beta \neq 0$ so that we have indeed found a nontrivial solution. ∎

(3.8) Theorem. *Let $n \in \mathbb{Z} \setminus \{0, 1\}$ be a square-free number.*

(a) *Suppose $n < 0$. Then $(\mathbb{Z} + \mathbb{Z}\sqrt{n})^\times = \{\pm 1\}$ for all $n \geq -2$ whereas $(\mathbb{Z} + i\mathbb{Z})^\times = \{\pm 1, \pm i\}$ for $n = -1$.*

(b) *Suppose $n > 0$ so that $\mathbb{Z} + \mathbb{Z}\sqrt{n} \subseteq \mathbb{R}$. There is a smallest unit u of $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ which is larger than 1, called the* **basis unit** *of $\mathbb{Z} + \mathbb{Z}\sqrt{n}$, and we have*

$$(\mathbb{Z} + \mathbb{Z}\sqrt{n})^\times = \{\pm u^m \mid m \in \mathbb{Z}\}\,.$$

Proof. (a) The norm of an element $z = x+y\sqrt{n}$ is $N(z) = x^2-ny^2 = x^2+|n|y^2 \geq 0$; hence z is a unit if and only if $1 = |N(z)| = N(z) = x^2 + |n|y^2$. For $n = -1$ this equation reads $x^2 + y^2 = 1$ so that the solutions in $\mathbb{Z}^2$ are $(\pm 1, 0)$ and $(0, \pm 1)$. For $|n| \geq 2$, the only solutions of $x^2 + |n|y^2 = 1$ in $\mathbb{Z}^2$ are obviously $(\pm 1, 0)$.

(b) Multiplication by -1 switches positive and negative units, and the inversion map $z \mapsto \frac{1}{z}$ switches the sets of units with $|z| > 1$ and $|z| < 1$, respectively. Hence all units of $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ other than ± 1 are of the form $\pm z$ or $\pm z^{-1}$ where z is a unit with $z > 1$. Now (3.7)(c) guarantees the existence of a unit $z = x + y\sqrt{n}$ with $x, y \in \mathbb{N}$ and hence $z \geq 1 + \sqrt{n} > 1$. † Since $\mathbb{N}$ is discrete, there is clearly a smallest unit u with $u > 1$. Obviously, all powers u^m with $m \in \mathbb{N}$ are again units larger than 1. It remains to show that these powers exhaust the set of units larger than 1. Suppose there is a unit $z > 1$ which is not a power of u. Then there is an exponent M with $u^M < z < u^{M+1}$. Multiplying this inequality by $u^{-M} > 0$, we obtain $1 < zu^{-M} < u$ so that zu^{-M} is a unit lying strictly between 1 and u. This clearly contradicts the choice of u. ∎

SINCE the general notion of a ring is an abstraction of the ring of integers, we can try to carry over the well-known notions of divisibility in $\mathbb{Z}$ to an arbitrary ring R. We could simply define that an element $a \in R$ be a divisor of an element $b \in R$ if there is an element $x \in R$ with $ax = b$. However, if the multiplication is not commutative, this does not imply that also $xa = b$. Hence we will restrict our attention to commutative rings. In $\mathbb{Z}$ we have the notion of the greatest common factor of given numbers. For example, $\gcd(12, 18, 30) = 6$ because 6 is the largest number dividing 12, 18 and 30 simultaneously. The word 'largest' only has meaning in a ring which possesses an ordering of its elements. Let us try to characterize greatest common divisors in a way that does not refer to the ordering given on $\mathbb{Z}$. For example, the common divisors of 12, 18 and 30 are $\pm 1, \pm 2, \pm 3, \pm 6$, and the number 6 has the property that it is divisible by all of these. This is a characterization we can use to define a greatest common divisor in arbitrary domains. To define least common multiples, we proceed similarly.

(3.9) Definitions. *Let R be a commutative ring and let $a, b, a_1, \ldots, a_n$ be elements of R.*

(a) *We say that a divides b and write $a \mid b$ if there is an element $r \in R$ such that $b = ra$. Equivalently, we say that b is* **divisible** *by a and call a a* **divisor** *or a* **factor** *of b. (If R has no zero-divisors such an element r is uniquely determined, and we write $r = b/a$.)*

(b) *We call $d \in R$ a* **common divisor** *of $a_1, \ldots, a_n$ if $d \mid a_k$ for $1 \leq k \leq n$.*

(c) *An element $d \in R$ is called a* **greatest common divisor** *(gcd) of $a_1, \ldots, a_n$ if d is a common divisor of $a_1, \ldots, a_n$ and if any other common divisor d' of $a_1, \ldots, a_n$ divides d.*

(d) *We call $m \in R$ a* **common multiple** *of $a_1, \ldots, a_n$ if $a_k \mid m$ for $1 \leq k \leq n$.*

(e) *An element $m \in R$ is called a* **least common multiple** *(lcm) of $a_1, \ldots, a_n$ if m is a common multiple of $a_1, \ldots, a_n$ and if any other common multiple m' of $a_1, \ldots, a_n$ is a multiple of m.*

---

† Since we studied the equation $x^2 - ny^2 = +1$ in (3.7), we even have $N(z) = 1$, but it may well happen that a unit $z > 1$ satisfies $N(z) = -1$; for example, take $z = 1+\sqrt{2}$ in $\mathbb{Z} + \mathbb{Z}\sqrt{2}$.

NOTE that two elements in a commutative ring do not necessarily possess a greatest common divisor or a least common multiple. For example, in the ring $R = 2\mathbb{Z}$ of all even integers, the element 6 has no divisors at all in R. It becomes clear at this point that even though we could *define* the basic notions of divisibility in an arbitrary commutative ring, we will have to specialize to a more restricted class of rings to obtain a reasonable theory. For example, if R is a ring without an identity element it is not even true in general that $a \mid a$ for all $a \in R$, and if we allow rings without identity it is not clear how to define that two elements are relatively prime. Also, if R has zero-divisors, we might find that there are two different elements $x_1 \neq x_2$ which satisfy the equation $ax = b$, and it does not make sense to talk about the quotient a/b if a is divisible by b. This is why we now introduce a class of rings which share three characteristic features with the ring of integers; namely commutativity, the existence of an identity element and the absence of zero-divisors; and are thus similar enough to the ring of integers to allow the development of a reasonable theory of divisibility. In fact, one calls these rings integral domains to express their similarity to the ring of integers.

(3.10) Definition. *An* **integral domain** *is a commutative ring with identity which has no zero-divisors.*

(3.11) Examples. (a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all integral domains.

(b) If R is an integral domain and $U \leq R$ a subring with $1 \in U$ then U is itself an integral domain. For example, $\mathbb{Z}[\sqrt{2}] \leq \mathbb{C}$ is an integral domain.

(c) $\mathbb{Z}_n$ is an integral domain if and only if n is a prime number.

(d) If R is an integral domain, then so are the polynomial ring $R[x]$ and the power series ring $R[[x]]$. (See problem 28 below.)

EVEN in an integral domain not all the usual facts known about the integers are true; for example, it is still possible that two elements do not possess a greatest common divisor or a least common multiple.

(3.12) Example. The elements 6 and $2+2\sqrt{-5}$ have neither a greatest common divisor nor a least common multiple in the integral domain $\mathbb{Z}[\sqrt{-5}]$.

Indeed, suppose $a+b\sqrt{-5}$ is a common divisor of 6 and $2+2\sqrt{-5}$. Taking norms, we see that a^2+5b^2 is a common divisor of 36 and 24 in $\mathbb{Z}$. Consequently, $a^2+5b^2 \mid 12$ which only leaves the possibilities $(\pm 1, 0)$, $(\pm 2, 0)$ and $(\pm 1, \pm 1)$ for (a, b). Since $\pm(1-\sqrt{-5})$ are not divisors of $1+\sqrt{-5}$, the common divisors of 6 and $2+2\sqrt{-5}$ are the six elements ± 1, ± 2 and $\pm(1+\sqrt{-5})$. It is easy to see that none of these is divisible by all the others; hence there is no greatest common divisor.

Furthermore, suppose that 6 and $2+2\sqrt{-5}$ possess a least common multiple $a+b\sqrt{-5}$. Then a^2+5b^2 is a common multiple of 36 and 24, hence a multiple of 12. On the other hand, $a+b\sqrt{-5}$ divides every common multiple of 6 and $2+2\sqrt{-5}$ so that for example $a+b\sqrt{-5}$ divides 12 and $6(1+\sqrt{-5})$. But this implies that a^2+5b^2 divides 144 and 216, hence divides 72. The two conditions together show that $a^2+5b^2 = 12, 24, 36$ or 72. This leaves for (a, b) the possibilities $(\pm 2, \pm 2), (\pm 4, \pm 2)$ and $(\pm 6, \pm 0)$. Now 6 is not divisible by $2+2\sqrt{-5}$, and $2 \pm 2\sqrt{-5}$ and $4 \pm 2\sqrt{-5}$ are not divisible by 6. So the assumption that $a+b\sqrt{-5}$ is a least common multiple of 6 and $2+2\sqrt{-5}$ leads to a contradiction.