UNIVERSITY OF PRIMORSKA
FACULTY OF MATHEMATICS, INFORMATICS AND NATURAL SCIENCES

Exercises and Solutions in Rings and Fields

Notebook for Algebra IV – Algebraic structures

Amar Bapić

OTHER STUDY TEXTBOOK
PAGES 78

Mathematics, 1st Bologna cycle

1st edition

Koper, 2021

Contents

Preface

In front of you is a collection of solved problems and exercises covered in the course **Algebra IV - Algebraic Structures**, intended for students of the study program Mathematics at UP FAMNIT. I hope you find this notebook useful, though it is definitely not meant to be a substitute for tutorials and lectures, where things are explained in more detail and more comprehensively.

The content and assignments are in line with the curriculum. The topics that are covered include: rings, fraction fields, factorisation of polynomials over fields, integral domains, ideals, factor rings, extension fields, finite fields, field automorphisms.

The solutions are written as accurately and precisely as possible. In addition, every section contains a theoretical background and additional tasks that are left as an exercise for the reader.

Koper, August 2021

Amar Bapić
amar.bapic@famnit.upr.si

1. Rings

1.1 Introduction to Rings

1.1.1 Theoretical background

Definition 1.1.1 A **ring** $(R,+,\cdot)$ is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms hold:

(R1) $(R,+)$ is an abelian group.

(R2) Multiplication is associative.

(R3) For all $a,b,c \in R$ it holds

$$(a+b)\cdot c = a\cdot c + b\cdot c \text{ and } c\cdot(a+b) = c\cdot a + c\cdot a.$$

We denote the neutral element for addition with 0 or 0_R (if it is not clear from context). If the ring R has a neutral element for multiplication, we will call it the **unity** and denote it with 1 or 1_R. In this case we say that R is a **ring with unity**. If multiplication is commutative in R, then R is a **commutative ring**. The additive inverse of $a \in R$ is denoted with $-a$. We define na to be

$$na = \begin{cases} a+a+\ldots+a, & n>0 \\ 0_R, & n=0\ (0_R \in R,\ 0 \in \mathbb{Z}) \\ (-a)+(-a)+\ldots+(-a), & n<0 \end{cases}$$

The multiplicative inverse of an element a in a ring R with unity $1 \neq 0$ is the element $a^{-1} \in R$, for which it holds that $aa^{-1} = a^{-1}a = q$. In this case, we say that a is a **unit**.

If in a ring R with unity $1 \neq 0$ all nonzero elements are units, then we say that R is a **division ring**. Furthermore, if a division ring is commutative, we call it a **field**.

Definition 1.1.2 A subset S of a ring R is a **subring** of $(R,+,\cdot)$, if $(S,+,\cdot)$ is a ring.

Theorem 1.1.1 The subset $S \subset R$ of a ring R is a subring of R if and only if:

1. $0_R \in S$,
2. $(a-b) \in S$, $\forall a,b \in S$,
3. $ab \in S$, $\forall a,b \in S$.

Theorem 1.1.2 Let R be a ring with zero 0. Then, for all $a,b \in R$, it holds:

(i) $0a = a0 = 0$.

(ii) $a(-b) = (-a)b = -(ab)$.

(iii) $(-a)(-b) = ab$

Definition 1.1.3 Let $(K,+_K,\cdot_K)$ in $(R,+_R,\cdot_R)$ be two rings. The mapping $\phi : K \to R$ is called a **homomorphism**, if for all $a,b \in K$ it holds:

1. $\phi(a +_K b) = \phi(a) +_R \phi(b)$.
2. $\phi(a \cdot_K b) = \phi(a) \cdot_R \phi(b)$.

We define the **kernel** of ϕ to be the set

$$\ker\phi = \{x \in K : \phi(x) = 0_R\},$$

and the **image** of ϕ to be

$$\mathrm{im}\phi = \{\phi(x) : x \in K\}.$$

Theorem 1.1.3 Let $\phi : R \to R'$ be a ring homomorphism. If 0 is the additive identity in R, then $\phi(0) = 0'$ is the additive identity in R', if $a \in R$, then $\phi(-a) = -\phi(a)$. If S is a subring of R, then $\phi[S] = \{\phi(s) : s \in S\}$ is a subring of R'. If R has a unity 1, then $\phi(1)$ is the unity in $\phi[R]$.

R $\phi(1)$ is not necessarily the unity in R'.

■ **Example 1.1** Let $R_1, R_2, \ldots, R_n$ be rings. For an arbitrary $i \in \{1,\ldots,n\}$ we define a mapping $\pi_i : R_1 \times R_2 \times \ldots \times R_n \to R_i$ with $\pi_i(x_1,x_2,\ldots,x_n) = x_i$ which we call the projective homomorphism. ■

1.1.2 Problems

1. Let X be a nonempty set and $R = 2^X$ its power set. Is $(R,\cup,\cap)$ a ring?
2. Let X be a nonempty set. Show that the power set $R = 2^X$, together with the set operations of symmetric difference $A+B := A\triangle B = (A\cap\overline{B})\cup(B\cap\overline{A})$ and intersection $AB = A\cap B$, is a ring. Is R commutative? Does it have a unity?
3. Let $(G,+)$ be an abelian group. In G we define the product $ab = 0$ for all $a,b \in G$. Show that G is a ring.
4. In the ring $R = \mathbb{R}^{2\times 2}$ we are given the subset M of all matrices of the form $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$.

   (a) Show that M is a subring of R.

(b) Is M commutative? Does it have a unity?

5. If it exists, find an example of a homomorphism $\phi : K \to K'$, where K and K' are rings with unity $1 \neq 0$ and $1' \neq 0'$, respectively. Furthermore, it holds $\phi(1) \neq 0'$ and $\phi(1) \neq 1'$.
6. Find all ring homomorphisms of the ring $\mathbb{Z}$ to $\mathbb{Z}$.
7. Find all ring homomorphisms of $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.
8. Let $(R, +, \cdot)$ be an algebraic structure that satisfies all the ring axioms except commutativity of addition. Show that if R has a unity, then R is a ring.
9. Show that the ring R does not contain a nonzero nilpotent[1] if and only if 0 is the only solution of the equation $x^2 = 0$ in R.
10. Show that every Boolean ring[2] is also von Neumann regular[3]. Is it commutative?
11. Let R be a ring without nonzero nilpotents. Then, for every idempotent $e \in R$ and every $x \in R$, it holds $xe = ex$.

1.1.3 Solutions

1. No, because $(K, \cup)$ is not a group. More precisely, for an arbitrary set $A \neq \emptyset$, there does not exist a set $\overline{A}$ such that $A \cup \overline{A} = \emptyset$.
2. Let $A, B, C \in R$ be arbitrary sets. The first thig one **always** has to check, is the **closure** of the operations of addition and multiplication. It is easy to see that $A + B$ and $A \cdot B$ are always contained in R.

(a) i. associativity of addition.

$$\begin{aligned}
A+(B+C) &= (A \cap \overline{B+C}) \cup (\overline{A} \cap (B+C)) \\
&= (A \cap \overline{(B \cap \overline{C}) \cup (\overline{B} \cap C)}) \cup (\overline{A} \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C))) \\
&= (A \cap (\overline{B} \cup C) \cap (B \cup \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \\
&= (A \cap \overline{B} \cap B) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap C \cap B) \cup \\
&\cup (A \cap C \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \\
&= (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)
\end{aligned}$$

Similarly, one computes that

$$(A+B)+C = (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C).$$

Thus, the operation is associative.

ii. existence of neutral element. Let A be an arbitrary set in R. Since

$$A + \emptyset = \emptyset + A = A,$$

we have that $\emptyset \in R$ is the additive identity.

[1] An element a of a ring R is called **nilpotent** if there exists a positive integer $n \in \mathbb{Z}^+$ such that $a^n = 0$.

[2] A ring R with unity is said to be **Boolean** if for all $a \in R$ we have $a^2 = a$. That is, every element is an **idempotent**.

[3] A nontrivial ring with unity R in which for every element $x \in R$ exists $y \in R$, such that $xyx = x$, is said to be **von Neumann regular**.

iii. existence of units. for an arbitrary set $A \in R$ there exists a set $\overline{A} = A$ such that

$$A + \overline{A} = \overline{A} + A = \emptyset.$$

iv. commutativity. Because of the commutativity of the operations $\cup$ and $\cap$, it holds

$$A + B = (A \cap \overline{B}) \cup (\overline{A} \cap B) = (B \cap \overline{A}) \cup (\overline{B} \cap A) = B + A.$$

Thus, $(R, +)$ is an abelian group.

(b) It is easy to see that

$$A \cdot (B \cdot C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cdot B) \cdot C$$

because of the associativity of $\cap$. Thus, $(R, \cdot)$ is a semigroup.

(c) distributivity laws.

$$\begin{aligned}
A \cdot (B + C) &= A \cap (B + C) = A \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C)) \\
&= (A \cap (B \cap \overline{C})) \cup (A \cap (\overline{B} \cap C)) \\
&= (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap C) \\
A \cdot B + A \cdot C &= (A \cap B) + (A \cap C) = ((A \cap B) \cap \overline{(A \cap C)}) \cup (\overline{(A \cap B)} \cap (A \cap C)) \\
&= ((A \cap B) \cap (\overline{A} \cup \overline{C}) \cup ((\overline{A} \cup \overline{B}) \cap (A \cap C)) \\
&= (A \cap B \cap \overline{A}) \cup (A \cap B \cap \overline{C}) \cup (\overline{A} \cap A \cap C) \cup (\overline{B} \cap A \cap C) \\
&= (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap C)
\end{aligned}$$

Thus, $A \cdot (B + C) = A \cdot B + B \cdot C$. Analogously, one shows that $(A + B) \cdot C = A \cdot C + B \cdot C$.

Hence, we conclude that $(R, +, \cdot)$ is a ring. Since $\cap$ is commutative, it follows that $A \cdot B = B \cdot A$. The ring R contains a unity $1 = X$, because for an arbitrary set $\emptyset \neq A \in K$ it holds $A \cdot X = X \cdot A = A$. Thus, R is a commutative ring with unity X.

3. We need to check if $(G, \cdot)$ is a semigroup and if the distributivity laws hold. Let $a, b, c \in G$ be arbitrary. Since $a \cdot b = 0 \in G$, the operation is closed. Associativity holds as well:

$$\begin{aligned}
a \cdot (b \cdot c) &= a \cdot 0 = 0, \\
(a \cdot b) \cdot c &= 0 \cdot c = 0.
\end{aligned}$$

Hence, $(G, \cdot)$ is a semigroup. One can easily confirm distributivity as well.

4. (a) We will use Theorem 1.1.2. The additive identity in the ring $R = \mathbb{R}^{2\times 2}$ is $O_R = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and obviously $O_R \in M$. Let $A, B \in M$ be arbitrary.

$$A - B = \begin{bmatrix} a & b \\ b & a \end{bmatrix} - \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} \underbrace{a-b}_{\in\mathbb{R}} & \underbrace{b-d}_{\in\mathbb{R}} \\ b-d & a-b \end{bmatrix} \in M$$

$$AB = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{bmatrix} \in M$$

Since all conditions of Theorem 1.1.2 are satisfied, we conclude that M is a subring of R with standard operations $+$ and $\cdot$ in $\mathbb{R}^{2\times 2}$.

(b) From the commutativity of $+$ and $\cdot$ in $\mathbb{R}$, one easily confirms that $A \cdot B = B \cdot A$. The ring M has unity $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Thus, M is a commutative ring with unity I_2.

5. Let us consider the mapping $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $\phi(n) = (n,0)$. One can easily show that ϕ is a ring homomorphism. The unity in $\mathbb{Z}$ is 1, in $\mathbb{Z} \times \mathbb{Z}$ it is $1' = (1,1)$ and it holds that $1 \neq 1'$. On the other hand, $\phi(1) = (1,0) \neq (1,1) = 1'$.
6. Ring homomorphisms preserve idempotents. Thus, since in $\mathbb{Z}$ it holds that $1^2 = 1$ we have $\phi(1)^2 = \phi(1)$. This implies that $\phi(1) = 1$ or $\phi(1) = 0$. Furthermore,

$$\phi(n) = \phi(n \cdot 1) = \phi(1 + 1 + \ldots + 1) = \phi(1) + \ldots + \phi(1) = n\phi(1)$$

and since $\phi(-n) = -\phi(n)$ we have that for every $n \in \mathbb{Z}$, $\phi(n) = 0$ or $\phi(n) = n$. This are the only homomorphisms, the trivial and identity homomorphism.
7. Since $(0,1)$ and $(1,0)$ generate the additive group $\mathbb{Z} \times \mathbb{Z}$, their images determine the seeked homomorphisms:

$$\begin{aligned} \varphi(m,n) &= \varphi(m(1,0) + n(0,1)) = \varphi(m(1,0)) + \varphi(n(0,1)) \\ &= \varphi(\underbrace{(1,0) + \ldots + (1,0)}_{m}) + \varphi(\underbrace{(0,1) + \ldots + (0,1)}_{n}) \\ &= \underbrace{\varphi(1,0) + \ldots + \varphi(1,0)}_{m} + \underbrace{\varphi(0,1) + \ldots + \varphi(0,1)}_{n} \\ &= m\varphi(1,0) + n\varphi(0,1). \end{aligned}$$

Since $(0,1)$ and $(1,0)$ are idempotents in $\mathbb{Z} \times \mathbb{Z}$, they have to map to 0 or 1. Thus:

$$\begin{aligned} \varphi_1(m,n) &= 0, \\ \varphi_2(m,n) &= m, \\ \varphi_3(m,n) &= n, \\ \varphi_4(m,n) &= m + n. \end{aligned}$$

We can easily confirm that φ_1, φ_2 in φ_3 are ring homomorphisms. Since

$$\varphi_4(m,n) = \varphi_4((1,1)(m,n)) = \varphi_4(1,1)\varphi_4(m,n) = (1+1)(m+n) = 2(m+n) = 2\varphi_4(m,n), \lightning$$

φ_4 is not a ring homomorphism.
8. Let $a, b \in R$ be arbitrary. Since R has unity 1, it holds:

$$0 = b \cdot 0 = b \cdot (1 + (-1)) = b \cdot 1 + b \cdot (-1) \Rightarrow b(-1) = -b.$$

On the other hand,

$$\begin{aligned} &0 = (-b) + (-a) + a + b = b(-1) + a(-1) + a + b = (b+a)(-1) + a + b \\ &\quad \Rightarrow a + b = -(b+a)(-1) \text{ in} \\ &0 = (b+a) \cdot 0 = (b+a) \cdot ((-1) + 1) = (b+a)(-1) + b + a \\ &\quad \Rightarrow b + a = -(b+a)(-1). \end{aligned}$$

Thus, $a + b = b + a$.

9. $\boxed{\Rightarrow}$ If R has no nonzero nilpotents, the only solution of the equation $x^2 = 0$ is $x = 0$. $\boxed{\Leftarrow}$ Let $x = 0$ be the only solution of the equation $x^2 = 0$ and let $a \neq 0$ be a nilpotent. With n we denote the smallest positive integer for which $a^n = 0$.If n is even, then

$$\underbrace{a^{\frac{n}{2}}}_{\text{not a nilpotent}} \neq 0 \Rightarrow a^n = \left(a^{\frac{n}{2}}\right)^2 = 0 \Rightarrow a^{\frac{n}{2}} \text{ is a nonzero solution of } x^2 = 0 \ ↯$$

If n is odd, then

$$a^{\frac{n+1}{2}} \neq 0 \Rightarrow \left(a^{\frac{n+1}{2}}\right)^2 = a^{n+1} = a^n a = 0a = 0 \Rightarrow a^{\frac{n+1}{2}} \text{ is a nonzero solution of } x^2 = 0 \ ↯$$

Torej, R has no nonzero nilpotents.

10. Let R be a Boolean ring and let $x \in R$ be arbitrary. If we take $y = x$ we have

$$xyx = x^3 = x^2 x = xx = x^2 = x,$$

thus R is von Neumann regular. Let $a, b \in R$ be arbitrary.

$$\begin{aligned} a + b = (a+b) &= a^2 + ab + ba + b^2 = a + ab + ba + b \\ &\Rightarrow a + b = a + b + ab + ba \ \ ((R,+) \text{ abelian group}) \\ &\Rightarrow 0 = ab + ba \ \ (\text{cancellation laws}) \\ &\Rightarrow ab = -ba \end{aligned}$$

For $b = a$ we have $aa = -aa \Rightarrow a^2 = -a^2 \Rightarrow a = -a$. Thus, every element in R is its own additive inverse. More precisely, since $ba \in R$ it follows $ba = -ba$. Thus, $ab = -ba = ba$.

11. Let us consider the elements $(xe - exe)^2$ and $(ex - exe)^2$.

$$\begin{aligned} (xe - exe)^2 &= (xe - exe)(xe - exe) \\ &= xexe - xe^2xe - exexe + exe^2xe \\ &= xexe - xexe - exexe + exexe \\ &= 0 \\ &\Rightarrow xe - exe = 0 \ \ (\text{Problem 9}) \end{aligned}$$

$$\begin{aligned} (ex - exe)^2 &= (ex - exe)(ex - exe) \\ &= exex - exexe - exe^2x + exe^2xe \\ &= exex - exexe - exex + exexe \\ &= 0 \\ &\Rightarrow ex - exe = 0 \ \ (\text{Problem 9}) \end{aligned}$$

Thus,

$$xe - exe = ex - exe \Rightarrow xe = ex.$$

1.1.4 Additional problems

1. Examine if the following sets are rings with respect to the defined binary operations:
   (a) $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $+$ and $\cdot$ are the usual addition and multiplication in $\mathbb{Q}$.
   (b) $R = \{(a,b) : a, b \in \mathbb{Z}\}$, $+$ and $\cdot$ are defined with
   $$(a,b) + (c,d) = (a+c, b+d),\ \ (a,b)\cdot(c,d) = (ac+bd, ad+bc).$$
   (c) The set of all vectors in the 3-dim Euclidean space with respect to vector addition and vector multiplication.
2. Prove that the set $\mathrm{End}(G)$ of all endomorphisms of the abelian group G is a ring with respect to addition and multiplication defined by
   $$(f+g)(a) = f(a) + g(a),\ \ (f\cdot g)(a) = f(g(a)),$$
   for $f, g \in \mathrm{End}(G)$.
3. Show that the ring of $n \times n$ matrices over some field F is von Neumann regular.
4. If a ring R has a unique left identity 1_l, prove that 1_l is then the identity (it should also be the right). Does it hold if we leave out the word “unique”?
5. * Let R be a finite ring of order $n > 1$, where n is a product of distinct primes. Prove that R is commutative.
6. Prove that for every prime p there exists a non-commutative ring of order p^2.
   Hint: Let $R = \{(x,y) : x, y = 0, 1, \ldots, p-1\}$. Addition is defined with $(x_1,x_2) + (y_1,y_2) = (x_1 +_p y_1, x_2 +_p y_2)$ and multiplication with $(x_1,x_2)\cdot(y_1,y_2) = (x_1 \cdot_p (y_1 +_p y_2), x_2 \cdot_p (y_1 +_p y_2))$. Show that $(R, +, \cdot)$ is a non-commutative ring of order p^2.
7. Let $\mathbb{Z}_n$ be the ring of integers modulo n (set of equivalence classes of integers modulo n), whose elements are denoted with $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. If $m, n > 1$ are coprime, prove that $\mathbb{Z}_{mn}$ contains at least two idempotents different from $\overline{0}$ and $\overline{1}$.
8. ** Let R be a ring in which $x^3 = x$ for all $x \in R$. Show that R is commutative.
   Hint: Pretty nasty proof (at least the one I have). The hint is that this is a special case of a certain theorem by N. Jacobson ☺.

1.2 Divisors of zero. Integral domains

1.2.1 Theoretical background

Definition 1.2.1 If $a, b \in R$ are nonzero elements for which
$$ab = 0,$$
we say that a is the **left divisor of zero**, and b the **right divisor of zero**. We point out that $0 \in R$ is not a divisor of zero.

Definition 1.2.2 A commutative ring with unity $1 \neq 0$ and no divisors of zero is called an **integral domain**.

Theorem 1.2.1

- In the ring $\mathbb{Z}_n$, the divisors of zero are all the elements which are not coprime with

n.

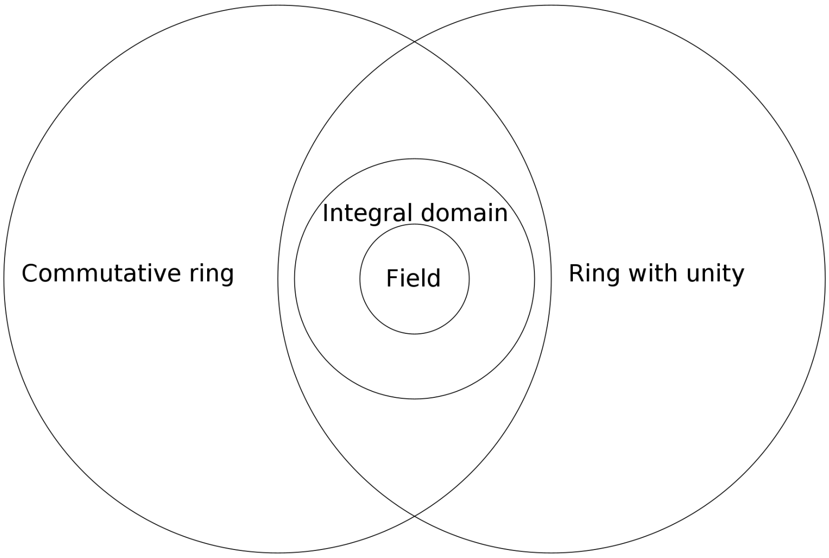
- If p is a prime, then $\mathbb{Z}_p$ has no divisors of zero.
- The cancellation laws hold in the ring R if and only if R has no divisors of zero.
- Every field F is an integral domain.
- Every finite integral domain is a field.

R Let $f : A \to B$ be a homomorphism.

f ENDOMORPHISM $\Leftrightarrow f$ surjection $\qquad$ f ISOMORPHISM $\Leftrightarrow f$ bijection

f MONOMORPHISM $\Leftrightarrow f$ injection $\qquad$ f AUTOMORPHISM $\Leftrightarrow f$ bijective and $B = A$

R



1.2.2 Problems

1. Is a divisor of zero a unit in a ring with unity?
2. Find some examples of divisors of zero in the rings $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}^{2\times 2}$. Are there rings without zero divisors?
3. Show that in a division ring there are exactly two idempotents.
4. If R is finite a ring with unity $1 \neq 0$ and with no zero divisors, then R is a division ring.
5. Let $R \neq 0$ be a finite ring. Show that R contains a right identity if and only if there exists a nonzero element in R which is not a divisor of zero.
6. Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. Are $\mathbb{R}$ and $\mathbb{C}$ isomorphic?
7. Let R be a ring with p elements, p prime. Prove that if R contains at least one nonzero product, then $R \cong (\mathbb{Z}_p, +, \cdot)$.
8. Let R be a ring in which $xy = \pm yx$ for all $x, y \in R$. Prove that exactly one of the following statements holds: R is commutative or $xy = -yx$, for all $x, y \in R$.

9. Let R be a finite ring such that at least one of its elements is not a divisor of zero. Prove:
   (a) R is a ring with unity.
   (b) If $b \in R$ does not have a multiplicative inverse, then b is a divisor of zero.

1.2.3 Solutions

1. Let R be a ring with unity $1 \neq 0$. Suppose that such elements exist. That is, $ab = 0$ for some $0 \neq a, b \in R$. If a is invertible, we can find an element $a^{-1} \in R$ such that $a^{-1}a = aa^{-1} = 1$. Hence,

$$a^{-1}a = 1 \Rightarrow (a^{-1}a)b = b \Rightarrow a^{-1}(ab) = b \Rightarrow 0 = b \lightning$$

2. In $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ only $\overline{2} \cdot \overline{2} = 2 \cdot 2 \mod 4 = 0$. Thus $\overline{2}$ is both the left and right divisor of zero. In $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ we have $\overline{2} \cdot \overline{3} = 2 \cdot 3 \mod 6 = 0$ and $\overline{3} \cdot \overline{4} = 3 \cdot 4 \mod 6 = 0$. In $\mathbb{Z}^{2\times 2}$ there are infinitely many divisors of zero. For $a, b \neq 0$ we have

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

The rings $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ have no divisors of zero.
Comment: There are infinite rings with divisors of zero. For example, let $X \neq \emptyset$. The ring $B = (2^X, \triangle, \cap)$ is a Boolean ring, ie, $A^2 = A$ for all $A \in 2^X$. If $A \neq \emptyset, X$, then A and $X \setminus A$ are divisors of zero. Let $R = B \times B \times \ldots \times B \times \ldots$ be a direct product of countably many copies of B. R is an infinite ring with zero divisors.

3. The obvious idempotents are 0 and 1. Suppose $a \neq 0, 1$ is an idempotent, ie, $a^2 = a$. Since we are in a division ring, a^{-1} exists and multiplying it with both sides we get $a = 1$. $\lightning$

4. We need to show that every $a \neq 0$ has an inverse a^{-1} such that $aa^{-1} = a^{-1}a = 1$. Since R is finite, WLOG we can write

$$R = \{0, 1, a_1, \ldots, a_n\}.$$

Let $a \neq 1$ be an arbitrary element in R. Let $S = aR$, that is,

$$S = \{0, a, aa_1, \ldots, aa_n\}.$$

We claim that all elements in S are pairwise distinct. Since there are no divisors of zero, the cancellation laws hold. So, if $aa_i = aa_j$, then $a_i = a_j$, which is not possible. Hence, it has to follow that

$$S = \{0, a, aa_1, \ldots, aa_n\} = \{0, 1, a_1, \ldots, a_n\} = R.$$

In other words, there exists some $a_i \in R$ such that $aa_i = 1$. Similarly, for taking $S = Ra$, we obtain that there is some a_j such that $a_j a = 1$. If an element has left and right inverse, they have to be equal. Thus, $aa_i = a_i a = 1$. Since a was arbitrary, the result follows.

5. $\boxed{\Rightarrow}$ Let $e \in R$ be the right identity in R, that is, $ae = a$ for all $a \in R$. Since $R \neq 0$ then $e \neq 0$. If $xe = 0$ we have that $x = 0$, thus e is not a right divisor of zero.

$\boxed{\Leftarrow}$ Suppose R contains an element $d \neq 0$, which is not a right divisor of zero. Thus,

$$ad \neq 0,\ \forall a \in R \setminus \{0\}.$$

We consider the map $f : R \to R$ defined by $f(x) = xd$. We claim that f is injective.

$$\begin{aligned} f(x) = f(y) &\Rightarrow xd = yd \\ &\Rightarrow xd - yd = 0 \\ &\Rightarrow (x-y)d = 0 \\ &\Rightarrow x - y = 0 \ \ (d \text{ is not a div. of zero}) \\ &\Rightarrow x = y \end{aligned}$$

Since R is finite and f injective, f is surjective. Thus, there exists such $x \in R$ for which $f(x) = d$. We will show that x is the right identity in R.

$$\begin{aligned} f(x) = d &\Rightarrow xd = d \\ &\Rightarrow y(xd) = yd,\ \forall y \in R \\ &\Rightarrow (yx)d - yd = 0,\ \forall y \in R \\ &\Rightarrow (yx - y)d = 0,\ \forall y \in R \\ &\Rightarrow yx - y = 0,\ \forall y \in R \\ &\Rightarrow yx = y,\ \forall y \in R \end{aligned}$$

6. If $f : 2\mathbb{Z} \to 3\mathbb{Z}$ is an isomorphism, from group theory, for the aditive groups $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ we know that either $f(2) = 3$ or $f(2) = -3$. Thus, the possible homomorphisms are $f(2n) = 3n$ or $f(2n) = -3n$.
   - $f(2n) = 3n$. For $n = 2$ we have $f(4) = 6$, but $f(2)f(2) = 9$.
   - $f(2n) = -3n$. For $n = 2$ we have $f(4) = -6$, but $f(2)f(2) = 9$.

   Thus, $(2\mathbb{Z}, +, \cdot) \ncong (3\mathbb{Z}, +, \cdot)$.
   Assume that $f : \mathbb{C} \to \mathbb{R}$ is an isomorphism. Ring homomorphisms preserve idempotents, therefore we have $f(1) = 1$. A ring homomorphism must also preserve additive inverses, therefore $f(-1) = -1$. Let $a = f(i)$. We then have

$$a^2 = f(i)f(i) = f(i^2) = f(-1) = -1,$$

   but we know that there is no $a \in \mathbb{R}$ such that $r^2 = -1$. Therefore there can't be an isomorphism between $\mathbb{C}$ and $\mathbb{R}$.
7. Let R be a ring with p elements, p prime. Since every group of prime order is cyclic, so is $(R, +)$. If a is one of the generators of the group, we have

$$R = \{a, 2a, 3a, \ldots, (p-1)a, pa = 0\}.$$

   Let $a^2 = ka,\ 1 \leq k \leq p$. If $k = p$, then all products in R are equal to 0, which contradicts our assumption that there is at least one nonzero product. So, $k \neq p$. In other words, $\gcd(k, p) = 1$. From number theory:

$$(\exists l, m \in \mathbb{Z})\ lk + mp = 1.$$

   We claim that $f : \mathbb{Z}_p \to R$ defined by $f(\bar{i}) = ila$ is a ring isomorphism.

(i) *injectivity*. Let $\bar{i},\bar{j} \in \mathbb{Z}_p$ be arbitrary.

$$\begin{aligned} f(\bar{i}) = f(\bar{j}) &\Rightarrow ila = jla \\ &\Rightarrow ila - jla = 0 \\ &\Rightarrow (i-j)la = 0 \\ &\overset{(\star)}{\Rightarrow} i - j = 0 \\ &\Rightarrow i = j \\ &\Rightarrow \bar{i} = \bar{j} \end{aligned}$$

$(\star)$: $a \neq 0$, because a is a generator. $l \neq 0$, otherwise $mp = 1$ which is impossible because $p > 1$.

(ii) *surjectivity*. Since R is finite and f is an injection, f is a surjection.

(iii) *homomorphism*. Let $\bar{i},\bar{j} \in \mathbb{Z}_p$ be arbitrary.

$$f(\bar{i}+\bar{j}) = f(\overline{i+j}) = (i+j)la = ila + jla = f(\bar{i}) + f(\bar{j})$$

$$f(\bar{i})f(\bar{j}) = (ila)(jla) = \underbrace{(a+a+\ldots+a)}_{il}\underbrace{(a+a+\ldots+a)}_{jl} = ijl^2a^2 = ijl^2ka = ijllka$$

$$= ijl(1-mp)a = ijla - ijm\underbrace{(pa)}_{=0} = ijla = f(\overline{ij})$$

From $(i),(ii),(iii)$ follows that f is an isomorphism between R and $\mathbb{Z}_p$.

8. Let $a \in R$ be arbitrary but fixed. We define the sets

$$\begin{aligned} C_a &= \{x \in R | xa = ax\} \\ D_a &= \{x \in R | xa = -ax\}. \end{aligned}$$

We have that $R = C_a \cup D_a$, $C_a \cap D_a = \emptyset$ for all $a \in R$. If $R \neq C_a$ and $R \neq D_a$, then there exists elements $c \in C_a \setminus D_a$ and $d \in D_a \setminus C_a$. Since $(R,+)$ is an abelian group, we have that $c + d \in R$. Thus, for $a \in R$ we have that $(c+d)a = a(c+d)$ or $(c+d) = -a(c+d)$. If $(c+d)a = a(c+d)$, then $ca + da = ac + ad \Rightarrow da = ad$ which means that $d \in C_a$, contradiction. Similarly we get that $c \in D_a$, contradiction. Thus, $R = C_a \veebar R = D_a$. We denote

$$\begin{aligned} U &= \{a \in R : C_a = R\} \\ V &= \{a \in R : D_a = R\} \end{aligned}$$

We see that $R = U \cup V$. If $R \neq U$ and $R \neq V$, we can find elements $u \in U \setminus V$ and $v \in V \setminus U$.

$$\begin{aligned} u \in U \setminus V &\Rightarrow C_u = R \ \wedge C_u \neq D_u \Rightarrow xu = ux \ \wedge xu \neq -ux \\ v \in V \setminus U &\Rightarrow D_v = R \ \wedge D_v \neq C_v \Rightarrow xv = -vx \ \wedge xv \neq vx \end{aligned}$$

Since $u + v \in R$ we have that $u + v \in U$ or $u + v \in V$. If $u + v \in U$, then $C_{u+v} = R$. This means that for all $x \in R$, $x(u+v) = (u+v)x \Rightarrow xu + xv = ux + vx$. Since $ux = xu$, it follows that $xv = vx$, $\forall x \in R$. Thus, $C_v = R$ which would imply that $v \in U$, contradiction. By similar reasoning we would obtain that $D_u = R$, which would mean that $u \in V$, contradiction. Thus, $R = U \veebar R = V$. In other words, either R is a commutative ring or $xy = -yx$, for all $x, y \in R$.

9. (a) Let $a \in R$ be an element which is not a divisor of zero. Then there must exists positive integers m and n such that $a^m = a^n$, because R is finite. Assume that $m < n$. We have that $a^{m-1}\left(a - a^{n-m+1}\right) = 0$ and since a is not a divisor of zero, $a^{n-m+1} = a$.
   Let $b \in R$ be arbitrary. Then $ba = ba^{n-m+1}$, which is equivalent with $(b - ba^{n-m})a = 0$, so $b = ba^{n-m}$ (since a is not a divisor of zero). Analogously, we obtain $b = a^{n-m}b$. So, a^{n-m} is the unity of the ring R.
   (b) From (a) we have that every element a, which is not a divisor of zero, has an inverse $a^{-1} = a^{n-m-1}$. By contraposition, if $b \in R$ does not have an inverse, then b must be a divisor of zero.

1.2.4 Additional problems

1. Show that $\mathbb{Z}_n$ has divisors of zero if and only if n is not a prime.
2. Let R be a ring that contains at least two elements. Suppose for each nonzero $a \in R$, there exists a unique $b \in R$ such that $aba = a$.
   (a) Show that R has no divisors of zero.
   (b) Show that $bab = b$.
   (c) Show that R has unity.
   (d) Show that R is a division ring.
3. Let R be a finite ring that contains an element a, which is not a left divisor of zero, and an element b, which is not a right divisor of zero. Show that R has unity.
   Hint: By defining two really similar bijective mappings from R to R, depending on a and b of course, and considering some equalities will give you the solution.
4. Let R be a commutative ring with unity and e an idempotent different from 0 and 1. Show that:
   (a) $1 - e$ is an idempotent,
   (b) Re and $R(1-e)$ are subrings with unity,
   (c) $R \cong Re \times R(1-e)$.
5. Prove that in a finite ring in which there exists an element a which is not a left divisor of zero and an element b which is not a right divisor of zero, is a ring with unity.
6. Let R be a ring of $n \times n$ matrices with elements in a field F. Prove that the set of upper triangular matrices is a subring of R.
7. Prove:
   (a) A subring S of a ring with unity R does not have to be a ring with unity.
   (b) A subring S of a ring R without unity can contain a unity.
   (c) A subring S of a ring R can have a unity which is different than 1_R.
8. Let L be a subring of R. If L has a unity and R does not have a unity, then R has divisors of zero.
9. Prove that if in a ring with unity R for every $a, b \in R$ it holds $(a+b)^2 = a^2 + b^2$, then R is commutative.
10. If a and b are nilpotents of a commutative ring R, prove that $a + b$ is also a nilpotent.

1.3 Ring characteristic. Euler's and Fermat's theorems. Euler's function

1.3.1 Theoretical background

Definition 1.3.1 If for a ring R a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring** R. If no such n exists, we say that R has **characteristic 0**. We denote it with $char(R)$.

Theorem 1.3.1 — Fermat's little theorem. For every integer a and every prime p such that $p \nmid a$, it holds that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corollary 1.3.2 For every integer a and prime p, it holds that

$$a^p \equiv a \pmod{p}.$$

Definition 1.3.2 Euler's function $\varphi : \mathbb{N} \to \mathbb{N}$ is a multiplicative arithmetic function of an arbitrary positive integer n, which counts the positive integers d that are relatively prime to n and $d < n$. In other words:

$$\varphi(n) = |\{d \in \mathbb{N} : \gcd(d,n) = 1,\ 1 \leq d < n\}|.$$

Theorem 1.3.3 — Euler. For every integer a and positive integer n coprime with a, it holds that

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

1.3.2 Problems

1. Find the remainder of 37^{49} when divided by 7.
2. Describe all solutions of the given congruences:
   (a) $2x \equiv 6 \pmod{4}$
   (b) $155x \equiv 75 \pmod{65}$
   (c) $39x \equiv 52 \pmod{130}$
3. Find the remainder of $2^{2^{17}} + 1$ when dividing by 19.
4. Prove that for every $n \in \mathbb{N}$ it holds that $n^{33} \equiv n (\text{mod } 15)$.
5. Compute $\varphi(p_1 p_2 \dots p_r)$, where $p_1, \dots, p_r$ are pairwise distinct primes.
6. Compute $\varphi(p^n)$, where p is a prime.
7. Compute $\varphi(n)$ for an arbitrary positive integer n. Using the obtained formula and Euler's theorem, find the last two digits of 19^{4322}.
8. Prove that the characteristic of an integral domain D is either 0 or p, where p is a prime.
9. Let R be a commutative ring with identity and let $char(R) = 3$. Compute and simplify $(a+b)^9$, $a, b \in R$.
10. Prove that 1 and $p-1$ are the only elements of $\mathbb{Z}_p$ that are their own inverses.
11. Let D be an integral domain which contains an element $0 \neq a \in D$ and there exists an $n \in \mathbb{N}$ such that $na = 0$. Show that the characteristic of D is a positive integer d, which is a divisor of n.

12. Let R be a ring and n a positive integer for which $x^n = x$, for all $x \in R$. Prove: if n is odd, then $char(R)$ equals the product of distinct prime numbers, and if n is even, then $char(R) = 2$.
13. Let $(R,+,\cdot)$ be a ring in which every element is an idempotent. Show that $char(R) = 2$ and R is commutative.

1.3.3 Solutions

1. Since $\gcd(37,7) = 1$, by Fermat's little theorem we have that $37^6 \equiv 1 \pmod 7$. We use standard mathematical operations like exponenting and multiplying, to obtain 37^{49}. (Similarly as if you would be working with "standard" equations).

$$\begin{aligned} 37^6 &\equiv 1 \pmod 7 \Big|^{8} \\ 37^{48} &\equiv 1 \pmod 7 \Big| \cdot 37 \\ 37^{49} &\equiv 37 \pmod 7 \\ 37^{49} &\equiv 2 \pmod 7 \end{aligned}$$

2. If $a,n \in \mathbb{N}$ and $b \in \mathbb{Z}$, the congruence $ax \equiv b \pmod n$ has a solution **iff** $d|b$, where $d = \gcd(a,n)$. If this condition is satisfied, the congruence has exactly d noncongruent solutions modulo n of the form

$$x_0 + \frac{n}{d}t,\ t = 0,1,\ldots,d-1,$$

where x_0 is the unique solution of the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \ (\text{mod } \frac{m}{d}).$$

If $d \nmid b$, the congrence has no solution.

(a) Since $\gcd(2,4) = 2$ and $2|6$, the congruence has exactly two solutions. We will consider the congruence $x \equiv 3 \pmod 2$. From here, it is easy to see that $x_0 = 3$ which means that the seeked solutions are $x \equiv 3 \pmod 4$ and $x \equiv 5 \pmod 4 \equiv 1 \pmod 4$.

(b) To find $\gcd(155,65)$ we will use Euklid's algorithm.

$$\begin{aligned} 155 &= 2\cdot 65 + 25 \\ 65 &= 2\cdot 25 + 15 \\ 25 &= 1\cdot 15 + 10 \\ 15 &= 1\cdot 10 + 5 \\ 10 &= 2\cdot 5 \end{aligned}$$

Since $\gcd(155,65) = 5$ and $5|75$, the congruence has exactly 5 solutions. We will consider the congruence $31x \equiv 15 \pmod{13}$. Now, in the previous case it was super easy to see what x_0 was since we had only x on the left side of the congruence. Solving this would add more work for us, that's why we will work out what x_0 is from the Euclidean algorithm above (and this method always works and is super easy, we just have to be careful with calculations). What we want to do is go in the reverse order to see for which integers $x, y \in \mathbb{Z}$ we have $5 = 155x + 65y$.

$$\begin{aligned}5 &= 15 - 10\\ &= 15 - (25 - 15)\\ &= 2 \cdot 15 - 25\\ &= 2 \cdot (65 - 2 \cdot 25) - 25\\ &= 2 \cdot 65 - 5 \cdot 25\\ &= 65 - 5 \cdot (155 - 2 \cdot 65)\\ &= 12 \cdot 65 + (-5) \cdot 155\end{aligned}$$

So we have, $155 \cdot (-5) + 65 \cdot 12 = 5$. Multiplying this equality with 15 we get $155 \cdot (-75) + 65 \cdot 180 = 75$, or in other words, $155 \cdot (-75) \equiv 75 \pmod{65}$. So, $x_0 \equiv -75 \pmod{65} \equiv -10 \pmod{65} \equiv 55 \pmod{65}$. One solution is $x \equiv 55 \pmod{65}$. For $t = 1, \dots, 4$ we work out that the remaining noncongruent solutions modulo 65 are $x \equiv 3, 16, 29, 42 \pmod{65}$.

(c) Since $\gcd(39, 130) = 13$ and $13|52$, there are exactly 13 solutions to the given congruence. We consider $3x \equiv 4 \pmod{10}$, It is easy to see that $x_0 = 8$. Thus the solutions of the given congruence are $x \equiv 8 + 10t \pmod{130}$, where $t = 0, 1, \dots, 12$.

3. Since $\gcd(2, 19) = 1$, by Fermat's little theorem we have that $2^{18} \equiv 1 \pmod{19}$. Let us consider what $2^{17} \mod 18$ equals to.

$$2^{17} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 \cdot 2 \equiv (-2) \cdot (-2) \cdot (-2) \cdot (-2) \cdot 2 \pmod{18} \equiv 32 \pmod{18} \equiv 14 \pmod{18}$$

In other words, there exists some $q \in \mathbb{Z}$ such that $2^{17} = 18q + 14$. Hence,

$$2^{2^{17}} = 2^{18q+14} = (2^{18})^q \cdot 2^{14} \equiv 1^q \cdot 2^{14} \pmod{19}.$$

It remains to show what $2^{14} \mod 19$ equals to:

$$2^{14} = (2^4)^3 \cdot 2^2 \equiv (-3)^3 \cdot 4 \pmod{19} \equiv -108 \pmod{19} \equiv -13 \pmod{19} \equiv 6 \pmod{19}.$$

Thus,

$$2^{2^{17}} \equiv 6 \pmod{19} \Rightarrow 2^{2^{17}} + 1 \equiv 7 \pmod{19}.$$

4. Since $15 = 3 \cdot 5$, it suffices to show that $n^{33} \equiv n \pmod{3}$ and $n^{33} \equiv n \pmod{5}$. If $3|n$, then $3|n(n^{32} - 1) \Rightarrow 3|(n^{33} - n)$, or in other words $n^{33} \equiv n \pmod{3}$. If $3 \nmid n$, from Fermat's little theorem, we have that

$$\begin{aligned} n^2 \equiv 1 \pmod{3}\Big|^{16} &\Rightarrow n^{32} \equiv 1 \pmod{3}\\ &\Rightarrow n^{33} \equiv n \pmod{3}\end{aligned}$$

Thus, for all $n \in \mathbb{N}$, it holds that $n^{33} \equiv n \pmod{3}$. One shows similarly that $n^{33} \equiv n \pmod{5}$, for all $n \in \mathbb{N}$.

5. Let m and n be two coprime integers. Let us consider the rings $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$. In our case, we know that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Since both rings are finite, the number of units in $\mathbb{Z}_m \times \mathbb{Z}_n$ equals the number of units in $\mathbb{Z}_m$ times the number of units in $\mathbb{Z}_n$. The number of units in $\mathbb{Z}_n$ equals $\varphi(n)$. Thus, because of the isomorphism, the number of units in $\mathbb{Z}_{mn}$ is $\varphi(mn)$ and that equals $\varphi(m)\varphi(n)$. Using the fact that $p_1, \ldots, p_r$ are all pairwise coprime and $\varphi(p_i) = p_i - 1$, we conclude that
$$\varphi(p_1 p_2 \ldots p_r) = (p_1 - 1)(p_2 - 1) \ldots (p_r - 1).$$
6. All positive integers less than p^n that are not divisible by p are relatively prime to p. Thus, we delete from $p^n - 1$ integers less that p^n, the integers $p, 2p, \ldots, (p^{n-1} - 1)p$. Hence,
$$\varphi(p^n) = p^n - 1 - (p^{n-1} - 1) = p^n - p^{n-1} = p^{n-1}(p-1).$$
7. Let $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ be the prime factorisation of n. For every $1 \leq i, j \leq r$, $i \neq j$, we have that $\gcd(p_i^{k_i}, p_j^{k_j}) = 1$. Following the observations from the previous two problems we obtain that
$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \ldots \varphi(p_r^{k_r}) \\ &= p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \ldots p_r^{k_r-1}(p_r - 1)\end{aligned}$$
If we take the factor p_i from $(p_i - 1)$, we obtain that
$$\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$
Since $\gcd(19, 100) = 1$ and, by the above formula, $\varphi(100) = 40$, from Euler's theorem we have that $19^{40} \equiv 1 \pmod{100}$. Exponentiating this by 108 we have $19^{4320} \equiv 1 \pmod{100}$. Since $19^2 = 361 \equiv 61 \pmod{100}$, we conclude that $19^{4322} \equiv 61 \pmod{100}$. In other words, the last two digits of 19^{4322} are 61.
8. Let D be an integral domain with unity 1. We will consider two cases, based on the additive order of 1:
   (a) $ord(1)$ is infinite. In this case, there cannot exist a positive integer $n \in \mathbb{N}$ such that $n \cdot 1 = 0$. Thus, $char(D) = 0$.
   (b) $ord(1) = n$. Suppose that $n = kl$ for some $1 < k, l < n$. From
   $$0 = n \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1)$$
   and since D has no divisors of zero, we must have that $k \cdot 1 = 0$ or $l \cdot 1 = 0$, which is a contradiction with n being the smallest integer for which $n \cdot 1 = 0$. Thus, n must be a prime. Furthermore, if $a \in D$ is arbitrary, we have that $na = (n \cdot 1) \cdot a = 0a = 0$, that is $char(D) = n$.
9. Since R is **commutative**, the binomial theorem holds. That is, for any two $a, b \in R$ and $n \in \mathbb{N}$ we have
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$
For $n = 9$, we have
$$(a+b)^9 = a^9 + \sum_{k=1}^{8} \binom{9}{k} a^{9-k} b^k + b^9.$$

Since $char(R) = 3$ and $3|\binom{9}{k}$ for $1 \leq k \leq 8$, we have that the middle sum above equals zero. In other words, $(a+b)^9 = a^9 + b^9$.

10. If $a \in \mathbb{Z}_p$ is its own inverse, then $a \cdot a = a^2 = 1$. In other words $a^2 - 1 = (a-1)(a+1)$. Since $\mathbb{Z}_p$ has no divisors of zero, either $a - 1 = 0 \mod p$ or $a + 1 = 0 \mod p$. Hence, $a = 1$ or $a = -1 \mod p = p - 1$.
11. Let $char(D) = d$, where $d \leq n$. Since

$$0 = na = (n \cdot 1) \cdot \underbrace{a}_{\neq 0} \Rightarrow n \cdot 1 = 0, \ \forall n.$$

If we take an arbitrary $x \in D$, then $nx = n \cdot 1 \cdot x = 0$. Let us suppose that $d \nmid n$. In other words, there exists $k, l \in \mathbb{Z}$ such that $n = kd + l, \ l < d$. Multiplying his equality with x we obtain

$$0 = nx = \underbrace{kdx}_{=0} + lx \Rightarrow lx = 0,$$

which is a contradiction because $l < d$.

12. Let $k \in \mathbb{N}$ and $x \in R$, then $kx \in R$. Thus,

$$\begin{aligned} &(kx)^n = kx \\ \Leftrightarrow &k^n x^n = kx \\ \Leftrightarrow &k^n x = kx \\ \Leftrightarrow &(k^n - k)x = 0 \end{aligned}$$

Firstly we will prove the following.

Claim: If $char(R) = c > 0$ and $dx = 0$ for all $x \in R$, then $c|d$.

Proof. Suppose that $c \nmid d$. By the Quotient remainder theorem, there exist $l, k \in \mathbb{Z}^+$ such that $d = kc + l$ and $l < c$. If we multiply this equality by $x \in R$ we obtain

$$0 = dx = k(cx) + lx = 0 + lx = lx,$$

however this is a contradiction because $char(R) = c > l$. Thus, it must hold that $c|d$. ■

Hence, in our case, it must hold that $char(R)|(k^n - k)$ for every $k \in \mathbb{N}$. Without loss of generality, assume that $char(R) = p^2$, for some odd prime prime p. We have that

$$p^2|(k^n - k), \ \forall k \in \mathbb{N} \Rightarrow p^2|(p^n - p) \Rightarrow p^2|p(p^{n-1} - 1) \Rightarrow p|p^{n-1} - 1,$$

but this is not true. In other words, p equals the product of distinct primes. If $x \in R$ then $-x \in R$. Let $n = 2k$, then:

$$-x = (-x)^n = (-x)^{2k} = [(-x)^2]^k = [x^2]^k = x^{2k} = x.$$

Thus, it must follow that $x = -x$, in other words $2x = 0$, which implies that $char(R) = 2$.

13. Let $x \in R$ be arbitrary. Since every element is an idempotent, this means that also $x + x$ is an idempotent, thus

$$(x+x)^2 = x + x \Leftrightarrow x^2 + x^2 + x^2 + x^2 = x + x \Rightarrow x + x + x + x = x + x \Rightarrow 2x = 0.$$

Since x was arbitrary, it follows that $char(R) = 2$. Let $x, y \in R$ be arbitrary and distinct. We have:

$$(x+y)^2 = x+y \Rightarrow x^2+xy+yx+y^2 = x+y \Rightarrow x+xy+yx+y = x+y \Rightarrow xy+yx = 0$$

Since $xy \in R$, we have that $2xy = 0$ Hence, $xy+yx = 2xy \Rightarrow yx = xy$.

1.3.4 Additional problems

1. Show that there do not exist positive integers m and n such that $\varphi(n) = 2 \cdot 7^{5m+4}$.
2. Find the smallest positive integer which has exactly 10 positive divisors.
3. If $\gcd(a,55) = \gcd(b,55) = 1$, prove that $a^{20} - b^{20}$ is divisible by 55.
4. Find, if it exists, a prime p such that:
   (a) $p^2 | 11^{p^2} + 1$.
   (b) $p^2 | 31^{p^2} + 1$.

1.4 Fraction fields. Rings of polynomials

1.4.1 Theoretical background

Every field is also an integral domain; however, there are many integral domains that are not fields. A question that naturally arises is how we might associate an integral domain with a field. There is a natural way to construct the rationals $\mathbb{Q}$ from the integers: the rationals can be represented as formal quotients of two integers. The rational numbers are certainly a field. In fact, it can be shown that the rationals are the smallest field that contains the integers. Given an integral domain D, our question now becomes how to construct a smallest field F containing D. We will do this in the same way as we constructed the rationals from the integers.

An element $p/q \in \mathbb{Q}$ is the quotient of two integers p and q. However, different pairs of integers can represent the same rational number. For instance, $1/2 = 2/4 = 3/6$. We know that

$$\frac{a}{c} = \frac{c}{d} \Leftrightarrow ad = bc.$$

A more formal way of considering this problem is to examine fractions in terms of equivalence relations. We can think of elements in $\mathbb{Q}$ as ordered pairs in $\mathbb{Z} \times \mathbb{Z}$. The fraction p/q can be written as (p,q). However, there are problems if we consider all possible pairs in $\mathbb{Z} \times \mathbb{Z}$. There is no fraction $5/0$ corresponding to $(5,0)$. Also, the pairs $(3,6)$ and $(2,4)$ both represent $1/2$. The first problem is easily solved if we require the second coordinate to be nonzero. The second problem is solved by considering two pairs (a,b) and (c,d) to be equivalent if $ad = bc$.

If we use the approach of ordered pairs instead of fractions, then we can study integral domains in general. Let D be any integral domain and let

$$S = \{(a,b) : a, b \in D, b \neq 0\}.$$

Define a relation on S by $(a,b) \sim (c,d) \Leftrightarrow ad = bc$.

Lemma 1.1 The relation $\sim$ between elements of S is an equivalence relation.

Proof. The proof is left to the reader. ■

We will denote the set of equivalence classes on S by F_D. We now need to define the operations of addition and multiplication on F_D. If we denote the equivalence class of $(a,b) \in S$ with $[(a,b)]$, then we are led to define the operations of addition and multiplication on F_D by

$$[(a,b)]+[(c,d)] = [(ad+bc,bd)] \text{ and } [(a,b)]\cdot[(c,d)] = [(ac,bd)], \qquad (1.1)$$

respectively. The next lemma demonstrates that these operations are independent of the choice of representatives from each equivalence class.

Lemma 1.2 The operations of addition and multiplication on F_D are well-defined.

Proof. The proof is left to the reader. ■

Lemma 1.3 The set of equivalence classes of S, F_D, under the equivalence relation $\sim$ together with the operations of addition and multiplication defined by (1.1) is a field.

Proof. 1. $(F_D,+)$ *is a commutative group.*

- associativity. Holds because of the associativity of the operation $+$ in D.
- additive identity (zero). The additive identity in F_D is $[(0,1)]$, because for every $[(a,b)] \in F_D$ it holds

$$[(0,1)]+[(a,b)] = [(0\cdot b+1\cdot a, 1\cdot b)] = [(a,b)]$$
$$[(a,b)]+[(0,1)] = [(a\cdot 1+b\cdot 0, b\cdot 1)] = [(a,b)]$$

- additive inverse. For every element $[(a,b)] \in F_D$ there exists a unique element $[(-a,b)] \in F_D$ such that

$$[(a,b)]+[(-a,b)] = [(a\cdot b+b\cdot(-a), b\cdot b)] = [(0,b^2)]$$
$$[(-a,b)]+[(a,b)] = [(-a\cdot b+b\cdot a, b\cdot b)] = [(0,b^2)]$$

Because $(0,b^2)\sim(0,1) \Leftrightarrow 0\cdot 1 = b^2\cdot 0 \Leftrightarrow 0=0$, it holds that $[(0,b^2)] = [(0,1)]$.

- commutativity. For every $[(a,b)],[(c,d)] \in F_D$, it holds that

$$[(a,b)]+[(c,d)] = [(ad+bc,bd)] = [(cb+da,db)] = [(c,d)]+[(a,b)],$$

where we used the fact that D is commutative.

Hence, $(F_D,+)$ is an abelian group.

2. *associativity of multiplication*. It holds because multiplication is associative in D.
3. *unity in F_D*. There exists an element $[(1,1)] \in F_D$ such that for every $[(a,b)] \in F_D$ it holds that

$$[(a,b)]\cdot[(1,1)] = [(1,1)]\cdot[(a,b)] = [(a,b)].$$

4. *multiplicative inverse*. For every element $[(a,b)] \in F_D \setminus \{[(0,1)]\}$ there exists an element $[(b,a)] \in F_D$ such that

$$[(a,b)]\cdot[(b,a)] = [(b,a)]\cdot[(a,b)] = [(ab,ab)].$$

Since $[(a,b)] \neq [(0,1)]$ it must hold that $a,b \neq 0$ and furthermore, since D has no divisors of zero, it holds that $ab \neq 0$. We note that $[(1,1)] = \{(a,a) : a \in D, a \neq 0\}$. Thus, it holds that $[(ab,ab)] = [(1,1)]$.

5. *commutativity*. Holds because D is commutative.
6. *distributivity*. Let $[(a,b)],[(c,d)],[(e,f)] \in F_D$ be arbitrary.

$$\begin{aligned}
[(a,b)]\cdot([(c,d)]+[(e,f)]) &= [(a,b)]\cdot[(cf+de,df)] = [(a(cf+de),bdf)] \\
[(a,b)]\cdot[(c,d)]+[(a,b)]\cdot[(e,f)] &= [(ac,bd)]+[(ae,bf)] \\
&= [(acbf+bdae,bdbf)] \\
&= [ba(cf+de),b(bdf)]
\end{aligned}$$

Since $(x,y)\sim(\alpha x,\alpha y)$ for $\alpha \neq 0$, we have that $[(ba(cf+de),b(bdf)] = [(a(cf+de),bdf)]$. Thus, we conclude that

$$[(a,b)]\cdot([(c,d)]+[(e,f)]) = [(a,b)]\cdot[(c,d)]+[(a,b)]\cdot[(e,f)].$$

In a similar manner one can show that the other distributive law holds as well.

Thus, $(F_D,+,\cdot)$ is a field. ■

Definition 1.4.1 The field F_D is called the **field of fractions** of the integral domain D.

Lemma 1.4 The map $i: D \to F_D$ s defined with $i(a) = [(a,1)]$ is an isomorphism of D with a subring of F_D.

Proof. The proof is left to the reader. ■

Since $[(a,b)] = [(a,1)][(1,b)] = [(a,1)]\cdot[(b,1)]^{-1} = i(a)\cdot i(b)^{-1} = i(a)/i(b)$ clearly holds in F_D, we have proved the following theorem.

Theorem 1.4.1 Any integral domain D can be enlarged to a field F_D such that every element in F_D can be expressed as a quotient of two elements of D.

Corollary 1.4.2 Let F be a field of characteristic zero. Then F contains a subfield isomorphic to $\mathbb{Q}$.

Corollary 1.4.3 Let F be a field of characteristic p. Then F contains a subfield isomorphic to $\mathbb{Z}_p$.

F_D can be in some sense regarded as a minimal field containing D. The following theorem shows that every field containing D contains a subfield which is a field of quotients of D, and that any two fields of quotients of D are isomorphic.

Theorem 1.4.4 Let F be a field of quotients of D and let L be any field containing D. Then there exists an isomorphism $\psi: F \to L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \in D$.

Proof. An element F is of the form $a/_F b$ where $/_F$ denotes the quotient of $a \in D$ by $b \in D$ regarded as elements of F. We want to map $a/_F b$ to $a/_L b$ where $/_L$ denotes the quotients in L. We define $\psi: F \to L$ with $\psi(a/_F b) = \psi(a)/_L \psi(b)$, where $\psi(x) = x$ for all $x \in D$. Let us show that this mapping is well-defined.

$$\begin{aligned} a/_F b = c/_F d \text{ in } F &\Rightarrow ad = bc \text{ in } D \\ &\Rightarrow \psi(ad) = \psi(bc) \\ &\Rightarrow \psi(a)\psi(d) = \psi(b)\psi(c) \\ &\Rightarrow \psi(a)/_L \psi(b) = \psi(c)/_L \psi(d) \end{aligned}$$

Thus ψ is well-defined. Furthermore,

$$\begin{aligned} \psi(xy) &= \psi((a/_F b)(c/_F d)) = \psi((ac)/_F(bd)) = (\psi(a)\psi(c))/_L(\psi(b)\psi(d)) \\ &= (\psi(a)/_L\psi(b))(\psi(c)/_L\psi(d)) = \psi(x)\psi(y) \end{aligned}$$

$$\begin{aligned} \psi(x+y) &= \psi((a/_F b)+(c/_F d)) = \psi((ad+bc)/_F(bd)) = \psi(ad+bc)/_L\psi(bd) \\ &= (\psi(a)\psi(d)+\psi(b)\psi(c))/_L(\psi(b)\psi(d)) = (\psi(a)/_L\psi(b))+(\psi(c)/_L\psi(d)) \\ &= \psi(a/_F b)+\psi(c/_F d) = \psi(x)+\psi(y), \end{aligned}$$

that is, ψ is a homomorphism. Since,

$$\begin{aligned} \psi(a/_F b) = \psi(c/_F d) &\Rightarrow \psi(a)/_L\psi(b) = \psi(c)/_F\psi(d) \\ &\Rightarrow \psi(a)\psi(d) = \psi(b)\psi(c) \\ &\Rightarrow ad = bc \\ &\Rightarrow a/_F b = c/_F d, \end{aligned}$$

ψ is one-to-one. ■

Corollary 1.4.5 Every field L containing an integral domain D contains a field of quotients of D.

Corollary 1.4.6 Any two fields of quotients of an integral domain D are isomorphic.

Definition 1.4.2 Let R be a ring. A polynomial $f(x)$ with coefficients in R is an infinite formal sum $\sum_{i=1}^{\infty} a_i x^i$ where $a_i \in R$ and $a_i = 0$ for all but finitely many values of i. The a_i are coefficients of $f(x)$. If for some $i \geq 0$ it is true that $a_i \neq 0$, the largest such value of i is the degree of $f(x)$.

Theorem 1.4.7 The set $R[x]$ of all polynomials in indeterminate x with coefficients in a ring R is a ring under polynomial addition and multiplication defined as follows.

Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$. Then

$$f(x)+g(x) = \sum_{i=0}^{\infty} c_i x^i,\ c_i = a_i + b_i,$$

and

$$f(x)g(x) = \sum_{i=0}^{\infty} d_i x^i,\ d_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

If R is commutative, then so is $R[x]$. If R is a ring with unity $1 \neq 0$, then 1 is also the unity of $R[x]$.

Theorem 1.4.8 — The Evaluation Homomorphism for Field Theory. Let F be a subfield of a field E, let α be any element of E, and let x be an indeterminate. The map $\phi_\alpha : F[x] \to E$ defined by

$$\phi_\alpha(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

for $\sum_{i=1}^n a_i x^i \in F[x]$ is a homomorphism of $F[x]$ into E. Also, $\phi_\alpha(x) = \alpha$ and ϕ_α maps F isomorphically by the identity map, that is, $\phi_\alpha(a) = a$, for $a \in F$. The homomorphism ϕ_α is the **evaluation at** α.

Definition 1.4.3 — zero of polynomial . Let F be a subfield of a field E, and let α be an element of E. Let $f(x) = \sum_{i=1}^n a_i x^i$ be in $F[x]$ and let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism. Let $f(\alpha)$ denote

$$\phi_\alpha(f(x)) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

If $f(\alpha) = 0$, then α is a **zero** of $f(x)$.

1.4.2 Problems

1. Find the product of $f(x) = 2x^2 + 3x + 4$ and $g(x) = 3x^2 + 2x + 3$ in $\mathbb{Z}_6[x]$.
2. How many polynomials of degree m are there in $\mathbb{Z}_n[x]$?
3. If $F = E = \mathbb{Z}_7$, compute the indicated evaluation homomorphism:
   (a) $\phi_3(((x^4 + 2x)(x^3 - 3x^2 + 3))$
   (b) $\phi_4(3x^{106} + 5x^{99} + 2x^{53})$
4. Use Fermat's theorem to find all zeroes in $\mathbb{Z}_5$ of $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$.
5. Consider the evaluation homomorphism $\phi_5 : \mathbb{Q}[x] \to \mathbb{R}$. Find six elements in the kernel of ϕ_5.
6. Let D be an integral domain. Show that then $D[x]$ is also an integral domain.
7. Let D be an integral domain and $f, g \in D[x]$. Prove that $\deg(fg) = \deg(f) + \deg(g)$. Does the statement hold if D contains divisors of zero?
8. What are the units in the integral domain $D[x]$?

1.4.3 Solutions

1. Always keep in mind that you are doing addition and multiplication modulo 6. Then, it is easy to compute that $f(x) \cdot g(x) = x^3 + 5x$.
2. Let $f(x) = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + a_m x^m$ be an arbitrary polynomial of degree m in $\mathbb{Z}_n[x]$. Since we need to have the leading coefficient a_m always present, we know that $a_m \in \{1, 2, \ldots, n-1\}$ and for the other a_i we can take any element of $\mathbb{Z}_n$. Thus in total there are $n^m \cdot (n-1)$ polynomials of degree m in $\mathbb{Z}_n[x]$.
3. (a) First, we note that $f(x) = (x^4 + 2x)(x^3 - 3x^2 + 3) = x^7 + 4x^6 + 5x^4 + x^3 + 6x$. Thus,

$$\phi_3(f(x)) = f(3) = 3^7 + 4 \cdot 3^6 + 5 \cdot 3^4 + 3^3 + 6 \cdot 3.$$

Using Fermat's little theorem and its corollary, we have that $3^7 \mod 7 = 3$

and $3^6 \mod 7 = 1$. Furthermore, it is easy to compute that $3^4 \mod 7 = 4$ and $3^3 \mod 7 = 6$. Hence,

$$\phi_3(f(x)) = 3+4+5\cdot 4+6+4 = 2.$$

(b) From Fermat's little theorem, we know that $4^6 \equiv 1 \pmod 7$. Now we try to "pack" 4^6 to get as close as we can to 4^{106}. In our case, $(4^6)^{17} = 4^{102} \equiv 1 \pmod 7$. On the other hand, $4^4 \equiv 4 \pmod 7$. By multiplying these two congruences, we obtain that $4^{106} \equiv 4 \pmod 7$. In a similar manner we compute that, $4^{99} \equiv 1 \pmod 7$ and $4^{53} \equiv 2 \pmod 7$. Hence,

$$\phi_4(3x^{106}+5x^{99}+2x^{53}) = 3\cdot 4+5\cdot 1+2\cdot 2 = 0.$$

4. From Fermat's little theorem, we know that $a^4 \equiv 1 \pmod 5$ for $a \in \{1,2,3,4\}$. In the expression of $f(x)$, let us write the exponents d of x as $d = 4q+l,\ l < d$. We obtain

$$f(x) = 2\cdot(x^4)^{54}\cdot x^3 + 3\cdot(x^4)^{18}\cdot x^2 + 2\cdot(x^4)^{14}\cdot x + 3\cdot(x^4)^{11}.$$

Now, it is easy to compute the values of $f(x)$ for $x \in \mathbb{Z}_5$.

$$\begin{aligned}
&f(0) = 0\\
&f(1) = 2+3+2+3 = 0\\
&f(2) = 1+2+4+3 = 0\\
&f(3) = f(-2) = 4+2+1+3 = 0\\
&f(4) = f(-1) = 3+3+3+3 = 2
\end{aligned}$$

Thus, the zeros of $f(x)$ are $0,1,2$ and 3.

5. Obviously, $f_1(x) = x-5 \in \ker(\phi_5)$. Any multiple of f_1 will also be in $\ker(\phi_5)$.

6. From Theorem 1.4.7 we know that $D[x]$ is a commutative ring with unity $1 \neq 0$. It remains to check if $D[x]$ has zero divisors.
Let $f,g \in D[x]$ be two arbitrary nonzero polynomials. Without loss of generality, we may write

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i,\ a_i, b_j \in D,\ i = \overline{0,n}, j = \overline{0,m}.$$

Since D is an integral domain, it follows that $a_n b_m \neq 0$, thus

$$a_n b_m x^{n+m} \neq 0 \Rightarrow f(x)g(x) \neq 0.$$

In other words, $D[x]$ has no zero divisors.

7. Let

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i,\ a_i, b_j \in D,\ i = \overline{0,n}, j = \overline{0,m}$$

be two arbitrary nonzero polynomials in $D[x]$. The "highest" monomial that appears in $f(x)g(x)$ is x^{n+m} with the coefficient $a_n b_m$. However, since D is an integral domain, we know that $a_n b_m \neq 0$. Thus

$$\deg(fg) = n+m = \deg(f)+\deg(g).$$

Let us consider the ring $\mathbb{Z}_6[x]$. If we take $f(x) = 2x^2$ and $g(x) = 3x^3 + 2$, then $f(x)g(x) = 4x^2$. Hence,

$$\deg(fg) = 2 \neq 5 = \deg(f) + \deg(g).$$

8. Suppose that $f(x) \in D[x]$ is invertible. That is,

$$(\exists g(x) \in D[x])\ f(x)g(x) = 1.$$

From this, it follows that $\deg(fg) = \deg(1) = 0$. Without loss of generality, assume that $\deg(f) = n,\ \deg(g) = m,\ n, m \geq 0$. Since $D[x]$ is an integral domain, we have that $\deg(fg) = n + m = 0$, which implies that $n = m = 0$. In other words, f and g are constant polynomials, i.e., the invertible elements in $D[x]$ are exactly those elements that are invertible in D.

1.4.4 Additional problems

1. If F is a field, what is $Frac(F)$, the field of fractions of F? Prove your statement.
2. Find the units in $\mathbb{Z}[x]$ and $\mathbb{Z}_7[x]$.
3. Let F be a field of characteristic 0 and let D be the formal polynomial differentiation map, so that

$$D\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

   (a) Show that $D : F[x] \to F[x]$ us a group automorphism of $(F[x], +)$. Is D a ring homomorphism?
   (b) Find $\ker(D)$.
   (c) Find $\operatorname{im}(D)$.
4. Let F be a subfield of E.
   (a) Define an evaluation homomorphism $\phi_{\alpha_1,\ldots,\alpha_n} : F[x_1,\ldots,x_n] \to E,\ \alpha_i \in E$, stating the analog of Theorem 1.4.8.
   (b) With $F = E = \mathbb{Q}$, compute $\phi_{-3,2}(x_1^2 x_2^3 + 3x_1^4 x_2)$.
   (c) Define the concept of a zero of a polynomial $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ in a way analogous to the definition of a zero of $f(x)$.
5. Let F be a field and F^F the set of all functions from $F \to F$. For $\phi, \psi \in F^F$ we define addition $\phi + \psi$ with

$$(\phi + \psi)(a) = \phi(a) + \psi(a)$$

and multiplication $\phi \cdot \psi$ with

$$(\phi \cdot \psi)(a) = \phi(a) \cdot \psi(a)$$

where $a \in F$.
   (a) Show that $(F^F, +, \cdot)$ is a ring.

An element $\phi \in F^F$ is a polynomial if there exists $f(x) \in F[x]$, such that $\phi(a) = f(a)$ for all $a \in F$.
   (b) Show that the set P_F of all polynomials over F is a subring of F^F.
   (c) Show that P_F is not necessarily isomorphic to $F[x]$. (Hint: Show that if F is finite, $F[x]$ and F^F do not have the same cardinality).
   (d) Show that $F = \mathbb{Z}_2^{\mathbb{Z}_2}$ implies $P_F = F^F$.

1.5 Factorisation of polynomials over a field

1.5.1 Theoretical background

Theorem 1.5.1 — Division algorithm. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ be two elements of $F[x]$, with $a_n, b_m \neq 0$ and $m > 0$. Then there are **unique** polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Corollary 1.5.2 — Factor Theorem. An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

Definition 1.5.1 A nonconstant polynomial $f(x) \in F[x]$ is **irreducible over** F or is an **irreducible polynomial in** $F[x]$ if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $f(x), h(x) \in F[x]$ both of lower degree than $\deg(f)$. If a polynomial is not irreducible over F, we say that it is **reducible over** F.

Theorem 1.5.3 Let $f(x) \in F[x]$ and let $\deg(f) = 2$ or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.

Theorem 1.5.4 If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorisation with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.

Theorem 1.5.5 — Eisenstein Criterion. Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_n x^n + \ldots + a_0$ is in $\mathbb{Z}[x]$, and $p \nmid a_n$ but $p \mid a_i$ for all $i < n$, with $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 1.5.6 Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

Corollary 1.5.7 If $p(x)$ is irreducible in $F[x]$ and $p(x)$ divides the product $r_1(x) \ldots r_n(x)$ for $r_i(x) \in F[x]$, then $p(x)$ divides $r_i(x)$ for at least one i.

1.5.2 Problems

1. Find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x) = g(x)q(x) + r(x)$ with $\deg(r) < \deg(g)$, if $f(x) = x^5 - 2x^4 + 3x - 5$ and $g(x) = 2x + 1$ in $\mathbb{Z}_{11}[x]$.
2. The polynomial $f(x) = 2x^3 + 3x^2 - 7x - 5$ can be written as a product of linear terms in $\mathbb{Z}_{11}[x]$. Find that factorisation.
3. Is $x^3 + 2x + 3$ an irreducible polynomial of $\mathbb{Z}_5[x]$? Why? Express it as a product of irreducible polynomials of $\mathbb{Z}_5[x]$.
4. How many irreducible polynomials of degree 2 are there in $\mathbb{Z}_p[x]$?
5. Show that $x^p + a$ is reducible in $\mathbb{Z}_p[x]$ for all $a \in \mathbb{Z}_p$, where p is a prime number.
6. Show that $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{Q}$. Is $f(x)$ irreducible over $\mathbb{R}$? Over

$\mathbb{C}$?

7. Demonstrate that x^3+3x^2-8 is irreducible over $\mathbb{Q}$.
8. If a polynomial $p(x)$ is irreducible over a field F, the the polynomial $p(x+a)$, with $a \in F$, is also irreducible over F.
9. Let F be a field. For a polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$ we define its derivative $f'(x)$ with
$$f'(x) = \sum_{i=0}^{n} ia_ix^{i-1}.$$
   (a) Show that the mapping $D : F[x] \to F[x]$ defined with $D(f(x)) = f'(x)$ is a linear mapping between vector spaces.
   (b) Find $\ker(D)$.
   (c) Prove that D satisfies Leibniz's rule: $D(f(x)g(x)) = D(f(x))g(x) + f(x)D(g(x))$, for all $f(x), g(x) \in F[x]$.

1.5.3 Solutions

1. $q(x) = 6x^4+7x^3+2x^2+10x+2,\ r(x) = 4$

$$
\begin{array}{rr}
 & 6x^4+7x^3+2x^2+10x+2 \\
\cline{2-2}
2x+1 \big) & x^5-2x^4+0x^3+0x^2+\ \ 3x-5 \\
 & \underline{x^5+6x^4} \quad \downarrow \qquad\qquad\qquad\qquad\qquad \\
 & 3x^4+0x^3 \qquad\qquad\qquad\qquad\quad \\
 & \underline{3x^4+7x^3} \quad \downarrow \qquad\qquad\qquad\quad \\
 & 4x^3+0x^2 \qquad\qquad\qquad \\
 & \underline{4x^3+2x^2} \quad \downarrow \qquad\quad \\
 & 9x^2+\ \ 3x \qquad \\
 & \underline{9x^2+10x} \quad \downarrow \\
 & 4x+6 \\
 & \underline{4x+2} \\
 & 4
\end{array}
$$

2. $x=3$ is a zero of $f(x)$. Thus, $x-3$ is one linear term in the factorisation. Let us divide the given polynomial with $x-3$.

$$
\begin{array}{rr}
 & 2x^2+9x+9 \\
\cline{2-2}
x-3 \big) & 2x^3+3x^2-7x-5 \\
 & \underline{2x^3+5x^2} \quad \downarrow \qquad\qquad \\
 & 9x^2+4x \qquad\quad \\
 & \underline{9x^2+6x} \quad \downarrow \\
 & 9x+6 \\
 & \underline{9x+6} \\
 & 0
\end{array}
$$

Thus $f(x) = (x-3)(2x^2+9x+9)$. Since $x=4$ is a zero of the latter, let us divide $2x^2+9x+9$ with $x-4$.

$$
\begin{array}{r}
2x+6 \\
x-4\,\big)\overline{\,2x^2+9x+9} \\
\underline{2x^2+3x}\quad\downarrow \\
6x+9 \\
\underline{6x+9} \\
0
\end{array}
$$

Hence, $f(x) = (x-3)(x-4)(2x+6)$.

3. No, since $x=3$ is a zero of $f(x)$ and $\deg(f) = 3$, from Theorem 1.5.3, it follows that $f(x)$ is reducible.

$$
\begin{array}{r}
x^2+4x+3 \\
x-4\,\big)\overline{\,x^3+0x^2+2x+3} \\
\underline{x^3+\ \ x^2}\quad\downarrow\qquad\quad \\
4x^2+2x \\
\underline{4x^2+4x}\quad\downarrow \\
3x+3 \\
\underline{3x+3} \\
0
\end{array}
$$

By inspection, 2 and 4 are zeros of x^2+4x+3 and thus $f(x) = (x-2)(x-4)(x+4)$.

4. Without loss of generality, any quadratic polynomial can be written in the form $a(x^2+px+q)$, where $a,p,q \in \mathbb{Z}_p$ and $a \neq 0$. Since we are interested in the zeros, we will consider x^2+px+q. Suppose that

$$x^2+px+d = (x-c)(x-d).$$

If $c \neq d$, then there are $\binom{p}{2}$ choices for c and d, and if $c = d$, then there are p choices. In total, there are $p + \binom{p}{2} = \frac{p(p+1)}{2}$ reducible polynomials of degree 2 in $\mathbb{Z}_p$. From Problem 2 in Section 1.4.2, we have that there are $p^2(p-1)$ quadratic polynomials in $\mathbb{Z}_p[x]$. Hence, the number of irreducible quadratic polynomials in $\mathbb{Z}_p[x]$ equals

$$p^2(p-1) - \frac{p(p+1)}{2} = \frac{p^2-p^2-p^2-p}{2} = \frac{p^3-p^2-p}{2} = \frac{p(p-1)^2}{2}.$$

5. If $p=2$, then the two possible polynomials are $x^2 = x \cdot x$ and $x^2+1 = x^2+1^2 = (x+1)^2$, which are both reducible. Assume that $p \neq 2$, then p is odd. For $a \in \mathbb{Z}_p$ we have that $-a \in \mathbb{Z}_p$. From

$$(-a)^p + a = -a^p + a = -a + a = 0,$$

it follows that $-a$ is a zero of $x^p + a$, i.e., $x^p + a$ is reducible.

6. For $p = 2$, we have that $p|8$, $p|2$, $p \nmid 1$ and $p^2 \nmid 2$. Thus, following Eisenstein's Criterion, we have that $f(x)$ is irreducible over $\mathbb{Q}$. Since,
$$D = b^2 - 4ac = 64 + 8 = 72 > 0$$
it follows that $f(x)$ has a root in $\mathbb{R}[x]$, that is, $f(x)$ is reducible over $\mathbb{R}$. Since $\mathbb{R} \subset \mathbb{C}$, $f(x)$ is also reducible over $\mathbb{C}$.
7. If $x^3 + 3x^2 - 8$ is reducible over $\mathbb{Q}$, then by Theorem 1.5.4, it factors in $\mathbb{Z}[x]$, and must therefore have a linear factor of the form $x - a$ in $\mathbb{Z}[x]$. Then a must be a zero of the polynomial and must divide -8, so the possibilities are $a = \pm 1, \pm 2, \pm 4, \pm 8$. Computing the polynomial at these eight values, we find that none of them is a zero of the polynomial, which is therefore irreducible over $\mathbb{Q}$.
8. Suppose that $p(x+a)$ is reducible over F, that is
$$p(x+a) = q(x)s(x),$$
where $q(x)$ and $s(x)$ are polynomials of positive degree. If we substitute $x \leftrightarrow x - a$ in the upper equation, then
$$p(x) = q(x-a)s(x-a),$$
where $q(x-a)$ and $s(x-a)$ are also polynomials of positive degree. However, this means that $p(x)$ is reducible over F, which is not possible. Hence, $p(x+a)$ has to be irreducible over F.
9. (a) Let $g(x) = b_0 + b_1x + \ldots + b_mx^m$. Without loss of generality, suppose that $n \geq m$. Thus, we can easily write $g(x) = \sum_{i=0}^{n} b_ix^i$ with $b_{m+1} = \ldots = b_n = 0$.
$$\begin{aligned} D(f(x)+g(x)) &= D(\sum_{i=0}^{n}(a_i+b_i)x^i) = \sum_{i=0}^{n} i(a_i+b_i)x^{i-1} \\ &= \sum_{i=0}^{n} ia_ix^{i-1} + \sum_{i=0}^{n} ib_ix^{i-1} = D(f(x)) + D(g(x)) \end{aligned}$$
Similarly, one shows that $D(\alpha f(x)) = \alpha D(f(x))$ for all $\alpha \in F$. Hence, D is a linear mapping.

   (b) Suppose $char(F) = p$.
$$\begin{aligned} D(f(x)) = 0 &\Leftrightarrow \sum_{i=0}^{n} ia_ix^{i-1} = 0 \\ &\Leftrightarrow ia_i = 0,\ \forall i = 0,\ldots,n \\ &\Leftrightarrow a_i = 0,\ \forall i = 0,\ldots,n \text{ such that } p \nmid i \end{aligned}$$
Thus, $\ker(D) = \{a_0 + a_px^p + a_{2p}x^{2p} + \ldots + a_{np}x^{np} : a_i \in F, n \in \mathbb{Z}_{\geq 0}\}$. Če je $char(F) = 0$, potem je očitno $\ker(D) = F$.

   (c) Firstly, let su show that the statement holds if $f(x) = x^n$. Without loss of generality, let us assume that $n \geq m$.
$$D(x^ng(x)) = D(x^n \cdot \sum_{i=0}^{m} b_ix^i) = \sum_{i=0}^{m}(i+n)b_ix^{i+n-1} = \sum_{i=0}^{m} ib_ix^{i+n-1} + \sum_{i=0}^{m} nb_ix^{i+n-1}$$

$$= x^n \sum_{i=0}^{m} i b_i x^{i-1} + n x^{n-1} \sum_{i=0}^{m} b_i x^i = x^n D(g(x)) + D(x^n) g(x)$$

We will prove the rest of the problem using mathematical induction on $\deg(f(x)g(x)) = d$. If $d = 0$, since $F[x]$ is a field, it follows that $D(f(x)) = D(g(x)) = 0$. Then

$$D(f(x)g(x)) = 0 = 0 \cdot g(x) + f(x) \cdot 0 = D(f(x))g(x) + f(x)D(g(x)).$$

Suppose now that the statement holds for $d = n-1 > 0$. Let us consider the case $d = n$. We denote with $f_{n-1}(x) = \sum_{i=0}^{n-1} a_i x^i$.

$$\begin{aligned}
D(f(x)g(x)) &= D((a_n x^n + f_{n-1}(x))g(x)) = D(a_n x^n g(x) + f_{n-1}(x)g(x)) \\
&= a_n D(x^n g(x)) + D(f_{n-1}(x)g(x)) \\
&= a_n \cdot (n x^{n-1} g(x) + x^n D(g(x))) + D(f_{n-1}(x))g(x) + f_{n-1}(x)D(g(x)) \\
&= (n a_n x^{n-1} + D(f_{n-1}(x)))g(x) + (x^n + f_{n-1}(x))D(g(x)) \\
&= D(f(x))g(x) + f(x)D(g(x))
\end{aligned}$$

1.5.4 Additional problems

1. Inspect the irreducibility of the following polynomials over $\mathbb{Q}$.

   (a) $x^2 + 4x + 2$

   (b) $x^4 - 10x^2 + 1$

   (c) $x^3 + 3x^2 + 6x + 3$

   (d) $x^3 - x^2 - 4$

   (e) $4x^3 - 2x^2 + x + 1$

   (f) $x^5 0 + 14x - 56$

2. Factorize the polynomials $f(x) = x^4 - 1$ and $g(x) = 4x^5 + 4x^4 - 13x^3 - 11x^2 + 10x + 6$ over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.
3. Find the quotient and remainder when dividing $f(x)$ with $g(x)$ in $\mathbb{Z}_n[x]$, if:

   (a) $f(x) = 4x^5 + 3x^2 + 2x + 4,\ g(x) = 2x^2 + 5,\ n = 7$

   (b) $f(x) = x^7 + 7x^5 + 3x^2 + 11x + 5,\ g(x) = x^4 + 3x^2 + 8x + 4,\ n = 13.$
4. Find all prime numbers p such that $x + 2$ is a factor of $x^4 + x^3 + x^2 - x + 1$ in $\mathbb{Z}_p[x]$.
5. Find all irreducible polynomials of degree 3 in $\mathbb{Z}_3[x]$.

1.6 Divisibility and reducibility in integral domains. Gaussian Rings.

1.6.1 Theoretical background

Prime and composite numbers in $\mathbb{Z}$ have different meanings in an Integral Domain!

Definition 1.6.1 If $a, b \in R$, R a commutative ring, we say that b **divides** a (denoted $b|a$) if there is an element $c \in R$ such that $a = bc$.

Definition 1.6.2 Let D be an integral domain, and $a, b, c \in D$.

1. If $a = ub$ for some unit u, then a and b are **associates** (denoted $a \sim b$).
2. A nonzero element a of an integral domain D is called **irreducible** if a is not a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit.
3. A nonzero element a of an integral domain D is called **prime** if a is not a unit and $a|bc$ implies $a|b$ or $a|c$.

Definition 1.6.3 Let D be an integral domain. The element $d \in D$ is a **common divisor** of the elements $a_1, \dots, a_n \in D$ if $d | a_i$ for all $i = 1, \dots, n$.

Definition 1.6.4 Let D be an integral domain and $a, b \in D$ We say that $d \in D$ is the **greatest common divisor** of a and b (denoted $\gcd(a,b) = d$) if d is a common divisor of a and b, and if p is a common divisor of a and b, then $p | d$.

Definition 1.6.5 Let D be an integral domain and $f(x), g(x) \in D[x]$ We say that $d(x) \in D[x]$ is the **greatest common divisor** of $f(x)$ and $g(x)$ if:

1. $d(x)$ is a common divisor of $f(x)$ and $g(x)$;
2. if $p(x)$ is a common divisor of $f(x)$ and $g(x)$, then $p(x) | d(x)$;
3. $d(x)$ is monic.

R If $1 \neq d \in \mathbb{Z}$ and d is not divisible by the square of a prime number, then $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ is an integral domain.

Definition 1.6.6 Let D be an integral domain. The mapping $N : D \to \mathbb{N}_0$ is called a **multiplicative norm** on D, if:

1. $N(a) = 0 \Leftrightarrow a = 0$
2. $N(ab) = N(a)N(b)$ for all $a, b \in D$

R The mapping $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}_0$ defined with $N(a + b\sqrt{d}) = |a^2 - db^2|$ is a multiplicative norm on $\mathbb{Z}[\sqrt{d}]$.

Proposition 1.6.1 Let N be a multiplicative norm on an integral domain D. Then

1. $N(x) = 1$ if and only if x is a unit in D.
2. If $N(x)$ is prime, then x is irreducible in D.

■ **Example 1.2** Let us find all the units in $D = \mathbb{Z}[\sqrt{-5}]$. We have that, $a + b\sqrt{-5} \in D$ is a unit if and only if $N(a + b\sqrt{-5}) = |a^2 + 5b^2| = a^2 + 5b^2 = 1$ in $\mathbb{Z}$. Thus, we have that $a = \pm 1$ and $b = 0$. In other words, -1 and 1 are the units in D. ■

Theorem 1.6.2 In an integral domain, every prime is an irreducible.

Proof. Suppose $p \in D$ is prime. Assume $p = ab$. Then $p | a$ or $p | b$. Without loss of generality, let $a = pt$ so that $p = ptb$. Since we are in an integral domain, the cancellation laws hold and it follows that $tb = 1$, i.e., b is a unit. ■

In general, the converse does not hold.

■ **Example 1.3** Let us consider the element $1 + \sqrt{5} \in \mathbb{Z}[\sqrt{5}]$. If $1 + \sqrt{5} = (a + b\sqrt{5})(c + d\sqrt{5})$, then

$$4 = N(1+\sqrt{5}) = N(a+b\sqrt{5})N(c+d\sqrt{5}) = |(a^2-5b^2)(c^2-5d^2)| \Rightarrow (a^2-5b^2)(c^2-5d^2) = \pm 4.$$

Let us consider $a^2 - 5b^2 = \pm 2$ in $\mathbb{Z}_4$, that is, $a^2 - b^2 = \pm 2$. For $x \in \mathbb{Z}_4$ we have that $x^2 \in \{0, 1\}$, but then $a^2 - b^2 \neq \pm 2$ for any $a, b \in \mathbb{Z}_4$. Hence, we must have $a^2 - 5b^2 = \pm 1$, i.e. $a + b\sqrt{5}$ is a unit. By definition, $1 + \sqrt{5}$ is irreducible.

To show that it is not a prime, we note that

$$1+\sqrt{5}|(1+\sqrt{5})(1-\sqrt{5}) = -4 = 2\cdot(-2).$$

If $1+\sqrt{5}|2$, then $(1+\sqrt{5})(a+b\sqrt{5}) = 2$ yields $a+b=0$ and $a+5b=2$. However, this would mean that $a=-\frac{1}{2}$, which is not possible. A similar conclusion follows, if $1+\sqrt{5}|-2$. Hence, $1+\sqrt{5}$ is not a prime. ■

Definition 1.6.7 An integral domain D is called a **Gaussian Ring** or a **Unique Factorisation Domain** (in short UFD) if the following holds:

1. every nonzero non-unit element $a \in D$ can be written as a finite product $a = a_1 \dots a_n$ of irreducible elements $a_1, \dots, a_n \in D$ and
2. the previous factorisation is unique up to the permutation of the factors and associativity of the elements: if $a = b_1 \dots b_m$ is another factorisation of a, then $m=n$ and there exists a permutation $\sigma \in S_n$ such that $a_i \sim b_{\sigma(i)}$ for all $1 \le i \le n$.

1.6.2 Problems

1. Find the $d(x) = \gcd(f(x), g(x)$ and express it as $d(x) = s(x)f(x)+t(x)g(x)$, if $f(x) = 2x^3+2x^2$ and $g(x) = x^4+2x^3+x$ in $\mathbb{Z}_3[x]$.
2. Show that there exists an integral domain which contains two elements that do not have a gcd.
3. Show that 5 is reducible in $\mathbb{Z}[i]$ and irreducible in $\mathbb{Z}[\sqrt{2}]$.
4. Let $D \neq 0$ be an integral domain such that each pair of nonzero elements from D are associated. Prove that D is a field.
5. Find the $\gcd(3, 1+i\sqrt{5})$ in $\mathbb{Z}[i\sqrt{5}]$.
6. In $\mathbb{Z}[\sqrt{-5}]$, there is no greatest common divisor of 6 and $2(1+\sqrt{-5})$.
7. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a Gaussian ring.

1.6.3 Solutions

1.

$$\begin{array}{r|l} & \qquad\qquad\quad 2x+2 \\ \hline 2x^3+2x^2+0x+0 & x^4+2x^3+0x^2+x+0 \\ & \underline{x^4+x^3+0x^2+0x} \quad \downarrow \\ & \qquad x^3+0x^2+x+0 \\ & \qquad \underline{x^3+x^2+0x+0} \\ & \qquad\quad 2x^2+x+0 \end{array} \qquad \begin{array}{r|l} & \qquad\qquad x+2 \\ \hline 2x^2+x+0 & 2x^3+2x^2+0x+0 \\ & \underline{2x^3+x^2+0x} \quad \downarrow \\ & \qquad x^2+0x+0 \\ & \qquad \underline{x^2+2x+0} \\ & \qquad\qquad x+0 \end{array}$$

$$\begin{array}{ll} q_1(x) = 2x^2+2,\ r_1(x) = 2x^2+x & g(x) = q_1(x)f(x)+r_1(x) \\ q_2(x) = x+2,\ r_2(x) = x & f(x) = q_2(x)r_1(x)+r_2(x) \\ q_3(x) = 2x+1,\ r_3(x) = 0 & r_1(x) = q_3(x)r_2(x) \end{array}$$

Hence, we have that

$$r_2(x) = f(x) - q_2(x)r_1(x) = f(x) - q_2(x)(g(x) - q_1(x)f(x))$$

$$\begin{aligned} &= (1-q_1(x)q_2(x))f(x) - q_2(x)g(x) \\ x &= (2x^2+2)f(x) + (2x+1)g(x) \end{aligned}$$

2. Let F be a field. With S we denote the subset

$$S = \{\sum_{i=0}^{n} a_i x^i \in F[x] : n \in \mathbb{N}, a_1 = 0\}$$

consisting of all polynomials in $F[x]$ without the linear factor.
We claim that S is a integral subdomain of $F[x]$. It suffices to show that S is a subring. Let $f(x), g(x) \in S$ be arbitrary.
   - $0 \in S$
   - $f(x) - g(x) \in S(x)$, since $a_1 - b_1 = 0 - 0 = 0$
   - $f(x)g(x) \in S(x)$, since $a_1 b_0 - a_0 b_1 = 0$

   Thus, by the Subring Test, it follows that $S \leq F[x]$, i.e., S is an integral domain. Let us consider the elements $x^5, x^6 \in S$.
The monic divisors of x^5 are $1, x^2$ and x^3. The monic divisors of x^6 are $1, x^2, x^3$ and x^4. The common ones are $1, x^2$ and x^3. However there is not a greatest common divisors because the 2. condition of the definition is not satisfied ($x^2 \nmid 1$, $x^3 \nmid x^2$, $x^2 \nmid x^3$).
3. The units in $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$. Since $5 = (2+i)(2-i)$ and $N(2+i) = N(2-i) = 5$ is prime, 5 can be written as a product of irreducible elements (remember, by definition, irreducible elements are **non-units**) in $\mathbb{Z}[i]$ and thus, 5 is reducible in $\mathbb{Z}[i]$.
The units in $\mathbb{Z}[\sqrt{2}]$ are

$$\{a+b\sqrt{2} : N(a+b\sqrt{2}) = 1\} = \{a+b\sqrt{2} : a^2 - 2ab^2 = \pm 1\}.$$

If 5 is reducible in $\mathbb{Z}[\sqrt{2}]$, then we would have that

$$5 = (a+b\sqrt{2})(c+d\sqrt{2}) \Rightarrow 25 = N(a+b\sqrt{2})N(c+d\sqrt{2}) = |(a^2-2b^2)(c^2-2d^2)|.$$

Since $a^2 - 2b^2, c^2 - 2d^2 \in \mathbb{Z}$ we have the following cases:
(i) $a^2 - 2b^2 = \pm 5$. If we consider this equation in $\mathbb{Z}_5$, we have that $a^2 - 2b^2 = 0$. From the table:

a,b	$a^2, b^2 \pmod 5$	$2b^2 \pmod 5$
0	0	0
1	1	2
2	4	3
3	4	3
4	1	2

we see that $a^2 - 2b^2 \mod 5 = 0$ only if $a = b = 0$. Which means that in $\mathbb{Z}$ we have that a and b are divisible with 5. We conclude:

$$25 | a^2, b^2 \Rightarrow 25 | (a^2 - 2b^2) \Rightarrow 25 | \pm 5 \ \lightning.$$

(ii) $a^2 - 2b^2 = \pm 1$. Then $a + b\sqrt{2}$ is a unit.
(iii) $a^2 - 2b^2 = \pm 25$. Then $c^2 - 2d^2 = \pm 1$, that is, $c + d\sqrt{2}$ is a unit.

We conclude that 5 is a product of two elements, out of which at least one is a unit. Hence, 5 is irreducible in $\mathbb{Z}[\sqrt{2}]$.

4. If $a \neq 0$ is an element of D, then by hypothesis, a and a^2 must be associates in D. Then $a^2 = au$ for a suitable unit $u \in D$. Hence, $a(a-u) = 0$. Since we are in an integral domain and $a \neq 0$ we have that $a - u = 0$. So, each nonzero element in D is a unit. Thus, D is a field.
5. If $d = \gcd(3, 1+i\sqrt{5})$ in $\mathbb{Z}[i\sqrt{5}]$, then $N(d)$ divides $N(3) = 9$ and $N(d)$ divides $N(1+i\sqrt{5}) = 6$. Thus, $N(d) \in \{1,3\}$. If we consider $a^2+5b^2 = 3$ in $\mathbb{Z}_5$, then we have $a^2 = 3$. However, 3 is not a square in $\mathbb{Z}_5$. Hence, we must have $N(d) = 1$, that is, d is a unit in $\mathbb{Z}[i\sqrt{5}]$. The units in $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1, hence $1 = \gcd(3, 1+i\sqrt{5})$.
6. We note that $N(6) = 36$ and $N(2(1+\sqrt{-5})) = 24$. If $x+y\sqrt{-5} = d = \gcd(6, 2(1+\sqrt{-5}))$, then $N(d)|36$ and $N(d)|24$. Thus we have that $N(d) \in \{1,2,3,4,6,12\}$. On the other hand, 2 divides $2(1+\sqrt{-5})$ and $1+\sqrt{-5}$ divides 6 ($6 = (1+\sqrt{-5})(1-\sqrt{-5})$). Hence, $N(2) = 4$ and $N(1+\sqrt{-5}) = 6$ divide $N(d)$. It follows that $N(d) = 12$. If we consider the equation $a^2+5b^2 = 12$ in $\mathbb{Z}_5$, then $a^2 = 2$. However, 2 is not a square in $\mathbb{Z}_5$. Hence, there are no $a, b \in \mathbb{Z}$ such that $a^2+5b^2 = 12$. In other words, the $\gcd(6, 2(1+\sqrt{-5}))$ does not exist.
7. Any element of the ring $\mathbb{Z}[\sqrt{-5}]$ is of the form $a+b\sqrt{-5}$ for some integers a, b. The associated norm N is given by

$$N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2.$$

Consider the case when $a = 2, b = 1$. Then we have

$$(2+\sqrt{-5})(2-\sqrt{-5}) = 9 = 3\cdot 3. \tag{1.2}$$

We claim that the numbers $3, 2\pm\sqrt{-5}$ are irreducible elements in the ring $\mathbb{Z}[\sqrt{-5}]$. To prove the claim at once, **we show that any element in $\mathbb{Z}[\sqrt{-5}]$ of norm 9 is irreducible**.

Let α be an element in $\mathbb{Z}[\sqrt{-5}]$ such that $N(\alpha) = 9$. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$. Out goal is to show that either β or γ is a unit. We have

$$9 = N(\alpha) = N(\beta)N(\gamma).$$

Since the norms are nonnegative integers, $N(\beta)$ is one of $1, 3, 9$. If $N(\beta) = 1$, then it yields that β is a unit. If $N(\beta) = 3$, then we write $\beta = a+b\sqrt{-5}$ for some integers a, b, and we obtain

$$3 = N(\beta) = a^2+5b^2.$$

A quick inspection yields that there are no integers a, b satisfying this equality. Thus $N(\beta) = 3$ is impossible. If $N(\beta) = 9$, then $N(\gamma) = 1$ and thus γ is a unit. Therefore, we have shown that either β or γ is a unit. Note that the elements $3, 2\pm\sqrt{-5}$ have norm 9, and hence they are irreducible by what we have just proved.

Since the units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, obviously $3 \nsim 2\pm\sqrt{-5}$. In other words, the factorisation is not unique. Thus, the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

1.6.4 Additional problems

1. Find the gcd for the listed pairs of polynomials over the given field:

(a) $f_1(x) = x^3 - x^2 - x + 1,\ g_1(x) = x^4 - 3x^2 - 2x + 4$ over $\mathbb{Q}$
(b) $f_2(x) = x^4 + 3x^2 + 4x,\ g_2(x) = 2x^2 - 2x - 4$ over $\mathbb{Q}$
(c) $f_3(x) = x^5 + 3x^3 + x^2 + 2x + 2,\ g_3(x) = x^4 + 3x^3 + 3x^2 + x + 2$ over $\mathbb{Z}_5$

For every pair of polynomials $f_i(x)$ and $g_i(x)$, express the gcd as $s_i(x)f_i(x) + t_i(x)g_i(x)$, $i = 1,2,3$.

2. Find the associates of $a + ib \in \mathbb{Z}[i]$.
3. What are the irreducible elements in $\mathbb{Z}$?
4. Which of the integers $\{2,3,5,7,11,13,17,19\}$ are irreducible in $\mathbb{Z}[\sqrt{5}]$?
5. Is 2 prime in $\mathbb{Z}[\sqrt{-5}]$?
6. Prove that in an integral domain D with multiplicative norm N, it holds that $N(1) = 1$ and $N(u) = 1$ for every unit $u \in D$.
7. Prove that $N(a + b\sqrt{-5}) = a^2 + 5b^2$ defines a norm on $\mathbb{Z}[\sqrt{-5}]$.
8. Show that $\mathbb{Z}[\sqrt{-6}]$ is not a UFD (Hint: Consider the element 10).
9. Show that $\sqrt{-2}, 1 - \sqrt{-2}, 1 + \sqrt{-2}, 5$ and 7 are all irreducible in $\mathbb{Z}[\sqrt{-2}]$.
10. In the ring $\mathbb{Z}[\sqrt{2}]$, show that 5 is a prime but 7 is not.
11. Show that there are infinitely many units in $\mathbb{Z}[\sqrt{2}]$. (Hint: Consider the element $(1 + \sqrt{2})^n$, $n \in \mathbb{N}$).
12. Find $\gcd(5, 1 + 3i)$ in $\mathbb{Z}[i]$.
13. In the ring $R = \mathbb{Z}[\sqrt{-6}]$ verify that the following hold:
    (a) there are no elements of norm equal to 2 or 5;
    (b) the elements $2, 5, 2 - \sqrt{-6}$ are irreducible but not prime;
    (c) $\gcd(5, 2 + \sqrt{-6}) = 1$, where 1 is the unity in R;
    (d) $\gcd(10, 4 + 2\sqrt{-6})$ does not exist.

2. Ideals and Factor Rings

2.1 Homomorphisms and Factor Rings. Ideals.

2.1.1 Theoretical background

In Section 1.1 we have already introduced the notion and basic properties of ring homomorphisms. Similarly as one defines factor groups in group theory, we can talk about their analogue, factor (quotient) rings in ring theory. Before we define them, we state the following useful theorems.

Theorem 2.1.1 Let $\phi : R \to R'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by

$$(a+H)+(b+H)=(a+b)+H \tag{2.1}$$

and the product of cosets is defined by

$$(a+H)(b+H)=(ab)+H. \tag{2.2}$$

Also, the map $\mu : R/H \to \phi[R]$ defined by $\mu(a+H)=\phi(a)$ is an isomorphism.

In the following theorem we characterize exactly those H for which (2.2) is well-defined.

Theorem 2.1.2 Let H be a subring of R. Multiplication of additive cosets of H is well defined by the equation

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

if and only if $ah \in H$ and $hb \in H$ for all $a,b \in R$ and $h \in H$.

In group theory, normal subgroups are precisely the type of substructure of groups required to form a factor group with a well-defined operation on cosets given by operating with chosen representatives.

From Theorem 2.1.2, we see that in ring theory, the analogous substructure must be subring H of R such that $aH \subseteq H$ and $Hb \subseteq H$ for all $a, b \in R$, where $aH = \{ah : h \in H\}$ and $Hb = \{hb : h \in H\}$. From now on we will use N rather than H, so that we known we are talking about the ring analogous of normal subgroups. Fro this purpose, we define the following important structure.

Definition 2.1.1 An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \ \wedge \ Nb \subseteq N, \ \forall a, b \in R$$

is called an (two-sided) **ideal**.

R If $RN \subseteq N$ ($NR \subseteq N$) we say that N is a **left** (**right**) ideal of R.

Theorem 2.1.3 $N \subseteq R$ is a left (right) ideal in R if and only if the following hold:
(i) $0 \in N$
(ii) $a - b \in N, \ \forall a, b \in N$
(iii) $na \in N \ (an \in N), \ \forall n \in N, \ a \in R$

R Obviously every ideal in a ring R (left, right or two-sided) is a subring of R.

We are now able to define factor rings.

Corollary 2.1.4 Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with the binary operations defined by (2.1) and (2.2), for $N = H$.

Definition 2.1.2 The ring R/N in the preceding corollary is the **factor ring** (or **quotient ring**) **of R by N.**

R Do not confuse the term *quotient ring* with the notion of *field of quotients* of an integral domain.

To conclude, we note the following important and useful result.

Theorem 2.1.5 Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then $\phi[R]$ is a ring, and the map $\mu : R/N \to \phi[R]$ given by $\mu(x+N) = \phi(x)$ is an isomorphism. If $\gamma : R \to R/N$ is the ring homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$, we have that $\phi(x) = \mu(\gamma(x))$.

2.1.2 Problems

1. Find all ideals of the ring $\mathbb{Z}$. Is $\mathbb{Z}$ an ideal in $\mathbb{Q}$?
2. Let K be a ring with unity 1 and J an arbitrary (one or two-sided) ideal in K. Prove:
   (a) If $1 \in J$, then $J = K$.
   (b) If K is an arbitrary field, then 0 and K are the only ideals in K.
3. Find all ideals in the ring $\mathbb{Z}_{18}$. Generalize to $\mathbb{Z}_n$.
4. Let R and R' be rings and I' and ideal in R'. Let $f^{-1}(I') = I$ be the preimage of I' by f. Show that I is an ideal in R.
5. Let R and R' be commutative rings and let $f : R \to R'$ be a ring homomorphism. Let I and I' be ideals of R and R', respectively.
   (a) Prove that $f(\sqrt{I}) \subset \sqrt{f(I)}$[1]
   (b) Prove that $\sqrt{f^{-1}(I')} = f^{-1}(\sqrt{I'})$
   (c) Suppose that f is surjective and $\ker(f) \subset I$. Then prove that $f(\sqrt{I}) = \sqrt{f(I)}$
6. Is it true that a set of nilpotent elements in a commutative ring R is an ideal of R. Can we omit the word 'commutative".
7. Suppose that $f : R \to R'$ is a surjective ring homomorphism. Prove that if R is a Noetherian[2] ring, then so is R'.
8. Let R be a ring and I its ideal. Prove that the quotient ring R/I is commutative if and only if $(rs - sr) \in I$ for every $r, s \in R$.
9. Let R be a ring with unity and I a left ideal in R. If some element $a \in I$ has a left multiplicative inverse, prove that then $I = R$.
10. Let $R = \left\{ \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} : u, v \in \mathbb{Q} \right\}$ a ring with standard addition and multiplication of matrices. Show that $I = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{Q} \right\}$ is an ideal in R. Prove that the quotient ring R/J is isomorphic to $\mathbb{Q}$.

2.1.3 Solutions

1. Let I be an ideal in $\mathbb{Z}$. Then I is a subring of $\mathbb{Z}$. Hence, $(I, +) \leq (\mathbb{Z}, +) \Rightarrow I = m\mathbb{Z}$ for some $m \in \mathbb{N}_0$.
   Claim: I is an ideal in $\mathbb{Z}$ if and only if $I = m\mathbb{Z},\ m \in \mathbb{N}_0$.
   $\boxed{\Rightarrow}$ Already confirmed.
   $\boxed{\Leftarrow}$ Let $I = m\mathbb{Z}$ for an arbitrary $m \in \mathbb{N}_0$. Since I is a subring of $\mathbb{Z}$, we have that (i) and (ii) from Theorem 2.1.3 hold. It remains to show (iii). Let $x \in \mathbb{Z}$ and $y \in m\mathbb{Z}$ be arbitrary.

$$\begin{aligned}
&\Rightarrow y = m\tilde{y},\ \tilde{y} \in \mathbb{Z} \\
&\Rightarrow xy = xm\tilde{y} = m(x\tilde{y}) \in m\mathbb{Z} \\
& yx = m\tilde{y}x = m(\tilde{y}x) \in m\mathbb{Z} \\
&\Rightarrow I \text{ is an ideal in } \mathbb{Z}
\end{aligned}$$

   Since $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$, we have that (i) and (ii) from Theorem 2.1.3 hold. Let us check (iii). If we take $x = 2 \in \mathbb{Z}$ and $y = \frac{1}{3} \in \mathbb{Q}$ we have that $yx = \frac{2}{3} \notin \mathbb{Z}$. Hence, $\mathbb{Z}$ is not an ideal in $\mathbb{Q}$.

[1] For an ideal I in R we define its **radical ideal** $\sqrt{I}$ as $\sqrt{I} = \{a \in R : a^n \in I \text{ for some } n \in \mathbb{N}\}$.

[2] A ring R is said to be **Noetherian** if for an increasing chain of ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$ in R there exists such a number $N \in \mathbb{N}$ for which $I_N = I_{N+1} = \ldots$.

2. (a) Let us take an arbitrary $k \in K$. Since $k = k \cdot 1$ and $1 \in J$, it follows that $k \in J$ (since J is an ideal in K). Hence, $K \subseteq J$. Obviously, $J \subseteq K$ and thus we must have that $J = K$.

   (b) Let J be an arbitrary ideal. If $J = \{0\}$, we are done. Suppose that $J \neq \{0\}$. Hence, there exists an element $0 \neq x \in J$. Since F is a field, we can find its inverse $x^{-1} \in F$. So $x^{-1} \cdot x = 1 \in J$. From (a) we must have that $J = K$.

3. Every ideal in a ring is also a subring and as such it is an additive subgroup in the additive group of the ring. The cyclic group $\mathbb{Z}_{18}$ contains the following subgroups:

$$\{0\} = 18\mathbb{Z}_{18},\ 9\mathbb{Z}_{18},\ 6\mathbb{Z}_{18},\ 3\mathbb{Z}_{18},\ 2\mathbb{Z}_{18},\ \mathbb{Z}_{18}.$$

For reader: Confirm that al of the above sets are indeed ideals in $\mathbb{Z}_{18}$.

Generalization: For every $n \in \mathbb{N}$, the ideals in $\mathbb{Z}_n$ are exactly the sets $k\mathbb{Z}_n$, where k is a divisor of n.

Proof. Let I be an arbitrary ideal in $\mathbb{Z}_n$. We know that $(I,+) \leq (\mathbb{Z}_n,+)$. Since (the additive group) $\mathbb{Z}_n$ is cyclic, all of its subgroups are cyclic as well. Moreover, we know that all of them are of the form $k\mathbb{Z}_n$, where k is a divisor of n. Let $x \in \mathbb{Z}_n$ and $y \in k\mathbb{Z}_n$ be arbitrary. We have that

$$y = k\tau,\ \tau \in \mathbb{Z}_n \Rightarrow xy = yx = k \cdot (x\tau) \in k\mathbb{Z}_n.$$

Hence, $I = k\mathbb{Z}_n$ for all $k \in \mathbb{N}$ such that $k|n$.

4. We need to show two things: $(I,+) \leq (R,+)$ and $IR, RI \subseteq I$.
   - Let $a,b \in I$ be arbitrary. From here, we have that $f(a), f(b) \in I'$. Since I' is an ideal, it follows that $f(a) - f(b) \in I'$. Furthermore, f is a ring homomorphism and thus $f(a-b) \in I'$. This implies that $a - b \in f^{-1}(I') = I$.
   - Let $a \in I$ and $r \in R$ be arbitrary. Since $f(a) \in I', f(r) \in R'$ and from the fact that I' is an ideal in R', we have that $f(r)f(a) \in I'$, $f(a)f(r) \in I'$. Furthermore, f is a homomorphism and thus $f(ra), f(ar) \in I'$. Hence, $ra, ar \in f^{-1}(I') = I$.

   In other words, I is an ideal in R.

5. (a) Let $x \in f(\sqrt{I})$ be arbitrary. Then there exists an element $a \in \sqrt{I}$ such that $f(a) = x$. Since $a \in \sqrt{I}$, there exists an integer $n \in \mathbb{N}$ such that $a^n \in I$. Hence, since f is a homomorphism, it follows that $x^n = f(a)^n = f(a^n) \in f(I)$. In other words, $x \in \sqrt{f(I)}$, i.e., $f(\sqrt{I}) \subseteq \sqrt{f(I)}$.

   (b) $\boxed{\subseteq}$ Let $x \in \sqrt{f^{-1}(I')}$ be arbitrary. It follows that:

$$\begin{aligned}(\exists n \in \mathbb{N})\ x^n \in f^{-1}(I') &\Rightarrow f(x^n) \in I' \\ &\Rightarrow f(x)^n \in I'\ (f \text{ homomorphism}) \\ &\Rightarrow f(x) \in \sqrt{I'}\end{aligned}$$

   $\boxed{\supseteq}$ Let $x \in f^{-1}(\sqrt{I'})$ be arbitrary. It follows that:

$$\begin{aligned}f(x) \in \sqrt{I'} &\Rightarrow (\exists n \in \mathbb{N})\ f(x)^n \in I' \\ &\Rightarrow f(x^n) \in I' \\ &\Rightarrow x^n \in f^{-1}(I') \Rightarrow x \in \sqrt{f^{-1}(I')}\end{aligned}$$

   Hence, $f^{-1}(\sqrt{I'}) = \sqrt{f^{-1}(I')}$.

(c) $\boxed{\subseteq}$ Follows from (a).

$\boxed{\supseteq}$ Let $x \in \sqrt{f(I)} \subseteq R'$ be arbitrary. This means that there exists an integer $n \in \mathbb{N}$ such that $x^n \in f(I)$, i.e., there exists an element $a \in I$ such that $x^n = f(a)$. Because f is surjective, we know that there exists an element $y \in R$ such that $f(y) = x$. In other words

$$f(a) = x^n = f(y)^n = f(y^n) \Rightarrow f(a) - f(y^n) = 0 \Rightarrow f(a - y^n) = 0 \Rightarrow a - y^n \in \ker(f) \subseteq I.$$

Since $a \in I$, we must also have that $y^n \in I$, that is, $y \in \sqrt{I}$. From this, we have that $f(y) = x \in f(\sqrt{I})$, i.e., $\sqrt{f(I)} \subseteq f(\sqrt{I})$. Hence, $f(\sqrt{I}) = \sqrt{f(I)}$.

6. With $N(R) = \{x \in R : (\exists n \in \mathbb{N})\ x^n = 0\}$ we denote the set of all nilpotent elements in R. Obviously, $0 \in N(R)$. Let $x \in N(R)$ and $a \in R$ be arbitrary. Thus, there exists an integer $n \in \mathbb{N}$ such that $x^n = 0$. But then also, $a^n x^n = 0 \Leftrightarrow (ax)^n = (xa)^n = 0$ (R commutative). In other words, $ax, xa \in N(R)$. Let now $x, y \in N(R)$ be arbitrary. Hence, $x^n = 0$ and $y^m = 0$ for some $n, m \in \mathbb{N}$. We have that, since R is commutative,

$$(x - y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = 0,$$

if $p - k \geq n$ and $k \geq m$. In other words, $p \geq n + m$. So, $(x - y)^{n+m} = 0$, that is, $x - y \in N(R)$. We conclude that $N(R)$ is indeed an ideal in R.

If R is not commutative, then $N(R)$ is not necessarily an ideal in R. Counterexample: Let R be the ring of 2×2 real matrices. Take

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R.$$

It is easy to compute that $A^2 = 0$ and $B^2 = 0$, i.e. $A, B \in N(R)$. However, $A + B$ is not a nilpotent because

$$(A + B)^n = \begin{cases} A + B, & n = 2k + 1 \\ I_2, & n = 2k \end{cases}, \; k \in \mathbb{N}$$

7. Let $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$ be an increasing chain of ideals in R'. From Problem 4 it follows that the preimages $f^{-1}(I_k)$ of the ideals I_k under the homomorphism f are ideals in R. Hence, we get an increasing chain of ideals in R

$$f^{-1}(I_1) \subseteq f^{-1}(I_2) \subseteq \ldots \subseteq f^{-1}(I_k) \ldots$$

Since R is Noetherian, there exists an integer $N \in \mathbb{N}$ such that

$$f^{-1}(I_N) = f^{-1}(I_{N+1}) = \ldots$$

Since f is a surjective homomorphism, it holds that

$$f(f^{-1}(I_k)) = I_k,$$

for every $k \in \mathbb{N}$. Thus, we obtain that

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

In other words, R' is Noetherian.

8.

$$\begin{aligned} R/I \text{ commutative } &\Leftrightarrow (r+I)(s+I) = (s+I)(r+I),\ \forall r,s \in R \\ &\Leftrightarrow rs+I = sr+I,\ \forall r,s \in R \\ &\Leftrightarrow (rs+I)-(sr+I) = I,\ \forall r,s \in R\ (0_{K/I} = I) \\ &\Leftrightarrow (rs-sr)+I = I,\ \forall r,s \in R \\ &\Leftrightarrow rs-sr \in I,\ \forall r,s \in R \end{aligned}$$

9. Let I be a left ideal in R and let $a \in I$ be a unit. Thus, there exists $a^{-1} \in R$. Since I is a left ideal, it holds that $aa^{-1} = 1 \in I$. From Problem 2a it follows that $I = R$.

10. Let

$$\alpha = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \beta = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in I$$

be arbitrary. Since $0, \alpha - \beta \in I$. It follows that I is an additive group. Let

$$\gamma = \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} \in R$$

be arbitrary. Since

$$\begin{aligned} \gamma\alpha &= \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & ua \\ 0 & 0 \end{bmatrix} \in I \text{ and} \\ \alpha\gamma &= \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} = \begin{bmatrix} 0 & au \\ 0 & 0 \end{bmatrix} \in I, \end{aligned}$$

we conclude that I is an ideal in R. Let us define a mapping $\phi : R \to \mathbb{Q}$ with

$$\phi\left(\begin{bmatrix} u & v \\ 0 & u \end{bmatrix}\right) = u.$$

For reader: Show that ϕ is a ring homomorphism.

Let us compute $\ker(\phi)$ and $\operatorname{im}(\phi)$. **Claim:** $\ker(\phi) = I$.

$\boxed{\subseteq}$ Let

$$\rho = \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} \in \ker(\phi)$$

be arbitrary. Then $\phi(\rho) = u = 0$. Thus,

$$\rho = \begin{bmatrix} 0 & v \\ 0 & 0 \end{bmatrix} \in I \Rightarrow \ker(\phi) \subseteq I.$$

$\boxed{\supseteq}$ Let

$$\begin{bmatrix} 0 & v \\ 0 & 0 \end{bmatrix} \in I$$

be arbitrary. Since $\phi(\rho) = 0$, it follows that $\rho \in \ker(\phi)$. That is, $I \subseteq \ker(\phi)$. We conclude that $I = \ker(\phi)$. Obviously, since ϕ is a surjective mapping, we have that $\operatorname{im}(\phi) = \mathbb{Q}$. From Theorem 2.1.5 we conclude that

$$R/\ker(\phi) \cong \operatorname{im}(\phi) \Leftrightarrow R/I \cong \mathbb{Q}.$$

2.1.4 Additional problems

1. Let R be a commutative ring and $a \in R$. Show that $I_a = \{x \in R : ax = 0\}$ is an ideal of R.
2. Show that a countable intersection of ideals in a ring R is again an ideal in R.
3. If $S = \left\{ \left[\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right] : a, b \in \mathbb{R} \right\}$, prove that the mapping
$$f : \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mapsto a$$
is a ring homomorphism of the ring S onto $\mathbb{R}$. Find the kernel $\ker(f)$ and the factor ring $S/\ker(f)$.
4. Show that the factor ring $R/N(R)$, where $N(R)$ is the ideal of nilpotent elements in R, does not contain nilpotent elements.
5. Let R be a ring and I an ideal in R. If $a \in R$, prove that $A = \{r \in R : ra - ar \in I\}$ is a subring of R.
6. Let R be a commutative ring with unity in which every element is either nilpotent or a unit. Prove that $R/N(R)$ is a field, where $N(R)$ is the ideal of nilpotent elements in R.
7. Prove that the ring $F^{n \times n}$ of $n \times n$, $n \geq 2$, matrices over the field F has only trivial ideals.
8. Let R be a ring without zero divisors in which every subring is an ideal. Prove that R is commutative.
9. Let I be an ideal in a commutative ring R.
   (a) Show that $\sqrt{I} = \{r \in R : (\exists n \in \mathbb{N})\ r^n \in I\}$ is an ideal too.
   (b) Verify the following equalities: $\sqrt{\sqrt{I}} = \sqrt{I}$, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ and $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

2.2 Maximal, principle and prime ideals

2.2.1 Theoretical background

In this section we will discus the notion of ideals in integral domains and fields.

Definition 2.2.1 Let R be a ring. An ideal $P \neq R$ is said to be **prime**, if for all $a, b \in R$ it holds:
$$ab \in P \Rightarrow a \in P \ \vee\ b \in P.$$

■ **Example 2.1** The zero ideal in any integral domain is prime since $ab = 0$ if and only if $a = 0$ or $b = 0$. If p is a prime integer, then the ideal $p\mathbb{Z}$ is prime since $ab \in p\mathbb{Z}$ means that $p|ab$, which implies that either $p|a$ or $p|b$, or equivalently, $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. ■

Definition 2.2.2 A proper ideal $M \subset R$ of a ring $R \neq 0$ is said to be **maximal**, if for any ideal I in R such that $M \subseteq I \subseteq R$, it follows that either $I = M$ or $I = R$.

■ **Example 2.2** The ideal $3\mathbb{Z}$ is maximal in $\mathbb{Z}$, but the ideal $4\mathbb{Z}$ is not since $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$.
■

Theorem 2.2.1 Let R be a commutative ring with unity. Then the following hold:
1. R/P is an integral domain if and only if P is a prime ideal in R.

2. R/M is a field if and only if M is a maximal ideal in R.
3. Every maximal ideal of R is a prime ideal.

Definition 2.2.3 If R is a commutative ring with unity and $a \in R$, the ideal $\{ra : r \in R\}$ of all multiples of a is the **principle ideal generatred by** a and is denoted with $\langle a \rangle$. An ideal N of R is a **principle ideal** if $N = \langle a \rangle$ for some $a \in R$.

Definition 2.2.4 An integral domain in which every ideal is principle is called a **principle ideal domain** (**PID**).

Theorem 2.2.2 Let F be a field. Then the following hold:

1. Every ideal in $F[x]$ is principal.
2. An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.

Noehter's Isomorphism Theorems:

Theorem 2.2.3 — First Isomorphsim Theorem. If $f : R \to R'$ is a ring homomorphism. Then:

1. $\ker(f)$ is an ideal of R.
2. $\operatorname{im}(f)$ is a subring of R'.
3. $R/\ker(f) \cong \operatorname{im}(f)$.

In particular, if f is surjective, then $R/\ker(f) \equiv R'$.

Theorem 2.2.4 — Second Isomorphism Theorem. Let R be a ring, S a subring of R and I an ideal of R. Then:

1. The sum $S+I = \{s+i : s \in S, i \in I\}$ is a subring of R,
2. $S \cap I$ is an ideal of S.
3. $(S+I)/I \cong S/(S \cap I)$.

Theorem 2.2.5 — Third Isomorphism Theorem. Let R be a ring and let A, B be ideals of R, with $B \subseteq A \subseteq R$. Then:

1. The set A/B is an ideal of the quotient ring R/B.
2. $(R/B)/(A/B) \cong R/A$.

2.2.2 Problems

1. Find all prime and maximal ideals in $\mathbb{Z}_6$.
2. Find all prime and maximal ideals in $\mathbb{Z}_{12}$.
3. Find all prime and maximal ideals in $\mathbb{Z}_2 \times \mathbb{Z}_2$.
4. Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/\langle x^3 + c \rangle$ is a field.
5. Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/\langle x^3 + x^2 + c \rangle$ is a field.
6. Let F be a field and $f(x), g(x) \in F[x]$. Show that $f(x)$ divides $g(x)$ if and only if $g(x) \in \langle f(x) \rangle$.
7. Prove that in a commutative ring with unity R a proper ideal M is maximal if and only if for every $r \notin M$ there exists an element $x_r \in R$ such that $1 + rx_r \in M$.

8. Let R be a commutative ring with unity $1 \neq 0$. Suppose that for each element $a \in R$ there exists a positive integer n such that $a^n = a$. Prove that every prime ideal is maximal.
9. Show that the ideal $P = \langle 2, \sqrt{10} \rangle = \{a + b\sqrt{10} | a, b \in \mathbb{Z}, 2|a\}$ of the ring $\mathbb{Z}[\sqrt{10}]$ is prime.
10. Let R be a PID. Let $a \in R$ be a nonzero, non-unit element. Show that the following are equivalent:
    (a) The ideal $\langle a \rangle$ is maximal.
    (b) The ideal $\langle a \rangle$ is prime.
    (c) The element a is irreducible.
11. In a PID, any irreducible element is a prime element.

2.2.3 Solutions

1. We know that every ideal in $\mathbb{Z}_n$ is exactly of the form $k\mathbb{Z}_n$, where $k|n$. Because a finite integral domain is a field, the prime and the maximal ideals coincide.

Ideals in $\mathbb{Z}_6$	Prime Ideal	Maximal Ideal
$\mathbb{Z}_6$	YES	NO
$2\mathbb{Z}_6 = \{0,2,4\}$	YES	YES
$3\mathbb{Z}_6 = \{0,3\}$	YES	YES
$6\mathbb{Z}_6 = \{0\}$	NO	NO

We note the following useful theorem:

Theorem 2.2.6 $\mathbb{Z}_n/\langle d \rangle$ is an integral domain if and only if $d \neq n$ is prime.

2.

Ideals in $\mathbb{Z}_{12}$	Prime Ideal	Maximal Ideal
$\mathbb{Z}_{12}$	NO	NO
$2\mathbb{Z}_{12}$	YES	YES
$3\mathbb{Z}_{12}$	YES	YES
$4\mathbb{Z}_{12}$	NO	NO
$6\mathbb{Z}_{12}$	NO	NO
$12\mathbb{Z}_{12} = \{0\}$	NO	NO

3. If R and S are rings with unity, then every ideal in $R \times S$ is of the form $I \times J$ where I and J are ideals in R and S, respectively.

Ideals in $\mathbb{Z}_2 \times \mathbb{Z}_2$	Prime Ideal	Maximal Ideal
$\{0\} \times \{0\}$	NO	NO
$\{0\} \times \mathbb{Z}_2$	YES	YES
$\mathbb{Z}_2 \times \{0\}$	YES	YES
$\mathbb{Z}_2 \times \mathbb{Z}_2$	NO	NO

We note the following:

R Let R and S be rings, I and J ideals of R and S respectively. Then

$$(R \times S)/(I \times J) \cong (R/I) \times (S/J). \tag{2.3}$$

From (2.3) we have that $(\mathbb{Z}_2\times\mathbb{Z}_2)/(\{0\}\times\mathbb{Z}_2)\cong\mathbb{Z}_2$ and $(\mathbb{Z}_2\times\mathbb{Z}_2)/(\mathbb{Z}_2\times\{0\})\cong\mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field, from Theorem 2.2.1, it follows that $\mathbb{Z}_2\times\{0\}$ and $\{0\}\times\mathbb{Z}_2$ are maximal, and also prime.

4. From Theorems 2.2.2 and 2.2.1, if F is a field and $f(x)\in F[x]$, we have that

$$F/\langle f(x)\rangle \text{ is a field } \Leftrightarrow \langle f(x)\rangle \text{ is maximal } \Leftrightarrow f(x) \text{ is irreducible over } F$$

Hence, we need to find all $c\in\mathbb{Z}_3$ such that $f(x)=x^3+c$ is irreducible over $\mathbb{Z}_3$. By inspecting the values for $c=0,1$ and 2, we observe that only for no value of c we have that f is irreducible.

5. Similarly as in the previous problem, we need to determine all $c\in\mathbb{Z}_3$ for which the polynomial $f(x)=x^3+x^2+c$ is irreducible over $\mathbb{Z}_3$. The preceding is satisfied only for $c=2$.

6.
$$f(x)|g(x)\Leftrightarrow(\exists q(x)\in F[x])g(x)=f(x)q(x)\Leftrightarrow g(x)\in\langle f(x)\rangle.$$

R Every nonzero polynomial $g(x)\in\langle f(x)\rangle$ is of degree at least $\deg(f)$.

7. $\boxed{\Rightarrow}$ Let M be a maximal ideal. Then for $r\notin M$, $M+rR=R$, since $M+rR$ is an ideal which properly contains M. Thus, for some $m\in M$ and $x\in R$ we must have $m+rx=1$, in other words, if we denote with $x_r=-x$, we obtain that $1+rx_r=m\in M$.

$\boxed{\Leftarrow}$ Suppose that for every element $r\notin M$ there exists an element $x_r\in M$ such that $1+rx_r=m\in M$. Since the ideal $M+rR$ contains 1, we must have that $M+rR=R$ (Problem 2a). Thus, if $M\subseteq I$ and $M\neq I$, then for $r\in I\setminus M$, $rR\subseteq I$ and $M+rR=R\subseteq I$, that is, $I=R$. Thus, M is maximal.

8. Let I be a prime ideal of the ring R. To prove that I is a maximal ideal, it suffices to show that the quotient R/I is a field. Let $\bar{a}=a+I$ be a nonzero element of R/I, where $a\in R$. It follows from the assumption that there exists an integer $n>1$ such that $a^n=a$. Then we have

$$\bar{a}^n=a^n+I=a+I=\bar{a}.$$

Thus we have
$$\bar{a}(\bar{a}^{n-1}-1)=0$$

in R/I. Note that R/I is an integral domain since I is a prime ideal. Since $\bar{a}\neq 0$, the above equality yields that $\bar{a}^{n-1}-1=0$, and hence

$$\bar{a}\cdot\bar{a}^{n-2}=1.$$

It follows that $\bar{a}$ has a multiplicative inverse $\bar{a}^{n-2}$. This proves that each nonzero element of R/I is invertible, hence R/I is a field.

9. Suppose that $a+b\sqrt{10},c+d\sqrt{10}\in\mathbb{Z}[\sqrt{10}]$ and the product

$$(a+b\sqrt{10})(c+d\sqrt{10})\in P.$$

Then expanding the product, we have

$$ac+10bd+(ad+bc)\sqrt{10}\in P.$$

Since $ac+10bd$ must be an even number, we have that either a or c is even. Hence either

$$a+b\sqrt{10}\in P \text{ or } c+d\sqrt{10}\in P,$$

and we conclude that P is a prime ideal.

10.

$\boxed{(a)\Rightarrow(b)}$ Follows from Theorem 2.2.1.

$\boxed{(b)\Rightarrow(c)}$ Now suppose that the ideal $\langle a\rangle$ is prime. Let $a=bc$ for some elements $b,c\in R$. Then the element $a=bc$ is in the prime ideal $\langle a\rangle$, and thus we have either b or c is in $\langle a\rangle$. Without loss of generality, we assume that $b\in\langle a\rangle$. Then we have $b=ad$ for some $d\in R$. It follows that

$$a=bc=adc$$

and since R is a domain, we have

$$1=dc$$

and hence c is a unit. Therefore the element a is irreducible.

$\boxed{(c)\Rightarrow(a)}$ Suppose that a is an irreducible element. Let I be an ideal of R such that

$$\langle a\rangle\subseteq I\subseteq R.$$

Since R is a PID, there exists $b\in R$ such that $I=\langle b\rangle$. Then since $\langle a\rangle\subseteq\langle b\rangle$, we have $a=bc$ for some $c\in R$. The irreducibility of a implies that either b or c is a unit. If b is a unit, then we have $I=R$. If c is a unit, then we have $\langle a\rangle=I$. Therefore the ideal $\langle a\rangle$ is maximal.

11. Let p be an irreducible element in R, R is a PID. From the previous problem we have that this statement is equivalent to saying that the ideal $\langle p\rangle$ is prime. We will show that this is further equivalent to saying that p is a prime element.

Let $\langle p\rangle$ be a prime ideal and suppose that $p|ab$, then there exists an element $r\in R$ such that $pr=ab$. This means that $ab\in\langle p\rangle$. Since $\langle p\rangle$ is prime, we have that either $a\in\langle p\rangle$ or $b\in\langle p\rangle$, in other words, $p|a$ or $p|b$. In a similar manner, one can show the other implication.

R Every PID is also a UFD. But not every UFD is a PID.

2.2.4 Additional problems

1. Let R be an integral domain in which every sets S of ideals contains an ideal I such that no other ideal $J\in S$ is not contained in I (we say that I is a minimal element of the set S). Prove that R is a field.
2. Let R be a ring with unity which contains exactly one maximal left ideal M. Prove:
   (a) M is the set of all elements in R which do not have a left multiplicative inverse.
   (b) No element in M has a right multiplicative inverse.
3. Let R be a ring with unity which has only one maximal left ideal M. Prove:

(a) M is a two-sided ideal which contains all proper left and right ideals of the ring R.

(b) R/M is a skew-field (division ring).

4. Let M be a maximal ideal in a commutative ring R with unity in which for every $x \in M$, $1+x$ has a multiplicative inverse. Prove that M is the only maximal ideal in R. (Hint: Use the previous problem.)
5. Let R be a ring with unity which contains exactly one maximal left ideal M. Show that the only idempotents of R are 0 and 1.

3. Extension Fields

3.1 Introduction to Extension Fields

3.1.1 Theoretical background

We are now in the position to show that, loosely speaking, every non-constant polynomial has a zero. Firstly, before stating the result, we note the following definition.

Definition 3.1.1 A field E is an extension field of a field F if $F \leq E$ and we denote it with $E : F$.

Theorem 3.1.1 — Kronecker's Theorem. Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there exists an extension field E of F and $\alpha \in E$ such that $f(\alpha) = 0$.

When talking about elements of an extension field, we will distinguish two categories.

Definition 3.1.2 An element α of an extension field E of a field F is **algebraic over** F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$. Otherwise, we say that α is **transcendental over** F.

■ **Example 3.1** $\mathbb{C}$ is an extension field of $\mathbb{Q}$. Since $\sqrt{2} \in \mathbb{C}$ is a zero of $x^2 + 2 \in \mathbb{Q}[x]$, we see that $\sqrt{2}$ is algebraic over $\mathbb{Q}$. It is well known (but not easy to prove ☺) that π and e are transcendental over $\mathbb{Q}$. ■

The next theorem gives us a useful characterisation of algebraic and transcendental elements over F in an extension field E of F.

Theorem 3.1.2 Let E be an extension field of a field F and let $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism of $F[x]$ into E such that $\phi_\alpha(a) = a$ for $a \in F$ and

$\phi_\alpha(x) = \alpha$. Then α is transcendental over F if and only if ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E, that is, if and only if ϕ_α is injective.

We note the following theorem which will be of key significance in future work.

Theorem 3.1.3 Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. Then there is an irreducible polynomial $p(x)$ over F such that $p(\alpha) = 0$. The irreducible polynomial $p(x)$ is uniquely determined up to a constant factor in F and is a polynomial of positive degree in $F[x]$ having α as a zero. If $f(\alpha) = 0$ for $f(x) \in F[x]$, with $f(x) \neq 0$, then $p(x)|f(x)$.

R By multiplying with a suitable constant in F, we can assume that the coefficient of the highest power of x appearing in $p(x)$ is 1. We say that in that case $p(x)$ is **monic**.

Definition 3.1.3 Let E be an extension field of a field F and let α be algebraic over F. The unique monic polynomial $p(x)$ having the property described in the previous theorem is the **irreducible polynomial for** α **over** F and will be denoted with $\text{irr}(\alpha, F)$. The degree of $\text{irr}(\alpha, F)$ is the **degree of** α **over** F, denoted by $\deg(\alpha, F)$.

Definition 3.1.4 Let E be an extension field of F and let $\alpha \in E$. The smallest subfield of E containing both F and α is called the **simple extension** of F and is denoted by $F(\alpha)$. If α is algebraic over F, then $F(\alpha) = \phi_\alpha[F[x]]$. If α is transcendental over F, then $F(\alpha)$ is the quotient field of $\phi_\alpha[F[x]]$.

The following remark is **important** and please read it carefully so that you do not get confused with the notation going onwards.

R Let $E : F$ be an extension of the field F and $\alpha \in E$. With $F[\alpha]$ we denote the smallest **subring** of E which contains F and α. Moreover, $F[\alpha] = \{f(\alpha) : f \in F[x]\}$.

Let $S \subseteq E$ be an arbitrary set. With $F(S)$ we denote the smallest **subfield** in E which contains F and S. In case that S has finitely many elements $a_1, \dots, a_n$ we write $F(a_1, \dots, a_n)$ instead of $F(S)$.

Theorem 3.1.4 Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. Let $n = \deg(\alpha, F)$. Then

$$F(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_0, \ldots, a_{n-1} \in F\}.$$

3.1.2 Problems

1. Show that the given elements $\alpha \in \mathbb{C}$ are algebraic over $\mathbb{Q}$:

   (a) $\alpha = 1 + \sqrt{2}$ (b) $\alpha = 1 + i$ (c) $\alpha = \sqrt{1 + \sqrt[3]{2}}$

2. Let $E : F$ be a field extension of F and $\alpha \in E$ algebraic over F. Prove: If $f \in F[x]$ is irreducible and $f(\alpha) = 0$, then $f = c \cdot \text{irr}(\alpha, F)$ for some $c \in F$.
3. Find $\text{irr}(\alpha, \mathbb{Q})$ and $\deg(\alpha, \mathbb{Q})$ for:

(a) $\alpha = \sqrt{3-\sqrt{6}}$ (b) $\alpha = \sqrt{3}+\sqrt{2}$

4. Show that π^2 and $\pi+2$ are transcendental over $\mathbb{Q}$.
5. Determine if the given $\alpha \in \mathbb{C}$ is algebraic or transcendental over the given field F. If it is algebraic, find $\deg(\alpha, F)$.

   (a) $\alpha = \sqrt{\pi},\ F = \mathbb{Q}$ (b) $\alpha = \sqrt{\pi},\ F = \mathbb{R}$ (c) $\alpha = \pi^2,\ F = \mathbb{Q}(\pi^3)$

6. Let $\mathbb{Z}_2(\alpha)$ be the extension of $\mathbb{Z}_2$, where α is the zero of the polynomial x^2+x+1. Determine that the polynomial is indeed irreducible over $\mathbb{Z}_2$ and write the elements of $\mathbb{Z}_2(\alpha)$. Factorize the polynomial x^2+x+1 in $(\mathbb{Z}_2(\alpha))[x]$.
7. Let E be the extension field of the finite field F, where $|F| = q$. Let $\alpha \in E$ be algebraic over F with $\deg(\alpha, F) = n$. Show that $F(\alpha)$ has exactly q^n elements.
8. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
9. Prove that the polynomial $f(x) = x^3+9x+6$ is irreducible over the field of rational numbers $\mathbb{Q}$. Let θ be a root of $f(x)$. Then find the inverse of $1+\theta$ in the field $\mathbb{Q}(\theta)$.

3.1.3 Solutions

1. (a)

$$\begin{aligned} \alpha &= 1+\sqrt{2} \\ \alpha - 1 &= \sqrt{2} \\ (\alpha-1)^2 &= 2 \\ \alpha^2 - 2\alpha - 1 &= 0 \end{aligned}$$

   α is a zero of $x^2-2x-1 \in \mathbb{Q}[x]$. Thus α is an algebraic number.

   (b) Similarly as before, one obtains that α is a zero of $x^2-2x+2 \in \mathbb{Q}[x]$, and as such it is an algebraic number.

   (c) α is a zero of the polynomial $x^6-3x^4+3x^2-3 \in \mathbb{Q}[x]$, and thus it is an algebraic number.

2. Let $g(x) = \operatorname{irr}(\alpha, F)$ be the irreducible polynomial for α over F. Then $g(\alpha) = 0$. Since $f(\alpha) = 0$, we have that $\deg(f) \geq \deg(\alpha, F)$. This means, because of the irreducibility of g, that f contains g as a factor. Since f is irreducible, the only possibility is that $f(x) = cg(x)$ for $c \in F$.

3. (a) It can be easily shown that α is a root of the polynomial $f(x) = x^4-6x^2+3 \in \mathbb{Q}[x]$. For $p = 3$, by Eisenstein's criteria, it follows that f is irreducible over $\mathbb{Q}$. Furthermore, since f is monic, it follows that $\operatorname{irr}(\alpha, \mathbb{Q}) = f(x)$ and $\deg(\alpha, \mathbb{Q}) = 4$.

   (b) α is a root of the polynomial $f(x) = x^4-10x^2+1 \in \mathbb{Q}[x]$. Let us show that f is irreducible over $\mathbb{Q}$. Firstly, if f has a zero in $\mathbb{Q}$, from Theorem 1.5.4, it must have a zero $\alpha \in \mathbb{Z}$ and this zero must divide 1. Thus $\alpha = \pm 1$, but

$$f(1) = -8 \ \text{ and } \ f(-1) = -8.$$

   In other words, $f(x)$ has no linear factors. The only other possibility is that it factors as two quadratic polynomials. In this case we may write

$$f(x) = (x^2+ax+b)(x^2+cx+d),$$

and by Theorem 1.5.4 we may assume that $a,b,c,d\in\mathbb{Z}$. If we equate coefficients, then we get the following equations:

$$bd=1,\ \ ad+bc=0,\ \ b+d+ac=-10,\ \text{ and }\ a+c=0.$$

From $bd=1$, it follows that $b=d=1$ or -1. Then, from the third equation, we have that $ac=-12$ or -18. Since $a=-c$, we have that $c^2=12$ or 18 in $\mathbb{Z}$, but there is no $c\in\mathbb{Z}$ for which this holds. Thus, $f(x)$ must be irreducible over $\mathbb{Q}$. Since f is monic, it follows that $\operatorname{irr}(\alpha,\mathbb{Q})=f(x)$ and $\deg(\alpha,\mathbb{Q})=4$.

4. If we suppose that π^2 is algebraic over $\mathbb{Q}$, then there exists a polynomial $p(x)in\mathbb{Q}[x]$ such that $p(\pi^2)=0$. From here it follows that $q(x)=p(x^2)$ is also a polynomial with rational coefficients and it holds that $q(\pi)=p(\pi^2)=0$, which implies that π is algebraic over $\mathbb{Q}$, which is not true. Thus π^2 is transcendental over $\mathbb{Q}$. A similar conclusion implies that $\pi+2$ is also transcendental over $\mathbb{Q}$.
5. (a) Suppose that $\sqrt{\pi}$ is algebraic over $\mathbb{Q}$. Then there exists a polynomial $p(x)\in\mathbb{Q}[x]$ such that $p(\sqrt{\pi})=0$. In the product $p(x)p(-x)$, all terms with odd powers cancel each other. Thus the product $p(x)p(-x)$ can be considered as a polynomial in the variable x^2.

   $$p(x)p(-x)=q(x^2)\Rightarrow q(\pi)=q(\sqrt{\pi}^2)=p(\sqrt{\pi})p(-\sqrt{\pi})=0,$$

   which is a contradiction with the fact that π is transcendental over $\mathbb{Q}$. Hence, α has to be transcendental as well.

   (b) Since $\sqrt{\pi}\in\mathbb{R}$, it is algebraic over $\mathbb{R}$. It is the root of the polynomial $x-\sqrt{\pi}\in\mathbb{R}[x]$. Thus, $\deg(\sqrt{\pi},\mathbb{R})=1$.

   (c) The polynomial $x^3-(\pi^3)^2$ is a polynomial in $\mathbb{Q}(\pi^3)[x]$ and π^2 is a root of that polynomial. Thus π^2 is algebraic over $\mathbb{Q}(\pi^3)$ and $\deg(\pi^2,\mathbb{Q}(\pi^3))=3$.
6. The polynomial $x^2+x+1\in\mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$, because it is of degree 2,and 0 and 1 are not its roots. Thus $x^2+x+1=\operatorname{irr}(\alpha,\mathbb{Z}_2)$ and $\deg(\alpha,\mathbb{Z}_2)=2$. From Theorem 3.1.4, the elements of $\mathbb{Z}_2(\alpha)$ are $0+0\alpha, 0+1\alpha, 1+0\alpha, 1+1\alpha$, that is,

   $$\mathbb{Z}_2(\alpha)=\{0,1,\alpha,\alpha+1\}.$$

   Let us form the addition and multiplication table for $\mathbb{Z}_2(\alpha)$.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

   Since α is a root of x^2+x+1, it must contain $x+\alpha$ as a factor. Using long divison and the tables above we obtain that

   $$x^2+x+1=(x+\alpha)(x+1+\alpha).$$
7. Follows directly from Theorem 3.1.4 and the fact that $|F|=q$.

8. It is easy to see that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$.
   Now note that

$$(\sqrt{2}+\sqrt{3})^{-1} = \frac{1}{\sqrt{2}+\sqrt{3}} = \frac{\sqrt{2}-\sqrt{3}}{2-3} = \sqrt{3}-\sqrt{2}$$

   and thus $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since addition is closed in a field, we have that

$$\sqrt{2}+\sqrt{3}+\sqrt{3}-\sqrt{2} = 2\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

   and hence $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Note that by a similar argument you get $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Thus, it holds that $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
9. Note that $f(x)$ is a monic polynomial and the prime number 3 divides all non-leading coefficients of $f(x)$. Also the constant term 6 of $f(x)$ is not divisible by 3^2. Hence by Eisenstein's criterion, the polynomial $f(x)$ is irreducible over $\mathbb{Q}$.
   We divide the polynomial $f(x)$ by $x+1$ and obtain

$$x^3+9x+6 = (x+1)(x^2-x+10)-4$$

   by long division. Then it follows that in the field $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/\langle f(x)\rangle$ (note that $f(x) = \operatorname{irr}(\theta,\mathbb{Q})$), we have

$$0 = (\theta+1)(\theta^2-\theta+10)-4,$$

   and hence this yields that we have the inverse

$$(1+\theta)^{-1} = \frac{1}{4}(\theta^2-\theta+10).$$

3.1.4 Additional problems

1. Show that the polynomial x^2+1 is irreducible over $\mathbb{Z}_3$. Let α be a root of the polynomial x^2+1 in the extension of $\mathbb{Z}_3$. Write down the multiplication and addition tables for the field $\mathbb{Z}_3(\alpha)$. Factorize x^2+1 in $\mathbb{Z}_3(\alpha)[x]$.
2. Show that $f(x) = x^3+x^2+1$ is irreducible over $\mathbb{Z}_2$. Let α be a root of $f(x)$ in $\mathbb{Z}_2(\alpha)$. Factorize $f(x)$ in $\mathbb{Z}_2(\alpha)[x]$.
3. Let E be an extension field of $\mathbb{Z}_2$ and let $\alpha \in E$ be algebraic of degree 3 over $\mathbb{Z}_2$. Denote $G = \mathbb{Z}_2(\alpha)$. Classify the groups $(G,+)$ and $(G^*,\cdot)$ according to the Fundamental Theorem of finitely generated abelian groups. As usual G^* is the set of nonzero elements of G.
4. Suppose that u is algebraic over the field F, and that $a \in F$. Show that $u+a$ is algebraic over F, find its irreducible polynomial over F and show that $\deg(u+a,F) = \deg(u,F)$.
5. Show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.
6. Let E be an extension field of F. If $u \in E$ is transcendental over F, then show that every element of $F(u)$ that is not in F is also transcendental over F.
7. Show that the polynomial $f(x) = x^3+x+1$ is irreducible over $\mathbb{Q}$. Let $\alpha \in \mathbb{C}$ be a root of f. Express $\frac{1}{\alpha}$ and $\frac{1}{\alpha+2}$ as a linear combination of the elements $1, \alpha$ and α^2.
8. Find the multiplicative inverse of the element $1+\sqrt{2}+\sqrt{3}+\sqrt{6}$ in the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$.
9. Let α and β be two different transcendental numbers. Is $\alpha\beta$ also transcendental?

3.2 Vector Spaces. Algebraic Extension

3.2.1 Theoretical background

Definition 3.2.1 Let F be a field. A vector space over F (or F-vector space) consists of an abelian group $(V,+)$ with an operation of scalar multiplication of each element of V by each element of F on the left, such that for all $a,b \in F$ and all $\alpha,\beta \in V$ the following conditions hold:
($\mathscr{V}1$) $a\alpha \in V$
($\mathscr{V}2$) $a(b\alpha) = (ab)\alpha$
($\mathscr{V}3$) $(a+b)\alpha = (a\alpha)+(b\alpha)$
($\mathscr{V}4$) $a(\alpha+\beta) = (a\alpha)+(a\beta)$
($\mathscr{V}5$) $1\alpha = \alpha$
The elements of V are called vectors, and the elements of F scalars.

■ **Example 3.2** Let E be an extension field over F. Then E can be regarded as a vector space over F, where addition of vectors is the usual addition in E and scalar multiplication $a\alpha$ is the usual field multiplication in E with $a \in F, \alpha \in E$. ■

Definition 3.2.2 Let V be an F-vector space. The spanning set for V is a set of vectors $\{\alpha_i : i \in I\}$ in V, such that every $\beta \in V$ can be written as a linear combination of the vectors α_i, that is, we have $\beta = \sum_{i\in I} a_i\alpha_i$, where all $a_i \in F$.

Definition 3.2.3 An F-vector space V is finite dimensional if there is a finite subset of V whose vectors span V.

■ **Example 3.3** If $F \leq E$ and $\alpha \in E$ is algebraic over F, then $F(\alpha)$ is a finite-dimensional vector space over F. ■

Definition 3.2.4 A set of vectors $\{\alpha_i : i \in I\}$ is linearly independent if whenever $\sum_{i\in I} a_i\alpha_i = 0$, we have that $a_i = 0$ for all $i \in I$. Otherwise, we say that they are linearly dependent.

■ **Example 3.4** If E is a field extension of F and $\alpha \in E$ is algebraic over F such that $\deg(\alpha,F) = n$, then every element of $F(\alpha)$ can be uniquely written as a linear combination of $\{1,\alpha,\dots,\alpha^{n-1}\}$. Hence, the set of powers of α is linearly independent. ■

Definition 3.2.5 A basis for a vector space is a linearly independent spanning set. If V is finite-dimensional over F, we say that the dimension of V over F is the number of elements in the basis.

Theorem 3.2.1 Let $F \leq E$ and $\alpha \in E$ be algebraic over F. If $\deg(\alpha,F) = n$ then $F(\alpha)$ is a vector space over F of dimension n, with basis $\{1,\alpha,\dots,\alpha^{n-1}\}$. Furthermore, every $\beta \in F(\alpha)$ is algebraic over F and $\deg(\beta,F) \leq \deg(\alpha,F)$.

Definition 3.2.6 An extension field E of F is an algebraic extension of F if every element in E is algebraic over F.

Definition 3.2.7 Let E be an extension field of F. If E is finite-dimensional as a vector space over F, with dimension n say, then we say that E is a finite extension of degree n

over F. We write $[E:F]$ for the degree n of E over F.

R This is just a finite extension, we are not saying that the fields involved are finite. Furthermore, note that $[E:F]=1$ if and only if $E=F$.

Theorem 3.2.2 Every finite extension is an algebraic extension.

Theorem 3.2.3 Tower Law for field extensions If E is a finite extension of F and K is a finite extension of E, then K is a finite extension of F and

$$[K:F]=[K:E][E:F].$$

3.2.2 Problems

1. Find the basis for the given vector space over the given field:

   (a) $\mathbb{R}(\sqrt{2})$ over $\mathbb{R}$ (b) $\mathbb{C}$ over $\mathbb{R}$ (c) $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$

2. Compute $[E:\mathbb{Q}]$ and find a basis of E over $\mathbb{Q}$ if

   (a) $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$ (b) $E=\mathbb{Q}(\sqrt[3]{5},\sqrt{-2})$

3. Show that x^2-3 is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.
4. Let α be an algebraic element of odd degree over a field F. Show that $F(\alpha)=F(\alpha^2)$.
5. Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces, but not as fields.
6. Show that if E is a finite extension of F and $[E:F]$ is prime, then E is a simple extension of F and $E=F(\alpha)$ for every $\alpha\in E$ such that $\alpha\notin F$.
7. Let E be a finite extension of the field F and let $p(x)$ be irreducible over F of degree d such that $d\nmid[E:F]$. Show that $p(x)$ has no zeros in E.
8. Let $f(x)$ be an irreducible polynomial in $K[x]$. Show that if F is an extension field of K such that $\deg(f(x))$ is relatively prime to $[F:K]$, then $f(x)$ is irreducible over $F[x]$.

3.2.3 Solutions

1. (a) Since $\sqrt{2}\in\mathbb{R}$ and it is a root of the polynomial $x-\sqrt{2}\in\mathbb{R}[x]$ of degree 1, it follows that the basis is $\{1\}$.
   (b) Note that $\mathbb{R}=\mathbb{C}(i)$. We have that i is the root of the irreducible polynomial x^2+1 over $\mathbb{R}$ of degree 2. Thus, $\deg(i,\mathbb{R})=2$ and the basis for $\mathbb{C}$ over $\mathbb{R}$ is $\{1,i\}$ (from Theorem 3.2.1).
   (c) $\sqrt[4]{2}$ is a root of the irreducible polynomial x^4-2 over $\mathbb{Q}$ of degree 4. Thus $\deg(\sqrt[4]{2},\mathbb{Q})=4$ and the basis for $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$ is $\{1,\sqrt[4]{2},\sqrt[4]{4},\sqrt[4]{8}\}$.
2. (a) First we note that $E=K(\sqrt{3})$ where $K=\mathbb{Q}(\sqrt{2})$. Let us consider these two simple extensions.

   First, $\sqrt{2}$ is a root of $\text{irr}(\sqrt{2},\mathbb{Q})=x^2-2$. Thus, $B=\{1,\sqrt{2}\}$ is a basis for K over $\mathbb{Q}$. In other words, every element u in K can be written as $u=a+b\sqrt{2}$ for some $a,b\in\mathbb{Q}$.

On the other hand, $\sqrt{3}$ is a root of $\operatorname{irr}(\sqrt{3},K) = x^2-3$. Thus, $B' = \{1,\sqrt{3}\}$ is a basis for E over K. In other words, every element v in E can be written as $v = u_1+u_2\sqrt{3}$ for some $u_1,u_2 \in K$, which further implies that,

$$v = a_1+b_1\sqrt{2}+(a_2+b_2\sqrt{2})\sqrt{3} = a_1+b_1\sqrt{2}+a_2\sqrt{3}+b_2\sqrt{6}$$

for some $a_i,b_i \in \mathbb{Q}$. Thus, v is a linear combination of the vectors in $U = \{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. From $v=0$ it follows that $a_1 = a_2 = b_1 = b_2 = 0$, that is, U is a basis for E over $\mathbb{Q}$ and $[E:\mathbb{Q}] = 4$.

(b) Similarly as before, we will consider the simple extensions of E over K and of K over $\mathbb{Q}$, where $K = \mathbb{Q}(\sqrt[3]{5})$. It is easy to see that the basis for K over $\mathbb{Q}$ is $\{1,\sqrt[3]{5},\sqrt[3]{5}^2\}$ and the basis for E over K is $\{1,\sqrt{-2}\}$. Hence, the basis for E over $\mathbb{Q}$ is the product of elements in the previous two bases, that is, $\{1,\sqrt[3]{5},\sqrt[3]{5}^2,\sqrt{-2},\sqrt[3]{5}\cdot\sqrt{-2},\sqrt[3]{5}^2\sqrt{-2}\}$ and $[E:\mathbb{Q}] = 6$.

3. If x^2-3 would be irreducible over $\mathbb{Q}(\sqrt[3]{2})$, we can write is as a product of linear factors over $\mathbb{Q}(\sqrt[3]{2})$. This means that $\sqrt{3}$ lies in $\mathbb{Q}(\sqrt[3]{2})$ and we have that $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt[3]{2})$. On the other hand,

$$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}:\mathbb{Q}(\sqrt{3})]\cdot[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] \Rightarrow [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] \mid [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] \Rightarrow 2|3,$$

which is not true. Thus, x^2-3 is irreducible over $\mathbb{Q}$.

4. Since $\alpha^2 \in F(\alpha)$ it follows that $F \leq F(\alpha^2) \leq F(\alpha)$. Since α is a root of the polynomial $p(x) = x^2-\alpha^2$ of degree 2 over $F(\alpha^2)$, it follows that $[F(\alpha):F(\alpha^2)] \leq 2$. Since

$$[F(\alpha):F] = [F(\alpha):F(\alpha^2)][F(\alpha^2):F],$$

and $[F(\alpha):F]$ is odd, it must follow that $[F(\alpha):F(\alpha^2)] = 1$. Thus, $F(\alpha) = F(\alpha^2)$.

5. i is a root of the irreducible polynomial x^2+1 over $\mathbb{Q}$, thus $[\mathbb{Q}(i):\mathbb{Q}] = 2$. Similarly, $\sqrt{2}$ is a root of the irreducible polynomial x^2-2 over $\mathbb{Q}$, thus $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. Since $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are, as vector spaces over $\mathbb{Q}$, of the same dimension, they are isomorphic to each other.

Let us know suppose that there is a field isomorphism $f:\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(i)$. This means, that for some $a,b \in \mathbb{Q}$ we have that $f(\sqrt{2}) = a+ib$. Any homomorphism between two fields over $\mathbb{Q}$ fixes the elements of $\mathbb{Q}$. Hence, $f(q) = q$ for all $q \in \mathbb{Q}$. Thus, we have:

$$2 = f(2) = f(\sqrt{2}\sqrt{2}) = f(\sqrt{2})^2 = a^2-b^2+2abi$$

From the above equation we must have $ab = 0$ and $a^2-b^2 = 2$, which means that either $a = 0$ and $b^2 = -2$ or $b = 0$ and $a^2 = 2$, which is not possible. Hence, such an isomorphism cannot exist.

6. Since $F \leq E$ and $\alpha \in E$, it is easy to see that $F(\alpha) \leq E$. Thus

$$[E:F] = [E:F(\alpha)][F(\alpha):F] = p,$$

where p is prime. Since $\alpha \notin F$, we must have that $[F(\alpha):F] > 1$, which means that $[F(\alpha):F] = p$ and thus $[E:F(\alpha)] = 1$. In other words, $E = F(\alpha)$.

7. Suppose that $\alpha \in E$ is a zero of $p(x)$. Since $p(x)$ is irreducible over F, we have that $[F(\alpha):F] = \deg(p(x)) = d$. From $[E:F] = [E:F(\alpha)][F(\alpha):F]$ it follows that $[F(\alpha):F] = d \mid [E:F]$, which is not possible. Hence, $p(x)$ has no zeros in E.

8. Let α be a root of $f(x)$ contained in some field extension of F. Observe that

$$[F(\alpha):F][F:K] = [F(\alpha):K] = [F(\alpha):K(\alpha)][K(\alpha):K]. \tag{3.1}$$

Note that $[K(\alpha):K] = \deg(f(x))$, since α is a root of $f(x)$ which is irreducible over K. From (3.1), it follows that $[K(\alpha):K] \mid [F(\alpha):F][F:K]$. Since $\gcd([K(\alpha):K],[F:K]) = 1$, it follows that $[K(\alpha):K] \mid [F(\alpha):F]$. Because $K \leq F$ it follows that $K[x] \leq F[x]$ and thus $f(x) \in F[x]$. Since $f(\alpha) = 0$, we must have that $\operatorname{irr}(\alpha,F) =: g|f$, and thus $\deg(g) \leq \deg(f)$. In other words, $[F(\alpha):F] \leq [K(\alpha):K]$. Hence, we must have that $[F(\alpha):F] = [K(\alpha):K]$. If f would be reducible over F, then $\deg(\alpha,F) < \deg(\alpha,K)$, which is not possible. Hence, f must be irreducible over F.

3.2.4 Additional problems

1. Find a basis for each of the following field extensions. What is the degree of each extension?
   (a) $\mathbb{Q}(\sqrt{3},\sqrt{6})$ over $\mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3})$ over $\mathbb{Q}$
   (c) $\mathbb{Q}(\sqrt{2},i)$ over $\mathbb{Q}$
   (d) $\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7})$ over $\mathbb{Q}$
   (e) $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$ over $\mathbb{Q}$
   (f) $\mathbb{Q}(\sqrt{8})$ over $\mathbb{Q}(\sqrt{2})$
   (g) $\mathbb{Q}(i,\sqrt{2}+i,\sqrt{3}+i)$ over $\mathbb{Q}$
   (h) $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ over $\mathbb{Q}(\sqrt{5})$
   (i) $\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10})$ over $\mathbb{Q}(\sqrt{3}+\sqrt{5})$
2. Prove that $\mathbb{Q}(\sqrt{3},\sqrt[4]{3},\sqrt[8]{3},\ldots)$ is an algebraic extension of $\mathbb{Q}$ but not a finite extension.
3. Prove or disprove: π is algebraic over $\mathbb{Q}(\pi^3)$.
4. Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are isomorphic as vector spaces but not as fields.
5. Prove that the fields $\mathbb{Q}(\sqrt[4]{3})$ and $\mathbb{Q}(\sqrt[4]{3}i)$ are isomorphic but not equal.
6. Let K be an algebraic extension of E and E an algebraic extension of F. Prove that K is algebraic over F. (Note: Do not assume that the extensions are finite.)
7. Let E be a field extension of F and $\alpha \in E$. Determine $[F(\alpha):F(\alpha^3)]$.

3.3 Algebraic closure. Constructible numbers

3.3.1 Theoretical background

Given a field F, the question arises whether or not we can find a field E such that every polynomial $p(x) \in F[x]$ has a root in E. This leads us to the following theorem.

Theorem 3.3.1 Let E be an extension field of F. The set of elements in E that are algebraic over F form a field.

Corollary 3.3.2 The set of all algebraic numbers forms a field; that is, the set of all complex numbers that are algebraic over $\mathbb{Q}$ makes up a field.

Definition 3.3.1 Let E be a field extension of a field F. We define the algebraic closure of a field F in E, denoted by $\overline{F}_E$, to be the field consisting of all elements in E that are algebraic over F. A field F is algebraically closed if every nonconstant polynomial in $F[x]$ has a root in F.

Theorem 3.3.3 A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors into linear factors over $F[x]$.

Corollary 3.3.4 An algebraically closed field F has no proper algebraic extension E.

Theorem 3.3.5 Every field F has a unique algebraic closure.

We now state the Fundamental Theorem of Algebra, first proven by Gauss at the age of 22 in his doctoral thesis. This theorem states that every polynomial with coefficients in the complex numbers has a root in the complex numbers.

Theorem 3.3.6 — Fundamental Theorem of Algebra. The field of complex numbers is algebraically closed.

In ancient Greece, three classic problems were posed. These problems are geometric in nature and involve straightedge-and-compass constructions from what is now high school geometry; that is, we are allowed to use only a straightedge and compass to solve them. The problems can be stated as follows.

1. Given an arbitrary angle, can one trisect the angle into three equal subangles using only a straightedge and compass?
2. Given an arbitrary circle, can one construct a square with the same area using only a straightedge and compass?
3. Given a cube, can one construct the edge of another cube having twice the volume of the original? Again, we are only allowed to use a straightedge and compass to do the construction.

After puzzling mathematicians for over two thousand years, each of these constructions was finally shown to be impossible. We will use the theory of fields to provide a proof that the solutions do not exist. It is quite remarkable that the long-sought solution to each of these three geometric problems came from abstract algebra. First we note the following definition.

Definition 3.3.2 A real number α is constructible if we can construct a line segment of length $|\alpha|$ in a finite number of steps from a segment of unit length by using a straightedge and compass.

Theorem 3.3.7 The set of all constructible real numbers forms a subfield of real numbers.

Lemma 3.1 If α is a constructible number, then $\sqrt{\alpha}$ is a constructible number.

Theorem 3.3.8 The field F of constructible real numbers consists precisely of all real numbers that we can obtain from $\mathbb{Q}$ by taking square roots of positive numbers a finite number of times and applying a finite number of field operations.

Corollary 3.3.9 If γ is constructible and $\gamma \notin \mathbb{Q}$, then there is a finite sequence of real numbers $\alpha_1, \ldots, \alpha_n = \gamma$ such that $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ is an extension of $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ of degree 2. In particular, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$ for some integer $r \geq 0$.

Corollary 3.3.10 The field of all constructible numbers is an algebraic extension of $\mathbb{Q}$.

As we can see by the field of constructible numbers, not every algebraic extension of a field is a finite extension.

We are now ready to investigate the classical problems of doubling the cube and squaring the circle. We can use the field of constructible numbers to show exactly when a particular geometric construction can be accomplished.

Theorem 3.3.11 *Doubling the cube is impossible*, that is, given a side of a cube, it is not possible to construct with a straightedge and a compass the side of a cube that has double the volume of the original cube.

Proof. Let the given cube have a side of length 1, and hence a volume of 1. The new cube would have volume 2 and hence a side of length $\sqrt[3]{2}$. But $\sqrt[3]{2}$ is a root of the irreducible polynomial $x^3 - 2$ over $\mathbb{Q}$, so

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

From Corollary 3.3.9, we have that $3 = 2^r$ for some integer r, but no such r exists. ■

Theorem 3.3.12 *Squaring the circle is impossible*, that is, given a circle, it is not always possible to construct with a straightedge and compass a square having area equal to the area of the given circle.

Proof. Let the given circle have radius 1 and hence an area of π. We would need to construct a square of side $\sqrt{\pi}$. Since π is transcendental over $\mathbb{Q}$, so is $\sqrt{\pi}$. The impossibility of the construction follows from Corollary 3.3.10. ■

Theorem 3.3.13 *Trisecting an angle is impossible*, that is, there exists an angle that cannot be trisected with a straightedge and a compass.

Proof. An angle θ can be constructed if and only if a segment of length $|\cos\theta|$ can be constructed. Now 60° is a constructible angle, and we will show that it cannot be trisected. Let $\alpha = \cos 20°$. From the formula $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$, we have that

$$4\alpha^3 - 3\alpha = \frac{1}{2}.$$

That is, α is a zero of $8x^3 - 6x - 1$. This polynomial is irreducible in $\mathbb{Q}[x]$ (it is left to the reader as an exercise). Thus,

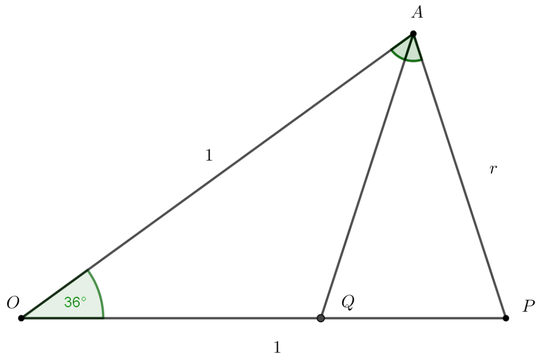
$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

and by Corollary 3.3.9, α is not constructible. Hence, 60° cannot be trisected. ■

R Not that the regular n-gon, $n \geq 3$, is constructible if and only if the angle $2\pi/n$ is constructible, which is the case if and only if a line segment of length $|2\pi/n|$ is constructible.

3.3.2 Problems

1. Let E be an extension field of F. Prove that every $\alpha \in E$ that is not in the algebraic closure of $\overline{F}_E$ of F in E is transcendental over $\overline{F}_E$.
2. Let E be an algebraically closed extension field of F. Show that the algebraic closure $\overline{F}_E$ of F in E is algebraically closed.
3. Prove that the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is not a finite extension of $\mathbb{Q}$.
4. Show that every finite extension of $\mathbb{R}$ is either $\mathbb{R}$ or isomorphic to $\mathbb{C}$.
5. Show that the regular 9-gon is not constructible.
6. Show algebraically that it is possible to construct an angle of 30°.
7. Referring to the figure below, where $\overline{AQ}$ bisects the angle OAP, show that the regular 10-gon (and therefore, regular 5-gon) is constructible.



3.3.3 Solutions

1. If α is algebraic over $K = \overline{F}_E$, then $K(\alpha)$ is algebraic over K. By definition, we also have that K is algebraic over F. Thus we have that K is algebraic over F, and in particular, that α is algebraic over F. Thus, $\alpha \in K$, which is not possible. Thus α is transcendental over K.
2. Let $f(x)$ be a nonconstant polynomial in $K[x]$, $K = \overline{F}_E$. Now, $f(x) \in E[x]$ and, by hypothesis, E is algebraically closed, so $f(x)$ has a root α in E. From the previous problem, if $\alpha \notin K$, then α would be transcendental over K, which cannot be true, because α is a root of $f(x) \in K[x]$. Hence, we must have that $\alpha \in K$, which shows that K is algebraically closed.
3. For all $n \in \mathbb{Z}$, $n \geq 2$, the polynomial $x^n - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criteria for $p = 2$. This shows that $\mathbb{Q}$ has a finite extension of arbitrary degree in $\mathbb{C}$. If $\overline{\mathbb{Q}}_{\mathbb{C}}$ were a finite extension of $\mathbb{Q}$ of degree r, then there would be no algebraic extension of $\mathbb{Q}$ in $\mathbb{C}$ of degree greater than r, which is not true. Thus the algebraic closure $\overline{\mathbb{Q}}_{\mathbb{C}}$ cannot be a finite extension of $\mathbb{Q}$ in $\mathbb{C}$.
4. Because $[\mathbb{C} : \mathbb{R}] = 2$ and $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$, it must be that every irreducible polynomial $p(x) \in \mathbb{R}[x]$ of degree greater than 1, is actually of degree

2. If α is a root of such a polynomial, we note that $\mathbb{C} = \mathbb{R}(\alpha)$ and (see proof of Kronecker's theorem) it holds that

$$\mathbb{C} \cong \mathbb{R}[x]/\langle p(x) \rangle \tag{3.2}$$

Let E be a field extension of $\mathbb{R}$. If $E \neq \mathbb{R}$, then there exists an element $\alpha \in E$ such that $\alpha \notin \mathbb{R}$. From the above explanation, it holds that $p(x) = \operatorname{irr}(\beta, \mathbb{R})$ has degree 2. Since $\mathbb{R}(\beta) \cong \mathbb{R}[x]/\langle p(x) \rangle$, it follows from (3.2) that $\mathbb{R}(\beta) \cong \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, so is $\mathbb{R}(\beta)$ and thus admits no proper algebraic extensions. Since E is an algebraic extension of $\mathbb{R}(\beta)$, we must have $E = \mathbb{R}(\beta)$ and thus $E \cong \mathbb{C}$.

5. If a regular 9-gon could be constructed, then the angle $360^\circ/90^\circ = 40^\circ$ could be constructed, and using bisection, an angle of 20° could be constructed. As seen in the proof of Theorem 3.3.13, we know that such an angle is not constructible.
6. One can construct an angle of 30° if and only if one can construct a line segment of length $|\cos 30^\circ| = \sqrt{3}/2$. Because $\sqrt{3}$ is constructible and quotients of constructible numbers are constructible, an angle of 30° is constructible.
7. Since
   - $\angle OAP = \angle APO = \frac{180^\circ - 36^\circ}{2} = 72^\circ$ (the triangle OAP is isosceles)
   - $\angle QAP = \angle AOP = 36^\circ$

   from the Angle-Angle (AA) rule, it holds that $\triangle OAP \sim \triangle AQP$. The triangle APQ is isosceles, thus $|\overline{AP}| = |\overline{AQ}| = r$. Also, the triangle OAQ is isosceles, and thus $|\overline{OQ}| = |\overline{AQ}| = r$. Taking ratios of the corresponding sides, we obtain

$$\frac{\overline{AP}}{\overline{OP}} = \frac{\overline{OA}}{\overline{AP}} \Leftrightarrow \frac{r}{1-r} = \frac{1}{r} \Leftrightarrow r^2 + r - 1 = 0.$$

   By the quadratic formula we obtain that

$$r = \frac{-1+\sqrt{5}}{2}$$

   which is a constructible number. Thus we can construct an angle of 36° by taking a line segment $\overline{OP}$ of length 1, drawing a circle of radius 1 at O and one of radius r at P, and finding a point A of intersection of the two circles. Then $\angle AOP$ measures 36°. Thus a regular 10-gon which has central angles of 36° is constructible. A regular pentagon is obtained by starting at a vertex 1 of a regular 10-gon and drawing a line segments to vertex 3, from 3 to vertex 5, from 5 to 7, from 7 to 9, and then from 9 back to 1. The vertices $1, 2, \ldots, 10$ are ordered , e.g. clockwise.

3.3.4 Additional problems

1. (a) Consider the prime field $\mathbb{Z}_p$ of characteristic $p \neq 2$. Show that not every element in $\mathbb{Z}_p$ is a square of an element in $\mathbb{Z}_p$. (Hint: $1^2 = (p-1)^2 = 1$ in $\mathbb{Z}_p$. Deduce the desired conclusion *by counting*.)

   (b) Show that no finite field of odd characteristic is algebraically closed. (Hint: By counting, show that for such a finite field F, some polynomial $x^2 - a$ for some $a \in F$, has no zero in F. Similar idea as in (a).)
2. Prove that if E is an algebraic extension of a field F and contains all zeros in $\overline{F}_E$ of every $f(x) \in F[x]$, then E is an algebraically closed field.

3. Show that the regular 20-gon is constructible.
4. Show that the regular 30-gon is constructible.
5. Show that the angle 72° can be trisected.
6. Show that the regular 15-gon can be constructed.
7. Show that $\cos 1^\circ$ is algebraic but not constructible (Hint: Represent $\cos 1^\circ$ using Euler's formula $e^{i\varphi} = \cos\varphi + i\sin\varphi$.)

3.4 Finite fields

3.4.1 Theoretical background

For every prime p and positive integer n, there is exactly one finite field (up to isomorphism) of order p^n. This field $GF(p^n)$ or $\mathbb{F}_{p^n}$ is usually referred to as the **Galois field of order** p^n.

Theorem 3.4.1 Let E be a finite extension of degree n over F. If $|F| = q$, then $|E| = q^n$.

Corollary 3.4.2 Let E be a finite field of prime characteristic p, then $|E| = p^n$ for some positive integer n.

Theorem 3.4.3 Let E be a finite field of p^n elements contained in the algebraic closure $\overline{\mathbb{Z}_p}$ of $\mathbb{Z}_p$. The elements of E are precisely the zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Definition 3.4.1 An element α of a field is an **n-th root of unity** if $\alpha^n = 1$. It is a **primitive n-th root of unity** if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.

Theorem 3.4.4 The multiplicative group $\langle F^*, \cdot \rangle$ of nonzero elements of a finite field is cyclic.

Corollary 3.4.5 Every finite extension of a finite field is a simple extension.

Theorem 3.4.6 A finite field $GF(p^n)$ of o^n elements exists for every prime power p^n.

Corollary 3.4.7 Let F be a finite field. Then for every n there exists an irreducible polynomial in $F[x]$ of degree n.

3.4.2 Problems

1. Find the number of primitive 8-th roots of unity in $GF(9)$.
2. Find the number of primitive 10-th roots of unity in $GF(23)$.
3. Let $\overline{\mathbb{Z}_2}$ be an algebraic closure of $\mathbb{Z}_2$ and let $\alpha, \beta \in \overline{\mathbb{Z}_2}$ be zeros of $p(x) = x^3 + x^2 + 1$ and $q(x) = x^3 + x + 1$, respectively. Show that $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2(\beta)$.
4. Show that a finite field of p^n elements has exactly one finite subfield of p^m elements for each divisor m of n.
5. Let F be a field of characteristic p. Show that the mapping $\phi : F \to F$ defined with

$\phi(x) = x^p$ is an automorphism.

6. Let F be a finite field. Show that every element of F is a sum of two squares in F.
7. Show that every irreducible polynomial in $\mathbb{Z}_p[x]$ divides $x^{p^n} - x$ for some n.

3.4.3 Solutions

1. Let z be primitive n-th root of unity. A power $w = z^k$ of z is a primitive l-th root of unity for $l = \frac{n}{\gcd(k,n)}$. This result comes from the fact that kl is the smallest multiple of k that is also a multiple of n. In other words

$$lk = \operatorname{lcm}(k,n) \Rightarrow l = \frac{kn}{k \gcd(k,n)} = \frac{n}{\gcd(k,n)}.$$

Thus, if k and n are coprime, z^k is also a primitive n-th root of unity. Therefore there are $\phi(n)$ (ϕ is Euler's totient function) distinct primitive n-th roots of unity.

The subgroup of a cylic group is cyclic. Moreover, for a finite cyclic group of order n, every subgroup's order is a divisor of n, and there is exactly one subgroup for each divisor.

Since $GF(9)^*$ has order 8. The number of generators of subgroups (in this case the whole group) of order 8 is $\phi(8) = \phi(2^3) = 4$. Thus, there are 4 primitive 8-th roots of unity.

2. If we would have a primitive 10-th root of unity α, then $\alpha^10 = 1$. However, $|GF(23)^*| = 22$, and thus $GF(23)^*$ contains no element of order 10. Hence, there are no 10-th roots of unity in $GF(23)$.
3. Both of the polynomials $p(x)$ and $q(x)$ are irreducible over $\mathbb{Z}_2$, and thus both $\mathbb{Z}_2(\alpha)$ and $\mathbb{Z}_2(\beta)$ are extensions of $\mathbb{Z}_2$ of degree 3, and as such are subfields of $\overline{\mathbb{Z}_2}$ containing 2^3 elements. From Theorem 3.4.3 both of these fields must consist precisely of the zeros in $\overline{\mathbb{Z}_2}$ of the polynomial $x^8 - x$. Thus, we must have $\mathbb{Z}(\alpha) = \mathbb{Z}(\beta)$.
4. Let $F = GF(p^n)$. Consider the set

$$S_m(F) = \{\omega \in F : \omega^{p^m} = \omega\}.$$

To be in this set, ω must be a zero of $x^{p^m} - x$. Thus, it must be that $|S_m(F)| \leq p^m$. If F would have two subfields of p^m elements, say S_1 and S_2, then

$$S_1 \cup S_2 \subseteq S_m(F) \Rightarrow |S_1 \cup S_2| \leq p^m \Rightarrow S_1 = S_2.$$

Thus, F has at most one subfield with p^m elements. The zeros of $x^{p^m} - x$ in $\overline{\mathbb{Z}_p}$ for a field with p^m elements. So, it suffices to show that all these zeros are in F. We know that F^* is cyclic. Let α be a generator, that is, all elements of F can be written as α^i for some positive integer i. Since α^i is a zero of $x^{p^m} - x$, we must have that $ip^m = i \mod p^n - 1$, or equivalently, $(p^n - 1) \mid i(p^m - 1)$. There are exactly $p^m - 1$ such elements (since m is a divisor of n). In other words, all $p^m - 1$ nonzero elements of $\overline{\mathbb{Z}_p}$ that are zeros of $x^{p^m} - x$ are in F. Trivially, 0 is also a zero of that polynomial and is in F. Hence, all zeros are in F and thus form a subfield in F with p^m elements.

5. Since F has characteristic p, it holds that $(\alpha + \beta)^p = \alpha^p + \beta^p$. From this, one can easily confirm that ϕ is indeed a homomorphism. Since F is finite, ϕ is surjective.

Furthermore, $\ker\phi$ is a proper ideal of F. Since F is a field, it only contains trivial ideals and thus we must have that $\ker\phi = \{0\}$. In other words, ϕ is also injective, which implies that ϕ is indeed an automorphism.

> The mapping ϕ is called the Frobenious automorphism. If F is a finite field of characteristic p, this means that for every element $\alpha \in F$ we can find an element $\beta \in F$ such that $\alpha = \beta^p$.

6. We will consider two cases based on the characteristic of F.
   - $char(F) = 2$. Let us cosinder the Frobenious automorphism $\phi(x) = x^2$. Then, for every $\alpha \in F$ we can find a $\beta \in F$ such that $\alpha = \beta^2 = \beta^2 + 0^2$.
   - $char(F) = p > 2$. Let $\psi : F^* \to F^*$ be defined with $\psi(\alpha) = \alpha^2$. If $\psi(\alpha) = \psi(\beta)$, then $\alpha^2 = \beta^2$. In other words, $\alpha = \beta$ or $\alpha = -\beta$. Since $\beta \neq 0$ and $char(F) > 2$, we must have $\beta \neq -\beta$. Thus, ψ is a 2-to-1 mapping, which implies, since 0 is also a square, that there are
   $$\frac{|F^*|}{2} + 1 = \frac{|F| - 1}{2} + 1 = \frac{|F| + 1}{2}$$
   squares in F. Let $A = \{\alpha^2 : \alpha \in F\}$ and, for an arbitrary but fixed $x \in F$, $B = \{x - \beta^2 : \beta \in F\}$. Obviously, $|A| = |B| = \frac{|F|+1}{2}$. If $A \cap B = \emptyset$, we would have that $|A \cup B| = |A| + |B| = |F| + 1 > |F|$, which is not possible. Hence, there exist $\alpha, \beta \in F$ such that $\alpha^2 = x - \beta^2$, that is, $x = \alpha^2 + \beta^2$. Since x was arbitrary, any element of the field can be written as a sum of two squares.
7. Let f be an irreducible polynomial in $\mathbb{Z}_p[x]$ and let E be an extension field of $\mathbb{Z}_p$ containing a zero α of F such that $[E : \mathbb{Z}_p]$ is finite, say n. Then E is a finite field of order p^n. This means that for every $z \in E^*$ we have that $z^{p^n} = z$. In other words, every $z \in E^*$ is a zero of $x^{p^n} - x$. Particularly, α is a zero of $x^{p^n} - x$.
   Let $I = \langle f, x^{p^n} - x\rangle$ be an ideal in $\mathbb{Z}_p[x]$ and $J = \langle f, x^{p^n} - x\rangle$ be an ideal in $E[x]$. We have that $x - \alpha$ is a common factor of f and $x^p - x$ in $E[x]$, thus $J = \langle x - \alpha\rangle$. Note that $1 \notin J$, because otherwise $J = E$, which is not possible. This implies also that $1 \notin I$, that is, $I \neq \mathbb{Z}_p[x]$. Since $f \in I$ we have that $\langle f(x)\rangle \subseteq I \subsetneq \mathbb{Z}_p[x]$. Because $\langle f(x)\rangle$ is maximal, we must have $I = \langle f(x)\rangle$. Now, since $x^{p^n} - x \in I$, it follows that $f(x) | x^{p^n} - x$.

4. Automorphisms of Fields

4.0.1 Theoretical background

In this section, we show that if E is an algebraic extension of F with $\alpha, \beta \in E$, then α and β have the same algebraic properties if and only if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$. We shall phrase this in terms of mappings. More precisely, if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$, then there exists an isomorphism $\psi_{\alpha,\beta}$ of $F(\alpha)$ onto $F(\beta)$ that maps each element of F onto itself and maps α onto β. Let us introduce some terminology.

Definition 4.0.1 Let E be an algebraic extension of F. Two elements $\alpha, \beta \in E$ are **conjugate over** F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$, that is, if α, β are zeros of the same irreducible polynomial over F.

Theorem 4.0.1 — Conjugation Isomorphism. Let F be a field and let α, β be algebraic over F with $\deg(\alpha, F) = n$. The map $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ defined by

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \ldots + c_{n-1}\beta^{n-1}$$

for $c_i \in F$ is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugate over F.

Definition 4.0.2 An isomorphism of a field onto itself is an **automorphism of the field**.

Definition 4.0.3 If σ is an isomorphism of a field E onto some field, then an element a of E is **left fixed by** σ if $\sigma(a) = a$. A collection S of isomorphisms of E **leaves a subfield** F **of** E **fixed** if each $a \in F$ is left fixed for every $\sigma \in S$. If $\{\sigma\}$ leaves F fixed, then σ **leaves** F **fixed**.

Theorem 4.0.2 Let $\{\sigma_i : i \in I\}$ be a collection of automorphisms of a field E. Then the set $E_{\{\sigma_i\}}$ of all $a \in E$ left fixed by every σ_i for $i \in I$ forms a subfield of E.

Definition 4.0.4 The field $E_{\{\sigma_i\}}$ of the previous theorem is the **fixed field of** $\{\sigma_i : i \in I\}$. For a single automorphism σ, we shall refer to $E_{\{\sigma\}}$ as the **fixed field of** σ.

Theorem 4.0.3 The set of all automorphisms of a field E is a group under function composition.

Theorem 4.0.4 Let E be a field, and let F be a subfield of E. Then the set $G(E/F)$ of all automorphisms of E leaving F fixed forms a subgroup of the group of all automorphisms of E. Furthermore, $F \leq E_{G(E/F)}$.

Definition 4.0.5 The group $G(E/F)$ is the **group of automorphisms of** E **leaving** F **fixed**, or, more briefly, the **group of** E **over** F.

Theorem 4.0.5 Let F be a field of characteristic p. Then the map $\sigma_p : F \to F$ defined by $\sigma_p(a) = a^p$ for $a \in F$ is an automorphism, the **Frobenius automorphism**, of F. Also, $F_{\{\sigma_p\}} \cong \mathbb{Z}_p$.

4.0.2 Problems

1. Find all conjugates in $\mathbb{C}$ of:
   (a) $\sqrt{2}+i$ over $\mathbb{Q}$;
   (b) $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}(\sqrt{2})$.
2. Let $E = \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. If $\tau_2 = \psi_{\sqrt{2},-\sqrt{2}}$ and $\tau_3 = \psi_{\sqrt{3},-\sqrt{3}}$ are the conjugation isomorphisms (in this case they are automorphisms of E) such that

$$\tau_2 : \mathbb{Q}(\sqrt{3},\sqrt{5})(\sqrt{2}) \to \mathbb{Q}(\sqrt{3},\sqrt{5})(-\sqrt{2}),\ \tau_3 : \mathbb{Q}(\sqrt{2},\sqrt{5})(\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{5})(-\sqrt{3}),$$

   compute $(\tau_3\tau_2)(\sqrt{2}+3\sqrt{5}) \in E$. Find the fixed field of of the automorphisms τ_3, $\tau_3\tau_2$ and of the set of automorphisms $\{\tau_2,\tau_3\}$ of E.
3. The fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(3+\sqrt{2})$ are the same, of course. Let $\alpha = 3+\sqrt{2}$.
   (a) Find a conjugate $\beta \neq \alpha$ of α over $\mathbb{Q}$.
   (b) Referring to the previous part, compare the conjugation automorphism $\psi_{\sqrt{2},-\sqrt{2}}$ of $\mathbb{Q}(\sqrt{2})$ with the conjugation isomorphism $\psi_{\alpha,\beta}$.
4. Describe the value of the Frobenius automorphism σ_2 on each element of the finite field $\mathbb{Z}_2(\alpha) = \{0,1,\alpha,1+\alpha\}$, where $\alpha^2+\alpha+1 = 0$.
5. Let E be an algebraic extension of a field F. Let $S = \{\sigma_i : i \in I\}$ be a collection of automorphisms of E such that every σ_i leaves each element of F fixed. Show that if S generates the subgroup H of $G(E/F)$, then $E_S = E_H$.
6. Determine the group $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.
7. Determine the group $G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$.

4.0.3 Solutions

1. Two elements are said to be conjugate if they are the roots of the same irreducible polynomial over some field. Thus, for the given algebraic elements we need to find its irreducible polynomial and after that all the roots of that polynomial are the conjugates of the considered element.

   (a)

$$\begin{aligned} \alpha &= \sqrt{2}+i \\ \alpha^2 &= 2+2\sqrt{2}i-1 \\ \alpha^2-1 &= 2\sqrt{2}i \\ (\alpha^2-1)^2 &= -8 \\ (\alpha^2-1)^2+8 &= 0 \end{aligned}$$

   Thus, $f(x) = irr(\alpha,\mathbb{Q}) = (x^2-1)^2+8 \in \mathbb{Q}[x]$. One can easily compute that the roots of f in $\mathbb{C}$, and thus the conjugates of α, are $\sqrt{2} \pm i$, $-\sqrt{2} \pm i$.

   (b)

$$\begin{aligned} \alpha &= \sqrt{1+\sqrt{2}} \\ \alpha^2 &= 1+\sqrt{2} \\ \alpha^2-(1+\sqrt{2}) &= 0 \end{aligned}$$

   Thus, $f(x) = \mathrm{irr}(\alpha, \mathbb{Q}(\sqrt{2}) = x^2-(1+\sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$ and the conjugates in $\mathbb{C}$ are obviously $\pm\sqrt{1+\sqrt{2}}$.

2. The automorphism τ_2 affects only $\sqrt{2}$ and maps it to $-\sqrt{2}$, whilst τ_3 maps $\sqrt{3}$ to $-\sqrt{3}$. The other elements are fixed. Thus, we have that

$$\tau_3\tau_2(\sqrt{2}+3\sqrt{5}) = \tau_3(-\sqrt{2}+3\sqrt{5}) = -\sqrt{2}+3\sqrt{5}.$$

   To find the fixed fields of some set of automorphisms, we will use the following method. First, we determine the basis of the field as a vector space over $\mathbb{Q}$. After that we see which elements the automorphisms affect. The ones that remain unaffected determine the fixed field.

   The basis of E over $\mathbb{Q}$ is

$$\{1,\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{6},\sqrt{10},\sqrt{15},\sqrt{30}\}.$$

   The automorphism τ_3 does not affect

$$\{1,\sqrt{2},\sqrt{5},\sqrt{10}\}$$

   which is the basis of $\mathbb{Q}(\sqrt{2},\sqrt{5})$ over $\mathbb{Q}$. Thus, $E_{\{\tau_3\}} = \mathbb{Q}(\sqrt{2},\sqrt{5})$. Since

$$\tau_3\tau_2(\sqrt{6}) = \tau_3\tau_2(\sqrt{2}\sqrt{3}) = \tau_3(-\sqrt{2}\sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6},$$

   the automorphism $\tau_3\tau_2$ does not affect

$$\{1,\sqrt{5},\sqrt{6},\sqrt{30}\},$$

which is the basis of $\mathbb{Q}(\sqrt{5},\sqrt{6})$ over $\mathbb{Q}$. Thus, $E_{\{\tau_3\tau_2\}} = \mathbb{Q}(\sqrt{5},\sqrt{6})$. The automorphisms $\{\tau_2,\tau_3\}$ do not affect

$$\{1,\sqrt{5}\},$$

which is the basis of $\mathbb{Q}(\sqrt{5})$. Thus, $E_{\{\tau_2,\tau_3\}} = \mathbb{Q}(\sqrt{5})$.

3. (a) It is easy to see that $\alpha = 3+\sqrt{2}$ is the root of the irreducible polynomial $(x-3)^2-2$ over $\mathbb{Q}$. The other remaining root of the same polynomial is $3-\sqrt{2}$. Thus, $3\pm\sqrt{2}$ are conjugates over $\mathbb{Q}$.

   (b) Both $\psi_{\sqrt{2},-\sqrt{2}}$ and $\psi_{\alpha,\beta}$ are automorphisms of $\mathbb{Q}(\sqrt{2})$. Each element of $\mathbb{Q}(\sqrt{2})$ can be written as $x+\sqrt{2}y$ for some $x,y\in\mathbb{Q}$. Since the automorphisms leave x and y fixed, let us consider where $\sqrt{2}$ is mapped under these automorphisms. We have the following:

$$\begin{aligned}\psi_{\sqrt{2},-\sqrt{2}}(\sqrt{2}) &= -\sqrt{2}\\ \psi_{\alpha,\beta}(\sqrt{2}) &= \psi_{\alpha,\beta}(-3+(3+\sqrt{2})) = -3+(3-\sqrt{2}) = -\sqrt{2}\end{aligned}$$

   Thus, we conclude that $\psi_{\sqrt{2},-\sqrt{2}} = \psi_{\alpha,\beta}$.

4.

$$\begin{aligned}\sigma_2(0) &= 0^2 = 0\\ \sigma_2(1) &= 1^2 = 1\\ \sigma_2(\alpha) &= \alpha^2 = -\alpha-1 = \alpha+1\\ \sigma_2(\alpha+1) &= (\alpha+1)^2 = \alpha^2+1 = -\alpha-1+1 = -\alpha = \alpha\end{aligned}$$

   Thus, it is easy to see that $\mathbb{Z}_2(\alpha)_{\{\sigma_2\}} = \mathbb{Z}_2$.

5. Since $S\subset H$, obviously $E_H \subseteq E_S$ (because the set S is smaller than H, thus there are at least as many automorphisms that fix S as there are for H). Let $x\in E_S$ and let $\psi\in H$ be arbitrary. Since S generates H, there exists $\sigma_1,\dots,\sigma_k\in S$ such that $\psi = \sigma_1\dots\sigma_k$. We note that

$$\psi(x) = \sigma_1\dots\sigma_{k-1}\sigma_k(x) = \sigma_1\dots\sigma_{k-1}(x) = \dots = \sigma_1(x) = x.$$

   In other words, x is fixed by an arbitrary automorphism in H, that is, $x\in E_H$. Hence, $E_S\subseteq E_H$ and thus $E_S = E_H$.

6. An automorphism in $G(E/\mathbb{Q})$ is completely determined by its values on $\sqrt[3]{2}$, where $E = \mathbb{Q}(\sqrt[3]{2})$. Let $\sigma\in G(E/\mathbb{Q})$ be arbitrary. We have that

$$\begin{aligned}\sigma(c_0+c_1\sqrt[3]{2}+c_2\sqrt[3]{2}^2) &= \sigma(c_0)+\sigma(c_1)\sigma(\sqrt[3]{2})+\sigma(c_2)\sigma(\sqrt[3]{2}^2)\\ &= c_0+c_1\sigma(\sqrt[3]{2})+c_2\sigma(\sqrt[3]{2}),\end{aligned}$$

   since σ fixes the elements in $\mathbb{Q}$. Note that $\mathrm{irr}(\sqrt[3]{2},\mathbb{Q}) = x^2-2$. Furthermore,

$$\sigma(\sqrt[3]{2})^3-2 = \sigma(\sqrt[3]{2}^3)-\sigma(2) = \sigma(\sqrt[3]{2}^3-2) = \sigma(0) = 0,$$

   that is, $\sigma(\sqrt[3]{2})$ is a root of $x^3-2\in\mathbb{Q}[x]$. Since the only real root (more precisely, only root in $\mathbb{Q}(\sqrt[3]{2})$) of x^3-2 is $\sqrt[3]{2}$, we must have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus, $\sigma = \iota$. Hence, $G(E/\mathbb{Q}) = \{\iota\}$.

7. If we consider $\mathbb{Q}(\sqrt{2},\sqrt{3})$ as $\mathbb{Q}(\sqrt{3})(\sqrt{2})$, the conjugation isomorphism $\psi_{\sqrt{2},-\sqrt{2}}$ defined by
$$\psi_{\sqrt{2},-\sqrt{2}}(a+b\sqrt{2}) = a-b\sqrt{2},\ a,b\in\mathbb{Q}(\sqrt{3})$$
is an automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, which has $\mathbb{Q}(\sqrt{3})$ as a fixed field (similar conclusions as in Problem 2). Analogously, $\psi_{\sqrt{3},-\sqrt{3}}$ is an automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ having $\mathbb{Q}(\sqrt{2})$ as a fixed field. Let ι be the identity, $\sigma_1 = \psi_{\sqrt{2},-\sqrt{2}}$, $\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}}$ and $\sigma_3 = \sigma_1\sigma_2$ (which is also an automorphism as a composition of automorphisms). The group of all automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ has a fixed field, by Theorem 4.0.2. Trivially, this fixed field must contain $\mathbb{Q}$ as automorphisms of a field leave 1 fixed and, as a consequence of that, leave $\mathbb{Q}$ fixed. If we consider the set of automorphisms $G=\{\iota,\sigma_1,\sigma_2,\sigma_3\}$, they move all elements of the basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$, except 1. Thus, $\mathbb{Q}(\sqrt{2},\sqrt{3})_G=\mathbb{Q}$. It can be easily checked that G forms a group under function composition. The group table for G is given below:

$\circ$	ι	σ_1	σ_2	σ_3
ι	ι	σ_1	σ_2	σ_3
σ_1	σ_1	ι	σ_3	σ_2
σ_2	σ_2	σ_3	ι	σ_1
σ_3	σ_3	σ_2	σ_1	ι

We will now show that $G=G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. Since the basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ is $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$, an automorphism τ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ leaving $\mathbb{Q}$ fixed, is completely determined by its values on $\sqrt{2}$ and $\sqrt{3}$. Now, ι, σ_1, σ_2 and σ_3 give all possible combinations of values on $\sqrt{2}$ and $\sqrt{3}$, and hence all possible automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

4.0.4 Additional problems

1. Find all conjugates in $\mathbb{C}$ of
   (a) $\sqrt{2}-\sqrt{3}$ over $\mathbb{Q}$;
   (b) $\sqrt{2}+i$ over $\mathbb{R}$;
   (c) $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$.
2. With the same notation as in Problem 2, compute the indicated element of E:
   (a) $\tau_2(\sqrt{2}+\sqrt{5})$;
   (b) $(\tau_5\tau_3)\left(\frac{\sqrt{2}-3\sqrt{5}}{2\sqrt{3}-\sqrt{2}}\right)$;
   (c) $(\tau_5^2\tau_3\tau_2)(\sqrt{2}+\sqrt{45})$,
   where $\tau_5=\psi_{\sqrt{5},-\sqrt{5}}:(\mathbb{Q}(\sqrt{2},\sqrt{3}))(\sqrt{5})\rightarrow(\mathbb{Q}(\sqrt{2},\sqrt{3}))(-\sqrt{5})$.
3. Referring to the previous example, compute the fixed fields of the automorphisms or set of automorphisms of E:
   (a) σ_3^2;
   (b) $\{\sigma_2,\sigma_3,\sigma_5\}$;
   (c) $\sigma_5\sigma_3\sigma_2$.
4. Let $F(\alpha_1,\dots,\alpha_n)$ be an extension field of F. Show that any automorphism σ of $F(\alpha_1,\dots,\alpha_n)$ leaving F fixed is completely determined by the n values of $\sigma(\alpha_i)$. (Hint: Use mathematical induction on n).
5. Determine the group $G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$.

Index