

MTH 310
Lecture Notes
Based on Hungerford, Abstract Algebra

Ulrich Meierfrankenfeld

Department of Mathematics
Michigan State University
East Lansing MI 48824
meier@math.msu.edu

April 20, 2020

Contents

1	Rings	5
1.1	Definitions and Examples	5
1.2	Elementary Properties of Rings	10
1.3	The General Associative, Commutative and Distributive Laws in Rings	14
1.4	Divisibility and Congruence in Rings	18
1.5	Congruence in the ring of integers	26
1.6	Modular Arithmetic in Commutative Rings	30
1.7	Subrings	38
1.8	Units in Rings	41
1.9	The Euclidean Algorithm for Integers	46
1.10	Integral Primes	51
1.11	Isomorphism and Homomorphism	53
1.12	The ‘Associated’ Relation on a Ring	64
2	Polynomial Rings	69
2.1	Addition and Multiplication	69
2.2	The degree of a polynomial	75
2.3	Divisibility in $F[x]$	78
2.4	The Euclidean Algorithm for Polynomials	84
2.5	Irreducible Polynomials	89
2.6	Polynomials and Homomorphism	96
2.7	Polynomial function	99
2.8	Irreducibility in $\mathbb{Q}[x]$	106
2.9	The Congruence Relation	112
2.10	Congruence Class Arithmetic	115
2.11	$F_p[\alpha]$ when p is irreducible	119
3	Ideals and Quotients	123
3.1	Ideals	123
3.2	Quotient Rings	127

A	Set, Relations and Functions	135
A.1	Logic	135
A.2	Rules of Logic	140
A.3	Sets	144
A.4	Relations and Functions	149
A.5	The Natural Numbers and Induction	157
A.6	Equivalence Relations	161
A.7	Partitions	166
B	Real numbers, integers and natural numbers	169
B.1	Definition of the real numbers	169
B.2	Algebraic properties of the integers	171
B.3	Properties of the order on the integers	171
B.4	Properties of the natural numbers	171
C	The Associative, Commutative and Distributive Laws	173
C.1	The General Associative Law	173
C.2	The general commutative law	174
C.3	The General Distributive Law	176
D	Verifying Ring Axioms	179
E	Constructing rings from given rings	181
E.1	Direct products of rings	181
E.2	Matrix rings	181
E.3	Polynomial Rings	184
F	Cardinalities	191
F.1	Cardinalities of Finite Sets	191
G	List of Important Theorems and Definitions	193

Chapter 1

Rings

1.1 Definitions and Examples

Let A and B be sets. Then $a \in A$ means that a is a member of A . Recall from A.4.3 that

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

(so $A \times B$ is the set consisting of all ordered pairs whose first coordinate is in A and the second in B .)

Definition 1.1.1. A ring is a triple $(R, +, \cdot)$ such that

- (i) R is a set;
- (ii) $+$ is a function (called ring addition) and $R \times R$ is a subset of the domain of $+$. For $(a, b) \in R \times R$, $a + b$ denotes the image of (a, b) under $+$;
- (iii) $\cdot$ is a function (called ring multiplication) and $R \times R$ is a subset of the domain of $\cdot$. For $(a, b) \in R \times R$, $a \cdot b$ (and also ab) denotes the image of (a, b) under $\cdot$;

and such that the following eight statements hold:

- (Ax 1) $a + b \in R$ for all $a, b \in R$; [closure of addition]
- (Ax 2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$; [associative addition]
- (Ax 3) $a + b = b + a$ for all $a, b \in R$. [commutative addition]
- (Ax 4) there exists an element in R , denoted by 0_R and called ‘zero R ’, [additive identity]
such that $a = a + 0_R$ and $a = 0_R + a$ for all $a \in R$;
- (Ax 5) for each $a \in R$ there exists an element in R , denoted by $-a$ [additive inverses]
and called ‘negative a ’, such that $a + (-a) = 0_R$ and $(-a) + a = 0_R$;

(Ax 6) $ab \in R$ for all $a, b \in R$; [closure of multiplication]

(Ax 7) $a(bc) = (ab)c$ for all $a, b, c \in R$; [associative multiplication]

(Ax 8) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$. [distributive laws]

In the following we will often just write R for $(R, +, \cdot)$.

Definition 1.1.2. Let R be a ring. Then R is called commutative if

(Ax 9) $ab = ba$ for all $a, b \in R$. [commutative multiplication]

Definition 1.1.3. Let R be a ring. We say that R is a ring with identity if there exists an element, denoted by 1_R and called ‘one R ’, such that

(Ax 10) $a = 1_R \cdot a$ and $a = a \cdot 1_R$ for all $a \in R$. [multiplicative identity]

Example 1.1.4. (a) $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

(b) $(\mathbb{Q}, +, \cdot)$ is a commutative ring with identity.

(c) $(\mathbb{R}, +, \cdot)$ is a commutative ring with identity.

(d) $(\mathbb{C}, +, \cdot)$ is a commutative ring with identity.

(e) If R is a ring, then R cannot be the empty set. Indeed, **Ax 4** implies that there exists an element (namely 0_R) in R . But note that all other axioms do hold for $R = \emptyset$.

(f) Suppose $R = \{0_R\}$ and define an addition $+$ and multiplication $\cdot$ on R by

$$\begin{array}{c|c} + & 0_R \\ \hline 0_R & 0_R \end{array} \quad \text{and} \quad \begin{array}{c|c} \cdot & 0_R \\ \hline 0_R & 0_R \end{array}$$

Then $(R, +, \cdot)$ is a commutative ring with identity $1_R = 0_R$.

(g) Let $\mathbb{Z}_2 = \{0, 1\}$ and define an addition $\oplus$ and a multiplication $\odot$ on $\mathbb{Z}_2$ by

$$\begin{array}{c|cc} \oplus & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \odot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Then $(\mathbb{Z}_2, \oplus, \odot)$ is a commutative ring with identity.

(h) Let $2\mathbb{Z}$ be the set of even integers. Then $(2\mathbb{Z}, +, \cdot)$ is a commutative ring without a multiplicative identity.

- (i) Let $n \in \mathbb{Z}$ with $n > 1$. The set $M_n(\mathbb{R})$ of $n \times n$ matrices with coefficients in $\mathbb{R}$ together with the usual addition and multiplication of matrices is a non-commutative ring with identity.
- (j) Let $n \in \mathbb{Z}$ with $n > 1$. Then $M_n(2\mathbb{Z})$ is non-commutative ring without an identity.

Example 1.1.5. Let $R = \{0, 1\}$ and $a, b \in R$. Define an addition and multiplication on R by

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & a \end{array} \quad \text{and} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & b \end{array}$$

For which values of a and b is $(R, +, \cdot)$ a ring?

Note first that 0 is the additive identity, so $0_R = 0$.

Case 1. Suppose that $a = 1$:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & b \end{array}$$

Then $1 + x = 1 \neq 0 = 0_R$ for all $x \in R$ and so 1 does not have an additive inverse. Hence R is not a ring.

Case 2. Suppose that $a = 0$ and $b = 1$:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Then $(R, +, \cdot)$ is $(\mathbb{Z}_2, \oplus, \odot)$ and so R is commutative ring with identity 1.

Case 3. Suppose that $a = 0$ and $b = 0$:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 0 \end{array}$$

Then $xy = 0$ for all $x, y \in R$. Note also that $0 + 0 = 0$. It follows that Axioms 6-8 hold, indeed all expressions evaluate to 0. Axiom 1-5 hold since the addition is the same as in $\mathbb{Z}_2$. So R is a ring. R is commutative, but does not have an identity.

Example 1.1.6. Let $R = \{0, 1\}$. Define an addition and multiplication on R by

$$\begin{array}{c|cc} \oplus & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \otimes & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}$$

Is $(R, \oplus, \otimes)$ a ring?

Note that 1 is an additive identity, so $0_R = 1$. Also 0 is a multiplicative identity. So $1_R = 0$. Using the symbols 0_R and 1_R we can write the addition and multiplication table as follows:

$$\begin{array}{c|cc} \oplus & 0_R & 1_R \\ \hline 0_R & 0_R & 1_R \\ 1_R & 1_R & 0_R \end{array} \quad \text{and} \quad \begin{array}{c|cc} \otimes & 0_R & 1_R \\ \hline 0_R & 0_R & 0_R \\ 1_R & 0_R & 1_R \end{array}$$

Indeed, most entries in the tables are determined by the fact that 0_R and 1_R are the additive and multiplicative identity, respectively. Also $1_R \oplus 1_R = 0 \oplus 0 = 1 = 0_R$ and $0_R \otimes 0_R = 1 \otimes 1 = 1 = 0_R$.

Observe now that the new tables are the same as for $\mathbb{Z}_2$. So $(R, \oplus, \otimes)$ is a ring.

Theorem 1.1.7. Let R and S be rings. Recall from A.4.3 that $R \times S = \{(r, s) \mid r \in R, s \in S\}$. Define an addition and multiplication on $R \times S$ by

$$\begin{aligned} (r, s) + (r', s') &= (r + r', s + s') \\ (r, s)(r', s') &= (rr', ss') \end{aligned}$$

for all $r, r' \in R$ and $s, s' \in S$. Then

- (a) $R \times S$ is a ring;
- (b) $0_{R \times S} = (0_R, 0_S)$;
- (c) $-(r, s) = (-r, -s)$ for all $r \in R, s \in S$;
- (d) if R and S are both commutative, then so is $R \times S$;
- (e) if both R and S have an identity, then $R \times S$ has an identity and $1_{R \times S} = (1_R, 1_S)$.

Proof. See Exercise 1.1#6. □

Example 1.1.8. Determine the addition and multiplication table of the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Recall from (1.1.4)(b) that $\mathbb{Z}_2 = \{0, 1\}$. So

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

and

·	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)
(1,0)	(0,0)	(0,0)	(1,0)	(1,0)
(1,1)	(0,0)	(0,1)	(1,0)	(1,1)

Exercises 1.1:

1.1#1. Verify that the triple $(\mathbb{Z}_2, \oplus, \odot)$ from Example (1.1.4)(g) is a ring.

1.1#2. Let R be a ring and $a, b, c, d \in R$. Prove that

$$(a + b)(c + d) = ((ac + ad) + bd) + bc$$

In each step of your proof, quote exactly one axiom of a ring.

1.1#3. Prove or give a counterexample:

If R is a ring with identity, then $1_R \neq 0_R$.

1.1#4. Let $E = \{0, e, b, c\}$ with addition and multiplication defined by the following tables. Assume associativity and distributivity and show that R is a ring with identity. Is R commutative?

+	0	e	b	c	·	0	e	b	c
0	0	e	b	c	0	0	0	0	0
e	e	0	c	b	e	0	e	b	c
b	b	c	0	e	b	0	b	b	0
c	c	b	e	0	c	0	c	0	c

1.1#5. Below are parts of the addition table and parts of the multiplication table of a ring. Complete both tables.

+	w	x	y	z
w	w			
x			y	z
y			z	w
z		w		y

·	w	x	y	z
w				
x			y	
y				
z				

1.1#6. Prove Theorem 1.1.7.

1.2 Elementary Properties of Rings

Theorem 1.2.1. *Let R be ring and $a, b \in R$. Then*

$$(b + a) + (-b) = (a + b) + (-b) = a$$

and

$$(-b) + (a + b) = (-b) + (b + a) = a.$$

Proof.

$$\begin{aligned}
 (b + a) + (-b) &= (a + b) + (-b) && \text{-- Ax 3} \\
 &= a + (b + (-b)) && \text{-- Ax 2} \\
 &= a + 0_R && \text{-- Ax 5} \\
 &= a && \text{-- Ax 4}
 \end{aligned}$$

Hence the first statement holds. The second statement is proved similarly, see Exercise 1.2#1. $\square$

In the proof of the next theorem we will use the Principal of Substitution, see A.1.1:

Let $\Phi(x)$ be a formula involving a variable x . For an object a let $\Phi(a)$ be the formula obtained by replacing all occurrences of x by b . Then

$$a = b \implies \Phi(a) = \Phi(b)$$

For example if $a = b$, then the Principal of Substitution applied with $\Phi(x) = x^3 + x$ gives $a^3 + a = b^3 + b$.

Theorem 1.2.2 (Additive Cancellation Law). *Let R be ring and $a, b, c \in R$. Then*

$$\begin{aligned}
& a = b \\
\iff & c + a = c + b \\
\iff & a + c = b + c
\end{aligned}$$

Proof.

$$\begin{aligned}
& a = b \\
\implies & c + a = c + b \quad - \text{Principal of Substitution A.1.1 with } \Phi(x) = c + x \\
\implies & a + c = b + c \quad - \mathbf{Ax\,3}, \text{ twice} \\
\implies & (a + c) + (-c) = (b + c) + (-c) \quad - \text{Principal of Substitution A.1.1 with } \Phi(x) = x + (-c) \\
\implies & a = b \quad - 1.2.1, \text{ twice}
\end{aligned}$$

□

Definition 1.2.3. Let R be a ring and $a \in R$. Then a is called an additive identity of R if

$$a + c = c \quad \text{and} \quad c + a = c$$

for all $c \in R$.

Theorem 1.2.4 (Additive Identity Law). Let R be a ring and $a, c \in R$. Then

$$\begin{aligned}
& a = 0_R \\
\iff & c + a = c \\
\iff & a + c = c
\end{aligned}$$

In particular, 0_R is the unique additive identity of R .

Proof. By the Additive Cancellation Law 1.2.2

$$a = b \iff c + a = c + b \iff a + c = b + c$$

For $b = 0_R$ this gives

$$a = 0_R \iff c + a = c + 0_R \iff a + c = 0_R + c$$

By **Ax 4** $c + 0_R = c$ and $0_R + c = c$. So :

$$a = 0_R \iff c + a = c \iff a + c = c.$$

□

Definition 1.2.5. Let R be a ring and $c \in R$. An additive inverse of c is an element a in R with

$$a + c = 0_R \quad \text{and} \quad c + a = 0_R.$$

Theorem 1.2.6 (Additive Inverse Law). Let R be a ring and $a, c \in R$. Then

$$\begin{aligned} a &= -c \\ \iff c + a &= 0_R \\ \iff a + c &= 0_R \end{aligned}$$

In particular, $-c$ is the unique additive inverse of c .

Proof. By the Additive Cancellation Law 1.2.2

$$a = b \iff c + a = c + b \iff a + c = b + c$$

For $b = -c$ this gives

$$a = 0_R \iff c + a = c + (-c) \iff a + c = (-c) + c$$

By **Ax 5** $c + (-c) = 0_R$ and $(-c) + c = 0_R$. So :

$$a = 0_R \iff c + a = 0_R \iff a + c = 0_R.$$

□

Definition 1.2.7. Let R be a ring and $a, b \in R$. Then $a - b := a + (-b)$. Note here that $-b \in R$ by **Ax 5** and so $a - b = a + (-b) \in R$ by **Ax 1**.

Theorem 1.2.8. Let R be ring and $a, b, c \in R$. Then

$$\begin{aligned} c &= b - a \\ \iff c + a &= b \\ \iff a + c &= b \end{aligned}$$

Proof.

$$\begin{aligned} a + c &= b \\ \iff c + a &= b && - \text{Ax 3} \\ \iff (c + a) + (-a) &= b + (-a) && - \text{Additive Cancellation Law 1.2.2} \\ \iff c &= b - a && - 1.2.1 \text{ and Definition of } b - a \end{aligned}$$

□

Theorem 1.2.9. Let R be a ring and $a, b, c \in R$. Then

- (a) $-0_R = 0_R$ (g) $-(a + b) = (-a) + (-b) = (-a) - b$.
 (b) $a - 0_R = a$. (h) $-(a - b) = (-a) + b = b - a$.
 (c) $a \cdot 0_R = 0_R = 0_R \cdot a$. (i) $(-a) \cdot (-b) = ab$.
 (d) $a \cdot (-b) = -(ab) = (-a) \cdot b$. (j) $a \cdot (b - c) = ab - ac$ and $(a - b) \cdot c = ac - bc$.
 (e) $-(-a) = a$. (k) If R has an identity 1_R , then
 (f) $b - a = 0_R$ if and only if $a = b$. $(-1_R) \cdot a = -a = a \cdot (-1_R)$.

Proof. (a) By **Ax 4** $0_R + 0_R = 0_R$ and so by the Additive Inverse Law 1.2.6 $0_R = -0_R$.

$$(b) \quad a - 0_R \stackrel{\text{Def: } -}{=} a + (-0_R) \stackrel{(a)}{=} a + 0_R \stackrel{\text{Ax 4}}{=} a.$$

(c) We compute

$$a \cdot 0_R \stackrel{\text{Ax 4}}{=} a \cdot (0_R + 0_R) \stackrel{\text{Ax 8}}{=} a \cdot 0_R + a \cdot 0_R,$$

and so by the Additive Identity Law 1.2.4 $a \cdot 0_R = 0_R$. Similarly $0_R \cdot a = 0_R$.

(d) We have

$$ab + a \cdot (-b) \stackrel{\text{Ax 8}}{=} a \cdot (b + (-b)) \stackrel{\text{Def: } -b}{=} a \cdot 0_R \stackrel{(c)}{=} 0_R.$$

So by the Additive Inverse Law 1.2.6 $-(ab) = a \cdot (-b)$. Similarly, $(-a) \cdot b = -(ab)$.

(e) By **Ax 5**, $a + (-a) = 0_R$ and so by the Additive Inverse Law 1.2.6, $a = -(-a)$.

(f) By Theorem 1.2.8 we have

$$c = b - a \quad \Longleftrightarrow \quad c + a = b$$

With $c = 0_R$ this gives

$$0_R = b - a \quad \Longleftrightarrow \quad 0_R + a = b.$$

By **Ax 4** $0_R + a = a$ and so the Principal of Substitution gives

$$0_R = b - a \quad \Longleftrightarrow \quad a = b.$$

(g)

$$(a + b) + ((-a) + (-b)) \stackrel{\text{Ax 2}}{=} ((a + b) + (-a)) + (-b) \stackrel{1.2.1}{=} b + (-b) \stackrel{\text{Ax 5}}{=} 0_R.$$

and so by the Additive Inverse Law 1.2.6 $-(a + b) = (-a) + (-b)$. By definition of ‘ $-$ ’, $(-a) + (-b) = (-a) - b$.

(h)

$$-(a - b) \stackrel{\text{Def: } -}{=} -(a + (-b)) \stackrel{(g)}{=} (-a) + (-(-b)) \stackrel{(e)}{=} (-a) + b \stackrel{\text{Def: } -}{=} b - a.$$

$$(i) \quad (-a) \cdot (-b) \stackrel{(d)}{=} a \cdot (-(-b)) \stackrel{(e)}{=} a \cdot b.$$

$$(j) \quad a \cdot (b - c) \stackrel{\text{Def}}{=} a \cdot (b + (-c)) \stackrel{\text{Ax 8}}{=} a \cdot b + a \cdot (-c) \stackrel{(d)}{=} ab + (-ac) \stackrel{\text{Def}}{=} ab - ac.$$

Similarly $(a - b) \cdot c = ab - ac$.

(k) Suppose now that R has an additive identity. Then

$$(-1_R)a \stackrel{(d)}{=} -(1_R a) \stackrel{\text{Ax 10}}{=} -a.$$

□

Exercises 1.2:

1.2#1. Let R be ring and $a, b \in R$. Show that $(-b) + (a + b) = (-b) + (b + a) = a$.

1.2#2. Let R be a ring and $a, b, c, d \in R$. Prove that

$$(a - b)(c - d) = ((ac - ad) + bd) - bc$$

In each step of your proof, quote exactly one Axiom, Definition or Theorem.

1.2#3. Let R be a ring and let $a, b, c, d, e \in R$. Show that

$$(ab + e) + b = d - ac \quad \Longleftrightarrow \quad a(b + c) + b = d - e.$$

1.2#4. Let R be a ring with identity. Show that $R = \{0_R\}$ if and only if $1_R = 0_R$.

1.2#5. Let R be a ring such that $a \cdot a = 0_R$ for all $a \in R$. Show that $ab = -(ba)$ for all $a, b \in R$.

1.2#6. Let R be a ring such that $a \cdot a = a$ for all $a \in R$. Show that

$$(a) \quad a + a = 0_R \text{ for all } a \in R$$

$$(b) \quad R \text{ is commutative.}$$

1.3 The General Associative, Commutative and Distributive Laws in Rings

Example 1.3.1. Let a, b, c, d be elements in the ring R . Consider the expression

$$a + b + c + d$$

This expression is not defined without parenthesis. How many ways are there to choose parentheses? Are the resulting sums the same?

$$(a + (b + c)) + d, \quad (a + b) + (c + d), \quad ((a + b) + c) + d, \quad a + (b + (c + d)), \quad a + ((b + c) + d)$$

Also

$$((a + b) + c) + d \stackrel{\mathbf{Ax} 2}{=} (a + (b + c)) + d \stackrel{\mathbf{Ax} 2}{=} a + ((b + c) + d) \stackrel{\mathbf{Ax} 2}{=} a + (b + (c + d)) \stackrel{\mathbf{Ax} 2}{=} (a + b) + (c + d)$$

so all five sums are the same.

Definition 1.3.2. Let R be a ring, $n \in \mathbb{N}^1$ and $a_1, a_2, \dots, a_n \in R$. Recursively, we say that z is a sum of $(a_1, \dots, a_n)$ in R provided that one of the following holds:

- (1) $n = 0$ and $z = 0_R$.
- (2) $n = 1$ and $z = a_1$.
- (3) $n > 1$ and there exist an integer k with $1 \leq k < n$ and $x, y \in R$ such that
 - (i) x is sum of $(a_1, \dots, a_k)$ in R ,
 - (ii) y is a sum of $(a_{k+1}, a_{k+2}, \dots, a_n)$ in R , and
 - (iii) $z = x + y$.

Example 1.3.3. Let R be a ring and $a, b, c, d \in R$. List all sums of $()$, (a) , (a, b) , (a, b, c) and (a, b, c, d) in R .

Sums of $()$: We have $n = 0$ and 0_R is the only sum of $()$.

Sums of (a) : We have $n = 1$ and a is the only sum of (a) .

Sums of (a, b) : Then $n = 2$ and $1 \leq k < 2$. So $k = 1$. Thus x is a sum of (a) and y a sum of (b) . Hence $x = a, y = b$ and $z = x + y = a + b$, So $a + b$ is the only sum of (a, b) .

Sums of (a, b, c) : We have $n = 3$ and $1 \leq k < 3$. So $k = 1$ or 2 .

If $k = 1$, then x is a sum of (a) and y a sum of (b, c) . So $x = a, y = b + c$ and $z = x + y = a + (b + c)$.

If $k = 2$, then x is a sum of (a, b) and y a sum of (c) . So $x = a + b, y = c$ and $z = x + y = (a + b) + c$.

So $a + (b + c)$ and $(a + b) + c$ are the sums of (a, b, c) .

Sums of (a, b, c, d) : We have $n = 4$ and $1 \leq k < 4$. Thus $k = 1, 2$ or 3 .

If $k = 1$, then x is a sum of (a) and y a sum of (b, c, d) . So $x = a$ and $y = b + (c + d)$ or $y = (b + c) + d$. As $z = x + y$ we get $z = a + (b + (c + d))$ or $z = a + ((b + c) + d)$.

If $k = 2$, then x is a sum of (a, b) and y a sum of (c, d) . So $x = a + b, y = c + d$ and $z = x + y = (a + b) + (c + d)$.

If $k = 3$, then x is a sum of (a, b, c) and y a sum of (d) . So $x = a + (b + c)$ or $x = (a + b) + c$, and $y = d$. As $z = x + y$ we get $z = (a + (b + c)) + d$ or $z = ((a + b) + c) + d$,

¹ $\mathbb{N}$ is the set on natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

So the sums of (a, b, c, d) are $a + (b + (c + d))$, $a + ((b + c) + d)$, $(a + b) + (c + d)$, $(a + (b + c)) + d$ and $((a + b) + c) + d$

We remark that the numbers of formal sums of an $n + 1$ -tuple is the n -th Catalan number

$$C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{2n!}{n!(n+1)!}$$

For example the number of formal sums of a 4-tuple is $C_3 = \frac{6!}{3!4!} = \frac{6 \cdot 5}{6} = 5$.

Definition 1.3.4. Let R be a ring, $n \in \mathbb{N}$ and $a_1, a_2, \dots, a_n \in R$. Suppose $n > 0$ or R has an identity. Products of $(a_1, \dots, a_n)$ in R are defined similarly as in (1.3.2)(3), just replace ‘sum’ by ‘product’, ‘+’ by ‘ $\cdot$ ’ and ‘ 0_R ’ by ‘ 1_R ’.

Theorem 1.3.5 (General Associative Law, GAL). Let R be a ring, $n \in \mathbb{N}$ and $a_1, a_2, \dots, a_n$ elements of R .

- (a) Let z and z' be sums of $(a_1, a_2, \dots, a_n)$ in R . Then $z = z'$.
- (b) Suppose $n > 0$ or R has an identity. Let z and z' be products of $(a_1, a_2, \dots, a_n)$ in R . Then $z = z'$.

Proof. See C.1.3 □

Notation 1.3.6. Let R be a ring, $n \in \mathbb{N}$ and $a, a_1, a_2, \dots, a_n \in R$.

- (a) We denote the unique sum of $(a_1, \dots, a_n)$ in R by

$$\sum_{i=1}^n a_i \quad \text{and also by} \quad a_1 + a_2 + \dots + a_n;$$

- (b) We define

$$na := \sum_{i=1}^n a = \underbrace{a + a + \dots + a}_{n\text{-times}}$$

For (c) and (d) suppose that $n > 0$ or R has an identity:

- (c) We denote the unique product of $(a_1, \dots, a_n)$ by

$$\prod_{i=1}^n a_i \quad \text{and also by} \quad a_1 a_2 \dots a_n.$$

- (d) We define

$$a^n := \prod_{i=1}^n a = \underbrace{aa \dots a}_{n\text{-times}}$$

Example 1.3.7. Let a, b, c, d, e be elements in a ring. Then by the GAL (for addition)

$$a + b + c + d + e = ((a + b) + (c + d)) + e = a + ((b + (c + d)) + e) = (a + ((b + c) + d)) + e$$

and the GAL (for multiplication)

$$abcde = (((ab)c)d)e = (ab)((cd)e)$$

Theorem 1.3.8 (General Commutative Law, GCL). *Let R be a ring, $n \in \mathbb{Z}^{+2}$, $a_1, a_2, \dots, a_n \in R$ and*

$$f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

a bijection.

(a)

$$\sum_{i=1}^n a_i = \sum_{i=1}^n a_{f(i)},$$

that is, if z is sum of $(a_1, \dots, a_n)$ and z' is a sum of $(a_{f(1)}, \dots, a_{f(n)})$, then $z = z'$.

(b) *Suppose that R is commutative. Then*

$$\prod_{i=1}^n a_i = \prod_{i=1}^n a_{f(i)}.$$

that is, if z is product of $(a_1, \dots, a_n)$ and z' is a product of $(a_{f(1)}, \dots, a_{f(n)})$, then $z = z'$.

Proof. See C.2.2 □

Example 1.3.9. Let R be a ring and a, b, c, d, e in R . Then by the General Commutative Law:

$$a + b + c + d + e = d + c + a + b + e = b + a + c + d + e.$$

and if R is commutative:

$$abc = acb = bac = bca = cab = cba.$$

Theorem 1.3.10 (General Distributive Law, GDL). *Let R be a ring, $n, m \in \mathbb{Z}^+$ and $a_1, \dots, a_n, b_1, \dots, b_m \in R$. Then*

$$\left(\sum_{i=1}^n a_i \right) \cdot \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \left(\sum_{j=1}^m a_i b_j \right) = \sum_{j=1}^m \left(\sum_{i=1}^n a_i b_j \right)$$

Proof. See C.3.2. □

² $\mathbb{Z}^+$ is the set of positive integers: $\mathbb{Z}^+ = \{1, 2, 3, 4, \dots\}$

Example 1.3.11. Let R be a ring and a, b, c, d, e in R . Then by the General Distributive Law:

$$\begin{aligned}(a + b + c)(d + e) &= (ad + ae) + (bd + be) + (cd + ce) \\ &= (ad + bd + ed) + (ae + be + de)\end{aligned}$$

Exercises 1.3:

1.3#1. Prove or give a counterexample:

Let R be a ring and $a, b \in R$. Then

$$(a + b)^2 = a^2 + 2ab + b^2.$$

(Recall here that according to Notation (1.3.6)(b) $2d := d + d$ for any d in R .)

1.3#2. Let R be a commutative ring with identity. Suppose that $1_R + 1_R = 0_R$. Prove that

$$(a + b)^2 = a^2 + b^2.$$

for all $a, b \in R$.

1.3#3. Let $S := \{a, b, c, d\}$ and let $+$ be the addition on S defined by

$+$	a	b	c	d
a	b	a	d	a
b	c	d	b	a
c	d	a	c	c
d	b	d	b	c

Compute all possible sums of (a, b, c, d) , where ‘sum’ is defined as in (1.3.2)(3).

1.4 Divisibility and Congruence in Rings

Definition 1.4.1. Let R be ring and $a, b \in R$. Then we say that a divides b in R and write $a|b$ if there exists $c \in R$ with $b = ac$ □

Example 1.4.2. (1) Does $7|133$ in $\mathbb{Z}$?

Yes, since $133 = 7 \cdot 19$.

(2) Does $2|3$ in $\mathbb{Z}$?

No since $2 \cdot k$ is even, $3 \neq 2k$ for all $k \in \mathbb{Z}$.

(3) Does $2|3$ in $\mathbb{Q}$?

Yes, since $3 = 2 \cdot \frac{3}{2}$.

(4) Does $2|2$ in $2\mathbb{Z}$ (the ring of even integers)?

No, if k is an even integers, then $2k$ is divisible by 4 and so $2 \nmid 2k$.

(5) For which $a, b, c, d \in \mathbb{R}$ does $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ divide $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $M_2(\mathbb{R})$?

$$\begin{aligned}
 & \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] \left| \left| \begin{array}{cc} a & b \\ c & d \end{array} \right. \right. \\
 \iff & \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] \cdot A = \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \text{ for some } A \in M_2(\mathbb{R}) & \quad - \text{ definition of 'divide' } \\
 \iff & \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] \cdot \left[\begin{array}{cc} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{array} \right] = \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \text{ for some } \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{R} & \quad - \text{ definition of } M_2(\mathbb{R}) \\
 \iff & \left[\begin{array}{cc} \tilde{a} & \tilde{b} \\ 0 & 0 \end{array} \right] = \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \text{ for some } \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{R} & \quad - \text{ definition of matrix multiplication } \\
 \iff & \tilde{a} = a, \tilde{b} = b, 0 = c \text{ and } 0 = d \text{ for some } \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{R} & \quad - \text{ definition of a matrix } \\
 \iff & c = 0 \text{ and } d = 0
 \end{aligned}$$

For example

$$\left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] \left| \left| \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right. \right. \quad \text{but} \quad \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] \not\left| \left| \begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array} \right. \right.$$

Note that

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

So $ca = b$ does not imply that $a|b$.

Theorem 1.4.3. *Let R be a ring and $a \in R$.*

(a) $a|0_R$.

(b) $0_R | a$ if and only if $a = 0_R$.

(c) If R is a ring with identity, then $1_R | a$ and $a | a$.

Proof. (a) By (1.2.9)(c), $0_R = a \cdot 0_R$ and so $a | 0_R$.

(b) By (a) applied with $a = 0_R$ we have $0_R | 0_R$.

Suppose now that $a \in R$ with $0_R | a$. Then there exists $b \in R$ with $a = 0_R b$. By (1.2.9)(c) we have $0_R b = 0_R$ and so $a = 0_R$.

(c) By **Ax 10** $a = 1_R a$, and so $1_R | a$. Also $a = a 1_R$ and so $a | a$. $\square$

Theorem 1.4.4. Let R be a ring and $a, b, c, u, v \in R$.

(a) $|$ is transitive, that is if $a | b$ and $b | c$, then $a | c$.

(b) $a | b \iff a | (-b) \iff (-a) | (-b) \iff (-a) | b$.

(c) Suppose that $a | b$ and $a | c$. Then

$a | (b+c)$, $a | (b-c)$, $a | (bu+c)$, $a | (bu-c)$, $a | (bu+cv)$, $a | bu - cv$, $a | (b+cv)$, $a | (b-cv)$, and $a | (bu-c)$.

Proof. (a) Let $a, b, c \in R$ such that $a | b$ and $b | c$. Then by definition of ‘divide’ there exist r and s in R with

$$(*) \quad b = ar \quad \text{and} \quad c = bs.$$

Hence

$$c \stackrel{(*)}{=} bs \stackrel{(*)}{=} (ar)s \stackrel{\text{Ax 7}}{=} a(rs).$$

Since R is closed under multiplication, $rs \in R$ and so $a | c$ by definition of ‘divide’.

(b) Let $a, b \in R$. We will first show

$$(**) \quad a | b \implies a | (-b) \quad \text{and} \quad (-a) | b.$$

Suppose that a divides b . Then by definition of ‘divide’ there exists $r \in R$ with $b = ar$. Thus

$$-b = -(ar) \stackrel{(1.2.9)(d)}{=} a(-r) \quad \text{and} \quad b = ar \stackrel{(1.2.9)(i)}{=} (-a)(-r)$$

By **Ax 5**, $-r \in R$ and so $a | (-b)$ and $(-a) | b$ by definition of ‘divide’. Thus $(**)$ holds.

Suppose $a | b$. Then by $(**)$ $a | (-b)$.

Suppose that $a | (-b)$, then by $(**)$ applied with $-b$ in place of b , $(-a) | (-b)$.

Suppose that $(-a) | (-b)$. Then by $(**)$ applied with $-a$ and $-b$ in place of a and b , $(-a) | (-b)$.

By (1.2.9)(e), $-(-b) = b$ and so $-a | b$.

Suppose that $(-a) \mid b$. Then by $(**)$ applied with $-a$ in place of a , $-(-a) \mid b$. By (1.2.9)(e), $-(-a) = a$ and so $a \mid b$.

(c) Let $a, b, c \in R$ with $a \mid b$ and $a \mid c$. Then by definition of ‘divide’ there exist r and s in R with

$$(***) \quad b = ar \quad \text{and} \quad c = as$$

Thus

$$b + c \stackrel{(***)}{=} ar + as \stackrel{\mathbf{Ax8}}{=} a(r + s) \quad \text{and} \quad b - c \stackrel{(***)}{=} ar - as \stackrel{(1.2.9)(j)}{=} a(r - s).$$

By **Ax 1** and 1.2.7, R is closed under addition and subtraction. Thus $r + s \in R$ and $r - s \in R$ and so

$$(+)\quad a \mid b + c \quad \text{and} \quad a \mid b - c.$$

By definition of ‘divide’, $b \mid bu$. By (a) ‘divide’ is transitive. Since $a \mid b$ and $b \mid bu$ we conclude that $a \mid bu$. Thus $a \mid bu$ and $a \mid c$ and $(+)$ applied with bu in place of b gives

$$a \mid (bu + c) \quad \text{and} \quad a \mid (bu - c).$$

Similarly, as $a \mid c$ and $c \mid cv$ we have $a \mid cv$. So $a \mid b$ and $a \mid cv$ and $(+)$ applied with cv in place of c gives

$$a \mid (b + cv) \quad \text{and} \quad a \mid (b - cv).$$

Moreover, since $a \mid bu$ and $a \mid cv$, we can apply $(+)$ with bu and cv in place of b and c . So

$$a \mid (bu + cv) \quad \text{and} \quad a \mid (bu - cv).$$

□

Definition 1.4.5. Let R be a ring and $n \in R$. Then the relation ‘ $\equiv \pmod{n}$ ’ on R is defined by

$$a \equiv b \pmod{n} \iff n \mid a - b.$$

If $a \equiv b \pmod{n}$ we say that a is congruent to b modulo n in R .

Example 1.4.6. (1) Consider the ring $\mathbb{Z}$:

$6 \equiv 4 \pmod{2}$ is true since 2 divides $6 - 4$.

But $3 \equiv 8 \pmod{2}$ is false since 2 does not divide $3 - 8$. Thus $3 \not\equiv 8 \pmod{2}$.

Suppose a and b are integers. Then

$$a \equiv b \pmod{2} \iff 2 \mid b - a \iff b - a \text{ is even}$$

Thus $a \equiv b \pmod{2}$ if and only if either both a and b are even, or both a and b are odd.

Hence $a \not\equiv b \pmod{2}$ if and only if one of a and b is even and the other is odd.

For example

$$2 \equiv 6 \pmod{2}, \quad 3 \equiv -7 \pmod{2}, \quad 5 \not\equiv 12 \pmod{2}, \quad -14 \not\equiv 7 \pmod{2}.$$

(2) Consider the ring $\mathbb{Q}$:

Is $3 \equiv 8 \pmod{2}$? Yes: $3 - 8 = -5$ and $-5 = 2 \cdot (-\frac{5}{2})$. Hence 2 divides $3 - 8$ in $\mathbb{Q}$ and thus $3 \equiv 8 \pmod{2}$.

(3) Let R be a ring and $a, b \in R$. Then

$$\begin{aligned} & a \equiv b \pmod{0_R} \\ \iff & 0_R | a - b && \text{-- Definition of ' } a \equiv b \pmod{0_R} \text{' } \\ \iff & a - b = 0_R && \text{-- (1.4.3)(b)} \\ \iff & a = b && \text{-- (1.2.9)(f)} \end{aligned}$$

So congruence modulo 0_R is the equality relation.

(4) Let R be a ring with identity and $a, b \in R$. By (1.4.3)(c) we have $1_R | a - b$ and so

$$a \equiv b \pmod{1_R} \quad \text{for all } a, b \in R$$

(5) When is

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{bmatrix} \left(\pmod{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}} \right)$$

in $M_2(\mathbb{R})$?

$$\begin{aligned}
& \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{bmatrix} \left(\text{mod} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right) \\
\iff & \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{bmatrix} \right. \quad \text{-- definition of '}\equiv\text{' } \\
\iff & \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \left| \begin{bmatrix} a - \tilde{a} & b - \tilde{b} \\ c - \tilde{c} & d - \tilde{d} \end{bmatrix} \right. \\
\iff & c - \tilde{c} = 0 \quad \text{and} \quad d - \tilde{d} = 0 \quad \text{-- see Example (1.4.2)(5)} \\
\iff & c = \tilde{c} \quad \text{and} \quad d = \tilde{d}
\end{aligned}$$

Theorem 1.4.7. *Let R be a ring and $n \in R$. Then the relation ' $\equiv \pmod{n}$ ' is an equivalence relation on R .*

Proof. We have to show that ' $\equiv \pmod{n}$ ' is reflexive, symmetric and transitive. Let $a, b, c \in R$.

Reflexive: By (1.2.9)(f) (c) we have $a - a = 0_R = n \cdot 0_R$. Hence $n \mid a - a$ and so $a \equiv a \pmod{n}$. Thus ' $\equiv \pmod{n}$ ' is reflexive.

Symmetric: Suppose that $a \equiv b \pmod{n}$. Then $n \mid (a - b)$. By (1.4.4)(b) this gives $n \mid -(a - b)$. By (1.2.9)(h) we have $-(a - b) = b - a$. Hence $n \mid b - a$ and so $b \equiv a \pmod{n}$. Thus ' $\equiv \pmod{n}$ ' is symmetric.

Transitive: Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n \mid a - b$ and $n \mid b - c$. Thus (1.4.4)(c) shows that

$$n \mid (a - b) + (b - c).$$

A routine calculation shows that $(a - b) + (b - c) = a - c$. Indeed:

$$\begin{aligned}
(a - b) + (b - c) &= (a + (-b)) + (b + (-c)) && \text{-- definition of '}-\text{' } \\
&= (a + ((-b) + b)) + (-c) && \text{-- GAL} \\
&= (a + 0_R) + (-c) && \text{-- Ax 5} \\
&= a + (-c) && \text{-- Ax 4} \\
&= a - c && \text{-- definition of '}-\text{' }
\end{aligned}$$

Hence $n \mid a - c$ and $a \equiv c \pmod{n}$. Thus ' $\equiv \pmod{n}$ ' is transitive. □

Definition 1.4.8. *Let R be a ring and $n \in R$. Recall from 1.4.7 that the relation ' $\equiv \pmod{n}$ ' is an equivalence relation.*

(a) For $a \in R$ we denote the equivalence class of ' $\equiv \pmod{n}$ ' containing a by $[a]_n$. So

$$[a]_n = \{b \in R \mid a \equiv b \pmod{n}\}.$$

$[a]_n$ is called the congruence class of a modulo n in R .

(b) R_n denotes the set of equivalence classes of ' $\equiv \pmod{n}$ '. So

$$R_n = \{ [a]_n \mid a \in R \}.$$

Theorem 1.4.9. Let R be a ring and $a, b, n \in R$. Then the following statements are equivalent

- | | |
|---|---------------------------------------|
| (a) $a = b + nk$ for some $k \in R$ | (g) $[a]_n = [b]_n$. |
| (b) $a - b = nk$ for some $k \in R$. | (h) $a \in [b]_n$. |
| (c) $n \mid a - b$. | (i) $b \equiv a \pmod{n}$ |
| (d) $a \equiv b \pmod{n}$. | (j) $n \mid b - a$. |
| (e) $b \in [a]_n$. | (k) $b - a = nl$ for some $l \in R$. |
| (f) $[a]_n \cap [b]_n \neq \emptyset$. | (l) $b = a + nl$ for some $l \in R$. |

Proof. (a) $\iff$ (b): Apply 1.2.8 with $c = nk$.

(b) $\iff$ (c): Follows from the definition of 'divide'.

(c) $\iff$ (d): Follows from the definition of ' $\equiv \pmod{n}$ '.

By 1.4.7 ' $\equiv \pmod{n}$ ' is an equivalence relation. So Theorem A.6.5 implies that (d)-(i) are equivalent.

Applying the fact that statements (a) to (d) are equivalent with a and b interchanged, shows that (i) to (l) are equivalent.

We proved that (a)-(d) are equivalent, that (d) to (i) are equivalent and that (i) to (l) are equivalent. Hence (a)-(l) are equivalent. $\square$

Theorem 1.4.10. Let R be a ring and $a, n \in R$. Then

$$[a]_n = \{a + nl \mid l \in R\}.$$

Proof. Let $b \in R$. Then

$$\begin{aligned} & b \in [a]_n \\ \iff & b = a + nl \text{ for some } l \in R && - 1.4.9 \\ \iff & b \in \{a + nl \mid l \in R\} && - \text{Definition of } \{a + nk \mid k \in R\} \end{aligned}$$

Hence $[a]_n = \{a + nl \mid l \in R\}$ by A.3.1. $\square$

Example 1.4.11. (1) Consider the ring $\mathbb{Z}$.

$$[3]_5 \stackrel{1.4.10}{=} \{3 + 5l \mid l \in \mathbb{Z}\} = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}.$$

(2) Consider the ring $\mathbb{Q}$:

$$[3]_5 \stackrel{1.4.10}{=} \{3 + 5l \mid l \in \mathbb{Q}\} = \{3 + k \mid k \in \mathbb{Q}\} = \mathbb{Q}.$$

(3) Consider the ring $M_2(\mathbb{R})$.

$$\begin{aligned} \left[\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right] \left[\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right] &\stackrel{1.4.10}{=} \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot A \mid A \in M_2(\mathbb{R}) \right\} \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \mid c, d \in \mathbb{R} \right\}. \end{aligned}$$

(4) Consider any ring R and $a \in R$. Then

$$[a]_{0_R} \stackrel{1.4.10}{=} \{a + 0_R l \mid l \in R\} \stackrel{(1.2.9)(c)}{=} \{a + 0_R \mid l \in R\} \stackrel{\mathbf{Ax} 4}{=} \{a\}$$

Exercises 1.4:

1.4#1. Which of the following statements are true in the given ring:

- (a) $7 \equiv 21 \pmod{3}$ in $\mathbb{Z}$.
- (b) $7 \equiv 21 \pmod{3}$ in $\mathbb{Q}$.
- (c) $11 \equiv 17 \pmod{\pi}$ in $\mathbb{R}$.
- (d) $-5 \equiv -14 \pmod{-3}$ in $\mathbb{Z}$.
- (e) $5 \equiv 7 \pmod{0}$ in $\mathbb{Z}$.

(f) $5 \equiv 5 \pmod{0}$ in $\mathbb{Z}$.

1.4#2. Compute the following congruence classes in the given ring:

(a) $[7]_3$ in $\mathbb{Z}$.

(b) $[7]_3$ in $\mathbb{Q}$.

(c) $[11]_\pi$ in $\mathbb{R}$.

(d) $[-5]_{-3}$ in $\mathbb{Z}$

(e) $[5]_0$ in $\mathbb{Z}$.

1.4#3. Consider the ring $M_2(\mathbb{R})$.

(a) Does $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ divide $\begin{bmatrix} 2 & 3 \\ 2 & 3 \end{bmatrix}$ in $M_2(\mathbb{R})$?

(b) Does $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ divide $\begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}$ in $M_2(\mathbb{R})$?

(c) Compute $\left[\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right] \left[\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right]$.

(d) Let $a, b, c, d, \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{R}$. Show that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{bmatrix} \left(\text{mod} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right)$$

if and only of

$$a - c = \tilde{a} - \tilde{c} \quad \text{and} \quad b - d = \tilde{b} - \tilde{d}.$$

1.5 Congruence in the ring of integers

For a general ring it is difficult to explicitly determine all the equivalence classes of relation $\equiv \pmod{n}$. But thanks to the division algorithm it is fairly easy for the ring of integers. In the proof of the Division Algorithm we will use the Well-Ordering Axiom of the natural numbers, see B.4.2.

Theorem 1.5.1 (The Division Algorithm). *Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Proof. We will first show that q and r exist. Put

$$S := \{a - bx \mid x \in \mathbb{Z} \text{ and } a - bx \geq 0\}.$$

Note that $S \subseteq \mathbb{N}$. We would like to apply the Well-Ordering Axiom B.4.2 to S , so we need to verify that S is not empty. That is we need to find $x \in \mathbb{Z}$ such that $a - bx \geq 0$.

If $a \geq 0$, then $a - b \cdot 0 = a \geq 0$ and we can choose $x = 0$.

So suppose $a < 0$. Let's try $x = a$. Then $a - bx = 1a - ba = (1 - b)a$. Since $b > 0$ and b is an integer, $b \geq 1$ and so $1 - b \leq 0$. Since $a < 0$, this implies $(1 - b)a \geq 0$ and so $a - bx \geq 0$. So we can indeed choose $x = a$.

We proved that S is non-empty subset of $\mathbb{N}$. Hence by the Well-ordering Axiom B.4.2 S has a minimal element r . Thus

$$(*) \quad r \in S \quad \text{and} \quad r \leq s \quad \text{for all } s \in S.$$

Since $r \in S$, the definition of S implies that there exists $q \in \mathbb{Z}$ with $r = a - bq$. Then $a = r + bq = bq + r$ and it remains to show $0 \leq r < b$. Since $r \in S$, we know that $r \geq 0$. Suppose for a contradiction that $r \geq b$. Then $r - b \geq 0$. Hence

$$a - b(q + 1) = (a - bq) - b = r - b \geq 0$$

and $q + 1 \in \mathbb{Z}$. Thus $r - b \in S$. Since r is a minimal element of S this implies $r \leq r - b$, see $(*)$. It follows that $b \leq 0$, a contradiction since $b > 0$ by the hypothesis of the theorem.

This contradiction shows that $r < b$, so the existence assertion in the theorem is proved. To show the uniqueness let $q, r, \tilde{q}$ and $\tilde{r}$ be integers with

$$(**) \quad (a = bq + r \text{ and } 0 \leq r < b) \quad \text{and} \quad (a = b\tilde{q} + \tilde{r} \text{ and } 0 \leq \tilde{r} < b).$$

We need to show that $q = \tilde{q}$ and $r = \tilde{r}$.

From $a = bq + r$ and $a = b\tilde{q} + \tilde{r}$ we have

$$bq + r = b\tilde{q} + \tilde{r}$$

and so

$$(***) \quad b(q - \tilde{q}) = \tilde{r} - r.$$

By $(**)$ we have $0 \leq r < b$. Multiplying with -1 gives $0 \geq -r > -b$ and so

$$-b < -r \leq 0.$$

By (**)

$$0 \leq \tilde{r} < b$$

and adding the last two equations yields

$$-b < \tilde{r} - r < b$$

By (* *) we have $b(q - \tilde{q}) = \tilde{r} - r$. Thus

$$-b < b(q - \tilde{q}) < b.$$

Since $b > 0$ we can divide by b and get

$$-1 < q - \tilde{q} < 1.$$

The only integer strictly between -1 and 1 is 0 . Hence $q - \tilde{q} = 0$ and so $q = \tilde{q}$. Hence (*) gives $\tilde{r} - r = b(q - \tilde{q}) = b \cdot 0 = 0$ and so also $\tilde{r} = r$. $\square$

Theorem 1.5.2 (Division Algorithm). *Let a and c be integers with $c \neq 0$. Then there exist unique integers q and r such that*

$$a = cq + r \text{ and } 0 \leq r < |c|.$$

Proof. See Exercise 1.5#1 $\square$

Definition 1.5.3. *Let a and b be integers with $b \neq 0$. According to the Division Algorithm there exist unique integers q and r with $a = bq + r$ and $0 \leq r < |b|$. Then r is called the remainder of a when divided by b in $\mathbb{Z}$. q is called the integral quotient of a when divided by b in $\mathbb{Z}$.*

Example 1.5.4. (1) What is the remainder of 42 when divided by 8 in $\mathbb{Z}$?

$42 = 8 \cdot 5 + 2$ and $0 \leq 2 < 8$. So the remainder of 42 when divided by 8 is 2.

(2) What is the remainder of -42 when divided by 8 in $\mathbb{Z}$?

$-42 = 8 \cdot -6 + 6$ and $0 \leq 6 < 8$. So the remainder of -42 when divided by 8 is 6.

Theorem 1.5.5. *Let a, b, n be integers with $n \neq 0$. Then*

$$a \equiv b \pmod{n}$$

if and only if

a and b have the same remainder when divided by n .

Proof. By the division algorithm there exist integers q_1, r_1, q_2, r_2 with

$$(*) \quad a = nq_1 + r_1 \quad \text{and} \quad 0 \leq r_1 < |n|$$

and

$$(**) \quad b = nq_2 + r_2 \quad \text{and} \quad 0 \leq r_2 < |n|.$$

Note that, by definition, r_1 and r_2 are the remainders of a and b , respectively when divided by n in $\mathbb{Z}$.

$\implies$: Suppose $a \equiv b \pmod{n}$. Then by 1.4.9 we have $a = b + nk$ for some integer k . Thus

$$a = b + nk \stackrel{(*)}{=} (nq_2 + r_2) + nk = n(q_2 + k) + r_2.$$

Since $q_2 + k \in \mathbb{Z}$ and $0 \leq r_2 < |n|$, we conclude that r_2 is the remainder of a when divided by n . So $r_1 = r_2$ and a and b have the same remainder when divided by n .

$\impliedby$: Suppose a and b have the same remainder when divided by n . Then $r_1 = r_2$ and so

$$a - b \stackrel{(*)}{=} \stackrel{(**)}{=} (nq_1 + r_1) - (nq_2 + r_2) = n(q_1 - q_2) + (r_1 - r_2) = n(q_1 - q_2).$$

Thus $n|a - b$ and so $a \equiv b \pmod{n}$. □

Example 1.5.6. Is $42 \equiv -42 \pmod{8}$?

By Example 1.5.4 the remainders of 42 and -42 when divided by 8 are 2 and 6 respectively. As $2 \neq 6$ we conclude from 1.5.5 that

$$42 \not\equiv -42 \pmod{8}?$$

Theorem 1.5.7. Let n be positive integer.

- (a) Let $a \in \mathbb{Z}$. Then there exists a unique $r \in \mathbb{Z}$ with $0 \leq r < n$ and $[a]_n = [r]_n$, namely r is the remainder of a when divided by n .
- (b) There are exactly n distinct congruence classes modulo n , namely

$$[0], [1], [2], \dots, [n-1].$$

- (c) $|\mathbb{Z}_n| = n$, that is $\mathbb{Z}_n$ has exactly n elements.

Proof. (a) Let $a \in \mathbb{Z}$, let s be the remainder of a when divided by n and let $r \in \mathbb{Z}$ with $0 \leq r < n$. We need to show that $[a]_n = [r]_n$ if and only if $r = s$.

Since $r = n0 + r$ and $0 \leq r < n$, we see that r is the remainder of r when divided by n . By 1.4.9 $[a]_n = [r]_n$ if and only if $a \equiv r \pmod{n}$ and so by 1.5.5 if and only if a and r have the same remainder when divided by n , that is if and only if $r = s$.

(b) By definition each congruence class modulo n is of the form $[a]_n$, with $a \in \mathbb{Z}$. By (a), $[a]_n$ is equal to exactly one of

$$[0], [1], [2], \dots, [n-1].$$

So (b) holds.

- (c) Since $\mathbb{Z}_n$ is the set of congruence classes modulo n , (c) follows from (b). □

Example 1.5.8. Determine $\mathbb{Z}_5$.

$$\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\} = \{[0]_5, [1]_5, [2]_5, [-2]_5, [-1]_5\} = \{[0]_5, [\pm 1]_5, [\pm 2]_5\}$$

Note here that $3 - 5 = -2$ and $4 - 5 = -1$. So $[3]_5 = [-2]_5$ and $[4]_5 = [-1]_5$.

Exercises 1.5:

1.5#1. Let a and c be integers with $c \neq 0$. Prove that there exist unique integers q and r such that

$$a = cq + r \text{ and } 0 \leq r < |c|.$$

1.5#2. Prove that the square of an integer is either of the form $3k$ or the form $3k + 1$ for some integer k .

1.5#3. Use the Division Algorithm to prove that every odd integer is of the form $4k + 1$ or $4k + 3$ for some integer k .

1.5#4. (a) Divide 5^2 , 7^2 , 11^2 , 15^2 and 27^2 by 8 and note the remainder in each case.

(b) Make a conjecture about the remainder when the square of an odd number is divided by 8.

(c) Prove your conjecture.

1.5#5. Prove that the cube of any integer has be exactly one of these forms: $9k$, $9k + 1$ or $9k + 8$ for some integer k .

1.5#6. (a) Let k be an integer with $k \equiv 1 \pmod{4}$. Compute the remainder of $6k + 5$ when divided by 4.

(b) Let r and s be integer with $r \equiv 3 \pmod{10}$ and $s \equiv -7 \pmod{10}$. Compute the remainder of $2r + 3s$ when divided by 10.

1.6 Modular Arithmetic in Commutative Rings

Theorem 1.6.1. Let R be a commutative ring and $a, \tilde{a}, b, \tilde{b}$ and n elements of R . Suppose that

$$[a]_n = [\tilde{a}]_n \quad \text{and} \quad [b]_n = [\tilde{b}]_n.$$

or that

$$a \equiv \tilde{a} \pmod{n} \quad \text{and} \quad b \equiv \tilde{b} \pmod{n}$$

Then

$$[a + b]_n = [\tilde{a} + \tilde{b}]_n \quad \text{and} \quad [ab]_n = [\tilde{a}\tilde{b}]_n.$$

and

$$a + b \equiv \tilde{a} + \tilde{b} \pmod{n} \quad \text{and} \quad ab \equiv \tilde{a}\tilde{b} \pmod{n}$$

Proof. Since

$$[a]_n = [\tilde{a}]_n \quad \text{and} \quad [b]_n = [\tilde{b}]_n.$$

or

$$a \equiv \tilde{a} \pmod{n} \quad \text{and} \quad b \equiv \tilde{b} \pmod{n}$$

we conclude from 1.4.9 that

$$\tilde{a} = a + nk \quad \text{and} \quad \tilde{b} = b + nl$$

for some $k, l \in R$. Hence

$$\tilde{a} + \tilde{b} = (a + nk) + (b + nl) \stackrel{\text{GCL}}{=} (a + b) + (nk + nl) \stackrel{\mathbf{Ax} 8}{=} (a + b) + n(k + l).$$

By **Ax 1** $k + l \in R$, so 1.4.9 gives

$$[a + b]_n = [\tilde{a} + \tilde{b}]_n \quad \text{and} \quad a + b \equiv \tilde{a} + \tilde{b} \pmod{n}$$

Since R is commutative, we can use the General Commutative Law for multiplication:

$$\begin{aligned} \tilde{a} \cdot \tilde{b} &= (a + nk)(b + nl) \stackrel{\text{GDL}}{=} ab + nkb + anl + nkn l \\ &\stackrel{\text{GCL}}{=} ab + nkb + nal + nkn l \stackrel{\text{GDL}}{=} ab + n(al + kb + knl), \end{aligned}$$

By **Ax 1** and **Ax 6** $al + kb + knl \in R$, so 1.4.9 implies

$$[ab]_n = [\tilde{a}\tilde{b}]_n \quad \text{and} \quad ab \equiv \tilde{a}\tilde{b} \pmod{n}.$$

□

In view of 1.6.1 the following definition is well-defined.

Definition 1.6.2. Let R be commutative ring and a, b and n elements of R . Define

$$[a]_n \oplus [b]_n := [a + b]_n \quad \text{and} \quad [a]_n \odot [b]_n := [ab]_n.$$

The function

$$R_n \times R_n \rightarrow R_n, \quad (A, B) \mapsto A \oplus B$$

is called the addition on R_n , and the function

$$R_n \times R_n \rightarrow R_n, \quad (A, B) \mapsto A \odot B$$

is called the multiplication on R_n .

Example 1.6.3. (1) Compute $[3]_8 \odot [7]_8$.

$$[3]_8 \odot [7]_8 = [3 \cdot 7]_8 = [21]_8 = [8 \cdot 2 + 5]_8 = [5]_8.$$

Note that $[3]_8 = [11]_8$ and $[7]_8 = [-1]_8$. So we could also have used the following computation:

$$[11]_8 \odot [-1]_8 = [11 \cdot -1]_8 = [-11]_8 = [-11 + 8 \cdot 2]_8 = [5]_8.$$

Theorem 1.6.1 ensures that we will always get the same answer, not matter what representative we pick for the congruence class.

(2) Compute $[21]_{31} \oplus [18]_{31}$.

$$[21]_{31} \oplus [18]_{31} = [21 + 18]_{31} = [39]_{31} = [39 - 31]_{31} = [8]_{31}.$$

Note that $[21]_{31} = [21 - 31]_{31} = [-10]_{31}$ and $[18]_{31} = [18 - 31]_{31} = [-13]_{31}$. Also

$$[-10]_{31} \oplus [-13]_{31} = [-10 - 13]_{31} = [-23]_{31} = [-23 + 31]_{31} = [8]_{31}.$$

(3) **Warning:** Congruence classes can not be used as exponents:

We have

$$[2^4]_3 = [16]_3 = [1]_3 \quad \text{and} \quad [2^1]_3 = [2]_3$$

So

$$[2^4]_3 \neq [2^1]_3 \quad \text{even though} \quad [4]_3 = [1]_3$$

Theorem 1.6.4. Let R be a commutative ring and $n \in R$.

- (a) $(R_n, \oplus, \odot)$ is a commutative ring.
- (b) $0_{R_n} = [0_R]_n$.
- (c) $-[a]_n = [-a]_n$ for all $a \in R$.
- (d) If R has an identity, then $[1_R]_n$ is an identity for R_n .

Proof. We need to verify the eight Axioms of a ring. If $d \in R$ we will just write $[d]$ for $[d]_n$.

Let $A, B, C \in R_n$. By definition of R_n there exist a, b and c in R with

$$(*) \quad A = [a], \quad B = [b], \quad \text{and} \quad C = [c].$$

Ax 1: We have

$$\begin{aligned} A \oplus B &= [a] \oplus [b] && - (*) \\ &= [a + b] && - \text{Definition of } \oplus \end{aligned}$$

Since $a + b \in R$ we conclude that $A \oplus B \in R_n$.

Ax 2:

$$\begin{aligned} A \oplus (B \oplus C) &= [a] \oplus ([b] \oplus [c]) && - (*) \\ &= [a] \oplus [b + c] && - \text{Definition of } \oplus \\ &= [a + (b + c)] && - \text{Definition of } \oplus \\ &= [(a + b) + c] && - \mathbf{Ax 2} \\ &= [a + b] \oplus [c] && - \text{Definition of } \oplus \\ &= ([a] \oplus [b]) \oplus [c] && - \text{Definition of } \oplus \\ &= (A \oplus B) \oplus C. && - (*) \end{aligned}$$

Ax 3:

$$\begin{aligned} A \oplus B &= [a] \oplus [b] && - (*) \\ &= [a + b] && - \text{Definition of } \oplus \\ &= [b + a] && - \mathbf{Ax 2} \\ &= [b] \oplus [a] && - \text{Definition of } \oplus \\ &= B \oplus A. && - (*) \end{aligned}$$

Ax 4: Define

$$(**) \quad 0_{R_n} := [0_R]$$

Then

$$\begin{aligned} A \oplus 0_{R_n} &= [a] \oplus [0_R] && - (*) \text{ and } (**) \\ &= [a + 0_R] && - \text{Definition of } \oplus \\ &= [a] && - \mathbf{Ax 4} \\ &= A && - (*) \end{aligned}$$

and so, using **Ax 3** for R_n :

$$0_{R_n} \oplus A \stackrel{\mathbf{Ax 3}}{=} A \oplus 0_{R_n} = A.$$

Thus **Ax 4** holds.

Ax 5: Put

$$(* * *) \quad -A := [-a]$$

Then $-A \in R_n$ and

$$\begin{aligned} A \oplus -A &= [a] \oplus [-a] && - (*) \text{ and } (* * *) \\ &= [a + (-a)] && - \text{Definition of } \oplus \\ &= [0_R] && - \mathbf{Ax 4} \\ &= 0_{R_n} && - (***) \end{aligned}$$

and so, using **Ax 3** for R_n :

$$-A \oplus A \stackrel{\mathbf{Ax 3}}{=} A \oplus -A = 0_{R_n}.$$

Thus **Ax 5** holds.

Ax 6: Similarly to **Ax 1** we have $A \odot B = [a] \odot [b] = [ab]$ and so $A \odot B \in R_n$.

Ax 7: Similarly to **Ax 2** we can use the definition of $\odot$ and the fact that multiplication in R is associative to compute

$$\begin{aligned} A \odot (B \odot C) &= [a] \odot ([b] \odot [c]) = [a] \odot [bc] = [a(bc)] = [(ab)c] \\ &= [ab] \odot [c] = ([a] \odot [b]) \odot [c] = (A \odot B) \odot C. \end{aligned}$$

Ax 8:

$$\begin{aligned} A \odot (B \oplus C) &= [a] \odot ([b] \oplus [c]) && - (*) \\ &= [a] \odot [b + c] && - \text{Definition of } \oplus \\ &= [a(b + c)] && - \text{Definition of } \odot \\ &= [ab + bc] && - \mathbf{Ax 8} \\ &= [ab] \oplus [ac] && - \text{Definition of } \oplus \\ &= ([a] \odot [b]) \oplus ([a] \odot [c]) && - \text{Definition of } \odot \\ &= (A \odot B) \oplus (A \odot C) && - (*) \end{aligned}$$

and similarly

$$\begin{aligned}
 (A \oplus B) \odot C &= ([a] \oplus [b]) \odot [c] = [a+b] \odot [c] = [(a+b)c] \\
 &= [ac+bc] = [ac] \oplus [bc] = ([a] \odot [c]) \oplus ([b] \odot [c]) \\
 &= (A \odot C) \oplus (B \odot C).
 \end{aligned}$$

Ax 9 Similarly to **Ax 3** we can use the definition of $\odot$ and the fact that multiplication in R is commutative to compute

$$A \odot B = [a] \odot [b] = [ab] = [ba] = [b] \odot [a] = B \odot A.$$

Ax 10 Suppose R is a ring with identity. Put

$$(+)\quad 1_{R_n} := [1_R]_n$$

Similarly to **Ax 4** we can use the definition of $\odot$ and the fact that 1_R is a multiplicative identity in R to compute

$$A \odot 1_{R_n} = A \odot [1_R] = [a] \odot [1_R] = [a1_R] = [a] = A,$$

and

$$1_{R_n} \odot A = [1_R] \odot [a] = [1_R] \odot [a] = [1_R a] = [a] = A.$$

Thus 1_{R_n} is an identity for R_n .

□

Theorem 1.6.5. *Let R be a commutative ring, $a, n \in R$ and $k \in \mathbb{Z}^+$. Then $[a]_n^k = [a^k]_n$*

Proof. We will do a proof by induction (see section A.5 in the appendix). First we will show that the statement holds for $k = 1$:

We have $[a]^1 = [a] = [a^1]$ and so statement indeed holds for $k = 1$.

Next we assume the statement holds for k and show that it also holds for $k + 1$. So we assume that

$$(*)\quad [a^k] = [a^k]$$

Then

$$\begin{aligned}
 [a]^{k+1} &= [a]^k \odot [a] && \text{– Definition of } [a]^{k+1}, \text{ 1.3.4} \\
 &= [a^k] \odot [a] && \text{– Induction assumption } (*) \\
 &= [a^k a] && \text{– Definition of } \odot, \text{ 1.6.2} \\
 &= [a^{k+1}] && \text{– Definition of } a^{k+1}
 \end{aligned}$$

Hence the statement also holds for $k + 1$. So by the Principal of Induction A.5.2 shows that the Theorem holds for all $k \in \mathbb{N}$. $\square$

Notation 1.6.6 (R_n -notation). *Let R be a commutative ring and $a, b, n \in R$. . We will often just write a for $[a]_n$, $a + b$ for $[a]_n \oplus [b]_n$ and ab (or $a \cdot b$) for $[a]_n \odot [b]_n$. This notation is only to be used if it clear from the context that the symbols represent congruence classes modulo n . Exponents are always integers and never congruences class.*

Remark 1.6.7. *Consider the expression*

$$2^5 + 3 \cdot 7$$

in $\mathbb{Z}_n$ -notation. It is not clear which element of $\mathbb{Z}_n$ this represents, indeed it could be any of the following:

$$\begin{aligned} & [2^5 + 3 \cdot 7]_n \\ & [2^5]_n \oplus [3 \cdot 7]_n \\ & [2^5]_n \oplus ([3]_n \odot [7]_n) \\ & [2]_n^5 \oplus [3 \cdot 7]_n \\ & [2]_n^5 \oplus ([3]_n \odot [7]_n) \end{aligned}$$

But thanks to Theorem 1.6.1 and Theorem 1.6.5 all these elements are actually equal. So our simplified notation is not ambiguous. In other words, our use of the simplified notation is only justified by Theorem 1.6.1 and Theorem 1.6.5.

Example 1.6.8. (1) Compute $[13^{34567}]_{12}$ in $\mathbb{Z}_{12}$.

$$[13^{34567}]_{12} = [13]_{12}^{34567} = [1]_{12}^{34567} = [1^{34567}]_{12} = [1]_{12}$$

In $\mathbb{Z}_{12}$ -notation this becomes

$$13^{34567} = 1^{34567} = 1$$

Why is the calculation shorter? In simplified notation the expression

$$[13^{34567}]_{12} \quad \text{and} \quad [13]_{12}^{34567}$$

are both written as

$$13^{34567}$$

So the step

$$[13^{34567}]_{12} = [13]_{12}^{34567}$$

is invisibly performed by the simplified notation. Similarly, the step

$$[1]_{12}^{34567} = [1^{34567}]_{12}$$

disappears through our use of the simplified notation.

- (2) Compute $[7]_{50}^{198}$ in $\mathbb{Z}_{50}$.

In $\mathbb{Z}_{50}$ -notation:

$$7^{198} = (7^2)^{99} = 49^{99} = (-1)^{99} = -1 = 49.$$

- (3) Determine the remainder of $53 \cdot 7^{100} + 47 \cdot 7^{71} + 4 \cdot 7^3$ when divided by 50.

In $\mathbb{Z}_{50}$ -notation:

$$\begin{aligned} 53 \cdot 7^{100} + 47 \cdot 7^{71} + 4 \cdot 7^3 &= 3 \cdot (7^2)^{50} - 3 \cdot (7^2)^{35} \cdot 7 + 4 \cdot 7^2 \cdot 7 \\ &= 3 \cdot (-1)^{50} - 3 \cdot (-1)^{35} \cdot 7 + 4 \cdot -1 \cdot 7 \\ &= 3 + 21 - 28 = 3 - 7 = -4 = 46. \end{aligned}$$

In regular notation we have $[53 \cdot 7^{100} + 47 \cdot 7^{71} + 4 \cdot 7^3]_{50} = [46]_{50}$. Since $0 \leq 46 < 50$, (1.5.7)(a) shows that the remainder in question is 46.

- (4) Let $\text{Fun}(\mathbb{R})$ be the set of functions from $\mathbb{R}$ to $\mathbb{R}$. Define an addition and multiplication on $\text{Fun}(\mathbb{R})$ by

$$(f + g)(a) = f(a) + g(a) \quad \text{and} \quad (fg)(a) = f(a)g(a).$$

for all $f, g \in \text{Fun}(\mathbb{R})$ and $a \in \mathbb{R}$. Given that $(\text{Fun}(\mathbb{R}), +, \cdot)$ is a commutative ring (see Exercise 1.6#5). Compute

$$[\sin x]_{\cos x}^2.$$

Note that $\cos x \equiv 0 \pmod{\cos x}$.

So in $\text{Fun}(\mathbb{R})_{\cos x}$ -notation:

$$\sin^2 x = 1 - \cos^2 x = 1 - 0^2 = 1.$$

Thus $[\sin x]_{\cos x}^2 = [1]_{\cos x}$.

Exercises 1.6:

1.6#1. Let $a, m, n \in \mathbb{Z}$ with $m, n > 0$. Prove that $[a^m]_2 = [a^n]_2$.

1.6#2. (a) Show that $10^n \equiv 1 \pmod{9}$ for every positive integer n .

- (b) Prove that every positive integer is congruent to the sum of its digits mod 9. [for example, $38 \equiv 11 \pmod{9}$].

1.6#3. Compute the remainder of 5^{2018} when divided by 31 in $\mathbb{Z}$.

1.6#4. Let a be an integer with $a \equiv 2 \pmod{4}$. Prove that do not exist integers c and d with $a = c^2 - d^2$.

1.6#5. Let R be a ring and I a set. Let $\text{Fun}(I, R)$ be the set of functions from I to R . For $f, g \in \text{Fun}(I, R)$ let $f + g$ and $f \cdot g$ be the functions from I to R defined by

$$(f + g)(i) = f(i) + g(i) \quad \text{and} \quad (f \cdot g)(i) = f(i) \cdot g(i).$$

for all $i \in I$. Show that

- (a) $(\text{Fun}(I, R), +, \cdot)$ is a ring.
- (b) If R has an identity, then $\text{Fun}(I, R)$ has an identity.
- (c) If R is commutative, then $\text{Fun}(I, R)$ is commutative.

1.7 Subrings

Definition 1.7.1. Let $(R, +, \cdot)$ be a ring and S a subset of R . Then $(S, +, \cdot)$ is called a subring of $(R, +, \cdot)$ provided that $(S, +, \cdot)$ is a ring.

Theorem 1.7.2 (Subring Theorem). Suppose that R is a ring and S a subset of R . Then S is a subring of R if and only if the following four conditions hold:

- (I) $0_R \in S$.
- (II) S is closed under addition (that is: if $a, b \in S$, then $a + b \in S$);
- (III) S is closed under multiplication (that is: if $a, b \in S$, then $ab \in S$);
- (IV) S is closed under negatives (that is: if $a \in S$, then $-a \in S$)

Proof. $\implies$: Suppose first that S is a subring of R .

By **Ax 4** for S there exists $0_S \in S$ with $0_S + a = a$ for all $a \in S$. In particular, $0_S + 0_S = 0_S$. So the Additive Identity Law 1.2.4 implies that

$$(*) \quad 0_S = 0_R.$$

Since $0_S \in S$, this gives $0_R \in S$ and (I) holds.

By **Ax 1** for S , $a + b \in S$ for all $a, b \in S$. So (II) holds.

By **Ax 6** for S , $ab \in S$ for all $a, b \in S$. So (III) holds.

Let $s \in S$. Then by **Ax 5** for S , there exists $t \in S$ with $s + t = 0_S$. By $(*)$ $0_S = 0_R$ and so $s + t = 0_R$. The Additive Inverse Law 1.2.6 shows that $t = -s$. Since $t \in S$ this gives $-s \in S$ and (IV) holds.

$\Leftarrow$: Suppose now that (I)-(IV) hold.

Since S is a subset of R , S is a set. Hence Condition (i) in the definition of a ring holds for S .

Since S is a subset of R , $S \times S$ is a subset $R \times R$. By Conditions (ii) and (iii) in the definition of a ring, $R \times R$ is a subset of the domains of $+$ and $\cdot$. Hence also $S \times S$ is a subset of the domains of $+$ and $\cdot$. Thus Conditions (ii) and (iii) in the definition of a ring hold for S .

By (II) $a + b \in S$ for all $a, b \in S$ and so **Ax 1** holds for S .

By **Ax 2** $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$. Since $S \subseteq R$ we conclude that $(a+b)+c = a+(b+c)$ for all $a, b, c \in S$. Thus **Ax 2** holds for S .

Similarly, since **Ax 3** holds for all elements in R it also holds for all elements of S .

Put $0_S := 0_R$. Then (I) implies $0_S \in S$. By **Ax 4** for R , $a = 0_R + a$ and $a = a + 0_R$ for all $a \in R$. Thus $a = 0_S + a$ and $a = a + 0_S$ for all $a \in S$ and so **Ax 4** holds for S .

Let $s \in S$. By **Ax 6** $s + (-s) = 0_R$ and $(-s) + s = 0_R$. Since $0_S = 0_R$, the Principal of Substitution gives $s + (-s) = 0_S$ and $(-s) + s = 0_S$. By (IV) $-s \in S$ and so **Ax 5** holds for S .

By (III) $ab \in S$ for all $a, b \in S$ and so **Ax 6** holds for S .

Since **Ax 7** and **Ax 8** hold for all elements of R they also hold for all elements of S . Thus **Ax 7** and **Ax 8** hold for S .

We proved that **Ax 1-Ax 8** hold for $(S, +, \cdot)$ and so $(S, +, \cdot)$ is a ring. Hence, by definition, S is a subring of R . $\square$

Example 1.7.3. (1) Show that $\mathbb{Z}$ is a subring of $\mathbb{Q}$, and $\mathbb{Q}$ is a subring of $\mathbb{R}$.

Note that $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathbb{Q} \subseteq \mathbb{R}$. By example 1.1.4 $\mathbb{Z}$ and $\mathbb{Q}$ are rings. So by definition of a subring, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$.

(2) Is $\mathbb{N}$ a subring of $\mathbb{Z}$?

$2 \in \mathbb{N}$, but $-2 \notin \mathbb{N}$. Thus conditions (IV) of the Subring Theorem 1.7.2 fails. Hence $\mathbb{N}$ is not a subring of $\mathbb{Z}$. Alternatively, $\mathbb{N}$ is not a ring since **Ax 5** fails, so $\mathbb{N}$ is not a subring of $\mathbb{Z}$.

(3) Let R be a ring and $n \in R$. Put $nR := \{nk \mid k \in R\}$. Show that nR is subring of R .

Note first that since R is closed under multiplication, nR is a subset of R . We will now verify the four conditions of the Subring Theorem for $S = nR$.

Observe first that since $nR = \{nk \mid k \in R\}$,

$$(*) \quad a \in nR \quad \Longleftrightarrow \quad \text{there exists } k \in R \text{ with } a = nk.$$

Let $a, b \in nR$. Then by $(*)$

$$(**) \quad a = nk \quad \text{and} \quad b = nl \quad \text{for some } k, l \in R$$

- (I): $0_R \stackrel{(1.2.9)(c)}{=} n0_R$. By **Ax 4**, $0_R \in R$ and so $(*)$ shows that $0_R \in nR$.
- (II): $a + b \stackrel{(**)}{=} nk + nl \stackrel{\text{Ax 8}}{=} n(k + l)$. By **Ax 2**, $k + l \in R$ and so $(*)$ shows $a + b \in R$. So nR is closed under addition.
- (III): $ab \stackrel{(**)}{=} (nk)(nl) \stackrel{\text{Ax 7}}{=} n(k(nl))$. Using **Ax 6** twice gives $k(nl) \in R$ and so $(*)$ shows $ab \in R$. So nR is closed under multiplication.
- (IV): $-a \stackrel{(**)}{=} -(nk) \stackrel{(1.2.9)(d)}{=} n(-k)$. By **Ax 5**, $-k \in R$ and so $(*)$ shows $-a \in R$. So nR is closed under negatives.

Thus all four conditions of the Subring Theorem hold and hence nR is a subring of R .

- (4) Show that $\{[0]_4, [2]_4\}$ is a subring of $\mathbb{Z}_4$.

We use $\mathbb{Z}_4$ -notation.

$0_{\mathbb{Z}_4} = 0 \in \{0, 2\}$ and so Condition (I) of the Subring Theorem holds. Moreover,

$$\begin{array}{c|cc} + & 0 & 2 \\ \hline 0 & 0 & 2 \\ 2 & 2 & 0 \end{array}, \quad \begin{array}{c|cc} \cdot & 0 & 2 \\ \hline 0 & 0 & 0 \\ 2 & 0 & 0 \end{array} \quad \text{and} \quad \begin{array}{c|cc} x & 0 & 2 \\ \hline -x & 0 & 2 \end{array}$$

So $\{0, 2\}$ is closed under addition, multiplication and negatives. Thus $\{0, 2\}$ is a subring of $\mathbb{Z}_4$ by the Subring Theorem.

Exercises 1.7:

1.7#1. Which of the following nine sets are subrings of $M_2(\mathbb{R})$? Which ones have an identity? (You don't need to justify your answers)

- $$\begin{array}{lll} (1) \left\{ \begin{bmatrix} 0 & r \\ 0 & 0 \end{bmatrix} \mid r \in \mathbb{Q} \right\} & (4) \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{Q}, b \in \mathbb{Z} \right\} & (7) \left\{ \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} \mid a \in \mathbb{R} \right\} \\ (2) \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\} & (5) \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \mid a, b \in \mathbb{R} \right\} & (8) \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R} \right\} \\ (3) \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{Z}, b \in \mathbb{Q} \right\} & (6) \left\{ \begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix} \mid a \in \mathbb{R} \right\} & (9) \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{R} \right\} \end{array}$$

1.7#2. Let $\mathbb{Z}[i]$ denote the set $\{a + bi \mid a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

1.7#3. Let R be a ring and d a fixed element of R . Let

$$S := \{a \in R \mid ad = da\}$$

Show that S is a subring of R .

1.7#4. Let R be a ring and S and T subrings of R . Show that $S \cap T$ is a subring of R .

1.7#5. Let R be a ring and S and T subrings of R . Show that $S \cup T$ is a subring of R if and only if $S \subseteq T$ or $T \subseteq S$.

1.8 Units in Rings

Definition 1.8.1. Let R be a ring with identity.

(a) Let $u \in R$. Then u is called a unit in R if there exists an element in R , denoted by u^{-1} and called ‘ u -inverse’, with

$$uu^{-1} = 1_R \quad \text{and} \quad u^{-1}u = 1_R$$

(b) Let $u, v \in R$. Then v is called an (multiplicative) inverse of u if $uv = 1_R$ and $vu = 1_R$.

(c) Let $e \in R$. Then e is called an (multiplicative) identity of R , if $ea = a$ and $ae = a$ for all $a \in R$.

Example 1.8.2. (1) Units in $\mathbb{Z}$: Let u be a unit in $\mathbb{Z}$. Then $uv = 1$ for some $v \in \mathbb{Z}$. Thus $u = \pm 1$.

(2) Units in $\mathbb{Q}$: Let u be a non-zero rational number. Then $u = \frac{n}{m}$ for some $n, m \in \mathbb{Z}$ with $n \neq 0$ and $m \neq 0$. Thus $\frac{1}{u} = \frac{m}{n}$ is rational. So all non-zero elements in $\mathbb{Q}$ are units.

(3) Units in $\mathbb{Z}_8$: By 1.5.7 $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and so $\mathbb{Z}_8 = \{0, \pm 1, \pm 2, \pm 3, 4\}$. We compute

$\cdot$	0	± 1	± 2	± 3	4
0	0	0	0	0	0
± 1	0	$\boxed{\pm 1}$	± 2	± 3	4
± 2	0	± 2	4	± 2	0
± 3	0	± 3	± 2	$\boxed{\pm 1}$	4
4	0	4	0	4	0

So $\pm 1, \pm 3$ (that is $1, 3, 5, 7$) are the units in $\mathbb{Z}_8$.

Theorem 1.8.3. (a) Let R be a ring and $e, e' \in R$. Suppose that

$$(*) \quad ea = a \quad \text{and} \quad (**) \quad ae' = a$$

for all $a \in R$. Then $e = e'$ and e is a multiplicative identity in R . In particular, a ring has at most one multiplicative identity.

(b) Let R be a ring with identity and $x, y, u \in R$ with

$$(+) \quad xu = 1_R \quad \text{and} \quad (++) \quad uy = 1_R.$$

Then $x = y$, u is a unit in R and x is an inverse of u . In particular, u has at most one inverse in R .

Proof. (a)

$$e \stackrel{(*)}{=} ee' \stackrel{(**)}{=} e'.$$

(b)

$$y \stackrel{\mathbf{Ax}10}{=} 1_R y \stackrel{(+)}{=} (xu)y \stackrel{\mathbf{Ax}7}{=} x(uy) \stackrel{(++)}{=} x1_R \stackrel{\mathbf{Ax}10}{=} x.$$

□

Theorem 1.8.4 (Multiplicative Inverse Law). *Let R be a ring with identity and $u, v \in R$. Suppose u is a unit. Then*

$$\begin{aligned} v &= u^{-1} \\ \iff vu &= 1_R \\ \iff uv &= 1_R \end{aligned}$$

Proof. Recall first that by definition of a unit:

$$(*) \quad uu^{-1} = 1_R \quad \text{and} \quad (**) \quad u^{-1}u = 1_R$$

‘First Statement $\implies$ Second Statement’: Suppose $v = u^{-1}$. Then $vu = u^{-1}u \stackrel{(**)}{=} 1_R$.

‘Second Statement $\implies$ Third Statement’: Suppose that $vu = 1_R$. By $(*)$ $uu^{-1} = 1_R$. Hence

$$vu = 1_R \quad \text{and} \quad uu^{-1} = 1_R$$

and (1.8.3)(b) applied with $x = v$ and $y = u^{-1}$ gives $v = u^{-1}$. Thus $uv = uu^{-1} \stackrel{(*)}{=} 1_R$.

‘Third Statement $\implies$ First Statement’: Suppose that $uv = 1_R$. By $(**)$ $u^{-1}u = 1_R$. Hence

$$u^{-1}u = 1_R \quad \text{and} \quad uv = 1_R$$

and (1.8.3)(b) applied with $x = u^{-1}$ and $y = v$ gives $u^{-1} = v$. □

Theorem 1.8.5. *Let R be a ring with identity and a and b units in R .*

(a) a^{-1} is a unit and $(a^{-1})^{-1} = a$.

(b) ab is a unit and $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. (a) By definition of a^{-1} , $aa^{-1} = 1_R$ and $a^{-1}a = 1_R$. Hence also $a^{-1}a = 1_R$ and $aa^{-1} = 1_R$. Thus a^{-1} is a unit and by the Multiplicative Inverse Law 1.8.4, $a = (a^{-1})^{-1}$.

(b) See Exercise 1.8#6. □

Definition 1.8.6. A ring R is called an integral domain provided that

(i) R is commutative,

(ii) R has an identity,

(iii) $1_R \neq 0_R$, and

(Ax 11) whenever $a, b \in R$ with $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.

Theorem 1.8.7 (Multiplicative Cancellation Law for Integral Domains). Let R be an integral domain and $a, b, c \in R$ with $a \neq 0_R$. Then

$$\begin{aligned} ab &= ac \\ \iff b &= c \\ \iff ba &= ca \end{aligned}$$

Proof. 1st $\implies$ 2nd: Suppose $ab = ac$. Then

$$\begin{aligned} a(b - c) &= ab - ac && (1.2.9)(j) \\ &= ab - ab && \text{Principal of Substitution, } ab = ac \\ &= 0_R && (1.2.9)(f) \end{aligned}$$

Since R is an integral domain, **Ax 11** holds. As $a(b - c) = 0_R$ this implies $a = 0_R$ or $b - c = 0_R$. By assumption $a \neq 0_R$ and so $b - c = 0_R$. Thus by (1.2.9)(f), $b = c$.

2nd $\implies$ 3rd: If $b = c$, then $ba = ca$ by the Principal of Substitution.

3rd $\implies$ 1st: Suppose $ba = ca$. Since integral domains are commutative, we conclude that $ab = ac$. □

Definition 1.8.8. A ring R is called a field provided that

(i) R is commutative,

(ii) R has an identity,

(iii) $1_R \neq 0_R$, and

(Ax 12) each $a \in R$ with $a \neq 0_R$ is a unit in R .

Example 1.8.9. Which of the following rings are fields? Which are integral domains?

- (1) $\mathbb{Z}$. (3) $\mathbb{Z}_3$. (5) $M_2(\mathbb{R})$.
 (2) $\mathbb{Q}$. (4) $\mathbb{Z}_8$.

All of the rings have a non-zero identity. All but $M_2(\mathbb{R})$ are commutative. If a, b are non zero real numbers then $ab \neq 0$. So **Ax 11** holds for $\mathbb{R}$ and so also for $\mathbb{Z}$ and $\mathbb{Q}$. Thus $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are integral domains.

(1) 2 does not have an inverse in $\mathbb{Z}$. So $\mathbb{Z}$ is an integral domain, but not a field.

(2) By (1.8.2)(1) all non-zero elements on $\mathbb{Q}$ are units. So $\mathbb{Q}$ is an integral domain and a field.

(3) ± 1 are the only non-zero elements in $\mathbb{Z}_3$. $1 \cdot 1 = 1$ and $-1 \cdot -1 = 1$. So ± 1 are units and $\mathbb{Z}_3$ is a field. Also $\pm 1 \cdot \pm 1 = \pm 1 \neq 0$ and so $\mathbb{Z}_3$ is an integral domain.

(4) By Example 1.8.2 the units in $\mathbb{Z}_8$ are ± 1 and ± 3 . Thus 2 is not a unit and so $\mathbb{Z}_8$ is not a field. Note that $2 \cdot 4 = 8 = 0$ in $\mathbb{Z}_8$ and so $\mathbb{Z}_8$ is not an integral domain

(5) By (1.1.4)(i) $M_2(\mathbb{R})$ is not commutative. Also for all $a, b, c, d \in \mathbb{R}$:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_{M_2(\mathbb{R})}.$$

Thus $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is not a unit, so **Ax 12** fails. Moreover, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0_{M_2(\mathbb{R})}$ and so **Ax 11** fails. Hence $M_2(\mathbb{R})$ fails all conditions of a field and integral domain, except that $M_2(\mathbb{R})$ has a non-zero identity.

Theorem 1.8.10. *Every field is an integral domain.*

Proof. Let F be a field. Then by definition, F is a commutative ring with identity and $1_F \neq 0_F$. So it remains to verify **Ax 11** in 1.8.6. For this let $a, b \in F$ with

$$(*) \quad ab = 0_F.$$

Suppose that $a \neq 0_F$. Then by the definition of a field, a is a unit. Thus a has multiplicative inverse a^{-1} . We compute

$$\begin{aligned} & ab = 0_F && - (*) \\ \implies & a^{-1}(ab) = a^{-1}0_F && - \text{Principal of Substitution} \\ \implies & (a^{-1}a)b = 0_F && - \text{Ax 7 and (1.2.9)(c)} \\ \implies & 1_F b = 0_F && - \text{Definition of } a^{-1} \\ \implies & b = 0_F && - \text{Ax 10} \end{aligned}$$

We have proved that $a \neq 0_F$ implies $b = 0_F$. So $a = 0_F$ or $b = 0_F$. Hence **Ax 11** holds and F is an integral domain. $\square$

Theorem 1.8.11. *Every finite integral domains is a field.*

Proof. Let R be a finite integral domain. Then R is a commutative ring with identity and $1_R \neq 0_R$. So it remains to show that every $a \in R$ with $a \neq 0_R$ is a unit in R . Put

$$S := \{ar \mid r \in R\}.$$

and define

$$f: R \rightarrow S, \quad r \mapsto ar.$$

We will show that f is a bijection. Let $b, c \in R$ with $f(b) = f(c)$. Then $ab = ac$. As $a \neq 0_R$ the Multiplicative Cancellation Law for Integral Domains 1.8.7 gives $b = c$. Thus f is injective. Let $s \in S$. The definition of S implies that $s = ar$ for some $r \in R$. Then $f(r) = ar = s$ and f is surjective. Hence f is a bijection and so $|R| = |S|$. Since $S \subseteq R$ and R is finite we conclude $R = S$. In particular, $1_R \in S$ and so there exists $b \in R$ with $ab = 1_R$. Since R is commutative, this gives $ba = 1_R$ and so a is a unit. $\square$

Definition 1.8.12. *Let R be a ring with identity, a a unit of R and $n \in \mathbb{Z}^+$. Then*

$$a^{-n} := (a^{-1})^n.$$

Exercises 1.8:

1.8#1. Let R be a ring and $a \in R$. Let $n, m \in \mathbb{Z}$ such that a^n and a^m are defined. (So $n, m \in \mathbb{Z}^+$, or R has an identity and $n, m \in \mathbb{N}$, or R has an identity, a is a unit and $n, m \in \mathbb{Z}$.) Show that

(a) $a^n a^m = a^{n+m}$.

(b) $a^{nm} = (a^n)^m$.

1.8#2. Find all units in $\text{Fun}(\mathbb{R}, \mathbb{R})$.

1.8#3. Find all units in $\mathbb{Z}_{12}$.

1.8#4. An element e of a ring is said to be an **idempotent** if $e^2 = e$.

(a) Find four idempotents in $M_2(\mathbb{R})$.

(b) Find all idempotents in $\mathbb{Z}_{12}$.

(c) Prove that the only idempotents in an integral domain R are 0_R and 1_R .

1.8#5. Prove or give a counter example:

(a) If R and S are integral domains, then $R \times S$ is an integral domain.

(b) If R and S are fields, then $R \times S$ is a field.

1.8#6. (a) If a and b are units in a ring with identity, prove that ab is a unit with inverse $b^{-1}a^{-1}$.

(b) Give an example to show that if a and b are units, then $a^{-1}b^{-1}$ does not need to be the multiplicative inverse of ab .

1.8#7. Let R be a ring with identity. If ab and a are units in R , prove that b is a unit.

1.8#8. Let R be a commutative ring with identity $1_R \neq 0_R$. Prove that R is an integral domain if and only if cancellation holds in R , (that is whenever $a, b, c \in R$ with $a \neq 0_R$ and $ab = ac$ then $b = c$.)

1.8#9. Let R be a ring with identity and $a, b, c \in R$. Suppose that a is a unit in R . Show that

$$(a) \quad ab = ac \iff b = c \iff ba = ca.$$

$$(b) \quad ab = 0_R \iff b = 0_R \iff ba = 0_R.$$

1.9 The Euclidean Algorithm for Integers

Theorem 1.9.1. Let a and b be integers and suppose that $b|a$ and $a \neq 0$. Then

$$1 \leq |b| \leq |a|.$$

Proof. Since $a|b$ we have $a = bk$ for some k in $\mathbb{Z}$. Since $a \neq 0$ we get $b \neq 0$ and $k \neq 0$. Hence $|b|$ and $|k|$ are positive integers and so $1 \leq |b|$ and $1 \leq |k|$. Hence also $|b| \cdot 1 \leq |b| \cdot |k|$ and so

$$1 \leq |b| = |b| \cdot 1 \leq |b| \cdot |k| = |bk| = |a|.$$

□

Definition 1.9.2. (a) Let R be a ring and $a, b, c \in R$. We say that c is a common divisor of a and b in R provided that

$$c|a \quad \text{and} \quad c|b.$$

(b) Let a, b and d be integers. We say that d is a greatest common divisor of a and b in $\mathbb{Z}$, and we write

$$d = \gcd(a, b),$$

provided that

- (i) d is a common divisor of a and b in $\mathbb{Z}$; and
- (ii) if c is a common divisor of a and b in $\mathbb{Z}$, then $c \leq d$.

Example 1.9.3. (1) The largest integer dividing both 24 and 42 is 6. So 6 is a greatest common divisor of 24 and 42.

- (2) All integers divide 0 and 0. So there does not exist a greatest common divisor of 0 and 0.
- (3) Let a be a non-zero integer, then $|a| = \gcd(a, 0)$.

Theorem 1.9.4. *Let a, b, q, r and d be integers with*

$$a = bq + r \quad \text{and} \quad d = \gcd(b, r).$$

Then

$$d = \gcd(a, b).$$

Proof. We need to verify the two conditions (i) and (ii) of the gcd.

(i): Since $d = \gcd(b, r)$ we know that $d|b$ and $d|r$. As $a = bq + r$ we conclude that d divides a , see (1.4.4)(c). Thus d is a common divisor of a and b .

(ii) Let c be a common divisor of a and b . Since $a = bq + r$ we have $r = a - bq$, see 1.2.8. Since $c|a$ and $c|b$ we get $c|r$, see (1.4.4)(c). Thus c is a common divisor of b and r . Since $d = \gcd(b, r)$ this gives $c \leq d$. $\square$

Theorem 1.9.5 (Euclidean Algorithm). *Let a and b be integers not both 0 and let E_{-1} and E_0 be the equations*

$$\begin{aligned} E_{-1} : a &= a \cdot 1 + b \cdot 0 \\ E_0 : b &= a \cdot 0 + b \cdot 1 \end{aligned}$$

Let $i \in \mathbb{N}$ and suppose inductively we already defined equation $E_k, -1 \leq k \leq i$ of the form

$$E_k : r_k = a \cdot x_k + b \cdot y_k.$$

Suppose $r_i \neq 0$ and let $t_{i+1}, q_{i+1} \in \mathbb{Z}$ with

$$r_{i-1} = r_i q_{i+1} + t_{i+1} \quad \text{and} \quad |t_{i+1}| < |r_i|.$$

(Note here that such t_{i+1}, q_{i+1} exist by the division algorithm 1.5.2)

Let E_{i+1} be the equation of the form $r_{i+1} = ax_{i+1} + by_{i+1}$ obtained by subtracting q_{i+1} -times equation E_i from E_{i-1} , that is

$$r_{i+1} := r_{i-1} - r_i q_{i+1}, \quad x_{i+1} := x_{i-1} - x_i q_{i+1}, \quad y_{i+1} := y_{i-1} - x_i q_{i+1}.$$

Then there exists $m \in \mathbb{N}$ with $r_{m-1} \neq 0$ and $r_m = 0$. Put $d := |r_{m-1}|$. Then

- (a) $r_k, x_k, y_k \in \mathbb{Z}$ for all $k \in \mathbb{Z}$ with $-1 \leq k \leq m$.
- (b) $d = \gcd(a, b)$.
- (c) *There exist $x, y \in \mathbb{Z}$ with $d = ax + by$.*

Proof. For $k \in \mathbb{Z}$ with $k \geq -1$, let $P(k)$ be the statement that r_k, x_k and y_k are integers and, if $k \geq 1$, then $|r_k| < |r_{k-1}|$.

By the definition of E_0 and E_1 we have $r_{-1} = a, x_{-1} = 1, y_{-1} = 0, r_0 = b, x_0 = 0$ and $y_0 = 1$. Hence all of these are integers and so $P(-1)$ and $P(0)$ hold. Suppose now that $i \in \mathbb{N}$, that $P(k)$ holds for all $k \in \mathbb{Z}$ with $-1 \leq k \leq i$ and that $r_i \neq 0$. We have

$$\begin{aligned} E_{i-1} &: r_{i-1} = ax_{i-1} + by_{i-1} \\ E_i &: r_i = ax_i + by_i. \end{aligned}$$

and subtracting q_{i+1} times E_i from E_{i-1} we obtain

$$E_{i+1} : r_{i-1} - r_i q_{i+1} = a(x_{i-1} - x_i q_{i+1}) + b(y_{i-1} - x_i q_{i+1}).$$

Hence

$$r_{i+1} := r_{i-1} - r_i q_{i+1}, \quad x_{i+1} := x_{i-1} - x_i q_{i+1}, \quad y_{i+1} := y_{i-1} - x_i q_{i+1}.$$

By choice, q_{i+1} is an integer. By the induction assumption, x_i, x_{i-1}, y_{i-1} and y_i are integers. Hence also r_{i+1}, x_{i+1} and y_{i+1} are integers. By choice of q_{i+1} and t_{i+1}

$$r_{i-1} = r_i q_{i+1} + t_{i+1} \quad \text{and} \quad |t_{i+1}| < |r_i|$$

So

$$t_{i+1} = r_i q_{i+1} - r_{i-1} = r_{i+1} \quad \text{and} \quad |r_{i+1}| < |r_i|.$$

Hence $P(i+1)$ holds. So by the principal of complete induction, $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq -1$ (for which E_n is defined).

In particular, (a) holds and

$$|r_0| > |r_1| > |r_2| > |r_3| > \dots > |r_i| > \dots$$

By the Well Ordering Axiom the set $\{r_i \mid i \in \mathbb{N}, r_i > 0\}$ has a minimal element. Thus there exists $m \in \mathbb{N}$ with $r_{m-1} \neq 0$ and $r_m = 0$.

From $r_{i-1} = r_i q_{i+1} + t_{i+1} = r_i q_{i+1} + r_{i+1}$ and 1.9.4 we have $\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1})$ and so

$$\gcd(a, b) = \gcd(r_{-1}, r_0) = \gcd(r_0, r_1) = \dots = \gcd(r_{m-1}, r_m) = \gcd(r_{m-1}, 0) = |r_{m-1}| = d.$$

So (b) holds.

By equation E_{m-1} we have

$$r_{m-1} = ax_{m-1} + by_{m-1}.$$

If $r_{m-1} > 0$, then

$$d = |r_{m-1}| = r_{m-1} = ax_{m-1} + by_{m-1},$$

and if $r_{m-1} < 0$, then

$$d = |r_{m-1}| = -r_{m-1} = a(-x_{m-1}) + b(-y_{m-1}).$$

In either case (c) holds. □

Example 1.9.6. Let $a = 1492$ and $b = 1066$. Then

$$\begin{array}{llllll}
 E_{-1}: & 1492 & = & 1492 & \cdot & 1 & + & 1066 & \cdot & 0 \\
 E_0: & 1066 & = & 1492 & \cdot & 0 & + & 1066 & \cdot & 1 \\
 E_1: & 426 & = & 1492 & \cdot & 1 & + & 1066 & \cdot & -1 & | E_{-1} & - & E_0 \\
 E_2: & 214 & = & 1492 & \cdot & -2 & + & 1066 & \cdot & 3 & | E_0 & - & 2E_1 \\
 E_3: & 212 & = & 1492 & \cdot & 3 & + & 1066 & \cdot & -4 & | E_1 & - & E_2 \\
 E_4: & 2 & = & 1492 & \cdot & -5 & + & 1066 & \cdot & 7 & | E_2 & - & E_3 \\
 E_5: & 0 & & & & & & & & & | E_3 & - & 106E_4
 \end{array}$$

So $2 = \gcd(1492, 1066)$ and $2 = 1492 \cdot -5 + 1066 \cdot 7$.

Theorem 1.9.7. Let a and b be integers, not both zero, and let $d \in \mathbb{Z}$ with $d = \gcd(a, b)$. Then d is the smallest positive integer of the form $au + bv$ with $u, v \in \mathbb{Z}$.

Proof. By the Euclidean Algorithm 1.9.5 $d = ax + by$ for some $x, y \in \mathbb{Z}$ and so has the required form.

Now let e be any positive integer of the form $e = au + bv$ for some $u, v \in \mathbb{Z}$. Since $d = \gcd(a, b)$, d divides a and b . Thus by (1.4.4)(c), d divides e . Hence 1.9.1 shows that $d \leq |d| \leq |e| = e$. Thus d is the smallest positive integer of the form $au + bv$ with $u, v \in \mathbb{Z}$. $\square$

un

Theorem 1.9.8. Let a, b be integers. Then $1 = \gcd(a, b)$ if and only if there exist integers u and v with $1 = au + bv$.

Proof. If $1 = \gcd(a, b)$, then $1 = au + bv$ for some $u, v \in \mathbb{Z}$ by the Euclidean Algorithm 1.9.5.

Conversely, suppose that $1 = au + bv$ for some $u, v \in \mathbb{Z}$. Since 1 is the smallest positive integer this shows that 1 is the smallest positive integer of the form $au + bv, u, v \in \mathbb{Z}$. From 1.9.7 we conclude that $1 = \gcd(a, b)$. $\square$

Theorem 1.9.9. Let n be a non-zero integer and $a \in \mathbb{Z}$. Then $1 = \gcd(a, n)$ if and only if $[a]_n$ is a unit in $\mathbb{Z}_n$.

Proof.

$$\begin{array}{llll}
 & 1 = \gcd(a, n) & & \\
 \iff & 1 = au + nv & \text{for some } u, v \in \mathbb{Z} & - 1.9.8 \\
 \iff & [1]_n = [au]_n & \text{for some } u \in \mathbb{Z} & - 1.4.9 \\
 \iff & [1]_n = [a]_n[u]_n & \text{for some } u \in \mathbb{Z} & - \text{Definition of multiplication in } \mathbb{Z}_n \\
 \iff & [1]_n = [a]_n U & \text{for some } U \in \mathbb{Z}_n & - \text{Definition of } \mathbb{Z}_n \\
 \iff & 1_{\mathbb{Z}_n} = [a]_n U & \text{for some } U \in \mathbb{Z}_n & - 1_{\mathbb{Z}_n} = [1]_n \text{ by 1.6.4} \\
 \iff & 1_{\mathbb{Z}_n} = [a]_n U \text{ and } 1_{\mathbb{Z}_n} = U[a]_n & \text{for some } U \in \mathbb{Z}_n & - \mathbb{Z}_n \text{ is commutative} \\
 \iff & [a]_n \text{ is a unit in } \mathbb{Z}_n & & - \text{Definition of a unit}
 \end{array}$$

□

Theorem 1.9.10. *Let a and b be integers and let d a positive integer. Then $d = \gcd(a, b)$ if and only if*

- (I) d is a common divisor of a and b ; and
- (II) if c is a common divisor of a and b , then $c \mid d$.

Proof. $\implies$: Suppose first that $d = \gcd(a, b)$. Then (I) holds by the definition of $\gcd$. By 1.9.5 $d = ax + by$ for some $x, y \in \mathbb{Z}$. So if c is a common divisor of a and b , then (1.4.4)(c) shows that $c \mid d$. Thus (II) holds.

$\impliedby$: Suppose next that (I) and (II) holds. Then by (I) d is a common divisor of a and b . Let c be a common divisor of a and b . Then by (II), $c \mid d$. Thus by 1.9.1, $c \leq |c| \leq |d| = d$. Hence by definition, $d = \gcd(a, b)$. □

Theorem 1.9.11. *Let a and b integers with $1 = \gcd(a, b)$. Let c be an integer with $a \mid bc$. Then $a \mid c$.*

Proof. Since $1 = \gcd(a, b)$, 1.9.5 shows that $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Hence

$$c = 1c = (ax + by)c = a(xc) + (bc)y.$$

Note that $a \mid a$ and $a \mid bc$, and that xc and y are integers. So by (1.4.4)(c), a divides $a(xc) + (bc)y$. Thus $a \mid c$. □

Exercises 1.9:

1.9#1. Let a, b and c be integers. If $a \mid c$ and $b \mid c$, must ab divide c ? What if $\gcd(a, b) = 1$?

1.9#2. Let a, b and e be integers. Suppose a and b are not both zero and that e is a positive common divisor of a and b . Let $d \in \mathbb{Z}$ with $d = \gcd(a, b)$.

- (a) Show that there exist integers $\tilde{a}, \tilde{b}$ and $\tilde{d}$ with $a = \tilde{a}e, b = \tilde{b}e$ and $d = \tilde{d}e$.
- (b) Prove that $\tilde{d} = \gcd(\tilde{a}, \tilde{b})$.
- (c) Show that there exist integers $\hat{a}$ and $\hat{b}$ with $a = \hat{a}d$ and $b = \hat{b}d$.
- (d) Prove that $\gcd(\hat{a}, \hat{b}) = 1$.

1.9#3. Prove or disprove each of the following statements.

- (a) If $2 \nmid a$, then $4 \mid (a^2 - 1)$.
- (b) If $2 \nmid a$, then $8 \mid (a^2 - 1)$.

1.9#4. Let n be a positive integers and a and b integers with $\gcd(a, b) = 1$. Use induction to show that $\gcd(a, b^n) = 1$.

1.9#5. Let a, b, c be integers with a, b not both zero. Prove that the equation $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$.

1.9#6. Prove that $\gcd(n, n+1) = 1$ for any integer n .

1.9#7. Prove or disprove each of the following statements.

(a) If $2 \nmid a$, then $24 \mid (a^2 - 1)$.

(b) If $2 \nmid a$ and $3 \nmid a$, then $24 \mid (a^2 - 1)$.

1.9#8. Let n be an integer. Then $\gcd(n+1, n^2 - n + 1) = 1$ or 3 .

1.9#9. Let a, b, c be integers with $a \mid bc$. Show that there exist integers $\tilde{b}, \tilde{c}$ with $\tilde{b} \mid b, \tilde{c} \mid c$ and $a = \tilde{b}\tilde{c}$.

1.10 Integral Primes

Definition 1.10.1. An integer p is called a prime if $p \notin \{0, 1, -1\}$ and the only divisors of p in $\mathbb{Z}$ are $1, -1, p$ and $-p$.

Theorem 1.10.2. (a) Let p be an integer. Then p is a prime if and only if $-p$ is prime.

(b) Let p be a prime integer and a an integer. Then either $(p \mid a \text{ and } |p| = \gcd(a, p))$ or $(p \nmid a \text{ and } 1 = \gcd(a, p))$.

(c) Let p and q be primes with $p \mid q$. Then $p = q$ or $p = -q$.

Proof. (a) Note that

$$(*) \quad p \notin \{0, \pm 1\} \quad \text{if and only if} \quad -p \notin \{0, \pm 1\},$$

By 1.4.4 $a \mid p \iff a \mid -p$. So

(**) p and $-p$ have the same divisors.

Moreover,

$$(***) \quad \pm p = \pm(-p)$$

Thus the following statements are equivalent:

- | | | |
|--------|--|--------------------------|
| | p is a prime | |
| $\iff$ | $p \notin \{0, \pm 1\}$ and the only divisors of p are ± 1 and $\pm p$ | - Definition of a prime. |
| $\iff$ | $-p \notin \{0, \pm 1\}$ and the only divisors of $-p$ are ± 1 and $\pm(-p)$ | - (*), (**) and (***) |
| $\iff$ | $-p$ is a prime. | - Definition of a prime. |

So (a) holds.

(b): Let $d \in \mathbb{Z}$ with $d = \gcd(a, p)$. Then $d|p$ and since p is prime, $d \in \{\pm 1, \pm p\}$. Since d is positive we conclude that

$$(+) \quad d = 1 \quad \text{or} \quad d = |p|.$$

Case 1: Suppose $p|a$.

Since $p|p$, we conclude that p is a common divisor of a and p . Thus by (1.4.4)(b) also $-p$ is a common divisor of a and p . Thus $|p|$ is a common divisor of a and p . As $d = \gcd(a, p)$ this gives $|p| \leq d$. By definition of a prime we have $p \notin \{0, \pm 1\}$, so $|p| > 1$. Hence also $d > 1$ and thus $d \neq 1$. Together with (+) we get $d = |p|$. So $|p| = \gcd(a, p)$ and, by the hypothesis of case 1, $p|a$. Thus (b) holds in this case.

Case 2: Suppose $p \nmid a$.

Since $p \nmid a$, (1.4.4)(b) shows that $-p \nmid a$. So also $|p| \nmid a$. As $d = \gcd(a, p)$, we have $d|a$ and so $d \neq |p|$. Hence by (+) $d = 1$. Thus $1 = \gcd(a, p)$ and by the hypothesis of case 2, $p \nmid a$. So (b) also holds in this case.

(c): Suppose p and q are primes with $p|q$. Since q is a prime we get $p \in \{\pm 1, \pm q\}$. Since p is prime, we know that $p \notin \{\pm 1\}$ and so $p \in \{\pm q\}$. $\square$

Theorem 1.10.3. *Let p be an integer with $p \notin \{0, \pm 1\}$. Then the following two statements are equivalent:*

(a) p is a prime.

(b) If a and b are integers with $p|ab$, then $p|a$ or $p|b$.

Proof. ‘ $\implies$ ’: Suppose p is prime and let a and b be integers with $p|ab$. We need to show that $p|a$ or $p|b$. So we may assume that $p \nmid a$. Then 1.10.2 gives $1 = \gcd(a, p)$. Since $p|ab$, 1.9.11 now implies that $p|b$.

‘ $\impliedby$ ’: For the converse, see Exercise 1.10#2. $\square$

Theorem 1.10.4. *Let $n \in \mathbb{Z}$ with $n \neq 0$ and $n \neq \pm 1$. Then n is the product of primes in $\mathbb{Z}$. In particular, there exists prime p with $p|n$ in $\mathbb{Z}$.*

Proof. We will prove the Theorem by complete induction on $|n|$.

Suppose first that n is a prime. Then $n = n$ is the product of one prime.

Suppose next that n is not a prime. Then the definition of a prime shows there exists an integer m with $m|n$, $m \neq \pm 1$ and $m \neq \pm n$. Then $n = mk$ for some $k \in \mathbb{Z}$. Since $m \neq \pm 1$ and $m \neq \pm n$ we get $|m| < |n|$ and $|k| < |n|$. By induction we conclude that both m and k are products of primes. So also $n = mk$ is a product of primes. $\square$

Theorem 1.10.5. *Let p be a prime integer. Then $\mathbb{Z}_p$ is a field.*

Proof. By 1.6.4 $\mathbb{Z}_p$ is a commutative ring with identity $[1]_p \neq [0]_p$. So we just need to show that every non-zero $A \in \mathbb{Z}_p$ is a unit. Note that $A = [a]_p$ for some $a \in \mathbb{Z}$ with $p \nmid a$. Thus (1.10.2)(b) gives $\gcd(a, p) = 1$. So $A = [a]_p$ is a unit in $\mathbb{Z}_p$ by 1.9.9. $\square$

Exercises 1.10:

1.10#1. Let p be an integer other than $0, \pm 1$. Prove that p is a prime if and only if it has this property: Whenever r and s are integers such that $p = rs$, then $r = \pm 1$ or $s = \pm 1$.

1.10#2. Let p be an integer other than $0, \pm 1$ with this property

(*) Whenever b and c are integers with $p \mid bc$, then $p \mid b$ or $p \mid c$. Prove that p is a prime.

1.10#3. Prove that $1 = \gcd(a, b)$ if and only if there does not exist a prime integer p with $p \mid a$ and $p \mid b$.

1.10#4. Prove or disprove each of the following statements:

- (a) If p is a prime and $p \mid a^2 + b^2$ and $p \mid c^2 + d^2$, then $p \mid (a^2 - c^2)$
- (b) If p is a prime and $p \mid a^2 + b^2$ and $p \mid c^2 + d^2$, then $p \mid (a^2 + c^2)$
- (c) If p is a prime and $p \mid a$ and $p \mid a^2 + b^2$, then $p \mid b$

1.10#5. Let a and b be integers. Then $a \mid b$ if and only if $a^3 \mid b^3$.

1.10#6. Prove or disprove: Let n be a positive integer, then there exists $p, a \in \mathbb{Z}$ such that $n = p + a^2$ and either $p = 1$ or p is a prime.

1.11 Isomorphism and Homomorphism

Definition 1.11.1. Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings and let $f : R \rightarrow S$ be a function.

(a) f is called a homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ if

$$f(a + b) = f(a) \oplus f(b) \quad [f \text{ respects addition}]$$

and

$$f(a \cdot b) = f(a) \odot f(b) \quad [f \text{ respects multiplication}]$$

for all $a, b \in R$.

- (b) f is called an isomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$, if f is a homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ and f is bijective.
- (c) $(R, +, \cdot)$ is called isomorphic to $(S, \oplus, \odot)$, if there exists an isomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$.

Example 1.11.2. (1) Consider the function

$$g: \mathbb{R} \rightarrow \mathbb{R}, \quad a \mapsto -a.$$

Let $a, b \in \mathbb{R}$. Then

$$g(a + b) = -(a + b) = -a + (-b) = g(a) + g(b).$$

and so g respects addition.

$$g(ab) = -(ab) \quad \text{and} \quad g(a)g(b) = (-a)(-b) = ab$$

For $a = b = 1$ we conclude that

$$g(1 \cdot 1) = -(1 \cdot 1) = -1 \quad \text{and} \quad g(1)g(1) = 1 \cdot 1 = 1.$$

So $g(1 \cdot 1) \neq g(1) \cdot g(1)$. Thus g does not respect multiplication, and g is not a homomorphism. But note that g is a bijection.

(2) Let R and S be rings and consider the function

$$h: R \rightarrow S, \quad r \mapsto 0_S.$$

Let $a, b \in R$. Then

$$h(a + b) = 0_S = 0_S + 0_S = h(a) + h(b) \quad \text{and} \quad h(ab) = 0_S = 0_S 0_S = h(a)h(b).$$

So h is a homomorphism. h is injective if and only if $R = \{0_R\}$ and h is surjective if and only if $S = \{0_S\}$. Hence h is an isomorphism if and only if $R = \{0_R\}$ and $S = \{0_S\}$.

(3) Let S be a ring and R a subring of S . Consider the function

$$\text{id}_{R,S}: R \rightarrow S, \quad r \mapsto r.$$

Let $a, b \in R$. Then

$$\text{id}_{R,S}(a + b) = a + b = \text{id}_{R,S}(a) + \text{id}_{R,S}(b) \quad \text{and} \quad \text{id}_{R,S}(ab) = ab = \text{id}_{R,S}(a)\text{id}_{R,S}(b)$$

and so $\text{id}_{R,S}$ is a homomorphism. Note that $\text{id}_{R,S}$ is injective. Moreover, $\text{id}_{R,S}$ is surjective if and only if $R = S$. Hence $\text{id}_R := \text{id}_{R,R}$ is an isomorphism.

(4) Let R be a commutative ring and $n \in R$. Consider the function

$$k: R \rightarrow R_n, \quad a \mapsto [a]_n.$$

Let $a, b \in R$. By definition of the addition and multiplication in R_n

$$k(a+b) = [a+b]_n = [a]_n \oplus [b]_n = k(a) \oplus k(b) \quad \text{and} \quad k(ab) = [ab]_n = [a]_n \odot [b]_n = k(a) \odot k(b).$$

So k is homomorphism.

Let $A \in R_n$. The definition of R_n shows that $A = [a]_n$ for some $a \in R$. Hence $k(a) = A$ and so k is surjective.

Note that

$$k(n) = [n]_n = [0_R]_n = k(0_R).$$

If $n \neq 0_R$ we conclude that k is not injective.

Suppose $n = 0_R$. Then by Example (1.4.6)(3) $a \equiv b \pmod{n}$ if and only if $a = b$. Hence also $[a]_n = [b]_n$ if and only if $a = b$. Thus k is injective.

Example 1.11.3. Consider the function

$$f: \mathbb{C} \rightarrow M_2(\mathbb{R}), \quad r + si \mapsto \begin{bmatrix} r & s \\ -s & r \end{bmatrix}.$$

Let $a, b \in \mathbb{C}$. Then $a = r + si$ and $b = \tilde{r} + \tilde{s}i$ for some $r, s, \tilde{r}, \tilde{s} \in \mathbb{R}$. So

$$\begin{aligned} f(a+b) &= f((r+si) + (\tilde{r}+\tilde{s}i)) \\ &= f((r+\tilde{r}) + (s+\tilde{s})i) \\ &= \begin{bmatrix} r+\tilde{r} & s+\tilde{s} \\ -(s+\tilde{s}) & r+\tilde{r} \end{bmatrix} \\ &= \begin{bmatrix} r & s \\ -s & r \end{bmatrix} + \begin{bmatrix} \tilde{r} & \tilde{s} \\ -\tilde{s} & \tilde{r} \end{bmatrix} \\ &= f(r+si) + f(\tilde{r}+\tilde{s}i) \\ &= f(a) + f(b) \end{aligned}$$

and

$$\begin{aligned}
f(ab) &= f((r+si)(\tilde{r}+\tilde{s}i)) \\
&= f((r\tilde{r}-s\tilde{s})+(r\tilde{s}+s\tilde{r})i) \\
&= \begin{bmatrix} r\tilde{r}-s\tilde{s} & r\tilde{s}+s\tilde{r} \\ -(r\tilde{s}+s\tilde{r}) & r\tilde{r}-s\tilde{s} \end{bmatrix} \\
&= \begin{bmatrix} r & s \\ -s & r \end{bmatrix} \begin{bmatrix} \tilde{r} & \tilde{s} \\ -\tilde{s} & \tilde{r} \end{bmatrix} \\
&= f(r+si)f(\tilde{r}+\tilde{s}i) \\
&= f(a)f(b).
\end{aligned}$$

Thus f is a homomorphism.

If $f(a) = f(b)$, then

$$\begin{bmatrix} r & s \\ -s & r \end{bmatrix} = \begin{bmatrix} \tilde{r} & \tilde{s} \\ -\tilde{s} & \tilde{r} \end{bmatrix}$$

and so $r = \tilde{r}$ and $s = \tilde{s}$. Hence $a = r+si = \tilde{r}+\tilde{s}i = b$ and so f is injective.

Since $1 \neq 0$ we have that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} r & s \\ -s & r \end{bmatrix}$ for all $r, s \in \mathbb{R}$. Thus f is not surjective.

Put

$$S := \text{Im}(f) = \left\{ \begin{bmatrix} r & s \\ -s & r \end{bmatrix} \mid r, s \in \mathbb{R} \right\}.$$

Using the Subring theorem it is straight forward to check that S is a subring of $M_2(\mathbb{R})$. Alternatively, Theorem 1.11.11 below also shows that S is a subring of $M_2(\mathbb{R})$. It follows that

$$\tilde{f}: \mathbb{C} \rightarrow S, \quad r+is \mapsto \begin{bmatrix} r & s \\ -s & r \end{bmatrix}.$$

is an isomorphism of rings. Thus

$$\mathbb{C} \quad \text{and} \quad \left\{ \begin{bmatrix} r & s \\ -s & r \end{bmatrix} \mid r, s \in \mathbb{R} \right\}.$$

are isomorphic rings.

Notation 1.11.4. (a) ‘ $f: R \rightarrow S$ is a ring homomorphism’ stands for the more precise statement ‘ $(R, +, \cdot)$ and $(S, \oplus, \odot)$ are rings and f is a ring homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$.’

- (b) Usually we will use the symbols $+$ and $\cdot$ also for the addition and multiplication on S and so the two conditions for a homomorphism become

$$f(a + b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b).$$

Remark 1.11.5. Let $R = \{r_1, r_2, \dots, r_n\}$ be a ring with n elements. Suppose that the addition and multiplication table is given by

$$A: \begin{array}{c|ccccc} & + & r_1 & \dots & r_j & \dots & r_n \\ \hline r_1 & a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_i & a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_n & a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{array} \quad \text{and} \quad M: \begin{array}{c|ccccc} & \cdot & r_1 & \dots & r_j & \dots & r_n \\ \hline r_1 & b_{11} & \dots & b_{1j} & \dots & b_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_i & b_{i1} & \dots & b_{ij} & \dots & b_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_n & b_{n1} & \dots & b_{nj} & \dots & b_{nn} \end{array}$$

So $r_i + r_j = a_{ij}$ and $r_i r_j = b_{ij}$ for all $1 \leq i, j \leq n$.

Let S be a ring and $f: R \rightarrow S$ a function. For $r \in R$ put $r' = f(r)$. Consider the tables A' and M' obtain from the tables A and M by replacing all entries by its image under f :

$$A': \begin{array}{c|ccccc} & r'_1 & \dots & r'_j & \dots & r'_n \\ \hline r'_1 & a'_{11} & \dots & a'_{1j} & \dots & a'_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r'_i & a'_{i1} & \dots & a'_{ij} & \dots & a'_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r'_n & a'_{n1} & \dots & a'_{nj} & \dots & a'_{nn} \end{array} \quad \text{and} \quad M': \begin{array}{c|ccccc} & r'_1 & \dots & r'_j & \dots & r'_n \\ \hline r'_1 & b'_{11} & \dots & b'_{1j} & \dots & b'_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r'_i & b'_{i1} & \dots & b'_{ij} & \dots & b'_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r'_n & b'_{n1} & \dots & b'_{nj} & \dots & b'_{nn} \end{array}$$

- (a) f is a homomorphism if and only if A' and M' are the tables for the addition and multiplication of the elements $r'_1, \dots, r'_n$ in S , that is $r'_i + r'_j = a'_{ij}$ and $r'_i r'_j = b'_{ij}$ for all $1 \leq i, j \leq n$.
- (b) f is injective if and only if $r'_1, \dots, r'_n$ are pairwise distinct.
- (c) f is surjective if and only if $S = \{r'_1, r'_2, \dots, r'_n\}$.
- (d) f is an isomorphism if and only if A' is an addition table for S and M' is a multiplication table for S .

Proof. (a) f is a homomorphism if and only if

$$f(a + b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b)$$

for all $a, b \in R$. Since $R = \{r_1, \dots, r_n\}$, this holds if and only if

$$f(r_i + r_j) = f(r_i) + f(r_j) \quad \text{and} \quad f(r_i r_j) = f(r_i) f(r_j)$$

for all $1 \leq i, j \leq n$. Since $r_i + r_j = a_{ij}$ and $r_i r_j = b_{ij}$ this holds if and only if

$$f(a_{ij}) = f(r_i) + f(r_j) \quad \text{and} \quad f(b_{ij}) = f(r_i) f(r_j)$$

for all $1 \leq i, j \leq n$. Since $f(r) = r'$, this is equivalent to

$$a'_{ij} = r'_i + r'_j \quad \text{and} \quad b'_{ij} = r'_i r'_j$$

for all $1 \leq i, j \leq n$

(b) f is injective if and only if (for all $a, b \in R$) $f(a) = f(b)$ implies $a = b$ and so if and only if $a \neq b$ implies $f(a) \neq f(b)$. Since for each $a \in R$ there exists a unique $1 \leq i \leq n$ with $a = r_i$, f is injective if and only (for all $1 \leq i, j \leq n$) $i \neq j$ implies $f(r_i) \neq f(r_j)$, that is $i \neq j$ implies $r'_i \neq r'_j$.

(c) f is surjective if and only if $\text{Im } f = S$. Since $R = \{r_1, \dots, r_n\}$, $\text{Im } f = \{f(r_1), \dots, f(r_n)\} = \{r'_1, \dots, r'_n\}$. So f is surjective if and only if $S = \{r'_1, \dots, r'_n\}$.

(d) Follows from (a)-(c). □

Example 1.11.6. Let R be the ring with additions and multiplication table

$$\begin{array}{c|cc} \oplus & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \boxtimes & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}$$

Note here that R is indeed a ring, see Example 1.1.6. Show that

$$f: R \rightarrow \mathbb{Z}_2, \quad 0 \mapsto 1, \quad 1 \mapsto 0$$

is an isomorphism.

We will use 1.11.5. So we will replace 0 by $0' = f(0) = 1$ and 1 by $1' = f(1) = 0$ in the above tables:

$$\begin{array}{c|cc} & 1 & 0 \\ \hline 1 & 0 & 1 \\ 0 & 1 & 0 \end{array} \quad \text{and} \quad \begin{array}{c|cc} & 1 & 0 \\ \hline 1 & 1 & 0 \\ 0 & 0 & 0 \end{array}.$$

Note that these are addition and multiplication tables for $\mathbb{Z}_2$ and so 1.11.5 shows that f is indeed an isomorphism.

Theorem 1.11.7. *Let $f : R \rightarrow S$ be a homomorphism of rings. Then*

- (a) $f(0_R) = 0_S$.
- (b) $f(-a) = -f(a)$ for all $a \in R$.
- (c) $f(a - b) = f(a) - f(b)$ for all $a, b \in R$.

Proof. (a) We have

$$\begin{aligned} f(0_R) + f(0_R) &= f(0_R + 0_R) && - f \text{ respects addition} \\ &= f(0_R) && - \mathbf{Ax 4} \text{ for } R. \end{aligned}$$

So the Additive Identity Law 1.2.4 for S implies that $f(0_R) = 0_S$.

(b) We compute

$$\begin{aligned} f(a) + f(-a) &= f(a + (-a)) && - f \text{ respects addition} \\ &= f(0_R) && - \mathbf{Ax 5} \text{ for } R. \\ &= 0_S && - \text{by (a)} \end{aligned}$$

So the Additive Inverse Law 1.2.6 for S implies that $f(-a) = -f(a)$.

(c)

$$f(a - b) \stackrel{\text{def } \hookrightarrow}{=} f(a + (-b)) \stackrel{\text{f hom}}{=} f(a) + f(-b) \stackrel{(b)}{=} f(a) + (-f(b)) \stackrel{\text{def } \hookrightarrow}{=} f(a) - f(b).$$

□

Example 1.11.8. Show that $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic.

Put $R := \mathbb{Z}_2 \times \mathbb{Z}_2$. Since $x + x = [0]_2$ for all $x \in \mathbb{Z}_2$ we also have

$$(x, y) + (x, y) = (x + x, y + y) = ([0]_2, [0]_2) = 0_R.$$

for all $x, y \in \mathbb{Z}_2$. Thus

$$(*) \quad r + r = 0_R$$

for all $r \in R$. Let S be any ring isomorphic to R . We claim that $s + s = 0_S$ for all $s \in S$. Indeed, let $f : R \rightarrow S$ be an isomorphism and let $s \in S$. Since f is surjective, there exists $r \in R$ with $f(r) = s$. Thus

$$s + s = f(r) + f(r) \stackrel{\text{f hom}}{=} f(r + r) \stackrel{(*)}{=} f(0_R) \stackrel{(1.11.7)(a)}{=} 0_S$$

Since $[1]_4 + [1]_4 = [2]_4 \neq [0]_4$ we conclude that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem 1.11.9. *Let $f : R \rightarrow S$ be a homomorphism of rings. Suppose that R has an identity and that f is surjective. Then*

- (a) S is a ring with identity and $f(1_R) = 1_S$.
- (b) If u is a unit in R , then $f(u)$ is a unit of S and $f(u^{-1}) = f(u)^{-1}$.

Proof. (a) We will first show that $f(1_R)$ is an identity of S . For this let $s \in S$. Since f is surjective, we know that $s = f(r)$ for some $r \in R$. Thus

$$s \cdot f(1_R) = f(r)f(1_R) \stackrel{\text{f hom}}{=} f(r1_R) \stackrel{\mathbf{Ax 10}}{=} f(r) = s,$$

and similarly $f(1_R) \cdot s = s$. So $f(1_R)$ is an identity of S . By (1.8.3)(a) S has at most one identity and so $f(1_R) = 1_S$.

- (b) Let u be a unit in R . We will first show that $f(u^{-1})$ is an inverse of $f(u)$:

$$f(u)f(u^{-1}) \stackrel{\text{f hom}}{=} f(uu^{-1}) \stackrel{\text{def inv}}{=} f(1_R) \stackrel{(a)}{=} 1_S.$$

Similarly $f(u^{-1})f(u) = 1_S$. Thus $f(u^{-1})$ is an inverse of $f(u)$ and so $f(u)$ is a unit. By 1.8.4 $f(u)^{-1}$ is the unique inverse of $f(u)$ and so $f(u^{-1}) = f(u)^{-1}$. $\square$

Example 1.11.10. Find all surjective homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_2 \times \mathbb{Z}_3$.

We start with setting up some convenient notation. For $a, b \in \mathbb{Z}$ and h a function from $\mathbb{Z}_6$ to $\mathbb{Z}_2 \times \mathbb{Z}_3$ define

$$[a] := [a]_6, \quad h[a] := h([a]_6), \quad \text{and} \quad [a, b] := ([a]_2, [b]_3).$$

Let $a, b, c, d \in \mathbb{Z}$. Then

$$[a, b] + [c, d] = ([a]_2, [b]_3) + ([c]_2, [d]_3) = ([a]_2 + [c]_2, [b]_3 + [d]_3) = ([a + c]_2, [b + d]_3) = [a + c, b + d].$$

Thus

$$(*) \quad [a, b] + [c, d] = [a + c, b + d] \quad \text{and similarly} \quad [a, b] \cdot [c, d] = [a \cdot c, b \cdot d]$$

‘Uniqueness of a surjective homomorphism’:

Let $f : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ be a surjective homomorphism. We will compute $f[r]$ for $0 \leq r \leq 5$ and thereby prove that f is uniquely determined. Since f is an surjective homomorphism, (1.11.9)(a) gives $f(1_{\mathbb{Z}_6}) = 1_{\mathbb{Z}_2 \times \mathbb{Z}_3}$. Since $[1]$ is the identity in $\mathbb{Z}_6$ and $[1, 1]$ is the identity in $\mathbb{Z}_2 \times \mathbb{Z}_3$ this gives $f[1] = [1, 1]$. Similarly, by (1.11.7)(a), $f(0_{\mathbb{Z}_6}) = 0_{\mathbb{Z}_2 \times \mathbb{Z}_3}$ and thus $f[0] = [0, 0]$. We compute

$$\begin{aligned}
f[0] &= [0, 0] \\
f[1] &= [1, 1] \\
f[2] &= f[1 + 1] = f[1] + f[1] = [1, 1] + [1, 1] = [2, 2] = [0, 2] \\
f[3] &= f[2 + 1] = f[2] + f[1] = [2, 2] + [1, 1] = [3, 3] = [1, 0] \\
f[4] &= f[3 + 1] = f[3] + f[1] = [3, 3] + [1, 1] = [4, 4] = [0, 1] \\
f[5] &= f[4 + 1] = f[4] + f[1] = [4, 4] + [1, 1] = [5, 5] = [1, 2]
\end{aligned}$$

By 1.5.7 $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. Hence f is uniquely determined.

‘Existence of a surjective homomorphism’:

Define the function $g : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ by

$$(**) \quad g[r] = [r, r] \quad \text{for all } r \in \mathbb{Z} \text{ with } 0 \leq r \leq 5.$$

We will show that g is an isomorphism, and so also a surjective homomorphism. For this we first show that $g[m] = [m, m]$ for all $m \in \mathbb{Z}$. Indeed, by the Division Algorithm, $m = 6q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < 6$. Then by 1.4.9 $[m]_6 = [r]_6$. Moreover, $m = 2(3q) + r = 3(2q) + r$ and so $[m]_2 = [r]_2$ and $[m]_3 = [r]_3$. Hence $[m] = [r]$ and $[m, m] = [r, r]$ and we conclude

$$(* **) \quad g[m] = g[r] = [r, r] = [m, m].$$

Thus

$$g[n + m] \stackrel{(***)}{=} [n + m, n + m] \stackrel{(*)}{=} [n, n] + [m, m] \stackrel{(***)}{=} g[n] + g[m],$$

and

$$g[nm] \stackrel{(***)}{=} [nm, nm] \stackrel{(*)}{=} [n, n][m, m] \stackrel{(***)}{=} g[n]g[m].$$

So g is a homomorphism of rings. Since $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ and $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ we have

$$\begin{aligned}
\mathbb{Z}_2 \times \mathbb{Z}_3 &= \{(x, y) \mid x \in \mathbb{Z}_2, y \in \mathbb{Z}_3\} = \{[0, 0], [0, 1], [0, 2], [1, 0], [1, 1], [1, 2]\} \\
&= \{[0, 0], [4, 4], [2, 2], [3, 3], [1, 1], [5, 5]\} \\
&= \{g[0], g[4], g[2], g[3], g[1], g[5]\}
\end{aligned}$$

and so g is surjective. Note that g is also injective. Thus g is an isomorphism and so

$$(+) \quad \mathbb{Z}_6 \text{ is isomorphic to } \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Theorem 1.11.11. *Let $f : R \rightarrow S$ be a homomorphism of rings. Then $\text{Im } f$ is a subring of S . (Recall here that $\text{Im } f = \{f(r) \mid r \in R\}$).*

Proof. It suffices to verify the four conditions in the Subring Theorem 1.7.2. Observe first that for $s \in S$,

$$(*) \quad s \in \text{Im } f \quad \Longleftrightarrow \quad s = f(r) \text{ for some } r \in R$$

Let $x, y \in \text{Im } f$. Then by $(*)$:

$$(**) \quad x = f(a) \quad \text{and} \quad y = f(b) \quad \text{for some } a, b \in R.$$

(I) By (1.11.7)(a) $f(0_R) = 0_S$. By **Ax 4** $0_R \in R$ and so $0_S \in \text{Im } f$ by $(*)$

(II) $x + y \stackrel{(**)}{=} f(a) + f(b) \stackrel{\text{f hom}}{=} f(a + b)$. By **Ax 1** $a + b \in R$. So $x + y \in \text{Im } f$ by $(*)$.

(III) $xy \stackrel{(**)}{=} f(a)f(b) \stackrel{\text{f hom}}{=} f(ab)$. By **Ax 6** $ab \in R$. So $xy \in \text{Im } f$ by $(*)$.

(IV) $-x \stackrel{(**)}{=} -f(a) \stackrel{(1.11.7)(b)}{=} f(-a)$. By **Ax 5** $-a \in R$. So $-x \in \text{Im } f$ by $(*)$. □

Definition 1.11.12. Let R be a ring. For $n \in \mathbb{Z}$ and $a \in R$ define $na \in R$ as follows:

(i) $0a = 0_R$.

(ii) If $n \geq 0$ and na already has been defined, define $(n + 1)a = na + a$.

(iii) If $n < 0$ define $na = -((-n)a)$.

Exercises 1.11:

1.11#1. Let R be ring, $n, m \in \mathbb{Z}$ and $a, b \in R$. Show that

- | | | |
|--------------------|----------------------------|-----------------------------|
| (a) $1a = a$. | (c) $(n + m)a = na + ma$. | (e) $n(a + b) = na + nb$. |
| (b) $(-1)a = -a$. | (d) $(nm)a = n(ma)$. | (f) $n(ab) = (na)b = a(nb)$ |

1.11#2. Let $f : R \rightarrow S$ be a ring homomorphism. Show that $f(na) = nf(a)$ for all $n \in \mathbb{Z}$ and $a \in R$.

1.11#3. Let R be a ring. Show that:

- (a) If $f : \mathbb{Z} \rightarrow R$ is a homomorphism, then $f(1)^2 = f(1)$.
- (b) Let $a \in R$ with $a^2 = a$. Then there exists a unique homomorphism $g : \mathbb{Z} \rightarrow R$ with $g(1) = a$.

1.11#4. Let $S = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} \mid a, b \in \mathbb{Z}_2 \right\}$. Given that S is a subring of $M_2(\mathbb{Z}_2)$. Show that S is isomorphic to the ring R from Exercise 1.1#4.

1.11#5. (a) Give an example of a ring R and a function $f : R \rightarrow R$ such that $f(a+b) = f(a) + f(b)$ for all $a, b \in R$, but $f(ab) \neq f(a)f(b)$ for some $a, b \in R$.

(b) Give an example of a ring R and a function $f : R \rightarrow R$ such that $f(ab) = f(a)f(b)$ for all $a, b \in R$, but $f(a+b) \neq f(a) + f(b)$ for some $a, b \in R$.

1.11#6. Let L be the ring of all matrices in $M_2(\mathbb{Z})$ of the form $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ with $a, b, c \in \mathbb{Z}$. Show that the

function $f : L \rightarrow \mathbb{Z}$ given by $f\left(\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}\right) = a$ is a surjective homomorphism but is not an isomorphism.

1.11#7. Let n and m be positive integers with $n \equiv 1 \pmod{m}$. Define $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_{nm}, [x]_m \mapsto [xn]_{nm}$. Show that

(a) f is well-defined. (That is if x, y are integers with $[x]_m = [y]_m$, then $[xn]_{nm} = [yn]_{nm}$)

(b) f is a homomorphism.

(c) f is injective.

(d) If $n > 1$, then f is not surjective.

1.11#8. Let $f : R \rightarrow S$ be a ring homomorphism. Let B be a subring of S and define

$$A = \{r \in R \mid f(r) \in B\}.$$

Show that A is a subring of R .

1.11#9. Show that the two rings are not isomorphic.

(a) $2\mathbb{Z}$ and $\mathbb{Z}$.

(c) $\mathbb{Z}_2 \times \mathbb{Z}_{14}$ and $\mathbb{Z}_{16}$.

(e) $\mathbb{Z} \times \mathbb{Z}_2$ and $\mathbb{Z}$.

(b) $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ and $M_2(\mathbb{R})$.

(d) $\mathbb{Q}$ and $\mathbb{R}$.

(f) $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16}$.

1.11#10. Let $f : R \rightarrow S$ and $g : S \rightarrow T$ be homomorphism of rings.

(a) Show that $g \circ f : R \rightarrow T$ is a homomorphism of rings.

(b) If f and g are isomorphisms, show that $g \circ f$ is an isomorphism.

(c) Suppose f is an isomorphism. For $s \in S$ let s' be the unique element of R with $f(s') = s$. Show that the function $h : S \rightarrow R, s \mapsto s'$ is an isomorphism of rings.

1.11#11. Let $f : R \rightarrow S$ be an isomorphism of rings. If R is an integral domain, show that S is an integral domain.

1.12 The ‘Associated’ Relation on a Ring

Definition 1.12.1. Let R be ring with identity and let $a, b \in R$. We say that a is associated to b , or that b is an associate of a and write $a \sim_R b$ if there exists a unit u of R with $au = b$.

Remark 1.12.2. (a) We will usually just write $a \sim b$ for the more precise $a \sim_R b$.

(b) Until now we have used ‘ $\sim$ ’ to denote an arbitrary relation. From now on the symbol ‘ $\sim$ ’ will be reserved for the relation ‘associated’ on a ring R .

Example 1.12.3. (1) Let $n \in \mathbb{Z}$. Find all associates of n in $\mathbb{Z}$.

By 1.8.2 the units in $\mathbb{Z}$ are ± 1 . So the associates of n are $n \cdot \pm 1$, that is $\pm n$.

(2) Find all associates of 0, 1, 2 and 5 in $\mathbb{Z}_{10}$.

By 1.5.7 $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and so $\mathbb{Z}_{10} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, 5\}$.

We compute (in $\mathbb{Z}$)

n	0	± 1	± 2	± 3	± 4	5
$\gcd(n, 10)$	10	$\boxed{1}$	2	$\boxed{1}$	2	5

and so by 1.9.9 the units in $\mathbb{Z}_{10}$ are ± 1 and ± 3 .

Hence the associates of $a \in \mathbb{Z}_{10}$ are $a \cdot \pm 1$ and $a \cdot \pm 3$, that is $\pm a$ and $\pm 3a$. We compute

a	associates of a	associates of a , simplified
0	$\pm 0, \pm 3 \cdot 0$	0
± 1	$\pm 1, \pm 3 \cdot 1$	$\pm 1, \pm 3$
± 2	$\pm 2, \pm 3 \cdot 2$	$\pm 2, \pm 4$
5	$\pm 5, \pm 3 \cdot 5$	5

Theorem 1.12.4. Let R be a ring with identity. Then the relation $\sim$ (‘is associated to’) is an equivalence relation on R .

Proof. Reflexive: Let $a \in R$. By **Ax 10**, $1_R = 1_R 1_R$. Hence 1_R is a unit in R . By **Ax 10a** $1_R a = a$ and so $a \sim a$ by definition of ‘ $\sim$ ’. Thus $\sim$ is reflexive.

Symmetric: Let $a, b \in R$ with $a \sim b$. By definition of ‘ $\sim$ ’ this means that exists a unit $u \in R$ with $au = b$. Since u is a unit, u has an inverse u^{-1} . As $b = au$ the Principal Of Substitution gives

$$bu^{-1} = (au)u^{-1} \stackrel{\text{Ax 2}}{=} a(uu^{-1}) \stackrel{\text{def } u^{-1}}{=} a1_R \stackrel{\text{Ax 10}}{=} a.$$

By (1.8.5)(a) u^{-1} is a unit in R and so $b \sim a$. Thus $\sim$ is symmetric.

Transitive: Let $a, b, c \in R$ with $a \sim b$ and $b \sim c$. Then

$$(*) \quad au = b \quad \text{and} \quad bv = c$$

for some units u and v in R . Hence

$$c \stackrel{(*)}{=} bv \stackrel{(*)}{=} (au)v \stackrel{\mathbf{Ax} 2}{=} a(uv)$$

By (1.8.5)(b) uv is a unit in R and so $a \sim c$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, $\sim$ is an equivalence relation. $\square$

Example 1.12.5. Determine the equivalence classes of $\mathbb{Z}_{10}$ with respect to $\sim$.

Note that for $a \in \mathbb{Z}_{10}$, $[a]_{\sim} = \{b \in \mathbb{Z}_{10} \mid a \sim b\}$ is the set of associates of a . So by Example 1.12.3

$$\begin{aligned} [0]_{\sim} &= \{0\} \\ [1]_{\sim} &= \{\pm 1, \pm 3\} \\ [2]_{\sim} &= \{\pm 2, \pm 4\} \\ [5]_{\sim} &= \{5\} \end{aligned}$$

By 1.5.7 $\mathbb{Z}_{10} = \{0, 1, \dots, 9\} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, 5\}$. Each of these elements appears in one of the four classes listed above, so for each $x \in \mathbb{Z}_{10}$ there exists $y \in \{0, 1, 2, 5\}$ with $x \in [y]_{\sim}$. Thus by A.6.5 $[x]_{\sim} = [y]_{\sim}$. Hence $[0]_{\sim}, [1]_{\sim}, [2]_{\sim}, [5]_{\sim}$ are all the equivalence classes of $\sim$.

Theorem 1.12.6. Let R be a ring with identity and $a, b \in R$ with $a \sim b$. Then $a \mid b$ and $b \mid a$ in R .

Proof. Since $a \sim b$, $au = b$ for some unit $u \in R$. So $a \mid b$.

By 1.12.4 the relation $\sim$ is symmetric and so $a \sim b$ implies $b \sim a$. Hence we can apply the result of the previous paragraph with a and b interchanged and conclude that $b \mid a$. $\square$

Theorem 1.12.7. Let R be a commutative ring with identity and $r \in R$. Then the following four statements are equivalent:

- (a) $1_R \sim r$.
- (b) $r \mid 1_R$
- (c) There exists s in R with $rs = 1_R$.
- (d) r is a unit.

Proof. (a) $\implies$ (b): If $1_R \sim r$ then 1.12.6 gives $r \mid 1_R$.

(b) $\implies$ (c): Follows from the definition of 'divide'.

(c) $\implies$ (d): Suppose that $rs = 1_R$ for some $s \in R$. Since R is commutative, we get $sr = 1_R$. So r is a unit.

(d) $\implies$ (a): Suppose r is a unit. By **Ax 10**, $1_R r = r$. Since r is a unit, the definition of ' $\sim$ ' shows that $1_R \sim r$. $\square$

Theorem 1.12.8. *Let R be a ring with identity and $a, b, c, d \in R$ with $a \sim b$ and $c \sim d$. Then $a|c$ if and only if $b|d$.*

Proof. ‘ $\implies$ ’: Suppose that $a|c$. Since $a \sim b$ 1.12.6 shows $b|a$. Hence we have $b|a$ and $a|c$ and since $\dagger$ is transitive by (1.4.4)(a) we conclude that $b|c$. As $c \sim d$ we know that $c|d$, see 1.12.6. Thus $b|c$ and $c|d$ and since $\dagger$ is transitive we get $b|d$.

‘ $\impliedby$ ’: Observe the set-up is symmetric. So the backward direction follows from the forward direction applied with (c, d, a, b) in place of (a, b, c, d) . $\square$

Definition 1.12.9. *Let R be a ring and $a, b \in R$. We say that a and b divide each other in R and write $a \approx b$ if*

$$a|b \quad \text{and} \quad b|a.$$

Exercises 1.12:

1.12#1. Let $R = \mathbb{Z}_{18}$.

- (a) Find all units in R .
- (b) Determine the equivalence classes of the relation $\sim$ on R .

1.12#2. Let R be a ring with identity. Prove that:

- (a) $\approx$ is an equivalence relation on R .
- (b) Let $a, b, c, d \in R$ with $a \approx b$ and $c \approx d$. Then $a|c$ if and only if $b|d$.

1.12#3. Let n be a positive integer and $a, b \in \mathbb{Z}$. Put $d = \gcd(a, n)$ and $e = \gcd(b, n)$. Prove that:

- (a) $[a]_n | [d]_n$ in $\mathbb{Z}_n$.
- (b) $[a]_n \approx [d]_n$.
- (c) Let $r, s \in \mathbb{Z}$ with $r|n$ in $\mathbb{Z}$. Then $[r]_n | [s]_n$ in $\mathbb{Z}_n$ if and only if $r|s$ in $\mathbb{Z}$.
- (d) $[d]_n | [e]_n$ in $\mathbb{Z}_n$ if and only if $d|e$ in $\mathbb{Z}$.
- (e) $[a]_n | [b]_n$ in $\mathbb{Z}_n$ if and only if $d|e$ in $\mathbb{Z}$.
- (f) $[d]_n \approx [e]_n$ if and only if $d = e$.
- (g) $[a]_n \approx [b]_n$ if and only if $d = e$.

1.12#4. Let R be an integral domain and $a, b, c \in R$ such that $a \neq 0_R$ and $ba|ca$. Then $b|c$.

1.12#5. Is A associated to B in $M_2(\mathbb{R})$?

$$(a) \quad A = \begin{bmatrix} 2 & 4 \\ 3 & 6 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 10 & 6 \\ 15 & 9 \end{bmatrix}.$$

$$(b) \quad A = \begin{bmatrix} 2 & 4 \\ 3 & 6 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 12 & 20 \\ 15 & 25 \end{bmatrix}.$$

Chapter 2

Polynomial Rings

2.1 Addition and Multiplication

Definition 2.1.1. Let R and P be rings and $x \in P$. Then P is called a polynomial ring in x with coefficients in R provided that the following four conditions hold:

- (i) R has an identity, and R is subring of P .
- (ii) $ax = xa$ for all $a \in R$.
- (iii) For each $f \in P$, there exist $n \in \mathbb{N}$ and $f_0, f_1, \dots, f_n \in R$ such that

$$f = \sum_{i=0}^n f_i x^i \quad (= f_0 + f_1 x + \dots + f_n x^n).$$

- (iv) Whenever $n, m \in \mathbb{N}$ with $n \leq m$ and $f_0, f_1, \dots, f_n, g_0, \dots, g_m \in R$ with

$$\sum_{i=0}^n f_i x^i = \sum_{i=0}^m g_i x^i,$$

then $f_i = g_i$ for all $0 \leq i \leq n$ and $g_i = 0_R$ for all $n < i \leq m$.

Remark 2.1.2. Let P be a polynomial ring in x with coefficients in the ring R .

- (a) The elements of P are called polynomials in x with coefficients in R . **Polynomials are not functions.** See section 2.7 for the connections between polynomials and polynomial functions.
- (b) x is a fixed element of P . **x is not a variable.**

We remark that by E.3.1 there exists a ring P and $x \in P$ such that P is polynomial ring in x with coefficients in R , namely the elements of P are the sequences

$$(a_i)_{i=0}^{\infty} = (a_0, a_1, a_2, \dots, a_i, \dots)$$

such that $a_i \in R$ for all $i \in \mathbb{N}$ and there exists $n \in \mathbb{N}$ with $a_i = 0_R$ for all $i > n$. Also

$$\begin{aligned} x &= (0_R, 1_R, 0_R, 0_R, \dots, 0_R, \dots) \\ (a_0, a_1, a_2, \dots, a_i, \dots) + (b_0, b_1, b_2, \dots, b_i, \dots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_i + b_i, \dots) \end{aligned}$$

and

$$\begin{aligned} (a_0, a_1, a_2, \dots, a_i, \dots) \cdot (b_0, b_1, b_2, \dots, b_i, \dots) \\ = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots, a_0 b_i + a_1 b_{i-1} + a_{i-1} b_1 + a_i b_0, \dots) \end{aligned}$$

Theorem 2.1.3. *Let R be ring with identity and $a, b \in R$.*

- (a) $a^{n+m} = a^n a^m$ for all $n, m \in \mathbb{N}$.
- (b) If $ab = ba$, then $ab^n = b^n a$ for all $n \in \mathbb{N}$

Proof. (a) If $n = 0$, then $a^{n+m} = a^m = 1_R a^m = a^0 a^m$. So we may assume that $n > 0$. Similarly we may assume that $m > 0$. Then

$$a^n a^m = (\underbrace{aa \dots a}_{n\text{-times}}) (\underbrace{aa \dots a}_{m\text{-times}}) \stackrel{\text{GAL}}{=} \underbrace{aa \dots a}_{n+m\text{-times}} = a^{n+m}.$$

(b) Suppose that

$$(*) \quad ab = ba.$$

For $n = 0$ we have $ab^0 = a1_R = a = 1_R a = b^0 a$. Thus (b) holds. Suppose (b) holds for $n = k$. Then

$$(**) \quad ab^k = b^k a.$$

We compute

$$\begin{aligned} ab^{k+1} &= a(b^k b) && \text{-- definition of } b^{k+1} \\ &= (ab^k)b && \text{-- A x 7} \\ &= (b^k a)b && \text{-- (**)} \\ &= b^k(ab) && \text{-- A x 7} \\ &= b^k(ba) && \text{-- (*)} \\ &= (b^k b)a && \text{-- A x 7} \\ &= b^{k+1}a. && \text{-- definition of } b^{k+1} \end{aligned}$$

Thus (b) also holds for $n = k + 1$. So by the Principle Of Induction, (b) holds for all $n \in \mathbb{N}$. $\square$

Theorem 2.1.4. *Let R be a ring with identity and P a polynomial ring in x with coefficients in R . Then 1_R is an identity of P . In particular, $1_P = 1_R$ and $x = 1_R x$.*

Proof. To show that 1_R is an identity of P , let $f \in P$. Then by Condition (2.1.1)(iii) of a polynomial ring there exist $n \in \mathbb{N}$ and $f_0, f_1, \dots, f_n \in R$ with

$$(*) \quad f = \sum_{i=0}^n f_i x^i.$$

Let $1 \leq i \leq n$. By Condition (2.1.1)(ii) of an polynomial ring $1_R x = x 1_R$ and so by (2.1.3)(b)

$$(**) \quad 1_R x^i = x^i 1_R.$$

Thus

$$(* * *) \quad (f_i x^i) 1_R \stackrel{\mathbf{Ax} \mathbf{7}}{=} f_i (x^i 1_R) \stackrel{(**)}{=} f_i (1_R x^i) \stackrel{\mathbf{Ax} \mathbf{7}}{=} (f_i 1_R) x^i \stackrel{\mathbf{Ax} \mathbf{10} \text{ for } R}{=} f_i x^i$$

and

$$f 1_R \stackrel{(*)}{=} \left(\sum_{i=0}^n f_i x^i \right) 1_R \stackrel{\text{GDL}}{=} \sum_{i=0}^n (f_i x^i) 1_R \stackrel{(* * *)}{=} \sum_{i=0}^n f_i x^i \stackrel{(*)}{=} f.$$

Similarly,

$$1_R f \stackrel{(*)}{=} 1_R \left(\sum_{i=0}^n f_i x^i \right) \stackrel{\text{GDL}}{=} \sum_{i=0}^n 1_R (f_i x^i) \stackrel{\mathbf{Ax} \mathbf{7}}{=} \sum_{i=0}^n (1_R f_i) x^i \stackrel{\mathbf{Ax} \mathbf{10} \text{ for } R}{=} \sum_{i=0}^n f_i x^i \stackrel{(*)}{=} f.$$

and so 1_R is a multiplicative identity of P . Thus $1_R = 1_P$. Since $x \in P$ this gives $1_R x = 1_P x = x$. $\square$

Theorem 2.1.5. *Let P be a ring with identity, R a subring of P , $x \in P$ and $f, g \in P$. Suppose that*

- (i) $ax = xa$ for all $a \in R$;
- (ii) there exist $n \in \mathbb{N}$ and $f_0, \dots, f_n \in R$ with $f = \sum_{i=0}^n f_i x^i$; and
- (iii) there exist $m \in \mathbb{N}$ and $g_0, \dots, g_m \in R$ with $g = \sum_{i=0}^m g_i x^i$.

Put $f_i := 0_R$ for $i > n$ and $g_i := 0_R$ for $i > m$. Then

$$(a) \quad f + g = \sum_{i=0}^{\max(n,m)} (f_i + g_i) x^i.$$

$$(b) \quad -f = \sum_{i=0}^n (-f_i) x^i.$$

(c)

$$\begin{aligned} fg &= \sum_{i=0}^n \left(\sum_{j=0}^m f_i g_j x^{i+j} \right) = \sum_{k=0}^{n+m} \left(\sum_{i=\max(0, k-m)}^{\min(n, k)} f_i g_{k-i} \right) x^k = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k f_i g_{k-i} \right) x^k \\ &= f_n g_m x^{n+m} + (f_{n-1} g_m + f_n g_{m-1}) x^{n+m-1} + (f_{n-2} g_m + f_{n-1} g_{m-1} + f_n g_{m-2}) x^{n+m-2} + \dots \\ &\quad \dots + (f_0 g_2 + f_1 g_1 + f_2 g_0) x^2 + (f_0 g_1 + f_1 g_0) x + f_0 g_0. \end{aligned}$$

Proof. (a) Put $p := \max(n, m)$. Then $f_i = 0_R = 0_P$ for all $n < i \leq p$ and $g_i = 0_P$ for all $m < i \leq p$. Hence

$$(*) \quad f = \sum_{i=0}^p f_i x^i \quad \text{and} \quad g = \sum_{i=0}^p g_i x^i.$$

Thus

$$\begin{aligned} f + g &= \left(\sum_{i=0}^p f_i x^i \right) + \left(\sum_{i=0}^p g_i x^i \right) && -(*) \\ &= \sum_{i=0}^p (f_i x^i + g_i x^i) && -\text{GCL} \\ &= \sum_{i=0}^p (f_i + g_i) x^i && - \mathbf{Ax} \mathbf{8} \end{aligned}$$

So (a) holds.

(b) Using (a) we compute

$$f + \sum_{i=0}^n (-f_i) x^i = \sum_{i=0}^n (f_i + (-f_i)) x^i = \sum_{i=0}^n 0_P x^i = \sum_{i=0}^n 0_P = 0_P.$$

and so $-f = \sum_{i=0}^n (-f_i) x^i$ by the Additive Inverse Law.

(c) Let $a \in R$ and $b \in \mathbb{N}$. By hypothesis (i) we have $ax = xa$ and so by (2.1.3)(b)

$$(**) \quad ax^n = x^n a.$$

We compute fg :

$$\begin{aligned} fg &= \left(\sum_{i=0}^n f_i x^i \right) \cdot \left(\sum_{j=0}^m g_j x^j \right) && - \text{(ii) and (iii)} \\ &= \sum_{i=0}^n \left(\sum_{j=0}^m (f_i x^i)(g_j x^j) \right) && - \text{GDL} \\ &= \sum_{i=0}^n \left(\sum_{j=0}^m (f_i (x^i g_j)) x^j \right) && - \text{GAL} \\ &= \sum_{i=0}^n \left(\sum_{j=0}^m (f_i (g_j x^i)) x^j \right) && - x^i g_j = g_j x^i \text{ by } (**) \\ &= \sum_{i=0}^n \left(\sum_{j=0}^m (f_i g_j) (x^i x^j) \right) && - \text{GAL} \\ &= \sum_{i=0}^n \left(\sum_{j=0}^m (f_i g_j) x^{i+j} \right) && - x^i x^j = x^{i+j}, \text{ by (2.1.3)(a)} \end{aligned}$$

Let $i, j, k \in \mathbb{Z}$ with $k = i + j$. We will show that

$$(+ \quad) \quad 0 \leq i \leq n \text{ and } 0 \leq j \leq m \quad \Longleftrightarrow \quad 0 \leq k \leq n + m \text{ and } \max(0, k - m) \leq i \leq \min(k, n)$$

Suppose first that $0 \leq i \leq n$ and $0 \leq j \leq m$. Then $0 \leq k = i + j \leq n + m$. Since $j \leq m$ we have $m - j \geq 0$ and so $k - m = i + j - m = i - (m - j) \leq i$. Together with $0 \leq i$ this gives $\max(0, k - m) \leq i$. Since $j \geq 0$ we have $i \leq i + j = k$. Together with $i \leq n$ we get $i \leq \min(k, n)$.

Suppose next that $0 \leq k \leq n + m$ and $\max(0, k - m) \leq i \leq \min(k, n)$. Then $0 \leq i \leq n$. Since $i \leq k$ we get $0 \leq k - i = j$. As $k \leq n + m$ and $i \leq n$ we have $j = k - i \leq (n + m) - n \leq m$. We proved that $0 \leq i \leq n$ and $0 \leq j \leq m$, so $(***)$ holds.

Put

$$\begin{aligned} A &:= \{(i, j) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq i \leq n, 0 \leq j \leq m\} \\ B &:= \{(k, i) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq k \leq n + m, \max(0, k - m) \leq i \leq \min(k, n)\}. \end{aligned}$$

It follows that the function

$$A \rightarrow B, \quad (i, j) \mapsto (i + j, i)$$

is a bijection with inverse

$$B \rightarrow A, \quad (k, i) \mapsto (i, k - i).$$

Hence the substitution $k = i + j$ (and so $j = k - i$) and the GCL and GAL imply that

$$\begin{aligned} (++) \quad \sum_{i=0}^n \left(\sum_{j=0}^m f_i g_j x^{i+j} \right) &= \sum_{k=0}^{n+m} \left(\sum_{i=\max(0, k-m)}^{\min(k, n)} f_i g_{k-i} x^k \right) \\ &= \sum_{k=0}^{n+m} \left(\sum_{i=\max(0, k-m)}^{\min(k, n)} f_i g_{k-i} \right) x^k \quad \text{--GDL} \end{aligned}$$

Suppose $0 \leq i < \max(0, k - m)$. Then $i < k - m$, so $k - i > m$ and $g_{k-i} = 0_R$. Hence $f_i g_{k-i} = f_i 0_R = 0_R$ (by (1.2.9)(c)).

Suppose $\min(k, n) < i \leq k$. Then $\min(n, k) \neq k$ and so $\min(n, k) = n$. Hence $n < i$, so $f_i = 0_R$. Thus $f_i g_{k-i} = 0_R g_{k-i} = 0_R$. It follows that

$$\sum_{i=\max(0, k-m)}^{\min(k, n)} f_i g_{k-i} = \sum_{i=0}^k f_i g_{k-i}$$

and so

$$(+++) \quad \sum_{k=0}^{n+m} \left(\sum_{i=\max(0, k-m)}^{\min(k, n)} f_i g_{k-i} \right) x^k = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k f_i g_{k-i} \right) x^k.$$

Combining $(***)$, $(++)$ and $(+++)$ gives (c). □

Example 2.1.6. Let P be a polynomial ring in x with coefficients in $\mathbb{Z}_6$. Let

$$f = 1 + 2x + 3x^2 \quad \text{and} \quad g = 1 + 4x + 5x^2 + 2x^3.$$

Compute $f + g$ and $f \cdot g$ in P .

$$\begin{aligned} f + g &= 1 + 2x + 3x^2 \\ &\quad + 1 + 4x + 5x^2 + 2x^3 \\ &= 2 + 6x + 8x^2 + 2x^3 \\ &= 2 \quad + 2x^2 + 2x^3. \end{aligned}$$

$$\begin{aligned} fg &= (1 + 2x + 3x^2)(1 + 4x + 5x^2 + 2x^3) \\ &= (1 \cdot 1) + (1 \cdot 4 + 2 \cdot 1)x + (1 \cdot 5 + 2 \cdot 4 + 3 \cdot 1)x^2 \\ &\quad + (1 \cdot 2 + 2 \cdot 5 + 3 \cdot 4)x^3 + (2 \cdot 2 + 3 \cdot 5)x^4 + (3 \cdot 2)x^5 \\ &= 1 + 6x + 16x^2 + 24x^3 + 19x^4 + 6x^5 \\ &= 1 \quad + 4x^2 \quad + x^4. \end{aligned}$$

Exercises 2.1:

2.1#1. Let P be a polynomial ring in x with coefficients in R . Perform the indicated operation in P and simplify your answer:

(a) $(3x^4 + 2x^3 - 4x^2 + x + 4) + (4x^3 + x^2 + 4x + 3)$ if $R = \mathbb{Z}_5$.

(b) $(x + 1)^3$ if $R = \mathbb{Z}_3$

(c) $(x - 1)^5$ if $R = \mathbb{Z}_5$.

(d) $(x^2 - 3x + 2)(2x^3 - 4x + 1)$ if $R = \mathbb{Z}_7$.

(e) $\left(x + \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right) \left(x - \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right)$ if $R = M_2(\mathbb{R})$.

2.1#2. For $b \in \mathbb{R}$ define

$$\mathbb{Q}[b] := \{a_0 + a_1b + a_2b^2 + \dots + a_nb^n \mid n \in \mathbb{N}, a_0, a_1, \dots, a_n \in \mathbb{Q}\}.$$

Given that (for each $b \in \mathbb{R}$) $\mathbb{Q}[b]$ is a subring of $\mathbb{R}$.

(a) Is $\mathbb{Q}[\sqrt{2}]$ a polynomial ring in $\sqrt{2}$ with coefficients in $\mathbb{Q}$?

(b) Is $\mathbb{Q}[\pi]$ a polynomial ring in π with coefficients in $\mathbb{Q}$? (You don't need to justify your answer for (b).)

2.2 The degree of a polynomial

Definition 2.2.1. Let R be a ring with identity.

- (a) $R[x]$ denotes a polynomial ring in x with coefficients in R .
- (b) Let $f \in R[x]$ and let $n \in \mathbb{N}$ and $a_0, a_1, \dots, a_n \in R$ with $f = \sum_{i=0}^n a_i x^i$. Let $i \in \mathbb{N}$. If $i \leq n$ define $f_i = a_i$. If $i > n$ define $f_i = 0_R$. Then f_i is called the coefficient of x^i in f . (Observe that this is well defined by 2.1.1)
- (c) $\mathbb{N}^* := \mathbb{N} \cup \{-\infty\}$. For $n \in \mathbb{N}^*$ we define $n + (-\infty) = -\infty$ and $-\infty + n = -\infty$. We extend the relation ' $\leq$ ' on $\mathbb{N}$ to $\mathbb{N}^*$ via $-\infty \leq n$ for all $n \in \mathbb{N}^*$.
- (d) Let $f \in R[x]$. If $f = 0_R$ define $\deg f := -\infty$ and $\text{lead}(f) = 0_R$. If $f = \sum_{i=0}^n f_i x^i$ with $f_i \in R$ and $f_n \neq 0$, define $\deg f := n$ and $\text{lead}(f) = f_n$.
- (e) A polynomial $f \in R[x]$ is called constant if $f \in R$.

Theorem 2.2.2. Let R be a ring with identity and $f \in R[x]$.

- (a) $f = 0_R$ if and only if $\deg f = -\infty$ and if and only if $\text{lead}(f) = 0_R$.
- (b) $\deg f = 0$ if and only if $f \in R$ and $f \neq 0_R$.
- (c) f is a constant polynomial if and only if $f \in R$ if and only if $\deg f \leq 0$ and if and only if $f = \text{lead}(f)$.
- (d) $f = \sum_{i=0}^{\deg f} f_i x^i$. Recall here that, for $f = 0_R$, the empty sum $\sum_{i=0}^{-\infty} f_i x^i$ is defined to be 0_R .

Proof. This follows directly from the definitions of $\deg f$, $\text{lead} f$ and f_i . □

Theorem 2.2.3. Let R be a ring with identity and $f, g \in R[x]$. Then

- (a) $\deg(f + g) \leq \max(\deg f, \deg g)$.
- (b) $\deg(-f) = \deg f$.
- (c) Exactly one of the following holds:
 - (1) $\deg(fg) = \deg f + \deg g$ and $\text{lead}(fg) = \text{lead}(f)\text{lead}(g)$.
 - (2) $\deg(fg) < \deg f + \deg g$, $\text{lead}(f)\text{lead}(g) = 0_R$, $f \neq 0_R$ and $g \neq 0_R$.

In particular, $\deg fg \leq \deg f + \deg g$.

Proof. Put $n := \deg f$ and $m := \deg g$. By (2.2.2)(d) we have

$$f = \sum_{i=0}^n f_i x^i \quad \text{and} \quad g = \sum_{i=0}^m g_i x^i.$$

(a) By (2.1.5)(a), $f + g = \sum_{i=0}^{\max(n,m)} (f_i + g_i)x^i$ and so $(f + g)_k = 0_R$ for $k > \max(\deg f, \deg g)$. Thus (a) holds.

(b) If $f = 0_R$, then $-f = -0_R = 0_R$ and so $\deg f = -\infty = \deg(-f)$. Suppose $f \neq 0_R$. Then $f_n \neq 0_R$ and so also $-f_n \neq 0_R$. Also by (2.1.5)(b) $-f = -(\sum_{i=0}^n f_i x^i) = \sum_{i=0}^n (-f_i)x^i$. Since $-f_n \neq 0_R$ this gives $\deg(-f) = n = \deg f$.

(c) Suppose first that $f = 0_R$. Then $fg = 0_R g = 0_R$. Hence $\deg f = -\infty$, $\deg(fg) = -\infty$, $\text{lead} f = 0_R$ and $\text{lead}(fg) = 0_R$. Thus

$$\deg(fg) = -\infty = -\infty + \deg g = \deg f + \deg g \text{ and } \text{lead}(fg) = 0_R = 0_R \cdot \text{lead}(g) = \text{lead}(f)\text{lead}(g).$$

So (c:1) holds in this case. Similarly, (c:1) holds if $g = 0_R$.

So suppose $f \neq 0_R \neq g$. By (2.1.5)(c),

$$fg = f_n g_m x^{n+m} + (f_{n-1} g_m + f_n g_{m-1})x^{n+m-1} + \dots +$$

Note that $f_n = \text{lead}(f)$ and $g_m = \text{lead}(g)$. Suppose that $f_n g_m \neq 0_R$. Then $\deg(f + g) = n + m$ and $\text{lead}(fg) = f_n g_m = \text{lead}(f)\text{lead}(g)$. Thus (c:1) holds.

Suppose that $f_n g_m = 0$. Then $\deg(f + g) < n + m$ and $\text{lead}(f)\text{lead}(g) = f_n g_m = 0_R$. Thus (c:2) holds. $\square$

Theorem 2.2.4. *Let R be a commutative ring with identity. Then $R[x]$ is commutative ring with identity 1_R .*

Proof. By 2.1.4 $R[x]$ is a ring with identity 1_R . So we just need to show that $R[x]$ is commutative. Let $f, g \in R[x]$ and put $n := \deg f$ and $m := \deg g$. Then

$$\begin{aligned} fg &= \left(\sum_{i=0}^n f_i x^i \right) \left(\sum_{j=0}^m g_j x^j \right) && \text{-(2.2.2)(d)} \\ &= \sum_{i=0}^n \sum_{j=0}^m f_i g_j x^{i+j} && \text{-(2.1.5)(c)} \\ &= \sum_{i=0}^n \sum_{j=0}^m g_j f_i x^{j+i} && \text{- } R \text{ is commutative} \\ &= \sum_{j=0}^m \sum_{i=0}^n g_j f_i x^{j+i} && \text{- GCL} \\ &= \left(\sum_{j=0}^m g_j x^j \right) \left(\sum_{i=0}^n f_i x^i \right) && \text{-(2.1.5)(c)} \\ &= gf && \text{-(2.2.2)(d)} \end{aligned}$$

We proved that $fg = gf$ for all $f, g \in R[x]$ and so $R[x]$ is commutative. $\square$

Theorem 2.2.5. *Let R be field or an integral domain. Then*

(a) $\deg(fg) = \deg f + \deg g$ and $\text{lead}(fg) = \text{lead}(f)\text{lead}(g)$ for all $f, g \in R[x]$.

- (b) $\deg(fr) = \deg f$ and $\text{lead}(fr) = r \text{lead}(f)$ for all $f \in R[x]$ and $r \in R$ with $r \neq 0_R$.
- (c) $R[x]$ is an integral domain.

Proof. By Theorem 1.8.10 any field is an integral domain. So in any case R is an integral domain. Let $f, g \in R[x]$. We will first show that

(*) If $\text{lead}(f)\text{lead}(g) = 0_R$ then $f = 0_R$ or $g = 0_R$.

Suppose that $\text{lead}(f)\text{lead}(g) = 0_R$. Since R is an integral domain we get $\text{lead}(f) = 0_R$ or $\text{lead}(g) = 0_R$. Now 2.2.2 shows $f = 0_R$ or $g = 0_R$.

(a) By (2.2.3)(c) we have

- (1) $\deg(fg) = \deg f + \deg g$ and $\text{lead}(fg) = \text{lead}(f)\text{lead}(g)$, or
- (2) $\deg(fg) < \deg f + \deg g$, $\text{lead}(f)\text{lead}(g) = 0_R$, $f \neq 0_R$ and $g \neq 0_R$.

In the first case, (a) holds. The second case contradicts (*) and so does not occur.

(b) Let $r \in R$ with $r \neq 0_R$. By 2.2.2 $\deg(r) = 0$ and $\text{lead}(r) = r$. Using (b) we conclude that

$$\deg(fr) = \deg f + \deg r = \deg f + 0 = \deg f \quad \text{and} \quad \text{lead}(fr) = \text{lead}(f)\text{lead}(r) = \text{lead}(f)r.$$

(c) Since R is a integral domain, R is a commutative ring with identity $1_R \neq 0_R$. So by 2.2.4, $R[x]$ is a commutative ring with identity. Since R is an integral domain $1_R \neq 0_R$ and thus

$$1_{R[x]} \stackrel{2.1.4}{=} 1_R \neq 0_R \stackrel{1.7.2}{=} 0_{R[x]}.$$

Let $fg \in R[x]$ with $fg = 0_R$. Then by (a) $\text{lead}(f)\text{lead}(g) = \text{lead}(fg) = \text{lead}(0_R) = 0_R$ and by (*), $f = 0_R$ or $g = 0_R$. Hence $R[x]$ is an integral domain. $\square$

Exercises 2.2:

2.2#1. Let R be a ring with identity and suppose that $1_R \neq 0_R$. Which of the following subsets of $R[x]$ are subrings of $R[x]$? (You don't need to justify your answer).

- (a) $\{f \in R[x] \mid f_0 = 0_R\}$.
- (b) $\{f \in R[x] \mid \deg f = 2\}$.
- (c) $\{f \in R[x] \mid \deg f \leq k\}$, where k is a fixed positive integer.
- (d) $\{f \in R[x] \mid f_{2n+1} = 0_R \text{ for all } n \in \mathbb{N}\}$.
- (e) $\{f \in R[x] \mid f_{2n} = 0_R \text{ for all } n \in \mathbb{N}\}$.

2.2#2. Let R be a ring with identity. An element $r \in R$ is called a *zero-divisor* in R if $r \neq 0_R$ and there exists $s \in R$ with $s \neq 0_R$ and $rs = 0_R$.

Let $f \in R[x]$. Prove or give a counter example:

- (a) If f is a zero-divisor in $R[x]$, then $\text{lead}(f)$ is a zero-divisor in R .
- (b) If $\text{lead}(f)$ is a zero-divisor in $R[x]$, then f is a zero-divisor in $R[x]$.

2.2#3. Which of the following rings are integral domains?

- (a) $\mathbb{Z}_2[x]$
- (b) $\mathbb{Z}_4[x]$
- (c) $M_2(\mathbb{R})[x]$.
- (d) $\mathbb{Z}[x]$

2.3 Divisibility in $F[x]$

In a general ring it may or may not be easy to decide whether a given element divides another. But for polynomial over a field it is easy, thanks to the division algorithm:

Theorem 2.3.1 (Division Algorithm). *Let R be a ring with identity $1_R \neq 0_R$ and $f, g \in R[x]$ such that $\text{lead}(g)$ is a unit of R . Then there exist uniquely determined $q, r \in R[x]$ with*

$$f = gq + r \quad \text{and} \quad \deg r < \deg g.$$

Proof. Fix $g \in R[x]$ such that $g \neq 0_R$ and $\text{lead}(g)$ is unit in R and let $f \in R[x]$.

Existence of q and r :

Put $m := \deg g$. We will first show

(*) $g \neq 0_R$. In particular, $m = \deg g \geq 0$, $m \in \mathbb{N}$ and $g_m = \text{lead}(g) \neq 0_R$.

Note that $0_R r = 0_R \neq 1_R$ for all $r \in R$ and so 0_R is not a unit in R . As $\text{lead}(g)$ is a unit this implies that $\text{lead}(g) \neq 0_R$. Hence $g \neq 0_R$ and (*) is proved.

For $n \in \mathbb{N}$ consider the statement

$P(n)$: If $f \in R[x]$ with $\deg f < n$, then there exist $q, r \in R[x]$ with

(**) $f = gq + r \quad \text{and} \quad \deg r < \deg g$

We will first treat a special case:

(***) If $\deg f < \deg g$, then (**) holds with $q = 0_R$ and $r = f$

Indeed, this follows from $f = q \cdot 0_R + f$.

In general we will use induction to show that $P(n)$ holds for all $n \in \mathbb{N}$.

To show that $P(0)$ holds, let $f \in R[x]$ with $\deg f < 0$. By (*) $0 \leq \deg g$ and so $\deg f < \deg g$. Now (***) shows that $P(0)$ holds.

Suppose inductively that $P(k)$ holds for some $k \in \mathbb{N}$. To show that $P(k+1)$ holds, let $f \in R[x]$ with $\deg f < k+1$. Then $\deg f \leq k$ and we need to show that $(**)$ holds for some $q, r \in R[x]$. If $\deg g > k$, then $\deg f < \deg g$ and we are done by $(***)$.

Hence we may suppose $\deg g \leq k$. By $(*)$ $m \in \mathbb{N}$ and $g_m = \text{lead}(g)$. hypothesis $\text{lead}(g)$ is a unit in R and so g_m has an inverse g_m^{-1} . Define

$$(+) \quad \tilde{f} := f - g \cdot g_m^{-1} f_k x^{k-m}.$$

We compute

$$\begin{array}{rcll} f : & f_k x^k & + & f_{k-1} x^{k-1} + \dots + \\ g : & g_m x^m & + & g_{m-1} x^{m-1} + \dots + \\ g \cdot g_m^{-1} f_k x^{k-m} : & g_m g_m^{-1} f_k x^k & + & g_{m-1} g_m^{-1} f_k x^{k-1} + \dots + \\ & = & & f_k x^k + g_{m-1} g_m^{-1} f_k x^{k-1} + \dots + \\ \tilde{f} = f - g \cdot g_m^{-1} f_k x^{k-m} : & & & (f_{k-1} - g_{m-1} g_m^{-1} f_k) x^{k-1} + \dots + \end{array}$$

The above calculation shows that $\deg \tilde{f} < k$. By the induction assumption, $P(k)$ -holds. So there exist $\tilde{q}$ and $\tilde{r} \in R[x]$ with

$$(++) \quad \tilde{f} = g\tilde{q} + \tilde{r} \quad \text{and} \quad \deg \tilde{r} < \deg g.$$

We compute

$$\begin{aligned} f &= \tilde{f} + g \cdot g_m^{-1} f_k x^{k-m} && - (+), 1.2.8 \\ &= (g\tilde{q} + \tilde{r}) + g \cdot g_m^{-1} f_k x^{k-m} && - (++) \\ &= (g\tilde{q} + g \cdot g_m^{-1} f_k x^{k-m}) + \tilde{r} && - \text{GCL} \\ &= g \cdot (\tilde{q} + g_m^{-1} f_k x^{k-m}) + \tilde{r} && - \mathbf{Ax 8} \end{aligned}$$

Put $q := \tilde{q} + g_m^{-1} f_k x^{k-m}$ and $r := \tilde{r}$. Then by $(+++)$ $f = gq + r$ and by $(++)$, $\deg r = \deg \tilde{r} < \deg g$. Thus $(**)$ holds and $P(k)$ is proved.

By the Principal of Induction A.5.2 we conclude that $P(n)$ holds for all $n \in \mathbb{N}$. This shows the existence of q and r .

To show uniqueness, let $q_i, r_i \in R[x]$ for $i = 1, 2$ such that

$$(\#) \quad f = gq_i + r_i \quad \text{and} \quad \deg r_i < \deg g.$$

Then

$$gq_1 + r_1 = gq_2 + r_2$$

and so

$$(\#\#) \quad g \cdot (q_1 - q_2) = r_2 - r_1.$$

Suppose $q_1 - q_2 \neq 0_R$. Then $\deg(q_1 - q_2) \geq 0$ and $\text{lead}(q_1 - q_2) \neq 0_R$. Since $\text{lead}(g)$ is a unit in R this implies $\text{lead}(g)\text{lead}(q_1 - q_2) \neq 0_R$, see Exercise 1.8#9 (Exercise 5 on Homework 8). Thus

$$\begin{aligned} \deg g &\leq \deg g + \deg(q_1 - q_2) && - \deg(q_1 - q_2) \geq 0 \\ &= \deg(g \cdot (q_1 - q_2)) && - \text{lead}(g)\text{lead}(q_1 - q_2) \neq 0_R, (2.2.3)(c:1) \\ &= \deg(r_2 - r_1) && - (\#\#) \\ &\leq \max(\deg r_1, \deg r_2) && - 2.2.3 \\ &< \deg g && - (\#) \end{aligned}$$

This contradiction shows $q_1 - q_2 = 0_R$. Hence, $r_2 - r_1 \stackrel{(\#\#)}{=} g \cdot (q_1 - q_2) = g \cdot 0_R = 0_R$. Thus $q_1 = q_2$ and $r_1 = r_2$, see (1.2.9)(f). $\square$

Definition 2.3.2. Let R be a ring with identity $1_R \neq 0_R$ and $f, g \in R[x]$ such that $\text{lead}(g)$ is a unit in R . Let $q, r \in R[x]$ be the unique polynomials with

$$f = gq + r \quad \text{and} \quad \deg r < \deg g$$

Then r is called the remainder of f when divided by g in $R[x]$.

Example 2.3.3. Consider the polynomials $f = x^4 + x^3 - x + 1$ and $g = -x^2 + x - 1$ in $\mathbb{Z}_3[x]$. Compute the remainder of f when divided by g .

$$\begin{array}{rcl} & & \begin{array}{ccccccc} -x^2 & + & x & - & 1 & & \\ \hline x^4 & + & x^3 & & & - & x & + & 1 \\ x^4 & - & x^3 & + & x^2 & & & & \end{array} & | \quad g \cdot (-x^2) \\ \hline & & \begin{array}{ccccccc} 2x^3 & - & x^2 & - & x & + & 1 \\ \hline - & x^3 & - & x^2 & - & x & + & 1 \\ - & x^3 & + & x^2 & - & x & & & \end{array} & | \quad \begin{array}{l} \text{in } \mathbb{Z}_3[x] \\ g \cdot x \end{array} \\ \hline & & \begin{array}{ccccccc} & & - & 2x^2 & & + & 1 \\ \hline & & & x^2 & & + & 1 \\ & & & x^2 & - & x & + & 1 \\ \hline & & & & & & x \end{array} & | \quad \begin{array}{l} \text{in } \mathbb{Z}_3[x] \\ g \cdot 1 \end{array} \end{array}$$

Thus

$$x^4 + x^3 - x + 1 = (-x^2 + x - 1) \cdot (-x^2 + x - 1) + x.$$

Since $\deg x = 1 < 2 = \deg(-x^2 + x - 1)$, the remainder of $x^4 + x^3 - x + 1$ when divided by $-x^2 + x - 1$ in $\mathbb{Z}_3[x]$ is x .

Theorem 2.3.4. *Let R be a ring with identity $1_R \neq 0_R$ and $f, g \in R[x]$ such that $\text{lead}(g)$ is a unit in R . Then g divides f in $R[x]$ if and only if the remainder of f when divided by g in $R[x]$ is 0_R .*

Proof. Note first that since $\text{lead}(g)$ is a unit in R the remainder of f when divided by g is defined.

$\implies$: Suppose that $g \mid f$. Then by Definition 1.4.1 $f = gq$ for some $q \in R[x]$. Thus $f = gq + 0_R$. Since $\deg 0_R = -\infty < \deg g$, Definition 2.3.2 shows that 0_R is the remainder of f when divided by g .

$\impliedby$: Suppose that the remainder of f when divided by g is 0_R . Then by Definition 2.3.2 $f = gq + 0_R$ for some $q \in R[x]$. Thus $f = gq$ and so Definition 1.4.1 shows that $g \mid f$. $\square$

Theorem 2.3.5. *Let R be a field or an integral domain and $f, g \in R[x]$. If $g \neq 0_R$ and $f \mid g$, then $\deg f \leq \deg g$.*

Proof. Since $f \mid g$, there exists $h \in R[x]$ with $g = fh$. If $h = 0_R$, then by (1.2.9)(c), $g = fh = f0_R = 0_R$, contrary to the assumption. Thus $h \neq 0_R$ and so $\deg h \geq 0$. Since R is a field or an integral domain we can apply (2.2.5)(a) and conclude

$$\deg g = \deg fh = \deg f + \deg h \geq \deg f.$$

$\square$

Theorem 2.3.6. *Let F be a field and $f \in F[x]$. Then the following statements are equivalent:*

- (a) $\deg f = 0$.
- (b) $f \in F$ and $f \neq 0_F$.
- (c) $f \mid 1_F$ in $F[x]$.
- (d) $f \sim 1_F$.
- (e) f is a unit in $F[x]$.

Proof. (a) $\implies$ (b): See (2.2.2)(b).

(b) $\implies$ (c): Suppose that $f \in F$ and $f \neq 0_F$. Since F is a field, **Ax 12** holds and so f is a unit in F . Hence f has an inverse f^{-1} in F . So $ff^{-1} = 1_F$ and since $f^{-1} \in F \subseteq F[x]$ we conclude that $f \mid 1_F$ in $F[x]$.

(c) $\implies$ (d): and (d) $\implies$ (e): See 1.12.7.

(e) $\implies$ (a): Since f is a unit, there exists $g \in F[x]$ with $1_F = fg$. Since F is a field we know that $1_F \neq 0_F$. As $1_F \in F$ this gives $\deg(1_F) = 0$ (see (2.2.2)(b)). Since F is a field we conclude from (2.2.5)(a) that

$$\deg f + \deg g = \deg(fg) = \deg(1_F) = 0,$$

and so also $\deg f = \deg g = 0$. $\square$

Theorem 2.3.7. *Let F be a field and $f, g \in F[x]$. Then the following statements are equivalent:*

- (a) $f \sim g$.
- (b) $f|g$ and $g|f$.
- (c) $\deg f = \deg g$ and $f|g$.
- (d) $g = fu$ for some non-zero $u \in F$.
- (e) $g \sim f$.

Proof. (a) $\implies$ (b): See 1.12.8.

(b) $\implies$ (c): Suppose that $f|g$ and $g|f$. We need to show that $\deg f = \deg g$. Assume first that $g = 0_F$, then since $g|f$, we get from 1.4.3 that $f = 0_F$. Hence $f = 0_F = g$ and so also $\deg f = \deg g$. Thus (c) holds. Similarly, (c) holds if $f = 0_F$.

Assume that $f \neq 0_F$ and $g \neq 0_F$. Since $f|g$ and $g|f$ we conclude from 2.3.5 that $\deg f \leq \deg g$ and $\deg g \leq \deg f$. Thus $\deg g = \deg f$ and (c) holds.

(c) $\implies$ (d): Suppose that $\deg f = \deg g$ and $f|g$. If $f = 0_F$, then $\deg g = \deg f = -\infty$ and so $g = 0_F$. Hence $f = g$ and so $f \sim g$ since $\sim$ is an equivalence relation and so reflexive, see 1.12.4.

Thus we may assume $f \neq 0_F$. Since $f|g$ we have $g = fu$ for some $u \in F[x]$. Thus by (2.2.5)(a), $\deg g = \deg f + \deg u$. As $\deg f = \deg g$ this gives $\deg f = \deg f + \deg u$. Since $f \neq 0_F$ we have $\deg f \in \mathbb{N}$ and we conclude that $\deg u = 0$. Thus by 2.3.6, $u \in F$ and $u \neq 0_F$.

(d) $\implies$ (e): Suppose $g = fu$ for some $u \in F$ with $u \neq 0_F$. 2.3.6, u is a unit in $F[x]$. As $g = fu$ this shows that $g \sim f$ by definition of $\sim$.

(e) $\implies$ (a): This holds since $\sim$ is symmetric by 1.12.4. □

Definition 2.3.8. Let F be a field and $f \in F[x]$.

- (a) f is called *monic* if $\text{lead}(f) = 1_F$.
- (b) Suppose that $f \neq 0_F$. Then $\check{f} := f \cdot \text{lead}(f)^{-1}$. (Note here that $\text{lead}(f) \neq 0_F$ and so $\text{lead}(f)$ is a unit in F since F is a field). $\check{f}$ is called the *monic polynomial associated to f* .
- (c) Suppose that $f = 0_F$. Then $\check{f} := 0_F$.

Example 2.3.9. Let $f = 3x^4 + 2x^3 + 4x^2 + x + 2 \in \mathbb{Z}_5[x]$. Then $\text{lead}(f)^{-1} = 3^{-1} = 1 \cdot 3^{-1} = 6 \cdot 3^{-1} = 2$ and

$$\check{f} = (3x^4 + 2x^3 + 4x^2 + x + 2) \cdot 2 = 6x^4 + 4x^3 + 8x^2 + 2x + 4 = x^4 + 4x^3 + 3x^2 + 2x + 4.$$

Theorem 2.3.10. Let F be a field and $f, g \in F[x]$.

- (a) $f = \check{f} \cdot \text{lead}(f)$ and $f \sim \check{f}$.
- (b) If f and g are monic and $f \sim g$, then $f = g$.
- (c) If $f \neq 0_F$, then $\check{f}$ is the unique monic polynomial associated to f .
- (d) $\deg \check{f} = \deg f$.

(e) $f \sim g$ if and only if $\check{f} = \check{g}$.

Proof. Recall from 1.12.4 that $\sim$ is an equivalence relation and so reflexive, symmetric and transitive.

(a) Suppose that $f = 0_F$. Then $\check{f} = 0_F$ and so $\check{f} \cdot \text{lead}(f) = 0_F \cdot \text{lead}(f) = 0_F = f$. Also $\check{f} = 0_F = f$ and so $f \sim \check{f}$ as $\sim$ is reflexive.

Suppose that $f \neq 0_F$. Then $\check{f} \cdot \text{lead}(f) = (f \cdot \text{lead}(f)^{-1}) \cdot \text{lead}(f) = f$. As $\text{lead}(f)$ is a unit in F and so also in $F[x]$, this shows that $f \sim \check{f}$.

(b) By definition of $f \sim g$ we have $fu = g$ for some unit u in $F[x]$. Thus 2.3.6 implies $0_F \neq u \in F$. Hence

$$1_F \stackrel{g \text{ monic}}{=} \text{lead}(g) \stackrel{fu=g}{=} \text{lead}(fu) \stackrel{u \in F, (2.2.5)(b)}{=} \text{lead}(f)u \stackrel{f \text{ monic}}{=} 1_F u \stackrel{\mathbf{Ax 10}}{=} u$$

and so $u = 1_F$. Therefore $g = fu = f1_F = f$.

(c) Suppose $f \neq 0_F$. Then

$$\text{lead}(\check{f}) = \text{lead}(f \cdot \text{lead}(f)^{-1}) \stackrel{(2.2.5)(b)}{=} \text{lead}(f)\text{lead}(f)^{-1} = 1_F.$$

So $\check{f}$ is monic. By (a) we have $f \sim \check{f}$ and so $\check{f}$ is a monic polynomial associated to f .

Suppose g is a monic polynomial with $f \sim g$. By (a) $f \sim \check{f}$. As $\sim$ is symmetric and transitive this gives $\check{f} \sim f$ and $\check{f} \sim g$. Since both $\check{f}$ and g are monic we conclude from (b) that $\check{f} = g$.

(d) By (a) $f \sim \check{f}$ and so by 2.3.7 $\deg f = \deg \check{f}$.

(e) Suppose first that $f = 0_F$. Then also $\check{f} = 0$. Hence

$$f \sim g \iff 0_F \sim g \iff g = 0_F \iff \check{g} = 0_F \iff 0_F \sim \check{g} \iff \check{f} \sim \check{g}.$$

So we may assume that $f \neq 0_F$ and similarly, $g \neq 0_F$. Then both $\check{f}$ and $\check{g}$ are monic. By (a) $f \sim \check{f}$ and $g \sim \check{g}$. Thus by A.6.5

$$(*) \quad [f]_{\sim} = [\check{f}]_{\sim} \quad \text{and} \quad [g]_{\sim} = [\check{g}]_{\sim}.$$

Using this we get

$$\begin{aligned} f &\sim g \\ \iff [f]_{\sim} &= [g]_{\sim} && - \text{A.6.5} \\ \iff [\check{f}]_{\sim} &= [\check{g}]_{\sim} && - (*) \\ \iff \check{f} &\sim \check{g} && - \text{A.6.5} \\ \iff \check{f} &= \check{g} && - (c) \end{aligned}$$

□

Exercises 2.3:

2.3#1. Let R be a ring with identity and $f, g \in R[x]$. Find polynomials q and r in $R[x]$ such that $f = gq + r$ and $\deg r < \deg g$, if

- (a) $R = \mathbb{Q}$, $f = 3x^4 - 2x^3 + 6x^2 - x + 2$ and $g = x^2 + x + 1$;
- (b) $R = \mathbb{Q}$, $f = x^4 - 7x + 1$ and $g = 2x^2 + 1$;
- (c) $R = \mathbb{Z}_5$, $f = 2x^4 + x^2 - x + 1$ and $g = 2x - 1$;
- (d) $R = \mathbb{Z}_7$, $f = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $g = 3x^2 + 2$.

(e) $R = M_2(\mathbb{R})$, $f = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} x^4 + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} x^3 + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} x^2 + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and

$$g = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} x^2 + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

2.3#2. Let R be an integral domain and suppose that for all $f, g \in R[x]$ with $g \neq 0_R$ there exist $q, r \in R[x]$ with $f = gq + r$ and $\deg r < \deg g$. Prove that R is a field. *Hint:* Let $a \in R$ with $a \neq 0_R$. Consider $f = 1_R$ and $g = a$.

2.3#3. Consider $f := 1$ and $g := 2$ in $\mathbb{Z}[x]$. Do there exist $q, r \in \mathbb{Z}[x]$ with

$$f = gq + r \quad \text{and} \quad \deg(r) < \deg(g)?$$

2.3#4. Let F be a field and $f \in F[x]$. Compute $\check{f}$ (see 2.3.8) if

- (a) $f = 3x^3 + 4x^2 + 5x + 1$ and $F = \mathbb{Q}$;
- (b) $f = 4x^5 + 6x^3 + 5x^2 + 2x + 3$ and $F = \mathbb{Z}_7$;
- (c) $f = 6x^3 + 9x^2 + 15x + 3$ and $F = \mathbb{Z}_3$.

2.4 The Euclidean Algorithm for Polynomials

Definition 2.4.1. Let F be a field and $f, g, d \in F[x]$. We say that d is a greatest common divisor of f and g and write

$$d = \gcd(f, g)$$

provided that

- (i) d is a common divisor of f and g ;
- (ii) if c is a common divisor of f and g , then $\deg c \leq \deg d$; and

(iii) d is monic.

Example 2.4.2. Let F be a field and $f \in F[x]$. Find a greatest common divisor of f and 0_F .

If $f = 0_f$, then x^n divides f and 0_F for all $n \in \mathbb{N}$. So there does not exist a greatest common divisor of 0_F and 0_F .

Suppose $f \neq 0_F$. We claim that $\tilde{f} = \gcd(f, 0_F)$. Observe that $\tilde{f}$ is a common divisor of f and 0_F . Also if c is any common divisor of f and 0_F , then $c|f$ and so by 2.3.5 $\deg c \leq \deg f = \deg \tilde{f}$. Thus $\tilde{f}$ fulfills all three conditions of the ‘gcd’.

Theorem 2.4.3. Let F be a field and $f, g, d \in F[x]$ in $F[x]$ with $d = \gcd(f, g)$.

(a) Suppose that $q, r \in F[x]$ with $f \sim gq + r$, Then $d = \gcd(g, r)$.

(b) Suppose that $\tilde{f}, \tilde{g} \in F[x]$ with $\tilde{f} \sim f$ and $\tilde{g} \sim g$. Then $d = \gcd(\tilde{f}, \tilde{g})$.

Proof. (a): Put $\tilde{f} := gq + r$. Then $\tilde{f} \sim f$ by the hypothesis of (a). We will now verify that d fulfills the three conditions on $d = \gcd(g, r)$.

(i): Since $d = \gcd(f, g)$, the definition of the greatest common divisor shows that $d|f$ and $d|g$. As $f \sim \tilde{f}$ we conclude from 1.12.8 that $d|\tilde{f}$. Since $\tilde{f} = gq + r$ we have $r = \tilde{f} - gq$. As $d|\tilde{f}$ and $d|g$, (1.4.4)(c) shows that $d|r$. Hence d is a common divisor of g and r .

(ii): Let c be any common divisor of g and r in $F[x]$. As $\tilde{f} = gq + r$, (1.4.4)(c) shows that $c|\tilde{f}$. As $f \sim \tilde{f}$, 1.12.8 gives $c|f$. Thus c is a common divisor of f and g . As $d = \gcd(f, g)$ this gives $\deg c \leq \deg d$.

(iii): Since $d = \gcd(f, g)$ the definition of ‘gcd’ shows that d is monic.

Thus d is a greatest common divisor of g and r .

(b): Note that $f \sim \tilde{f}$ and $\tilde{f} = g \cdot 0_F + \tilde{f}$. So $f \sim g \cdot 0_F + \tilde{f}$ and (a) shows that $d = \gcd(g, \tilde{f})$. We proved that

$$d = \gcd(f, g) \implies d = \gcd(g, \tilde{f}).$$

This result with $(g, \tilde{f})$ in place of (f, g) gives

$$d = \gcd(g, \tilde{f}) \implies d = \gcd(\tilde{f}, \tilde{g}).$$

So (b) holds. □

Theorem 2.4.4 (Euclidean Algorithm). Let F be a field and $f, g \in F[x]$ not both 0_F . Define $m \in \mathbb{N}$ and equations

$$\begin{aligned} E_k &: r_k = a \cdot u_k + b \cdot x_k & 0 \leq k \leq m \\ F_k &: s_k = a \cdot v_k + b \cdot y_k & 0 \leq k \leq m \\ G_k &: t_k = a \cdot w_k + b \cdot z_k & 1 \leq k < m \end{aligned}$$

as follows:

- (•) If E_k has been defined for some $k \in \mathbb{N}$, put $\epsilon_k = \begin{cases} \text{lead}(r_k)^{-1} & \text{if } r_k \neq 0_F \\ 1_F & \text{if } r_k = 0_F \end{cases}$ and let F_k be the equation obtained by multiplying E_k with ϵ_k :

$$F_k := E_k \cdot \epsilon_k$$

(•)

$$\begin{aligned} E_0 &: a = a \cdot 1_F + b \cdot 0_F \\ E_1 &: b = a \cdot 0_F + b \cdot 1_F \end{aligned}$$

Suppose now that $i \in \mathbb{N}$ with $i \geq 1$ and E_k has been defined for all $0 \leq k \leq i$.

- (•) If $s_i = 0_F$, put $m = i$ and the Algorithm stops.
- (•) Suppose $s_i \neq 0_F$. Let $q_i \in F[x]$ such that $\deg(s_{i-1} - s_i q_i) < \deg(s_i)$. (Note that such q_i exists by the division algorithm 2.3.1).

Let G_i be the equation obtained by multiplying F_i with $-q_i$ and let E_{i+1} be the equation obtained by adding F_{i-1} and G_i :

$$\begin{aligned} G_i &= F_i \cdot -q_i \\ E_{i+1} &= F_{i-1} + G_i \end{aligned}$$

Then the algorithm stops after finitely many steps. Put $d = s_{m-1}$, $x = v_{m-1}$ and $y = y_{m-1}$. Then $d, x, y \in F[x]$ and

$$d = \gcd(a, b) \quad \text{and} \quad d = ax + by.$$

Proof. We call r_k, u_k, y_k the coefficients of E_k , s_k, v_k, y_k the coefficients of F_k and t_k, w_k, z_k the coefficients of G_k . We will first show that each of these coefficients are in $F[x]$. By definition of E_0 and E_1 the coefficients of E_0 and E_1 are $a, 1, 0$ and $b, 0, 1$ respectively, and so all are in $F[x]$. Let $i \in \mathbb{N}$ with $i \geq 1$ and suppose inductively that the coefficients of E_k are in $F[x]$ for all $0 \leq k \leq i$. Let $0 \leq k \leq i$. Since $F_k = E_k \cdot \epsilon_k$ and $\epsilon_k \in F[x]$, also the coefficients of F_k are in $F[x]$. integers. As $G_k = F_k \cdot (-q_k)$ and $q_k \in F[x]$, also the coefficients of G_k are in $F[x]$. Hence since $E_{i+1} = F_{i-1} + G_i$, the coefficients of E_{i+1} are in $F[x]$. The principal of induction now shows that

- (*) The coefficients of E_i, F_i and G_i are in $F[x]$, whenever E_i, F_i or G_i is defined.

Let $i \in \mathbb{N}$ such that E_i is defined. We will show

- (**) $s_i = \tilde{r}_i \sim r_i$.

By definition of F_i we have $F_i = E_i \cdot \epsilon_i$ and so $s_i = r_i \epsilon_i$. If $r_i \neq 0_F$, then $\epsilon_i = \text{lead}(r_i)^{-1}$ and so ϵ_i is a unit and $s_i = r_i \text{lead}(r_i)^{-1} = \tilde{r}_i$. If $r_i = 0_F$, then $\epsilon_i = 1_F$ and so ϵ_i is a unit and $s_i = r_i 1_F = r_i = 0_F = \tilde{r}_i$. So the first sentence in (**) holds.

$$(\ast \ast \ast) \quad s_{i+1} \sim s_{i-1} - s_i q_i$$

By definition of E_{i+1} and G_i we have $E_{i+1} = F_i + G_i = F_i + F_{i-1} \cdot -q_i = F_{i-1} - F_i q_i$ and considering the first coefficient we see that $r_{i+1} = s_{i-1} - s_i q_i$. By $(\ast \ast)$, $s_{i+1} \sim r_{i+1}$ and so $(\ast \ast \ast)$ holds.

Suppose for a contradiction that Euclidean Algorithm does not stop. Then $s_i \neq 0_F$ and s_i is defined for all $i \in \mathbb{N}$. In particular, $\deg(s_i) \in \mathbb{N}$. By $(\ast \ast \ast)$ $s_{i+1} \sim s_{i-1} - s_i q_i$ and so 2.3.7 gives $\deg s_{i+1} = \deg(s_{i-1} - s_i q_i)$. By choice of q_i we have $\deg(s_{i-1} - s_i q_i) < \deg s_i$, so $\deg s_{i+1} < \deg s_i$. Thus

$$s_1 > s_2 > s_3 > s_3 > \dots s_i > s_{i+1} > \dots$$

It follows that the set $\{\deg s_i \mid i \geq 1\}$ does not have a minimal element. As $\deg s_i \in \mathbb{N}$, this contradicts the Well Ordering Axiom. This contradiction proves that Euclidean Algorithm stops after finitely many steps, that is, there exists a smallest $m \in \mathbb{N}$ with $m \geq 1$ and $s_m = 0_F$.

Since $d = s_{m-1} = \check{r}_{m-1}$ is monic, we conclude from 2.4.2 that

$$d = \gcd(0_F, d) = \gcd(s_m, s_{m-1}).$$

By $(\ast \ast \ast)$ $s_{i+1} \sim s_{i-1} - s_i q_i$. Hence (2.4.3)(a) implies:

$$\text{if } d = \gcd(s_{i+1}, s_i) \text{ then } d = \gcd(s_i, s_{i-1}).$$

As $d = \gcd(s_m, s_{m-1})$ the Principal of Induction shows that $d = \gcd(s_1, s_0)$. By $(\ast \ast)$ $s_1 = 0 \sim r_0$ and $s_1 \sim r_1$. As $r_0 = a$ and $r_1 = b$, this shows $s_0 \sim a$ and $s_1 \sim b$. Together with $d = \gcd(s_1, s_0)$ we conclude from (2.4.3)(b) that $d = \gcd(b, a)$ and so also $d = \gcd(a, b)$.

As F_{m-1} is the equation $s_{m-1} = a \cdot v_{m-1} + b \cdot y_{m-1}$, we get

$$d = ax + by.$$

By $(\ast)$ the coefficients of F_{m-1} are in $F[x]$ so $x, y \in F[x]$ and all parts of the Theorem have been proved. $\square$

Example 2.4.5. Let $f = 3x^4 + 4x^3 + 2x^2 + x + 1$ and $g = 2x^3 + x^2 + 2x + 3$ in $\mathbb{Z}_5[x]$. Find $u, v \in \mathbb{Z}_5[x]$ such that $fu + gv = \gcd(f, g)$.

In the following if a is an integer, we just write a for $[a]_5$.

<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">$E_0 :$</td> <td style="width: 40%;">$3x^4 + 4x^3 + 2x^2 + x + 1$</td> <td style="width: 10%;">$= f \cdot 1$</td> <td style="width: 10%;">$+ g \cdot 0$</td> <td style="width: 30%;"></td> </tr> <tr> <td>$F_0 :$</td> <td>$x^4 + 3x^3 + 4x^2 + 2x + 2$</td> <td>$= f \cdot 2$</td> <td>$+ g \cdot 0$</td> <td>$E_0 \cdot 3^{-1} = 2$</td> </tr> <tr> <td>$E_1 :$</td> <td>$2x^3 + x^2 + 2x + 3$</td> <td>$= f \cdot 0$</td> <td>$+ g \cdot 1$</td> <td></td> </tr> <tr> <td>$F_1 :$</td> <td>$x^3 + 3x^2 + x + 4$</td> <td>$= f \cdot 0$</td> <td>$+ g \cdot 3$</td> <td>$E_1 \cdot 2^{-1} = 3$</td> </tr> <tr> <td>$G_1 :$</td> <td>$*$</td> <td>$= f \cdot 0$</td> <td>$+ g \cdot 2x$</td> <td>$F_1 \cdot -x$</td> </tr> <tr> <td>$E_2 :$</td> <td>$3x^2 + 3x + 2$</td> <td>$= f \cdot 2$</td> <td>$+ g \cdot 2x$</td> <td>$F_0 + G_1$</td> </tr> <tr> <td>$F_2 :$</td> <td>$x^2 + x - 1$</td> <td>$= f \cdot -1$</td> <td>$+ g \cdot -x$</td> <td>$E_2 \cdot (3)^{-1} = 2$</td> </tr> <tr> <td>$G_2 :$</td> <td>$*$</td> <td>$= f \cdot (x+2) + g \cdot (x^2+2x)$</td> <td></td> <td>$F_2 \cdot -(x+2)$</td> </tr> <tr> <td>$F_3 = E_3 :$</td> <td>$1$</td> <td>$= f \cdot (x+2) + g \cdot (x^2+2x+3)$</td> <td></td> <td>$F_1 + G_2$</td> </tr> <tr> <td>$E_4$</td> <td>$0$</td> <td></td> <td></td> <td></td> </tr> </table>	$E_0 :$	$3x^4 + 4x^3 + 2x^2 + x + 1$	$= f \cdot 1$	$+ g \cdot 0$		$F_0 :$	$x^4 + 3x^3 + 4x^2 + 2x + 2$	$= f \cdot 2$	$+ g \cdot 0$	$ E_0 \cdot 3^{-1} = 2$	$E_1 :$	$2x^3 + x^2 + 2x + 3$	$= f \cdot 0$	$+ g \cdot 1$		$F_1 :$	$x^3 + 3x^2 + x + 4$	$= f \cdot 0$	$+ g \cdot 3$	$ E_1 \cdot 2^{-1} = 3$	$G_1 :$	$*$	$= f \cdot 0$	$+ g \cdot 2x$	$ F_1 \cdot -x$	$E_2 :$	$3x^2 + 3x + 2$	$= f \cdot 2$	$+ g \cdot 2x$	$ F_0 + G_1$	$F_2 :$	$x^2 + x - 1$	$= f \cdot -1$	$+ g \cdot -x$	$ E_2 \cdot (3)^{-1} = 2$	$G_2 :$	$*$	$= f \cdot (x+2) + g \cdot (x^2+2x)$		$ F_2 \cdot -(x+2)$	$F_3 = E_3 :$	1	$= f \cdot (x+2) + g \cdot (x^2+2x+3)$		$ F_1 + G_2$	E_4	0				<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">$x^3 + 3x^2 + x + 4$</td> <td style="width: 10%;">x^4</td> <td style="width: 50%;">$+ 3x^3 + 4x^2 + 2x + 2$</td> </tr> <tr> <td></td> <td>$x^4 + 3x^3$</td> <td>$+ x^2 + 4x$</td> </tr> <tr> <td></td> <td></td> <td>$3x^2 + 3x + 2$</td> </tr> <tr> <td>$x^2 + x - 1$</td> <td>$x^3 + 3x^2$</td> <td>$+ x + 4$</td> </tr> <tr> <td></td> <td>$x^3 + x^2$</td> <td>$- x$</td> </tr> <tr> <td></td> <td></td> <td>$2x^2 + 2x + 4$</td> </tr> <tr> <td></td> <td></td> <td>$2x^2 + 2x - 2$</td> </tr> <tr> <td></td> <td></td> <td>1</td> </tr> </table>	$x^3 + 3x^2 + x + 4$	x^4	$+ 3x^3 + 4x^2 + 2x + 2$		$x^4 + 3x^3$	$+ x^2 + 4x$			$3x^2 + 3x + 2$	$x^2 + x - 1$	$x^3 + 3x^2$	$+ x + 4$		$x^3 + x^2$	$- x$			$2x^2 + 2x + 4$			$2x^2 + 2x - 2$			1
$E_0 :$	$3x^4 + 4x^3 + 2x^2 + x + 1$	$= f \cdot 1$	$+ g \cdot 0$																																																																								
$F_0 :$	$x^4 + 3x^3 + 4x^2 + 2x + 2$	$= f \cdot 2$	$+ g \cdot 0$	$ E_0 \cdot 3^{-1} = 2$																																																																							
$E_1 :$	$2x^3 + x^2 + 2x + 3$	$= f \cdot 0$	$+ g \cdot 1$																																																																								
$F_1 :$	$x^3 + 3x^2 + x + 4$	$= f \cdot 0$	$+ g \cdot 3$	$ E_1 \cdot 2^{-1} = 3$																																																																							
$G_1 :$	$*$	$= f \cdot 0$	$+ g \cdot 2x$	$ F_1 \cdot -x$																																																																							
$E_2 :$	$3x^2 + 3x + 2$	$= f \cdot 2$	$+ g \cdot 2x$	$ F_0 + G_1$																																																																							
$F_2 :$	$x^2 + x - 1$	$= f \cdot -1$	$+ g \cdot -x$	$ E_2 \cdot (3)^{-1} = 2$																																																																							
$G_2 :$	$*$	$= f \cdot (x+2) + g \cdot (x^2+2x)$		$ F_2 \cdot -(x+2)$																																																																							
$F_3 = E_3 :$	1	$= f \cdot (x+2) + g \cdot (x^2+2x+3)$		$ F_1 + G_2$																																																																							
E_4	0																																																																										
$x^3 + 3x^2 + x + 4$	x^4	$+ 3x^3 + 4x^2 + 2x + 2$																																																																									
	$x^4 + 3x^3$	$+ x^2 + 4x$																																																																									
		$3x^2 + 3x + 2$																																																																									
$x^2 + x - 1$	$x^3 + 3x^2$	$+ x + 4$																																																																									
	$x^3 + x^2$	$- x$																																																																									
		$2x^2 + 2x + 4$																																																																									
		$2x^2 + 2x - 2$																																																																									
		1																																																																									

The remainder of $x^2 + x - 1$ when divided by 1 is 0 .

Hence

$$1 = \gcd(f, g) \quad \text{and} \quad 1 = f \cdot (x+2) + g \cdot (x^2 + 2x + 3).$$

Theorem 2.4.6. *Let F be a field and $f, g \in F[x]$ not both 0_F .*

- (a) *There exists a unique greatest common divisor d of f and g in $F[x]$.*
- (b) *There exist $u, v \in F[x]$ with $d = fu + gv$.*
- (c) *If c is a common divisor of f and g , then $c|d$.*

Proof. By the Euclidean algorithm 2.4.4 there exists $u, v, d \in F[x]$ such that $d = \gcd(f, g)$ and $d = fu + gv$. This proves the existence of d in (a) and also proves (b).

To prove (c) let c be any common divisor of a and b . Since $d = fu + gv$ we conclude from (1.4.4)(c) that $c|d$.

It remains to prove the uniqueness d . So let also e be a greatest common divisor of f and g . Then e is a common divisor of f and g , and since d is greatest common divisor of f and g we get $\deg e \leq \deg d$. Similarly, as d is a common divisor of e and f , and e is greatest common divisor of f and g we have $\deg e \leq \deg d$. Thus $\deg d = \deg e$.

Since e is a common divisor of g and f , (c) shows that $e|d$. As $\deg d = \deg e$, 2.3.7 gives $d \sim e$. As d and e are monic this implies that $d = e$, see (2.3.10)(b). Thus d is unique. $\square$

Theorem 2.4.7. *Let F be a field and $f, g \in F[x]$. Then $1_F = \gcd(f, g)$ if and only if there exist $u, v \in F[x]$ with $1_F = fu + gv$.*

Proof. $\implies$: Suppose that $1_F = \gcd(f, g)$. By Example 2.4.2 f and g are not both 0_F and so (2.4.6)(a) shows there exist $u, v \in F[x]$ with $fu + gv = 1_F$.

$\impliedby$: Suppose that there exist $u, v \in F[x]$ with $1_F = fu + gv$. Note that 1_F is a monic common divisor of f and g . Let c be any common divisor of f and g . Since $1_F = fu + gv$ we conclude that $c|1_F$ (see (1.4.4)(c)). Hence $\deg c \leq \deg 1_F$ by 2.3.5. Thus $1_F = \gcd(f, g)$ by definition of ‘gcd’. $\square$

Theorem 2.4.8. *Let F be a field and $f, g, h \in F[x]$. Suppose that $1_F = \gcd(f, g)$ and $f|gh$. Then $f|h$.*

Proof. Since $1_F = \gcd(f, g)$ we conclude from 2.4.7 that there exist $u, v \in F[x]$ with

$$\begin{aligned} & fu + gv = 1_F \\ \implies & (fu + gv)h = 1_F h \quad | \text{ Principal of Substitution} \\ \implies & (fu)h + (gv)h = h \quad | \text{ Ax 8 and Ax 10} \\ \implies & f(uh) + (gh)v = h \quad | \text{ GCL, twice} \end{aligned}$$

Since f divides f and f divides gh , (1.4.4)(c) now implies that $f|h$. $\square$

Exercises 2.4:**2.4#1.** Let F be a field.

- (a) Let $a \in \mathbb{F}$ and let d be a monic polynomial in $F[x]$ with $d|(x+a)$. Show that $d = 1_F$ or $d = x+a$.
- (b) Let $a, b \in F$ with $a \neq b$. Compute $\gcd(x+a, x+b)$.

2.4#2. Let F be a field and $f, g \in F[x]$. Find $d, f, g \in F[x]$ with $d = \gcd(f, g)$ and $d = fu + gv$ if

- (a) $F = \mathbb{Q}$, $f = x^4 - x^3 - x^2 + 1$ and $g = x^3 - 1$;
- (b) $F = \mathbb{Z}_5$, $f = x^4 + 3x^2 + 2x + 4$ and $g = x^2 - 1$;
- (c) $F = \mathbb{C}$, $f = x^3 - ix^2 + 4x - 4i$ and $g = x^2 + 1$
- (d) $F = \mathbb{Z}_2$, $f = x^4 + x + 1$ and $g = x^2 + x + 1$.

2.4#3. Let F be a field and $f \in F[x]$ such that $f|g$ for every non-constant polynomial $g \in F[x]$. Show that f is a constant polynomial.**2.4#4.** Let F be a field and $f, g, h \in F[x]$ with $1_F = \gcd(f, g)$. If $f|h$ and $g|h$, prove that $fg|h$.**2.4#5.** Let F be a field and $f, g, h \in F[x]$. Suppose that $g \neq 0_F$ and $1_F = \gcd(f, g)$. Show that $\gcd(fh, g) = \gcd(h, g)$.**2.4#6.** Let F be a field and $f, g, d \in F[x]$ such that $h \neq 0_F$ and $d = \gcd(f, g)$.

- (a) Show that there exist $\hat{f}, \hat{g} \in F[x]$ with $f = \hat{f}d$ and $g = \hat{g}d$.
- (b) Show that $\gcd(\hat{f}, \hat{g}) = 1_F$.

2.4#7. Let F be a field and $f, g, h \in F[x]$ with $f|gh$. Show that there exist $\tilde{g}, \tilde{h} \in F[x]$ with $\tilde{g}|g, \tilde{h}|h$ and $f = \tilde{g}\tilde{h}$.**2.5 Irreducible Polynomials**

Recall that an integer p is a prime if $p \neq 0, p \neq \pm 1$ and whenever a is an integer with $a|p$, then $a = \pm 1$ or $a = \pm p$.

Note that in $\mathbb{Z}$, $a \sim b$ if and only if $a = \pm b$. So we can restate the definition of a prime:

p is a prime if $p \neq 0, p \neq \pm 1$ and whenever $a \in \mathbb{Z}$ with $a|p$, then $a \sim 1$ or $a \sim p$.

This leads to the following definition:

Definition 2.5.1. Let F be a field and $f \in F[x]$.

- (a) f is called irreducible provided that
 - (i) $f \neq 0_F$ and $f \not\sim 1_F$, and

(ii) whenever $g \in F[x]$ with $g|f$, then

$$g \sim 1_F \quad \text{or} \quad g \sim f.$$

(b) f is called *reducible* provided that

(i) $f \neq 0_F$, and

(ii) there exists $g \in F[x]$ with

$$g|f, \quad g \not\sim 1_F, \quad \text{and} \quad g \not\sim f.$$

Remark 2.5.2. Let F be a field and $f \in F[x]$. Then the following statements are equivalent:

(a) f is not constant.

(b) $f \notin F$.

(c) $\deg f > 0$.

(d) $\deg f \geq 1$.

(e) $f \neq 0_F$ and $f \not\sim 1_F$.

Proof. We will show that the negation of the three statements are equivalent, that is we will show that

$$f \text{ is constant} \iff f \in F \iff \deg f \leq 0 \iff \deg f < 1 \iff f = 0_F \text{ or } f \sim 1_F.$$

By (2.2.2)(c) f is constant if and if $f \in F$ and if and only if $\deg f \leq 0$.

Since $\deg f \in \mathbb{N}^* = \mathbb{N} \cup \{-\infty\}$, we have $\deg f \leq 0$ if and only if $\deg f < 1$ and if and only if $\deg f = -\infty$ or $\deg f = 0$.

From (2.2.2)(a) we know that $\deg f = -\infty$ if and only if $f = 0_F$, and from 2.3.6 that $\deg f = 0$ if and only if $f \sim 1_F$. $\square$

Theorem 2.5.3. Let F be a field and $f \in F[x]$. Then the following statements are equivalent:

(a) f is reducible.

(b) f is divisible by a non-constant polynomial of lower degree.

(c) f is the product of two polynomials of lower degree.

(d) f is the product of two non-constant polynomials of lower degree.

(e) f is the product of two non-constant polynomials.

(f) f is not constant and f is not irreducible.

Proof. (a) $\implies$ (b): Suppose f is reducible. By definition of ‘reducible’ we conclude that $f \neq 0_F$ and there exists $g \in F[x]$ with $g \mid f$, $g \not\sim 1_F$ and $g \not\sim f$. As $g \mid f$ and $f \neq 0_F$ we have $g \neq 0_F$ (see 1.4.3). Since $g \neq 0_F$ and $g \not\sim 1_F$, Remark 2.5.2 shows that g is not constant. As $g \mid f$ and $f \neq 0_F$ we have $\deg g \leq \deg f$, see 2.3.5. Suppose that $\deg g = \deg f$. Since $g \mid f$ we get from 2.3.7 that $g \sim f$, a contradiction. Thus $\deg g < \deg f$ and so $\deg g < \deg f$. Hence g is a non-constant polynomial of lower degree than f which divides f . So (b) holds.

(b) $\implies$ (c): Let g be a non-constant polynomial of lower degree than f with $g \mid f$. Since g is not constant we have $\deg g > 0$ (by 2.5.2). Moreover, $\deg g < \deg f$ and $f = gh$ for some $h \in F[x]$. From $\deg g < \deg f$ we get $\deg f \neq -\infty$, so $f \neq 0_F$. As $f = gh$ we conclude that $h \neq 0_F$. By (2.2.5)(a) $\deg f = \deg g + \deg h$ and since $\deg g > 0$ this gives $\deg h < \deg f$. We proved that $f = gh$, $\deg g < \deg f$ and $\deg h < \deg f$. Thus (c) holds.

(c) $\implies$ (d): Suppose $f = gh$ with $\deg g < \deg f$ and $\deg h < \deg f$. By 2.2.5 $\deg f = \deg g + \deg h$. Since $\deg g < \deg f$ we conclude that $\deg h > 0$. So h is not constant (by 2.5.2). Similarly g is not constant. Thus (d) holds.

(d) $\implies$ (e): Obvious.

(e) $\implies$ (f): Suppose $f = gh$ where g and h are non-constant polynomials in $F[x]$. Then $g \mid f$. As g and h are non-constant we have $g \not\sim 1_F$, $\deg g \geq 1$ and $\deg h \geq 1$, see 2.5.2. By (2.2.5)(a) we know that $\deg f = \deg g + \deg h$ and so $\deg f > \deg g \geq 1$. Thus f is not constant and $\deg f \neq \deg g$. If $g \sim f$, then 2.3.7 implies $\deg g = \deg f$, a contradiction. Hence $g \not\sim f$.

We proved that $g \mid f$, $g \not\sim 1_F$ and $g \not\sim f$. Hence the second condition in the definition of ‘irreducible’ does not hold. So f is not irreducible. We already proved that f is not constant, so (f) holds.

(f) $\implies$ (a): Suppose f is not constant and f is not irreducible. By definition, f is irreducible, if $f \neq 0_F$, $f \not\sim 1_F$ and

$$\text{“ whenever } g \in F[x] \text{ with } g \mid f, \text{ then } g \sim 1_F \text{ or } g \sim f \text{ ”}$$

As f is non constant we know that $f \neq 0_F$ and $f \not\sim 1_F$, see 2.5.2. So the latter statement must be false. Hence there exists $g \in F[x]$ with $g \mid f$, $g \not\sim 1_F$ and $g \not\sim f$. Also $f \neq 0_F$ and the definition of ‘reducible’ now shows that f is reducible. Thus (a) holds. $\square$

Remark 2.5.4. Let F be a field.

- (a) A non-constant polynomial in $F[x]$ is reducible if and only if it is not irreducible.
- (b) A non-constant polynomial in $F[x]$ is irreducible if and only if it is not reducible.
- (c) A polynomial is irreducible if and only if it is not constant and not reducible.
- (d) A constant polynomial in $F[x]$ is neither reducible nor irreducible.

Proof. Let $f \in F[x]$. Then (2.5.3)(a),(f) shows that

$$(*) \quad f \text{ is reducible} \quad \text{if and only if} \quad f \text{ is non-constant and } f \text{ is not irreducible.}$$

(a): Let f be non-constant polynomial in $F[x]$. Then $(*)$ shows that f is reducible if and only if f is not irreducible.

(b): This is equivalent to (a) and so true.

(c) Suppose f is irreducible. Then $f \neq 0_F$ and $f \not\sim 1_F$. So f is not-constant, see 2.5.2. Now (b) implies f is not reducible.

Suppose f is not constant and not reducible. Then (b) shows that f is irreducible

(d): By (c) irreducible polynomials are not constant and by $(*)$ reducible polynomials are not constant. Thus constant polynomials are neither irreducible nor constant. $\square$

Theorem 2.5.5. *Let F be a field and p a non-constant polynomial in $F[x]$. Then the following statement are equivalent:*

- (a) p is irreducible.
- (b) Whenever $g, h \in F[x]$ with $p \mid gh$, then $p \mid g$ or $p \mid h$.
- (c) Whenever $g, h \in F[x]$ with $p = gh$, then g or h is constant.

Proof. (a) $\implies$ (b): Suppose p is irreducible and let $g, h \in F[x]$ with $p \mid gh$. Since p is non-constant we have $p \neq 0_F$ and so the Euclidean Algorithm 2.4.4 shows that there exists $d \in F[x]$ with $d = \gcd(p, g)$. By definition of ‘gcd’, $d \mid p$ and since p is irreducible we get that

$$d \sim 1_F \quad \text{or} \quad d \sim p.$$

We treat these two cases separately:

Suppose that $d \sim 1_F$. Since both d and 1_F are monic we conclude from 2.3.10 that $d = 1_F$. As $p \mid gh$ this implies $p \mid h$, see 2.4.8.

Suppose that $d \sim p$. As $d \mid g$ this gives $p \mid g$, see 1.12.8.

(b) $\implies$ (c): Suppose (b) holds and let $g, h \in F[x]$ with $p = gh$. Note that $p1_F = p = gh$ and so $p \mid gh$. From (b) we conclude $p \mid g$ or $p \mid h$. Since the situation is symmetric in g and h we may assume $p \mid g$. As p is not constant we have $p \neq 0_F$. Since $p = gh$ this gives $g \neq 0_F$ and $h \neq 0_F$. In particular, $\deg h \geq 0$. As $p \mid g$ we have $\deg p \leq \deg g$ by 2.3.5. Hence

$$\deg g \geq \deg p = \deg gh \stackrel{(2.2.5)(a)}{=} \deg g + \deg h \geq \deg g + 0 = \deg g.$$

Thus $\deg g = \deg g + \deg h$ and so $\deg h = 0$. Thus h is constant.

(c) $\implies$ (a): We will show that $\text{not}-(a) \implies \text{not}-(c)$. So suppose (a) does not hold. Then p is not constant (by hypothesis) and not irreducible. Hence (2.5.3)(f),(e) shows that p is the product of two non-constant polynomials. Thus (c) does not hold. $\square$

Theorem 2.5.6. *Let F be a field and let p be an irreducible polynomial in $F[x]$. If $a_1, \dots, a_n \in F[x]$ and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$.*

Proof. By induction on n . For $n = 1$ the statement is obviously true. So suppose the statement is true for $n = k$ and that $p|a_1 \dots a_k a_{k+1}$. By 2.5.5, $p|a_1 \dots a_k$ or $p|a_{k+1}$. In the first case the induction assumption implies that $p|a_i$ for some $1 \leq i \leq k$. Hence, in either case, $p|a_i$ for some $1 \leq i \leq k+1$. Thus the theorem holds for $k+1$ and so by the Principle of Mathematical Induction (A.5.2) the theorem holds for all positive integers n . $\square$

Theorem 2.5.7. *Let F be a field and p, q irreducible polynomials in $F[x]$. Then $p|q$ if and only if $p \sim q$.*

Proof. If $p \sim q$, then $p|q$ by 1.12.6. So suppose that $p|q$. Since q is irreducible we have $p \sim 1_F$ or $p \sim q$, and since p is irreducible we have $p \not\sim 1_F$. Thus $p \sim q$. $\square$

Theorem 2.5.8. *Let F be a field and $f, g \in F[x]$ with $f \sim g$. Then f is irreducible if and only if g is irreducible.*

Proof. Since $f \sim g$ we know that $\deg f = \deg g$ and that f and g have the same divisors, see 2.3.7 and 1.12.8.

By (2.5.4)(c) f is irreducible if and only if f is non-constant and not reducible. This holds if and only if $\deg f \geq 1$ and f is not divisible by a non-constant polynomial of lower degree, see (2.5.2)(d) and 2.5.3. The latter statement holds if and only if $\deg g \geq 1$ and g is not divisible by a polynomial of lower degree, and so if and only if g is irreducible. $\square$

Theorem 2.5.9 (Factorization Theorem). *Let F be a field and f a non-constant polynomial in $F[x]$. Then f is a product of irreducible polynomials in $F[x]$.*

The proof is by complete induction on $\deg f$. So suppose that every non-constant polynomial of lower degree than f is a product of irreducible polynomials.

Suppose that f is irreducible. Then f is the product of one irreducible polynomial (namely itself).

Suppose f is not irreducible. Since f is also non-constant we conclude from 2.5.3 that $f = gh$ where g and h are non-constant polynomials of lower degree than f . By the induction assumption both g and h are products of irreducible polynomials. Since $f = gh$ this shows that f is a product of irreducible polynomials.

Example 2.5.10. Consider the polynomial $f = 2x^4 - 2$ in $\mathbb{Q}[x]$. Then

$$f = 2(x^4 - 1) = 2(x^2 - 1)(x^2 + 1) = 2(x - 1)(x + 1)(x^2 + 1),$$

and so each of the following are factorizations of f as products of irreducible polynomials in $\mathbb{Q}[x]$:

$$\begin{aligned} f &= (2x - 2) (x + 1) (x^2 + 1) \\ &= (x - 1) (2x + 2) (x^2 + 1) \\ &= (x - 1) (x + 1) (2x^2 + 2) \\ &= (2x + 2) (x^2 + 1) (x - 1) \\ &= (6x + 6) (5^2x + 5) \left(\frac{1}{15}x - \frac{1}{15}\right) \end{aligned}$$

Theorem 2.5.11 (Unique Factorization Theorem). *Let F be a field and f a non-constant polynomial in $F[x]$. Suppose that n, m are positive integers and $p_1, p_2, \dots, p_n$ and $q_1, \dots, q_m$ are irreducible polynomials in $F[x]$ with*

$$f = p_1 p_2 \dots p_n \quad \text{and} \quad f = q_1 q_2 \dots q_m.$$

Then $n = m$ and, possibly after reordering the q_i 's,

$$p_1 \sim q_1, \quad p_2 \sim q_2, \quad \dots, \quad p_n \sim q_n.$$

In more precise terms: there exists a bijection $\pi : \{1, \dots, n\} \mapsto \{1, \dots, m\}$ such that

$$p_1 \sim q_{\pi(1)}, \quad p_2 \sim q_{\pi(2)}, \quad \dots, \quad p_n \sim q_{\pi(n)}.$$

Proof. The proof is by complete induction on n . So let k be a positive integer and suppose that the theorem holds whenever $n < k$. We will show that the theorem holds for $n = k$. So suppose that

$$(*) \quad f = p_1 p_2 \dots p_k \quad \text{and} \quad f = q_1 q_2 \dots q_m$$

where m is a positive integer and $p_1, \dots, p_k, q_1, \dots, q_m$ are irreducible polynomials in $F[x]$.

Suppose first that f is irreducible. Then by 2.5.5 f is not the product of two non-constant polynomials in $F[x]$. Hence $(*)$ implies $k = m = 1$. Thus $p_1 = f = q_1$. Since $\sim$ is reflexive this gives $p_1 \sim q_1$ and so the theorem holds in this case.

Suppose next that f is not irreducible. Since p_1 and q_1 are irreducible we get $f \neq p_1$ and $f \neq q_1$. Thus $k \geq 2$ and $m \geq 2$. Since F is a field, F and so also $F[x]$ is commutative, see 2.2.4. Hence we can apply the GCL for multiplication. Hence using $(*)$, $f = (p_1 \dots p_{k-1})p_k \stackrel{\text{GCL}}{=} p_k(p_1 \dots p_{k-1})$, so p_k divides f . By $(*)$ $f = q_1 \dots q_m$ and we conclude that p_k divides $q_1 \dots q_m$. Hence by 2.5.6, $p_k \mid q_j$ for some $1 \leq j \leq m$. As p_k and q_j are irreducible we get $p_k \sim q_j$, see 2.5.7. Reordering the q_i 's we may assume that

$$(**) \quad p_k \sim q_m.$$

The definition of $\sim$ now shows that

$$(* * *) \quad p_k = q_m u$$

for some unit $u \in F[x]$. Hence

$$((p_1 u) p_2 \dots p_{k-1}) q_m \stackrel{\text{GDL}}{=} (p_1 \dots p_{k-1}) (q_m u) \stackrel{(***)}{=} p_1 \dots p_{k-1} p_k \stackrel{(*)}{=} f \stackrel{(*)}{=} (q_1 \dots q_{m-1}) q_m.$$

By (2.2.5)(c) $F[x]$ is an integral domain. Since q_m is irreducible we have $q_m \neq 0_F$. Hence the Multiplicative Cancellation Law 1.8.7 gives

$$(p_1 u)p_2 \dots p_{k-1} = q_1 \dots q_{m-1}.$$

Since u is a unit, $p_1 u \sim p_1$. As p_1 is irreducible we conclude that also $p_1 u$ is irreducible, see by 2.5.8. The induction assumption now implies that $k - 1 = m - 1$ and that, after reordering the q_i 's,

$$p_1 u \sim q_1, \quad p_2 \sim q_2, \quad \dots \quad p_{k-1} \sim q_{k-1}.$$

From $k - 1 = m - 1$ we get $k = m$. As $p_1 \sim p_1 u$ and $p_1 u \sim q_1$ we have $p_1 \sim q_1$, by transitivity of $\sim$, see 1.12.4. Thus

$$p_1 \sim q_1, \quad p_2 \sim q_2, \quad \dots, \quad p_{k-1} \sim q_{k-1},$$

Moreover, as $p_k \sim q_m$ and $m = k$ we have $p_k \sim q_k$. Thus the theorem holds for $n = k$. By the principal of complete induction, the theorem holds for all positive integers n . $\square$

Exercises 2.5:

2.5#1. Find all irreducible polynomials of

- (a) degree two in $\mathbb{Z}_2[x]$.
- (b) degree three in $\mathbb{Z}_2[x]$.
- (c) degree two in $\mathbb{Z}_3[x]$.

2.5#2. (a) Show that $x^2 + 2$ is irreducible in $\mathbb{Z}_5[x]$.

- (b) Factor $x^4 - 4$ as a product of irreducibles in $\mathbb{Z}_5[x]$.

2.5#3. Let F be a field. Prove that every non-zero polynomial f in $F[x]$ can be written in the form $f = cp_1 p_2 \dots p_n$ with $c \in F$, $n \in \mathbb{N}$ and each p_i monic irreducible in $F[x]$. Show further that if $f = dq_1 \dots q_m$ with $d \in F$, $m \in \mathbb{N}$ and each q_i monic and irreducible in $F[x]$, then $m = n$, $c = d$ and after reordering, if necessary, $p_i = q_i$ for each i .

2.5#4. Let F be a field and $p \in F[x]$ with $p \notin F$. Show that the following two statements are equivalent:

- (a) p is irreducible
- (b) If $g \in F[x]$, then $p|g$ or $1_F = \gcd(p, g)$.

2.5#5. Let F be a field and let $p_1, p_2, \dots, p_n$ be irreducible monic polynomials in $F[x]$ such that $p_i \neq p_j$ for all $1 \leq i < j \leq n$. Let $f, g \in F[x]$ and suppose that $f = ap_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ and $g = bp_1^{l_1} p_2^{l_2} \dots p_n^{l_n}$ for $k_1, k_2, \dots, k_n, l_1, l_2, \dots, l_n \in \mathbb{N}$ and non-zero $a, b \in F$.

- (a) Show that $f|g$ in $F[x]$ if and only if $k_i \leq l_i$ for all $1 \leq i \leq n$.
- (b) For $1 \leq i \leq n$ define $m_i = \min(k_i, l_i)$. Show that $\gcd(f, g) = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}$.

2.6 Polynomials and Homomorphism

Theorem 2.6.1. *Let R and S be commutative rings with identities, let $\alpha : R \rightarrow S$ a homomorphism of rings with $\alpha(1_R) = 1_S$ and let $s \in S$.*

(a) *There exists a unique ring homomorphism $\alpha_s : R[x] \rightarrow S$ such that $\alpha_s(x) = s$ and $\alpha_s(r) = \alpha(r)$ for all $r \in R$.*

(b) $\alpha_s(f) = \sum_{i=0}^{\deg f} \alpha(f_i)s^i$ for all $f = \sum_{i=0}^{\deg f} f_i x^i$ in $R[x]$,

Proof. Suppose first that $\beta : R[x] \rightarrow S$ is a ring homomorphism with

$$(*) \quad \beta(x) = s \quad \text{and} \quad \beta(r) = \alpha(r)$$

for all $r \in R$. Let $f \in R[x]$.

Then

$$\begin{aligned} \beta(f) &= \beta\left(\sum_{i=0}^{\deg f} f_i x^i\right) && \text{--(2.2.2)(d)} \\ &= \sum_{i=0}^{\deg f} \beta(f_i x^i) && \text{--}\beta \text{ respects addition} \\ &= \sum_{i=0}^{\deg f} \beta(f_i) \beta(x)^i && \text{--}\beta \text{ respects multiplication} \\ &= \sum_{i=0}^{\deg f} \alpha(f_i) s^i. && \text{--} (*) \end{aligned}$$

This proves (b) and the uniqueness of α_s .

It remains to prove the existence. We use (b) to define α_s . That is we define

$$\alpha_s : R[x] \rightarrow S, \quad f \mapsto \sum_{i=0}^{\deg f} \alpha(f_i) s^i.$$

By hypothesis $\alpha(1_R) = 1_S$. It follows that

$$\begin{aligned} \alpha_s(x) &= \alpha_s(1_R x) && \text{-- 2.1.4} \\ &= \alpha(1_R) s && \text{-- definition of } \alpha_s \\ &= 1_S s && \text{-- } \alpha(1_R) = 1_S \\ &= s && \text{-- } \mathbf{Ax 10} \text{ for } S \end{aligned}$$

and similarly, and if $r \in R$, then

$$\alpha_s(r) = \alpha_s(rx^0) = \alpha(r)s^0 = \alpha(r)1_S = \alpha(r).$$

Let $f, g \in R[x]$. Put $n = \max(\deg f, \deg g)$ and $m = \deg f + \deg g$.

$$\begin{aligned}
\alpha_s(f+g) &= \alpha_s \left(\sum_{i=0}^n (f_i + g_i) x^i \right) && - (2.1.5)(a) \text{ with } R[x] \text{ in place of } P \\
&= \sum_{i=0}^n \alpha(f_i + g_i) s^i && - \text{definition of } \alpha_s \\
&= \sum_{i=0}^n (\alpha(f_i) + \alpha(g_i)) s^i && - \text{Since } \alpha \text{ respects addition} \\
&= \left(\sum_{i=0}^{\deg f} \alpha(f_i) s^i \right) + \left(\sum_{i=0}^{\deg g} \alpha(g_i) s^i \right) && - (2.1.5)(a) \text{ with } (S, S, s) \text{ in place of } (R, P, x) \\
&= \alpha_s(f) + \alpha_s(g) && - \text{definition of } \alpha_s, \text{ twice}
\end{aligned}$$

$$\begin{aligned}
\alpha_s(fg) &= \alpha_s \left(\sum_{k=0}^m \left(\sum_{i=0}^k f_i g_{k-i} \right) x^k \right) && - (2.1.5)(a) \text{ with } R[x] \text{ in place of } P \\
&= \sum_{k=0}^m \alpha \left(\sum_{i=0}^k f_i g_{k-i} \right) s^k && - \text{definition of } \alpha_s \\
&= \sum_{k=0}^m \left(\sum_{i=0}^k \alpha(f_i) \alpha(g_{k-i}) \right) s^k && - \alpha \text{ respects addition and multiplication} \\
&= \left(\sum_{i=0}^{\deg f} \alpha(f_i) s^i \right) \cdot \left(\sum_{j=0}^{\deg g} \alpha(g_j) s^j \right) && - (2.1.5)(a) \text{ with } (S, S, s) \text{ in place of } (R, P, x) \\
&= \alpha_s(f) \cdot \alpha_s(g) && - \text{definition of } \alpha_s, \text{ twice}
\end{aligned}$$

So α_s is a homomorphism and the theorem is proved. $\square$

Example 2.6.2. Let R and S be commutative rings with identities, $\alpha : R \rightarrow S$ a ring homomorphism with $\alpha(1_R) = 1_S$ and $s \in S$. Compute α_s in each the following cases:

(1) $S = R$ and $\alpha(r) = r$.

$$\alpha_s(f) = \sum_{i=0}^{\deg f} \alpha(f_i) s^i = \sum_{i=0}^{\deg f} f_i s^i.$$

(2) $S = R[x]$, $\alpha(r) = r$ and $s = x$.

$$\alpha_s(f) = \sum_{i=0}^{\deg f} \alpha(f_i) s^i = \sum_{i=0}^{\deg f} f_i x^i = f.$$

So α_s is identity function on $R[x]$.

- (3) $n \in R$, $S = R_n[x]$, $\alpha(r) = [r]_n$ and $s = x$.

Note first that by Example (1.11.2)(4) the function $R \rightarrow R_n, r \mapsto [r]_n$ is a homomorphism. So $\alpha : R \rightarrow R_n[x], r \mapsto [r]_n$ is a homomorphism. We compute

$$\alpha_s(f) = \sum_{i=0}^{\deg f} \alpha(f_i) s^i = \sum_{i=0}^{\deg f} [f_i]_n x^i$$

So $\alpha_s(f)$ is obtain from f by viewing each coefficient as congruence class modulo n .

For example if $R = \mathbb{Z}$ and $n = 3$, then

$$\begin{aligned} \alpha_x(6x^3 + 5x^2 + 10x + 9) &= [6]_3 x^3 + [5]_3 x^2 + [10]_3 x + [9]_3 = [0]_3 x^3 + [2]_3 x^2 + [1]_3 x + [0]_3 \\ &= (\text{in } \mathbb{Z}_3[x]) \quad 2x^2 + x. \end{aligned}$$

Definition 2.6.3. Let I be a set and R a ring.

- (a) $\text{Fun}(I, R)$ is the set of all functions from I to R .
 (b) For $\alpha, \beta \in \text{Fun}(I, R)$ define $\alpha + \beta$ in $\text{Fun}(I, R)$ by

$$(\alpha + \beta)(i) = \alpha(i) + \beta(i)$$

for all $i \in I$.

- (c) For $\alpha, \beta \in \text{Fun}(I, R)$ define $\alpha\beta$ in $\text{Fun}(I, R)$ by

$$(\alpha\beta)(i) = \alpha(i)\beta(i)$$

for all $i \in I$.

- (d) For $r \in R$ define $r^\diamond \in \text{Fun}(I, R)$ by

$$r^\diamond(i) = r$$

for all $i \in I$. $r^\diamond$ is called the constant function on I associated to r .

- (e) $\text{Fun}(R) = \text{Fun}(R, R)$.

Theorem 2.6.4. Let I be a set and R a ring.

- (a) $\text{Fun}(I, R)$ together with the above addition and multiplication is a ring.
 (b) $0_R^\diamond$ is the additive identity in $\text{Fun}(I, R)$.
 (c) If R has a multiplicative identity 1_R , then $1_R^\diamond$ is a multiplicative identity in $\text{Fun}(I, R)$.
 (d) $(-\alpha)(i) = -\alpha(i)$ for all $\alpha \in \text{Fun}(I, R)$, $i \in I$.

(e) The function $\tau : R \rightarrow \text{Fun}(I, R), r \mapsto r^\diamond$ is a homomorphism. If $I \neq \emptyset$, then τ is injective.

Proof. (a)-(d): See Exercise 7 on Homework 3 or E.1.2 in the Appendix.

(e) Let $a, b \in R$ and $i \in I$. Then

$$\begin{aligned} (a+b)^\diamond(i) &= a+b && \text{-- definition of } (a+b)^\diamond \\ &= a^\diamond(i) + b^\diamond(i) && \text{-- definition of } a^\diamond \text{ and } b^\diamond \\ &= (a^\diamond + b^\diamond)(i) && \text{-- definition of addition of functions} \end{aligned}$$

Thus $(a+b)^\diamond = a^\diamond + b^\diamond$ by A.4.14 and so $\tau(a+b) = \tau(a) + \tau(b)$ by definition of τ . Similarly,

$$\begin{aligned} (ab)^\diamond(i) &= ab && \text{-- definition of } (ab)^\diamond \\ &= a^\diamond(i)b^\diamond(i) && \text{-- definition of } a^\diamond \text{ and } b^\diamond \\ &= (a^\diamond b^\diamond)(i) && \text{-- definition of multiplication of function} \end{aligned}$$

Hence $(ab)^\diamond = a^\diamond b^\diamond$ by A.4.14 and so $\tau(ab) = \tau(a)\tau(b)$ by definition of τ .

Thus τ is a homomorphism.

Suppose in addition that $I \neq \emptyset$. To show that τ is injective let $a, b \in R$ with $\tau(a) = \tau(b)$. Then $a^\diamond = b^\diamond$. Since $I \neq \emptyset$ we can pick $i \in I$. Then

$$a = a^\diamond(i) = b^\diamond(i) = b$$

and so τ is injective. □

Exercises 2.6:

2.6#1. Let R and S be commutative rings with identity, $\alpha : R \rightarrow S$ a homomorphism of rings with $\alpha(1_R) = 1_S$, $s \in S$ and $f \in R[x]$. Compute $\alpha_s(f)$ if

- (a) $R = \mathbb{Z}, S = \mathbb{Z}_5, \alpha(n) = [n]_5$ for all $n \in \mathbb{Z}$, $s = [2]_5$ and $f = x^3 + 2x + 1$.
- (b) $R = \mathbb{R}, S = \mathbb{C}, \alpha(r) = r$ for all $r \in \mathbb{R}$, $s = i$ and $f = x^3 + 2x^2 + x + 2$.
- (c) $R = \mathbb{C}, S = \mathbb{C}[x], \alpha(a+bi) = a-bi$ for all $a, b \in \mathbb{R}$, $s = x$ and $f = ix^5 - x^4 + (2-i)x^3 + x^2 - ix + (3+2i)$.

2.7 Polynomial function

Notation 2.7.1. Let R be a commutative ring with identity. For $f = \sum_{i=0}^{\deg f} f_i x^i \in R[x]$ let f_R^* be the function

$$f_R^* : R \rightarrow R, \quad r \mapsto \sum_{i=0}^{\deg f} f_i r^i.$$

f_R^* is called the polynomial function on R induced by f . We will usually just write f^* for f_R^* .

Remark 2.7.2. Let R be a commutative ring with identity.

- (a) Let $\text{id} : R \rightarrow R, r \mapsto r$ be the identity function on R and for $r \in R$ let $\text{id}_r : R[x] \rightarrow R$ be the homomorphism from 2.6.1. Then

$$f^*(r) = \text{id}_r(f)$$

for all $f \in R[x]$ and $r \in R$.

- (b) Let $a \in R[x]$ be constant polynomial (that is $a \in R$). Then a^* is the constant function $a^\diamond$ on R associated to f

Proof. (a): By Example (2.6.2)(1) $\text{id}_r(f) = \sum_{i=0}^{\deg f} f_i r^i$ and so $\text{id}_r(f) = f^*(r)$.

(b) Since $a \in R$ we have $a = ax^0$ and so $a^*(r) = ar^0 = a1_R = a = a^\diamond(r)$ for all $r \in R$. Thus $a^* = a^\diamond$ $\square$

The following example shows that it is very important to distinguish between a polynomial f and its induced polynomial function f^* .

Example 2.7.3. Determine the functions on $\mathbb{Z}_2$ induced by the polynomials of degree at most two in $\mathbb{Z}_2[x]$.

f	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$f^*(0)$	0	1	0	1	0	1	0	1
$f^*(1)$	0	1	1	0	1	0	0	1

We conclude that $x^* = (x^2)^*$. So two distinct polynomials can lead to the same polynomial function. Also $(x^2+x)^*$ is the zero function but x^2+x is not the zero polynomial.

Theorem 2.7.4. Let R be commutative ring with identity.

- (a) $f^* \in \text{Fun}(R)$ for all $f \in R[x]$.
 (b) $(f+g)^*(r) = f^*(r) + g^*(r)$ and $(fg)^*(r) = f^*(r)g^*(r)$ for all $f, g \in R[x]$ and $r \in R$.
 (c) $(f+g)^* = f^* + g^*$ and $(fg)^* = f^*g^*$ for all $f, g \in R[x]$.
 (d) The function $R[x] \rightarrow \text{Fun}(R), f \mapsto f^*$ is a ring homomorphism.

Proof. (a) By definition f^* is a function from R to R . Hence $f^* \in \text{Fun}(R)$.

(b)

$$\begin{aligned}
 (f+g)^*(r) &= \text{id}_r(f+g) && -(2.7.2)(a) \\
 &= \text{id}_r(f) + \text{id}_r(g) && - \text{id}_r \text{ is a homomorphism} \\
 &= f^*(r) + g^*(r) && -(2.7.2)(a), \text{ twice}
 \end{aligned}$$

and similarly

$$\begin{aligned}
 (fg)^*(r) &= \text{id}_r(fg) && \text{---(2.7.2)(a)} \\
 &= \text{id}_r(f)\text{id}_r(g) && \text{--- id}_r \text{ is a homomorphism} \\
 &= f^*(r)g^*(r) && \text{---(2.7.2)(a), twice}
 \end{aligned}$$

(c) Let $r \in R$. Then

$$\begin{aligned}
 (f+g)^*(r) &= f^*(r) + g^*(r) && \text{--- (b)} \\
 &= (f^* + g^*)(r) && \text{--- Definition of addition in Fun}(R)
 \end{aligned}$$

So $(f+g)^* = f^* + g^*$. Similarly

$$\begin{aligned}
 (fg)^*(r) &= f^*(r)g^*(r) && \text{--- (b)} \\
 &= (f^*g^*)(r) && \text{--- Definition of multiplication in Fun}(R)
 \end{aligned}$$

and so $(fg)^* = f^*g^*$.

(d) Follows from (c). □

Theorem 2.7.5. *Let R be a commutative ring with identity $1_R \neq 0_R$, $f \in R[x]$ and $a \in R$. Then $f^*(a)$ is the remainder of f when divided by $x - a$ in $R[x]$.*

Proof. Let r be the remainder of f when divided by $x - a$. So $r \in R[x]$, $\deg r < \deg(x - a)$ and there exists $q \in R[x]$ with

$$(*) \quad f = q \cdot (x - a) + r.$$

Since $\deg(x - a) = 1$ we have $\deg r \leq 0$ and so $r \in R$. Thus

$$(**) \quad r^*(t) \stackrel{(2.7.2)(b)}{=} r^\diamond(t) = r$$

for all $t \in R$. We compute

$$\begin{array}{llll}
 f^*(a) & \stackrel{(*)}{=} & (q \cdot (x - a) + r)^*(a) & \stackrel{(2.7.4)(b)}{=} (q \cdot (x - a))^*(a) + r^*(a) \\
 & \stackrel{(2.7.4)(b)}{=} & q^*(a) \cdot (x - a)^*(a) + r^*(a) & \stackrel{\text{Def } (x-a)^*}{=} q^*(a)(a - a) + r^*(a) \\
 & \stackrel{(**)}{=} & q^*(a)(a - a) + r & \stackrel{(1.2.9)(f)}{=} q^*(a) \cdot 0_R + r \\
 & \stackrel{(1.2.9)(c)}{=} & 0_R + r & \stackrel{\mathbf{Ax 4}}{=} r
 \end{array}$$

□

Definition 2.7.6. Let R be a commutative ring with identity, $f \in R[x]$ and $a \in R$. Then a is called a root of f if $f^*(a) = 0_R$.

Theorem 2.7.7 (Factor Theorem). Let R be a commutative ring with identity $1_R \neq 0_R$. Let $f \in R[x]$ and $a \in R$. Then a is a root of f if and only if $x - a \mid f$ in $R[x]$.

Proof. Let r be the remainder of f when divided by $x - a$. Then

$$\begin{aligned}
 & (x - a) \mid f \\
 \iff & r = 0_R && - 2.3.4 \\
 \iff & f^*(a) = 0_R && - f^*(a) = r \text{ by 2.7.5} \\
 \iff & a \text{ is a root of } f && - \text{Definition of root}
 \end{aligned}$$

□

Theorem 2.7.8. Let R be commutative ring with identity and $f \in R[x]$.

- (a) Let $g \in R[x]$ with $g \mid f$. Then any root of g in R is also a root of f in R .
- (b) Let $a \in R$ and $g, h \in R[x]$ with $f = gh$. Suppose that R is field or an integral domain. Then a is a root of f if and only if a is a root of g or a is a root of h .

Proof. (a): Let a be a root of g . Then $g^*(a) = 0_R$. Since $g \mid f$, there exists $h \in R[x]$ with $f = gh$. Then

$$f^*(a) = (gh)^*(a) \stackrel{(2.7.4)(c)}{=} g^*(a)h^*(a) = 0_R \cdot h^*(a) = 0_R.$$

Thus a is a root of f . So (a) holds.

(b) : Suppose that R is field or an integral domain. By 1.8.10 all fields are integral domains. Thus R is an integral domain and so **Ax 11** holds. Hence

$$\begin{aligned}
 & a \text{ is a root of } f \\
 \iff & f^*(a) = 0_R && - \text{definition of root} \\
 \iff & (gh)^*(a) = 0_R && - f = gh \\
 \iff & g^*(a)h^*(a) = 0_R && - (2.7.4)(b) \\
 \iff & g^*(a) = 0_R \quad \text{or} \quad h^*(a) = 0_R && - \mathbf{Ax 11} \\
 \iff & a \text{ is a root of } g \quad \text{or} \quad a \text{ is a root of } h && - \text{definition of root, twice}
 \end{aligned}$$

□

Example 2.7.9. (1) Let R be a commutative ring with identity and $a \in R$. Find the roots of $x - a$ in R .

Let $b \in R$. Then $(x - a)^*(b) = b - a$. So b is a root of $x - a$ if and only if $b - a = 0_R$ and if and only if $b = a$. Hence a is the unique root of $x - a$.

(2) Find the roots of $x^2 - 1$ in $\mathbb{Z}$. Note that

$$x^2 - 1 = (x - 1)(x + 1) = (x - 1)(x - (-1)).$$

Since $\mathbb{Z}$ is an integral domain, 2.7.8 show that the roots of $x^2 - 1$ are the roots of $x - 1$ together with the roots of $x - (-1)$. So by (1) the roots of $x^2 - 1$ are 1 and -1 .

(3) Find the roots of $x^2 - 1$ in $\mathbb{Z}_8$.

Since $\mathbb{Z}_8$ is not an integral domain, the argument in (2) does not work. We compute in $\mathbb{Z}_8$:

$$0^2 - 1 = -1, (\pm 1)^2 - 1 = 1 - 1 = \boxed{0}, (\pm 2)^2 - 1 = 4 - 1 = 3, (\pm 3)^2 - 1 = 9 - 1 = 8 = \boxed{0}, 4^2 - 1 = 15 = -1.$$

So the roots of $x^2 - 1$ in $\mathbb{Z}_8$ are ± 1 and ± 3 . The four different roots correspond to the two different factorizations

$$x^2 - 1 = (x - 1)(x + 1) \quad \text{and} \quad x^2 - 1 = (x - 3)(x + 3)$$

of $x^2 - 1$ in $\mathbb{Z}_8$.

Theorem 2.7.10 (Root Theorem). *Let R be field or an integral domain and $f \in R[x]$ a non-zero polynomial. Then there exist $m \in \mathbb{N}$, elements $a_1, \dots, a_m \in R$ and $q \in R[x]$ such that*

- (a) $q \neq 0_R$ and $\deg f = \deg q + m$,
- (b) $f = q \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_m)$,
- (c) q has no roots in R , and
- (d) $\{a_1, a_2, \dots, a_m\}$ is the set of roots of f in R .

In particular, $m \leq \deg f$ and the number of roots of f is at most $\deg f$.

Proof. The proof is by complete induction on $\deg f$. So let $k \in \mathbb{N}$ and suppose that theorem holds for all polynomials of degree less than k . Let f be a polynomial of degree k .

Suppose that f has no roots in R . Then the theorem holds with $q = f$ and $m = 0$.

Suppose next that f has a root a in R . Then by the Factor Theorem 2.7.7, $x - a \mid f$ and so

$$(*) \quad f = (x - a) \cdot g \stackrel{\text{Ax 10}}{=} g \cdot (x - a)$$

for some $g \in R[x]$. Since $f \neq 0_R$ also $g \neq 0_R$. We compute

$$(**) \quad k = \deg f = \deg(g \cdot (x - a)) \stackrel{(2.2.5)(a)}{=} \deg g + \deg(x - a) = \deg g + 1$$

and so $\deg g = k - 1 < k$. Hence by the induction assumption there exist $n \in \mathbb{N}$, elements $a_1, \dots, a_n \in R$ and $q \in R[x]$ such that

- (A) $q \neq 0_R$ and $\deg g = \deg q + n$,
- (B) $g = q \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_n)$,
- (C) q has no roots in R , and
- (D) $\{a_1, a_2, \dots, a_n\}$ is the set of roots of g .

Put

$$(\ast \ast \ast) \quad m := n + 1 \quad \text{and} \quad a_m := a.$$

Then

$$\deg f \stackrel{(\ast \ast)}{=} \deg g + 1 \stackrel{(A)}{=} \deg q + n + 1 \stackrel{(\ast \ast \ast)}{=} \deg q + m,$$

so (a) holds.

We have

$$f \stackrel{(\ast)}{=} g \cdot (x - a_m) \stackrel{(C)}{=} q \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_n) \cdot (x - a_m).$$

and since $n = m - 1$ we see that (b) holds.

By (C) q has no roots and so (c) holds.

Let $b \in R$. Since $f = g \cdot (x - a_m)$, 2.7.8 shows that b is a root of f if and only if b is a root of g or b is a root of $x - a_m$. By (D) the roots of g are $a_1, a_2, \dots, a_n$ and by (2.7.9)(1) the root of $x - a_m$ is a_m . Thus the set of roots of f is $\{a_1, a_2, \dots, a_n, a_m\} = \{a_1, \dots, a_m\}$. Hence also (d) is proved. $\square$

Remark 2.7.11. $x^2 - 1$ has four roots in $\mathbb{Z}_8$, namely ± 1 and ± 3 , see Example (2.7.9)(3). So in rings without **Ax 11** a polynomial can have more roots than its degree.

Theorem 2.7.12. Let F be a field and $f \in F[x]$,

- (a) If $\deg f = 1$, then f is irreducible and f has a root in F .
- (b) If $\deg f \geq 2$ and f is irreducible, then f has no root in F .
- (c) If $\deg f = 2$ or 3 , then f is irreducible if and only if f has no roots in F .

Proof. See Exercise 2.7#1

$\square$

Exercises 2.7:

2.7#1. Let F be a field and $f \in F[x]$. Show that

- (a) If $\deg f = 1$, then f has a root in F .
- (b) If $\deg f \geq 2$ and f is irreducible, then f has no root in F .

- (c) If $\deg f = 2$ or 3 , then f is irreducible if and only if f has no roots in F .
- (d) Find an example for a field F and $f \in F[x]$ such that f is reducible and f has no root in F .

2.7#2. Let F be an infinite field.

- (a) Let $f, g \in F[x]$ with $f^* = g^*$. Show that $f = g$. *Hint:* What are the roots of $f - g$?
- (b) Show that the function $F[x] \rightarrow \text{Fun}(F), f \mapsto f^*$ is an injective homomorphism.

2.7#3. Let F be a field and $a_0, a_1, \dots, a_n \in F$. Show that $x - 1_F$ divides $a_n x^n + \dots + a_1 x + a_0$ in $F[x]$ if and only if $a_0 + a_1 + \dots + a_n = 0_F$.

2.7#4. (a) Show that $x^7 - x$ induces the zero function on $\mathbb{Z}_7$.

- (b) Use (a) and Theorem 2.7.10 to write $x^7 - x$ as a product of irreducible monic polynomials in $\mathbb{Z}_7$.

2.7#5. Let R be an integral domain and $n \in \mathbb{N}$. Let $f, g \in R[x]$. Put $n := \deg f$. If $f = 0_R$ define $f^\bullet = 0_R$ and $m_f = 0$. If $f \neq 0_R$ define

$$f^\bullet = \sum_{i=0}^n f_{n-i} x^i$$

and let $m_f \in \mathbb{N}$ be minimal with $f_{m_f} \neq 0_F$. Prove that

- (a) $\deg f = m_f + \deg f^\bullet$.
- (b) $f = x^{m_f} \cdot (f^\bullet)^\bullet$.
- (c) $(fg)^\bullet = f^\bullet g^\bullet$.
- (d) Let $k, l \in \mathbb{N}$ and suppose that $f_0 \neq 0_R$. Then f is the product of polynomials of degree k and l in $R[x]$ if and only if $f^\bullet$ is the product of polynomials of degree k and l in $R[x]$.
- (e) Suppose in addition that R is a field and let $a \in R$. Show that a is a root of $f^\bullet$ if and only if $a \neq 0_R$ and a^{-1} is a root of f .

2.7#6. Let p be a prime. Let $f, g \in \mathbb{Z}_p[x]$ and let $f^*, g^* : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be the corresponding polynomial functions. Show that:

- (a) If $\deg f < p$ and f^* is the zero function, then $f = 0_F$.
- (b) If $\deg f < p, \deg g < p$ and $f \neq g$, then $f^* \neq g^*$.
- (c) There are exactly p^p polynomials of degree less than p in $\mathbb{Z}_p[x]$.
- (d) There exist at least p^p polynomial functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.
- (e) There are exactly p^p functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.
- (f) All functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ are polynomial functions.

2.8 Irreducibility in $\mathbb{Q}[x]$

Theorem 2.8.1 (Rational Root Test). *Let $f = \sum_{i=0}^n f_i x^i \in \mathbb{Z}[x]$ with $f_n \neq 0$. Let $\alpha \in \mathbb{Q}$ be a root of f and suppose $\alpha = \frac{r}{s}$ where $r, s \in \mathbb{Z}$ with $s \neq 0$ and $\gcd(r, s) = 1$. Then $r \mid f_0$ and $s \mid f_n$ in $\mathbb{Z}$.*

Proof. Since α is a root of f , $f^*\left(\frac{r}{s}\right) = f^*(\alpha) = 0$. So

$$\sum_{i=0}^n f_i \left(\frac{r}{s}\right)^i = 0.$$

Multiplication with s^n gives

$$(*) \quad \sum_{i=0}^n f_i r^i s^{n-i} = 0.$$

If $i \geq 1$, then $r \mid r r^{i-1} = r^i$ and so $r^i \equiv 0 \pmod{r}$. Thus $(*)$ implies

$$f_0 s^n \equiv 0 \pmod{r}.$$

and so $r \mid f_0 s^n$. Since $\gcd(r, s) = 1$, Exercise 1.9#4 gives $\gcd(r, s^n) = 1$. 1.9.11 now implies that $r \mid f_0$.

Similarly, if $i < n$, then $s \mid s s^{n-i-1} = s^{n-i}$ and so $s^{n-i} \equiv 0 \pmod{s}$. Thus $(*)$ implies

$$f_n r^n \equiv 0 \pmod{s}.$$

and so $s \mid f_n r^n$. Since $\gcd(r, s) = 1$, gives $\gcd(s, r^n) = 1$ and then $s \mid f_n$. □

Example 2.8.2. Consider $f = 2x^3 + 3x^2 + 2x + 3 \in \mathbb{Q}[x]$. Find all roots of f in $\mathbb{Q}$.

Let $\alpha \in \mathbb{Q}$ be a root of f and write $\alpha = \frac{r}{s}$, where $r, s \in \mathbb{Z}$ with $s > 0$ and $\gcd(r, s) = 1$. The Rational Root Test show that $r \mid 3$ and $s \mid 2$. Thus r is one of ± 1 and ± 3 and, since $s > 0$, s is one of 1 and 2. Thus α is one of

$$\pm 1, \quad \pm 3, \quad \pm \frac{1}{2}, \quad \pm \frac{3}{2}.$$

Computing $f^*(\alpha)$ for each the eight possibilities shows that $\alpha = \frac{3}{2}$ is the only root of f in $\mathbb{Q}$.

We remark that the same result could have been obtained by factorizing f :

$$f = 2x^3 + 3x^2 + 2x + 3 = (2x + 3) \cdot (x^2 + 1)$$

The only root of $2x + 3$ is $-\frac{3}{2}$. Also $x^2 + 1$ has no roots in $\mathbb{Q}$ since $\alpha^2 + 1 \geq 1$ for all $\alpha \in \mathbb{Q}$. So (2.7.8)(b) shows that $-\frac{3}{2}$ is the only root of f .

Definition 2.8.3. Let p be a fixed prime and $f \in \mathbb{Z}[x]$. Put

$$\bar{f} = \sum_{i=0}^{\deg f} [f_i]_p x^i \in \mathbb{Z}_p[x].$$

Then $\bar{f}$ is called the reduction of f modulo p .

Theorem 2.8.4. Let p be a fixed prime and $f, g \in \mathbb{Z}[x]$.

(a) The function

$$\rho_p: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x], \quad f \mapsto \bar{f}$$

is a homomorphism of rings.

(b) $\overline{f+g} = \bar{f} + \bar{g}$ and $\overline{fg} = \bar{f}\bar{g}$.

(c) $\deg \bar{f} \leq \deg f$.

(d) If $f \neq 0$, then $\deg f = \deg \bar{f}$ if and only if $p \nmid \text{lead}(f)$.

Proof. (a) Consider the homomorphism $\alpha: \mathbb{Z} \rightarrow \mathbb{Z}_p[x], n \mapsto [n]_p$. By Example 2.6.2

$$\alpha_x(f) = \sum_{i=0}^{\deg f} [f_i]_p x^i = \bar{f} = \rho_p(f).$$

Thus $\rho_p = \alpha_x$. By 2.6.1 α_x is a homomorphism, so (a) holds.

(b) This follows from (a).

(c) Follows immediately from the definition of $\bar{f}$.

(d) Let $n = \deg f$. Then $\bar{f} = \sum_{i=0}^n [f_i]_p x^i$. Thus $\deg \bar{f} = n$ if and only if $[f_n]_p \neq [0]_p$ and if and only if $p \nmid f_n$. Since $\text{lead} f = f_n$ this gives (d). $\square$

Example 2.8.5. Consider $f = 5x^2 + 4$ and $g = 6x^3 + 8$ in $\mathbb{Z}[x]$. Let $p = 3$. Then

$$\bar{f} = 2x^2 + 1 \quad \text{and} \quad \bar{g} = 2 \quad \text{in } \mathbb{Z}_3[x].$$

Hence

$$\bar{f}\bar{g} = (2x^2 + 1)2 = 4x^2 + 2 = x^2 + 2 \quad \text{in } \mathbb{Z}_3[x].$$

Also

$$fg = (5x^2 + 4)(6x^3 + 8) = 30x^5 + 24x^3 + 40x^2 + 32,$$

and so

$$\overline{fg} = x^2 + 2 \quad \text{in } \mathbb{Z}_3[x].$$

Thus indeed $\overline{fg} = \bar{f}\bar{g}$.

Theorem 2.8.6. Let $f, g \in \mathbb{Z}[x]$ and let p a prime. If p divides all coefficients of fg , then p divides all coefficients of f or p divides all coefficients of g .

Proof. Let $h = \sum_{i=1}^n h_i x^i \in \mathbb{Z}[x]$. Then p divides all the coefficients of h if and only if $[h_i]_p = [0]_p$ for all $0 \leq i \leq n$ and so if and only if $\bar{h} = [0]_p$.

Since p divides all coefficients of fg , $\overline{fg} = [0]_p$ and so by 2.8.4 $\bar{f}\bar{g} = [0]_p$. By 1.10.5 $\mathbb{Z}_p$ is field and so $\mathbb{Z}_p[x]$ is integral domain by 2.2.5. Thus $\bar{f} = [0]_p$ or $\bar{g} = [0]_p$. Hence either p divides all coefficients of f or p divides all coefficients of g . $\square$

Definition 2.8.7. Let $f \in \mathbb{Z}[x]$ and put $n = \deg f$.

- (a) If $f \neq 0$, define $\text{ct}(f) = \gcd(f_0, f_1, \dots, f_n)$. If $f = 0$ define $\text{ct}(f) = 0$. $\text{ct}(f)$ is called the content of f .
- (b) f is called primitive if $\text{ct}(f) = 1$.

Example 2.8.8. Let $f = 12 + 8x + 20x^2$. Compute $\text{ct}(f)$ and $\text{ct}(f)^{-1}f$.

$$\text{ct}(f) = \gcd(12, 8, 20) = 4$$

and

$$\text{ct}(f)^{-1}f = \frac{1}{4}(12 + 8x + 20x^2) = 3 + 2x + 5x^2$$

Note that the latter polynomial is primitive.

Theorem 2.8.9. Let $f \in \mathbb{Z}[x]$.

- (a) Let $a \in \mathbb{Z}$. Then $\text{ct}(af) = |a|\text{ct}(f)$.
- (b) Let $m \in \mathbb{Z}^+$ with $m \mid \text{ct}(f)$ in $\mathbb{Z}$. Put $g := \frac{1}{m}f \in \mathbb{Q}[x]$. Then $g \in \mathbb{Z}[x]$, $f = mg$, $\deg f = \deg g$ and $\text{ct}(g) = \frac{\text{ct}(f)}{m}$.
- (c) Suppose $f \neq 0$ and put $g := \frac{1}{\text{ct}(f)}f \in \mathbb{Q}[x]$. Then $g \in \mathbb{Z}[x]$, $f = \text{ct}(f)g$, $\deg f = \deg g$ and g is primitive.

Proof. (a) If $a = 0$ or $f = 0$, then $\text{ct}(af) = \text{ct}(0) = 0 = |a|\text{ct}(f)$. So suppose that $a \neq 0$ and $f \neq 0$. Put $n = \deg f$. By Exercise 1.2.4 $\gcd(af_0, af_1) = |a|\gcd(f_0, f_1)$. An easy induction argument shows

$$\gcd(af_0, af_1, \dots, af_n) = |a|\gcd(f_0, f_1, \dots, f_n).$$

Thus $\text{ct}(af) = |a|\text{ct}(f)$.

(b) We have $mg = m(\frac{1}{m}f) = f$ and so $\deg g = \deg f$ by (2.2.5)(b). Let $i \in \mathbb{N}$. Then $\text{ct}(f) \mid f_i$. Since $m \mid \text{ct}(f)$ and ‘divide’ is transitive we get $m \mid f_i$. Hence $\frac{1}{m}f_i \in \mathbb{Z}$ and so $g \in \mathbb{Z}[x]$. We have

$$\text{ct}(f) = \text{ct}(mg) \stackrel{(a)}{=} |m|\text{ct}(g) = m\text{ct}(g).$$

thus $\text{ct}(g) = \frac{\text{ct}(f)}{m}$.

(c) By (a) applied with $m = \text{ct}(f)$ the first three assertion in (b) holds. Moreover, $\text{ct}(g) = \frac{\text{ct}(f)}{\text{ct}(f)} = 1$ and so g is primitive. $\square$

Theorem 2.8.10. Let $f, g \in \mathbb{Z}[x]$.

- (a) If f and g are primitive, then also fg is primitive.
- (b) $\text{ct}(fg) = \text{ct}(f)\text{ct}(g)$.

Proof. (a) Since f and g are primitive we have $\text{ct}(f) = 1 = \text{ct}(g)$, so $f \neq 0$ and $g \neq 0$. By 2.2.5 $\mathbb{Z}[x]$ is an integral domain and so $fg \neq 0$. Suppose for a contradiction that $\text{ct}(fg) \neq 1$. By 1.10.4 there exists a prime p with $p | \text{ct}(fg)$. Since $\text{ct}(fg)$ divides all coefficients of fg and since ‘divide’ is transitive, we conclude that p divides all coefficients of fg . As p is a prime, 2.8.6 shows that p divides all coefficients of f or p divides all coefficients of g . Hence $\text{ct}(f) \geq p$ or $\text{ct}(g) \geq p$, a contradiction. Thus $\text{ct}(fg) = 1$ and fg is primitive.

(b) Suppose first that $f = 0$ or $g = 0$. Then $fg = 0$. Also $\text{ct}(f) = 0$ or $\text{ct}(g) = 0$ and so $\text{ct}(fg) = 0 = \text{ct}(f)\text{ct}(g)$.

Suppose that $f \neq 0$ and $g \neq 0$. Put $d := \text{ct}(f)$, $e := \text{ct}(g)$, $\tilde{f} = \frac{1}{d}f$ and $\tilde{g} = \frac{1}{e}g$. Then by (2.8.9)(c),

$$(*) \quad f = d\tilde{f}, \quad g = e\tilde{g}$$

and $\tilde{f}$ and $\tilde{g}$ are primitive polynomials in $\mathbb{Z}[x]$. By (a) $\tilde{f}\tilde{g}$ is primitive. It follows that $\text{ct}(\tilde{f}\tilde{g}) = 1$ and so

$$\text{ct}(fg) \stackrel{(*)}{=} \text{ct}(d\tilde{f}e\tilde{g}) \stackrel{\text{GCL}}{=} \text{ct}(de\tilde{f}\tilde{g}) \stackrel{(2.8.9)(a)}{=} |de| \cdot \text{ct}(\tilde{f}\tilde{g}) = de \cdot 1 = de = \text{ct}(f)\text{ct}(g).$$

□

Theorem 2.8.11. *Let $f \in \mathbb{Z}[x]$ and $n, m \in \mathbb{N}$. Then f is the product of polynomials of degree n and m in $\mathbb{Q}[x]$ if and only if f is the product of polynomials of degree n and m in $\mathbb{Z}[x]$.*

Proof. The backwards direction is obvious. So suppose that

$$(*) \quad f = gh \text{ where } g, h \in \mathbb{Q}[x] \text{ with } \deg g = n \text{ and } \deg h = m.$$

Note that there exists $a \in \mathbb{Z}^+$ such that $ag \in \mathbb{Z}[x]$ (for example choose a to be absolute value of the product the denominators of the non-zero coefficients of g). Similarly choose $b \in \mathbb{Z}^+$ with $bh \in \mathbb{Z}[x]$. Put

$$(**) \quad \tilde{g} := ag \quad \text{and} \quad \tilde{h} := bh.$$

Then

$$(* * *) \quad \deg(\tilde{g}) \stackrel{(2.2.5)(b)}{=} \deg g \stackrel{(*)}{=} n, \quad \deg(\tilde{h}) = \deg h = m \quad \text{and} \quad abf = abgh \stackrel{\text{GCL}}{=} (ag)(bh) \stackrel{(**)}{=} \tilde{g}\tilde{h},$$

and so

$$ab \cdot \text{ct}(f) \stackrel{(2.8.9)(a)}{=} \text{ct}(abf) \stackrel{(* * *)}{=} \text{ct}(\tilde{g}\tilde{h}) \stackrel{(2.8.10)(b)}{=} \text{ct}(\tilde{g})\text{ct}(\tilde{h}).$$

It follows that $ab | \text{ct}(\tilde{g})\text{ct}(\tilde{h})$ in $\mathbb{Z}$ and hence, see Exercise 1.9#9,

$$(+) \quad ab = \hat{a}\hat{b},$$

where $\hat{a}$ and $\hat{b}$ are integers with $\hat{a} | \text{ct}(\tilde{g})$ and $\hat{b} | \text{ct}(\tilde{h})$ in $\mathbb{Z}$. Put

$$\hat{g} := \frac{1}{\hat{a}}\tilde{g} \quad \text{and} \quad \hat{h} := \frac{1}{\hat{b}}\tilde{h}.$$

By (2.8.9)(b) we have

$$(++) \quad \hat{g} \in \mathbb{Z}[x], \tilde{g} = \hat{a}\hat{g}, \deg \hat{g} = \deg \tilde{g} \stackrel{(***)}{=} n, \quad \hat{h} \in \mathbb{Z}[x], \tilde{h} = \hat{b}\hat{h}, \deg \hat{h} = \deg \tilde{h} = m.$$

We compute

$$abf \stackrel{(***)}{=} \tilde{g}\tilde{h} \stackrel{(++)}{=} (\hat{a}\hat{g})(\hat{b}\hat{h}) \stackrel{\text{GCL}}{=} (\hat{a}\hat{b})(\hat{g}\hat{h}) \stackrel{(+)}{=} (ab)(\hat{g}\hat{h}).$$

By 2.2.5 $\mathbb{Z}[x]$ is an integral domain. Since $a, b \neq 0$ also $ab \neq 0$ and the Cancellation Law 1.8.7 implies $f = \hat{g}\hat{h}$ and so f is the product of polynomials of degree n and m in $\mathbb{Z}[x]$. $\square$

Theorem 2.8.12. *Let f be a non-constant polynomial in $\mathbb{Z}[x]$ and suppose that f is not irreducible in $\mathbb{Q}[x]$.*

- (a) *There exist non-constant polynomials g and h in $\mathbb{Z}[x]$ of smaller degree than f with $f = gh$.*
- (b) *Suppose in addition that p is a prime with $p \nmid \text{lead}(f)$. Then $\deg \bar{f} = \deg f$ and $\bar{g}$ and $\bar{h}$ are non-constant polynomials of smaller degree than $\bar{f}$ with $\bar{f} = \bar{g}\bar{h}$.*

Proof. (a) Since f is not constant and not irreducible in $\mathbb{Q}[x]$ we conclude from 2.5.3 that $f = gh$ where g and h are non-constant polynomials in $\mathbb{Q}[x]$ of smaller degree than f . By 2.8.11 we can choose such g, h in $\mathbb{Z}[x]$.

(b) Since $p \nmid \text{lead}(f)$ and $\text{lead} f = \text{lead}(gh) \stackrel{(2.2.5)(a)}{=} \text{lead}(g)\text{lead}(h)$ we get $p \nmid \text{lead}(g)$ and $p \nmid \text{lead}(h)$. Thus by (2.8.4)(c), $\deg \bar{f} = \deg f$, $\deg \bar{g} = \deg g$ and $\deg \bar{h} = \deg h$. So $\bar{g}$ and $\bar{h}$ are non-constant polynomials of smaller degree than $\bar{f}$. By 2.8.4, $\bar{f} = \bar{g}\bar{h} = \overline{gh}$. So (b) holds. $\square$

Theorem 2.8.13 (Eisenstein Criterion). *Let $f = \sum_{i=0}^n f_i x^i \in \mathbb{Z}[x]$ be a non-constant polynomial. Suppose there exists a prime p such that*

- (i) $p \mid f_i$ for each $0 \leq i < n$,
- (ii) $p \nmid f_n$, and
- (iii) $p^2 \nmid f_0$

in $\mathbb{Z}$. Then f is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose for a contradiction that f is not irreducible in $\mathbb{Q}[x]$. Note that $f_n = \text{lead}(f)$ and so $p \nmid \text{lead}(f)$ by (ii). Hence 2.8.12 shows that $f = gh$ and $\bar{f} = \bar{g}\bar{h}$ where $g, h \in \mathbb{Z}[x]$ and none of $\bar{f}$, $\bar{g}$, $\bar{h}$ are constant. Since $p \mid f_i$ for all $0 \leq i < n$, we have $[f_i]_p = [0]_p$ for $0 \leq i < n$ and so $\bar{f} = \sum_{i=0}^n [f_i]_p x^i = [f_n]_p x^n$. Since $\bar{f} = \bar{g}\bar{h}$ we have $\bar{g} \mid \bar{f}$ in $\mathbb{Z}_p[x]$. Note that x is a monic irreducible polynomial in $\mathbb{Z}_p[x]$, so Exercise (2.5#5)(a) now shows that $\bar{g} = ax^i$ for some $i \in \mathbb{N}$ and $a \in \mathbb{Z}_p$. Since $\bar{g}$ is not constant, $i \geq 1$ and so $[g_0]_p = (\bar{g})_0 = [0]_p$. Thus $p \mid g_0$ and similarly $p \mid h_0$. By (2.1.5)(c) $f_0 = h_0 g_0$, and we conclude that $p^2 \mid f_0$, a contradiction to (iii). $\square$

Example 2.8.14. Show that $f = x^4 + 121x^3 + 55x^2 + 66x + 11$ is irreducible in $\mathbb{Q}[x]$.

We choose $p = 11$. Note that 11 divides 121, 55, 66 and 11, but 11 does not divide 1 and 11^2 does not divide 11. So f is irreducible by Eisenstein's Criterion.

Theorem 2.8.15. *Let $f \in \mathbb{Z}[x]$ and p a prime integer with $p \nmid \text{lead}(f)$. If the reduction $\bar{f}$ of f modulo p is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose f is not irreducible in $\mathbb{Q}[x]$. Since $p \nmid \text{lead}(f)$ we can apply (2.8.12)(b) and conclude that $\bar{f}$ is the product of two non-constant polynomials in $\mathbb{Z}_p[x]$. So by 2.5.3 $\bar{f}$ is not irreducible in $\mathbb{Z}_p[x]$, a contradiction. $\square$

Example 2.8.16. Show that $7x^3 + 11x^2 + 4x + 19$ is irreducible in $\mathbb{Q}[x]$.

We choose $p = 2$. Then $\bar{f} = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$. By Exercise 2.5#1 $\bar{f}$ is irreducible in $\mathbb{Z}_2[x]$, so f is irreducible in $\mathbb{Q}[x]$ by 2.8.15.

Exercises 2.8:

2.8#1. Use Eisenstein's Criterion to show that each polynomial is irreducible in $\mathbb{Q}[x]$.

- (a) $x^5 - 4x + 22$
- (b) $10 - 15x + 25x^2 - 7x^4$.
- (c) $5x^{11} - 6x^4 + 12x^3 + 36x - 6$.

2.8#2. Show that each polynomial f is irreducible in $\mathbb{Q}[x]$ by finding a prime p that does not divide the leading coefficient such that the reduction of f modulo p is irreducible in $\mathbb{Z}_p[x]$.

- (a) $7x^3 + 6x^2 + 4x + 6$.
- (b) $9x^4 + 4x^3 - 3x + 7$.

2.8#3. Let $f \in \mathbb{Z}[x]$ be monic and $n, m \in \mathbb{N}$. Then f is the product of polynomials of degree n and m in $\mathbb{Q}[x]$ if and only if f is the product of monic polynomials of degree n and m in $\mathbb{Z}[x]$.

2.8#4. Let f be a non-constant polynomial of degree n in $\mathbb{Z}[x]$ and let p be a prime. Suppose that

- (i) $p \mid f_i$ for all $1 \leq i \leq n$.
- (ii) $p \nmid f_0$.
- (iii) $p^2 \nmid f_n$.

Show that f is irreducible in $\mathbb{Q}[x]$.

- (e) $g \in [f]_p$.
- (f) $[f]_p \cap [g]_p \neq \emptyset$.
- (g) $[f]_p = [g]_p$.
- (h) $f \in [g]_p$.
- (i) $g \equiv f \pmod{p}$.
- (j) $p \mid g - f$.
- (k) $g - f = pl$ for some $l \in F[x]$.
- (l) $g = f + pl$ for some $l \in F[x]$.
- (m) f and g have the same remainder when divided by p .

Proof. By 1.4.9 the statements (a) - (l) are equivalent.

Let r_1 and r_2 be the remainders of f and g , respectively, when divided by p . Then there exist $q_1, q_2 \in F[x]$ with

$$(*) \quad \begin{array}{lll} f = pq_1 + r_1 & \text{and} & \deg r_1 < \deg p \\ g = pq_2 + r_2 & \text{and} & \deg r_2 < \deg p \end{array}$$

(m) $\implies$ (k): Suppose (m) holds. Then $r_1 = r_2$ and

$$g - f \stackrel{(*)}{=} (pq_2 + r_2) - (pq_1 + r_1) = p \cdot (q_2 - q_1) + (r_2 - r_1) = p \cdot (q_2 - q_1).$$

So (k) holds with $l = q_2 - q_1$.

(a) $\implies$ (m): Suppose $f = g + pk$ for some $k \in F[x]$. Then

$$f \stackrel{(*)}{=} (pq_2 + r_2) + pk = p \cdot (q_2 + k) + r_2.$$

Note that $q_2 + k \in F[x]$, $r_2 \in F[x]$ and $\deg r_2 < \deg p$. So r_2 is the remainder of f when divided by p . Hence $r_1 = r_2$ and (m) holds. $\square$

Theorem 2.9.4. *Let F be a field and $p \in F[x]$ with $p \neq 0_F$.*

(a) *Let $f \in F[x]$. Then there exists a unique $r \in F[x]$ with $\deg r < \deg p$ and $[f]_p = [r]_p$, namely r is the remainder of f when divided by p .*

(b) *The function*

$$\delta: \{r \in F[x] \mid \deg r < \deg p\} \rightarrow F[x]/(p), \quad r \mapsto [r]_p$$

is a bijection.

(c) $F[x]/(p) = \{[r]_p \mid r \in F[x], \deg r < \deg p\}$

Proof. (a): Let s be the remainder of f when divided by p and let $r \in F[x]$ with $\deg r < \deg p$. Since $r = p0_F + r$ and $\deg r < \deg p$, r is the remainder of r when divided by p . By 2.9.3, $[f]_p = [r]_p$ if and only if f and s have the same remainder when divided by n , and so if and only if $s = r$.

(b)': The uniqueness assertion in (a) shows that δ is injective. Let $A \in F[x]/(p)$. By definition of $F[x]/(p)$ there exists $f \in F[x]$ with $A = [f]_p$. By (a) there exists $r \in F[x]$ with $[f]_p = [r]_p$ and $\deg r < \deg p$. Then $\delta(r) = [r]_p = [f]_p = A$ and so δ is surjective.

(c): This holds since δ is surjective. □

Example 2.9.5. (1) List all elements of $\mathbb{Z}_3[x]/(x^2 + 1)$.

Put $p := x^2 + 1 \in \mathbb{Z}_3[x]$. Then $\deg p = 2$. Since $\mathbb{Z}_3 = \{0, 1, 2\}$, the polynomials of degree less than 2 in $\mathbb{Z}_3[x]$ are

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2.$$

Thus (2.9.4)(c) shows that

$$\begin{aligned} \mathbb{Z}_3[x]/(x^2 + 1) &= \{ [f]_p \mid f \in \mathbb{Z}_3[x], \deg f < 2 \} \\ &= \{ [0]_p, [1]_p, [2]_p, [x]_p, [x+1]_p, [x+2]_p, [2x]_p, [2x+1]_p, [2x+2]_p \}. \end{aligned}$$

(2) Determine $\mathbb{Q}[x]/(x^3 - x + 1)$.

Put $p := x^3 - x + 1$. Note that $\deg p = 3$. Thus (2.9.4)(c) shows that for each $A \in \mathbb{Q}[x]/(p)$ there exists a unique polynomial f of degree less than 3 with $A = [f]_p$. By definition of a polynomial ring there exists unique a, b, c in $\mathbb{Q}$ with $f = a + bx + cx^2$. Hence every element of $\mathbb{Q}[x]/(p)$ can be uniquely written as

$$[a + bx + cx^2]_p \quad \text{with } a, b, c \in \mathbb{Q}.$$

Exercises 2.9:

2.9#1. Let $f, g, p \in \mathbb{Q}[x]$. Determine whether $f \equiv g \pmod{p}$.

- (a) $f = x^5 - 2x^4 + 4x^3 - 3x + 1, \quad g = 3x^4 + 2x^3 - 5x^2 + 2, \quad p = x^2 + 1;$
 (b) $f = x^4 + 2x^3 - 3x^2 + x - 5, \quad g = x^4 + x^3 - 5x^2 + 12x - 25, \quad p = x^2 + 1;$
 (c) $f = 3x^5 + 4x^4 + 5x^3 - 6x^2 + 5x - 7, \quad g = 2x^5 + 6x^4 + x^3 + 2x^2 + 2x - 5, \quad p = x^3 - x^2 + x - 1.$

2.9#2. Show that, under congruence modulo $x^3 + 2x + 1$ in $\mathbb{Z}_3[x]$ there are exactly 27 congruence classes.

2.9#3. Prove or give a counterexample: Let F be a field and $f, g, k, p \in F[x]$. If $p \neq 0_F$, $1_F = \gcd(f, g)$ and $fk \equiv gk \pmod{p}$, then $f \equiv g \pmod{p}$.

2.9#4. Prove or give a counterexample. Let F be a field and $f, g, p \in F[x]$. If p is irreducible and $fg \equiv 0_F \pmod{p}$, then $f \equiv 0_F \pmod{p}$ or $g \equiv 0_F \pmod{p}$.

2.10 Congruence Class Arithmetic

Remark 2.10.1. Let F be a field and $p \in F[x]$. Recall from 1.6.2 that we defined an addition and multiplication on $F[x]/(p)$ by

$$[f]_p \oplus [g]_p = [f + g]_p \quad \text{and} \quad [f]_p \odot [g]_p = [f \cdot g]_p$$

for all $f, g \in F[x]$.

Example 2.10.2. Compute the addition and multiplication table for $\mathbb{Z}_2[x]/(x^2 + x)$.

We write $[f]$ for $[f]_{x^2+x}$. Since $\mathbb{Z}_2 = \{0, 1\}$, the polynomial of degree less than 2 in $\mathbb{Z}_2[x]$ are $0, 1, x, x + 1$. Thus (2.9.4)(c) gives

$$\mathbb{Z}_2[x]/(x^2 + x) = \{[0], [1], [x], [x + 1]\}.$$

We compute

$\oplus$	[0]	[1]	[x]	[x + 1]	$\odot$	[0]	[1]	[x]	[x + 1]
[0]	[0]	[1]	[x]	[x + 1]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[0]	[x + 1]	[x]	[1]	[0]	[1]	[x]	[x + 1]
[x]	[x]	[x + 1]	[0]	[1]	[x]	[0]	[x]	[x]	[0]
[x + 1]	[x + 1]	[x]	[1]	[0]	[x + 1]	[0]	[x + 1]	[0]	[x + 1]

Note here that

$$[x] \odot [x + 1] = [x(x + 1)] = [x^2 + x] = [0]$$

and

$$[x + 1] \odot [x + 1] = [(x + 1)(x + 1)] = [x^2 + 1] = [(x + 1) + (x^2 + x)] = [x + 1]$$

Observe from the above tables that $\mathbb{Z}_2[x]/(x^2 + x)$ contains the subring $\{[0], [1]\}$ isomorphic to $\mathbb{Z}_2$. The next theorem shows that a similar statement holds in general.

Theorem 2.10.3. Let F be a field and $p \in F[x]$.

(a) $F[x]/(p)$ is a commutative ring with identity $[1_F]_p$.

(b) The function

$$\sigma : F[x] \rightarrow F[x]/(p), \quad f \mapsto [f]_p.$$

is an surjective homomorphism of rings.

(c) Put $\hat{F} := \{[a]_p \mid a \in F\}$. Then $\hat{F}$ is a subring of $F[x]/(p)$.

(d) Suppose p is not constant. Then the function

$$\tau: F \rightarrow \hat{F}, \quad a \mapsto [a]_p.$$

is an isomorphism of rings. In particular, $\hat{F}$ is a subring of $F[x]/(p)$ isomorphic to F .

Proof. (a) This is a special case of 1.6.4.

(b) This is a special case of Example (1.11.2)(4).

(c) Note that $[0]_{F[x]/(p)} = [0]_p$, $[a]_p \dots$

(d) We need to show that τ is a injective and surjective homomorphism. By (b), σ is a homomorphism. Observe that $\tau(a) = \sigma(a)$ for all $a \in F$. Hence also τ is a homomorphism.

Let $d \in \hat{F}$. Then $d = [a]_p$ for some $a \in F$ and so $d = \tau(a)$. Thus τ is surjective.

To show that τ is injective, let $a, b \in F$ with $\tau(a) = \tau(b)$. Then $[a]_p = [b]_p$. Since p is not constant $\deg p > 0$ and since $a, b \in F$, $\deg a \leq 0$ and $\deg b \leq 0$, see 2.5.2. Thus $\deg a < \deg p$ and $\deg b < \deg p$. Since $[a]_p = [b]_p$ we conclude from (2.9.4)(a) that $a = b$. Thus τ is injective and (d) is proved. $\square$

Notation 2.10.4. Let R and S be commutative rings with identities. Suppose that S is a subring of R and $1_S = 1_R$. Let $f \in S[x]$ and $r \in R$. We identify the polynomial

$$f = \sum_{i=0}^n f_i x^i \quad \text{in } S[x]$$

with the polynomial

$$g = \sum_{i=0}^n f_i x^i \quad \text{in } R[x]$$

Note that with this identification, $f = g$ and $S[x]$ becomes a subring of $R[x]$. Observe that f gives now rise to two different functions:

$$f_S^*: S \rightarrow S, \quad s \mapsto \sum_{i=0}^n f_i s^i \quad \text{and} \quad f_R^*: R \rightarrow R, \quad r \mapsto \sum_{i=0}^n f_i r^i$$

Nevertheless, we will usually just write f^* for both of this functions.

Notation 2.10.5. Let F be a field and p a non-constant polynomial in $F[x]$.

(a) We ‘identify’ a in F with $[a]_p$ in $F[x]_p$.

(b) We write α for $[x]_p$.

(c) We write $F_p[\alpha]$ for $F[x]/(p)$ to indicate that we identified a and $[a]_p$. More formally, $F_p[\alpha]$ is the ring R constructed in E.3.3.

(d) If $F = \mathbb{Z}_q$ for some prime integer q , we will use the notation $\mathbb{Z}_{q,p}[\alpha]$ for $F_p[\alpha]$.

Theorem 2.10.6. Let F be a field and p a non-constant polynomial in $F[x]$.

- (a) Let $f \in F[x]$. Then $f^*(\alpha) = [f]_p$.
- (b) For each $\beta \in F_p[\alpha]$ there exists a unique $f \in F[x]$ with $\deg f < \deg p$ and $f^*(\alpha) = \beta$.
- (c) Let $n = \deg p$. Then for each $\beta \in F_p[\alpha]$ there exist unique $b_0, b_1, \dots, b_{n-1} \in F$ with
- $$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}.$$
- (d) Let $f \in F[x]$. Then $f^*(\alpha) = 0_F$ if and only if $p \mid f$ in $F[x]$.
- (e) α is a root of p in $F_p[\alpha]$.

Proof. (a) Let $m := \deg f$. Then $f = \sum_{i=0}^m f_i x^i$. We compute

$$\begin{aligned}
 f^*(\alpha) &= \sum_{i=0}^m f_i \alpha^i && \text{-- Definition of } f^*(\alpha) \\
 &= \sum_{i=0}^m f_i [x]_p^i && \text{-- Definition of } \alpha \\
 &= \sum_{i=0}^m [f_i]_p [x]_p^i && \text{-- We identified } a \in F \text{ with } [a]_p \in F_p[\alpha] \\
 &= \left[\sum_{i=0}^m f_i x^i \right]_p && \text{-- } f \mapsto [f]_p \text{ is a homomorphism by 2.10.3} \\
 &= [f]_p.
 \end{aligned}$$

(b) Let $\beta \in F_p[\alpha] = F[x]/(p)$. By 2.9.4 there exists a unique $f \in F[x]$ with $\deg f < \deg p$ and $[f]_p = \beta$. According to (a) we have $f^*(\alpha) = [f]_p$. It follows that f is also the unique $f \in F[x]$ with $\deg f < \deg p$ and $f^*(\alpha) = \beta$. Thus (b) holds.

(c) Let $b_0, \dots, b_{n-1} \in F$ and put $f = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$. Then f is a polynomial with $\deg f < \deg p$ and $b_0, \dots, b_{n-1}$ are uniquely determined by f . Also

$$f^*(\alpha) = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}$$

and so (c) follows from (b).

(d)

$$\begin{aligned}
 &f^*(\alpha) = 0_F \\
 \iff &f^*(\alpha) = 0_F^*(\alpha) && \text{-- definition of } 0_F^*(\alpha) \\
 \iff &[f]_p = [0_F] && \text{-- (a)} \\
 \iff &p \mid (f - 0_F) && \text{-- 2.9.3} \\
 \iff &p \mid f && \text{-- (1.2.9)(b)}
 \end{aligned}$$

(e) Note that $p \mid p$ and so $p^*(\alpha) = 0_F$ by (d). Thus α is a root of p in $F_p[\alpha]$. □

Example 2.10.7. Let $p = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Determine the addition and multiplication table of $\mathbb{Z}_{2,p}[\alpha]$.

By (2.10.6)(c) any element of $F[\alpha]$ can be uniquely written as $b_0 + b_1\alpha$ with $b_0, b_1 \in \mathbb{Z}_2$. By 1.5.7 $\mathbb{Z}_2 = \{0, 1\}$ and so

$$\mathbb{Z}_{2,p}[\alpha] = \{0 + 0\alpha, 0 + 1\alpha, 1 + 0\alpha, 1 + 1\alpha\} = \{0, 1, \alpha, 1 + \alpha\}.$$

Note that $\alpha + \alpha = 2\alpha = 0\alpha = 0$ and so we get

+	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

Since $\alpha + \alpha = 0$ we have $-\alpha = \alpha$. By (2.10.6)(e) $p^*(\alpha) = 0$. Hence $1 + \alpha + \alpha^2 = 0$ and thus

$$\alpha^2 = -1 - \alpha = 1 + \alpha.$$

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

Note here that by the Distributive Law, Column ‘ $1 + \alpha$ ’ is the sum of Column ‘1’ and Column ‘ α ’. Also Row ‘ $1 + \alpha$ ’ is the sum of Row ‘1’ and Row ‘ α ’

Exercises 2.10:

2.10#1. Let $p = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Determine the addition and multiplication table of $\mathbb{Z}_{2,p}[\alpha]$. Is $\mathbb{Z}_{2,p}[\alpha]$ a field?

2.10#2. Let $p = x^2 - 3 \in \mathbb{Q}[x]$. Each element of $\mathbb{Q}_p[\alpha]$ can be uniquely written in the form $b + c\alpha$, with $b, c \in \mathbb{Q}$ (Why?). Determine the rules of addition and multiplication in $\mathbb{Q}_p[\alpha]$. In other words, for $b, c, d, e \in \mathbb{Q}$ find $r, s, u, v \in \mathbb{Q}$ with

$$(b + c\alpha) + (d + e\alpha) = r + s\alpha \quad \text{and} \quad (b + c\alpha)(d + e\alpha) = u + v\alpha.$$

2.11 $F_p[\alpha]$ when p is irreducible

In this section we determine when $F_p[\alpha]$ is a field.

Theorem 2.11.1. *Let F be a field, let p be a non-constant polynomial in $F[x]$ and let f be any polynomial in $F[x]$.*

- (a) $f^*(\alpha)$ is a unit in $F_p[\alpha]$ if and only if $1_F = \gcd(f, p)$.
- (b) If $1_F = fg + ph$ for some $g, h \in F[x]$, then $g^*(\alpha)$ is the inverse of $f^*(\alpha)$ in $F_p[\alpha]$.

Proof. (a) We have

$$\begin{array}{lll}
 & f^*(\alpha) \text{ is a unit in } F_p[\alpha] & \\
 \iff & f^*(\alpha)\beta = 1_F \text{ for some } \beta \in F_p[\alpha] & - F_p[\alpha] \text{ is commutative, 1.12.7} \\
 \iff & f^*(\alpha)g^*(\alpha) = 1_F \text{ for some } g \in F[x] & - \text{By (2.10.6)(b) } \beta = g^*(\alpha) \text{ for some } g \in F[x] \\
 \iff & (fg)^*(\alpha) = 1_F \text{ for some } g \in F[x] & - 2.7.4 \\
 \iff & (fg)^*(\alpha) = 1_F^*(\alpha) \text{ for some } g \in F[x] & - \text{Definition of } 1_F^*(\alpha) \\
 \iff & [fg]_p = [1_F]_p \text{ for some } g \in F[x] & - (2.10.6)(a) \\
 \iff & 1_F = fg + ph \text{ for some } g, h \in F[x] & - 2.9.3(a)(i) \\
 \iff & 1_F = \gcd(f, p) & - 2.4.7
 \end{array}$$

(b) From the above list of equivalent statements, $1_F = fg + ph$ implies $f^*(\alpha)g^*(\alpha) = 1_F$. Since $F_p[\alpha]$ is commutative we also have $g^*(\alpha)f^*(\alpha) = 1_F$ and so $g^*(\alpha)$ is the inverse of $f^*(\alpha)$. $\square$

Theorem 2.11.2. *Let F be a field and p a non-constant polynomial in $F[x]$. Then the following statements are equivalent:*

- (a) p is irreducible in $F[x]$.
- (b) $F_p[\alpha]$ is a field.
- (c) $F_p[\alpha]$ is an integral domain.

Proof. (a) $\implies$ (b): Suppose p is irreducible. By (E.3.3)(c) $F_p[\alpha]$ is a commutative ring with additive identity 0_F and multiplicative identity 1_F . Since F is a field, $1_F \neq 0_F$. Thus it remains to show that every non-zero element in $F_p[\alpha]$ is a unit. So let $\beta \in F_p[\alpha]$ with $\beta \neq 0_F$. By (2.10.6)(b), $\beta = f^*(\alpha)$ for some $f \in F[x]$. Then $f^*(\alpha) \neq 0_F$ and (2.10.6)(d) gives $p \nmid f$. Since p is irreducible, Exercise 2.5#4 shows that $1_F = \gcd(f, p)$. Hence by Theorem 2.11.1 $f^*(\alpha)$ is a unit in $F_p[\alpha]$. As $\beta = f^*(\alpha)$ this shows that β is unit in $F_p[\alpha]$, so (b) holds.

(b) $\implies$ (c): If $F_p[\alpha]$ is a field, then by Theorem 1.8.10 $F_p[\alpha]$ is an integral domain.

(c) $\implies$ (a): Suppose $F_p[\alpha]$ is an integral domain and let $g, h \in F[x]$ with $p|gh$. We will show that $p|g$ or $p|h$. By (2.10.6)(d) α is a root of p and so $p^*(\alpha) = 0_F$. Since $p|gh$ we conclude from (2.7.8)(a) that α is a root of gh . Hence

$$0_F = (gh)^*(\alpha) \stackrel{2.7.4}{=} g^*(\alpha)h^*(\alpha).$$

Since **Ax 11** holds in integral domains this gives $g^*(\alpha) = 0_F$ or $h^*(\alpha) = 0_F$. By (2.10.6)(d) this implies that $p|g$ or $p|h$.

We proved that $p|gh$ implies $p|g$ or $p|h$. Thus 2.5.5 shows that p is irreducible. $\square$

Theorem 2.11.3. *Let F be a field and p an irreducible polynomial in $F[x]$. Then F is a subring of $F_p[\alpha]$, $F_p[\alpha]$ is a field and α is a root of p in $F_p[\alpha]$.*

Proof. By E.3.3 F is a subring of $F_p[\alpha]$. Since p is irreducible, 2.11.2 implies that $F_p[\alpha]$ is field. By (2.10.6)(e) α is a root of p in $F_p[\alpha]$. $\square$

Example 2.11.4. Put $K := \mathbb{R}_{x^2+1}[\alpha]$. Determine the addition and multiplication in K and show that K is a field.

By (2.10.6)(e) we know that α is a root of $x^2 + 1$ in K . Hence $\alpha^2 + 1 = 0$ and so

$$\alpha^2 = -1.$$

By 2.10.6, every element of K can be uniquely written as $a + b\alpha$ with $a, b \in \mathbb{R}$. We have

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$$

and

$$(a + b\alpha)(c + d\alpha) = ac + (bc + ad)\alpha + bd\alpha^2 = ac + (bc + ad)\alpha + bd(-1) = (ac - bd) + (ad + bc)\alpha.$$

Note that $x^2 + 1$ has no roots in $\mathbb{R}$ and so by 2.7.12 $x^2 + 1$ is irreducible. Hence 2.11.2 shows that K is a field.

We remark that is now straight forward to verify that

$$\phi : \mathbb{R}_{x^2+1}[\alpha] \rightarrow \mathbb{C}, \quad a + b\alpha \mapsto a + bi$$

is an isomorphism from $\mathbb{R}_{x^2+1}[\alpha]$ to the complex numbers $\mathbb{C}$.

Theorem 2.11.5. *Let F be a field and $f \in F[x]$.*

- (a) *Suppose f is not constant. Then there exists a field K such that F is a subring of K and f has a root in K .*
- (b) *There exist a field L , $n \in \mathbb{N}$, and elements $c, a_1, a_2, \dots, a_n$ in L such that F is a subring of L and*

$$f = c \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_n)$$

Proof. (a) By 2.5.9, f is a product of irreducible polynomials. In particular, there exists an irreducible polynomial p in $F[x]$ dividing f . By 2.11.3 $K := F_p[\alpha]$ is a field containing F and α is a root of p in K . Since $p|f$, 2.7.8 shows that α is a root of f in K .

(b) If $f = 0_F$, then (b) holds with $n = 0$, $c = f$ and $L = F$. So suppose $f \neq 0_F$. Let L be field containing K as a subring and let m_L be the number of roots of f in L . By the Root Theorem $m_L \leq \deg f$ and so we can choose L with m_L as large as possible. By the Root Theorem there exists $q \in L[x]$, $n \in \mathbb{N}$ and $a_1, \dots, a_n \in L$ such that

$$(*) \quad f = q \cdot (x - a_1) \cdot \dots \cdot (x - a_n),$$

q has no roots in L and $\{a_1, \dots, a_n\}$ is the set of roots of f in L .

Suppose for a contradiction that q is not a constant. Then by (a) applied with L and q in place of F and f , there exists a field K containing L and a root a of q in L . Since $q|f$, a is also a root of f in L , see (2.7.8)(a) and since q has no root in L , $a \notin L$. In particular, $a \notin \{a_1, \dots, a_m\}$ and so $m_K > m_L$. But this contradicts the choice of L .

Hence q is a constant, that is $q \in L$. So $(*)$ shows that (b) holds with $c = q$. □

Exercises 2.11:

2.11#1. In each part explain why $t \in F_p[\alpha]$ is a unit and find its inverse.

(a) $t = -3 + 2\alpha$, $F = \mathbb{Q}$, $p = x^2 - 2$

(b) $t = 1 + \alpha + \alpha^2$, $F = \mathbb{Z}_3$, $p = x^2 + 1$

(c) $t = 1 + \alpha + \alpha^2$, $F = \mathbb{Z}_2$, $p = x^3 + x + 1$

2.11#2. Determine whether $F_p[\alpha]$ is a field.

(a) $F = \mathbb{Z}_3$, $p = x^3 + 2x^2 + x + 1$.

(b) $F = \mathbb{Z}_5$, $p = 2x^3 - 4x^2 + 2x + 1$.

(c) $F = \mathbb{Z}_2$, $p = x^4 + x^2 + 1$.

2.11#3. (a) Verify that $\mathbb{Q}[\sqrt{3}] := \{r + s\sqrt{3} | r, s \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

(b) Show that $\mathbb{Q}[\sqrt{3}]$ is isomorphic to $\mathbb{Q}_{x^2-3}[\alpha]$.

2.11#4. Let $p = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

(a) Determine the addition and multiplication table of $\mathbb{Z}_{2,p}[\alpha]$.

(b) Is $\mathbb{Z}_{2,p}[\alpha]$ a field?

(c) Find all roots of p in $\mathbb{Z}_{2,p}[\alpha]$.

Chapter 3

Ideals and Quotients

3.1 Ideals

Definition 3.1.1. Let I be a subset of the ring R .

(a) We say that I absorbs R if

$$ra \in I \quad \text{and} \quad ar \in I \quad \text{for all } a \in I, r \in R$$

(b) We say that I is an ideal of R if I is a subring of R and I absorbs R .

Theorem 3.1.2 (Ideal Theorem). Let I be a subset of the ring R . Then I is an ideal of R if and only if the following four conditions holds:

- (i) $0_R \in I$.
- (ii) $a + b \in I$ for all $a, b \in I$.
- (iii) $ra \in I$ and $ar \in I$ for all $a \in I$ and $r \in R$.
- (iv) $-a \in I$ for all $a \in I$.

Proof. $\implies$: Suppose first that I is an ideal of R . By Definition 3.1.1 I absorbs R and I is a subring. Thus (iii) holds and by the Subring Theorem 1.7.2 also (i), (ii) and (iv) hold.

$\impliedby$: Suppose that (i)-(iv) hold. From (iii) we get that $ab \in I$ for all $a, b \in I$. Together with (i), (ii) and (iv) this shows that the four conditions of the Subring Theorem 1.7.2 hold for I . Thus I is a subring of R . By (iii), I absorbs R and so I is an ideal of R . $\square$

Example 3.1.3. (1) Let R be a ring, then both $\{0_R\}$ and R are ideals in R .

(2) $\{3n \mid n \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

(3) $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$.

- (4) Let F be a field and $a \in F$. Then $\{f \in F[x] \mid f^*(a) = 0_F\}$ is an ideal of $F[x]$.
- (5) Let R be a ring with identity, I an ideal in R . Then $\{f \in R[x] \mid f_i \in I \text{ for all } i \in \mathbb{N}\}$ is an ideal of R .
- (6) Let R and S be rings. Let I be an ideal of R and J an ideal of S . Then $I \times J$ is an ideal of $R \times S$. In particular, both $R \times \{0_S\}$ and $\{0_R\} \times S$ are ideals in $R \times S$.

Proof. See Exercise 3.1#2 □

Definition 3.1.4. Let R be a ring.

- (a) Let $a \in R$. Then $aR := \{ar \mid r \in R\}$.
- (b) Suppose R is commutative and $I \subseteq R$. Then I is called a *principal ideal* of R if $I = aR$ for some $a \in R$.

Theorem 3.1.5. Let R be a commutative ring and $a \in R$. Then aR is an ideal of R . Moreover, if R has an identity, then aR is the smallest ideal of R containing a , that is

- (a) $a \in aR$,
- (b) aR is an ideal of R , and
- (c) $aR \subseteq I$, whenever I is an ideal of R with $a \in I$.

Proof. To show that aR is an ideal of R let $b, c \in aR$ and $r \in R$. Then

$$b = as \quad \text{and} \quad c = at.$$

for some $s, t \in R$. Thus

$$\begin{aligned} 0_R &= a0_R \in aR, \\ b + c &= as + at = a(s + t) \in aR, \\ rb &= br = (as)r = a(sr) \in aR \\ -b &= -(as) = a(-s) \in aR. \end{aligned}$$

So by 3.1.2 aR is an ideal of R .

Suppose now that R has an identity. Then $a = a \cdot 1_R$ and so $a \in aR$.

Let I be any ideal of R containing a . Since $a \in I$ and I absorbs R , $ar \in I$ for all $r \in R$ and so $aR \subseteq I$. □

Definition 3.1.6. Let I be an ideal of the ring R . The relation $\equiv \pmod{I}$ on R is defined by

$$a \equiv b \pmod{I} \quad \text{if} \quad a - b \in I$$

Remark 3.1.7. Let R be a commutative ring and let $a, b, n \in R$. Then

$$a \equiv b \pmod{n} \iff a \equiv b \pmod{nR}$$

Proof.

$$\begin{aligned} & a \equiv b \pmod{n} \\ \iff & a - b = nk \text{ for some } k \in R \quad - \text{ 1.4.9} \\ \iff & a - b \in nR \quad - \text{ Definition of } nR, (3.1.4)(a) \\ \iff & a \equiv b \pmod{nR} \quad - \text{ Definition of ' } \equiv \pmod{I} \text{ ', 3.1.10} \end{aligned}$$

□

Theorem 3.1.8. Let I be an ideal of the ring R . Then ' $\equiv \pmod{I}$ ' is an equivalence relation on R .

Proof. We need to show that ' $\equiv \pmod{I}$ ' is reflexive, symmetric and transitive. Let $a, b, c \in R$.

Reflexive: By 1.2.9 $a - a = 0_R$ and by the Ideal Theorem $0_R \in I$. Thus $a - a \in I$ and so $a \equiv a \pmod{I}$ by definition of ' $\equiv \pmod{I}$ '.

Symmetric: Suppose $a \equiv b \pmod{I}$. Then $a - b \in I$ and so by the Ideal Theorem $-(a - b) \in I$. By 1.2.9 $b - a = -(a - b)$. Hence $b - a \in I$ and so $b \equiv a \pmod{I}$ by definition of ' $\equiv \pmod{I}$ '.

Transitive: Suppose $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a - b \in I$ and $b - c \in I$. Hence by the Ideal Theorem $(a - b) + (b - c) \in I$. As $a - c = (a - b) + (b - c)$ this gives $a - c \in I$. Thus $a \equiv c \pmod{I}$. □

Definition 3.1.9. Let R be a ring and I an ideal of R .

(a) Let $a \in R$. Then $a + I$ denotes the equivalence class of ' $\equiv \pmod{I}$ ' containing a , that is

$$a + I = \{b \in R \mid a \equiv b \pmod{I}\} = \{b \in R \mid a - b \in I\}$$

$a + I$ is called the coset of I in R containing a .

(b) R/I is the set of cosets of I in R , that is

$$R/I = \{a + I \mid a \in R\},$$

and R/I is the set of equivalence classes of ' $\equiv \pmod{I}$ '.

Theorem 3.1.10. Let R be ring and I an ideal of R . Let $a, b \in R$. Then the following statements are equivalent

- (a) $a = b + i$ for some $i \in I$.
- (b) $a - b = i$ for some $i \in I$.
- (c) $a - b \in I$.
- (d) $a \equiv b \pmod{I}$.
- (e) $b \in a + I$.
- (f) $(a + I) \cap (b + I) \neq \emptyset$.
- (g) $a + I = b + I$.
- (h) $a \in b + I$.
- (i) $b \equiv a \pmod{I}$.
- (j) $b - a \in I$.
- (k) $b - a = j$ for some $j \in I$.
- (l) $b = a + j$ for some $j \in I$.

Proof. (a) $\iff$ (b): By 1.2.8 $a = b + i$ if and only if $a - b = i$.

(b) $\iff$ (c): If $a - b = i$ and $i \in I$, then $a - b \in I$ by the Principal of Substitution. If $a - b \in I$, then (b) holds with $i = a - b$.

(c) $\iff$ (d): This holds by definition of ' $\equiv \pmod{I}$ '.

By 3.1.8 we know that ' $\equiv \pmod{I}$ ' is an equivalence relation. Also $a + I$ is the equivalence class of a and so Theorem A.6.5 implies that (d)-(i) are equivalent.

The result that (a)-(d) are equivalent applied with a and b interchanged shows that (i) - (l) are equivalent. $\square$

Theorem 3.1.11. *Let I be an ideal of the ring R .*

- (a) *Let $a \in R$. Then $a + I = \{a + i \mid i \in I\}$.*
- (b) *$0_R + I = I$. In particular, I is a coset of I in R .*
- (c) *Let A, B be cosets of I in R . Then either $A = B$ or $A \cap B = \emptyset$.*

Proof. (a) Let $a, b \in R$. By (3.1.10)(a),(h) we have $b \in a + I$ if and only if $b = a + i$ for some $i \in I$ and so if and only if $b \in \{a + i \mid i \in I\}$.

(b) By (a) $0_R + I = \{0_R + i \mid i \in I\} = \{i \mid i \in I\} = I$.

(c) Suppose $A \cap B \neq \emptyset$. By definition of 'coset', $A = a + I$ and $B = b + I$ for some $a, b \in I$. Then $(a + I) \cap (b + I) \neq \emptyset$ and (3.1.10)(f),(g) shows that $a + I = b + I$. Thus $A = B$. $\square$

Exercises 3.1:

3.1#1. Find all ideals in $\mathbb{Z}_8$.

3.1#2. Show that:

- (a) Let R be a ring, then both $\{0_R\}$ and R are ideals in R .
- (b) $\{3n \mid n \in \mathbb{Z}^+\}$ is an ideal of $\mathbb{Z}$.

- (c) $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$.
- (d) Let F be a field and $a \in F$. Then $\{f \in F[x] \mid f^*(a) = 0_F\}$ is an ideal of $F[x]$.
- (e) Let R be a ring with identity, I an ideal in R . Then $\{f \in R[x] \mid f_i \in I \text{ for all } i \in \mathbb{N}\}$ is an ideal of R .
- (f) Let R and S be rings. Let I be an ideal of R and J an ideal of S . Then $I \times J$ is an ideal of R . In particular, both $R \times \{0_S\}$ and $\{0_R\} \times S$ are ideals in $R \times S$.

3.1#3. Let $I_1, I_2, \dots, I_n$ be ideals in the ring R . Show that $I_1 + I_2 + \dots + I_n$ is the smallest ideal of R containing $I_1, I_2, \dots, I_n$ and I_n .

3.1#4. Is the set $J = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ an ideal of the ring $M_2(\mathbb{R})$ of 2×2 matrices over $\mathbb{R}$?

3.1#5. Let F be a field and I an ideal of $F[x]$. Show that I is a principal ideal. *Hint:* If $I \neq \{0_F\}$ choose $d \in I$ with $d \neq 0_F$ and $\deg(d)$ minimal. Show that $I = F[x]d$.

3.1#6. Let $\Phi : R \rightarrow S$ be a homomorphism of rings and let J be an ideal of S . Put $I = \{a \in R \mid \Phi(a) \in J\}$. Show that I is an ideal of R .

3.1#7. Let $I = \{f \in \mathbb{Z}[x] \mid f_0 \in 2\mathbb{Z}\}$.

- (a) Show that I is an ideal in $\mathbb{Z}[x]$.
- (b) Show that I is not a principal ideal, that is $I \neq f\mathbb{Z}[x]$ for all $f \in \mathbb{Z}[x]$.

3.2 Quotient Rings

Theorem 3.2.1. Let I be an ideal of R and $a, b, \tilde{a}, \tilde{b} \in R$ with

$$a + I = \tilde{a} + I \quad \text{and} \quad b + I = \tilde{b} + I.$$

Then

$$(a + b) + I = (\tilde{a} + \tilde{b}) + I \quad \text{and} \quad ab + I = \tilde{a}\tilde{b} + I.$$

Proof. Since $a + I = \tilde{a} + I$, we have $\tilde{a} = a + i$ for some $i \in I$, see 3.1.10. Similarly $\tilde{b} = b + j$ for some $j \in I$.

Thus

$$\tilde{a} + \tilde{b} = (a + i) + (b + j) = (a + b) + (i + j).$$

Since $i, j \in I$ and I is closed under addition, $i + j \in I$ and so by 3.1.10 $(a + b) + I = (\tilde{a} + \tilde{b}) + I$.

Also

$$\tilde{a}\tilde{b} = (a + i)(b + j) = ab + (aj + ib + ij)$$

Since $i, j \in I$ and I absorbs R we conclude that aj, ib and ij all are in I . Since I is closed under addition this implies that $aj + ib + ij \in I$ and so $ab + I = \tilde{a}\tilde{b} + I$ by 3.1.10. $\square$

Definition 3.2.2. Let I be an ideal of the ring R . We define an addition $\oplus$ and multiplication $\odot$ on R/I by

$$(a + I) \oplus (b + I) = (a + b) + I \quad \text{and} \quad (a + I) \odot (b + I) = ab + I$$

for all $a, b \in R$.

Note that this is well-defined by 3.2.1.

Remark 3.2.3. (a) Let R be a commutative ring and $n \in R$. Then $R_n = R/nR$.

(b) Let F be a field and $p \in F[x]$. Then $F[x]/(p) = F[x]/pF[x]$.

Proof. (a) By Remark 3.1.7 the relations ' $\equiv \pmod{n}$ ' and ' $\equiv \pmod{nR}$ ' are the same. So also their sets of equivalence classes R_n and R/nR are the same.

(b) Since $F[x]/(p) = F[x]_p$ this is a special case of (a). □

Theorem 3.2.4. Let R be a ring and I an ideal of R

(a) The function $\pi : R \rightarrow R/I$, $a \mapsto a + I$ is a surjective homomorphism.

(b) $(R/I, \oplus, \odot)$ is a ring.

(c) $0_{R/I} = 0_R + I = I$.

(d) If R is commutative, then R/I is commutative.

(e) If R has an identity, then R/I has an identity and $1_{R/I} = 1_R + I$.

Proof. (a) Let $a, b \in R$. Then

$$\pi(a + b) \stackrel{\text{Def } \pi}{=} (a + b) + I \stackrel{\text{Def } \oplus}{=} (a + I) \oplus (b + I) \stackrel{\text{Def } \pi}{=} \pi(a) \oplus \pi(b)$$

and

$$\pi(ab) \stackrel{\text{Def } \pi}{=} ab + I \stackrel{\text{Def } \odot}{=} (a + I) \odot (b + I) \stackrel{\text{Def } \pi}{=} \pi(a) \odot \pi(b)$$

So π is a homomorphism. Let $u \in R/I$. By definition, $R/I = \{a + I \mid a \in R\}$ and so there exists $a \in R$ with $u = a + I$. Thus $\pi(a) = a + I = u$ and so π is surjective.

(b), (c) and (d): By (a) π is a surjective homomorphism. Thus we can apply D.0.1 and conclude that (b), (c) and (d) hold.

(e): By (a) π is a surjective homomorphism. Thus (e) follows from (1.11.9)(a) □

Definition 3.2.5. Let $f : R \rightarrow S$ be a homomorphism of rings. Then

$$\text{Ker } f := \{a \in R \mid f(a) = 0_S\}.$$

$\text{Ker } f$ is called the kernel of f .

Theorem 3.2.6. Let $f : R \rightarrow S$ be a homomorphism of rings. Then $\text{Ker } f$ is an ideal of R .

Proof. By definition, $\text{Ker } f$ is a subset of R . We will now verify the four conditions of the Ideal Theorem 3.1.2. Let $r \in R$. By definition of $\text{Ker } f$ we have

$$(*) \quad r \in \text{Ker } f \quad \Longleftrightarrow \quad f(r) = 0_S.$$

Let $a, b \in \text{Ker } f$. By $(*)$

$$(**) \quad f(a) = 0_S \quad \text{and} \quad f(b) = 0_S.$$

$$(i) \quad f(0_R) \stackrel{(1.11.7)(a)}{=} 0_S \text{ and so } 0_R \in \text{Ker } f \text{ by } (*).$$

$$(ii) \quad f(a+b) \stackrel{f \text{ hom}}{=} f(a) + f(b) \stackrel{(**)}{=} 0_S + 0_S \stackrel{\mathbf{Ax 4}}{=} 0_S \text{ and so } a+b \in \text{Ker } f \text{ by } (*).$$

$$(iii) \quad f(ra) \stackrel{f \text{ hom}}{=} f(r)f(a) \stackrel{(**)}{=} f(r)0_S \stackrel{(1.2.9)(c)}{=} 0_S \text{ and so } ra \in \text{Ker } f \text{ by } (*).$$

Similarly, $ar \in \text{Ker } f$.

$$(iv) \quad f(-a) \stackrel{(1.11.7)(b)}{=} -f(a) \stackrel{(**)}{=} -0_S \stackrel{(1.2.9)(a)}{=} 0_S \text{ and so } -a \in \text{Ker } f \text{ by } (*). \quad \square$$

Example 3.2.7. Define

$$\Phi: \mathbb{R}[x] \rightarrow \mathbb{C}, \quad f \mapsto f^*(i)$$

Show that Φ is a surjective homomorphism and compute $\text{Ker } \Phi$.

Let $f, g \in \mathbb{R}[x]$, then

$$\begin{aligned} \Phi(f+g) &= (f+g)^*(i) && \text{-- Definition of } \Phi \\ &= f^*(i) + g^*(i) && \text{-- (2.7.4)(b)} \\ &= \Phi(f) + \Phi(g) && \text{-- Definition of } \Phi, \text{ twice} \end{aligned}$$

and

$$\begin{aligned} \Phi(fg) &= (fg)^*(i) && \text{-- Definition of } \Phi \\ &= f^*(i)g^*(i) && \text{-- (2.7.4)(b)} \\ &= \Phi(f)\Phi(g) && \text{-- Definition of } \Phi, \text{ twice} \end{aligned}$$

So Φ is a homomorphism. (Alternatively, consider the homomorphism $\rho = \text{id}_{\mathbb{R}, \mathbb{C}} : \mathbb{R} \rightarrow \mathbb{C}, r \mapsto r$ from Example (1.11.2)(2). Then Φ is the function ρ_i from Theorem 2.6.1. So Φ is a homomorphism.)

To show that f is surjective, let $c \in \mathbb{C}$. Then $c = a + bi$ for some $a, b \in \mathbb{R}$. Thus $\Phi(a + bx) = a + bi = c$ and so Φ is surjective.

To compute $\text{Ker } f$ let $f \in \mathbb{R}[x]$. We need to determine when $f^*(i) = 0$. According to the Division algorithm, $f = (x^2 + 1) \cdot q + r$, where $q, r \in \mathbb{R}[x]$ with $\deg(r) < \deg(x^2 + 1) = 2$. Then $r = a + bx$ for some $a, b \in \mathbb{R}$ and so

$$(*) \quad f^*(i) = \left((x^2 + 1) \cdot q + r \right)^*(i) \stackrel{(2.7.4)(b)}{=} (i^2 + 1) \cdot q^*(i) + r^*(i) = 0 \cdot q^*(i) + (a + bi) = a + bi$$

It follows that

$$\begin{array}{lll}
 & f \in \text{Ker}\Phi & \\
 \iff & \Phi(f) = 0 & \text{-- definition of } \text{Ker}\Phi \\
 \iff & f^*(i) = 0 & \text{-- definition of } \Phi \\
 \iff & a + bi = 0 & \text{-- } (*) \\
 \iff & a = 0 \text{ and } b = 0 & \text{-- Property of } \mathbb{C} \\
 \iff & a + bx = 0 & \text{-- definition of polynomial ring} \\
 \iff & r = 0 & \text{-- } r = a + bx \\
 \iff & x^2 + 1 \mid f & \text{-- 2.3.4} \\
 \iff & f = (x^2 + 1) \cdot q \text{ for some } q \in \mathbb{R}[x] & \text{-- Definition of 'divide'} \\
 \iff & f \in (x^2 + 1)\mathbb{R}[x] & \text{-- Definition of } (x^2 + 1)\mathbb{R}[x]
 \end{array}$$

Thus $\text{Ker}\Phi = (x^2 + 1)\mathbb{R}[x]$.

Theorem 3.2.8. *Let $f : R \rightarrow S$ be a homomorphism of rings.*

(a) *Let $a, b \in R$. Then*

$$\begin{array}{ll}
 & f(a) = f(b) \\
 \iff & a - b \in \text{Ker } f \\
 \iff & a + \text{Ker } f = b + \text{Ker } f
 \end{array}$$

(b) *f is injective if and only if $\text{Ker } f = \{0_R\}$.*

Proof. (a)

$$\begin{array}{lll}
 & f(a) = f(b) & \\
 \iff & f(a) - f(b) = 0_S & \text{-- (1.2.9)(f)} \\
 \iff & f(a - b) = 0_S & \text{-- (1.11.7)(c)} \\
 \iff & a - b \in \text{Ker } f & \text{-- Definition of } \text{Ker } f \\
 \iff & a + \text{Ker } f = b + \text{Ker } f & \text{-- 3.1.10}
 \end{array}$$

(b) $\implies$: Suppose f is injective and let $a \in R$. Then

$$\begin{array}{lll}
 & a \in \text{Ker } f & \\
 \iff & f(a) = 0_S & \text{-- Definition of } \text{Ker } f \\
 \iff & f(a) = f(0_R) & \text{-- (1.11.7)(a)} \\
 \iff & a = 0_R & \text{-- } f \text{ is injective}
 \end{array}$$

Thus $\text{Ker } f = \{0_R\}$.

$\Leftarrow$: Suppose $\text{Ker } f = \{0_R\}$ and let $a, b \in R$ with $f(a) = f(b)$. Then by (a) $a - b \in \text{Ker } f$. As $\text{Ker } f = \{0_R\}$ this gives $a - b = 0_R$, so $a = b$ by (1.2.9)(f). Hence f is injective. $\square$

Theorem 3.2.9 (First Isomorphism Theorem). *Let $f : R \rightarrow S$ be a homomorphism of rings. Recall that $\text{Im } f = \{f(a) \mid a \in R\}$. Then $\text{Im } f$ is a subring of S and the function*

$$\bar{f} : R/\text{Ker } f \mapsto \text{Im } f, \quad a + \text{Ker } f \mapsto f(a)$$

is a well-defined isomorphism of rings. In particular $R/\text{Ker } f$ and $\text{Im } f$ are isomorphic rings.

Proof. By 1.11.11 $\text{Im } f$ is a subring of S . Let $a, b \in R$. By 3.2.8 $f(a) = f(b)$ if and only if $a + \text{Ker } f = b + \text{Ker } f$. The forward direction shows that $\bar{f}$ is injective and backwards direction shows that $\bar{f}$ is well-defined.

If $s \in \text{Im } f$, then $s = f(a)$ for some $a \in R$ and so $\bar{f}(a + \text{Ker } f) = f(a) = s$. Hence $\bar{f}$ is surjective.

It remains to verify that $\bar{f}$ is a homomorphism. We compute

$$\begin{aligned} \bar{f}((a + \text{Ker } f) \oplus (b + \text{Ker } f)) &\stackrel{\text{Def } \oplus}{=} \bar{f}((a + b) + \text{Ker } f) \stackrel{\text{Def } \bar{f}}{=} f(a + b) \\ &\stackrel{f \text{ hom}}{=} f(a) + f(b) \stackrel{\text{Def } \bar{f}}{=} \bar{f}(a + \text{Ker } f) + \bar{f}(b + \text{Ker } f) \end{aligned}$$

and

$$\begin{aligned} \bar{f}((a + \text{Ker } f) \odot (b + \text{Ker } f)) &\stackrel{\text{Def } \odot}{=} \bar{f}(ab + \text{Ker } f) \stackrel{\text{Def } \bar{f}}{=} f(ab) \\ &\stackrel{f \text{ hom}}{=} f(a) \cdot f(b) \stackrel{\text{Def } \bar{f}}{=} \bar{f}(a + \text{Ker } f) \cdot \bar{f}(b + \text{Ker } f) \end{aligned}$$

and so $\bar{f}$ is a homomorphism. $\square$

Example 3.2.10. Apply the Isomorphism Theorem to the homomorphism

$$\Phi : \mathbb{R}[x] \rightarrow \mathbb{C}, \quad f \mapsto f^*(i)$$

from 3.2.7.

By 3.2.7 Φ is a surjective homomorphism and $\text{Ker } \Phi = (x^2 + 1)\mathbb{R}[x]$. Since Φ is surjective we have $\text{Im } \Phi = \mathbb{C}$. By the isomorphism theorem $\mathbb{R}[x]/\text{Ker } \Phi$ is isomorphic to $\text{Im } \Phi$. Thus $\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$ is isomorphic to $\mathbb{C}$.

By 3.2.3 $\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x] = \mathbb{R}[x]/(x^2 + 1) = \mathbb{R}_{x^2+1}[\alpha]$. Thus

$$\mathbb{R}_{x^2+1}[\alpha] \text{ is isomorphic to } \mathbb{C}.$$

Note that the already observed this in 2.11.4

Example 3.2.11. Let n and m be positive integers with $\gcd(n, m) = 1$. Apply the isomorphism theorem to the homomorphism

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m, \quad a \mapsto ([a]_n, [a]_m)$$

We first compute $\text{Ker } f$

$$\begin{aligned}
 & a \in \text{Ker } f \\
 \iff & f(a) = 0_{\mathbb{Z}_n \times \mathbb{Z}_m} && \text{-- definition of } \text{Ker } f \\
 \iff & f(a) = ([0]_n, [0]_m) && \text{-- (1.1.7)(b), (1.6.4)(b)} \\
 \iff & ([a]_n, [a]_m) = ([0]_n, [0]_m) && \text{-- definition of } f \\
 \iff & [a]_n = [0]_n \quad \text{and} \quad [a]_m = [0]_m && \text{-- A.4.2} \\
 \iff & n|a-0 \quad \text{and} \quad m|a-0 && \text{-- 1.4.9} \\
 \iff & n|a \quad \text{and} \quad m|a && \text{-- (1.2.9)(b)} \\
 \iff & nm|a && \text{-- } \gcd(n, m) = 1, \text{ Exercise 1.9\#1} \\
 \iff & a = nmk \quad \text{for some } k \in \mathbb{Z} && \text{-- definition of 'divide'} \\
 \iff & a \in nm\mathbb{Z} && \text{-- definition of } nm\mathbb{Z}
 \end{aligned}$$

Thus $\text{Ker } f = nm\mathbb{Z}$ and so

$$\mathbb{Z}/\text{Ker } f = \mathbb{Z}/nm\mathbb{Z} \stackrel{(3.2.3)(a)}{=} \mathbb{Z}_{nm}.$$

By the First Isomorphism Theorem $\mathbb{Z}/\text{Ker } f$ is isomorphic to $\text{Im } f$ and so

(*) $\mathbb{Z}_{nm}$ is isomorphic to $\text{Im } f$.

Thus

$$|\text{Im } f| = |\mathbb{Z}_{nm}| \stackrel{(1.5.7)(c)}{=} nm.$$

Also

$$|\mathbb{Z}_n \times \mathbb{Z}_m| \stackrel{(F.1.8)(b)}{=} |\mathbb{Z}_n| \cdot |\mathbb{Z}_m| \stackrel{(1.5.7)(c)}{=} nm,$$

Hence $|\text{Im } f| = |\mathbb{Z}_n \times \mathbb{Z}_m|$. Since $\text{Im } f \subseteq \mathbb{Z}_n \times \mathbb{Z}_m$ this gives $\text{Im } f = \mathbb{Z}_n \times \mathbb{Z}_m$. Hence (*) implies

$$\mathbb{Z}_{nm} \quad \text{is isomorphic to} \quad \mathbb{Z}_n \times \mathbb{Z}_m.$$

Exercises 3.2:

3.2\#1. Consider the function

$$\Phi: \mathbb{Q}[x] \rightarrow \mathbb{R}, \quad f \mapsto f^*(\sqrt{5})$$

Put $p := x^2 - 5 \in \mathbb{Q}[x]$ and $\mathbb{Q}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$.

- (a) Show that Φ is a homomorphism of rings.
- (b) Let $f \in \mathbb{Q}[x]$ and let r be the remainder of f when divided by p . Show that there exists $a, b \in \mathbb{Q}$ with $p = a + bx$ and that $\Phi(f) = a + b\sqrt{5}$.
- (c) Show that $\text{Ker}\Phi = p\mathbb{Q}[x]$.
- (d) Show that $\text{Im}\Phi = \mathbb{Q}[\sqrt{5}]$.
- (e) Show that $\mathbb{Q}[\sqrt{5}]$ is a subring of $\mathbb{R}$.
- (f) Show that $\mathbb{Q}[x]/p\mathbb{Q}[x]$ is isomorphic to $\mathbb{Q}[\sqrt{5}]$.

3.2#2. Let R be a ring and I an ideal in R . Show that R/I is commutative if and only if $ab - ba \in I$ for all $a, b \in I$.

Appendix A

Set, Relations and Functions

A.1 Logic

In this section we will provide an informal discussion of logic. A statement is a sentence which is either true or false, for example

- (1) $1 + 1 = 2$
- (2) $\sqrt{2}$ is a rational number.
- (3) π is a real number.
- (4) Exactly 1323 bald eagles were born in 2000 BC,

all are statements. Statement (1) and (3) are true. Statement (2) is false. Statement (4) is probably false, but verification might be impossible. It nevertheless is a statement.

Let P and Q be statements.

“ P and Q ” is the statement that P is true and Q is true. We illustrate the statement P and Q in the following *truth table*

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

“ P or Q ” is the statement that at least one of P and Q is true:

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

So “ P or Q ” is false exactly when both P and Q are false.

“not- P ” (pronounced ‘not P ’ or ‘negation of P ’) is the statement that P is false:

P	not- P
T	F
F	T

So not- P is true if P is false. And not- P is false if P is true.

“ $P \implies Q$ ” (pronounced “ P implies Q ”) is the statement “If P is true, then Q is true”:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note here that if P is true, then “ $P \implies Q$ ” is true if and only if Q is true. But if P is false, then “ $P \implies Q$ ” is true, regardless whether Q is true or false. Consider the statement “ Q or not- P ”:

P	Q	not- P	Q or not- P
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

(*) “ Q or not- P ” is true if and only “ $P \implies Q$ ” is true.

This shows that one can express the logical operator " $\implies$ " in terms of the operators "not-" and "or".

" $P \iff Q$ " (pronounced " P is equivalent to Q ") is the statement that P is true if and only if Q is true.:

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

So $P \iff Q$ is true if either both P and Q are true, or both P and Q are false. Hence

(**) " $P \iff Q$ " is true if and only " $(P \text{ and } Q) \text{ or } (\text{not-}P \text{ and not-}Q)$ " is true.

To show that P and Q are equivalent one often proves that P implies Q and that Q implies P . Indeed the truth table

P	Q	$P \implies Q$	$Q \implies P$	$(P \implies Q) \text{ and } (Q \implies P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

shows that

(***) " $P \iff Q$ " is true if and only " $(P \implies Q) \text{ and } (Q \implies P)$ " is true.

Often, rather than showing that a statement is true, one shows that the negation of the statement is false (This is called a proof by contradiction). To do this it is important to be able to determine the negation of statement. The negation of not- P is P :

P	not- P	not-(not- P)
T	F	T
F	T	F

The negation of " $P \text{ and } Q$ " is " $\text{not-}P \text{ or not-}Q$ ":

P	Q	P and Q	not- $(P$ and $Q)$	not- P	not- Q	not- P or not- Q
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	F	T

The negation of " P or Q " is "not- P and not- Q ":

P	Q	P or Q	not- $(P$ or $Q)$	not- P	not- Q	not- P and not- Q
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	F	T

The statement " $\text{not-}Q \implies \text{not-}P$ " is called the *contrapositive* of the statement " $P \implies Q$ ". It is equivalent to the statement " $P \implies Q$ ":

P	Q	$P \implies Q$	not- Q	not- P	not- $Q \implies \text{not-}P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The statement " $\text{not-}P \iff \text{not-}Q$ " is called the contrapositive of the statement " $P \iff Q$ ". It is equivalent to the statement " $P \iff Q$ ":

P	Q	$P \iff Q$	not- P	not- Q	not- $P \iff \text{not-}Q$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

The statement “ $Q \implies P$ ” is called the *converse* of the statement “ $P \implies Q$ ”. In general the converse is not equivalent to the original statement. For example the statement if $x = 0$ then x is an even integer is true. But the converse (if x is an even integer, then $x = 0$) is not true.

Theorem A.1.1 (Principal of Substitution). *Let $\Phi(x)$ be formula involving a variable x . For an object d let $\Phi(d)$ be the formula obtained from $\Phi(x)$ by replacing all occurrences of x by d . If a and b are objects with $a = b$, then $\Phi(a) = \Phi(b)$.*

Proof. This should be self evident. For an actual proof and the definition of a formula consult your favorite logic book. $\square$

Example A.1.2. Let $\Phi(x) = x^2 + 3 \cdot x + 4$.

If $a = 2$, then

$$a^2 + 3 \cdot a + 4 = 2^2 + 3 \cdot 2 + 4$$

Notation A.1.3. Let $P(x)$ be a statement involving the variable x .

- (a) “for all $x : P(x)$ ” is the statement that for all objects a the statements $P(a)$ is true. Instead of “for all $x : P(x)$ ” we will also use “ $\forall x : P(x)$ ”, “ $P(x)$ is true for all x ”, “ $P(x)$ holds for all x ” or similar phrases.
- (b) “there exists $x : P(x)$ ” is the statement there exists an object a such that the statements $P(a)$ is true. Instead of “there exists $x : P(x)$ ” we will also use “ $\exists x : P(x)$ ”, “ $P(x)$ is true for some x ”, “There exists x with $P(x)$ ” or similar phrases.

Example A.1.4. “for all $x : x + x = 2x$ ” is a true statement.

“for all $x : x^2 = 2$ ” is a false statement.

“there exists $x : x^2 = 2$ ” is a true statement.

“ $\exists x : x^2 = 2$ and x is an integer” is false statement

Notation A.1.5. Let $P(x)$ be a statement involving the variable x .

- (a) “There exists at most one $x : P(x)$ ” is the statement

$$\text{for all } x : \text{for all } y : \quad P(x) \text{ and } P(y) \implies x = y$$

- (b) “There exists a unique $x : P(x)$ ” is the statement

$$\text{there exists } x : \text{for all } y : \quad P(y) \iff y = x$$

Example A.1.6. “There exists at most one $x : (x^2 = 1 \text{ and } x \text{ is a real number})$ ” is false since $1^2 = 1$ and $(-1)^2 = 1$, but $1 \neq -1$.

“There exists a unique $x : (x^3 = -1 \text{ and } x \text{ is a real number})$ ” is true since $x = -1$ is the only element in $\mathbb{R}$ with $x^3 = -1$.

“There exists at most one $x : (x^2 = -1 \text{ and } x \text{ is a real number})$ ” is true, since there does not exist any element x in $\mathbb{R}$ with $x^2 = -1$.

“There exists a unique $x : (x^2 = -1 \text{ and } x \text{ is a real number})$ ” is false, since there does not exist any element x in $\mathbb{R}$ with $x^2 = -1$.

Theorem A.1.7. *Let $P(x)$ be a statement involving the variable x . Then*

$$\begin{aligned} & \left(\text{there exists } x : P(x) \right) \quad \text{and} \quad \left(\text{there exists at most one } x : P(x) \right) \\ & \text{if and only if} \\ & \text{there exists a unique } x : P(x) \end{aligned}$$

Proof. See A.2.2 in the appendix.. □

A.2 Rules of Logic

In the following we collect a few statements which are always true.

Theorem A.2.1. *Let P , Q and R be statements, let T be a true statement and F a false statement. Then each of the following statements holds.*

$$\text{(LR 1) } F \implies P.$$

$$\text{(LR 2) } P \implies T.$$

$$\text{(LR 3) } \text{not}-(\text{not } P) \iff P.$$

$$\text{(LR 4) } (\text{not } P \implies F) \implies P.$$

$$\text{(LR 5) } P \text{ or } T.$$

$$\text{(LR 6) } \text{not}-(P \text{ and } F).$$

$$\text{(LR 7) } (P \text{ and } T) \iff P.$$

$$\text{(LR 8) } (P \text{ or } F) \iff P.$$

$$\text{(LR 9) } (P \text{ and } P) \iff P.$$

$$\text{(LR 10) } (P \text{ or } P) \iff P.$$

$$\text{(LR 11) } P \text{ or not } P.$$

$$\text{(LR 12) } \text{not}-(P \text{ and not } P).$$

$$(LR\ 13) \ (P \text{ and } Q) \iff (Q \text{ and } P).$$

$$(LR\ 14) \ (P \text{ or } Q) \iff (Q \text{ or } P).$$

$$(LR\ 15) \ (P \iff Q) \iff ((P \text{ and } Q) \text{ or } (\text{not } P \text{ and } \text{not } Q))$$

$$(LR\ 16) \ (P \implies Q) \iff (\text{not } P \text{ or } Q).$$

$$(LR\ 17) \ \text{not } (P \implies Q) \iff (P \text{ and } \text{not } Q).$$

$$(LR\ 18) \ (P \text{ and } (P \implies Q)) \implies Q.$$

$$(LR\ 19) \ ((P \implies Q) \text{ and } (Q \implies P)) \iff (P \iff Q).$$

$$(LR\ 20) \ (P \iff Q) \implies (P \implies Q).$$

$$(LR\ 21) \ (P \implies Q) \iff (\text{not } Q \implies \text{not } P)$$

$$(LR\ 22) \ (P \iff Q) \iff (\text{not } P \iff \text{not } Q).$$

$$(LR\ 23) \ \text{not } (P \text{ and } Q) \iff (\text{not } P \text{ or } \text{not } Q)$$

$$(LR\ 24) \ \text{not } (P \text{ or } Q) \iff (\text{not } P \text{ and } \text{not } Q)$$

$$(LR\ 25) \ ((P \text{ and } Q) \text{ and } R) \iff (P \text{ and } (Q \text{ and } R)).$$

$$(LR\ 26) \ ((P \text{ or } Q) \text{ or } R) \iff (P \text{ or } (Q \text{ or } R)).$$

$$(LR\ 27) \ ((P \text{ and } Q) \text{ or } R) \iff ((P \text{ or } R) \text{ and } (Q \text{ or } R)).$$

$$(LR\ 28) \ ((P \text{ or } Q) \text{ and } R) \iff ((P \text{ and } R) \text{ or } (Q \text{ and } R)).$$

$$(LR\ 29) \ ((P \implies Q) \text{ and } (Q \implies R)) \implies (P \implies R)$$

$$(LR\ 30) \ ((P \iff Q) \text{ and } (Q \iff R)) \implies (P \iff R)$$

Proof. If any of these statements are not evident to you, you should use a truth table to verify it. $\square$

Theorem A.2.2. *Let $P(x)$ be a statement involving the variable x . Then*

$$(\text{there exists } x : P(x)) \quad \text{and} \quad (\text{there exists at most one } x : P(x))$$

if and only if

there exists a unique $x : P(x)$

Proof. $\implies$: Suppose first that

$$\left(\text{there exists } x : P(x) \right) \quad \text{and} \quad \left(\text{there exists at most one } x : P(x) \right)$$

holds. By definition of “There exists:” we conclude that there exists an object a such that

$$(*) \quad P(a) \text{ is true}$$

Also by definition of “There exists at most one”:

$$(**) \quad \text{for all } x : \text{for all } y : \quad P(x) \text{ and } P(y) \quad \implies \quad x = y.$$

From $(**)$ and the definition of “for all x :” we get

$$(* * *) \quad \text{for all } y : \quad P(a) \text{ and } P(y) \quad \implies \quad a = y$$

By (A.2.1)(LR 7) $P \iff (T \text{ and } P)$ whenever P is a statement and T is a true statement. Since $P(a)$ is a true statement we conclude that

$$\text{for all } y : \quad P(y) \quad \iff \quad P(a) \text{ and } P(y).$$

By (A.2.1)(LR 20) $P \equiv Q$ implies $P \implies Q$ and so we conclude that

$$(+) \quad \text{for all } y : \quad P(y) \quad \implies \quad P(a) \text{ and } P(y)$$

By (A.2.1)(LR 29)

$$\left((P \implies Q) \text{ and } (Q \implies T) \right) \quad \implies \quad (P \implies Q)$$

Together with $(+)$ and $(* * *)$ this gives

$$(++) \quad \text{for all } y : \quad P(y) \quad \implies \quad a = y.$$

If $a = y$, then since $P(a)$ is true, the Principal of Substitution shows that $P(y)$ is true. Thus

$$(+++) \quad \text{for all } y : \quad a = y \quad \implies \quad P(y)$$

By (A.2.1)(LR 20) $P \equiv Q$ if and only if $P \implies Q$ and $Q \implies P$. Together with $(++)$ and $(+++)$ we get

$$\text{for all } y : \quad P(y) \quad \iff \quad a = y.$$

Thus by definition of ‘there exists x :’ this gives

$$\text{there exists } x : \text{ for all } y : \quad P(y) \quad \Longleftrightarrow \quad x = y.$$

Hence the definition of “There exists a unique” gives

$$\text{There exists a unique } x : \quad P(x).$$

$\Leftarrow$: Suppose next that

$$\text{There exists a unique } x : \quad P(x)$$

holds. Then by definition of “There exists a unique”:

$$\text{there exists } x : \text{ for all } y : \quad P(y) \Longleftrightarrow x = y.$$

and so there exists an object a such that

$$(\#) \quad \text{for all } y : P(y) \quad \Longleftrightarrow \quad a = y.$$

In particular, by definition of “for all y ”:

$$P(a) \quad \Longleftrightarrow \quad a = a$$

Since $a = a$ is true, we conclude that $P(a)$ is true. Thus

$$(\#\#) \quad \text{there exists } x : \quad P(x).$$

holds.

Suppose “ $P(x)$ and $P(y)$ “ is true. Then $P(x)$ is true and $(\#)$ shows that $x = a$. Also $P(y)$ is true and $(\#)$ gives $y = a$. From $x = a$ and $y = a$ we get $x = y$ by the Principal of Substitution. We proved that

$$\text{for all } x : \text{ for all } y : \quad P(x) \text{ and } P(y) \implies x = y.$$

and so the definition of “There exists at most one” gives

$$(\#\#\#) \quad \text{There exists at most one } x : \quad P(x).$$

From $(\#\#)$ and $(\#\#\#)$ we have

$$\text{there exists } x : P(x) \quad \text{and} \quad \text{there exists at most one } x : P(x).$$

□

Theorem A.2.3. *Let S be a set, let $P(x)$ be a statement involving the variable x and $\Phi(x)$ a formula such that $\Phi(s)$ is defined for all s in S for which $P(s)$ is true. Then there exists a set, denoted by $\{\Phi(s) \mid s \in S \text{ and } P(s)\}$ such that*

$$t \in \{\Phi(s) \mid s \in S \text{ and } P(s)\} \iff \text{there exists } s \in S : (P(s) \text{ and } t = \Phi(s))$$

Proof. Define

$$(*) \quad \{\Phi(s) \mid s \in S \text{ and } P(s)\} := \{\Phi(s) \mid s \in \{r \in S \mid P(r)\}\}$$

Then

$$\begin{aligned} & t \in \{\Phi(s) \mid s \in S \text{ and } P(s)\} \\ \iff & t \in \{\Phi(s) \mid s \in \{r \in S \mid P(r)\}\} && \text{By } (*) \\ \iff & \text{there exists } s \in \{r \in S \mid P(r)\} \text{ with } t = \Phi(s) && \text{A.3.9} \\ \iff & \text{there exists } s \text{ with } \left(s \in \{r \in S \mid P(r)\} \text{ and } t = \Phi(s) \right) && \text{definition of 'there exists } s \in' \text{ see A.3.7} \\ \iff & \text{there exists } s \text{ with } \left((s \in S \text{ and } P(s)) \text{ and } t = \Phi(s) \right) && \text{A.3.5} \\ \iff & \text{there exists } s \text{ with } \left(s \in S \text{ and } (P(s) \text{ and } t = \Phi(s)) \right) && \text{Rule of Logic: (A.2.1)(LR 25) :} \\ & (P \text{ and } (Q \text{ and } R)) \iff ((P \text{ and } Q) \text{ and } R) \\ \iff & \text{there exists } s \in S \text{ with } (P(s) \text{ and } t = \Phi(s)) && \text{definition of 'there exists } s \in' \text{ see A.3.7} \end{aligned}$$

□

Exercises A.2:

A.2#1. Convince yourself that each of the statement in A.2.1 are true.

A.2#2. Use a truth table to verify the statements LR 17, LR 26, LR 27 and LR 28 in A.2.1.

A.3 Sets

First of all any *set* is a collection of objects.

For example

$$\mathbb{Z} := \{\dots, -4, -3, -2, -1, -0, 1, 2, 3, 4, \dots\}$$

is the set of integers. If S is a set and x an object we write $x \in S$ if x is a member of S and $x \notin S$ if x is not a member of S . In particular,

(*) For all x exactly one of $x \in S$ and $x \notin S$ holds.

Not all collections of objects are sets. Suppose for example that the collection $\mathcal{B}$ of all sets is a set. Then $\mathcal{B} \in \mathcal{B}$. This is rather strange, but by itself not a contradiction. So let's make this example a little bit more complicated. We call a set S nice if $S \notin S$. Let $\mathcal{D}$ be the collection of all nice sets and suppose $\mathcal{D}$ is a set. Then

$$\mathcal{D} \in \mathcal{D} \xLeftrightarrow{\text{Definition of } \mathcal{D}} \mathcal{D} \text{ is nice} \xLeftrightarrow{\text{Definition of nice}} \mathcal{D} \notin \mathcal{D}.$$

which contradicts the basis property of a set.

Theorem A.3.1. *Let A and B be sets. Then*

$$(A = B) \iff \left(\text{for all } x : (x \in A) \iff (x \in B) \right)$$

Proof. Naively this just says that two sets are equal if and only if they have the same members. In actuality this turns out to be one of the axioms of set theory. $\square$

Definition A.3.2. *Let A and B be sets. We say that A is subset of B and write $A \subseteq B$ if*

$$\text{for all } x : (x \in A) \implies (x \in B)$$

In other words, A is a subset of B if all the members of A are also members of B .

Theorem A.3.3. *Let A and B sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Proof.

$$\begin{aligned} & A \subseteq B \text{ and } B \subseteq A \\ \iff & \text{for all } x : (x \in A \implies x \in B) \text{ and } (x \in B \implies x \in A) && \text{--definition of subset} \\ \iff & \text{for all } x : x \in A \iff x \in B \\ & \text{--(A.2.1)(LR19) : } \left((P \implies Q) \text{ and } (Q \implies P) \right) \iff (P \iff Q) \\ \iff & A = B && \text{-- A.3.1} \end{aligned}$$

$\square$

Theorem A.3.4. *Let t be an object. Then there exists a set, denoted by $\{t\}$ such that*

$$\text{for all } x : x \in \{t\} \iff x = t$$

Proof. This is an axiom of Set Theory. $\square$

Theorem A.3.5. *Let S be a set and let $P(x)$ be a statement involving the variable x . Then there exists a set, denoted by $\{s \in S \mid P(s)\}$ such that*

$$\text{for all } x : \quad x \in \{s \in S \mid P(s)\} \iff x \in S \text{ and } P(x)$$

Proof. This follows from the so called replacement axiom in set theory. $\square$

Note that an object t is a member of $\{s \in S \mid P(s)\}$ if and only if t is a member of S and the statement $P(t)$ is true.

Example A.3.6.

$$\{x \in \mathbb{Z} \mid x^2 = 1\} = \{1, -1\}.$$

$$\{x \in \mathbb{Z} \mid x > 0\} \quad \text{is the set of positive integers.}$$

Notation A.3.7. *Let S be a set and $P(x)$ a statement involving the variable x .*

(a) “for all $x \in S : P(x)$ ” is the statement

$$\text{for all } x : \quad x \in S \implies P(x)$$

(b) “there exists $x \in S : P(x)$ ” is the statement

$$\text{there exists } x : \quad x \in S \text{ and } P(x)$$

Example A.3.8. (1) “for all $x \in \mathbb{R} : x^2 \geq 0$ ” is a true statement.

(2) “there exists $x \in \mathbb{Q} : x^2 = 2$ ” is a false statement.

Theorem A.3.9. *Let S be a set and let $\Phi(x)$ be a formula involving the variable x such that $\Phi(s)$ is defined for all s in S . Then there exists a set, denoted by $\{\Phi(s) \mid s \in S\}$ such that*

$$\text{for all } x : \quad x \in \{\Phi(s) \mid s \in S\} \iff \text{there exists } s \in S : x = \Phi(s)$$

Proof. This also follows from the replacement axiom in set theory. $\square$

Note that the members of $\{\Phi(s) \mid s \in S\}$ are all the objects of the form $\Phi(s)$, where s is a member of S .

Example A.3.10.

$$\{2x \mid x \in \mathbb{Z}\} \quad \text{is the set of even integers}$$

$$\{x^3 \mid x \in \{-1, 2, 5\}\} = \{-1, 8, 125\}$$

We now combine the two previous theorems into one:

Theorem A.3.11. *Let S be a set, let $P(x)$ be a statement involving the variable x and let $\Phi(x)$ a formula such that $\Phi(s)$ is defined for all s in S for which $P(s)$ is true. Then there exists a set, denoted by $\{\Phi(s) \mid s \in S \text{ and } P(s)\}$ such that*

$$\text{for all } x : \quad x \in \{\Phi(s) \mid s \in S \text{ and } P(s)\} \iff \text{there exists } s \in S : (P(s) \text{ and } x = \Phi(s))$$

Proof. Define

$$(*) \quad \{\Phi(s) \mid s \in S \text{ and } P(s)\} := \{\Phi(s) \mid s \in \{r \in S \mid P(r)\}\}$$

See A.2.3 for a formal proof that this set has the required properties. □

Note that the members of $\{\Phi(s) \mid s \in S \text{ and } P(s)\}$ are all the objects of the form $\Phi(s)$, where s is a member of S for which $P(s)$ is true.

Example A.3.12.

$$\{2n \mid n \in \mathbb{Z} \text{ and } n^2 = 1\} = \{2n \mid n \in \{s \in \mathbb{Z} \mid s^2 = 1\}\} = \{2n \mid n \in \{1, -1\}\} = \{2, -2\}$$

$$\{-x \mid x \in \mathbb{R} \text{ and } x > 0\} \quad \text{is the set of negative real numbers}$$

Theorem A.3.13. *Let A and B be sets.*

(a) *There exists a set, denoted by $A \cup B$ and called ‘ A union B ’, such that*

$$\text{for all } x : \quad x \in A \cup B \iff x \in A \text{ or } x \in B$$

(b) *There exists a set, denoted by $A \cap B$ and called ‘ A intersect B ’, such that*

$$\text{for all } x : \quad x \in A \cap B \iff x \in A \text{ and } x \in B$$

(c) *There exists a set, denoted by $A \setminus B$ and called ‘ A removed B ’, such that*

$$\text{for all } x : \quad x \in A \setminus B \iff x \in A \text{ and } x \notin B$$

(d) *There exists a set, denoted by $\emptyset$ and called ‘empty set’, such that*

$$\text{for all } x : \quad x \notin \emptyset$$

(e) *Let a and b be objects, then there exists a set, denoted by $\{a, b\}$, that*

$$\text{for all } x : \quad x \in \{a, b\} \iff x = a \text{ or } x = b$$

Proof. (a) This is another axiom of set theory.

(b) Applying A.3.5 with $P(x)$ being the statement “ $x \in B$ ” we can define

$$A \cap B := \{a \in A \mid a \in B\}$$

Then for all x :

$$\begin{aligned} & x \in A \cap B \\ \iff & x \in \{a \in A \mid a \in B\} \quad - \text{definition of } A \cap B \\ \iff & x \in A \text{ and } x \in B \quad - \text{Theorem A.3.5} \end{aligned}$$

(c) Applying A.3.5 with $P(x)$ being the statement “ $x \notin B$ ” we can define

$$A \setminus B := \{a \in A \mid a \notin B\}$$

Then for all x :

$$\begin{aligned} & x \in A \setminus B \\ \iff & x \in \{a \in A \mid a \notin B\} \quad - \text{definition of } A \setminus B \\ \iff & x \in A \text{ and } x \notin B \quad - \text{Theorem A.3.5} \end{aligned}$$

(d) One of the axioms of set theory implies the existence of a set D . Then we can define

$$\emptyset := D \setminus D$$

Then for all x :

$$\begin{aligned} & x \in \emptyset \\ \iff & x \in D \setminus D \quad - \text{definition of } \emptyset \\ \iff & x \in D \text{ and } x \notin D \quad - (c) \end{aligned}$$

The latter statement is false and so $x \notin \emptyset$ for all x .

(e) Define $\{a, b\} := \{a\} \cup \{b\}$. Then

$$\begin{aligned} & x \in \{a, b\} \\ \iff & x \in \{a\} \cup \{b\} \quad - \text{definition of } \{a, b\} \\ \iff & x \in \{a\} \text{ or } x \in \{b\} \quad - (a) \\ \iff & x = a \text{ or } x = b \quad - \text{A.3.4} \end{aligned}$$

□

Exercises A.3:**A.3#1.** Let A be a set. Prove that $\emptyset \subseteq A$.**A.3#2.** Let A and B be sets. Prove that $A \cap B = B \cap A$.**A.3#3.** Let a, b and c be objects. Show that there exists a set A such that

$$\text{for all } x : \quad x \in A \quad \Longleftrightarrow \quad (x = a \text{ or } x = b) \text{ or } x = c.$$

A.3#4. Let A and B be sets. Prove that

$$(a) \quad A \subseteq A \cup B.$$

$$(b) \quad A \cap B \subseteq A.$$

$$(c) \quad A \setminus B \subseteq A.$$

A.3#5. Let A, B and C be sets. Show that there exists a set D such that

$$\text{for all } x : \quad x \in D \quad \Longleftrightarrow \quad (x \in A \text{ or } x \in B) \text{ and } x \notin C.$$

A.3#6. List all elements of the following sets:

$$(a) \quad \{x \in \mathbb{Q} \mid x^2 - 3x + 2 = 0\}.$$

$$(b) \quad \{x \in \mathbb{Z} \mid x^2 < 5\}.$$

$$(c) \quad \{x^3 \mid x \in \mathbb{Z} \text{ and } x^2 < 5\}.$$

A.4 Relations and Functions**Definition A.4.1.** Let a, b and c be objects.(a) $(a, b) := \{\{a\}, \{a, b\}\}$. (a, b) is called the (ordered) pair formed by a and b .(b) $(a, b, c) := ((a, b), c)$. (a, b, c) is called the (ordered) triple formed by a, b and c .**Theorem A.4.2.** Let a, b, c, d, e and f be objects.

$$(a) \quad ((a, b) = (c, d)) \quad \Longleftrightarrow \quad (a = c \text{ and } b = d).$$

$$(b) \quad ((a, b, c) = (d, e, f)) \quad \Longleftrightarrow \quad ((a = d \text{ and } b = e) \text{ and } c = f)$$

Proof. (a): See Exercise A.4#1.

(b)

$$\begin{aligned}
 & (a, b, c) = (d, e, f) \\
 \iff & ((a, b), c) = ((d, e), f) \quad - \text{definition of triple} \\
 \iff & (a, b) = (d, e) \text{ and } (c, f) \quad - \text{Part (a) of this theorem} \\
 \iff & (a = d \text{ and } b = e) \text{ and } c = f \quad - \text{Part (a) of this theorem}
 \end{aligned}$$

□

Theorem A.4.3. *Let A and B be sets. Then there exists a set, denoted by $A \times B$, such that*

$$x \in A \times B \iff \text{there exists } a \in A : \text{there exists } b \in B : x = (a, b)$$

Proof. This can be deduced from the axioms of set theory. □

Example A.4.4. Let $A = \{1, 2\}$ and $B = \{2, 3, 5\}$. Then

$$A \times B = \{(1, 2), (1, 3), (1, 5), (2, 2), (2, 3), (2, 5)\}$$

Definition A.4.5. *Let A and B be sets.*

- (a) *A relation R from A to B is a triple (A, B, T) , such that T is a subset of $A \times B$. Let a and b be objects. We say that a is R -related to b and write aRb if $(a, b) \in T$. So aRb is a statement and*

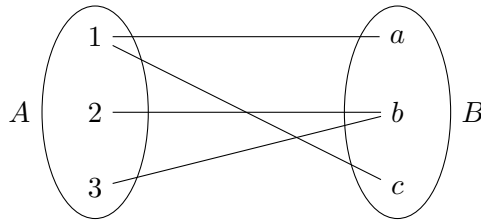
$$aRb \iff (a, b) \in T.$$

- (b) *A relation on A is a relation from A to A .*

Example A.4.6. (1) Using our formal definition of a relation, the familiar relation $\leq$ on the real numbers, would be the triple

$$(\mathbb{R}, \mathbb{R}, \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\})$$

- (2) Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $T = \{(1, a), (1, c), (2, b), (3, b)\}$. Then the relation $\sim := (A, B, T)$ can be visualized by the following diagram:



Also $1 \sim 1$ is a true statement, $1 \sim b$ is a false statement, $2 \sim a$ is false statement, and $2 \sim b$ is a true statement.

Definition A.4.7. (a) A function from A to B is a relation F from A to B such that for all $a \in A$ there exists a unique b in B with aFb . We denote this unique b by $F(a)$. So

$$\text{for all } a \in A : \text{ for all } b \in B : \quad b = F(a) \iff aFb$$

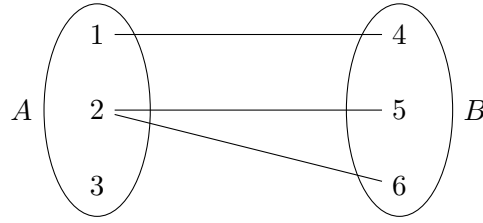
$F(a)$ is called the image of a under F . If $b = F(a)$ we will say that F maps a to b .

(b) We write “ $F : A \rightarrow B$ is function” for “ A and B are sets and F is a function from A to B ”.

Example A.4.8. (a) $F = (\mathbb{R}, \mathbb{R}, \{(x, x^2) \mid x \in \mathbb{R}\})$ is a function with $F(x) = x^2$ for all $x \in \mathbb{R}$.

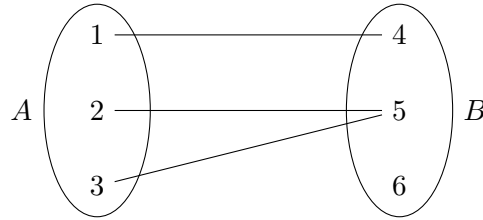
(b) $F = (\mathbb{R}, \mathbb{R}, \{(x^2, x^3) \mid x \in \mathbb{R}\})$ is the relation with $x^2 F x^3$ for all $x \in \mathbb{R}$. For $x = 1$ we see that $1F1$ and for $x = -1$ we see that $1F-1$. So F is not a function.

(c) Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6, \}$, $T = \{(1, 4), (2, 5), (2, 6)\}$ and $R = (A, B, T)$:



Then R is not a function from A to B . Indeed, there does not exist an element b in R with $1Rb$. Also there exist two elements b in B with $2Rb$ namely $b = 5$ and $b = 6$.

(d) Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6, \}$, $S = \{(1, 4), (2, 5), (3, 5)\}$ and $F = (A, B, T)$:



Then F is the function from A to B with $F(1) = 4$, $F(2) = 5$ and $F(3) = 5$.

Notation A.4.9. Let A and B be sets and suppose that $\Phi(x)$ is a formula involving a variable x such that for all a in A

$$\Phi(a) \text{ is defined} \quad \text{and} \quad \Phi(a) \in B.$$

Put

$$T := \{(a, \Phi(a)) \mid a \in A\} \quad \text{and} \quad F := (A, B, T).$$

Then F is a function from A to B . We denote this function by

$$F: A \rightarrow B, \quad a \mapsto \Phi(a).$$

So F is a function from A to B and $F(a) = \Phi(a)$ for all $a \in A$.

Example A.4.10. (1) $F: \mathbb{R} \rightarrow \mathbb{R}, r \mapsto r^2$ denotes the function from $\mathbb{R}$ to $\mathbb{R}$ with $F(r) = r^2$ for all $r \in \mathbb{R}$.

(2) $F: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto \frac{1}{x}$ is not a function, since $\frac{1}{0}$ is not defined.

(3) $F: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}, x \mapsto \frac{1}{x}$ is a function.

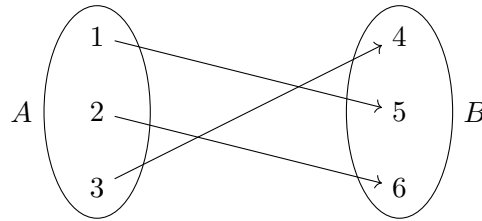
(4) $F: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+, x \mapsto \sqrt{x}$ is not a function, since $\sqrt{2} \notin \mathbb{Z}$.

(5) $F: \mathbb{Z}^+ \rightarrow \mathbb{R}^+, x \mapsto \sqrt{x}$ is a function.

Definition A.4.11. Let R be a relation from A to B .

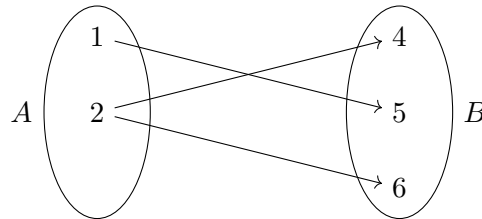
- (a) A is called the domain of R . B is called the codomain of R .
- (b) R is called injective (or 1-1) if for all $b \in B$ there exists at most one a in A with aRb .
- (c) R is called surjective (or onto) if for all $b \in B$ there exists (at least one) $a \in A$ with aRb .
- (d) R is called bijective (or a 1-1 correspondence) if for all $b \in B$ there exists a unique $a \in A$ with aRb .

Example A.4.12. (1) The function



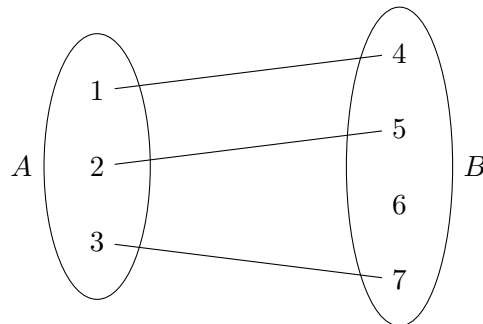
is bijective.

(2) The relation



is bijective, but it is not a function.

(3) The function



is injective but is neither surjective nor bijective.

Theorem A.4.13. *Let $f : A \rightarrow B$ be a function.*

(a) *Then f is bijective if and only if f is a injective and surjective.*

(b) *f is injective if and only*

$$\text{For all } a \in A : \text{For all } c \in A : \quad f(a) = f(c) \implies a = c$$

Proof. (a)

f is bijective

$\iff$ for all $b \in B$ there exists a unique $a \in A$ with $b = f(a)$ - Definition of bijective

$\iff$ for all $b \in B$ there exists at most one $a \in A$ with $b = f(a)$
and for all $b \in B$ there exists $a \in A$ with $b = f(a)$ - A.1.7

$\iff$ f is injective and surjective - Definition of injective and surjective

(b)

f is injective

$\iff$ for all $b \in B$: there exists at most one $a \in A$ with $b = f(a)$ - Definition of injective

$\iff$ for all $b \in B, a, c \in A$: $(b = f(a) \text{ and } b = f(c)) \implies a = c$ - Definition of 'exists at most one'

$\iff$ for all $a, c \in A$: $f(a) = f(c) \implies a = c$

□

Theorem A.4.14. *Let $f : A \rightarrow B$ and $g : C \rightarrow D$ be functions. Then $f = g$ if and only if $A = C$, $B = D$ and $f(a) = g(a)$ for all $a \in A$.*

Proof. By definition of a function, $f = (A, B, R)$ and $g = (C, D, S)$ where $R \subseteq A \times B$ and $S \subseteq C \times D$. By (A.4.2)(b) :

(*) $f = g$ if and only if $A = C$, $B = D$ and $R = S$.

$\implies$: If $f = g$, then the Principal of Substitution implies, $f(a) = g(a)$ for all $a \in A$. Also by (*), $A = C$ and $B = D$.

$\impliedby$: Suppose now that $A = C$, $B = D$ and $f(a) = g(a)$ for all $a \in A$. By (*) it suffices to show that $R = S$.

Let $a \in A$ and $b \in B$.

$$\begin{aligned}
 & (a, b) \in R \\
 \iff & afb \quad \text{--definition of } afb \\
 \iff & b = f(a) \quad \text{--the definition of } f(a) \\
 \iff & b = g(a) \quad \text{--since } f(a) = g(a) \\
 \iff & agb \quad \text{--definition of } g(a) \\
 \iff & (a, b) \in S \quad \text{--definition of } agb
 \end{aligned}$$

Since $A = C$ and $B = D$, both R and S are subsets of $A \times B$. Hence each element of R and S is of the form (a, b) , $a \in A, b \in B$. It follows that $x \in R$ if and only if $x \in S$ and so $R = S$ by A.3.1. $\square$

Definition A.4.15. (a) *Let A be a set. The identity function id_A on A is the function*

$$\text{id}_A : A \rightarrow A, \quad a \mapsto a$$

So $\text{id}_A(a) = a$ for all $a \in A$.

(b) *Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions. Then $g \circ f$ is the function*

$$g \circ f : A \rightarrow C, \quad a \mapsto g(f(a))$$

So $(g \circ f)(a) = g(f(a))$ for all $a \in A$.

Definition A.4.16. *Let $f : A \rightarrow B$ and $g : B \rightarrow A$ be functions.*

(a) *g is called a left inverse of f if $g \circ f = \text{id}_A$.*

(b) *g is called a right inverse of f if $f \circ g = \text{id}_B$.*

(c) *g is called an inverse of f if $g \circ f = \text{id}_A$ and $f \circ g = \text{id}_B$.*

Theorem A.4.17. *Let $f : A \rightarrow B$ and $h : B \rightarrow A$ be functions. Then the following statements are equivalent.*

- (a) g is a left inverse of f .
- (b) f is a right inverse of g .
- (c) $g(f(a)) = a$ for all $a \in A$.
- (d) For all $a \in A$ and $b \in B$:

$$f(a) = b \implies a = g(b)$$

Proof. (a) $\implies$ (b): Suppose that g is a left inverse of f . Then $g \circ f = \text{id}_A$ and so f is a right inverse of g .

(b) $\implies$ (c): Suppose that f is a right inverse of g . Then by definition of ‘right inverse’

$$(1) \quad g \circ f = \text{id}_A$$

Let $a \in A$. Then

$$\begin{aligned} g(f(a)) &= (g \circ f)(a) && \text{– definition of composition} \\ &= \text{id}_A(a) && \text{– (1)} \\ &= a && \text{– definition of id}_A \end{aligned}$$

(c) $\implies$ (d): Suppose that $g(f(a)) = a$ for all $a \in A$. Let $a \in A$ and $b \in B$ with $f(a) = b$. Then by the principle of substitution $g(f(a)) = g(b)$, and since $g(f(a)) = a$, we get $a = g(b)$.

(d) $\implies$ (a): Suppose that for all $a \in A, b \in B$:

$$(2) \quad f(a) = b \implies a = g(b)$$

Let $a \in A$ and put

$$(3) \quad b = f(a)$$

Then by (2)

$$(4) \quad a = g(b)$$

and so

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) && \text{– definition of composition} \\ &= g(b) && (3) \\ &= a && (4) \\ &= \text{id}_A(a) && \text{– definition of id}_A \end{aligned}$$

Thus by A.4.14 $g \circ f = \text{id}_A$. Hence g is a left inverse of f . □

Theorem A.4.18. *Let $f : A \rightarrow B$ and $h : B \rightarrow A$ be functions. Then the following statements are equivalent.*

- (a) g is an inverse of f .
- (b) f is a inverse of g .
- (c) $g(fa) = a$ for all $a \in A$ and $f(gb) = b$ for all $b \in A$.
- (d) For all $a \in A$ and $b \in B$:

$$fa = b \iff a = gb$$

Proof. Note that g is an inverse of f if and only if g is a left and a right inverse of f . Thus the theorem follows from A.4.17 □

Theorem A.4.19. *Let $f : A \rightarrow B$ be a function and suppose $A \neq \emptyset$.*

- (a) f is injective if and only if f has a right inverse.
- (b) f is surjective if and only if f has left inverse.
- (c) f is a injective correspondence if and only if f has inverse.

Proof. $\implies$: Since A is not empty we can fix an element $a_0 \in A$. Let $b \in B$. If $b \in \text{Im } f$ choose $a_b \in A$ with $fa_b = b$. If $b \notin \text{Im } f$, put $a_b = a_0$. Define

$$g : B \rightarrow A, \quad b \rightarrow a_b$$

(a) Suppose f is injective. Let $a \in A$ and $b \in B$ with $b = fa$. Then $b \in \text{Im } f$ and $fa_b = b = fa$. Since f is injective, we conclude that $a_b = a$ and so $ga = a_b = a$. Thus by A.4.17, g is right inverse of f .

(b) Suppose f is surjective. Let $a \in A$ and $b \in B$ with $gb = a$. Then $a = a_b$. Since f is surjective, $B = \text{Im } f$ and so $a \in \text{Im } f$ and $f(a_b) = b$. Hence $fa = b$ and so by A.4.17 (with the roles of f and f interchanged), g is left inverse of f .

(c) Suppose f is a injective correspondence. Then f is injective and surjective and so by the proof of (a) and (b), g is left and right inverse of f . So g is an inverse of f .

$\impliedby$:

(a) Suppose g is a left inverse of f and let $a, c \in A$ with $fa = fc$. Then by the principal of substitution, $g(fa) = g(fc)$. By A.4.17 $g(fa) = a$ and $g(fb) = b$. So $a = b$ and f is injective.

(b) Suppose g is a right inverse of f and let $b \in B$. Then by A.4.17, $f(gb) = b$ and so f is surjective.

(c) Suppose f has an inverse. Then f has a left and a right inverse and so by (a) and (b), f is injective and surjective. So f is a injective correspondence. □

Exercises A.4:

A.4#1. Let a, b, c, d be objects. Prove that

$$\left((a, b) = (c, d) \right) \iff \left((a = c) \text{ and } (b = d) \right)$$

A.4#2. Let A and B be sets. Let A_1 and A_2 be subsets of A and B_1 and B_2 subsets of B such that $A = A_1 \cup A_2$, $A_1 \cap A_2 = \emptyset$, $B = B_1 \cup B_2$ and $B_1 \cap B_2 = \emptyset$. Let $\pi_1 : A_1 \rightarrow B_1$ and $\pi_2 : A_2 \rightarrow B_2$ be bijections. Define

$$\pi : A \rightarrow B, a \mapsto \begin{cases} \pi_1(a) & \text{if } a \in A_1 \\ \pi_2(a) & \text{if } a \in A_2 \end{cases}$$

Show that π is a bijection.

A.4#3. Prove that the given function is injective

(a) $f : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto 2x$.

(b) $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^3$.

(c) $f : \mathbb{Z} \rightarrow \mathbb{Q}, x \mapsto \frac{x}{7}$.

(d) $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto -3x + 5$.

A.4#4. Prove that the given function is surjective.

(a) $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^3$.

(b) $f : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto x - 4$.

(c) $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto -3x + 5$.

(d) $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Q}, (a, b) \mapsto \begin{cases} \frac{a}{b} & \text{when } b \neq 0 \\ 0 & \text{when } b = 0. \end{cases}$

A.4#5. (a) Let $f : B \rightarrow C$ and $g : C \rightarrow D$ be functions such that $g \circ f$ is injective. Prove that f is injective.

(b) Give an example of the situation in part (a) in which g is not injective.

A.5 The Natural Numbers and Induction

A *natural number* is a non-negative integer. $\mathbb{N}$ denotes the collection of all natural numbers. So

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

It can be deduced from the Axioms of Set Theory that $\mathbb{N}$ is a set. We do assume familiarity with the basic properties of the natural numbers, like addition, multiplication and the order relation ' $\leq$ '.

A quick remark how to construct the natural numbers:

$$\begin{aligned}
0 &:= \emptyset \\
1 &:= \{0\} &= 0 \cup \{0\} \\
2 &:= \{0, 1\} &= 1 \cup \{1\} \\
3 &:= \{0, 1, 2\} &= 2 \cup \{2\} \\
4 &:= \{0, 1, 2, 3\} &= 3 \cup \{3\} \\
&\vdots \\
n+1 &:= \{0, 1, 2, 3, \dots, n\} = n \cup \{n\} \\
&\vdots
\end{aligned}$$

The relation $\leq$ on $\mathbb{N}$ can be defined by $i \leq j$ if $i \subseteq j$.

Definition A.5.1. Let S be a subset of $\mathbb{N}$. Then s is called a minimal element of S if $s \in S$ and $s \leq t$ for all $t \in S$.

The following property of the natural numbers is part of our assumed properties of the integers and natural numbers (see Appendix B).

Well-Ordering Axiom: Let S be a non-empty subset of $\mathbb{N}$. Then S has a minimal element

Using the Well-Ordering Axiom we now provide an important tool to prove statements which hold for all natural numbers:

Theorem A.5.2 (Principal Of Mathematical Induction). Suppose that for each $n \in \mathbb{N}$ a statement $P(n)$ is given and that

- (i) $P(0)$ is true, and
- (ii) if $P(k)$ is true for some $k \in \mathbb{N}$, then also $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Suppose for a contradiction that $P(n_0)$ is false for some $n_0 \in \mathbb{N}$. Put

$$(*) \quad S := \{s \in \mathbb{N} \mid P(s) \text{ is false}\}$$

Then $n_0 \in S$ and so S is not empty. The Well-Ordering Axiom B.4.2 now implies that S has a minimal element m . Hence, by definition of a minimal element

$$(**) \quad m \in S \quad \text{and} \quad m \leq s \text{ for all } s \in S$$

By (i) $P(0)$ is true and so $0 \notin S$. As $m \in S$ this gives $m \neq 0$. Thus $k := m - 1$ is a natural number. Note that $k < m$. If $k \in S$, then $(**)$ gives $m \leq k$, a contradiction. Thus $k \notin S$. By definition of S this means that $P(k)$ is true. So by (ii), $P(k+1)$ is true. But $k+1 = (m-1)+1 = m$ and so $P(m)$ is true. But $m \in S$ and so $P(m)$ is false. This contradiction show that $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

Theorem A.5.3 (Principal Of Complete Induction). *Suppose that for each $n \in \mathbb{N}$ a statement $P(n)$ is given and that*

- (i) *if $k \in \mathbb{N}$ and $P(i)$ is true for all $i \in \mathbb{N}$ with $i < k$, then $P(k)$ is true.*

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $Q(n)$ be the statement:

$$\text{for all } i \in \mathbb{N}: \quad i < n \implies P(i).$$

We will show that the two conditions in the Principal of Mathematical Induction hold for $Q(n)$ in place of $P(n)$. $Q(0)$ is statement

$$\text{for all } i \in \mathbb{N}: \quad i < 0 \implies P(i).$$

$i < 0$ is false for all $i \in \mathbb{N}$. Hence the implication $i < 0 \implies P(i)$ is true for all $i \in \mathbb{N}$. Thus

- (*) $Q(0)$ is true.

Suppose now that $Q(k)$ is true for some $k \in \mathbb{N}$. Then $P(i)$ is true for all $i \in \mathbb{N}$ with $i < k$. Then by (i), also $P(k)$ is true.

Let $i \in \mathbb{N}$ with $i < k + 1$. Then either $i < k$ or $i = k$. In either case $P(i)$ is true. Thus $Q(k + 1)$ is true. We proved

- (**) *If $Q(k)$ is true for some $k \in \mathbb{N}$, then also $Q(k + 1)$ is true.*

By (*) and (**) the hypothesis of the Principal of Mathematical Induction is fulfilled. Hence $Q(n)$ is true for all $n \in \mathbb{N}$. Let $n \in \mathbb{N}$. Then $Q(n + 1)$ is true and since $n < n + 1$, $P(n)$ is true. $\square$

Two more versions of the induction principal:

Theorem A.5.4. *Suppose that $r \in \mathbb{Z}$ and that for all $n \in \mathbb{Z}$ with $n \geq r$ a statement $P(n)$ is given. Also suppose that*

- (i) $P(r)$ is true, and
(ii) *if $k \in \mathbb{Z}$ such that $k \geq r$ and $P(k)$ is true, then $P(k + 1)$ is true.*

Then $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq r$.

Proof. See Exercise A.5#5. $\square$

Theorem A.5.5. *Suppose that $r \in \mathbb{Z}$ and that, for all $n \in \mathbb{Z}$ with $n \geq r$, a statement $P(n)$ is given. Also suppose that:*

- (i) *If $k \in \mathbb{Z}$ with $k \geq r$ and $P(i)$ holds for all $i \in \mathbb{Z}$ with $r \leq i < k$, then $P(k)$ holds.*

Then $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq r$.

Proof. See Exercise A.5#6. □

Exercises A.5:

A.5#1. Prove that the sum of the first n positive integers is $\frac{n(n+1)}{2}$.

Hint: Let $P(k)$ be the statement:

$$1 + 2 + \dots + k = \frac{k(k+1)}{2}.$$

A.5#2. Let r be a real number, $r \neq 1$. Prove that for every integer $n \geq 1$,

$$1 + r + r^2 + \dots + r^{n-1} = \frac{r^n - 1}{r - 1}.$$

A.5#3. Prove that for every positive integer n there exists an integer k with $2^{2n+1} + 1 = 2k$

A.5#4. Let B be a set of n elements.

- (a) If $n \geq 2$, prove that the number of two-elements subsets of B is $n(n-1)/2$.
- (b) If $n \geq 3$, prove that the number of three-element subsets of B is $n(n-1)(n-2)/3!$.

A.5#5. Suppose that $r \in \mathbb{Z}$ and that, for all $n \in \mathbb{Z}$ with $n \geq r$, a statement $P(n)$ is given. Also suppose that

- (i) $P(r)$ is true, and
- (ii) if $k \in \mathbb{Z}$ such that $k \geq r$ and $P(k)$ is true, then $P(k+1)$ is true.

Show that $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq r$.

A.5#6. Suppose that $r \in \mathbb{Z}$ and that, for all $n \in \mathbb{Z}$ with $n \geq r$, a statement $P(n)$ is given. Also suppose that:

- (i) If $k \in \mathbb{Z}$ with $k \geq r$ and $P(i)$ holds for all $i \in \mathbb{Z}$ with $r \leq i < k$, then $P(k)$ holds.

Show that $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq r$.

A.5#7. What is wrong with the following proof that all roses have the same color:

Proof. For a positive integer n let $P(n)$ be the statement:

Whenever A is set containing exactly n roses, then all roses in A have the same color.

If A is a set containing exactly one rose, then certainly all roses in A have the same color. Thus $P(1)$ is true.

Suppose now k is a positive integer such that $P(k)$ is true. So whenever D is a set containing exactly k roses then all roses in D have the same color. We need to show that $P(k+1)$ is true. So

let A be any set containing exactly $k + 1$ -roses. Since $k \geq 1$ we have $k + 1 \geq 2$. Hence A contains at least two roses and we can choose roses x and y in A with $x \neq y$. Consider the sets

$$B := A \setminus \{x\} \quad \text{and} \quad C := A \setminus \{y\}$$

Then B consist of all the elements of A other than x . Since A contains exactly $k + 1$ roses, B contains exactly k roses. By the induction assumption $P(k)$ is true and so all roses in B have the same color. Similarly all roses in C have the same color.

Now let z be any rose in A distinct from x and y . Then $z \neq x$ and so $z \in B$. Also $z \neq y$ and so $z \in C$.

We will show that all roses in A have the same color as z . For this let a be any rose in A . We will distinguish the cases $a \neq x$ and $a = x$.

Suppose first that $a \neq x$. Then $a \in B$. Recall that $z \in B$ and all roses in B have the same color. Thus a has the same color as z .

Suppose next that $a = x$. Since $x \neq y$ this gives $a \neq y$ and so $a \in C$. Recall that $z \in C$ and all roses in C have the same color. Thus a has the same color as z .

Hence in either case a has the same color as z and so all roses in A have the same color as z . Thus $P(k + 1)$ is true.

We proved that $P(1)$ is true and that $P(k)$ implies $P(k + 1)$. Hence by the Principal of Mathematical Induction, $P(n)$ is true for all positive integers n . Thus in any set of roses all the roses have the same color. So all roses have the same color. $\square$

A.5#8. Let x be a real number greater than -1 . Prove that for every positive integer n , $(1 + x)^n \geq 1 + nx$.

A.6 Equivalence Relations

Definition A.6.1. Let $\sim^1$ be a relation on the set A

(a) $\sim$ is called reflexive if $a \sim a$ for all $a \in A$.

(b) $\sim$ is called symmetric if $b \sim a$ for all $a, b \in A$ with $a \sim b$, that is if

$$a \sim b \quad \implies \quad b \sim a.$$

(c) $\sim$ is called transitive if $a \sim c$ for all $a, b, c \in A$ with $a \sim b$ and $b \sim c$, that is if

$$(a \sim b \quad \text{and} \quad b \sim c) \quad \implies \quad a \sim c$$

(d) $\sim$ is called an equivalence relation if $\sim$ is reflexive, symmetric and transitive.

¹ $\sim$ is pronounced ‘twiddle’

Example A.6.2. (1) Consider the relation ' $\leq$ ' on the real numbers:

$a \leq a$ for all real numbers a and so ' $\leq$ ' is reflexive.

$1 \leq 2$ but $2 \not\leq 1$ and so ' $\leq$ ' is not symmetric.

If $a \leq b$ and $b \leq c$, then $a \leq c$ and so ' $\leq$ ' is transitive.

Since ' $\leq$ ' is not symmetric, ' $\leq$ ' is not an equivalence relation.

(2) Consider the relation ' $=$ ' on any set A .

$a = a$ and so ' $=$ ' is reflexive.

If $a = b$, then $b = a$ and so ' $=$ ' is symmetric.

If $a = b$ and $b = c$, then $a = c$ and so ' $=$ ' is transitive.

' $=$ ' is reflexive, symmetric and transitive and so an equivalence relation.

(3) Consider the relation ' $\neq$ ' on any set A .

If $a \neq b$, then $b \neq a$ so ' $\neq$ ' is symmetric.

Suppose A has at least one element A . Then $a = a$ and so ' $\neq$ ' is not reflexive.

Suppose A has at least two distinct elements a, b . Then

$$a \neq b \quad \text{and} \quad b \neq a \quad \text{but not} \quad a \neq a$$

So ' $\neq$ ' is not transitive.

(4) Consider the relation S on $\mathbb{R}$ defined by

$$aSb \iff a - b \in \mathbb{Z}.$$

Let $a, b, c \in \mathbb{R}$.

$a - a = 0 \in \mathbb{Z}$ and so aSa . Thus S is reflexive

If aSb , then $a - b \in \mathbb{Z}$. Hence also $-(a - b) \in \mathbb{Z}$. So $b - a \in \mathbb{Z}$. Thus bSa and so S is symmetric.

If aSb and bSc , then $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$. Hence also $(a - b) + (b - c) \in \mathbb{Z}$. Thus $a - c \in \mathbb{Z}$ and S is transitive.

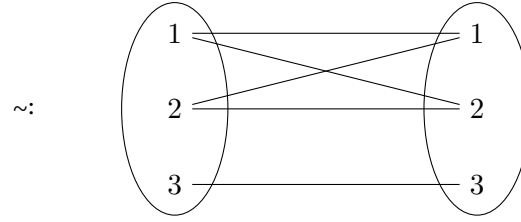
Since S is reflexive, symmetric and transitive, S is an equivalence relation.

Definition A.6.3. Let $\sim$ be an equivalence relation on the set A .

(a) For $a \in A$ we define $[a]_{\sim} := \{b \in A \mid a \sim b\}$. We often just write $[a]$ for $[a]_{\sim}$. $[a]_{\sim}$ is called the equivalence class of a with respect to $\sim$.

(b) $A/\sim := \{[a]_{\sim} \mid a \in A\}$. So $A/\sim$ is the set of equivalence classes with respect to $\sim$.

Example A.6.4. (1) Consider the relation



on the set $A = \{1, 2, 3\}$. Then $\sim$ is an equivalence relation. Also

$$[1]_{\sim} = \{a \in A \mid 1 \sim a\} = \{1, 2\}$$

$$[2]_{\sim} = \{a \in A \mid 2 \sim a\} = \{1, 2\}$$

$$[3]_{\sim} = \{a \in A \mid 3 \sim a\} = \{3\}$$

and so

$$A/\sim = \{\{1, 2\}, \{3\}\}$$

(2) Consider the relation S on $\mathbb{R}$ defined by

$$aSb \iff a - b \in \mathbb{Z}.$$

By Example (A.6.2)(4) S is an equivalence relation. We have

$$[0]_S = \{b \in \mathbb{R} \mid 0Sb\} = \{b \in \mathbb{R} \mid b - 0 \in \mathbb{Z}\} = \{b \in \mathbb{R} \mid b \in \mathbb{Z}\} = \mathbb{Z}$$

and

$$\begin{aligned} [\pi]_S &= \{b \in \mathbb{R} \mid \pi Sb\} \\ &= \{b \in \mathbb{R} \mid b - \pi \in \mathbb{Z}\} \\ &= \{b \in \mathbb{R} \mid b - \pi = k \text{ for some } k \in \mathbb{Z}\} \\ &= \{b \in \mathbb{R} \mid b = \pi + k \text{ for some } k \in \mathbb{Z}\} \\ &= \{\pi + k \mid k \in \mathbb{Z}\} \\ &= \{\dots, \pi - 4, \pi - 3, \pi - 2, \pi - 1, \pi, \pi + 1, \pi + 2, \pi + 3, \pi + 4, \dots\} \end{aligned}$$

Theorem A.6.5. *Let $\sim$ be an equivalence relation on the set A and let $a, b \in A$. Then the following statements are equivalent:*

- | | | |
|-------------------------|-------------------------------------|-------------------|
| (a) $a \sim b$. | (d) $[a] \cap [b] \neq \emptyset$. | (g) $a \in [b]$ |
| (b) $[b] \subseteq [a]$ | (e) $b \sim a$. | (h) $[a] = [b]$. |
| (c) $b \in [a]$. | (f) $[a] \subseteq [b]$. | |

Proof. Note first that, since $\sim$ is an equivalence relation, $\sim$ is reflexive, symmetric and transitive. Recall that $[b] = \{e \in A \mid b \sim e\}$. Hence for all $c \in A$:

$$(*) \quad c \in [b] \quad \Longleftrightarrow \quad b \sim c.$$

Since $\sim$ is reflexive, we know that $b \sim b$. So $(*)$ shows:

$$(**) \quad b \in [b].$$

(a) $\implies$ (b): Suppose that $a \sim b$. To show that $[b] \subseteq [a]$ we need to show that $c \in [a]$ for all $c \in [b]$. So let $c \in [b]$. Then $(*)$ gives $b \sim c$. Hence

$$a \sim b \quad \text{and} \quad b \sim c$$

As $\sim$ is transitive we see that $a \sim c$ and $(*)$ shows that $c \in [a]$. Thus $[b] \subseteq [a]$.

(b) $\implies$ (c): Suppose $[b] \subseteq [a]$. By $(**)$ $b \in [b]$. As $[b] \subseteq [a]$ this gives $b \in [a]$.

(c) $\implies$ (d): Suppose that $b \in [a]$. By $(**)$ $b \in [b]$, so $b \in [a] \cap [b]$ and thus $[a] \cap [b] \neq \emptyset$.

(d) $\implies$ (e): Suppose $[a] \cap [b] \neq \emptyset$. Then there exists $c \in [a] \cap [b]$. Thus $c \in [b]$ and $c \in [a]$, and $(*)$ implies

$$b \sim c \quad \text{and} \quad a \sim c.$$

As $\sim$ is symmetric, this gives

$$b \sim c \quad \text{and} \quad c \sim a.$$

Since $\sim$ is transitive, we infer that

$$b \sim a.$$

(e) $\implies$ (a): Since $\sim$ is symmetric, $b \sim a$ implies $a \sim b$.

We proved that statements (a) to (e) are equivalent. In particular,

$$a \sim b \quad \Longleftrightarrow \quad [b] \subseteq [a] \quad \Longleftrightarrow \quad b \in [a]$$

This result with a and b interchanged gives

$$b \sim a \quad \Longleftrightarrow \quad [a] \subseteq [b] \quad \Longleftrightarrow \quad a \in [b],$$

that is statements (e) to (g) are equivalent. It follows that statements (a) to (g) are equivalent.

(h) $\implies$ (f): Suppose (h) holds. Then $[a] \subseteq [b]$ and since (h) and (b) are equivalent we get $[b] \subseteq [a]$. Thus $[a] = [b]$. Thus (h) implies (f).

(f) $\implies$ (h): Suppose (f) holds. Then $[a] = [b]$ and so $[a] \subseteq [b]$. Thus (f) implies (h).

Hence (h) is equivalent to (f). As statements (a) to (g) are equivalent we conclude that statements (a) to (h) are equivalent. $\square$

Theorem A.6.6. *Let $\sim$ be an equivalence relation on the set A and let $a \in A$. Then there exists a unique equivalence class X with respect to $\sim$ with $a \in X$, namely $X = [a]_\sim$.*

Proof. Let X be an equivalence class of $\sim$. We need to show that $a \in X$ if and only if $X = [a]_\sim$. By definition of ‘equivalence class’ we know that $X = [b]_\sim$ for some $b \in A$. Then

$$\begin{array}{lll} & a \in X & \\ \iff & a \in [b]_\sim & - X = [b]_\sim, \text{Principal of Substitution} \\ \iff & [a]_\sim = [b]_\sim & - \text{A.6.5} \\ \iff & [a]_\sim = X & - X = [b]_\sim, \text{Principal of Substitution} \end{array}$$

$\square$

Exercises A.6:

A.6#1. Let $f : A \rightarrow B$ be a function and define a relation $\sim$ on A by

$$u \sim v \iff f(u) = f(v).$$

Prove that $\sim$ is an equivalence relation.

A.6#2. Let $A = \{1, 2, 3\}$. Draw a diagram to exhibit a relation on A with the stated properties.

- (a) Reflexive, not symmetric, not transitive.
- (b) Symmetric, not reflexive, not transitive.
- (c) Transitive, not reflexive, not symmetric.
- (d) Reflexive and symmetric, not transitive.
- (e) Reflexive and transitive, not symmetric.
- (f) Symmetric and transitive, not reflexive.

A.6#3. Let $\sim$ be the relation on the set $\mathbb{R}^*$ of non-zero real numbers defined by

$$a \sim b \iff \frac{a}{b} \in \mathbb{Q}.$$

Prove that $\sim$ is an equivalence relation.

A.6#4. Let $\sim$ be a symmetric and transitive relation on a set A . What is wrong with the following ‘proof’ that $\sim$ is reflexive.:

Let $a \in A$. We need to show that $a \sim a$. For this let $b \in A$ with $a \sim b$. Since ‘ $\sim$ ’ is symmetric we get $b \sim a$. Hence $a \sim b$ and $b \sim a$ and since ‘ $\sim$ ’ is transitive we conclude that $a \sim a$.

We proved that $a \sim a$ for all $a \in A$ and so ‘ $\sim$ ’ is reflexive.

A.6#5. Let A be a set and $\mathcal{B}$ a set of subsets of A . (So each element of $\mathcal{B}$ is a subset of A .) Suppose that for each $a \in A$ there exists a unique $B \in \mathcal{B}$ with $a \in B$. Define a relation $\sim$ on A by

$$a \sim b \iff \text{there exists } B \in \mathcal{B} \text{ with } a \in B \text{ and } b \in B.$$

Show that $\sim$ is an equivalence relation and that $\mathcal{B} = A/\sim$.

A.7 Partitions

Definition A.7.1. Let A be a set and Δ set of non-empty subsets of A .

(a) Δ is called a partition of A if for each $a \in A$ there exists a unique $D \in \Delta$ with $a \in D$.

(b) $\sim_\Delta = \left(A, A, \left\{ (a, b) \in A \times A \mid \{a, b\} \subseteq D \text{ for some } D \in \Delta \right\} \right)$.

Example A.7.2. The relation corresponding to a partition $\Delta = \{\{1, 3\}, \{2\}\}$ of $A = \{1, 2, 3\}$

$\{1, 3\}$ is the only member of Δ containing 1, $\{2\}$ is the only member of Δ containing 2 and $\{1, 3\}$ is the only member of Δ containing 3. So Δ is a partition of A .

Note that $\{1, 2\}$ is not contained in an element of Δ and so $1 \not\sim_\Delta 2$. $\{1, 3\}$ is contained in $\{1, 3\}$ and so $1 \sim_\Delta 3$. Altogether the relation $\sim_\Delta$ can be described by the following table

$\sim_\Delta$	1	2	3
1	x	$-$	x
2	$-$	x	$-$
3	x	$-$	x

where we placed an x in row a and column b of the table iff $a \sim_\Delta b$.

We now computed the classes of $\sim_\Delta$. We have

$$[1] = \{b \in A \mid 1 \sim_\Delta b\} = \{1, 3\}$$

$$[2] = \{b \in A \mid 2 \sim_\Delta b\} = \{2\}$$

and

$$[3] = \{b \in A \mid 3 \sim_\Delta b\} = \{1, 3\}$$

Thus $A/\sim_\Delta = \{\{1, 3\}, \{2\}\} = \Delta$.

So the set of classes of relation $\sim_\Delta$ is just the original partition Δ . The next theorem shows that this is true for any partition.

Theorem A.7.3. *Let A be set.*

- (a) *If $\sim$ is an equivalence relation, then $A/\sim$ is a partition of A and $\sim = \sim_{A/\sim}$.*
- (b) *If Δ is partition of A , then $\sim_\Delta$ is an equivalence relation and $\Delta = A/\sim_\Delta$.*

Proof. (a) Let $a \in A$. Since $\sim$ is reflexive we have $a \sim a$ and so $a \in [a]$ by definition of $[a]$. Let $D \in A/\sim$ with $a \in D$. Then $D = [b]$ for some $b \in A$ and so $a \in [b]$. A.6.5 implies $[a] = [b] = D$. So $[a]$ is the unique member of $A/\sim$ containing a . Thus $A/\sim$ is a partition of A . Put $\approx = \sim_{A/\sim}$. Then $a \approx b$ if and only if $\{a, b\} \subseteq D$ for some $D \in A/\sim$. We need to show that $a \approx b$ if and only if $a \sim b$.

So let $a, b \in A$ with $a \approx b$. Then $\{a, b\} \subseteq D$ for some $D \in A/\sim$. By the previous paragraph, $[a]$ is the only member of $A/\sim$ containing a . Thus $D = [a]$ and similarly $D = [b]$. Thus $[a] = [b]$ and A.6.5 implies $a \sim b$.

Now let $a, b \in A$ with $a \sim b$. Then both a and b are contained in $[b]$ and so $a \approx b$.

We proved that $a \approx b$ if and only if $a \sim b$ and so (a) is proved.

(b) Let $a \in A$. Since Δ is a partition, there exists $D \in \Delta$ with $a \in D$. Thus $\{a, a\} \subseteq D$ and hence $a \sim_\Delta a$. So $\sim_\Delta$ is reflexive. If $a \sim_\Delta b$ then $\{a, b\} \subseteq D$ for some $D \in \Delta$. Then also $\{b, a\} \subseteq D$ and hence $b \sim_\Delta a$. Thus $\sim$ is symmetric. Now suppose that $a, b, c \in A$ with $a \sim_\Delta b$ and $b \sim_\Delta c$. Then there exists $D, E \in \Delta$ with $a, b \in D$ and $b, c \in E$. Since b is contained in a unique member of Δ , $D = E$ and so $a \sim_\Delta c$. Thus $\sim_\Delta$ is an equivalence relation.

It remains to show that $\Delta = A/\sim_\Delta$. For $a \in A$ let $[a] = [a]_{\sim_\Delta}$. We will prove:

(*) *Let $D \in \Delta$ and $a \in D$. Then $D = [a]$.*

Let $b \in D$. Then $\{a, b\} \subseteq D$ and so $a \sim_\Delta b$ by definition of $\sim_\Delta$. Thus $b \in [a]$ by definition of $[a]$. It follows that $D \subseteq [a]$.

Let $b \in [a]$. Then $a \sim_\Delta b$ by definition of $[a]$ and thus $\{a, b\} \subseteq E$ for some $E \in \Delta$. Since Δ is a partition, a is contained in a unique member of Δ and so $E = D$. Thus $b \in D$ and so $[a] \subseteq D$. We proved $D \subseteq [a]$ and $[a] \subseteq D$ and so (*) holds.

Let $D \in \Delta$. Since Δ is a partition of A , D is non-empty subset of A . So we can pick $a \in D$ and (*) implies $D = [a]$. Thus $D \in A/\sim_\Delta$ and so $\Delta \subseteq A/\sim_\Delta$.

Let $E \in A/\sim_\Delta$. Then $E = [a]$ for some $a \in A$. Since Δ is a partition, $a \in D$ for some $D \in \Delta$. (*) gives $D = [a] = E$ and so $E \in \Delta$. This shows $A/\sim_\Delta \subseteq \Delta$.

Together with $\Delta \subseteq A/\sim_\Delta$ this gives $\Delta = A/\sim_\Delta$ and (b) is proved. $\square$

Appendix B

Real numbers, integers and natural numbers

In this part of the appendix we list properties of the real numbers, integers and natural numbers we assume to be true.

B.1 Definition of the real numbers

Definition B.1.1. *The real numbers are a quadruple $(\mathbb{R}, +, \cdot, \leq)$ such that*

($\mathbb{R}$ i) $\mathbb{R}$ is a set (whose elements are called real numbers)

($\mathbb{R}$ ii) $+$ is a function (called addition), $\mathbb{R} \times \mathbb{R}$ is a subset of the domain of $+$ and

$$a + b \in \mathbb{R} \quad (\text{Closure of addition})$$

for all $a, b \in \mathbb{R}$, where $a \oplus b$ denotes the image of (a, b) under $+$;

($\mathbb{R}$ iii) $\cdot$ is a function (called multiplication), $\mathbb{R} \times \mathbb{R}$ is a subset of the domain of $\cdot$ and

$$a \cdot b \in \mathbb{R} \quad (\text{Closure of multiplication})$$

for all $a, b \in \mathbb{R}$ where $a \cdot b$ denotes the image of (a, b) under $\cdot$. We will also use the notion ab for $a \cdot b$.

($\mathbb{R}$ iv) $\leq$ is a relation from $\mathbb{R}$ and $\mathbb{R}$;

and such that the following statements hold:

($\mathbb{R}$ Ax 1) $a + b = b + a$ for all $a, b \in \mathbb{R}$. (Commutativity of Addition)

($\mathbb{R}$ Ax 2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{R}$; (Associativity of Addition)

($\mathbb{R}$ Ax 3) *There exists an element in $\mathbb{R}$, denoted by 0 (and called zero), such that $a + 0 = a$ and $0 + a = a$ for all $a \in \mathbb{R}$;* (Existence of Additive Identity)

($\mathbb{R}$ Ax 4) *For each $a \in \mathbb{R}$ there exists an element in $\mathbb{R}$, denoted by $-a$ (and called negative a) such that $a + (-a) = 0$ and $(-a) + a = 0$;* (Existence of Additive Inverse)

($\mathbb{R}$ Ax 5) $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{R}$. (Right Distributivity)

($\mathbb{R}$ Ax 6) $(a + b)c = ac + bc$ for all $a, b, c \in \mathbb{R}$ (Left Distributivity)

($\mathbb{R}$ Ax 7) $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{R}$ (Associativity of Multiplication)

($\mathbb{R}$ Ax 8) *There exists an element in $\mathbb{R}$, denoted by 1 (and called one), such that $1a = a$ for all $a \in \mathbb{R}$.* (Multiplicative Identity)

($\mathbb{R}$ Ax 9) *For each $a \in \mathbb{R}$ with $a \neq 0$ there exists an element in $\mathbb{R}$, denoted by $\frac{1}{a}$ (and called ‘ a inverse’) such that $aa^{-1} = 1$ and $a^{-1}a = 1$;*

(Existence of Multiplicative Inverse)

($\mathbb{R}$ Ax 10) *For all $a, b \in \mathbb{R}$,*

$$(a \leq b \text{ and } b \leq a) \iff (a = b)$$

($\mathbb{R}$ Ax 11) *For all $a, b, c \in \mathbb{R}$,*

$$(a \leq b \text{ and } b \leq c) \implies (a \leq c)$$

($\mathbb{R}$ Ax 12) *For all $a, b, c \in \mathbb{R}$,*

$$(a \leq b \text{ and } 0 \leq c) \implies (ac \leq bc)$$

($\mathbb{R}$ Ax 13) *For all $a, b, c \in \mathbb{R}$,*

$$(a \leq b) \implies (a + c \leq b + c)$$

($\mathbb{R}$ Ax 14) *Each bounded, non-empty subset of $\mathbb{R}$ has a least upper bound. That is, if S is a non-empty subset of $\mathbb{R}$ and there exists $u \in \mathbb{R}$ with $s \leq u$ for all $s \in S$, then there exists $m \in \mathbb{R}$ such that for all $r \in \mathbb{R}$,*

$$(s \leq r \text{ for all } s \in S) \iff (m \leq r)$$

($\mathbb{R}$ Ax 15) *For all $a, b \in \mathbb{R}$ such that $b \neq 0$ and $0 \leq b$ there exists a positive integer n such that $a \leq nb$. (Here na is inductively defined by $1a = a$ and $(n + 1)a = na + a$).*

Definition B.1.2. *The relations $<$, $\geq$ and $>$ on $\mathbb{R}$ are defined as follows: Let $a, b \in \mathbb{R}$, then*

(a) $a < b$ if $a \leq b$ and $a \neq b$.

(b) $a \geq b$ if $b \leq a$.

(c) $a > b$ if $b \leq a$ and $a \neq b$

B.2 Algebraic properties of the integers

Theorem B.2.1. *Let $a, b, c \in \mathbb{Z}$. Then*

- (1) $a + b \in \mathbb{Z}$.
- (2) $a + (b + c) = (a + b) + c$.
- (3) $a + b = b + a$.
- (4) $a + 0 = a = 0 + a$.
- (5) *There exists $x \in \mathbb{Z}$ with $a + x = 0$.*
- (6) $ab \in \mathbb{Z}$.
- (7) $a(bc) = (ab)c$.
- (8) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
- (9) $ab = ba$.
- (10) $a1 = a = 1a$.
- (11) *If $ab = 0$ then $a = 0$ or $b = 0$.*

B.3 Properties of the order on the integers

Theorem B.3.1. *Let a, b, c be integers.*

- (a) *Exactly one of $a < b$, $a = b$ and $b < a$ holds.*
- (b) *If $a < b$ and $b < c$, then $a < c$.*
- (c) *If $c > 0$, then $a < b$ if and only if $ac < bc$.*
- (d) *If $c < 0$, then $a < b$ if and only if $bc < ac$.*
- (e) *If $a < b$, then $a + c < b + c$.*
- (f) *1 is the smallest positive integer.*

B.4 Properties of the natural numbers

Theorem B.4.1. *Let $a, b \in \mathbb{N}$. Then*

- (a) $a + b \in \mathbb{N}$.
- (b) $ab \in \mathbb{N}$.

Theorem B.4.2 (Well-Ordering Axiom). *Let S be a non-empty subset of $\mathbb{N}$. Then S has a minimal element. (Recall here that m is a minimal element of S if $m \in S$ and $m \leq s$ for all $s \in S$)* $\square$

Appendix C

The Associative, Commutative and Distributive Laws

C.1 The General Associative Law

Definition C.1.1. Let G be a set.

- (a) A binary operation on G is a function $+$ such that $G \times G$ is a subset of the domain of $+$ and $+(a, b) \in G$ for all $a, b \in G$.
- (b) If $+$ is a binary operation on G and $a, b \in G$, then we write $a + b$ for $+(a, b)$.
- (c) A binary operation $+$ on G is called associative if $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$.

Definition C.1.2. Let G be a set and $+: G \times G \rightarrow G, (a, b) \rightarrow a + b$ a function. Let n be a positive integer and $a_1, a_2, \dots, a_n \in G$.

Inductively, we say that z is a sum of $(a_1, \dots, a_n)$ provided that one of the following holds:

- (1) $n = 1$ and $z = a_1$.
- (2) $n > 1$ and there exists an integer k with $1 \leq k < n$ and $x, y \in G$ such that x is a sum of $(a_1, \dots, a_k)$, y is a sum of $(a_{k+1}, a_{k+2}, \dots, a_n)$ and $z = x + y$.

For example a is the only sum of (a) , $a + b$ is the only sum of (a, b) , $a + (b + c)$ and $(a + b) + c$ are the sums of (a, b, c) , and $a + (b + (c + d))$, $a + ((b + c) + d)$, $(a + b) + (c + d)$, $(a + (b + c)) + d$ and $((a + b) + c) + d$ are the sums of (a, b, c, d) .

Theorem C.1.3 (General Associative Law). Let $+$ be an associative binary operation on the set G . Let $n \in \mathbb{Z}^+$ and $a_1, a_2, \dots, a_n \in G$. Let z and z' be sums of $(a_1, a_2, \dots, a_n)$. Then $z = z'$.

We denote the unique sum of $(a_1, \dots, a_n)$ by $\sum_{i=1}^n a_i$.

Proof. The proof is by complete induction on n . For a positive integer n let $P(n)$ be the statement:

If $a_1, a_2, \dots, a_n$ are elements of G and z and z' sums $(a_1, a_2, \dots, a_n)$, then $z = z'$.

Suppose now that n is a positive integer and $P(k)$ is true all integers $1 \leq k < n$. Let $a_1, a_2, \dots, a_n$ be elements of G and let z and z' be sums of $(a_1, a_2, \dots, a_n)$. We need to show $z = z'$.

Assume that $n = 1$. By definition a_1 is the only sum of (a_1) . Thus $z = a_1 = z'$.

Assume next that $n > 1$. Then by definition of a sum there exists integers k, k' and $x, y, x', y' \in G$ such that

- (i) $1 \leq k < n$ and $1 \leq k' < n$
- (ii) x is a sum of $(a_1, \dots, a_k)$, and x' is a sum of $(a_1, \dots, a_{k'})$,
- (iii) y is a sum of $(a_{k+1}, \dots, a_n)$, and y' is a sum of $(a_{k'+1}, \dots, a_n)$
- (iv) $z = x + y$ and $z' = x' + y'$.

Suppose first that $k = k'$. Then both x and x' are sums of $(a_1, \dots, a_k)$. Since $k < n$ we know that $P(k)$ holds and so $x = x'$. Similarly, both y and y' are sums of $(a_{k+1}, \dots, a_n)$ and, since $n - k < n$, $P(n - k)$ holds. Thus $y = y'$. Hence $z = x + y = x' + y' = z'$.

Suppose next that $k \neq k'$. Without loss $k < k'$. Let w be any sum of $(a_{k+1}, \dots, a_{k'})$. Then both $x + w$ and x' are sums of $(a_1, \dots, a_{k'})$. Since $k' < n$, we know that $P(k')$ holds. So $x + w = x'$. Similarly $w + y'$ and y are sums of $(a_{k+1}, \dots, a_n)$ and since $n - k < n$, $P(n - k)$ holds. Thus $w + y' = y$. Hence

$$z = x + y = x + (w + y') = (x + w) + y' = x' + y' = x' + y' = x'$$

We proved that in both cases $z = z'$. Thus $P(n)$ holds. By the principal of complete induction, $P(n)$ holds for all positive integers n . $\square$

C.2 The general commutative law

Definition C.2.1. A binary operation $+$ on a set G is called commutative if $a + b = b + a$ for all $a, b \in G$.

Theorem C.2.2 (General Commutative Law I). Let $+$ be an associative and commutative binary operation on a set G . Let $a_1, a_2, \dots, a_n \in G$ and $f: [1 \dots n] \rightarrow [1 \dots n]$ a bijection. Then

$$\sum_{i=1}^n a_i = \sum_{i=1}^n a_{f(i)}$$

Proof. Observe that the theorem clearly holds for $n = 1$. Suppose inductively its true for $n - 1$.

Since f is surjective there exists a unique integer k with $f(k) = n$.

Define $g: \{1, \dots, n-1\} \rightarrow \{1, \dots, n-1\}$ by $g(i) = f(i)$ if $i < k$ and $g(i) = f(i+1)$ if $i \geq k$. We claim that g is a bijection. For this let $1 \leq l \leq n-1$ be an integer. Then $l = f(m)$ for some $1 \leq m \leq n$. Since $l \neq n$ and f is injective, $m \neq k$. If $m < k$, then $g(m) = f(m) = l$ and if $m > k$, then $g(m-1) = f(m) = l$.

Thus g is surjective and by (F.1.7)(b) g is also injective. By assumption the theorem is true for $n-1$ and so

$$(*) \quad \sum_{i=1}^{n-1} a_i = \sum_{i=1}^{n-1} a_{g(i)}$$

Using the general associative law (GAL, Theorem C.1.3) we have

$$\begin{aligned}
 & \sum_{i=1}^n a_{f(i)} \\
 \text{(GAL)} \quad &= (\sum_{i=1}^{k-1} a_{f(i)}) + (a_{f(k)} + \sum_{i=k+1}^n a_{f(i)}) \\
 (n = f(k)) \quad &= (\sum_{i=1}^{k-1} a_{f(i)}) + (a_n + \sum_{i=k+1}^n a_{f(i)}) \\
 ('+' \text{ commutative}) \quad &= (\sum_{i=1}^{k-1} a_{f(i)}) + (\sum_{i=k+1}^n a_{f(i)} + a_n) \\
 ('+' \text{ associative}) \quad &= ((\sum_{i=1}^{k-1} a_{f(i)}) + (\sum_{i=k+1}^n a_{f(i)})) + a_n \\
 \text{(Substitution } j = i + 1) \quad &= ((\sum_{i=1}^{k-1} a_{f(i)}) + (\sum_{j=k}^{n-1} a_{f(j+1)})) + a_n \\
 \text{(definition of } g) \quad &= ((\sum_{i=1}^{k-1} a_{g(i)}) + (\sum_{j=k}^{n-1} a_{g(j)})) + a_n \\
 \text{(GAL)} \quad &= (\sum_{i=1}^{n-1} a_{g(i)}) + a_n \\
 (*) \quad &= (\sum_{i=1}^{n-1} a_i) + a_n \\
 \text{(definition of } \sum) \quad &= \sum_{i=1}^n a_i
 \end{aligned}$$

So the Theorem holds for n and thus by the Principal of Mathematical induction for all positive integers. $\square$

Theorem C.2.3. *Let $+$ be an associative and commutative binary operation on a set G . I a non-empty finite set and for $i \in I$ let $b_i \in G$. Let $g, h : \{1, \dots, n\} \rightarrow I$ be bijections, then*

$$\sum_{i=1}^n b_{g(i)} = \sum_{i=1}^n b_{h(i)}$$

Proof. For $1 \leq i \leq n$, define $a_i = b_{g(i)}$. Let $f = g^{-1} \circ h$. Then f is a bijection. Moreover, $g \circ f = h$ and $a_{f(i)} = b_{g(f(i))} = b_{h(i)}$. Thus

$$\sum_{i=1}^n b_{h(i)} = \sum_{i=1}^n a_{f(i)} \stackrel{\text{C.2.2}}{=} \sum_{i=1}^n a_i = \sum_{i=1}^n b_{g(i)}$$

$\square$

Definition C.2.4. *Let $+$ be an associative and commutative binary operation on a set G . I a finite set and for $i \in I$ let $b_i \in G$. Then $\sum_{i \in I} b_i := \sum_{i=1}^n b_{f(i)}$, where $n = |I|$ and $f := \{1, \dots, n\}$ is bijection. (Observe here that by C.2.3 this does not depend on the choice of f .)*

Theorem C.2.5 (General Commutative Law II). *Let $+$ be an associative and commutative binary operation on a set G . I a finite set, $(I_j \mid j \in J)$ a partition of I and for $i \in I$ let $a_i \in G$. Then*

$$\sum_{i \in I} a_i = \sum_{j \in J} \left(\sum_{i \in I_j} a_i \right)$$

Proof. The proof is by induction on $|J|$. If $|J| = 1$, the result is clearly true. Suppose next that $|J| = 2$ and say $J = \{j_1, j_2\}$. Let $f_i : \{1, \dots, n_i\} \rightarrow I_{j_i}$ be a bijection and define $f : \{1, \dots, n_1 + n_2\} \rightarrow I$ by $f(i) = f_1(i)$ if $1 \leq i \leq n_1$ and $f(i) = f_2(i - n_1)$ if $n_1 + 1 \leq i \leq n_1 + n_2$. Then clearly f is a surjective and so by (F.1.7)(b), f is injective. We compute

$$\begin{aligned} \sum_{i \in I} a_i &= \sum_{i=1}^{n_1+n_2} a_{f(i)} \\ &\stackrel{\text{GAL}}{=} \left(\sum_{i=1}^{n_1} a_{f(i)} \right) + \left(\sum_{i=n_1+1}^{n_1+n_2} a_{f(i)} \right) \\ &= \left(\sum_{i=1}^{n_1} a_{f_1(i)} \right) + \left(\sum_{i=1}^{n_2} a_{f_2(i)} \right) \\ &= \left(\sum_{i \in I_{j_1}} a_i \right) + \left(\sum_{i \in I_{j_2}} a_i \right) \\ &= \sum_{j \in J} \left(\sum_{i \in I_j} a_i \right) \end{aligned}$$

Thus the theorem holds if $|J| = 2$. Suppose now that the theorem is true whenever $|J| = k$. We need to show it is also true if $|J| = k + 1$. Let $j \in J$ and put $Y = I \setminus J_j$. Then $(I_k \mid j \neq k \in J)$ is a partition of Y and (I_j, Y) is partition of I . By the induction assumption, $\sum_{i \in Y} a_i = \sum_{j \neq k \in J} \left(\sum_{i \in I_k} a_i \right)$ and so by the $|J| = 2$ -case

$$\begin{aligned} \sum_{i \in I} a_i &= \left(\sum_{i \in I_j} a_i \right) + \left(\sum_{i \in Y} a_i \right) \\ &= \left(\sum_{i \in I_j} a_i \right) + \left(\sum_{j \neq k \in J} \left(\sum_{i \in I_k} a_i \right) \right) \\ &= \sum_{j \in J} \left(\sum_{i \in I_j} a_i \right) \end{aligned}$$

The theorem now follows from the Principal of Mathematical Induction. □

C.3 The General Distributive Law

Definition C.3.1. *Let $(+, \cdot)$ be a pair of binary operation on the set G . We say that*

- (a) $(+, \cdot)$ is left-distributive if $a(b + c) = (ab) + (ac)$ for all $a, b, c \in G$.
- (b) $(+, \cdot)$ is right-distributive if $(b + c)a = (ba) + (ca)$ for all $a, b, c \in G$.
- (c) $(+, \cdot)$ is distributive if its is right- and left-distributive.

Theorem C.3.2 (General Distributive Law). *Let $(+, \cdot)$ be a pair of binary operations on the set G .*

(a) Suppose $(+, \cdot)$ is left-distributive and let $a, b_1, \dots, b_m \in G$. Then

$$a \cdot \left(\sum_{j=1}^m b_j \right) = \sum_{j=1}^m ab_j$$

(b) Suppose $(+, \cdot)$ is right-distributive and let $a_1, \dots, a_n, b \in G$. Then

$$\left(\sum_{i=1}^m a_i \right) \cdot b = \sum_{i=1}^n a_i b$$

(c) Suppose $(+, \cdot)$ is distributive and let $a_1, \dots, a_n, b_1, \dots, b_m \in G$. Then

$$\left(\sum_{i=1}^n a_i \right) \cdot \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \left(\sum_{j=1}^m a_i b_j \right)$$

Proof. (a) Clearly (a) is true for $m = 1$. Suppose now (a) is true for k and let $a, b_1, \dots, b_{k+1} \in G$. Then

$$\begin{aligned} & a \cdot \left(\sum_{i=1}^{k+1} b_i \right) \\ \text{(definition of } \Sigma) &= a \cdot \left(\left(\sum_{i=1}^k b_i \right) + b_{k+1} \right) \\ \text{(left-distributive)} &= a \cdot \left(\sum_{i=1}^k b_i \right) + a \cdot b_{k+1} \\ \text{(induction assumption)} &= \left(\sum_{i=1}^k ab_i \right) + ab_{k+1} \\ \text{(definition of } \Sigma) &= \sum_{i=1}^{k+1} ab_i \end{aligned}$$

Thus (a) holds for $k + 1$ and so by induction for all positive integers n .

The proof of (b) is virtually the same as the proof of (a) and we leave the details to the reader.

(c)

$$\left(\sum_{i=1}^m a_i \right) \cdot \left(\sum_{j=1}^k b_j \right) \stackrel{(b)}{=} \sum_{i=1}^n \left(a_i \sum_{j=1}^m b_j \right) \stackrel{(a)}{=} \sum_{i=1}^n \left(\sum_{j=1}^m a_i b_j \right)$$

□

Appendix D

Verifying Ring Axioms

Theorem D.0.1. *Let $(R, +, \cdot)$ be ring and $(S, \oplus, \odot)$ a set with binary operations $\oplus$ and $\odot$. Suppose there exists an surjective homomorphism $\Phi : R \rightarrow S$ (that is an surjective function $\Phi : R \rightarrow S$ with $\Phi(a + b) = \Phi(a) \oplus \Phi(b)$ and $\Phi(ab) = \Phi(a) \odot \Phi(b)$ for all $a, b \in R$. Then*

(a) $(S, \oplus, \odot)$ is a ring and Φ is ring homomorphism.

(b) If R is commutative, so is S .

Proof. (a) Clearly if S is a ring, then Φ is a ring homomorphism. So we only need to verify the eight ring axioms. For this let $a, b, c \in S$. Since Φ is surjective ther exist $x, y, z \in R$ with $\Phi(x) = a$, $\Phi(y) = b$ and $\Phi(z) = c$.

Ax 1 By assumption $\oplus$ is binary operation. So **Ax 1** holds for S .

Ax 2

$$\begin{aligned} a \oplus (b \oplus c) &= \Phi(x) \oplus (\Phi(y) \oplus \Phi(z)) = \Phi(x) \oplus \Phi(y + z) = \Phi(x + (y + z)) \\ &= \Phi((x + y) + z) = \Phi(x + y) \oplus \Phi(z) = (\Phi(x) \oplus \Phi(y)) \oplus \Phi(z) = (a \oplus b) \oplus c \end{aligned}$$

Ax 3 $a \oplus b = \Phi(x) \oplus \Phi(y) = \Phi(x + y) = \Phi(y + x) = \Phi(y) \oplus \Phi(x) = b \oplus a$

Ax 4 Put $0_S = \Phi(0_R)$. Then

$$a \oplus 0_S = \Phi(x) \oplus \Phi(0_R) = \Phi(x + 0_R) = \Phi(x) = a$$

$$0_S + a = \Phi(0_R) \oplus \Phi(x) = \Phi(0_R + x) = \Phi(x) = a.$$

Ax 5 Put $d = \Phi(-x)$. Then

$$a \oplus d = \Phi(x) \oplus \Phi(-x) = \Phi(x + (-x)) = \Phi(0_R) = 0_S$$

Ax 6 By assumption $\odot$ is binary operation . So **Ax 6** holds for S .

Ax 7

$$\begin{aligned}
a \odot (b \odot c) &= \Phi(x) \odot (\Phi(y) \odot \Phi(z)) = \Phi(x) \odot \Phi(yz) = \Phi(x(yz)) \\
&= \Phi((xy)z) = \Phi(xy) \odot \Phi(z) = (\Phi(x) \odot \Phi(y)) \odot \Phi(z) = (a \odot b) \odot c
\end{aligned}$$

Ax 8

$$\begin{aligned}
a \odot (b \oplus c) &= \Phi(x) \odot (\Phi(y) \oplus \Phi(z)) = \Phi(x) \odot \Phi(y+z) = \Phi(x(y+z)) \\
= \Phi(xy+xz) &= \Phi(xy) + \Phi(xz) = (\Phi(x) \odot \Phi(y)) + (\Phi(x) \odot \Phi(z)) = (a \odot b) \oplus (a \odot c)
\end{aligned}$$

Similarly $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

(b) Suppose R is commutative then

$$\mathbf{Ax\ 9} \quad a \odot b = \Phi(x) \odot \Phi(y) = \Phi(xy) = \Phi(yx) = \Phi(y) \odot \Phi(x) = b \odot a$$

□

Appendix E

Constructing rings from given rings

E.1 Direct products of rings

Definition E.1.1. Let $(R_i)_{i \in I}$ be a family of rings (that is I is a set and for each $i \in I$, R_i is a ring).

- (a) $\times_{i \in I} R_i$ is the set of all functions $r : I \rightarrow \bigcup_{i \in I} R_i, i \mapsto r_i$ such that $r_i \in R_i$ for all $i \in I$.
- (b) $\times_{i \in I} R_i$ is called the direct product of $(R_i)_{i \in I}$.
- (c) We denote $r \in \times_{i \in I} R_i$ by $(r_i)_{i \in I}$, $(r_i)_i$ or (r_i) .
- (d) For $r = (r_i)$ and $s = (s_i)$ in R define $r + s = (r_i + s_i)$ and $rs = (r_i s_i)$.

Theorem E.1.2. Let $(R_i)_{i \in I}$ be a family of rings.

- (a) $R := \times_{i \in I} R_i$ is a ring.
- (b) $0_R = (0_{R_i})_{i \in I}$.
- (c) $-(r_i) = (-r_i)$.
- (d) If each R_i is a ring with identity, then also $\times_{i \in I} R_i$ is a ring with identity and $1_R = (1_{R_i})$.
- (e) If each R_i is commutative, then $\times_{i \in I} R_i$ is commutative.

Proof. Left as an exercise. □

E.2 Matrix rings

Definition E.2.1. Let R be a ring and m, n positive integers.

- (a) An $m \times n$ -matrix with coefficients in R is a function

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \rightarrow R, \quad (i, j) \mapsto a_{ij}.$$

- (b) We denote an $m \times n$ -matrix A by $[a_{ij}]_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}}$, $[a_{ij}]_{ij}$, $[a_{ij}]$ or

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

- (c) Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $m \times n$ matrices with coefficients in R . Then $A + B$ is the $m \times n$ -matrix $A + B := [a_{ij} + b_{ij}]$.
- (d) Let $A = [a_{ij}]_{ij}$ be an $m \times n$ -matrix and $B = [b_{jk}]_{jk}$ an $n \times p$ matrix with coefficients in R . Then AB is the $m \times p$ matrix $AB = [\sum_{j=1}^n a_{ij}b_{jk}]_{ik}$.
- (e) $M_{mn}(R)$ denotes the set of all $m \times n$ matrices with coefficients in R . $M_n(R) = M_{nn}(R)$.

It might be useful to write out the above definitions of $A + B$ and AB in longhand notation:

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{bmatrix}$$

and

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} + \dots + a_{1n}b_{n1} & a_{11}b_{12} + a_{12}b_{22} + \dots + a_{1n}b_{n2} & \dots & a_{11}b_{1p} + a_{12}b_{2p} + \dots + a_{1n}b_{np} \\ a_{21}b_{11} + a_{22}b_{21} + \dots + a_{2n}b_{n1} & a_{21}b_{12} + a_{22}b_{22} + \dots + a_{2n}b_{n2} & \dots & a_{21}b_{1p} + a_{22}b_{2p} + \dots + a_{2n}b_{np} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{11} + a_{m2}b_{21} + \dots + a_{mn}b_{n1} & a_{m1}b_{12} + a_{m2}b_{22} + \dots + a_{mn}b_{n2} & \dots & a_{m1}b_{1p} + a_{m2}b_{2p} + \dots + a_{mn}b_{np} \end{bmatrix}$$

Theorem E.2.2. *Let n be an integer and R a ring. Then*

- (a) $(M_n(R), +, \cdot)$ is a ring.
- (b) $0_{M_n(R)} = (0_R)_{ij}$.
- (c) $-[a_{ij}] = [-a_{ij}]$ for any $[a_{ij}] \in M_n(R)$.
- (d) If R has an identity, then $M_n(R)$ has an identity and $1_{M_n(R)} = (\delta_{ij})$, where

$$\delta_{ij} = \begin{cases} 1_R & \text{if } i = j \\ 0_R & \text{if } i \neq j \end{cases}$$

Proof. Put $J = \{1, \dots, n\} \times \{1, \dots, m\}$ and observe that $(M_n(R), +) = (\times_{j \in J} R, +)$. So E.1.2 implies that **Ax 1-Ax 5**, (b) and (c) hold.

Clearly **Ax 6** holds. To verify **Ax 7** let $A = [a_{ij}]$, $B = [b_{jk}]$ and $C = [c_{kl}]$ be in $M_n(R)$. Put $D = AB$ and $E = BC$. Then

$$(AB)C = DC = \left[\sum_{k=1}^n d_{ik} c_{kl} \right]_{il} = \left[\sum_{k=1}^n \left(\sum_{j=1}^n a_{ij} b_{jk} \right) c_{kl} \right]_{il} = \left[\sum_{j=1}^n \sum_{k=1}^n a_{ij} b_{jk} c_{kl} \right]_{il}$$

and

$$A(BC) = AE = \left[\sum_{j=1}^n a_{ij} e_{jl} \right]_{il} = \left[\sum_{j=1}^n a_{ij} \left(\sum_{k=1}^n b_{jk} c_{kl} \right) \right]_{il} = \left[\sum_{j=1}^n \sum_{k=1}^n a_{ij} b_{jk} c_{kl} \right]_{il}$$

Thus $A(BC) = (AB)C$.

$$\begin{aligned} (A+B)C &= [a_{ij} + b_{ij}]_{ij} \cdot [c_{jk}]_{jk} = \left[\sum_{j=1}^n (a_{ij} + b_{ij}) c_{jk} \right]_{ik} \\ &= \left[\sum_{j=1}^n a_{ij} c_{jk} \right]_{ik} + \left[\sum_{j=1}^n b_{ij} c_{jk} \right]_{ik} = AC + BC. \end{aligned}$$

So $(A+B)C = AC + BC$ and similarly $A(B+C) = AB + AC$. Thus $M_n(R)$ is a ring.

Suppose now that R has an identity 1_R . Put $I = [\delta_{ij}]_{ij}$, where

$$\delta_{ij} = \begin{cases} 1_R & \text{if } i = j \\ 0_R & \text{if } i \neq j \end{cases}$$

If $i \neq j$, then $\delta_{ij} a_{jk} = 0_R a_{jk} = 0_R$ and if $i = j$ then $\delta_{ij} a_{jk} = 1_R a_{jk} = a_{ik}$. Thus

$$IA = \left[\sum_{j=1}^n \delta_{ij} a_{jk} \right]_{ik} = [a_{ik}]_{ik} = A$$

and similarly $AI = A$. Thus A is an identity in R and so (d) holds. □

E.3 Polynomial Rings

In this section we show that if R is ring with identity then existence of a polynomial ring with coefficients in R .

Theorem E.3.1. *Let R be a ring. Let P be the set of all functions $f: \mathbb{N} \rightarrow R$ such that there exists $m \in \mathbb{N}^*$ with*

$$(1) \quad f(i) = 0_R \text{ for all } i > m$$

We define an addition and multiplication on P by

$$(2) \quad (f + g)(i) = f(i) + g(i) \quad \text{and} \quad (fg)(i) = \sum_{k=0}^i f(k)g(i-k)$$

(a) P is a ring.

(b) For $r \in R$ define $r^\circ \in P$ by

$$(3) \quad r^\circ(i) := \begin{cases} r & \text{if } i = 0 \\ 0_R & \text{if } i \neq 0 \end{cases}$$

Then the function $R \rightarrow P, r \mapsto r^\circ$ is a injective homomorphism.

(c) Suppose R has an identity and define $x \in P$ by

$$x(i) := \begin{cases} 1_R & \text{if } i = 1 \\ 0_R & \text{if } i \neq 1 \end{cases}$$

Then (after identifying $r \in R$ with r° in P), P is a polynomial ring in x with coefficients in R .

Proof. Let $f, g \in P$. Let $\deg f$ be the minimal $m \in \mathbb{N}^*$ for which (1) holds. Observe that (2) defines functions $f + g$ and fg from $\mathbb{N}$ to R . So to show that $f + g$ and fg are in P we need to verify that (1) holds for $f + g$ and fg as well. Let $m = \max(\deg f, \deg g)$ and $n = \deg f + \deg g$. Then for $i > m$, $f(i) = 0_R$ and $g(i) = 0_R$ and so also $(f + g)(i) = 0_R$. Also if $i > n$ and $0 \leq k \leq i$, then either $k < \deg f$ or $i - k > \deg g$. In either case $f(k)g(i - k) = 0_R$ and so $(fg)(i) = 0_R$. So we indeed have $f + g \in P$ and $fg \in P$. Thus axiom **Ax 1** and **Ax 6** hold. We now verify the remaining axioms one by one. Observe that f and g in P are equal if and only if $f(i) = g(i)$ for all $i \in \mathbb{N}$. Let $f, g, h \in P$ and $i \in \mathbb{N}$.

(Ax 2)

$$\begin{aligned} ((f + g) + h)(i) &= (f + g)(i) + h(i) = (f(i) + g(i)) + h(i) = f(i) + (g(i) + h(i)) \\ &= f(i) + (g(i) + h(i)) = f(i) + (g + h)(i) = (f + (g + h))(i) \end{aligned}$$

$$\textbf{(Ax 3)} \quad (f + g)(i) = f(i) + g(i) = g(i) + f(i) = (g + f)(i)$$

$$\textbf{(Ax 4)} \quad \text{Define } 0_P \in P \text{ by } 0_P(i) = 0_R \text{ for all } i \in \mathbb{N}. \text{ Then}$$

$$(f + 0_P)(i) = f(i) + 0_P(i) = f(i) + 0_R = f(i)$$

$$(0_P + f)(i) = 0_P(i) + f(i) = 0_R + f(i) = f(i)$$

$$\textbf{Ax 5} \quad \text{Define } -f \in P \text{ by } (-f)(i) = -f(i) \text{ for all } i \in \mathbb{N}. \text{ Then}$$

$$(f + (-f))(i) = f(i) + (-f)(i) = f(i) + (-f(i)) = 0_R = 0_P(i)$$

Ax 7 Any triple of non-negative integers (k, l, p) with $k + l + p = i$ be uniquely written as $(k, j - k, i - j)$ where $0 \leq j \leq i$ and $0 \leq k \leq j - k$ and uniquely as $(k, l, i - k - l)$ where $0 \leq i \leq k$ and $0 \leq l \leq i - k$. This is used in the fourth equality sign in the following computation:

$$\begin{aligned} ((fg)h)(i) &= \sum_{j=0}^i (fg)(j) \cdot h(i-j) = \sum_{j=0}^i \left(\left(\sum_{k=0}^j f(k)g(j-k) \right) h(i-j) \right) \\ &= \sum_{j=0}^i \left(\sum_{k=0}^j f(k)g(j-k)h(i-j) \right) = \sum_{k=0}^i \left(\sum_{l=0}^{i-k} f(k)g(l)h(i-k-l) \right) \\ &= \sum_{k=0}^i \left(f(k) \left(\sum_{l=0}^{i-k} g(l)h(i-k-l) \right) \right) = \sum_{k=0}^i f(k) \cdot (gh)(i-k) \\ &= (f(gh))(i) \end{aligned}$$

Ax 8

$$\begin{aligned} (f \cdot (g + h))(i) &= \sum_{j=0}^i f(j) \cdot (g + h)(i-j) = \sum_{j=0}^i f(j) \cdot (g(i-j) + h(i-j)) \\ &= \sum_{j=0}^i f(j)g(i-j) + f(j)h(i-j) = \sum_{j=0}^i f(j)g(i-j) + \sum_{j=0}^i f(j)h(i-j) \\ &= (fg)(i) + (fh)(i) = (fg + fh)(i) \end{aligned}$$

$$\begin{aligned} ((f + g) \cdot h)(i) &= \sum_{j=0}^i (f + g)(j) \cdot h(i-j) = \sum_{j=0}^i (f(j) + g(j)) \cdot h(i-j) \\ &= \sum_{j=0}^i f(j)h(i-j) + g(j)h(i-j) = \sum_{j=0}^i f(j)h(i-j) + \sum_{j=0}^i g(j)h(i-j) \\ &= (fh)(i) + (gh)(i) = (fh + gh)(i) \end{aligned}$$

Since **Ax 1** through **Ax 8** hold we conclude that P is a ring and (a) is proved. Let $r, s \in R$ and $k, l \in \mathbb{N}$. We compute

$$(4) \quad (r+s)^\circ(i) = \begin{cases} r+s & \text{if } i=0 \\ 0_R & \text{if } i \neq 0 \end{cases} = r^\circ(i) + s^\circ(i) = (r^\circ + s^\circ)(i)$$

and

$$(r^\circ s)(i) = \sum_{k=0}^i r^\circ(k)s(i-k)$$

Note that $r^\circ(k) = 0_R$ unless $k=0$ and $s^\circ(i-k) = 0_R$ unless $i-k=0$. Hence $r^\circ(k)s(i-k) = 0_R$ unless $k=0$ and $i-k=0$ (and so also $i=0$). Thus $(r^\circ s)(i) = 0$ if $i \neq 0$ and $(r^\circ s)(0) = r^\circ(0)s^\circ(0) = rs$. This

$$(5) \quad r^\circ s^\circ = (rs)^\circ$$

Define $\rho: R \rightarrow P, r \mapsto r^\circ$. If $r, s \in R$ with $r^\circ = s^\circ$, then $r = r^\circ(1) = s^\circ(1) = s$ and so ρ is injective. By (4) and (5), ρ is a homomorphism and so (b) is proved.

Assume from now on that R has an identity.

For $k \in \mathbb{N}$ let $\delta_k \in P$ be defined by

$$(6) \quad \delta_k(i) := \begin{cases} 1_R & \text{if } i=k \\ 0_R & \text{if } i \neq k \end{cases}$$

Let $f \in P$. Then

$$(7) \quad (r^\circ f)(i) = \sum_{k=0}^i r^\circ(k)f(i-k) = r \cdot f(i) + \sum_{i=1}^k 0_R f(i-k) = r \cdot f(i)$$

and similarly

$$(8) \quad (f r^\circ)(i) = f(i) \cdot r$$

In particular, 1_R° is an identity in P . Since $\delta_0 = 1_R^\circ$ we conclude

$$(9) \quad \delta_0 = 1_R^\circ = 1_P$$

For $f = \delta_k$ we conclude that

$$(10) \quad (r^\circ \delta_k)(i) = (\delta_k r^\circ)(i) = \begin{cases} r & \text{if } i=k \\ 0_R & \text{if } i \neq k \end{cases}$$

Let $m \in \mathbb{N}$ and $a_0, \dots, a_m \in R$. Then (10) implies

$$(11) \quad \left(\sum_{k=0}^m a_k^\circ \delta \right)(i) = \begin{cases} a_i & \text{if } i \leq m \\ 0_R & \text{if } i > m \end{cases}$$

We conclude that if $f \in P$ and $a_0, a_1, a_2, \dots, a_m \in R$ then

$$(12) \quad f = \sum_{k=0}^m a_k^\circ \delta_k \iff m \geq \deg f \text{ and } a_k = f(k) \text{ for all } 0 \leq k \leq m$$

We compute

$$(13) \quad (\delta_k \delta_l)(i) = \sum_{j=0}^i \delta_k(j) \delta_l(i-j)$$

Since $\delta_k(j) \delta_l(i-j)$ is 0_R unless $j = k$ and $l = i-j$, that is unless $j = k$ and $i = l+k$, in which case it is 1_R , we conclude

$$(14) \quad (\delta_k \delta_l)(i) = \begin{cases} 1_R & \text{if } i = k+l \\ 0_R & \text{if } i \neq k+l \end{cases} = \delta_{k+l}(i)$$

and so

$$(15) \quad \delta_k \delta_l = \delta_{k+l}$$

Note that $x = \delta_1$. We conclude that

$$(16) \quad x^k = \delta_k$$

By (10)

$$(17) \quad r^\circ x = x r^\circ \quad \text{for all } r \in R$$

We will now verify the four conditions (i)-(iv) in the definition of a polynomial. By (b) we can identify r with r° in R . Then R becomes a subring of P . By (9), $1_R^\circ = 1_P$. So (i) holds. By (17), (ii) holds. (iii) and (iv) follow from (12) and (16). $\square$

Theorem E.3.2. *Let R be a ring with identity and for $i = 1, 2$ let P_i be a polynomial ring in x_i with coefficients in R . Then there exists an isomorphism $\Phi : P_1 \rightarrow P_2$ with $\Phi(x_1) = x_2$ and $\Phi(r) = r$ for all $r \in R$. Moreover*

$$\Phi(f) = \sum_{i=0}^{\deg f} f_i x_2^i$$

for all $f = \sum_{i=0}^{\deg f} f_i x_1^i \in P_1$.

Proof. Since P_1 is a polynomial ring in x_1 with coefficients in R we can apply 2.6.1 with $R[x_1] = P_1$, $S = P_2$, $\alpha = \text{id}_R$ and $s = x_2$. Hence there exists a unique homomorphism $\Phi : P_1 \rightarrow P_2$ with $\Phi(x_1) = x_2$ and $\Phi(r) = r$ for all $r \in R$ and

$$\Phi(f) = \sum_{i=0}^{\deg f} f_i x_2^i$$

for all $f = \sum_{i=0}^{\deg f} f_i x_1^i \in P_1$.

Suppose $\Phi(f) = \Phi(g)$ for some $f, g \in P_1$. Then

$$\sum_{i=0}^{\deg f} f_i x_2^i = \sum_{i=0}^{\deg g} g_i x_2^i$$

Since P_2 is a polynomial ring in x_2 with coefficients in R this gives $f_i = g_i$ for all $i \in \mathbb{N}$ and so $f = g$. Thus Φ is injective.

Let $h \in P_2$. Since P_2 is a polynomial ring in x_2 with coefficients in R , we have $h = \sum_{i=0}^{\deg h} h_i x_2^i$. Put $f = \sum_{i=0}^{\deg h} h_i x_1^i \in P_1$. Then $\Phi(f) = h$ and so Φ is surjective.

We proved that Φ is an injective and surjective homomorphism and so Φ is an isomorphism. $\square$

Let F be a field and p a non-constant polynomial in $F[x]$. Then 2.10.3 shows that $F[x]/(p)$ contains a subring isomorphic to F . This suggests that there exists a ring isomorphic to $F[x]/(p)$ containing F has a subring. The next theorem shows that this is indeed true.

Theorem E.3.3. *Let F be a field and p be a non-constant polynomial in $F[x]$. Then there exist a ring R and $\alpha \in R$ such that*

- (a) F is a subring of R ,
- (b) there exists an isomorphism $\Phi : R \rightarrow F[x]/(p)$ with $\Phi(\alpha) = [x]_p$ and $\Phi(a) = [a]_p$ for all $a \in F$,
- (c) R is a commutative ring with identity and $1_R = 1_F$.

Proof. As in 2.10.3 put $\hat{F} := \{[a]_p \mid a \in F\}$. Define

$$S := F[x]/(p) \setminus \hat{F} \quad \text{and} \quad R := F \cup S.$$

(So for $a \in F$ we removed $[a]_p$ from $F[x]/(p)$ and replaced it by a .) Define

$$\Phi: R \rightarrow F[x]/(p), \quad r \mapsto \begin{cases} [r]_p & \text{if } r \in F \\ r & \text{if } r \in S \end{cases}$$

Note that $R = F \cup S$, $S \cap F = \emptyset$, $F[x]/(p) = \hat{F} \cup S$ and $\hat{F} \cap S = \emptyset$. By 2.10.3 the function $F \rightarrow \hat{F}, a \rightarrow [a]_p$ is bijection. Also $\text{id}_S: S \rightarrow S, s \rightarrow s$ is a bijection. It follows that Φ is a bijection see Exercise A.4#2.

Next we define an addition $\oplus$ and a multiplication $\odot$ on R by

$$(*) \quad r \oplus s = \Phi^{-1}(\Phi(r) + \Phi(s)) \quad \text{and} \quad r \odot s := \Phi^{-1}(\Phi(r)\Phi(s)).$$

Observe that $\Phi(\Phi^{-1}(u)) = u$ for all $u \in F[x]/(p)$. So applying Φ to both sides of $(*)$ gives

$$\Phi(r \oplus s) = \Phi(r) + \Phi(s) \quad \text{and} \quad \Phi(r \odot s) = \Phi(r)\Phi(s)$$

for all $r, s \in R$. Hence D.0.1 implies that R is ring and Φ is an isomorphism. Put $\alpha = [x]_p$. Then $\alpha \in S$ and so $\alpha \in R$. Moreover $\Phi(\alpha) = \Phi([x]_p) = [x]_p$. Let $a \in F$. Then $a \in R$ and $\Phi(a) = [a]_p$. Thus (b) holds.

For $a, b \in F$ we have

$$a \oplus b = \Phi^{-1}(\Phi(a) + \Phi(b)) = \Phi^{-1}([a]_p + [b]_p) = \Phi^{-1}([a+b]_p) = \Phi^{-1}(\Phi(a+b)) = a+b \in F$$

and

$$a \odot b = \Phi^{-1}(\Phi(a)\Phi(b)) = \Phi^{-1}([a]_p[b]_p) = \Phi^{-1}([ab]_p) = \Phi^{-1}(\Phi(ab)) = ab \in F$$

It follows that 0_F is the additive identity of R and that the additive inverse $-a$ of a in F is also the additive inverse of a in R . Since $0_F \in F$ and $-a \in F$, the Subring Theorem now shows that F is a subring of R . Thus also (a) is proved.

By 2.10.3 $F[x]/(p)$ is a commutative ring with identity $[1_F]_p$. Since Φ is an isomorphism we conclude that R is a commutative ring with identity 1_F . $\square$

Appendix F

Cardinalities

F.1 Cardinalities of Finite Sets

Notation F.1.1. For $a, b \in \mathbb{Z}$ set $[a \dots b] := \{c \in \mathbb{Z} \mid a \leq c \leq b\}$.

Theorem F.1.2. Let $A \subsetneq [1 \dots n]$. Then there exists a bijection $\alpha : [1 \dots n] \rightarrow [1 \dots n]$ with $\alpha(A) \subseteq [1 \dots n-1]$.

Proof. Since $A \neq [1 \dots n]$ there exists $m \in [1 \dots n]$ with $m \notin A$. Define $\alpha : [1 \dots n] \rightarrow [1 \dots n]$ by $\alpha(n) = m$, $\alpha(m) = n$ and $\alpha(i) = i$ for all $i \in [1 \dots n]$ with $n \neq i \neq m$. It is easy to verify that α is bijection. Since $\alpha(m) = n$ and $m \notin A$, $\alpha(a) \neq n$ for all $a \in A$. So $n \notin \alpha(A)$ and so $\alpha(A) \subseteq [1 \dots n-1]$. $\square$

Theorem F.1.3. Let $n \in \mathbb{N}$ and let $\beta : [1 \dots n] \rightarrow [1 \dots n]$ be a function. If β is injective, then β is surjective.

Proof. The proof is by induction on n . If $n = 1$, then $\beta(1) = 1$ and so β is surjective. Let $A = \beta([1 \dots n-1])$. Since $\beta(n) \notin A$, $A \subsetneq [1 \dots n]$. Thus by F.1.2 there exists a bijection $\alpha : [1 \dots n]$ with $\alpha(A) \subseteq [1 \dots n-1]$. Thus $\alpha\beta([1 \dots n-1]) \subseteq [1 \dots n-1]$. By induction $\alpha\beta([1 \dots n-1]) = [1 \dots n-1]$. Since $\alpha\beta$ is injective we conclude that $\alpha\beta(n) = n$. Thus $\alpha\beta$ is surjective and $\alpha\beta$ is a bijection. Since α is also a bijection this implies that β is a bijection. $\square$

Definition F.1.4. A set A is finite if there exists $n \in \mathbb{N}$ and a bijection $\alpha : A \rightarrow [1 \dots n]$.

Theorem F.1.5. Let A be a finite set. Then there exists a unique $n \in \mathbb{N}$ for which there exists a bijection $\alpha : A \rightarrow [1 \dots n]$.

Proof. By definition of a finite set F.1.4 there exist $n \in \mathbb{N}$ and a bijection $\alpha : A \rightarrow [1 \dots n]$. Suppose that also $m \in \mathbb{N}$ and $\beta : A \rightarrow [1 \dots m]$ is a bijection. We need to show that $n = m$ and may assume that $n \leq m$. Let $\gamma : [1 \dots n] \rightarrow [1 \dots m]$, $i \mapsto i$ and $\delta := \gamma \circ \alpha \circ \beta^{-1}$. Then γ is an injective function from $[1 \dots m]$ to $[1 \dots m]$ and so by F.1.3, δ is surjective. Thus also γ is surjective. Since $\gamma([1 \dots n]) = [1 \dots n]$ we conclude that $[1 \dots n] = [1 \dots m]$ and so also $n = m$. $\square$

Definition F.1.6. Let A be a finite set. Then the unique $n \in \mathbb{N}$ for which there exists a bijection $\alpha : A \rightarrow [1 \dots n]$ is called the cardinality or size of A and is denoted by $|A|$.

Theorem F.1.7. Let A and B be finite sets.

- (a) If $\alpha : A \rightarrow B$ is injective then $|A| \leq |B|$, with equality if and only if α is surjective.
- (b) If $\alpha : A \rightarrow B$ is surjective then $|A| \geq |B|$, with equality if and only if α is injective.
- (c) If $A \subseteq B$ then $|A| \leq |B|$, with equality if and only if $|A| = |B|$.

Proof. (a) If α is surjective then α is a bijection and so $|A| = |B|$. So it suffices to show that if $|A| \geq |B|$, then α is surjective. Put $n = |A|$ and $m = |B|$ and let $\beta : A \rightarrow [1 \dots n]$ and $\gamma : B \rightarrow [1 \dots m]$ be bijection. Assume $n \geq m$ and let $\delta : [1 \dots m] \rightarrow [1 \dots n]$ be the inclusion map. Then $\delta\gamma\alpha\beta^{-1}$ is an injective function from $[1 \dots m]$ to $[1 \dots n]$ and so by F.1.3 it is surjective. Hence δ is surjective, $n = m$ and δ is bijection. Since also γ is bijection, this forces $\alpha\beta^{-1}$ to be surjective and so also α is surjective.

(b) Since α is surjective there exists $\beta : B \rightarrow A$ with $\alpha\beta = \text{id}_B$. Then β is injective and so by (a), $|B| \leq |A|$ and β is a bijection if and only if $|A| = |B|$. Since α is a bijection if and only if β is, (b) is proved.

(c) Follows from (a) applied to the inclusion map $A \rightarrow B$. □

Theorem F.1.8. Let A and B be finite sets. Then

- (a) If $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$.
- (b) $|A \times B| = |A| \cdot |B|$.

Proof. (a) Put $n = |A|$, $m = |B|$ and let $\beta : A \rightarrow [1 \dots n]$ and $\gamma : B \rightarrow [1 \dots m]$ be bijections. Define $\gamma : A \cup B \rightarrow [1 \dots n + m]$ by

$$\gamma(c) = \begin{cases} \alpha(c) & \text{if } c \in A \\ \beta(c) + n & \text{if } c \in B \end{cases}$$

Then it is readily verified that γ is a bijection and so $|A \cup B| = n + m = |A| + |B|$.

(b) The proof is by induction on $|B|$. If $|B| = 0$, then $B = \emptyset$ and so also $A \times B = \emptyset$. If $|B| = 1$, then $B = \{b\}$ for some $b \in B$ and so the map $A \rightarrow A \times B, a \mapsto (a, b)$ is a bijection. Thus $|A \times B| = |A| = |A| \cdot |B|$. Suppose now that (b) holds for any set B of size k . Let C be a set of size $k + 1$. Pick $c \in C$ and put $B = C \setminus \{c\}$. Then $C = B \cup \{c\}$ and so (a) implies $|B| = k$. So by induction $|A \times B| = |A| \cdot k$. Also $|A \times \{c\}| = |A|$ and so by (a)

$$|A \times C| = |A \times B| + |A \times \{c\}| = |A| \cdot k + |A| = |A| \cdot (k + 1) = |A| |C|$$

(b) now follows from the principle of mathematical induction A.5.2. □

Appendix G

List of Important Theorems and Definitions

Definition 1.1.1. A ring is a triple $(R, +, \cdot)$ such that

- (i) R is a set;
- (ii) $+$ is a function (called ring addition) and $R \times R$ is a subset of the domain of $+$. For $(a, b) \in R \times R$, $a + b$ denotes the image of (a, b) under $+$;
- (iii) $\cdot$ is a function (called ring multiplication) and $R \times R$ is a subset of the domain of $\cdot$. For $(a, b) \in R \times R$, $a \cdot b$ (and also ab) denotes the image of (a, b) under $\cdot$;

and such that the following eight statement hold:

- (Ax 1) $a + b \in R$ for all $a, b \in R$; [closure of addition]
- (Ax 2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$; [associative addition]
- (Ax 3) $a + b = b + a$ for all $a, b \in R$. [commutative addition]
- (Ax 4) there exists an element in R , denoted by 0_R and called ‘zero R ’, [additive identity]
such that $a = a + 0_R$ and $a = 0_R + a$ for all $a \in R$;
- (Ax 5) for each $a \in R$ there exists an element in R , denoted by $-a$ [additive inverses]
and called ‘negative a ’, such that $a + (-a) = 0_R$ and $(-a) + a = 0_R$;
- (Ax 6) $ab \in R$ for all $a, b \in R$; [closure of multiplication]
- (Ax 7) $a(bc) = (ab)c$ for all $a, b, c \in R$; [associative multiplication]
- (Ax 8) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$. [distributive laws]

Definition 1.1.2. Let R be a ring. Then R is called commutative if

(Ax 9) $ab = ba$ for all $a, b \in R$. [commutative multiplication]

Definition 1.1.3. Let R be a ring. We say that R is a ring with identity if there exists an element, denoted by 1_R and called ‘one R ’, such that

(Ax 10) $a = 1_R \cdot a$ and $a = a \cdot 1_R$ for all $a \in R$. [multiplicative identity]

Definition 1.8.6. A ring R is called an integral domain provided that

(i) R is commutative,

(ii) R has an identity,

(iii) $1_R \neq 0_R$, and

(Ax 11) whenever $a, b \in R$ with $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.

Definition 1.8.8. A ring R is called a field provided that

(i) R is commutative,

(ii) R has an identity,

(iii) $1_R \neq 0_R$, and

(Ax 12) each $a \in R$ with $a \neq 0_R$ is a unit in R .

Definition 1.11.1. Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings and let $f : R \rightarrow S$ be a function.

(a) f is called a homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ if

$$f(a + b) = f(a) \oplus f(b) \quad [f \text{ respects addition}]$$

and

$$f(a \cdot b) = f(a) \odot f(b) \quad [f \text{ respects multiplication}]$$

for all $a, b \in R$.

(b) f is called an isomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$, if f is a homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ and f is bijective.

(c) $(R, +, \cdot)$ is called isomorphic to $(S, \oplus, \odot)$, if there exists an isomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$.

Theorem 1.2.9. Let R be a ring and $a, b, c \in R$. Then

(a) $-0_R = 0_R$

(c) $a \cdot 0_R = 0_R = 0_R \cdot a$.

(b) $a - 0_R = a$.

(d) $a \cdot (-b) = -(ab) = (-a) \cdot b$.

- (e) $-(-a) = a$. (i) $(-a) \cdot (-b) = ab$.
 (f) $b - a = 0_R$ if and only if $a = b$. (j) $a \cdot (b - c) = ab - ac$ and $(a - b) \cdot c = ac - bc$.
 (g) $-(a + b) = (-a) + (-b) = (-a) - b$. If R has an identity 1_R ,
 (h) $-(a - b) = (-a) + b = b - a$. (k) $(-1_R) \cdot a = -a = a \cdot (-1_R)$.

Theorem 1.4.9. *Let R be a ring and $a, b, n \in R$. Then the following statements are equivalent*

- (a) $a = b + nk$ for some $k \in R$ (g) $[a]_n = [b]_n$.
 (b) $a - b = nk$ for some $k \in R$. (h) $a \in [b]_n$.
 (c) $n | a - b$. (i) $b \equiv a \pmod{n}$
 (d) $a \equiv b \pmod{n}$. (j) $n | b - a$.
 (e) $b \in [a]_n$. (k) $b - a = nl$ for some $l \in R$.
 (f) $[a]_n \cap [b]_n \neq \emptyset$. (l) $b = a + nl$ for some $l \in R$.

Theorem 1.5.1 (The Division Algorithm). *Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Theorem 1.5.5. *Let a, b, n be integers with $n \neq 0$. Then*

$$a \equiv b \pmod{n}$$

if and only if

a and b have the same remainder when divided by n .

Theorem 1.5.7. *Let n be positive integer.*

- (a) *Let $a \in \mathbb{Z}$. Then there exists a unique $r \in \mathbb{Z}$ with $0 \leq r < n$ and $[a]_n = [r]_n$, namely r is the remainder of a when divided by n .*
 (b) *There are exactly n distinct congruence classes modulo n , namely*

$$[0], [1], [2], \dots, [n-1].$$

- (c) $|\mathbb{Z}_n| = n$, that is $\mathbb{Z}_n$ has exactly n elements.

Theorem 1.7.2 (Subring Theorem). *Suppose that R is a ring and S a subset of R . Then S is a subring of R if and only if the following four conditions hold:*

- (I) $0_R \in S$.
- (II) S is closed under addition (that is : if $a, b \in S$, then $a + b \in S$);
- (III) S is closed under multiplication (that is: if $a, b \in S$, then $ab \in S$);
- (IV) S is closed under negatives (that is: if $a \in S$, then $-a \in S$)

Theorem 1.9.7. *Let a and b be integers, not both zero, and let $d \in \mathbb{Z}$ with $d = \gcd(a, b)$. Then d is the smallest positive integer of the form $au + bv$ with $u, v \in \mathbb{Z}$.*

Theorem 1.10.3. *Let p be an integer with $p \notin \{0, \pm 1\}$. Then the following two statements are equivalent:*

- (a) p is a prime.
- (b) If a and b are integers with $p|ab$, then $p|a$ or $p|b$.

Theorem 2.3.1 (Division Algorithm). *Let R be ring with identity and $f, g \in R[x]$ such that $g \neq 0_R$ and $\text{lead}(g)$ is unit in R . Then there exist uniquely determined $q, r \in R[x]$ with*

$$f = gq + r \quad \text{and} \quad \deg r < \deg g.$$

Theorem 2.4.6. *Let F be a field and $f, g \in F[x]$ not both 0_F .*

- (a) *There exists a unique $d \in F[x]$ with $d = \gcd(f, g)$.*
- (b) *There exists $u, v \in F[x]$ with $d = fu + gv$.*
- (c) *If c is a common divisor of f and g , then $c|d$.*

Theorem 2.5.9 (Factorization Theorem). *Let F be a field and f a non-constant polynomial in $F[x]$. Then f is the product of irreducible polynomials in $F[x]$.*

Theorem 2.5.11 (Unique Factorization Theorem). *Let F be a field and f a non-constant polynomial in $F[x]$. Suppose that n, m are positive integers and $p_1, p_2, \dots, p_n$ and $q_1, \dots, q_m$ are irreducible polynomials in $F[x]$ with*

$$f = p_1 p_2 \dots p_n \quad \text{and} \quad f = q_1 q_2 \dots q_m.$$

Then $n = m$ and, possibly after reordering the q_i 's,

$$p_1 \sim q_1, \quad p_2 \sim q_2, \quad \dots, \quad p_n \sim q_n.$$

Theorem 2.7.7 (Factor Theorem). *Let F a field, $f \in F[x]$ and $a \in F$. Then a is a root of f if and only if $x - a|f$ in $F[x]$.*

Theorem 2.7.8. *Let R be commutative ring with identity and $f \in R[x]$.*

- (a) *Let $g \in R[x]$ with $g|f$. Then any root of g in R is also a root of f in R .*

- (b) Let $a \in R$ and $g, h \in R[x]$ with $f = gh$. Suppose that R is field or an integral domain. Then a is a root of f if and only if a is a root of g or a is a root of h .

Theorem 2.10.6. Let F be a field and p a non-constant polynomial in $F[x]$. Let $\alpha \in F_p[\alpha]$ be as in 2.10.5.

- (a) Let $f \in F[x]$. Then $f(\alpha) = [f]_p$.
- (b) For each $\beta \in F_p[\alpha]$ there exists a unique $f \in F[x]$ with $\deg f < \deg p$ and $f(\alpha) = \beta$.
- (c) Let $n = \deg p$. Then for each $\beta \in F_p[\alpha]$ there exist unique $b_0, b_1, \dots, b_{n-1} \in F$ with

$$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}.$$

- (d) Let $f \in F[x]$, then $f(\alpha) = 0_F$ if and only if $p \mid f$ in $F[x]$.
- (e) α is a root of p in $F_p[\alpha]$.

Theorem 2.11.2. Let F be a field and p a non-constant polynomial in $F[x]$. Then the following statements are equivalent:

- (a) p is irreducible in $F[x]$.
- (b) $F_p[\alpha]$ is a field.
- (c) $F_p[\alpha]$ is an integral domain.

Theorem 3.1.2 (Ideal Theorem). Let I be a subset of the ring R . Then I is an ideal of R if and only if the following four conditions holds:

- (i) $0_R \in I$.
- (ii) $a + b \in I$ for all $a, b \in I$.
- (iii) $ra \in I$ and $ar \in I$ for all $a \in I$ and $r \in R$.
- (iv) $-a \in I$ for all $a \in I$.

Theorem 3.1.10. Let R be ring and I an ideal of R . Let $a, b \in R$. Then the following statements are equivalent

- | | |
|--------------------------------------|---|
| (a) $a = b + i$ for some $i \in I$. | (e) $b \in a + I$. |
| (b) $a - b = i$ for some $i \in I$ | (f) $(a + I) \cap (b + I) \neq \emptyset$. |
| (c) $a - b \in I$. | (g) $a + I = b + I$. |
| (d) $a \equiv b \pmod{I}$. | (h) $a \in b + I$. |

$$(i) \quad b \equiv a \pmod{I}.$$

$$(k) \quad b - a = j \text{ for some } j \in I.$$

$$(j) \quad b - a \in I.$$

$$(l) \quad b = a + j \text{ for some } j \in I.$$

Theorem 3.2.9 (First Isomorphism Theorem). *Let $f : R \rightarrow S$ be a ring homomorphism. Recall that $\text{Im } f = \{f(a) \mid a \in R\}$. The function*

$$\overline{f} : R/\text{Ker } f \mapsto \text{Im } f, \quad a + \text{Ker } f \mapsto f(a)$$

is a well-defined isomorphism. In particular $R/\text{Ker } f$ and $\text{Im } f$ are isomorphic rings

Bibliography

- [1] T.W. Hungerford *Abstract Algebra, An Introduction* second edition, Brooks/Cole **1997**.