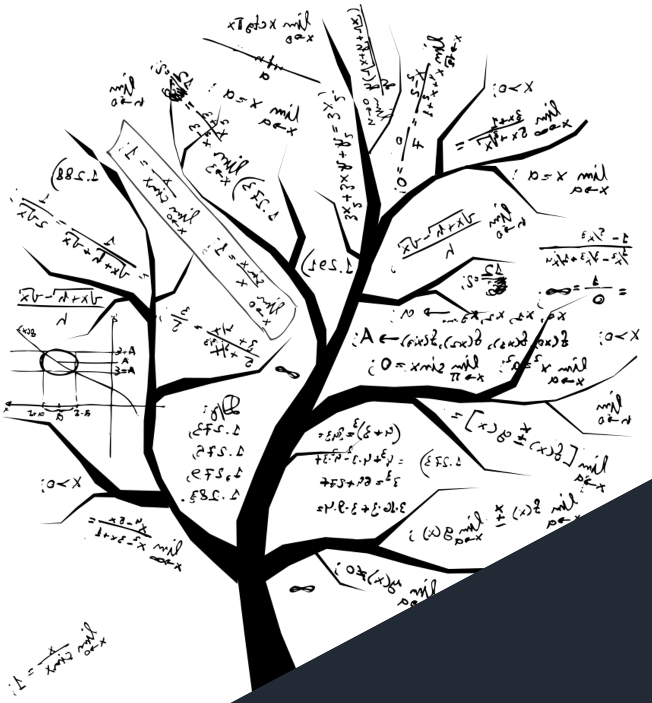
Lebanese University

Faculty of Sciences

Lebanese University
Faculty of Sciences

M1100
Algebra

Department of Mathematics



Fall Semester

2021/2022

PREFACE

This book is a course of algebra for the students of the of the first year of Mathematics, Statistics, Computer Sciences, Physics and Electronics of The Faculty of Science of The Lebanese University.

This course is divided into seven chapters. Chapter I is devoted to the study of the rules of logic and the sets. In chapter II, we study the mappings. Chapter III deals with the finite sets, while chapter IV deals with the binary operations. In chapter V, we study the algebraic structures: group, ring and field. Chapter VI is devoted to the study of the complex numbers and chapter VII is devoted to the study of the polynomials. At the end of the course we give the appendix I which contains the proofs of some theorems that are difficult for the students.

Finally a word about the notation: 1.2.3 will denote the third theorem of the 2nd section of chapter one and the first corollary of this theorem is denoted corollary 1.2.3.1. The symbol ■ will indicate the end of a definition, theorem and a corollary.

Contents

Chapter I Set theory.

Chapter II Mappings.

Chapter III Finite sets

Chapter IV Binary operation.

Chapter V Group ring and field.

Chapter VI Complex numbers.

Chapter VII Polynomials.

Appendix I. Proof of some theorems.

M1100

CHAPTER I

SET THEORY

§ 1.1. LOGIC.

Logic is a language for reasoning. It is a collection of rules dealing with statements. We are only interested with true or false statements. We shall use capital letters to represent such statements.

Let A and B be two statements.

We denote by $\neg A$ (or nonA), the negation of the statement A. The statements (A and B) and (A or B) have their usual meanings as in ordinary language.

(A and B) is denoted $A \wedge B$ and (A or B) is denoted $A \vee B$.

We shall adopt the following axioms:

Axiom 1. The statement $\neg A$ is true if A is false and it is false if A is true. ■

This axiom can be represented by the following table, called **truth table (or table of truthiness)**:

A	$\neg A$
T	F
F	T

where T stands for true and F stands for false.

Axiom 2. $A \wedge B$ is true if A and B are both true and it is false if at least one of A and B is false. ■

The truth table of $A \wedge B$ is:

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

Axiom 3. $A \vee B$ is true if at least one of A and B is true and it is false if A and B are both false. ■

The truth table of $A \vee B$ is:

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

We accept the following:
(i) the statement $(A \wedge \neg A)$ is always false. This is **the principal of non-contradiction**.
(ii) the statement $(A \vee \neg A)$ is always true. This is **the principal of excluded middle**.

A statement which is always true is called a **tautology**.

Definition 1. We say that A **implies** B, if whenever A is true, then B is true. ■

We also say that A implies B in the following cases:
(i) A is always false;
(ii) B is always true.

The statement "A implies B" is written $A \Rightarrow B$. It is read "A implies B" and called an **implication**. It is also called a **conditional** statement**.** A is called the **hypothesis** and B is called the **conclusion**.

The statement "A implies B" is also written in one of the following ways:
"A yields B";
"if A, then B";
"A is a sufficient condition of B".

The truth table of $A \Rightarrow B$ is:

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

The statement $B \Rightarrow A$ is called the **converse** of the statement $A \Rightarrow B$.

Definition 2. We say that A is **equivalent** to B, if A implies B and B implies A. ■

The statement "A is equivalent to B" is written $A \Leftrightarrow B$. It is read "A equivalent B" and called an **equivalence**. It is also called a **bi-conditional** statement.

In the statement "A is equivalent to B", the statement "A implies B" is called the **necessary condition,** abbreviated **N.C,** and the statement "B implies A" is called the **sufficient condition** and abbreviated **S.C**.

The statement "A is equivalent to B" is also written in one of the following ways:
"A if and only if B";
"A is a necessary and sufficient condition of B".

The truth table of $(A \Leftrightarrow B)$ is:

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

Theorems 1.1.1 through 1.1.4 contain most of the rules of logic and are stated without proof.

1.1.1. Let A, B and C be statements, then the following statements are a tautologies:
(i) $A \Leftrightarrow \neg(\neg A)$;
(ii) $(A\vee A)\Leftrightarrow A$; $(A\wedge A)\Leftrightarrow A$.
(iii) $(A\Rightarrow B) \Leftrightarrow B\vee(\neg A)$.
(iv) $[A\Rightarrow B] \Leftrightarrow [\neg B\Rightarrow\neg A]$.
(v) $(A\wedge B)\Leftrightarrow(B\wedge A)$; $(A\vee B)\Leftrightarrow(B\vee A)$.
(vi) $A\wedge(B\wedge C)\Leftrightarrow(A\wedge B)\wedge C$; $A\vee(B\vee C)\Leftrightarrow(A\vee B)\vee C$..
(vii) $A\wedge(B\vee C)\Leftrightarrow(A\wedge B)\vee(A\wedge C)$; $A\vee(B\wedge C)\Leftrightarrow(A\vee B)\wedge(A\vee C)$. ■

1.1.2. Let A, B, C and D be statements, then the following statements are a tautologies:
(i) $(A\Leftrightarrow B) \Leftrightarrow (B\Leftrightarrow A) \Leftrightarrow (\neg A\Leftrightarrow\neg B) \Leftrightarrow (\neg B\Leftrightarrow\neg A)$.
(ii) If $A\Rightarrow B$ and $B\Rightarrow C$, then $A\Rightarrow C$.
(iii) If $A\Leftrightarrow B$ and $B\Leftrightarrow C$, then $A\Leftrightarrow C$.
(iv) If $A\Rightarrow B$ and $C\Rightarrow D$, then

$$[(A\wedge C)\Rightarrow(B\wedge D)] \text{ and } [(A\vee C)\Rightarrow(B\vee D)].$$

(v) If $A\Leftrightarrow B$ and $C\Leftrightarrow D$, then

$$[(A\wedge C)\Leftrightarrow(B\wedge D)] \text{ and } [(A\vee C)\Leftrightarrow(B\vee D)]. \blacksquare$$

1.1.3. If A and B are statements, then the following are true
(i) $(A\wedge B)\Rightarrow B$.
(ii) If A is true, then $(A\wedge B)\Leftrightarrow B$.
(iii) $B\Rightarrow(A\vee B)$.
(iv) If A is false, then $(A\vee B)\Leftrightarrow B$. ■

1.1.4. The following hold
(i) $\neg(A\wedge B) \Leftrightarrow (\neg A)\vee(\neg B)$.
(ii) $\neg(A\vee B) \Leftrightarrow (\neg A)\wedge(\neg B)$.
(iii) $\neg(A\Rightarrow B) \Leftrightarrow [A\wedge\neg B]$. ■

Definition 3. We define the **contrapose** of the statement $(A\Rightarrow B)$ to be the statement

$$\neg B\Rightarrow\neg A. \blacksquare$$

SOME TYPES OF PROOFS.

Proof by contradiction: If after assuming that a statement A is false, we find a statement B, such that B is true and false at the same time, we say that we have a contradiction and we deduce that A is true. This way of the proof of truthiness of A is called **proof by contradiction**.

Direct proof: This a way of proving the truthiness of $(A\Rightarrow B)$. It consists of supposing A is true and then deduce that B is true.

Proof by contraposition: To prove that $(A\Rightarrow B)$, we show that its contrapose is true.

Proof by induction: This kind of proof can be used when we want to show that a property P(n) depending upon a natural number n, is true for all $n\geq k$, with k is a given natural number. We have two forms of induction whose proofs should be done in the course of M1102:

First form of induction: Let P(n) be a property that depends upon a natural number n. If k is a natural number, such that

(i) P(k) is true and

(ii) $(\forall t\geq k)[P(t)$ is true $\Rightarrow P(t+1)$ is true],

then P(n) is true, $\forall n\geq k$. ■

Second form of induction: Let P(n) be a property that depends upon a natural number n. If k is a natural number, such that

(i) P(k) is true and

(ii) $(\forall t\geq k)[P(s)$ is true, for all $k\leq s\leq t \Rightarrow P(t+1)$ is true],

then P(n) is true, $\forall n\geq k$. ■

To show that a property is true, for all $n\geq k$, by using the first form of induction we show that

(i) the property is true for n = k and

(ii) we suppose that it holds for n and we show it for n+1,

and by using the second form we show that

(i) the property is true for n=k and

(ii) we suppose that it holds up to n (i.e it holds, for all s, such that $k\leq s\leq n$) and we show it for n+1.

If we want to show a property that depends upon a natural number n by using one of the two forms of induction, then we say that we argue (or proceed) by induction on n.

§ 1.2. SETS.

Intuitively, we consider a set to be a collection of objects E satisfying the two axioms:

Axiom I. For any object x it is possible to determine whether or not x is an object (or element) of E. ■

Axiom II. E is not an element of itself. ■

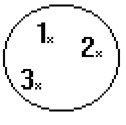
We write $x\in E$ (read: "x belongs to E") if x is an element of E and we write $x\notin E$ (read: "x doesn't belong to E") if x is not an element of E.

If we list the elements of E between two braces, such that every two consecutive elements in the list are separated by a comma, then we say that E is written in **extension**. If the elements of E are defined through a property P, then we write

$$E=\{x \,;\, x \text{ satisfies } P\} \text{ or } E=\{x \,/\, x \text{ satisfies } P\}.$$

In this case we say that the set E is given in **comprehension**.

If we list the elements of E inside a closed line of the plane, as for the set {1,2,3} below, then this representation is called the **Venn diagram** of E.



If P is a property, then the statement

"there exists at least one element of E, satisfying P"

is written

$$(\exists x\in E)(P) \text{ or } \exists x\in E\ ;\ P$$

read:

"there exists x in E, such that P" or "there exists x in E, we have P".

.

The statement

"every element of E satisfies P"

will be written

$$(\forall x\in E)(P) \text{ or } \forall x\in E\ ;\ P$$

read:

"for all x in E, such that P" or " for all x in E, we have P".

We have that

(i) the negation of the statement

"there exists at least one element of E, satisfying P"

is

"every element of E satisfies $\urcorner P$"

(ii) the negation of the statement

"every element of E satisfies P"

is

"There exists at least one element of E satisfying $\urcorner P$".

Thus

(i) $\urcorner[(\exists x\in E)(P)] \Leftrightarrow [(\forall x\in E)(\urcorner P)]$.

(ii) $\urcorner[(\forall x\in E)(P)] \Leftrightarrow [(\exists x\in E)(\urcorner P)]$.

The symbols $\exists$ and $\forall$ that stand for "there exists" and "for all" respectively are called the **quantifiers**.

The set containing no elements at all is called the **empty set** or **null set**. It is denoted by the symbol $\varnothing$ or by a pair of empty braces {}. Thus

"$x\notin\varnothing$" is always true

and

"$x\in\varnothing$" is always false.

Notice that $\{\varnothing\}$ is not empty, for it has an element in it, namely $\varnothing$.

Definition 4. A set consisting of just one element a is written {a} and called a **singleton** and a set consisting of two elements a and b is written {a,b} and called a **pair**. ■

Definition 5. Let E and F be sets. We say that F is a **subset** of E and we write $F\subseteq E$ (read: "F is contained in E"), if every element of F is an element of E. ■

Thus $F\subseteq E$ if and only if the implication

$$x\in F\Rightarrow x\in E$$

is true for every object x, i.e

$$F\subseteq E \Leftrightarrow (\forall x)(x\in F\Rightarrow x\in E).$$

If F is a subset of E, we also say that E contains F and we write $E\supseteq F$ (read: "E contains F").

We shall write $F \not\subset E$ (read: "F is not contained in E"), if F is not a subset of E. Thus

$$F \not\subset E \Leftrightarrow (\exists x)(x \in F \text{ and } x \notin E).$$

1.2.1. If A,B and C are sets, then
(i) $\emptyset \subseteq E$, for every set E.
(ii) $A \subseteq A$.
(iii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: (i) Since $x \in \emptyset$ is false, the implication "$x \in \emptyset \Rightarrow x \in E$" is always true, and so $\emptyset \subseteq E$.
(ii) As the implication "$x \in A \Rightarrow x \in A$" is true, then $A \subseteq A$.
(iii) We have $x \in A \Rightarrow x \in B \Rightarrow x \in C$, hence $A \subseteq C$. ∎

Definition 6. Two sets E and F are said to be **equal** and we write E=F (read: "E equals F"), if they have the same elements, that is, if every element of E is an element of F and vice-versa. ∎

Thus

$$E = F \Leftrightarrow (\forall x)(x \in E \Leftrightarrow x \in F).$$

We shall write $E \neq F$ (read " E different from F") if E and F are not equal sets.

1.2.2. If E and F are two sets, then
(i) $E \neq \emptyset \Leftrightarrow \exists x$, such that $x \in E$.
(ii) $[E = F] \Leftrightarrow [E \subseteq F$ and $F \subseteq E]$.
(iii) $[E \neq F] \Leftrightarrow [E \not\subset F$ or $F \not\subset E]$.
(iv) $[E \neq F] \Leftrightarrow [(\exists x)(x \in E \text{ and } x \notin F)]$ or $[(\exists x)(x \in F \text{ and } x \notin E)]$.

Proof: (i) Follows from the definition of $\emptyset$.
(ii) Follows from definitions 5 and 6.
(iii) By 1.1.4(i).
(iv) We have

$$[E \neq F] \Leftrightarrow [E \not\subset F \text{ or } F \not\subset E] \Leftrightarrow [(\exists x)(x \in E \text{ and } x \notin F)] \text{ or } [(\exists x)(x \in F \text{ and } x \notin E)].$$ ∎

Definition 7. We say F is **included strictly** in E and we write $F \subsetneqq E$, if $F \subseteq E$ and $F \neq E$. ∎

A subset F of E is called a **proper subset** of E if $F \neq E$ and $F \neq \emptyset$.

. Intuitively, every collection of objects of a set E is a subset of E and the collection of all subsets of E is a set, called the **power set** of E and denoted P(E). It is also called **the family of the subsets** of E. Thus

$$P(E) = \{X \,;\, X \subseteq E\}$$

and so

$$X \in P(E) \Leftrightarrow X \subseteq E.$$

1.2.3. If A and B are two sets, then

$$A \subseteq B \Leftrightarrow P(A) \subseteq P(B).$$

Proof: ⇒) We have

$$X \in P(A) \Rightarrow X \subseteq A \Rightarrow X \subseteq B \Rightarrow X \in P(B),$$

and so $P(A) \subseteq P(B)$.

⇐) Since $A\in P(A)$ and $P(A)\subseteq P(B)$, we then have that $A\in P(B)$, and so $A\subseteq B$. ■

§ 1.3. OPERATIONS ON SETS.

If E and F are two sets, then the collection of the objects of E together with those of F is a set, called the **union** of E and F and is denoted $E\cup F$ (read: "E union F"). Thus

$$E\cup F = \{x \,;\, x\in E \text{ or } x\in F\}$$

and so

$$(\forall x)(x\in E\cup F \Leftrightarrow x\in E \text{ or } x\in F).$$

1.3.1. Let A,B,C and D be sets. Then we have
(i) $A\subseteq A\cup B$ and $B\subseteq A\cup B$.
(ii) $x\notin A\cup B \Leftrightarrow x\notin A$ and $x\notin B$.
(iii) $A\cup B = B\cup A$.
(iv) $A\cup(B\cup C) = (A\cup B)\cup C$.
(v) $A\cup A = A$.
(vi) If $A\subseteq B$ and $C\subseteq D$, then $A\cup C\subseteq B\cup D$.
(vii) $A\cup\emptyset = \emptyset\cup A = A$.
(viii) $A\subseteq B \Leftrightarrow A\cup B = B$.

Proof: (i) through (vi) are easy.
(vii) We have

$$x\in A\cup\emptyset \Leftrightarrow x\in A \text{ or } x\in\emptyset \Leftrightarrow x\in A \text{ (because "}x\in\emptyset\text{" is false)}$$

hence $A\cup\emptyset=A$. As $A\cup\emptyset = \emptyset\cup A$, then $A\cup\emptyset = \emptyset\cup A = A$.
(viii) ⇒): We have $A\subseteq B$ and $B\subseteq B$, hence $A\cup B\subseteq B\cup B$, by (vi). But $B\cup B=B$, hence $A\cup B\subseteq B$ and as $B\subseteq A\cup B$, then $A\cup B=B$.
⇐): As $A\subseteq A\cup B$ and $A\cup B=B$, then $A\subseteq B$. ■

If E and F are two sets, then the common elements of E and F form a set, called the **intersection** of E and F and is denoted $E\cap F$ (read: "E intersect F"). Thus

$$E\cap F = \{x \,;\, x\in E \text{ and } x\in F\}$$

and so

$$(\forall x)(x\in E\cap F \Leftrightarrow x\in E \text{ and } x\in F).$$

Definition 8. Two sets A and B are said to be **disjoint** if $A\cap B=\emptyset$. ■

1.3.2. If A,B,C and D are sets, then
(i) $A\cap B\subseteq A$ and $A\cap B\subseteq B$.
(ii) $x\notin A\cap B \Leftrightarrow x\notin A$ or $x\notin B$.
(iii) $A\cap B = B\cap A$.
(iv) $A\cap(B\cap C) = (A\cap B)\cap C$.
(v) $A\cap A = A$.
(vi) If $A\subseteq B$ and $C\subseteq D$, then $A\cap C\subseteq B\cap D$.
(vii) $A\cap\emptyset = \emptyset\cap A = \emptyset$.
(viii) $A\subseteq B \Leftrightarrow A\cap B = A$.

Proof: (i) through (vi) are easy.
(vii) Suppose that $A\cap\emptyset\neq\emptyset$, then $\exists x$, such that $x\in A\cap\emptyset$. We have $x\in A$ and $x\in\emptyset$, hence $x\in\emptyset$, which is impossible. Thus

$$A\cap\emptyset=\emptyset.$$

As $\emptyset\cap A=A\cap\emptyset$, then $\emptyset\cap A=A\cap\emptyset=\emptyset$.

(viii) $\Rightarrow)$: We have $A\subseteq A$ and $A\subseteq B$, hence $A\cap A\subseteq A\cap B$. But $A\cap A=A$, whence $A\subseteq A\cap B$ and as $A\cap B\subseteq A$, then $A\cap B=A$.

$\Leftarrow)$: As $A\cap B\subseteq B$ and $A\cap B=A$, then $A\subseteq B$. ■

1.3.3. Let A,B and C be sets. Then we have

(i) $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$.

(ii) $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$.

Proof: (i) $x\in(A\cap B)\cup(A\cap C) \Leftrightarrow x\in(A\cap B)$ or $x\in(A\cap C)$

$\Leftrightarrow$ ($x\in A$ and $x\in B$) or ($x\in A$ and $x\in C$)

$\Leftrightarrow$ $x\in A$ and ($x\in B$ or $x\in C$) (by 1.1.1(vii))

$\Leftrightarrow$ $x\in A$ and $x\in(B\cup C)$

$\Leftrightarrow$ $x\in A\cap(B\cup C)$.

Hence $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$.

(ii) $x\in(A\cup B)\cap(A\cup C) \Leftrightarrow x\in(A\cup B)$ and $x\in(A\cup C)$

$\Leftrightarrow$ ($x\in A$ or $x\in B$) and ($x\in A$ or $x\in C$)

$\Leftrightarrow$ $x\in A$ or ($x\in B$ and $x\in C$) (by 1.1.1(vii))

$\Leftrightarrow$ $x\in A$ or $x\in(B\cap C)$

$\Leftrightarrow$ $x\in A\cup(B\cap C)$.

Hence $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$. ■

If E and F are two sets, then the elements of E that are not elements of F form a set, called the **difference** of E and F and is denoted E-F (read: "E minus F"). Thus

$$E-F = \{x\ ;\ x\in E \text{ and } x\notin F\}$$

and so

$$x\in E-F \Leftrightarrow x\in E \text{ and } x\notin F.$$

If $F\subseteq E$, then the set E-F is called the **complement** of F in E and is denoted $\complement_{E} F$ or $\overline{F}$.

1.3.4. If A is a subset of E, then

(i) $A\cap\overline{A}=\emptyset$,

(ii) $A\cup\overline{A}=E$,

(iii) $\overline{\overline{A}}=A$.

Proof: (i) Suppose that $A\cap\overline{A}\neq\emptyset$, then there exists x in $A\cap\overline{A}$. We have $x\in A$ and $x\in\overline{A}$. As $x\in\overline{A}$, then $x\notin A$, and so $x\in A$ and $x\notin A$, which is impossible. Therefore $A\cap\overline{A}=\emptyset$.

(ii) We have $A\subseteq E$ and $\overline{A}\subseteq E$, hence $A\cup\overline{A}\subseteq E$. Let $x\in E$. If $x\in A$, then $x\in A\cup\overline{A}$ and if $x\notin A$, then $x\in\overline{A}$, and so $x\in A\cup\overline{A}$. Therefore $E\subseteq A\cup\overline{A}$, and so $E=A\cup\overline{A}$.

(iii) We have

$x\in\overline{\overline{A}} \Leftrightarrow x\in E$ and $x\notin\overline{A} \Leftrightarrow x\in E$ and ($x\notin E$ or $x\in A$)

$$\Leftrightarrow \underbrace{(x\in E \text{ and } x\notin E)}_{\text{false}} \text{ or } (x\in E \text{ and } x\in A)$$

$\Leftrightarrow$ $x\in E$ and $x\in A$

$\Leftrightarrow$ $x\in E\cap A$

$\Leftrightarrow$ $x\in A$ (because $E\cap A=A$, since $A\subseteq E$)

hence $\overline{\overline{A}}=A$. ■

<u>1.3.5 (DeMorgan's Formula).</u> If A and B are two subsets of E, then

(i) $[_E(A\cup B)=([_E A)\cap([_E B)$.

(ii) $[_E(A\cap B)=([_E A)\cup([_E B)$.

<u>Proof:</u> (i) We have

$$\begin{aligned} x\in([_E A)\cap([_E B) &\Leftrightarrow x\in [_E A \text{ and } x\in [_E B \\ &\Leftrightarrow (x\in E \text{ and } x\notin A) \text{ and } (x\in E \text{ and } x\notin B) \\ &\Leftrightarrow (x\in E \text{ and } x\in E) \text{ and } (x\notin A \text{ and } x\notin B) \\ &\Leftrightarrow x\in E \text{ and } (x\notin A \text{ and } x\notin B) \Leftrightarrow x\in E \text{ and } x\notin(A\cup B) \\ &\Leftrightarrow. \ x\in [_E(A\cup B), \end{aligned}$$

hence $[_E(A\cup B)=([_E A)\cap([_E B)$.

(ii) We have

$$\begin{aligned} x\in([_E A)\cup([_E B) &\Leftrightarrow x\in [_E A \text{ or } x\in [_E B \\ &\Leftrightarrow (x\in E \text{ and } x\notin A) \text{ or } (x\in E \text{ and } x\notin B) \\ &\Leftrightarrow x\in E \text{ and } (x\notin A \text{ or } x\notin B) \\ &\Leftrightarrow x\in E \text{ and } x\notin(A\cap B) \\ &\Leftrightarrow x\in [_E(A\cap B), \end{aligned}$$

and so $[_E(A\cap B)=([_E A)\cup([_E B)$. ■

<u>§ 1.4. CARTESIAN PRODUCT OF SETS.</u>

<u>Definition 9.</u> Let $E_1...,E_n$ be non-empty sets. For each $a_1\in E_1,...,a_n\in E_n$, we define an **ordered n-tuple** of **components** $a_1,...,a_n$ to be the object $(a_1,...,a_n)$, where two ordered n-tuples $(a_1,...,a_n)$ and $(b_1,...,b_n)$ are equal if $a_1= b_1,...,a_n= b_n$. ■

The component a_i of $(a_1,...,a_n)$ is called the **ith component** of $(a_1,...,a_n)$.

If n=2, then the ordered 2-tuple (a_1,a_2) is called an **ordered pair**.

The collection of all ordered n-tuples $(a_1,...,a_n)$, where $a_1\in E_1$, ..., $a_n\in E_n$, is a set called the **cartesian product** of the sets $E_1,...,E_n$ and is denoted $E_1\times\cdots\times E_n$. If one of the sets $E_1,,...,E_n$ is empty, we define $E_1\times\cdots\times E_n$ to be the empty set. Thus

$$E_1\times\cdots\times E_n=\{(a_1,...,a_n)\ ;\ a_1\in E_1,\ ...,\ a_n\in E_n\}.$$

<u>Remark:</u> If A, B, C and D are sets, then

$$A\times B=C\times D \Leftrightarrow [\forall(x,y)][(x,y)\in A\times B \Leftrightarrow (x,y)\in C\times D].$$

If $E_1= \cdots = E_n=A$, then we write A^n for $E_1\times\cdots\times E_n$. The set of all ordered n-tuples $(a_1,...,a_n)$ of A^n, such that $a_1= \cdots = a_n$ is called the **diagonal** of A^n.

1.4.1. If A and B are sets, then

$$(x,y)\notin A\times B \Leftrightarrow x\notin A \text{ or } y\notin B.$$

Proof: We have

$(x,y)\notin A\times B \Leftrightarrow \text{non}[(x,y)\in A\times B] \Leftrightarrow \text{non}[x\in A \text{ and } y\in B] \Leftrightarrow \text{non}[x\in A] \text{ or non}[y\in B]$
$\Leftrightarrow x\notin A \text{ or } y\notin B.$ ■

§ 1.5. FAMILY OF SETS.

Let I be a non-empty set. If we associate with each element i of I a set A_i , then the set $\{A_i\ ; i\in I\}$ is called a **family of sets indexed by** I. This family is denoted $(A_i)_{i\in I}$.

Let $(A_i)_{i\in I}$ be a family of sets. The collection of all the elements of the sets A_i 's is a set, called **the union of the family** $(A_i)_{i\in I}$ (or **the union of the** A_i 's) and is denoted $\bigcup_{i\in I} A_i$. Thus

$$x\in \bigcup_{i\in I} A_i \Leftrightarrow (\exists i\in I)(x\in A_i)$$

and

$$x\notin \bigcup_{i\in I} A_i \Leftrightarrow (\forall i\in I)(x\notin A_i).$$

The collection of the common elements of the sets A_i 's, i.e the collection of the elements x, such that $x\in A_i$, for all $i\in I$, is a set, called **the intersection of the family** $(A_i)_{i\in I}$ (or **the intersection of the** A_i 's) and is denoted $\bigcap_{i\in I} A_i$. Thus

$$x\in \bigcap_{i\in I} A_i \Leftrightarrow (\forall i\in I)(x\in A_i)$$

and

$$x\notin \bigcap_{i\in I} A_i \Leftrightarrow (\exists i\in I)(x\notin A_i).$$

If I = {1,2,...,n}, then the sets $\bigcup_{i\in I} A_i$ and $\bigcap_{i\in I} A_i$ will be written $\bigcup_{i=1}^{n} A_i$ and $\bigcap_{i=1}^{n} A_i$ respectively. Thus

$$x\in \bigcup_{i=1}^{n} A_i \Leftrightarrow (\exists 1\le i\le n)(x\in A_i),$$

$$x\notin \bigcup_{i=1}^{n} A_i \Leftrightarrow (\forall 1\le i\le n)(x\notin A_i),$$

$$x\in \bigcap_{i=1}^{n} A_i \Leftrightarrow (\forall 1\le i\le n)(x\in A_i)$$

and

$$x\notin \bigcap_{i=1}^{n} A_i \Leftrightarrow (\exists 1\le i\le n)(x\notin A_i).$$

Let S be a set whose elements are sets, for example P(E). For each $X\in S$, let $A_X = X$. Then the union (resp. intersection) of the family $(A_X)_{X\in S}$ is called the union (resp.

intersection) of the elements of S and is denoted $\bigcup_{X\in S} X$ (resp. $\bigcap_{X\in S} X$). Thus

$$a\in \bigcup_{X\in S} X \Leftrightarrow (\exists X\in S)(a\in X),$$

$$a\notin \bigcup_{X\in S} X \Leftrightarrow (\forall X\in S)(a\notin X),$$

$$a\in \bigcap_{X\in S} X \Leftrightarrow (\forall X\in S)(a\in X)$$

and

$$a\notin \bigcap_{X\in S} X \Leftrightarrow (\exists X\in S)(a\notin X).$$

Definition 10. We say that the sets A_i's of a family $(A_i)_{i\in I}$ are **pairwise** (or **mutually**) **disjoint** if $A_s \cap A_t = \varnothing$, for all s,t∈I, with s≠t. ■

Intuitively, if $(A_i)_{i\in I}$ is a non-empty family of non-empty sets and if the A_i's are pairwise disjoint, then there exists a set E, such that $E\cap A_i$ is a singleton, for all i∈I, for it is enough to choose one element a_i from each set A_i and take $E=\{a_i\ ; i\in I\}$. Hence the necessity to assume the following axiom, known as the **axiom of choice**.

Axiom of choice: If $(A_i)_{i\in I}$ is a non-empty family of non-empty sets and if the A_i's are pairwise disjoint, then there exists a set E, such that $E\cap A_i$ is a singleton, for all i∈I. ■

M1100

CHAPTER I

EXERCISES.

Unless otherwise mentioned, the letter E denotes a set, and for each subset X of E, let $\overline{X} = \complement_E X$.

1- Which of the following are statements? What are the truth values of those that are statements?

(a) $2+3=8$.

(b) Close the door.

(c) $2+8>3$.

(d) $x+3<7$, for every real x.

(e) x is a real and $x+3=2$.

2- Let A and B be statements. Which of the following statements are tautologies?

(i) $A\Rightarrow(A\vee B)$, (ii) $A\Rightarrow(A\wedge B)$, (iii) $(A\vee B)\Rightarrow(A\wedge B)$,

(iv) $(A\wedge B)\Rightarrow(A\vee B)$, (v) $(A\vee B)\Rightarrow A$, (vi) $(A\wedge B)\Rightarrow A$.

3- Without using the truth tables, show that if A,B and C are statements, then

(a) $\neg[(A\Leftrightarrow B)] \Leftrightarrow [(A\vee B)\wedge(\neg A\vee\neg B)]$,

(b) $\neg[(A\Leftrightarrow B)] \Leftrightarrow [A\Leftrightarrow\neg B]$.

(c) $[(A\vee B)\Rightarrow C] \Leftrightarrow [(A\Rightarrow C)\wedge(B\Rightarrow C)]$.

(d) $[(A\wedge B)\Rightarrow C] \Leftrightarrow [A\Rightarrow(B\Rightarrow C)]$.

(e) $[(A\vee C)\Rightarrow(B\vee C)] \Leftrightarrow [A\Rightarrow(B\vee C)]$.

4- Let A and B be statements. Without using the truth tables, show that

(i) $[A\Rightarrow B] \Leftrightarrow [\neg B\Rightarrow\neg A]$.

(ii $[A\Leftrightarrow B] \Leftrightarrow [\neg A\Leftrightarrow\neg B]$.

(iii) $\neg(A\Rightarrow B) \Leftrightarrow [A\wedge\neg B]$.

5- Redo nº 2, 3 and 4, by using the truth tables.

6- Using the truth tables, verify the distributive laws:

(i) $[A\wedge(B\vee C)]\Leftrightarrow[(A\wedge B)\vee(A\wedge C)]$.

(iv) $[A\vee(B\wedge C)]\Leftrightarrow[(A\vee B)\wedge(A\vee C)]$.

7- Let P and R be properties. Give the negation of each of the following statements

(i) $(\forall x\in E)(\exists y\in E)(P)$, (ii) $(\exists x\in E)(\forall y\in E)(P)$,

(iii) $(\forall x\in E)([(\exists y\in E)(P)]\Rightarrow R)$, (iv) $[(\forall x\in E)(\exists y\in E)][P\Rightarrow R]$.

8- Say if each of the following statements is true or false and justify your answer, then give the negation of those that are true:

(i) $(\forall x\in \mathbb{R})[(x+1)^2>0]$, (ii) $[(\exists x\in \mathbb{R})(x+1=0)]$ and $[(\exists x\in \mathbb{R})(x+2=0)]$,

(iii) $(\forall x\in \mathbb{R})(x^2>0 \text{ or } x\leq 0)$, (iv) $[(\forall x\in \mathbb{R})(x^2>0)]$ or $[(\forall x\in \mathbb{R})(x\leq 0)]$,

(v) $(\forall x\in \mathbb{R})(\exists y\in \mathbb{R})(x\geq y)$, (vi) $(\exists x\in \mathbb{R})(\forall y\in \mathbb{R})(x\geq y)$.

9- Let f be a real function defined on $\mathbb{R}$. Using the quantifiers, write down the following statements and then give their negations:

(i) f never vanishes on $\mathbb{R}$,
(ii) f is the zero function,
(iii) f is constant on $\mathbb{R}$,
(iv) f is increasing on $\mathbb{R}$.

10- Using the quantifiers, write down the following statements and say if each of them is true or false with justification, then give their negations:

(i) every real number lies between two consecutive integers,
(ii) some real number is > its square,
(iii) no natural number is ≥ all the others,
(iv) there exists an integer which is a multiple of all the others.

11- Show each of the following statements using the indicated method

(i) Let n be natural number. If n is non-zero, then n^2+1 cannot be the square of a non-zero natural number (by contraposition).

(ii) Let a, b≥0. If $\frac{a}{1+b}=\frac{b}{1+a}$, then a=b (by contradiction).

12- Let E={1, {∅}, {1, 2}, $\mathbb{N}$}. Complete using the symbols ∈, ∉, ⊆ and ⊄:

∅…E; {∅}…E; ∅…P(E); $\mathbb{N}$…E ; {0, 1}…E; {1, 2}…E;
1…E; {∅, $\mathbb{N}$}…E; {{∅}, $\mathbb{N}$}…E; {1, $\mathbb{N}$}…P(E); {{1}, $\mathbb{N}$}…P(E).

13- Find P(E) in the following cases:

(i) E = ∅, (ii) E = {a}, (iii) E = {a,b}, (iv) E = {∅,{∅}}.

14- Let A and B be sets.

1- Show that if C is a set, then

$$A\subseteq B\cap C \Leftrightarrow A\subseteq B \text{ and } A\subseteq C.$$

2- Show that

(i) P(A∩B)=P(A)∩P(B).
(ii) P(A)∪P(B)⊆P(A∪B). Give an example where the inclusion is strict.

15- We define the **symmetric difference** of two sets E and F, denoted EΔF, to be

$$E\Delta F = (E-F)\cup(F-E).$$

1- Show that EΔF = (E∪F)-(E∩F).

2- Deduce that

$$x\notin E\Delta F \Leftrightarrow (x\notin E \text{ and } x\notin F) \text{ or } (x\in E \text{ and } x\in F).$$

3- Show that

$$x\in E\Delta F \Leftrightarrow (x\in E \text{ and } x\notin F) \text{ or } (x\notin E \text{ and } x\in F).$$

4- Prove that if A,B and C are sets, then

$$(A\Delta B)\Delta C = A\Delta(B\Delta C).$$

(<u>**Hint:**</u> Use 2) and 3)).

5- Show that if A and B are two sets, then

(i) AΔB = BΔA.
(ii) AΔ∅ = ∅ΔA = A.
(iii) AΔA = ∅.
(iv) AΔ(AΔB) = B.
(v) (AΔB)ΔB = A.

16- Let A be a subset of E.

1- Show that if $X\in P(E)$, then

(i) $[X\subseteq A$ and $X\subseteq \overline{A}\,] \Leftrightarrow X=\varnothing$.

(ii) $X=(X\cap A)\cup(X\cap \overline{A}\,)$.

2- Deduce that if $X\in P(E)$, then $X\cap A=X\cap \overline{A} \Leftrightarrow X=\varnothing$.

17- Show that if A and B are two subsets of E, then $A\subseteq B \Leftrightarrow \overline{B}\subseteq \overline{A}$.

18- Show that if A and B are two subsets of E, then

(i) $A\subseteq \overline{B} \Leftrightarrow A\cap B=\varnothing$.

(ii) $\overline{B}-\overline{A}=A-B$.

19- Let A and B be sets. Show that

(i) $A-(A\cap B)=A-B$.

(ii) $(A\cup B)-A=B-A$.

(iii) $(A\cup B)-(A-B)=B$

(iv) $A-(A-B)=A\cap B$.

20- Let A, B and C be sets. Which of the following statements is a tautology ?

(i) $A\cap B=A\cap C \Rightarrow B=C$.

(ii) $A\cup B=A\cup C \Rightarrow B=C$.

Show that $[A\cup B=A\cup C$ and $A\cap B=A\cap C] \Rightarrow B=C$.

21- Calculate $A\times B\times C$, where $A=\{1,2\}$, $B=\{3,4\}$ and $C=\{5,6,7\}$.

22- Prove that if A, B, C, E and F are sets, then the following hold

(i) If $A\neq\varnothing$ and $B\neq\varnothing$, then $A\times B\subseteq E\times F \Rightarrow A\subseteq E$ and $B\subseteq F$.

(ii) $[A\subseteq E$ and $B\subseteq F] \Rightarrow A\times B\subseteq E\times F$.

(iii) $[C\neq\varnothing$ and $A\times C=B\times C] \Rightarrow A=B$.

23- Show that if A, B, C and D are sets, then

(i) $A\times(B-C)=(A\times B)-(A\times C)$.

(ii) $(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$.

(iii) $E\times(F\cup G)=(E\times F)\cup(E\times G)$.

(iv) $(E\cup F)\times G=(E\times G)\cup(F\times G)$.

(v) $(A-B)\times(C-D)\subseteq(A\times C)-(B\times D)$. Give an example where $\subseteq$ is strict.

24- Let $(A_i)_{i\in I}$ be a non-empty family of sets. Show that

(i) $E-(\bigcup_{i\in I} A_i) = \bigcap_{i\in I}(E-A_i)$; (ii) $E-(\bigcap_{i\in I} A_i) = \bigcup_{i\in I}(E-A_i)$.

25- Show that if F and F' are two families of subsets of a set E, then

(i) $(\bigcup_{X\in F} X)\cap(\bigcup_{Y\in F'} Y) = \bigcup_{(X,Y)\in F\times F'}(X\cap Y)$

(ii) $F\subseteq F' \Rightarrow \bigcup_{X\in F} X\subseteq \bigcup_{Y\in F'} Y$ and $\bigcap_{Y\in F'} Y\subseteq \bigcap_{X\in F} X$.

M1100

CHAPTER II

MAPPINGS

Let A and B be two non-empty sets.

§ 2.1. DEFINITIONS AND EXAMPLES.

Definition 1. We call **correspondence** (or **assignment** or **relation**) from A to B every triple (A, B, G), where $G \subseteq A \times B$.■

Recall that two triples (A, B, G) and (A', B', G') are equal if A=A', B=B' and G=G'.

If (A, B, G) is a correspondence from A to B, then the set A is called the **domain** (or **initial set**), B the **codomain** (or **final set**) and G is called the **graph** of f.

A correspondence f = (A, B, G) from A to B is usually written $f : A \longrightarrow B$ or $A \xrightarrow{f} B$.

Definition 2. Let $f : A \longrightarrow B$ be a correspondence from A to B and let $x \in A$. For any $(x,y) \in G$, y is called **an image** of x by f and x is called a pre-image (or an inverse image) of y. ■

If G is the graph of f, we say that f **associates with** (or **assigns to**) the element x of A the elements y of B satisfying $(x,y) \in G$.

Definition 3. We define a **mapping** of A to B (or from A to B) to be every correspondence f from A to B that associates every element x of A with a unique image in B. ■

If $f : A \longrightarrow B$ is a mapping, the image of every element x of A by f is written f(x). Thus if $f : A \longrightarrow B$ is a mapping, then the implication

$$x = x' \Rightarrow f(x) = f(x')$$

is true for all $x, x' \in A$.

A mapping $f : A \longrightarrow B$ is also denoted $\begin{matrix} A \to & B \\ x \to & f(x). \end{matrix}$

Examples: 1) The correspondence from A to itself that associates every element x of A with x itself is a mapping, called the **identity mapping** of A and written id_A .

2) The correspondence f from $\mathbb{N}$ to $\mathbb{R}^+$ (the set of non-negative real numbers, i.e the set of all real numbers x, satisfying $x \geq 0$) that associates every element x of $\mathbb{N}$ with the elements y of $\mathbb{R}^+$, satisfying $y^2 = x$, is a mapping: Let $x \in \mathbb{N}$. Then $\sqrt{x} \in \mathbb{R}^+$, and so $\sqrt{x}$ is an image of x by f. Let y and y' be two images of x by f. Then $y^2 = x$ and $y'^2 = x$, and so $y^2 = y'^2$. But y and y' are both non-negative, hence y=y', and so every element x of $\mathbb{N}$ has a unique image by f, whence f is a mapping.

3) The correspondence f from $\mathbb{Z}$ to $\mathbb{R}$ that associates every element x of $\mathbb{Z}$ with the

elements y of $\mathbb{R}$ satisfying $y^2 = x$ is not a mapping because the element 4 of $\mathbb{Z}$ has two images -2 and +2 under f (or simply because the element -1 of $\mathbb{Z}$ has no image by f).

2.1.1. Two mappings $f : A \longrightarrow B$ and $g : A' \longrightarrow B'$ are equal if and only if A=A', B=B' and f(x)=g(x), for all $x \in A$.

Proof: Let G be the graph of f and G' be that of g. Then

$$f = (A,B,G) \text{ and } g = (A',B',G').$$

N.C: Since f = g, we then get A=A', B=B' and G=G'. Let $x \in A$. We have $(x,f(x)) \in G$, hence $(x,f(x)) \in G'$, and so f(x) is an image of x by g. But g(x) is the only image of x by g, whence f(x)=g(x).

S.C: Since A=A' and B=B', it is left to prove that G=G'. We have

$$(x,y) \in G \Leftrightarrow x \in A \text{ and } y = f(x) \Leftrightarrow x \in A' \text{ and } y = g(x) \Leftrightarrow (x,y) \in G'$$

hence G=G', as required. ■

Thus two mappings are equal if and only if they have the same initial set, same final set and give the same image to every element of the initial set.

NOTATION; The set of all mappings from A to B is denoted B^A.

Definition 4. We call a **function** of A to B (or from A to B) every correspondence from A to B that associates every element x of A with **at most one image** in B. ■

If $f : A \longrightarrow B$ is a function of A to B, then the subset X of A defined by

$$X=\{x \in A, \text{ x has an image by f}\}$$

is called **the domain of definition** of f and usually denoted D_f.

Remark: Some authors define a function from A to B to be a mapping from a subset of A to B.

Definition 5. Let $f : A \longrightarrow B$ and $g : A' \longrightarrow B'$ be two mappings. We say that g **extends** f (or that g is **an extension** of f) if $A \subseteq A'$, $B \subseteq B'$ and g(x)=f(x), for all $x \in A$. ■

Definition 6. Let $f : A \longrightarrow B$ be a mapping and let X be a non-empty subset of A. We define the **restriction** of f to X, denoted $f_{/X}$, to be the mapping

$$f_{/X} : X \longrightarrow B$$

defined by $(f_{/X})(x) = f(x)$, for all $x \in X$. ■

§ 2.2. COMPOSITION OF MAPPINGS.

2.2.1. If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are two mappings, then the correspondence h from A to C that associates every element x of A with the elements y of C satisfying y = g(f(x)) is a mapping.

Proof: Let $x \in A$. Then $f(x) \in B$, and so $g(f(x)) \in C$. Hence g(f(x)) is an image of x under h. Let y and y' be two images of x by h, then y=g(f(x)) and y'=g(f(x)), and so y=y'. Therefore h is a mapping. ■

Definition 7. The mapping h, defined in 2.2.1, is called the **composite** of f and g and is denoted $g \circ f$ (read: g round f). ■

Thus if $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are two mappings, then the mapping $g \circ f : A \longrightarrow C$ is defined by $(g \circ f)(x) = g(f(x))$, for all $x \in A$.

We shall write $g \circ f(x)$ for $(g \circ f)(x)$.

Remark: In general $f \circ g \neq g \circ f$, for take $A=\{1,2\}$ and let $f,g \in A^A$, such that

$$f(1)=f(2)=1 \text{ and } g(1)=g(2)=2$$

then $f \circ g(1)=1$ and $g \circ f(1)=2$, and so $f \circ g(1) \neq g \circ f(1)$, whence $f \circ g \neq g \circ f$.

2.2.2. The composition of mappings is associative, i.e, if

$$f : A \longrightarrow B,\ g : B \longrightarrow C \text{ and } h : C \longrightarrow D$$

are mappings, then $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof: We have that $h \circ g$ is a mapping of B to D, so that $(h \circ g) \circ f$ is a mapping of A to D. Similarly, $h \circ (g \circ f)$ is a mapping of A to D, and so $(h \circ g) \circ f$ and $h \circ (g \circ f)$ have the same initial set A and same final set D. Let $x \in A$. Then

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x))) \text{ and } [h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x)))$$

and so $[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x)$, for all $x \in A$, whence $(h \circ g) \circ f = h \circ (g \circ f)$. ■

2.2.3. Let $f : A \longrightarrow B$ be a mapping. Then $f \circ id_A = f$ and $id_B \circ f = f$.

Proof: We have $f \circ id_A$ and f are mappings of A to B. As $(f \circ id_A)(a)=f(id_A(a))=f(a)$, for all $a \in A$, then $f \circ id_A = f$. Similarly, we have $id_B \circ f$ and f are mappings of A to B and for every $a \in A$, $(id_B \circ f)(a)=id_B(f(a))=f(a)$, hence $id_B \circ f = f$. ■

2.2.4. Let $f : A \longrightarrow B$ be a mapping. If g and h are two mappings from B to A, such that $g \circ f = id_A$ and $f \circ h = id_B$, then $g = h$.

Proof: By 2.2.2 and 2.2.3, we have

$$g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h. ■$$

The diagram of mappings

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd}$$

is said to be **commutative** if $g \circ f = h$. Similarly, the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "u"'] & B \arrow[d, "g"] \\ C \arrow[r, "v"'] & D \end{tikzcd}$$

is said to be commutative if $g \circ f = v \circ u$.

§ 2.3. DIRECT IMAGE AND RECIPROCAL IMAGE.

Definition 8. Let $f : A \longrightarrow B$ be a mapping and let $X \subseteq A$. We define **the direct image** (or simply **the image**) of X by f, written f(X), to be the set

$$f(X) = \{f(x) \,;\, x \in X\}. \blacksquare$$

Thus $y \in f(X) \Leftrightarrow \exists x \in X$, such that $y = f(x)$.

Definition 9. Let $f : A \longrightarrow B$ be a mapping. We define **the image** of f, denoted Im(f), to be the set Im(f)=f(A). ■

Thus $\text{Im}(f) = \{f(x) \,;\, x \in A\}$.

2.3.1. If $f : A \longrightarrow B$ is a mapping, then we have

(i) If $X \subseteq A$, then

$$f(X)=\varnothing \Leftrightarrow X=\varnothing$$

where $\varnothing$ is the empty subset of A.

(ii) $f(\{a\}) =\{f(a)\}$, for all $a \in A$.

(iii) If $X,Y \in P(A)$, then

$$X \subseteq Y \Rightarrow f(X) \subseteq f(Y).$$

(iv) $f(X \cup Y)=f(X) \cup f(Y)$, for all $X,Y \in P(A)$.

(v) $f(X \cap Y) \subseteq f(X) \cap f(Y)$, for all $X,Y \in P(A)$.

Proof: (i) $\Rightarrow$): Assume $X \neq \varnothing$, then $\exists x \in X$. As $f(x) \in f(X)$ and $f(X)=\varnothing$, then we have a contradiction, and so $X=\varnothing$.

$\Leftarrow$): Assume that $f(X) \neq \varnothing$. Then $\exists x \in f(X)$, and so $\exists a \in X$, such that $x=f(a)$, which is impossible, since $X=\varnothing$. Therefore $f(X)=\varnothing$.

(ii) Let $a \in A$. As $a \in \{a\}$, then $f(a) \in f(\{a\})$, and so

$$\{f(a)\} \subseteq f(\{a\}).$$

Let $y \in f(\{a\})$, then $\exists x \in \{a\}$, such that $y=f(x)$. As $x \in \{a\}$, then $x=a$, and so $y=f(a)$, whence $y \in \{f(a)\}$. It follows that $f(\{a\}) \subseteq \{f(a)\}$, and so $f(\{a\})=\{f(a)\}$.

(iii) Let $X,Y \in P(A)$, and suppose that $X \subseteq Y$. We have

$$x \in f(X) \Rightarrow \exists a \in X, \text{ such that } x=f(a) \Rightarrow \exists a \in Y, \text{ such that } x=f(a) \Rightarrow x \in f(Y)$$

hence $f(X) \subseteq f(Y)$.

(iv) As $X \subseteq X \cup Y$ and $Y \subseteq X \cup Y$, then $f(X) \subseteq f(X \cup Y)$ and $f(Y) \subseteq f(X \cup Y)$, by (i), and so

$$f(X) \cup f(Y) \subseteq f(X \cup Y).$$

Let $x \in f(X \cup Y)$, then $\exists a \in X \cup Y$, such that $x=f(a)$. As $a \in X \cup Y$, then

$$a \in X \text{ or } a \in Y.$$

If $a \in X$, then $x \in f(X)$ and if $a \in Y$, then $x \in f(Y)$, and so $x \in f(X) \cup f(Y)$. Therefore $f(X \cup Y) \subseteq f(X) \cup f(Y)$, and so $f(X \cup Y)=f(X) \cup f(Y)$.

(v) As $X \cap Y \subseteq X$ and $X \cap Y \subseteq Y$, then $f(X \cap Y) \subseteq f(X)$ and $f(X \cap Y) \subseteq f(Y)$, by (i), and so $f(X \cap Y) \subseteq f(X) \cap f(Y)$. ■

Remarks: 1) If $E=\{1,2,3,4\}$, $A=\{1,2\}$ and $f : P(E) \longrightarrow P(E)$ is defined by $f(X)=A \cup X$, then to find $f(\varnothing)$ we should always distinguish between the case where $\varnothing$ is considered as the empty subset of P(E) and the case where $\varnothing$ is considered as an element of P(E), for in the first case $f(\varnothing)=\varnothing$, by 2.3.1(i) and in the second case $f(\varnothing)=A \cup \varnothing=A$.

2) If $f : A \longrightarrow B$ is a mapping and $X \subseteq A$, we may have $f(a) \in f(X)$ with $a \notin X$, for example if we take $f : \{1,2\} \longrightarrow \{4,5\}$, such that $f(1)= f(2)=4$, then $f(2) \in f(\{1\})$ and $2 \notin \{1\}$.

Definition 10. Let $f : A \longrightarrow B$ be a mapping and let $Y \subseteq B$. We call **reciprocal image** (or **inverse image**) of Y by f, the set $f^{-1}(Y) = \{x \in A \,;\, f(x) \in Y\}$. ■

Thus $x \in f^{-1}(Y) \Leftrightarrow f(x) \in Y$.

2.3.2. If $f : A \longrightarrow B$ is a mapping, then we have

(i) $f^{-1}(\varnothing) = \varnothing$, where $\varnothing$ is the empty subset of B.

(ii) $f^{-1}(B) = A$.

(iii) If $X, Y \in P(B)$, then

$$X \subseteq Y \Rightarrow f^{-1}(X) \subseteq f^{-1}(Y).$$

(iv) $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$, for all $X, Y \in P(B)$.

(v) $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$, for all $X, Y \in P(B)$.

Proof: (i) Assume that $f^{-1}(\varnothing) \neq \varnothing$. Then $\exists x \in f^{-1}(\varnothing)$. This implies that $f(x) \in \varnothing$, which is impossible. Therefore $f^{-1}(\varnothing) = \varnothing$.

(ii) Let $x \in A$. As $f(x) \in B$, then $x \in f^{-1}(B)$, and so $A \subseteq f^{-1}(B)$. But $f^{-1}(B) \subseteq A$, by definition of $f^{-1}(B)$, hence $f^{-1}(B) = A$.

(iii) Let $X, Y \in P(B)$, and suppose that $X \subseteq Y$. We have

$$x \in f^{-1}(X) \Rightarrow f(x) \in X \Rightarrow f(x) \in Y \Rightarrow x \in f^{-1}(Y)$$

hence $f^{-1}(X) \subseteq f^{-1}(Y)$.

(iv) We have

$$x \in f^{-1}(X \cup Y) \Leftrightarrow f(x) \in X \cup Y \Leftrightarrow f(x) \in X \text{ or } f(x) \in Y \Leftrightarrow x \in f^{-1}(X) \text{ or } x \in f^{-1}(Y)$$
$$\Leftrightarrow x \in f^{-1}(X) \cup f^{-1}(Y)$$

hence $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

(v) We have

$$x \in f^{-1}(X \cap Y) \Leftrightarrow f(x) \in X \cap Y \Leftrightarrow f(x) \in X \text{ and } f(x) \in Y \Leftrightarrow x \in f^{-1}(X) \text{ and } x \in f^{-1}(Y)$$
$$\Leftrightarrow x \in f^{-1}(X) \cap f^{-1}(Y)$$

hence $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$. ■

Remark: We may have $f^{-1}(X) = \varnothing$ even though $X \neq \varnothing$, for take $A = \{1,2\}$ and let $f : A \longrightarrow A$ be defined by $f(1) = f(2) = 1$, then $f^{-1}(\{2\}) = \varnothing$.

2.3.3. If $f : A \longrightarrow B$ is a mapping, then

(i) $X \subseteq f^{-1}(f(X))$, $\forall X \in P(A)$.

(ii) $f(f^{-1}(Y)) \subseteq Y$, $\forall Y \in P(B)$.

Proof: (i) Let $X \in P(A)$. $\forall x \in X$, we have that $f(x) \in f(X)$, hence $x \in f^{-1}(f(X))$, and so $X \subseteq f^{-1}(f(X))$.

(ii) Let $Y \in P(B)$ and let $x \in f(f^{-1}(Y))$. Then $\exists a \in f^{-1}(Y)$, such that $x = f(a)$. Since $a \in f^{-1}(Y)$, we then get $f(a) \in Y$, and so $x \in Y$. Hence $f(f^{-1}(Y)) \subseteq Y$. ■

§ 2.4. INJECTIVE, SURJECTIVE AND BIJECTIVE MAPPING.

Definition 11. Let $f : A \longrightarrow B$ be a mapping. We say that

(i) f is **injective** (or **one-to-one** or **an injection**) if every two distinct elements of A have two distinct images in B, that is if the implication

$$x \neq x' \Rightarrow f(x) \neq f(x')$$

is true for all $x,x' \in A$;

(ii) f is **surjective** (or **onto** or **a surjection**) if whenever $y \in B$, there exists $x \in A$, such that $y=f(x)$;

(iii) f is **bijective** (or **a bijection)** if it is injective and surjective. ■

Thus;

(i) f is injective if and only if the implication

$$f(x) = f(x') \Rightarrow x = x'$$

is true, for all $x,x' \in A$;

(ii) f is surjective if and only if every element of the final set is the image by f of at least one element of the initial set.

(iii) f is bijective $\Leftrightarrow \forall y \in B, \exists! x \in A$, such that $y=f(x)$.

Examples: 1) Let X be a non-empty subset of a set A. The mapping $f : X \longrightarrow A$, defined by $f(u) = u$, for all $u \in X$ is an injection, denoted i_X and called the **canonical injection** (or the **inclusion map**) of X. Thus $i_X : X \longrightarrow A$, is defined by $i_X(u) = u, \forall u \in X$.

2) If A and B are non-empty sets, then the mapping $Pr_1 : A \times B \longrightarrow A$, defined by $Pr_1(x,y) = x$, for all $(x,y) \in A \times B$ is a surjection, called the **first projection**.

Similarly, the mapping $Pr_2 : A \times B \longrightarrow B$, defined by $Pr_2(x,y) = y$, for all $(x,y) \in A \times B$ is a surjection, called the **second projection**.

3) The mapping $f : \mathbb{R} \longrightarrow \mathbb{R}$, defined by $f(x)=e^x$ is injective and not surjective.

4) The mapping $g : \mathbb{Z} \longrightarrow \mathbb{N}$, defined by $g(x)=|x|$ is surjective and not injective.

2.4.1. The following hold

(i) The identity mapping id_X of every non-empty set X is bijective.

(ii) If $f : A \longrightarrow B$ is a mapping, then f is surjective if and only if $Im(f)=B$.

Proof: (i) We have that the implication

$$id_X(a) = id_X(a') \Rightarrow a=a'$$

is true, for all $a,a' \in X$, hence id_X is injective. Also as $id_X(a)=a$, for all $a \in X$, then id_X is surjective, and so it is bijective.

(ii) **N.C:** Let $x \in B$, then $\exists a \in A$, such that $x=f(a)$, and so $x \in Im(f)$, whence $B \subseteq Im(f)$. But $Im(f) \subseteq B$, hence $Im(f)=B$.

S.C: Let $x \in B$, then $x \in Im(f)$, and so $\exists a \in A$, such that $x=f(a)$, whence f is surjective. ■

Remark: If $f : A \longrightarrow B$ is a mapping, then the correspondence $g : A \longrightarrow Im(f)$ that associates every element x of A with f(x), is a surjection.

2.4.2. Let $f : A \longrightarrow B$ be a mapping. Then we have

(i) If f is injective and g and h are two mappings from a non-empty set C to A, such that $f \circ g = f \circ h$, then g=h.

(ii) If f is surjective and g and h are two mappings from B to a non-empty set C, such that $g \circ f = h \circ f$, then g=h.

Proof: (i) Let $x \in C$, then $f \circ g(x) = f \circ h(x)$, and so $f(g(x))=f(h(x))$. But f is injective, hence $g(x)=h(x)$, and so g=h.

(ii) Let $x \in B$. As f is surjective, then $\exists a \in A$, such that $x=f(a)$. We have

$$g(x) = g(f(a)) = g \circ f(a) = h \circ f(a) = h(f(a)) = h(x)$$

hence g=h. ■

2.4.3. Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be a mappings. Then we have

(i) If f and g are injective (resp. surjective, bijective), then so is $g \circ f$.

(ii) If $g \circ f$ is injective, then so is f.

(iii) If $g \circ f$ is surjective, then g is surjective.

Proof: (i) Assume that f and g are injective. For every $x,x' \in A$, we have

$$g \circ f(x)=g \circ f(x') \Rightarrow g(f(x))=g(f(x')) \overset{\text{g injective}}{\Longrightarrow} f(x) = f(x') \overset{\text{f injective}}{\Longrightarrow} x=x'$$

and so $g \circ f$ is injective.

Suppose that f and g are surjective and let $y \in C$. Since g is surjective, there exists $b \in B$, such that $y=g(b)$. But f is surjective, hence $b=f(a)$, for some $a \in A$. We have $a \in A$ and

$$g \circ f(a) = g(f(a)) = g(b) = y$$

whence every element y of C is the image by $g \circ f$ of some element a of A, and so $g \circ f$ is surjective.

Now if f and g are bijective, then they are injective and surjective, and so $g \circ f$ is injective and surjective, whence $g \circ f$ is bijective.

(ii) Let $x,x' \in A$. Then

$$f(x)=f(x') \overset{\text{g mapping}}{\Longrightarrow} g(f(x))=g(f(x')) \Rightarrow g \circ f(x)=g \circ f(x') \overset{\text{gof injective}}{\Longrightarrow} x=x'$$

and so f is injective.

(iii) Let $y \in C$. Since $g \circ f$ is surjective, there exists $a \in A$, such that $y=g \circ f(a)$. Let $b=f(a)$. Then $b \in B$ and $g(b)=g(f(a))=g \circ f(a)=y$, whence every element y of C is the image by g of some element b of B, and so g is surjective. ■

2.4.4. If $f : A \longrightarrow B$ is a mapping, then the following are equivalent

(i) f is injective

(ii) $f^{-1}(f(X)) = X, \forall X \in P(A)$.

(iii) $f(X \cap Y) = f(X) \cap f(Y), \forall X,Y \in P(A)$.

Proof: (i)⇒(ii): Let $X \in P(A)$, then

$$X \subseteq f^{-1}(f(X))$$

by 2.3.3(i). Let $x \in f^{-1}(f(X))$. Then $f(x) \in f(X)$, and so $\exists a \in X$, such that $f(x)=f(a)$. But f is injective, hence $x = a$, and so $x \in X$, whence $f^{-1}(f(X)) \subseteq X$. Therefore $f^{-1}(f(X))=X$.

(ii)⇒(iii): Let $X,Y \in P(A)$, then

$$f(X \cap Y) \subseteq f(X) \cap f(Y)$$

by 2.3.1(vi). Let $x \in f(X) \cap f(Y)$, then $x \in f(X)$ and $x \in f(Y)$, and so

$$\exists a \in X, \text{ such that } x=f(a)$$

We have x=f(a) and $x \in f(Y)$, hence $f(a) \in f(Y)$, and so $a \in f^{-1}(f(Y))$. But $f^{-1}(f(Y))=Y$, hence $a \in Y$, and so $a \in X \cap Y$, whence $x \in f(X \cap Y)$. Therefore $f(X) \cap f(Y) \subseteq f(X \cap Y)$, and so

$$f(X \cap Y)=f(X) \cap f(Y).$$

<u>(iii)⇒(i):</u> Assume that f is not injective. Then $\exists a,b \in A$, such that

$$f(a) = f(b) \text{ and } a \neq b.$$

Since $a \neq b$, we then get that $\{a\} \cap \{b\} = \emptyset$, hence

$$f(\{a\} \cap \{b\}) = f(\emptyset) = \emptyset.$$

But $f(\{a\} \cap \{b\})=f(\{a\}) \cap f(\{b\})=\{f(a)\} \cap \{f(b)\}=\{f(a)\}$, for f(a)=f(b), hence $\{f(a)\}=\emptyset$, impossible. Therefore f must be injective. ■

<u>2.4.5.</u> If $f : A \longrightarrow B$ is a mapping, then the following are equivalent

(i) f is surjective

(ii) $f(f^{-1}(Y)) = Y, \forall Y \in P(B)$.

(iii) $f^{-1}(\{b\}) \neq \emptyset, \forall b \in B$.

<u>Proof:</u> <u>(i)⇒(ii):</u> Let $Y \in P(B)$, then

$$f(f^{-1}(Y)) \subseteq Y$$

by 2.3.3(ii). Let $x \in Y$. Since f is surjective and $x \in B$, we then get that $\exists a \in A$, such that x = f(a). As $f(a) \in Y$, then $a \in f^{-1}(Y)$, and so $f(a) \in f(f^{-1}(Y))$, whence $x \in f(f^{-1}(Y))$. Therefore $Y \subseteq f(f^{-1}(Y))$, and so $f(f^{-1}(Y))=Y$.

<u>(ii)⇒(iii):</u> Let $b \in B$. As $\{b\} \in P(B)$, then $f(f^{-1}(\{b\}))=\{b\}$. If $f^{-1}(\{b\})=\emptyset$, then $\{b\}= f(f^{-1}(\{b\})) = f(\emptyset) = \emptyset$, by 2.3.1(i), a contradiction. Therefore $f^{-1}(\{b\}) \neq \emptyset$.

<u>(iii)⇒(i):</u> Let $b \in B$. As $f^{-1}(\{b\}) \neq \emptyset$, then $\exists a \in f^{-1}(\{b\})$. We have $a \in A$ and f(a)=b, hence f is surjective. ■

<u>2.4.6.</u> If $f : A \longrightarrow B$ is a mapping, then

(i) f is injective if and only if there exists a mapping $g : B \longrightarrow A$, such that $g \circ f = id_A$.

(ii) f is surjective if and only if there exists a mapping $g : B \longrightarrow A$, such that $f \circ g = id_B$.

<u>Proof:</u> The proof is given in Appendix I. ■

<u>§ 2.5. INVERTIBLE MAPPING.</u>

<u>Definition 12.</u> A mapping $f : A \longrightarrow B$ is said to be **invertible** if there exists a mapping $g : B \longrightarrow A$, such that $g \circ f = id_A$ and $f \circ g = id_B$. ■

<u>2.5.1.</u> If $f : A \longrightarrow B$ is invertible, then the mapping g of B to A, satisfying $g \circ f = id_A$ and $f \circ g = id_B$, is unique.

<u>Proof:</u> Suppose that h is a mapping of B to A, such that $h \circ f = id_A$ and $f \circ h = id_B$. As $g \circ f = id_A$ and $f \circ g = id_B$, then g = h, by 2.2.4. ■

<u>Definition 13.</u> If $f : A \longrightarrow B$ is invertible, the unique mapping g of B to A, satisfying

$g \circ f = id_A$ and $f \circ g = id_B$, is called the **inverse** of f and denoted f^{-1}. ■

2.5.2. If $f : A \longrightarrow B$ and $g : B \longrightarrow A$ are mappings, then

$$f \text{ invertible and } g = f^{-1} \Leftrightarrow f \circ g = id_B \text{ and } g \circ f = id_A .$$

Proof: $\Rightarrow$): As $g = f^{-1}$, then $f \circ g = f \circ f^{-1} = id_B$ and $g \circ f = f^{-1} \circ f = id_A$.
$\Leftarrow$): As $f \circ g = id_B$ and $g \circ f = id_A$, then f is invertible and $g = f^{-1}$. ■

2.5.3. If A and B are non-empty sets, then a mapping $f : A \longrightarrow B$ is invertible if and only if f is bijective.

Proof: **N.C:** We have id_A is injective and $f^{-1} \circ f = id_A$, so that f is injective, by 2.4.3(ii). Since id_B is surjective and $f \circ f^{-1} = id_B$, we then get that f is surjective, by 2.4.3(iii). Therefore f is injective and surjective, and so it is bijective.
S.C: We have f is injective and surjective, hence there exist two mappings g and h from B to A, such that $g \circ f = id_A$ and $f \circ h = id_B$, by 2.4.6. As g=h, by 2.2.4, then $g \circ f = id_A$ and $f \circ g = id_B$, and so f is invertible. ■

2.5.4. If $f : A \longrightarrow B$ is invertible, then
(i) f^{-1} is invertible; (ii) $(f^{-1})^{-1} = f$, (iii) f^{-1} is bijective.

Proof: As $f \circ f^{-1} = id_B$ and $f^{-1} \circ f = id_A$, then f^{-1} is invertible and $(f^{-1})^{-1} = f$. Also as f^{-1} is invertible, then f^{-1} is bijective, by 2.5.3, and so (i), (ii) and (iii) hold. ■

2.5.5. If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are invertible, then so is $g \circ f$ and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Proof: We have

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ f \circ f^{-1} \circ g^{-1} = g \circ id_B \circ g^{-1} = g \circ g^{-1} = id_C$$

and

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ id_B \circ f = f^{-1} \circ f = id_A$$

hence $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, by 2.5.2. ■

M1100

CHAPTER II

EXERCISES

1- Let E be a set. For each subset A of E, we define the **characteristic function** of A, denoted 1_A to be the mapping $1_A : E \longrightarrow \{0,1\}$, defined by

$$1_A(x) = 1 \text{ if } x\in A \text{ and } 1_A(x) = 0 \text{ if } x\notin A.$$

1- Show that $\forall X,Y\in P(E)$

(i) $1_X = 1_Y \Leftrightarrow X=Y$.

(ii) $1_{(X\cap Y)}(x) = 1_X(x)1_Y(x)$, $\forall x\in E$.

(iii) $1_{(X\cup Y)}(x) = 1_X(x)+1_Y(x)-1_X(x)1_Y(x)$, $\forall x\in E$.

(iv) $1_{(E-X)}(x) = 1-1_X(x)$, $\forall x\in E$.

2- Deduce that if $A,B,C\in P(E)$, then

(i) $(A\cap B)\cup C = (A\cup C)\cap(B\cup C)$.

(ii) $E-(A\cap B) = (E-A)\cup(E-B)$.

2- Which of the following mappings are injective, surjective or bijective ?

$f : \mathbb{R} \longrightarrow \mathbb{R}$, defined by $f(x) = 4x-3$,

$g : \mathbb{R} \longrightarrow \mathbb{R}$, defined by $g(x) = x^2+x-6$ and

$h : \mathbb{R}-\{1\} \longrightarrow \mathbb{R}$, defined by $h(x) = \frac{x-2}{x-1}$.

Determine Im(f), Im(g) and Im(h).

3- Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ and $g : \mathbb{N} \longrightarrow \mathbb{N}$ be the mappings defined by

$$f(x) = 2x \text{ and } g(x)= \begin{cases} x/2 & \text{if } x \text{ is even} \\ (x-1)/2 & \text{if } x \text{ is odd.} \end{cases}$$

1- Are f and g injective ? surjective ?

2- Let A be the set of odd natural numbers. Give the restriction of g on A.

3- Find $f\circ g$ and $g\circ f$.

4- Let $f :]1 , +\infty[\longrightarrow]0 , +\infty[$ and $g :]0 , +\infty[\longrightarrow]1 , +\infty[$ be defined by

$$f(x) = x^2+2x+1 \text{ and } g(x) = \frac{x+1}{x}.$$

1- Show that f is injective but is not surjective.

2- Show that g is bijective and find g^{-1}.

3- Find $f\circ g$ and $g\circ f$. Are $f\circ g$ and $g\circ f$ injective ? surjective ?

5- Let $f : E \longrightarrow F$ be mapping.

1- Show that if f is injective, then for every subset A of E, we have

$$f(x)\in f(A) \Leftrightarrow x\in A.$$

2- Show that if f is bijective, then $f(\complement_E A) = \complement_F f(A)$, for all $A\in P(E)$.

6- Show that if $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are two mappings, then

(i) $g \circ f$ injective and f surjective $\Rightarrow$ g injective.

(ii) $g \circ f$ surjective and g injective $\Rightarrow$ f surjective.

7- Let $f : E \longrightarrow E$ be mapping. Prove that

(i) f is injective if and only if for every mappings g and h of E to E, we have

$$f \circ g = f \circ h \Rightarrow g = h.$$

(ii) f is surjective if and only if for every mappings g and h of E to E, we have

$$g \circ f = h \circ f \Rightarrow g = h.$$

8- Let $f : A \longrightarrow B$ and $g : A \longrightarrow C$ be two mappings. Show that if f is bijective, then there exists a unique mapping $h: B \longrightarrow C$, such that $h \circ f=g$.

9- A mapping $f : A \longrightarrow A$ is said to be **involutive** or that it is an **involution** if f is bijective and $f^{-1}=f$. Show that f is involutive if and only if $f \circ f = id_A$.

10- Let $f : E \longrightarrow E$ be mapping.

1- Show that $f(A)-f(B) \subseteq f(A-B)$, $\forall A,B \in P(E)$.

2- Show that the following are equivalent

(i) f injective.

(ii) $\forall A,B \in P(E)$, $A \cap B = \varnothing \Rightarrow f(A) \cap f(B) = \varnothing$.

(iii) $f(A-B) = f(A)-f(B)$, $\forall A,B \in P(E)$.

11- Let $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$ be mappings. Show that if $g \circ f$ and $h \circ g$ are bijective, then f, g and h are bijective.

12- Let $f : A \longrightarrow B$ be mapping.

1- Show that if E is a set and $x,y \in E$, then

$$x \neq y \Leftrightarrow \{x\} \cap \{y\} = \varnothing.$$

2- Deduce that f is injective if and only if $f(\{a\} \cap \{b\}) = f(\{a\}) \cap f(\{b\})$, for all $a,b \in A$.

13- Let $f : A \longrightarrow B$ be mapping. Show that

(i) f is injective if and only if $f^{-1}(f(\{a\}) =\{a\}$, for all $a \in A$.

(ii) f is surjective if and only if $f(f^{-1}(\{b\}) =\{b\}$, for all $b \in B$.

14- Let E be a non-empty set. For each subset X of E, let $\overline{X} = \complement_E X$. Let $f : E \longrightarrow E$ be a mapping, such that

$$f(\overline{X}) = \overline{f(X)}, \text{ for all } X \in P(E).$$

1- Show that $\overline{f(E)} = \varnothing$ and deduce that f is surjective.

2- Show that $\overline{f(A \cap B)} = f(\overline{A} \cup \overline{B})$, for all $A,B \in P(E)$.

3- Deduce that f is bijective.

15- Let A be a subset of a non-empty set E and let f : P(E)$\longrightarrow$P(E) be the mapping defined by

$$f(X) = X\cap A.$$

Find f(E), $f^{-1}(\{E\})$, f(∅), $f^{-1}(\varnothing)$ and $f^{-1}(\{\varnothing\})$ (to find f(∅), distinguish between the case where ∅ is an element of P(E) and the case where ∅ is a subset of P(E)).

16- Let f : E $\longrightarrow$F be a mapping of E to F and and let S be the set of all subsets X of E, satisfying $f^{-1}(f(X))=X$.

1- Show that $f^{-1}(f(A))\in S$, $\forall A\in P(E)$.

2- Show that S is closed under both union and intersection of sets, i.e $X\cup Y\in S$ and $X\cap Y\in S$, for all $X,Y\in S$.

3- Show that if $X\in S$ and $A\in P(E)$, such that $X\cap A=\varnothing$, then $X\cap f^{-1}(f(A))=\varnothing$.

4- Show that if X and X' are elements of S, then so is (X-X').

17- Let f : E$\longrightarrow$F be a mapping.

1- Show that if $(A_i)_{i\in I}$ is a family of subsets of E, then

(i) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$; (ii) $f(\bigcap_{i\in I} A_i)\subseteq \bigcap_{i\in I} f(A_i)$.

2- Show that if $(A_i)_{i\in I}$ is a family of subsets of F, then

(i) $f^{-1}(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f^{-1}(A_i)$; (ii) $f^{-1}(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f^{-1}(A_i)$.

M1100

CHAPTER III

FINITE SETS

§ 3.1. EQUIPOLLENT SETS.

Definition 1. We say that two sets E and F are **equipollent** and we write $E\approx F$ (read: "E equipollent to F") if there exists a bijection of E onto F. ■

3.1.1. If A, B and C are three sets, then
(i) $A\approx A$.
(ii) $A\approx B \Rightarrow B\approx A$.
(iii) $A\approx B$ and $B\approx C \Rightarrow A\approx C$.

Proof: (i) Since id_A is a bijection of A onto A, by 2.4.1(i), we then have $A\approx A$.

(ii) Assume that $A\approx B$. Then there exists a bijection f of A onto B. Since. f^{-1} is a bijection of B onto A, by 2.5.3 and 2.5.4, we then get $B\approx A$.

(iii) Suppose that $A\approx B$ and $B\approx C$. Then there exist two bijections f of A onto B and g of B onto C. Since $g\circ f$ is a bijection of A onto C, by 2.4.3, we then have $A\approx C$. ■

3.1.2. If $f : E\longrightarrow F$ is an injection and $X\subseteq E$, then $X\approx f(X)$.

Proof: Let $g : X\longrightarrow f(X)$ be the mapping defined by $g(x) = f(x)$.
g injective: Let $x,y\in X$, then

$$g(x)=g(y) \Rightarrow f(x)=f(y) \Rightarrow x=y$$

hence g is injective.
g surjective: Let $y\in f(X)$, then $\exists x\in X$, such that $y=f(x)=g(x)$, hence g is surjective.
It follows that g is bijective, and so $X\approx f(X)$. ■

3.1.3. If $A\approx\varnothing$, then $A=\varnothing$.

Proof: As $A\approx\varnothing$, then there exists a bijection $f : A\longrightarrow\varnothing$. As $f(A)=\varnothing$, then $A=\varnothing$, by 2.3.1(i). ■

3.1.4. If $A\approx B$ and $C\approx D$ and $A\cap C = B\cap D = \varnothing$, then $A\cup C\approx B\cup D$.

Proof: The proof is given in Appendix I. ■

§ 3.2. CARDINAL OF A FINITE SET.

For every $a,b\in\mathbb{N}$ we call **interval** $[a,b]$ of $\mathbb{N}$, the subset

$$[a, b] = \{x\in\mathbb{N} ;\ a\leq x\leq b\}.$$

Thus

$$[1, 0]=\varnothing,\ [1, 1]=\{1\},\ [1, 2]=\{1,2\},\ldots,\ [1, n]=\{1,2....,n\},\ \forall n\geq 2.$$

3.2.1. The following hold
(i) If $a,b\in\mathbb{N}$, then

$a<b \Leftrightarrow a\leq b-1$; and $a<b \Leftrightarrow a+1\leq b$.

(ii) if $n\geq 1$, then

$$[1, n] = [1, n-1]\cup\{n\} \text{ and } [1, n-1]\cap\{n\}=\varnothing.$$

(iii) if $n,m\in\mathbb{N}$, then

$[1, m+n] = [1, m]\cup[m+1, m+n]$ and $[1, m]\cap[m+1, m+n]=\varnothing$.

Proof: Easy enough. ■

3.2.2. If $a,b\in\mathbb{N}$ and $a\leq b$, then $[a, b]\approx[1, b-a+1]$.

Proof: Define $f : [a, b]\longrightarrow[1, b-a+1]$ by $f(t) = t-a+1$. As $a\leq t\leq b$, then $1\leq t-a+1\leq b-a+1$, and so f can be easily checked to be a mapping.

f injective: Let $s,t\in[a, b]$, then

$$f(s)=f(t) \Rightarrow s-a+1=t-a+1 \Rightarrow s=t$$

hence f is injective.

f surjective: Let $y\in[1, b-a+1]$ and let $t=y+a-1$. As $1\leq y\leq b-a+1$, then $a\leq t\leq b$, and so $t\in[a, b]$. We have $f(t)=t-a+1=y$, hence f is surjective, and so f is bijective, whence $[a, b]\approx[1, b-a+1]$. ■

3.2.3. If $n\geq 1$ and $x_1,\ldots, x_n$ are n pairwise distinct elements of $[1,n]$, then

$$[1,n]=\{x_1,\ldots,x_n\}.$$

Proof: The proof is given in Appendix I. ■

Corollary 3.2.3.1. If $m,n\in\mathbb{N}$ and $[1,m]\approx[1,n]$, then $m = n$.

Proof: If $n=0$, then $[1,n]=\varnothing$, and so $[1,m]=\varnothing$, by 3.1.3, whence $m=0$, and so $n=m$, in this case. Similarly if $m=0$, we get $n=0$, and so $n=m$, in this case also. Suppose that $n\neq 0$ and $m\neq 0$, then

$$n\geq 1 \text{ and } m\geq 1.$$

Assume that $n\leq m$ and let $f : [1,n] \longrightarrow[1,m]$ be a bijection. For each $1\leq t\leq m$, let $x_t=f^{-1}(t)$. As $n\leq m$ and f^{-1} is injective, then $x_1,\ldots,x_n$ are n pairwise distinct elements of $[1,n]$, and so 3.2.3 yields that

$$[1,n]=\{x_1,\ldots,x_n\}=\{f^{-1}(1),\ldots, f^{-1}(n)\}=f^{-1}([1,n]).$$

This implies that $f([1,n])=[1,n]$. But $f([1,n])=[1,m]$, hence $[1,n]=[1,m]$, and so $m=n$. ■

Definition 2. A set E is said to be **finite** if there exists $n\in\mathbb{N}$, such that $E\approx[1,n]$ and it is said to be **infinite** if it is not finite. ■

Examples: 1) If $a,b\in\mathbb{N}$ and $a\leq b$, then $[a,b]$ is finite, because $[a,b]\approx[1,b-a+1]$.

2) $\mathbb{N}$ is infinite, because if it is finite, then $\mathbb{N}\approx[1,n]$, for some $n\in\mathbb{N}$, and so there exists a bijection $f : \mathbb{N}\longrightarrow[1,n]$. As $f(1),\ldots,f(n)$ are n pairwise distinct elements of $[1,n]$, then $[1,n]=\{f(1),\ldots,f(n)\}$. But $f(n+1)\in[1,n]$, hence $f(n+1)\in\{f(1),...,f(n)\}$, and so $\exists t\in\{1,...,n\}$, such that $f(n+1)=f(t)$. As f is injective, then $n+1=t$, and so $n+1\leq n$, impossible. Therefore $\mathbb{N}$ is infinite.

Definition 3. If E is finite, we define the **cardinal** of E to be the natural number n, such that $E\approx[1,n]$. ■

Thus; E is a finite set of cardinal n if and only if the number of elements of E is n. If E is finite of cardinal n, then E can be written in the form:

$$E = \{x_1,....., x_n\}$$

for let $f : [1,n] \longrightarrow E$ be a bijection; then

$$E = f([1,n]) = f(\{1,....,n\}) = \{f(1),....,f(n)\}$$

so that we can take $x_1 = f(1),..., x_n = f(n)$.

Examples: card(∅)=0, card({x})=1,..., card($\{x_1,...,x_n\}$)=n.

3.2.4. E=∅ if and only if card(E)=0.

Proof: **N.C:** As E=∅, then E≈[1,0], and so card(E)=0.
S.C: We have E≈[1,0] and [1,0]=∅, hence E=∅, by 3.1.3. ■

3.2.5. If E is finite of cardinal n and if F≈E, then F is finite and card(F)=n.

Proof: Since F≈E and E≈[1,n], we then get that F≈[1,n], and so F is finite and card(F)=n. ■

3.2.6. If E and F are two finite sets and E∩F=∅, then E∪F is finite and

$$\text{card}(E\cup F)=\text{card}(E)+\text{card}(F).$$

Proof: Let card(E)=m and card(F)=n. Then E≈[1,m] and F≈[1,n]. By 3.2.2, we have that

$$[m+1\ ,\ m+n]\approx[1,\ (m+n)-(m+1)+1] = [1,n]$$

hence F≈[m+1 , m+n]. But E∩F=∅ and [1,m]∩[m+1 , m+n]=∅, hence

$$E\cup F\approx[1,m]\cup[m+1\ ,\ m+n] = [1,\ m+n]$$

by 3.1.4, and so E∪F is finite and card(E∪F)=m+n=card(E)+card(F). ■

Corollary 3.2.6.1. If $E_1,...., E_n$ are pairwise disjoint finite sets, then $E_1\cup....\cup E_n$ is finite and card($E_1\cup....\cup E_n$)=card(E_1)+····+card(E_n).

Proof: Use 3.2.6 and argue by induction on n. ■

3.2.7. If A is a subset of a finite set E, then A is finite and card(A)≤card(E).

Proof: The proof is given in Appendix I. ■

3.2.8. If E and F are two finite sets, then E∪F is finite and

$$\text{card}(E\cup F) = \text{card}(E)+\text{card}(F)-\text{card}(E\cap F).$$

Proof: Since F-E is finite, by 3.2.7 and E∪F=E∪(F-E) and E∩(F-E)=∅, we then have that E∪F is finite and

$$\text{card}(E\cup F)=\text{card}(E)+\text{card}(F-E) \qquad (1)$$

by 3.2.6. But F=(F-E)∪(E∩F) and (F-E)∩(E∩F)=∅, and E∩F is finite, by 3.2.7, hence card(F)=card(F-E)+card(E∩F), by 3.2.6. This implies that card(F-E)=card(F)-card(E∩F), whence (1) yields that card(E∪F) = card(E)+card(F)-card(E∩F). ■

3.2.9. If E is finite and A is a subset of E with card(A)=card(E), then A=E.

Proof: We have $E=A\cup\complement_E A$ and $A\cap\complement_E A=\varnothing$, hence $\mathrm{card}(E)=\mathrm{card}(A)+\mathrm{card}(\complement_E A)$, by 3.2.6. But card(E)=card(A), whence $\mathrm{card}(\complement_E A)=0$, and so $\complement_E A=\varnothing$, by 3.2.4. Thus E=A.■

3.2.10. If E and F are two finite sets, such that card(E)=card(F) and if $f : E\longrightarrow F$ is injective, then f is surjective.

Proof: As $E\approx f(E)$, by 3.1.2, then f(E) is finite and card(f(E))=card(E)=card(F). But $f(E)\subseteq F$ and F is finite, hence F=f(E), by 3.2.9, and so f is surjective. ■

Corollary 3.2.10.1. If E and F are two finite sets, such that card(E)=card(F) and if $f : E\longrightarrow F$ is a mapping, then the following are equivalent:

(i) f is bijective, (ii) f is injective, (iii) f is surjective.

Proof: (i)⇒(ii): By definition of bijective mapping.

(ii)⇒(iii): By 3.2.10.

(iii)⇒(i): Since f is surjective, there exists $g : F\longrightarrow E$, such that

$$f\circ g=\mathrm{id}_F$$

by 2.4.6(ii). We have g is injective, by 2.4.3(ii), hence g is surjective, by 3.2.10. It follows from 2.5.3 and 2.5.4 that g^{-1} exists and g^{-1} is bijective. As

$$g^{-1}=\mathrm{id}_F\circ g^{-1}=(f\circ g)\circ g^{-1}=f\circ(g\circ g^{-1})=f\circ\mathrm{id}_E=f$$

then f is bijective. ■

Corollary 3.2.10.2. If A is a finite set and $f : A\longrightarrow A$ is a mapping, then the following statements are equivalent:

(i) f is bijective, (ii) f is injective, (iii) f is surjective.

Proof: This is an immediate consequence of 3.2.10.1. ■

M1100

CHAPTER III

EXERCISES

1- Show that if E and F are sets, then $E\times F\approx F\times E$.

2- Show that if E and F are two finite sets, then $E\times F$ is finite and

$$\mathrm{card}(E\times F) = \mathrm{card}(E)\times\mathrm{card}(F).$$

Deduce that if E is finite and $n\in\mathbb{N}^*$, then E^n is finite and $\mathrm{card}(E^n) = (\mathrm{card}(E))^n$.

3- Let E and F be two finite sets and set

$$E = \{a_1, ..., a_n\}.$$

Show that the mapping $\varphi : F^E \longrightarrow F^n$, defined by

$$\varphi(f) = (f(a_1), ..., f(a_n))$$

is bijective. Deduce that F^E is finite and $\mathrm{card}(F^E) = (\mathrm{card}(F))^{\mathrm{card}(E)}$.

4- Show that if E is a finite set of cardinal n, then P(E) is finite and $\mathrm{card}(P(E))= 2^n$.

M1100

CHAPTER IV

BINARY OPERATIONS

§ 4.1. DEFINITION AND PROPERTIES.

Definition 1. Let E be a non-empty set. We call **binary operation** (or **internal composition law**) on E, every mapping of E×E to E. ∎

If $f : E\times E \longrightarrow E$ is a binary operation on E, then the image by f of every ordered pair (a,b) of E×E is denoted afb and called the **composite** of a and b.

Definition 2. A binary operation on E is said to be **additive** (resp. **multiplicative**) or that it is an **addition** (resp. **multiplication**) if the composite of any two elements a and b of E is denoted a+b (resp. ab or a×b). ∎

Examples: 1)If E = $\mathbb{N}$ (or $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$), then the binary operations

$$f : E\times E \longrightarrow E \quad \text{and} \quad g : E\times E \longrightarrow E$$

defined by $f(x,y) = x+y$ and $g(x,y) = xy$, are respectively called the **usual addition** and **usual multiplication** of E.

2)The mappings $f : P(E)\times P(E) \longrightarrow P(E)$ and $g : P(E)\times P(E) \longrightarrow P(E)$, defined by $f(X,Y) =X\cup Y$ and $g(X,Y) = X\cap Y$ are two binary operations on P(E). They are respectively called the **union** and the **intersection** and denoted ∪ and ∩.

3) The mapping $\varphi : E^E \times E^E \longrightarrow E^E$ defined by $\varphi(f,g) = f\circ g$, is a binary operation on E^E, called the **usual composition** of mappings and denoted ∘.

Definition 3. We call **magma** every ordered pair (E,∗), where E is a non-empty set and ∗ is a binary operation on E. ∎

We say that E is **endowed with** ∗ if (E,∗) is a magma.

If ∗ and T are two binary operations on E, then the statement

"E is endowed with ∗ and T"

is written (E,∗,T).

For the rest of this chapter, let (E,∗) be a magma.

Definition 4. We say that

(i) ∗ is **associative** if $a*(b*c) = (a*b)*c$, $\forall a,b,c\in E$.

(ii) ∗ is **commutative** if $a*b = b*a$, $\forall a,b\in E$. ∎

Examples: 1) The usual addition and multiplication of numbers are associative and commutative, while the subtraction is neither associative nor commutative.

2) The union and the intersection of sets are associative and commutative.

3) The composition of mappings is associative but is not in general commutative.

Remark: The composite of three elements a, b and c may be written in two different ways: $(a*b)*c$ and $a*(b*c)$, and if $*$ is associative, then the two formulas will give the same result, making the parenthesis unnecessary. Thus the composite of a, b and c may be written as $a*b*c$. It follows that if $*$ is associative, then the parenthesis in every expression are unnecessary and hence can be lifted.

4.1.1. If $n\geq 2$ and $a_1,a_2,....,a_n \in E$ and $*$ is associative and commutative, then

$$a_1*a_2*....*a_n = a_{i_1}*a_{i_2}*....*a_{i_n}, \text{ for all } \{i_1,i_2,...,i_n\} = \{1,2,...,n\}.$$

Proof: The proof is given in Appendix I. ■

Definition 5. Let $a\in E$. We call **left** (resp. **right**) **translation** by a, the mapping of E to E, denoted γ_a (resp. δ_a), defined by $\gamma_a(x) = a*x$ (resp. $\delta_a(x) = x*a$), for all $x\in E$. ■

4.1.2. The following are equivalent:
(i) $*$ is associative,
(ii) $\gamma_{(a*b)} = \gamma_a \circ \gamma_b$, for all $a,b\in E$,
(iii) $\delta_{(a*b)} = \delta_b \circ \delta_a$, for all $a,b\in E$.

Proof: (i)⇒(ii): For every $x\in E$, we have

$$\gamma_{(a*b)}(x) = (a*b)*x = a*(b*x) = \gamma_a(b*x) = \gamma_a(\gamma_b(x)) = \gamma_a \circ \gamma_b(x)$$

hence $\gamma_{(a*b)} = \gamma_a \circ \gamma_b$.

(ii)⇒(iii): Let $a,b\in E$. For every $x\in E$, we have

$$\delta_{(a*b)}(x) = x*(a*b) = \gamma_x(a*b) = \gamma_x(\gamma_a(b)) = \gamma_x \circ \gamma_a(b) = \gamma_{(x*a)}(b) = (x*a)*b$$
$$= \delta_b(x*a) = \delta_b(\delta_a(x)) = \delta_b \circ \delta_a(x)$$

hence $\delta_{(a*b)} = \delta_b \circ \delta_a$.

(iii)⇒(i): Let $a,b,c\in E$, then

$$a*(b*c) = \delta_{(b*c)}(a) = \delta_c \circ \delta_b(a) = \delta_c(\delta_b(a)) = \delta_c(a*b) = (a*b)*c$$

and so $*$ is associative. ■

Definition 6. Let T be a binary operation on E. We say that
(i) $*$ is **distributive on the left** over T if

$$x*(yTz) = (x*y)T(x*z), \forall x,y,z\in E,$$

(ii) $*$ is **distributive on the right** over T if

$$(xTy)*z = (x*z)T(y*z), \forall x,y,z\in E,$$

(iii) $*$ is **distributive** over T if it is distributive on the left and on the right over T. ■

Examples: 1) The usual multiplication of numbers is distributive over the usual addition of numbers.
2) Each of the union and the intersection of sets is distributive over the other.

§ 4.2. PARTICULAR ELEMENTS.

Definition 7. Let $e\in E$. We say that

(i) e is **neutral on the left** for $*$ if $e*a = a$, $\forall a\in E$.

(ii) e is **neutral on the right** for $*$ if $a*e = a$, $\forall a\in E$.

(iii) e is **neutral** for $*$ (or that e is a **neutral element** of $(E,*)$) if e is neutral on the left and on the right for $*$, i.e if $a*e = e*a = a$, $\forall a\in E$. ■

A neutral element of E is also called an **identity** of E.

Before giving examples on neutral element, we prove

4.2.1. If e and e' are two elements of E, such that e is neutral on the left and e' is neutral on the right, then e = e'.

Proof: We have $e*e' = e'$ and $e*e' = e$, hence $e = e'$. ■

Corollary 4.2.1.1. If e is a neutral element of $(E,*)$, then e is unique.

Proof: Let e' be a neutral element of $(E,*)$. Since e is neutral on the left and e' is neutral on the right, we then have e = e', by 4.2.1. ■

Examples: 1) If $E = \mathbb{N}$ (or $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$), then 0 is the neutral element of $(E,+)$ and 1 is the neutral element of $(E,\times)$.

2) $\varnothing$ is the neutral element of $(P(E), \cup)$ and E is the neutral element of $(P(E), \cap)$.

3) id_E is the neutral element of $(E^E, \circ)$.

4) Let $*$ be the binary operation defined on $\mathbb{N}$ by

$$x*y = xy+y,$$

then 0 is neutral on the left for $*$ and $(\mathbb{N},*)$ has neither neutral elements on the right nor neutral elements:

As $0*a=0\times a+a=a$, $\forall a\in \mathbb{N}$, then 0 is neutral on the left. If e is neutral on the right, then e=0, by 4.2.1, and so $a*0=a$, $\forall a\in \mathbb{N}$, whence $1*0=1$, which is impossible, since $1*0=0$. Therefore $(\mathbb{N},*)$ has no neutral elements on the right. As every neutral element is neutral on the right, then $(\mathbb{N},*)$ has no neutral elements.

5) Let $*$ be the binary operation defined on $\mathbb{Z}$ by

$$x*y = 3x-xy$$

then 2 is neutral on the right for $*$ and $(\mathbb{Z},*)$ has neither neutral elements on the left nor neutral elements:

As $a*2=3a-a\times 2=a$, $\forall a\in\mathbb{Z}$, then 2 is neutral on the right. If e is neutral on the left, then e=2, by 4.2.1, and so $2*a=a$, $\forall a\in\mathbb{Z}$, whence $2*0=0$, which is impossible, since $2*0=3\times 2-2\times 0=6$. Therefore $(\mathbb{Z},*)$ has no neutral elements on the left. As every neutral element is neutral on the left, then $(\mathbb{Z},*)$ has no neutral elements.

If e is a neutral element of $(E,*)$, then we say that e is a neutral element of E. We also say that e is a neutral element for $*$ in E. If $*$ is an addition (resp. multiplication), then the neutral element for $*$ is usually denoted 0 (resp. 1).

4.2.2. An element e of E is neutral for $*$ if and only if $\delta_e = \gamma_e = id_E$.

Proof: **N.C:** As e is neutral for $*$, then $x*e=e*x=x$, $\forall x\in E$, and so $\delta_e(x)=x=id_E(x)$ and $\gamma_e(x)=x=id_E(x)$, $\forall x\in E$, whence $\delta_e = \gamma_e = id_E$.
S.C: We have $\delta_e = \gamma_e = id_E$, hence $\delta_e(x)=\gamma_e(x)=id_E(x)$, $\forall x\in E$, and so $x*e=e*x=x$, $\forall x\in E$, whence e is neutral for $*$. ■

Definition 8. An element a of E is called **idempotent** for $*$, if $a*a=a$. ■

Example: Every element of P(E) is idempotent for $\cup$ and for $\cap$.

Definition 9. Let e be a neutral element of $(E,*)$ and let $x,y\in E$. We say that y is an **inverse** of x **on the left** and x is an **inverse** of y **on the right** for $*$, if $y*x = e$. ■

Definition 10. Let e be a neutral element of $(E,*)$ and let $x\in E$. We say that
(i) x is **invertible on the left** or **left invertible** (resp. **on the right** or **right invertible**) for $*$, if x has an inverse on the left (resp. right) for $*$.
(ii) x is **invertible** for $*$ if x is invertible on the left and on the right for $*$. ■

Examples: 1) In $(\mathbb{N},+)$, 0 is the only invertible element for + and in $(\mathbb{N},\times)$, 1 is the only invertible element for ×.
2) Every element of $(\mathbb{Z},+)$ is invertible and +1 and -1 are the only invertible elements of $(\mathbb{Z},\times)$.
3) Every non-zero element of $(\mathbb{Q},\times)$ is invertible for ×.

Definition 11. We say that $(E,*)$ is a **monoid** if $*$ is associative and has a neutral element in E. ■

A monoid $(E,*)$ is called commutative if $*$ is commutative.

4.2.3. If $(E,*)$ is a monoid with identity e, then an element x of E is invertible for $*$ if and only if $\exists x'\in E$, such that $x*x'=x'*x=e$.

Proof: **N.C:** Since x is invertible for $*$, it is invertible on the left and on the right for $*$, whence $\exists y,z\in E$, such that $x*y=e$ and $z*x=e$. We have

$$y = e*y = (z*x)*y = z*(x*y) = z*e = z$$

so that taking $x' = y$, we get that $x*x' = x'*x = e$.
S.C: Since $x*x' = e$ and $x'*x = e$, we then have that x is invertible on the left and on the right for $*$, and so x is invertible for $*$. ■

4.2.4. Suppose that $(E,*)$ is a monoid with identity e. If $x\in E$ is invertible for $*$, then the element x' of E satisfying $x*x' = x'*x = e$ is unique. (x' is called the **symmetric** or the **inverse** of x for $*$).

Proof: Let $x''\in E$, such that $x*x'' = x''*x = e$. Since $*$ is associative and $x*x' = x'*x = e$, we then get $x''=e*x''=(x'*x)*x''= x'*(x*x'')= x'*e= x'$, and so x' is unique. ■

Remark: 1) If $*$ is an addition, then the inverse of every element x of E is denoted -x and called the **opposite** of x.

2) If $*$ is a multiplication, then the inverse of every element x of E is denoted x^{-1}.

4.2.5. Assume that $(E,*)$ is a monoid with identity e. Let $x,y\in E$, then

(i) if x is invertible for $*$ with inverse x’, then x’ is invertible for $*$ and its inverse is x,

(ii) if x and y are invertible for $*$, with inverses x' and y' respectively, then $x*y$ is invertible for $*$ and its inverse is $y'*x'$.

Proof: (i) As $x*x'= x'*x=e$, then x’ is invertible for $*$ and its inverse is x, by 4.2.4.

(ii) Since $*$ is associative, we get that

$$(x*y)*(y'*x') = x*y*y'*x'= x*e*x' = x*x' = e$$

and

$$(y'*x')*(x*y) = y'*x'*x*y = y'*e*y = y'*y = e$$

and so $x*y$ is invertible for $*$ and its inverse is $y'*x'$, by 4.2.4. ■

Definition 12. Let $a\in E$. We say that

(i) a is **regular on the left** or that it is **left regular** for $*$, if the implication

$$a*x = a*y \Rightarrow x = y$$

is true, for all $x,y\in E$.

(ii) a is **regular on the right** or that it is **right regular** for $*$, if the implication

$$x*a = y*a \Rightarrow x = y$$

is true, for all $x,y\in E$.

(iii) a is **regular** for $*$ if a is both left and right regular for $*$. ■

Examples: 1) If $E = \mathbb{N}$ (or $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$), then every element of (E,+) is regular and every non-zero element of $(E,\times)$ is regular.

2) $\varnothing$ is a regular element of $(P(E),\cup)$ and E is a regular element of $(P(E),\cap)$).

3) In $(E^E,\circ)$, we have

(i) every injection of E to E is regular on the left,

(ii) every surjection of E onto E is regular on the right,

(iii) every bijection of E onto E is regular.

4.2.6. If $(E,*)$ is a monoid with identity e, then

(i) Every element of E that is invertible on the left (resp. right) for $*$ is left (resp. right) regular for $*$.

(ii) Every element of E which is invertible for $*$ is regular for $*$.

Proof: (i) Let $a\in E$. If a is invertible on the left for $*$, then $\exists a'\in E$, such that $a'*a = e$, and so $\forall x,y\in E$, we have

$$a*x = a*y \Rightarrow a'*(a*x) = a'*(a*y) \Rightarrow (a'*a)*x = (a'*a)*y \Rightarrow e*x = e*y \Rightarrow x = y$$

whence a is left regular for $*$. Similarly one can easily show that if a is right invertible for $*$, then it is right regular for $*$.

(ii) Let $a\in E$, such that a is invertible for $*$. As a is left and right invertible for $*$, then a is left and right regular for $*$, by (i), whence a is regular for $*$. ■

§ 4.3. INDUCED LAW.

Let A be a non-empty subset of E.

Definition 13. We say that A is **closed** under $*$, if $x*y\in A$, $\forall x,y\in A$. ■

Example: $\mathbb{N}$ is closed under the usual addition and multiplication of $\mathbb{Z}$.

4.3.1. If A is closed under $*$, then the correspondence f from $A\times A$ to A, that associates every element (x,y) of $A\times A$ with the element $x*y$ of A, is a binary operation on A, called the **law induced** by $*$ on A and denoted $*_A$.

Proof: We need to show that f is a mapping. Let $u\in A\times A$. Then $\exists x,y\in A$, such that $u = (x,y)$, and so $x*y$ is an image of u by f. Let v and w be two images of u by f. Then $\exists x,y\in A$, such that $u = (x,y)$ and $v = x*y$ and $\exists z,t\in A$, such that $u = (z,t)$ and $w = z*t$. As $(x,y) = (z,t)$, then $x*y = z*t$, because $*$ is a mapping of $E\times E$ to E, and so $v = w$. Therefore f is a mapping, and so it is a binary operation on A. ■

Thus; if A is closed under $*$, then $x*_A y = x*y$, $\forall x,y\in A$.

4.3.2. If A is closed under $*$, then

(i) If $*$ is commutative (resp. associative), then so is $*_A$.

(ii) If e is a neutral element for $*$ and $e\in A$, then e is a neutral element for $*_A$.

Proof: The proof is easy enough. ■

4.3.3. Let T be a binary operation on E. Suppose that A is closed under $*$ and T. Then we have

(i) If $*$ is distributive on the left (resp. right) over T, then $*_A$ is distributive on the left (resp. right) over T_A.

(ii) If $*$ is distributive over T, then $*_A$ is distributive over T_A.

Proof: (i) Suppose that $*$ is distributive on the left over T and let $x,y,z\in A$, then

$$x*_A(yT_A z) = x*(yTz) = (x*y)T(x*z) = (x*_A y)T_A(x*_A z)$$

and so $*_A$ is distributive on the left over T_A.

Suppose that $*$ is distributive on the right over T and let $x,y,z\in A$, then

$$(xT_A y)*_A z = (xTy)*z = (x*z)T(y*z) = (x*_A z)T_A(y*_A z)$$

and so $*_A$ is distributive on the right over T_A.

(ii) As $*$ is distributive on the left and on the right over T, then $*_A$ is distributive on the left and on the right over T_A, by (i), and so $*_A$ is distributive over T_A. ■

§ 4.4. HOMOMORPHISM.

Let $(E,*)$ and (F,T) be two magmas.

Definition 14. We call **magma homomorphism** of $(E,*)$ to (F,T), every mapping $f : E \longrightarrow F$, satisfying $f(x*y) = f(x)Tf(y)$, $\forall x,y\in E$. ■

Definition 15. If E (resp. F) is endowed with another law, denoted $\perp$ (resp. S), then a magma homomorphism of $(E,*,\perp)$ to (F,T,S) will be defined to be every mapping $f : E \longrightarrow F$, satisfying $f(x*y) = f(x)Tf(y)$ and $f(x\perp y) = f(x)Sf(y)$, $\forall x,y\in E$. ■

4.4.1. A mapping $f : E\longrightarrow F$ is a magma homomorphism of $(E,*,\perp)$ to (F,T,S) if and only if f is a magma homomorphism of $(E,*)$ to (F,T) and a magma homomorphism of $(E,\perp)$ to (F,S).

Proof: This is an immediate consequence of definition 15. ■

Definition 16. We call **magma isomorphism** of E onto F, every bijective magma homomorphism. ■

A magma homomorphism (resp isomorphism) of E to E is called **an endomorphism** (resp. **automorphism**) of E.

Thus if E is endowed with $*$ only, then an endomorphism of E is every mapping $f : E\longrightarrow E$, satisfying $f(x*y) = f(x)*f(y)$, $\forall x,y\in E$ and if E is endowed with another law $\perp$, then f also satisfies the condition $f(x\perp y) = f(x)\perp f(y)$, $\forall x,y\in E$.

4.4.2. If $f : E\longrightarrow F$ and $g : F\longrightarrow G$ are two magma homomorphism of $(E,*)$ to (F,T) and of (F,T) to (G,S) respectively, then $g\circ f$ is a magma homomorphism of $(E,*)$ to (G,S).

Proof: Let $x,y\in E$. Then

$$g\circ f(x*y) = g(f(x*y)) = g[f(x)Tf(y)] = g(f(x))Sg(f(y)) = g\circ f(x)Sg\circ f(y),$$

and so $g\circ f$ is a magma homomorphism of $(E,*)$ to (G,S). ■

4.4.3. If $f : E\longrightarrow F$ is a magma isomorphism of $(E,*)$ onto (F,T), then f^{-1} is a magma isomorphism of (F,T) onto $(E,*)$.

Proof: Since f is bijective, so is f^{-1}, by 2.5.4. Let $x,y\in F$. We have $f(f^{-1}(z)) = z$, for all $z\in F$, hence $f(f^{-1}(xTy)) = xTy = f(f^{-1}(x))Tf(f^{-1}(y)) = f[f^{-1}(x)*f^{-1}(y)]$. But f is injective, whence $f^{-1}(xTy) = f^{-1}(x)*f^{-1}(y)$, and so f^{-1} is a magma homomorphism. Therefore f^{-1} is a magma isomorphism. ■

Definition 17. We say that E is isomorphic to F and we write E≅F (read: " E isomorphic to F") if there exists a magma isomorphism of E onto F. ■

4.4.4. The following hold
(i) E≅E.
(ii) If E≅F, then F≅E.
(iii) If (G,⊥) is a magma and E≅F and F≅G, then E≅G.

Proof: (i) As id_E is a magma isomorphism of E onto E, then E≅E.

(ii) We have E≅F, hence there exists a magma isomorphism $f : E \longrightarrow F$. Since f^{-1} is a magma isomorphism of F onto E, by 4.4.3, we then get that F≅ E.

(iii) We have E≅F and F≅G, hence there exist two magma isomorphisms $f : E \longrightarrow F$ and $g : F \longrightarrow G$. Since $g \circ f$ is a bijective homomorphism of E onto G, by 2.4.3(i) and 4.4.2, we then get that $g \circ f$ is a magma isomorphism, and so E≅G. ■

M1100

CHAPTER IV

EXERCISES

1- In each of the following cases check if the binary operation $*$ is associative or commutative or has a neutral element and if there are invertible elements for $*$:

(i) E= $\mathbb{N}$ and $x*y=\begin{cases} x^y & \text{if } x \neq 0 \text{ or } y \neq 0 \\ 0 & \text{if } x = 0 \text{ and } y = 0 \end{cases}$.

(ii) E= $\mathbb{R}^+$ and $x*y=\sqrt{x^2+y^2}$.

(iii) E= $\mathbb{R}^+$ and $x*y=\sqrt{x+y}$.

2- Find the real numbers a and b for the binary operation T, defined on $\mathbb{R}$ by $xTy = ax+by$ is associative.

3- Let $*$ be a binary operation on E and let $a\in E$. Show that if $*$ is associative, then so is the binary operation T, defined on E by $xTy = x*a*y$.

4- Examine if each of the following magmas has a neutral element or not :

$(\mathbb{Z},\times)$, $(2\mathbb{Z},\times)$, $(P(E),\cup)$, $(P(E),\cap)$, $(\mathbb{N}^*,T)$

where $aTb = \gcd(a,b)$, $\forall a,b\in \mathbb{N}^*$.

5- Let E=]-1 , 1[. For every $x,y\in E$, let $x*y = \dfrac{x+y}{1+xy}$.

1- Show that $1+xy>0$, for all $x,y\in E$ and deduce that $*$ is a binary operation on E.

2- Show that $(E, *)$ is a monoid with identity e that should be determined.

3- Show that every element x of E is invertible for $*$ and find its inverse x'.

6- Let $*$ be the binary operation defined on $\mathbb{Z}$ by $x*y=x+y+xy$.

1- Show that $(\mathbb{Z},*)$ is a commutative monoid.

2- Are the elements 1 and 3 invertible for $*$?

3- Does $(\mathbb{Z},*)$ have invertible elements ?

4- Give an example showing that $*$ is not distributive over the addition of $\mathbb{Z}$.

5- Show that the mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, defined by $f(x)=x+1$, is a magma isomorphism of $(\mathbb{Z},*)$ onto $(\mathbb{Z},\times)$.

7- Let A be a subset of a set E and let $G=\{X\in P(E) ; A\subseteq X\}$.

1-Show that G is closed under $\cup$ and $\cap$.

2- Check if each of the induced laws by $\cup$ and $\cap$ on G, has a neutral element or not.

8- Let $(E, *)$ be a magma and suppose that $*$ is associative. Let $a,b\in E$.

1- Show that if γ_a is surjective and $\gamma_b(a)=a$, then b is neutral on the left for $*$.

2- Show that if δ_a is surjective and $\delta_b(a)=a$, then b is neutral on the right for $*$.

3- Deduce that if γ_a and δ_a are surjective, then (E, $*$) is a monoid.

4- Show that if γ_u and δ_u are surjective, for all $u \in E$, then every element x of E is invertible, for $*$.

9- Let (E, $*$) be a magma and suppose that $*$ is associative. Let $e \in E$ be a neutral element on the right, for $*$.

1- Show that e is an idempotent element of E.

2- Show that the left translation by e is an endomorphism of (E, $*$).

3- Let $A=\{y \in E \ ; \exists x \in E$, such that $y=e*x\}$.

(i) Show that A is closed under $*$.

(ii) Show that e is a neutral element of (A, $*_A$).

M1100

CHAPTER V

GROUP RING AND FIELD

§ 5.1. GROUP.

Definition 1. A non-empty set G is said to be a **group** if G is endowed with a binary operation $*$ satisfying the following conditions:

(i) $*$ is associative,

(ii) $*$ has a neutral element in G,

(iii) every element of G is invertible for $*$. ■

If G is a group whose binary operation is denoted $*$, then we say that G is a group under $*$. We also say that $(G,*)$ is a group.

Definition 2. Let $(G,*)$ be a group. We say that

(i) G is **abelian** (or **commutative**) if $*$ is commutative.

(ii) G is **multiplicative** (resp. **additive**) if $*$ is multiplicative (resp. additive). ■

Examples: 1) If E = $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$), then (E,+) is a commutative group.

2) If E = $\mathbb{Q}$ (or $\mathbb{R}$), then $(E^*,\times)$, where E^*= E-{0}, is an abelian group, while $(\mathbb{Z}^*,\times)$ is not a group, as the element 2 of $\mathbb{Z}^*$ is not invertible for ×.

3) If E is a non-empty set, then the set of all bijections of E onto E is a group under the usual composition of mappings. This group is called the **symmetric group** of E and denoted Sym(E). If E={1,2,…,n}, then Sym(E) is denoted S_n and called **the symmetric group of degree n**.

For the rest of this chapter let G be a multiplicative group. Let e be the neutral element of G and for each x in G let x^{-1} denote the inverse of x in G.

Remark: All results can be applied to additive groups by simply replacing xy by x+y and x^{-1} by -x, for every $x,y\in G$.

5.1.1. The following hold

(i) The neutral element e of G is unique.

(ii) If $x\in G$, then x is invertible and its inverse x^{-1} is unique in G and $(x^{-1})^{-1} = x$.

(iii) Every element of G is regular.

Proof: (i) By 4.2.1.1.

(ii) By 4.2.4 and 4.2.5(i).

(iii) Let $x\in G$. Since x is invertible, it is regular, by 4.2.6(ii). ■

Definition 3. A subset H of G is said to be a **subgroup** of G if $(H,\times_H)$ is a group, where $\times_H$ is the law induced by the multiplication of G on H. ■

Example: {e} and G are two subgroups of G, called **the trivial subgroups** of G.

5.1.2. If H is a subgroup of G, then $e\in H$ and e is the neutral element of $(H,\times_H)$.

Proof: We have $(H,\times_H)$ is a group, hence $\times_H$ has a neutral element e' in H. We have

$$e'e = e' = e'\times_H e' = e'e'$$

and e' is regular in G, by 5.1.1(iii), hence e'=e. Therefore $e\in H$ and e is the neutral element of $(H,\times_H)$. ■

5.1.3. If H is a subset of G, then the following are equivalent

(a) H is a subgroup;

(b) $H\neq\emptyset$, $xy\in H$, $\forall x,y\in H$, and $x^{-1}\in H$, $\forall x\in H$.

(c) $H\neq\emptyset$ and $xy^{-1}\in H$, $\forall x,y\in H$.

Proof: (a)⇒(b): Since H is a group, $H\neq\emptyset$. Let $x,y\in H$. We have $xy=x\times_H y$ and $(H,\times_H)$ is a group, hence $xy\in H$. By 5.1.2, we have $e\in H$ and

e is the neutral element of $(H,\times_H)$.

Let x' be the inverse of x in $(H,\times_H)$, then

$$xx' = x\times_H x' = e \text{ and } x'x = x'\times_H x = e$$

and so $x' = x^{-1}$, by 4.2.4, whence $x^{-1}\in H$. Therefore (b) holds.

(b)⇒(c): Let $x,y\in H$. As $y^{-1}\in H$, then $xy^{-1}\in H$, and so (c) holds.

(c)⇒(a): Since $H\neq\emptyset$, $\exists x\in H$. We have $xx^{-1}\in H$, and so

$$e\in H.$$

Let $x,y\in H$. As $e\in H$, then $ey^{-1}\in H$, and so $y^{-1}\in H$. This implies that $x(y^{-1})^{-1}\in H$, hence $xy\in H$, and so H is closed under the multiplication of G. But the multiplication of G is associative and $e\in H$, hence $\times_H$ is associative and has e as neutral element, by 4.3.2. Let $x\in H$. As $e\in H$, then $ex^{-1}\in H$, and so $x^{-1}\in H$. However $x\times_H x^{-1}=xx^{-1}=e$ and $x^{-1}\times_H x = x^{-1}x = e$. Therefore x is invertible for $\times_H$, and so $(H,\times_H)$ is a group, whence H is a subgroup of G. ■

5.1.4. If $(H_i)_{i\in I}$ is a family of subgroups of G, then so is $\bigcap_{i\in I} H_i$.

Proof: Since H_i is a subgroup of G, $e\in H_i$, for all $i\in I$, and so $e\in\bigcap_{i\in I} H_i$, whence $\bigcap_{i\in I} H_i\neq\emptyset$. Let $x,y\in\bigcap_{i\in I} H_i$. Then $x,y\in H_i$, $\forall i\in I$, and so $xy^{-1}\in H_i$, $\forall i\in I$, by 5.1.3, whence $xy^{-1}\in\bigcap_{i\in I} H_i$. Therefore $\bigcap_{i\in I} H_i$ is a subgroup of G, by 5.1.3. ■

In the rest of this section let (G_1,T) be a group with neutral element e_1. For each $x\in G_1$, let x’ be the inverse of x for T.

Definition 4. We call **homomorphism** (resp. **isomorphism**) **of groups** of G to G_1, every magma homomorphism (resp. isomorphism) of $(G,\times)$ to (G_1,T). ■

A homomorphism (resp. isomorphism) of groups is also called a **group**

homomorphism (resp. **group isomorphism**).

We call **endomorphism** (resp. **automorphism**) of G, every homomorphism (resp. isomorphism) of G to G.

5.1.5. The following hold

(i) If G_2 is a group and $f : G \longrightarrow G_1$ and $g : G_1 \longrightarrow G_2$ are two group homomorphisms, then so is $g \circ f$.

(ii) If $f : G \longrightarrow G_1$ is a group isomorphism, then so is f^{-1}.

Proof: By 4.4.2 and 4.4.3. ■

Definition 5. The groups G and G_1 are said to be **isomorphic** and we write $G \cong G_1$ if there exists a group isomorphism of G onto G_1. ■

Thus the two groups G and G_1 are isomorphic if and only if the magmas $(G,\times)$ and (G_1,T) are isomorphic.

5.1.6. The following hold
(i) $G \cong G$.
(ii) If $G \cong G_1$, then $G_1 \cong G$.
(iii) If G_2 is a group and $G \cong G_1$ and $G_1 \cong G_2$, then $G \cong G_2$.

Proof: By 4.4.4. ■

Definition 6. Let $f : G \longrightarrow G_1$ be a group homomorphism. We define **the kernel** of f, written Ker(f), to be the set $\mathrm{Ker}(f) = \{x \in G \,;\, f(x) = e_1\}$. ■

Thus $\mathrm{Ker}(f) = f^{-1}(\{e_1\})$ and $x \in \mathrm{Ker}(f) \Leftrightarrow x \in G$ and $f(x) = e_1$.

5.1.7. If $f : G \longrightarrow G_1$ is a group homomorphism, then
(i) $f(e) = e_1$.
(ii) $f(x^{-1}) = (f(x))'$, $\forall x \in G$, where $(f(x))'$ is the inverse of f(x) in (G_1,T).
(iii) If H is a subgroup of G, then f(H) is a subgroup of G_1.
(iv) If H is a subgroup of G_1, then $f^{-1}(H)$ is a subgroup of G.

Proof: (i) We have $f(e)Te_1 = f(e) = f(ee) = f(e)Tf(e)$, and f(e) is regular for T, by 5.1.1(iii), hence $f(e) = e_1$.

(ii) We have $f(x)Tf(x^{-1}) = f(xx^{-1}) = f(e) = e_1$ and $f(x^{-1})Tf(x) = f(x^{-1}x) = f(e) = e_1$, by (i), hence $f(x^{-1}) = (f(x))'$, by 4.2.4.

(iii) Since $e \in H$, $f(e) \in f(H)$, and so $f(H) \neq \emptyset$. Let $x,y \in f(H)$. Then $\exists u,v \in H$, such that $x = f(u)$ and $y = f(v)$. We have $xTy' = f(u)T(f(v))' = f(u)Tf(v^{-1}) = f(uv^{-1})$ and $uv^{-1} \in H$, hence $xTy' \in f(H)$, and so f(H) is a subgroup of G_1, by 5.1.3.

(iv) We have $e_1 \in H$ and $f(e)=e_1$, hence $e \in f^{-1}(H)$, and so $f^{-1}(H) \neq \varnothing$. Let $x,y \in f^{-1}(H)$, then $f(x),f(y) \in H$. As H is a subgroup of G_1, then $f(x)T(f(y))' \in H$. But

$$f(x)T(f(y))' = f(x)Tf(y^{-1}) = f(xy^{-1})$$

hence $f(xy^{-1}) \in H$, and so $xy^{-1} \in f^{-1}(H)$, whence $f^{-1}(H)$ is a subgroup of G. ■

Corollary 5.1.7.1. If $f : G \longrightarrow G_1$ is a group homomorphism, then
(i) Im(f) is a subgroup of G_1.
(ii) Ker(f) is a subgroup of G.

Proof: (i) We have Im(f) = f(G) and G is a subgroup of G, hence Im(f) is a subgroup of G_1, by 5.1.7(iii).

(ii) As $\{e_1\}$ is a subgroup of G_1 and $Ker(f)=f^{-1}(\{e_1\})$, then Ker(f) is a subgroup of G, by 5.1.7(iv). ■

5.1.8. A group homomorphism $f : G \longrightarrow G_1$ is injective if and only if Ker(f) = {e}.

Proof: **N.C:** We have that

$$x \in Ker(f) \Leftrightarrow f(x) = e_1 \Leftrightarrow f(x) = f(e) \Leftrightarrow x = e \Leftrightarrow x \in \{e\}$$

hence Ker(f) = {e}.
S.C: Let $x,y \in G$. Then

$$f(x) = f(y) \Rightarrow f(x)T(f(y))' = e_1 \Rightarrow f(x)Tf(y^{-1}) = e_1 \Rightarrow f(xy^{-1}) = e_1 \Rightarrow xy^{-1} \in Ker(f)$$
$$\Rightarrow xy^{-1} \in \{e\} \Rightarrow xy^{-1} = e \Rightarrow x = y$$

and so f is injective. ■

§ 5.2. RING AND FIELD.

Definition 7. A non-empty set A is said to be **a ring** if there are defined in A an addition and a multiplication satisfying:
(i) (A,+) is an abelian group,
(ii) the multiplication is associative and distributive over the addition. ■

Examples: If E = $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$), then E, endowed with the usual addition and multiplication of numbers, is a ring.

Remark: If A is a ring, we also say that (A,+,×) is a ring and conversely.

Definition 8. Let A be a ring. We say that
(i) A is **a commutative ring** if the multiplication of A is commutative.
(ii) A is **a unitary ring** or that A is **a ring with identity** provided that the multiplication of A has a neutral element in A. ■

In the rest of this section let A be a ring. We denote by 0_A the neutral element of the addition of A and by -x the inverse for the addition of every element x of A. 0_A is called the **zero** of A and -x is called the **opposite** of x. If A is unitary, then the neutral element of the multiplication of A is denoted 1_A and called the **identity** (or **unit**) **element** of A. If $a,b \in A$, we write a-b for a+(-b).

Definition 9. We define a **subring** of A to be every subset B of A satisfying:
(i) B is a subgroup of (A,+),
(ii) B is closed under the multiplication of A, i.e $ab\in B$, $\forall a,b\in B$. ■

5.2.1. A subset B of A is a subring of A if and only if
(i) $B\neq\emptyset$
(ii) $x-y\in B$ and $xy\in B$, for all $x,y\in B$.

Proof: The proof is very easy. ■

Examples: 1) $\{0_A\}$ and A are two subrings of A.
2) For each $x\in A$, the sets $xA = \{xa ; a\in A\}$ and $Ax = \{ax ; a\in A\}$ are two subrings of A.

Definition 10. A non-empty set K is said to be **a field** if there are defined in K an addition and a multiplication satisfying:
(i) K is a unitary commutative ring with $1_K \neq 0_K$,
(ii) every element of $K-\{0_K\}$ is invertible for the multiplication of K. ■

Examples: The sets $\mathbb{Q}$ and $\mathbb{R}$, endowed with the usual addition and multiplication of numbers, are fields, while the set $\mathbb{Z}$ is not a field under these two laws.

5.2.2. K is a field if and only if K is endowed with an addition and a multiplication, such that
(i) (K,+) is an abelian group;
(ii) $(K^*,\times)$ is an abelian group, with $K^* = K-\{0_K\}$;
(iii) × is distributive over +.

Proof: The proof is very easy. ■

5.2.3. If K is a field, then
(i) If $a\in K^*$ and $b\in K^*$, then $ab\in K^*$ and $(ab)^{-1} = b^{-1}a^{-1}$.
(ii) If $a,b\in K$ and $ab=0_K$, then $a=0_K$ or $b=0_K$.
(iii) If $a\in K^*$, then $a^{-1}\in K^*$ and $(a^{-1})^{-1}=a$.

Proof: (i) As K^* is a group for the multiplication, then $ab\in K^*$ and $(ab)^{-1} = b^{-1}a^{-1}$.
(ii) Suppose that $a\neq 0_K$ and $b\neq 0_K$. Then $a\in K^*$ and $b\in K^*$, and so $ab\in K^*$, by (i), whence $ab\neq 0_K$, a contradiction. Therefore $a=0_K$ or $b=0_K$.
(iii) As K^* is a multiplicative group, then $a^{-1}\in K^*$ and $(a^{-1})^{-1}=a$. ■

Definition 11. Let K be a field. A subset F of K is said to be a **subfield** of K if $(F,+_F,\times_F)$ is a field. ■

5.2.4. If F is a subfield of K, then $0_F = 0_K$ and $1_F = 1_K$.

Proof: As $(F,+_F)$ is a group, by 5.2.2(i), then F is a subgroup of (K,+), hence $0_K \in F$ and 0_K is the neutral element of $(F,+_F)$, by 5.1.2, whence $0_F = 0_K$, by 5.1.1(i).

Also as (F^*,$\times_F$) is a group, by 5.2.2(ii), then F^* is a subgroup of (K^*,$\times$), hence $1_K \in F^*$ and 1_K is the neutral element of (F^*,$\times_F$), whence $1_F = 1_K$. ■

<u>5.2.5.</u> Let K be a field. Then a subset F of K is a subfield of K if and only if
(i) $1_K \in$F,
(ii) x-y$\in$F and $xy^{-1} \in$F, for all x,y$\in$F, with y$\neq 0_K$.

<u>Proof:</u> **<u>N.C:</u>** (i) By 5.2.4.

(ii) Let x,y$\in$F, with y$\neq 0_K$. As (F,$+_F$) is a group, then x-y$\in$F. If x=0_K, then $xy^{-1}=0_K$, and so $xy^{-1} \in$F in this case. If x$\neq 0_K$, then x,y$\in F^*$, and so as (F^*,$\times_F$) is a group, we get $xy^{-1} \in F^*$, whence $xy^{-1} \in$F. Therefore (ii) holds.

<u>S.C:</u> As $1_K \in$F, then F$\neq\varnothing$. Let x,y$\in$F. If y=0_K, then x-y=x$\in$F and if y$\neq 0_K$, then x-y$\in$F, and so x-y$\in$F, for all x,y$\in$F, whence F is a subgroup of (K,+), and so

(F,$+_F$) is a group.

We have $1_K \in F^*$, hence $F^* \neq\varnothing$. Let x,y$\in F^*$, then x,y$\in$F and y$\neq 0_K$, and so $xy^{-1} \in$F. But x$\neq 0_K$ and $y^{-1}\neq 0_K$, hence $xy^{-1}\neq 0_K$, by 5.2.3(ii), and so $xy^{-1} \in F^*$. Therefore F^* is a subgroup of (K^*,$\times$), and so (F^*,$\times_F$) is a group. We have + and × are commutative, hence $+_F$ and $\times_F$ are commutative, by 4.3.2(i), and so

(F,$+_F$) and (F^*,$\times$) are abelian groups.

As × is distributive over +, then $\times_F$ is distributive over $+_F$, by 4.3.3(ii), and so (F,$+_F$,$\times_F$) is a field, by 5.2.2, whence F is a subfield of K. ■

CHAPTER V

EXERCISES

1- Show that $\mathbb{Z}$ is a group for be the binary operation $*$ defined by $x*y = x+y+1$.

2- Show that if E is a non-empty set, then

(i) $(P(E), \cap)$ and $(P(E), \cup)$ are not groups,

(ii) $(P(E), \Delta)$ is an abelian group, where $X\Delta Y=(X-Y)\cup(Y-X)$, $\forall X,Y\in P(E)$.

3- Let $G = \mathbb{R}^*\times\mathbb{R}$ and let $*$ be the law defined on G by

$$(a,b)*(c,d) = (ac , ad+b).$$

1- Show that $(G,*)$ is a group.

2- Is $(G,*)$ abelian? Justify your answer.

3- Show that $H=\{(a,0) ; a\in\mathbb{R}^*\}$ is a subgroup of $(G, *)$.

4- Show that if G is a multiplicative group, such that $x^2 = e$, $\forall x\in G$, then G is abelian.

5- Let E be a non-empty set. Show that if $a\in E$, then the set

$$H = \{f\in Sym(E) ; f(a) = a\}$$

is a subgroup of $(Sym(E),\circ)$.

6- Let G be a multiplicative group. For each $x,a\in G$, let $x^a = a^{-1}xa$ and let

$$H^a =\{ h^a ; h\in H\}.$$

Show that if H is a subgroup of G and if $a\in G$, then H^a is a subgroup of G.

7- Let A be a ring and E a non-empty set. Let $M=A^E$. For every $f,g\in M$, we define

$f+g : E\longrightarrow A$ and $fg : E\longrightarrow A$ by :

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

1- Show that M is a ring for the above addition and multiplication, such that 0_M is the zero mapping, i.e $0_M : E\longrightarrow A$ is defined by $0_M(x)=0_A$, $\forall x\in E$ and if $f\in M$, then $-f : E\longrightarrow A$ is defined by $(-f)(x)=-f(x)$, $\forall x\in E$.

2- Show that if A is commutative, then so is M.

3- Prove that if A is unitary, then M is unitary and $1_M : E\longrightarrow A$ is the mapping defined by $1_M(x)=1_A$, $\forall x\in E$.

4- Show that if $a\in E$, then the set $B = \{f\in M ; f(a) = 0_A\}$ is a subring of M.

8- Show that if A is a ring, then

(i) $\{0_A\}$ and A are two subrings of A.

(ii) if $x\in A$, the sets $xA=\{xa ; a\in A\}$ and $Ax =\{ax ; a\in A\}$ are subrings of A.

M1100

CHAPTER VI

COMPLEX NUMBERS

§ 6.1. FIELD OF COMPLEX NUMBERS.

Let K=$\mathbb{R}\times\mathbb{R}$. We define in K an addition and a multiplication as follows:

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

6.1.1. The set K is a field under the above addition and multiplication, such that

(i) $0_K = (0,0)$; (ii) $1_K = (1,0)$; (iii) $-(a,b) = (-a,-b), \forall(a,b)\in K$;

(iv) if $(a,b)\in K-\{0_K\}$, then $(a,b)^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$.

Proof: The proof is given in Appendix I. ■

6.1.2. Let

$$K' = \{(a,0) ; a\in\mathbb{R}\}.$$

Then K' is a subfield of K and the mapping $f : \mathbb{R}\longrightarrow K'$ defined by f(a)=(a,0) is an isomorphism of ($\mathbb{R}$,+, ×) onto (K',+, ×). In particular $\mathbb{R}$ and K' are isomorphic.

Proof: Since $1_K=(1,0)$, $1_K\in K'$. Let $u,v\in K'$, with $v\neq 0_K$. Then $\exists a,b\in\mathbb{R}$, such that u=(a,0) and v=(b,0). We have $v^{-1} = (\frac{1}{b},0)$ and

$$u-v = (a,0)-(b,0) = (a,0)+(-b,0) = (a+(-b),0+0) = (a-b,0)$$

and

$$uv^{-1} = (a,0)(\frac{1}{b},0) = (a\times\frac{1}{b}-0\times0, a\times0+0\times\frac{1}{b}) = (\frac{a}{b},0)$$

hence $u-v\in K'$ and $uv^{-1}\in K'$, and so K' is a subfield of K, by 5.2.5.

f homomorphism: $\forall a,b\in\mathbb{R}$, we have

$$f(a)+f(b) = (a,0)+(b,0) = (a+b,0+0) = (a+b,0) = f(a+b)$$

and

$$f(a)f(b) = (a,0)(b,0) = (a\times b-0\times0, a\times0+b\times0) = (ab,0) = f(ab)$$

hence f is a homomorphism of ($\mathbb{R}$,+, ×) to (K',+, ×).

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

$$f(a) = f(b) \Rightarrow (a,0) = (b,0) \Rightarrow a = b$$

and so f is injective.

f surjective: Let $y\in K'$. Then $\exists a\in\mathbb{R}$, such that y = (a,0) = f(a), and so f is surjective.

Therefore f is an isomorphism, and so $\mathbb{R}$ and K' are isomorphic. ■

Remark: Since the mapping $f : \mathbb{R}\longrightarrow K'$, defined by f(a)=(a,0), is an isomorphism of $\mathbb{R}$onto K', by 6.1.2, we identify every element of $\mathbb{R}$ with its image by f. Thus; we regard $\mathbb{R}$ as a subfield of K and $\forall a\in\mathbb{R}$, we can write a = (a,0).

6.1.3. Let i = (0,1). Then we have

(i) $i^2 = -1$.

(ii) $(x,y) = x+iy$, $\forall x,y\in \mathbb{R}$.

(iii) Every element z of K is uniquely written in the form $z = a+ib$, where $a,b\in \mathbb{R}$, i.e $\forall z\in K$, $\exists a,b\in\mathbb{R}$, such that $z = a+ib$ and if $z = a'+ib'$, where $a',b'\in\mathbb{R}$, then $a=a'$ and $b=b'$.

(iv) If $z = a+ib$ and $z' = a'+ib'$, then $z+z' = (a+a')+i(b+b')$ and $zz' = (aa'-bb')+i(ab'+a'b)$.

(v) If $z = a+ib$ and $z\neq 0$, then $z^{-1} = (\frac{a}{a^2+b^2})+i(\frac{-b}{a^2+b^2})$.

Proof: (i) We have $i^2 = (0,1)(0,1) = (0\times 0-1\times 1, 0\times 1+1\times 0) = (-1,0) = -1$.

(ii) $x+iy = (x,0)+(0,1)(y,0) = (x,0)+(0\times y-1\times 0, 0\times 0+1\times y) = (x,0)+(0,y) = (x+0,0+y) = (x,y)$.

(iii) Let $z\in K$. Then $\exists a,b\in\mathbb{R}$, such that $z=(a,b)$, and so $z=a+ib$, by (ii). Suppose $z=a'+ib'$, with $a',b'\in\mathbb{R}$. Then $z=(a',b')$, by (ii), and so $(a,b)=(a',b')$, whence $a=a'$ and $b=b'$.

(iv) By (ii), we have $z=(a,b)$ and $z'=(a',b')$, so that

$$z+z' = (a,b)+(a',b') = (a+a' , b+b') = (a+a')+i(b+b')$$

and

$$zz' = (a,b)(a',b') = (aa'-bb' , ab'+a'b) = (aa'-bb')+i(ab'+a'b).$$

(v) We have $z=(a,b)$, hence $z^{-1}=(a,b)^{-1} =(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})=(\frac{a}{a^2+b^2})+i(\frac{-b}{a^2+b^2})$. ■

If $z\neq 0$, then z^{-1} is denoted $\frac{1}{z}$. Thus if $z = a+ib$ and $z\neq 0$, then

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

Every element of the field K is called a **complex number** and the field K is called the **field of complex numbers** and denoted by the symbol $\mathbb{C}$.

Let $z\in\mathbb{C}$ and let $a,b\in\mathbb{R}$, such that $z = a+ib$. Then this writing of z is called the **algebraic form** of z, a is called the **real part** of z and is written R(z) and b is called the **imaginary part** of z and is denoted I(z). Thus

$$z = R(z)+iI(z).$$

Definition 1. Let $z\in\mathbb{C}$. We say that

(i) z is **real** if $I(z) = 0$.

(ii) z is **pure imaginary** if $R(z) = 0$. ■

Thus the set of the pure imaginary complex numbers is $i\mathbb{R}= \{ix ; x\in \mathbb{R}\}$.

§ 6.2. CONJUGATE OF A COMPLEX NUMBER.

Definition 2. Let $z\in\mathbb{C}$ and let $a,b\in\mathbb{R}$, such that $z = a+ib$. We define the **conjugate** of z, written $\overline{z}$ to be $\overline{z} = a-ib$. ■

6.2.1. The following hold, for all $z,z'\in\mathbb{C}$

(i) $\overline{z} = 0 \Leftrightarrow z = 0$,

(ii) $\overline{z+z'} = \overline{z}+\overline{z'}$,

(iii) $\overline{zz'} = \overline{z}\,\overline{z'}$,

(iv) if $z'\neq 0$ and $u = \frac{z}{z'}$, then $\overline{u} = \frac{\overline{z}}{\overline{z'}}$,

(v) $\bar{\bar{z}} = z$,
(vi) $R(z) = R(\bar{z})$ and $I(z) = -I(\bar{z})$,
(vii) $R(z) = \frac{z+\bar{z}}{2}$ and $I(z) = \frac{z-\bar{z}}{2i}$,
(viii) z is real if and only if $\bar{z} = z$,
(ix) z is pure imaginary if and only if $\bar{z} = -z$.

Proof: Let $z,z' \in \mathbb{C}$. Then $\exists a,b,c,d \in \mathbb{R}$, such that $z = a+ib$ and $z' = c+id$, and so

$$\bar{z} = a-ib \text{ and } \overline{z'} = c-id.$$

(i) $\bar{z}=0 \Leftrightarrow a-ib=0 \Leftrightarrow a+i(-b)=0 \Leftrightarrow a=-b=0 \Leftrightarrow a=b=0 \Leftrightarrow z = 0$.

(ii) As $z+z' = (a+c)+i(b+d)$, then $\overline{z+z'} = (a+c)-i(b+d) = (a-ib)+(c-id) = \bar{z}+\overline{z'}$.

(iii) As $zz' = (ac-bd)+i(ad+bc)$, then $\overline{zz'} = (ac-bd)-i(ad+bc)$, and so

$$\bar{z}\,\overline{z'} = (a-ib)(c-id) = a(c-id)-ib(c-id) = ac-iad-ibc+i^2bd = ac-iad-ibc-bd$$
$$= (ac-bd)-i(ad+bc) = \overline{zz'}.$$

(iv) We have $z=uz'$, hence $\bar{z} = \overline{uz'} = \bar{u}\,\overline{z'}$, by (iii). But $z' \neq 0$, hence $\overline{z'} \neq 0$, by (i), and so $\bar{u} = \frac{\bar{z}}{\overline{z'}}$.

(v) We have $\bar{z} = a-ib = a+i(-b)$, hence $\bar{\bar{z}} = a-i(-b) = a+ib = z$.

(vi) As $z = a+ib$ and $\bar{z} = a-ib = a+i(-b)$, then $R(z) = a = R(\bar{z})$ and $I(z) = b = -(-b) = -I(\bar{z})$.

(vii) $\frac{z+\bar{z}}{2} = \frac{a+ib+a-ib}{2} = \frac{2a}{2} = a = R(z)$ and $\frac{z-\bar{z}}{2i} = \frac{a+ib-(a-ib)}{2i} = \frac{a+ib-a+ib}{2i} = \frac{2ib}{2i} = b = I(z)$.

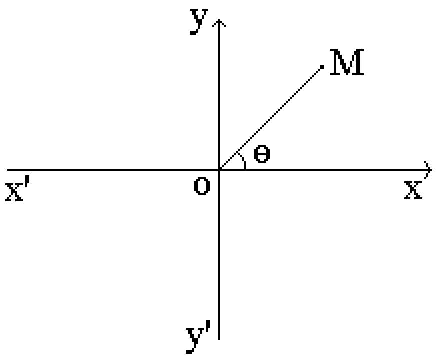
(viii) Using (vii), we have z is real $\Leftrightarrow I(z)=0 \Leftrightarrow \frac{z-\bar{z}}{2i}=0 \Leftrightarrow z-\bar{z}=0 \Leftrightarrow \bar{z} = z$.

(ix) Also using (vii), we get

$$z \text{ is pure imaginary} \Leftrightarrow R(z)=0 \Leftrightarrow \frac{z+\bar{z}}{2}=0 \Leftrightarrow z+\bar{z}=0 \Leftrightarrow \bar{z}=-z. \blacksquare$$

§ 6.3. TRIGONOMETRIC FORM OF A COMPLEX NUMBER.

Assume that there is an orthonormal system Oxy in the plane (P).



If $z = a+ib$ is a complex number, then the point M(a,b) of (P) is called **the image** of z in (P) and z is called the **affix** of M and denoted affix(M). We also say that the vector $\vec{u}$ (a,b) is the image of z in the plane and z is called the affix of $\vec{u}$.

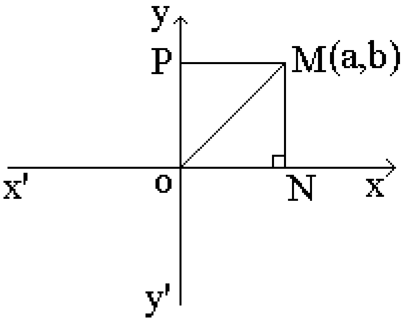
If the affix of every point M is denoted z_M, then the affix of the vector $\overrightarrow{AB}$ is $z_B - z_A$.

Notice that the y-axis is the set of pure imaginary complex numbers and the x-axis is the set of real complex numbers, thus the y-axis is called the **imaginary axis** and the x-axis is called the **real axis**. The plane (P) will be refered to as the **complex plane** (or **the plane of complex numbers**).

Definition 3. Let $z \in \mathbb{C}$ and let M be the image of z in (P). We define the **module** (or **modulus**) of z, denoted $|z|$, to be the length of the line segment OM and if $z \neq 0$, we define the **argument** of z, denoted arg(z), to be the angle θ of $\overset{\rightarrow}{OX}$ and $\overset{\rightarrow}{OM}$. ■

6.3.1. Let $z \in \mathbb{C}$ and let $a,b \in \mathbb{R}$, such that $z = a+ib$. Then $|z|^2 = z\bar{z} = a^2+b^2$.

Proof: Let M(a,b) be the image of z in the plane (P) and let N and P be the orthogonal projections of M on x'ox and y'oy respectively.



Then $\overline{ON} = a$ and $\overline{NM} = b$. Since the triangle ONM is right angled at N, we then have

$$\overline{OM}^2 = \overline{ON}^2 + \overline{NM}^2 = a^2+b^2$$

hence

$$|z|^2 = a^2+b^2.$$

On the other hand, we have that $\bar{z} = a-ib$, hence

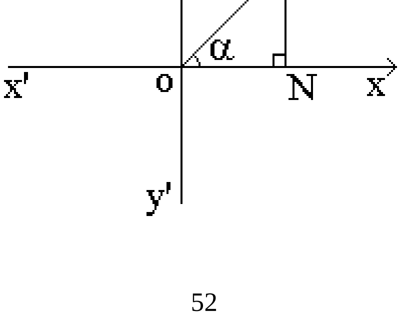
$$z\bar{z} = (a+ib)(a-ib) = a^2-i^2b^2 = a^2+b^2$$

and so $|z|^2 = z\bar{z} = a^2+b^2$. ■

6.3.2 Let $z \in \mathbb{C}$ and let $a,b \in \mathbb{R}$, such that $z = a+ib$. If $z \neq 0$ and $\alpha = \arg(z)$, then

(i) $\cos\alpha = \frac{a}{|z|}$ and $\sin\alpha = \frac{b}{|z|}$, (ii) $z = |z|(\cos\alpha + i\sin\alpha)$.

Proof: Let M(a,b) be the image of z in the plane (P) and let N and P be the orthogonal projections of M on x'ox and y'oy respectively.



Then

$$\overline{ON} = a \text{ and } \overline{NM} = b.$$

(i) The triangle ONM is right angled at N, hence

$$\cos\alpha = \frac{\overline{ON}}{OM} = \frac{a}{|z|} \text{ and } \sin\alpha = \frac{\overline{NM}}{OM} = \frac{b}{|z|}.$$

(ii) Since $a=|z|\cos\alpha$ and $b=|z|\sin\alpha$, by (i), and $z=a+ib$, we then have

$$z=|z|\cos\alpha+i|z|\sin\alpha=|z|(\cos\alpha+i\sin\alpha).$$ ■

6.3.3. If $z\in\mathbb{C}$, then $\exists r,\alpha\in\mathbb{R}$, such that $r\geq 0$ and $z = r(\cos\alpha+i\sin\alpha)$.

Proof: If $z = 0$, then $z = 0(\cos(0)+i\sin(0))$, hence we take $r=0$ and $\alpha=0$. If $z\neq 0$, then we take $r = |z|$ and $\alpha = \arg(z)$. We have that $r,\alpha\in\mathbb{R}$, $r\geq 0$ and $z = r(\cos\alpha+i\sin\alpha)$, by 6.3.2(ii). ■

6.3.4. If $z\neq 0$ and $z = r(\cos\alpha+i\sin\alpha)$ and $z = r'(\cos\alpha'+i\sin\alpha')$, where $r,\alpha,r',\alpha'\in\mathbb{R}$ and $r\geq 0$ and $r'\geq 0$, then $r = r'$ and $\exists k\in\mathbb{Z}$, such that $\alpha' = \alpha+2k\pi$.

Proof: We have that $z = (r\cos\alpha)+i(r\sin\alpha)$ and $z = (r'\cos\alpha')+i(r'\sin\alpha')$ and $r\cos\alpha$, $r\sin\alpha$, $r'\cos\alpha'$ and $r'\sin\alpha'$ are real numbers, hence

$$r\cos\alpha = r'\cos\alpha' \text{ and } r\sin\alpha = r'\sin\alpha'$$

by 6.1.3(iii). Since $\cos^2\alpha+\sin^2\alpha = \cos^2\alpha'+\sin^2\alpha' = 1$, we then get that

$$r^2 = r^2(\cos^2\alpha+\sin^2\alpha)= r^2\cos^2\alpha+r^2\sin^2\alpha=(r\cos\alpha)^2+(r\sin\alpha)^2=(r'\cos\alpha')^2+(r'\sin\alpha')^2$$
$$= r'^2\cos^2\alpha'+r'^2\sin^2\alpha' = r'^2(\cos^2\alpha'+\sin^2\alpha') = r'^2.$$

But $r\geq 0$ and $r'\geq 0$, hence $r = r'$. This implies that $r\cos\alpha = r\cos\alpha'$ and $r\sin\alpha = r\sin\alpha'$, and as $z\neq 0$ and $z = r(\cos\alpha+i\sin\alpha)$, then $r\neq 0$, and so $\cos\alpha = \cos\alpha'$ and $\sin\alpha = \sin\alpha'$, whence $\exists k\in\mathbb{Z}$, such that $\alpha' = \alpha+2k\pi$. ■

Corollary 6.3.4.1. If $z\neq 0$ and $z = r(\cos\alpha+i\sin\alpha)$, where $r,\alpha\in\mathbb{R}$ and $r\geq 0$, then

$$|z| = r \text{ and } \exists k\in\mathbb{Z}, \text{ such that } \arg(z) = \alpha+2k\pi.$$

Proof: Let $\alpha' = \arg(z)$. Then $z = |z|(\cos\alpha'+i\sin\alpha')$, by 6.3.2(ii), and so $|z| = r$ and $\exists k\in\mathbb{Z}$, such that $\arg(z) = \alpha' = \alpha+2k\pi$. ■

Definition 4. We define the **trigonometric form** of a complex numbre z to be the writing of z in the form $z = r(\cos\alpha+i\sin\alpha)$, where $r,\alpha\in\mathbb{R}$ and $r\geq 0$. ■

Remark: The trigonometric form $z = r(\cos\alpha+i\sin\alpha)$ of the complex number z is usually written $[r,\alpha]$.

6.3.5. If $z=r(\cos\alpha+i\sin\alpha)$ and $z'=r'(\cos\alpha'+i\sin\alpha')$, where $r,\alpha,r',\alpha'\in\mathbb{R}$ and $r\geq 0$ and $r'\geq 0$, then

(i) $zz' = rr'[\cos(\alpha+\alpha')+i\sin(\alpha+\alpha')]$,

(ii) $\dfrac{z}{z'} = \dfrac{r}{r'}[\cos(\alpha-\alpha')+i\sin(\alpha-\alpha')]$.

Proof: (i) We have that

$$zz' = [r(\cos\alpha+i\sin\alpha)][r'(\cos\alpha'+i\sin\alpha')] = rr'[(\cos\alpha+i\sin\alpha)(\cos\alpha'+i\sin\alpha')]$$

$= rr'[(\cos\alpha\cos\alpha'-\sin\alpha\sin\alpha')+i(\cos\alpha\sin\alpha'+\cos\alpha\sin\alpha')] = rr'[\cos(\alpha+\alpha')+i\sin(\alpha+\alpha')]$.

(ii) We have that

$$\frac{z}{z'} = \frac{r(\cos\alpha+i\sin\alpha)}{r'(\cos\alpha'+i\sin\alpha')} = \frac{r}{r'}[\frac{\cos\alpha+i\sin\alpha}{\cos\alpha'+i\sin\alpha'}] = \frac{r}{r'}[\frac{(\cos\alpha+i\sin\alpha)(\cos\alpha'-i\sin\alpha')}{(\cos\alpha'+i\sin\alpha')(\cos\alpha'-i\sin\alpha')}]$$

$$= \frac{r}{r'}[\frac{(\cos\alpha\cos\alpha'+\sin\alpha\sin\alpha')+i(-\cos\alpha\sin\alpha'+\sin\alpha\cos\alpha')}{\cos^2\alpha'+\sin^2\alpha'}]$$

$$= \frac{r}{r'}[\frac{\cos(\alpha-\alpha')+i\sin(\alpha-\alpha')}{1}] = \frac{r}{r'}[\cos(\alpha-\alpha')+i\sin(\alpha-\alpha')]. \blacksquare$$

<u>Corollary 6.3.5.1.</u> If $z,z'\in\mathbb{C}$, then

(i) $|zz'| = |z|\,|z'|$ and if $zz'\neq0$, then $\exists k\in\mathbb{Z}$, such that $\arg(zz') = \arg(z)+\arg(z')+2k\pi$

(ii) $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$, and if $\frac{z}{z'}\neq0$, then $\exists k\in\mathbb{Z}$, such that $\arg(\frac{z}{z'}) = \arg(z)-\arg(z')+2k\pi$.

<u>Proof:</u> Let $\alpha = \arg(z)$ and $\alpha' = \arg(z')$ whenever $z\neq0$ and $z'\neq0$.

(i) If $zz' = 0$, then $z = 0$ or $z' = 0$, hence $|z|=0$ or $|z'|=0$, and so $|z|\,|z'| =0$ and as $|zz'| = 0$, then $|zz'|=|z|\,|z'|$ in this case. Suppose that $zz'\neq0$. Then $z\neq0$ and $z'\neq0$, and so

$$z = |z|(\cos\alpha+i\sin\alpha) \text{ and } z' = |z'|(\cos\alpha'+i\sin\alpha')$$

by 6.3.2(ii). This yields that

$$zz' = |z|\,|z'|[\cos(\alpha+\alpha')+i\sin(\alpha+\alpha')]$$

by 6.3.5(i). But $zz'\neq0$, hence 6.3.4.1 gives that

$$|zz'|=|z|\,|z'| \text{ and } \exists k\in\mathbb{Z}, \text{ such that } \arg(zz') = \alpha+\alpha'+2k\pi = \arg(z)+\arg(z')+2k\pi.$$

(ii) If $\frac{z}{z'} = 0$, then $z = 0$, hence $|z| = 0$ and as $z'\neq0$, for $\frac{z}{z'}$ is not defined for $z' = 0$, then $|z'|\neq0$, and so $\frac{|z|}{|z'|} = 0$; but $\left|\frac{z}{z'}\right| = 0$, whence $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$. Assume that $\frac{z}{z'}\neq0$, then $z\neq0$. As $z'\neq0$, then

$$z = |z|(\cos\alpha+i\sin\alpha) \text{ and } z' = |z'|(\cos\alpha'+i\sin\alpha')$$

by 6.3.2(ii), and so $\frac{z}{z'} = \frac{|z|}{|z'|}[\cos(\alpha-\alpha')+i\sin(\alpha-\alpha')]$, by 6.3.5(ii). But $\frac{z}{z'}\neq0$, hence

$$\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|} \text{ and } \exists k\in\mathbb{Z}, \text{ such that } \arg(\frac{z}{z'}) = \arg(z)-\arg(z')+2k\pi$$

by 6.3.4.1. ■

<u>6.3.6. (De Moivre's Formula).</u> For every $\alpha\in\mathbb{R}$, we have

$$(\cos\alpha+i\sin\alpha)^n = \cos(n\alpha)+i\sin(n\alpha), \text{ for all } n\in\mathbb{N}^*.$$

<u>Proof:</u> We argue by induction on n. It is true for $n = 1$, since $(\cos\alpha+i\sin\alpha)^1=\cos\alpha+i\sin\alpha$. Suppose that it holds up to n and let's show it for n+1, then

$$(\cos\alpha+i\sin\alpha)^n = \cos(n\alpha)+i\sin(n\alpha),$$

by induction hypothesis, and so

$$(\cos\alpha+i\sin\alpha)^{n+1} = (\cos\alpha+i\sin\alpha)(\cos\alpha+i\sin\alpha)^n = (\cos\alpha+i\sin\alpha)(\cos(n\alpha)+i\sin(n\alpha))$$
$$= \cos(\alpha+n\alpha)+i\sin(\alpha+n\alpha) = \cos(n+1)\alpha+i\sin(n+1)\alpha$$

by 6.3.5(i), and so the formula is true for n+1. Therefore it is true, $\forall n \in \mathbb{N}^*$. ■

This formula is important as it connects complex numbers and trigonometry. Since the multiplication in $\mathbb{C}$ is commutative, the binomial formula holds for the complex numbers, and so by applying it to $(\cos\alpha+i\sin\alpha)^n$ and then comparing the imaginary and real parts we can derive useful expressions for $\cos(n\alpha)$ and $\sin(n\alpha)$ in terms of $\cos\alpha$ and $\sin\alpha$. For example as $\cos(2\alpha)+i\sin(2\alpha) = (\cos\alpha+i\sin\alpha)^2 = (\cos^2\alpha-\sin^2\alpha)+i(2\cos\alpha\sin\alpha)$, then $\cos(2\alpha) = \cos^2\alpha-\sin^2\alpha$ and $\sin(2\alpha) = 2\cos\alpha\sin\alpha$.

Corollary 6.3.6.1. If $z\in\mathbb{C}$ and $n\in\mathbb{N}^*$, then $\left|z^n\right| = |z|^n$ and if $z^n\neq 0$, then $\exists k\in\mathbb{Z}$, such that $\arg(z^n) = n\arg(z)+2k\pi$.

Proof: If $z^n=0$, then $z = 0$, because $n\in\mathbb{N}^*$, hence $|z|=0$, and so $|z|^n=0$; but $\left|z^n\right| = 0$, hence $\left|z^n\right| = |z|^n$ in this case. Suppose that $z^n\neq 0$, then $z\neq 0$. Let $\alpha = \arg(z)$, then

$$z = |z|(\cos\alpha+i\sin\alpha)$$

by 6.3.2(ii), and so $z^n = |z|^n(\cos(n\alpha)+i\sin(n\alpha))$, by 6.3.6. But $z^n\neq 0$, hence 6.3.4.1 yields that $\left|z^n\right| = |z|^n$ and $\exists k\in\mathbb{Z}$, such that $\arg(z^n) = n\alpha+2k\pi = n\arg(z)+2k\pi$. ■

If θ is a real number, we define

$$e^{i\theta} = \cos\theta+i\sin\theta.$$

This equation is known as **Euler's equation**. Notice that if α and β are real numbers, then

$$e^{i\alpha}\, e^{i\beta} = e^{i(\alpha+\beta)} \text{ and } \frac{e^{i\alpha}}{e^{i\beta}} = e^{i(\alpha-\beta)}$$

by 6.3.5.

Thus if $z=r(\cos\alpha+i\sin\alpha)$, with $r,\alpha\in\mathbb{R}$ and $r\geq 0$, then $z=re^{i\alpha}$. This expression is called the **exponential form** of z.

§ 6.4. NTH ROOT OF A COMPLEX NUMBER.

Definition 5. Let $z\in\mathbb{C}$ and $n\in\mathbb{N}^*$. We call **nth root** of z, every complex number u satisfying $u^n = z$. ■

6.4.1. Let $z\in\mathbb{C}^*$ and let $n\in\mathbb{N}^*$and $r,\alpha\in\mathbb{R}$, such that $r\geq 0$ and

$$z = r(\cos\alpha+i\sin\alpha).$$

For each natural number t, such that $0\leq t\leq n-1$, let

$$z_t = \sqrt[n]{r}\,[\cos(\frac{\alpha+2t\pi}{n})+i\sin(\frac{\alpha+2t\pi}{n})].$$

Then $z_0, z_1,..., z_{n-1}$ are all the nth roots of z.

Proof: First, we show that each z_t is an nth root of z. We have that

$$(z_t)^n = (\sqrt[n]{r})^n [\cos[n(\frac{\alpha + 2t\pi}{n})]+i\sin[n(\frac{\alpha + 2t\pi}{n})]] = r[\cos(\alpha+2t\pi)+i\sin(\alpha+2t\pi)]$$
$$= r(\cos\alpha+i\sin\alpha) = z$$

hence z_t is an nth root of z. Let $u\in\mathbb{C}$ be an nth root of z. Then $u^n = z$. Since $z\neq0$, $u\neq0$, and so letting $\beta = \arg(u)$, we obtain $u = |u|(\cos\beta+i\sin\beta)$, by 6.3.2(ii). It follows that

$$z = u^n = |u|^n(\cos(n\beta)+i\sin(n\beta))$$

by De Moivre's formula. Using 6.3.4.1, we get that

$$|u|^n = r \text{ and } \exists k\in\mathbb{Z}\text{, such that } n\beta = \arg(z)+2k\pi = \alpha+2k\pi$$

which yields that

$$|u| = \sqrt[n]{r} \text{ and } \beta = \frac{\alpha+2k\pi}{n}.$$

Let s be the quotient and t the remainder of the division of k by n. Then

$$0\leq t\leq n\text{-}1 \text{ and } k = ns+t$$

and so $\beta = \frac{\alpha+2(ns+t)\pi}{n} = \frac{\alpha+2t\pi}{n}+2s\pi$. Therefore

$$u = \sqrt[n]{r}[\cos(\frac{\alpha+2t\pi}{n}+2s\pi)+i\sin(\frac{\alpha+2t\pi}{n}+2s\pi)] = \sqrt[n]{r}\ [\cos(\frac{\alpha+2t\pi}{n})+i\sin(\frac{\alpha+2t\pi}{n})] = z_t$$

and so z_0, z_1,..., z_{n-1} are all the nth roots of z. ■

Definition 6. We call **nth root of unity**, every nth root of z = 1. ■

Corollary 6.4.1.1. Let $n\in\mathbb{N}^*$ and $u = \cos(\frac{2\pi}{n})+i\sin(\frac{2\pi}{n})$. Then 1, u,....., u^{n-1} are all the nth roots of unity.

Proof: We have that 1 = 1(cos(0)+isin(0)), hence the nth roots of z = 1 are z_0, z_1,..., z_{n-1}, where for each $0\leq t\leq n$-1, we have that

$$z_t = \sqrt[n]{1}[\cos(\frac{0+2t\pi}{n})+i\sin(\frac{0+2t\pi}{n})]=\cos(\frac{2t\pi}{n})+i\sin(\frac{2t\pi}{n}) = [\cos(\frac{2\pi}{n})+i\sin(\frac{2\pi}{n})]^t = u^t.$$

Therefore the nth roots of unity are 1, u,....., u^{n-1} . ■

Examples: 1) The **square roots** (i.e the 2nd roots) of unity are

$$z_1 = 1 \text{ and } z_2 = \cos(\frac{2\pi}{2})+i\sin(\frac{2\pi}{2}) = -1.$$

2) The **cube roots** (i.e the 3rd roots) of unity are

$$z_1 = 1\ ,\ z_2 = \cos(\frac{2\pi}{3})+i\sin(\frac{2\pi}{3}) = -\frac{1}{2}+i\frac{\sqrt{3}}{2} \text{ and } z_3 = \cos(\frac{4\pi}{3})+i\sin(\frac{4\pi}{3}) = -\frac{1}{2}-i\frac{\sqrt{3}}{2}.$$

Remarks: 1) **Calculation of square roots:** Without using the trigonometric form, we may calculate the square roots of any complex number z=a+ib, with $a,b\in\mathbb{R}$, as follows:

Let u=x+iy, where $x,y\in\mathbb{R}$, be a square root of z. We have $(x+iy)^2$ =a+ib, hence

$$x^2 - y^2 = a \text{ and } 2xy = b.$$

Noticing that $|x+iy|^2 = |a+ib|$, we get the useful relation $x^2 + y^2 = \sqrt{a^2+b^2}$. Now using this relation, we get $2x^2 = a+\sqrt{a^2+b^2}$, and so we obtain x. To calculate y we replace x by its value in the equation 2xy = b. For example if z=3+4i, we get $2x^2 = 3+5 = 8$ and 2xy=4, and so x=2 or x = -2, whence for x=2, we get y=1 and for x=-2, we get y=-1. Therefore the square roots of 3+4i are 2+i and -2-i.

2) **Calculation of the roots of a quadratic equation:** Given the quadratic equation

$$az^2 + bz + c = 0$$

where $a,b,c \in \mathbb{C}$ and $a \neq 0$. We show that the roots of this equation are

$$z' = \frac{-b+w}{2a} \text{ and } z'' = \frac{-b-w}{2a}$$

where w is a square root of the complex number $\Delta = b^2 - 4ac$, as follows:

$$az^2 + bz + c = a(z^2 + \frac{b}{a}z + \frac{c}{a}) = a\left[\left(z + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right] = a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right]$$

$$= a\left[\left(z + \frac{b}{2a}\right)^2 - \left(\frac{w}{2a}\right)^2\right] = a\left(z + \frac{b}{2a} + \frac{w}{2a}\right)\left(z + \frac{b}{2a} - \frac{w}{2a}\right)$$

so that as $a \neq 0$, then

$$az^2 + bz + c = 0 \Leftrightarrow \left(z + \frac{b}{2a} + \frac{w}{2a}\right)\left(z + \frac{b}{2a} - \frac{w}{2a}\right) = 0 \Leftrightarrow z + \frac{b}{2a} + \frac{w}{2a} = 0 \text{ or } z + \frac{b}{2a} - \frac{w}{2a} = 0$$

$$\Leftrightarrow z = \frac{-b+w}{2a} \text{ or } z = \frac{-b+w}{2a}$$

whence the roots of the equation are $z' = \dfrac{-b+w}{2a}$ and $z'' = \dfrac{-b+w}{2a}$.

Δ is called **the discriminant** of the equation $az^2 + bz + c = 0$.

M1100

CHAPTER VI

EXERCISES

1- Find the real numbers x and y in the following cases:
(i) $(1+2i)x+(3-5i)y = 1-3i$; (ii) $(1+i)x-(1-i)y = 3i-2$.

2- Write the algebraic form of each of the following complex numbers :

(a) $(1+i)^2$. (b) $(3+2i)^2-(3-2i)^2$. (c) $(1-3i)^5$.

(d) $(1+2i+3i^2+4i^3)^2$. (e) $\dfrac{1}{(1+i)(2+3i)}$. (f) $\dfrac{(1-i)^7-(1+i)^4}{(1+i)^3+(1-i)^5}$.

3- Find the trigonometric form of z in the following cases and if n is given, then find the n^th roots of z:

(a) $z = 1+i$; n=8. (b) $z = 2-2i\sqrt{3}$; n=12. (c) $z = -\sqrt{6}-i\sqrt{2}$.

(d) $z = 1+\cos x+i\sin x$. (e) $z = 2+\sqrt{3}+i$; n=5. (f) $z = 1+i\sqrt{3}+\sqrt{3}-i$.

4- Show that if $a,b,x,y\in\mathbb{R}$ and $n\in\mathbb{N}^*$, such that $x+iy = (a+ib)^n$, then

$$x^2+y^2 = (a^2+b^2)^n .$$

5- Show that if the complex numbers z, z' and z'' have module 1, then

(i) $\dfrac{z+z'}{1+zz'}$ is real; (ii) $|z+z'+z''| = |zz'+zz''+z'z''|$.

6- Let z and z' be two complex numbers.

1- Show that $|z+z'|\leq |z|+|z'|$.

2- Show that $|z+z'|^2+|z-z'|^2 = 2(|z|^2+|z'|^2)$.

3- Deduce that if u and v are a square roots of z and z' respectively, then

$$\left|\frac{z+z'}{2}+uv\right|+\left|\frac{z+z'}{2}-uv\right| = |z|+|z'| .$$

7- Express cos5x and sin5x in terms of cosx and sinx.

8- Show that if A and B are two points of affixes z_A and z_B respectively, then

$|z_A-z_B|$ =AB and if A≠B, then $\arg(z_A-z_B) = (\overrightarrow{Ox},\overrightarrow{BA})$ (mod 2π).

Deduce that if A, B and C are pairwise distinct points of the plane, then

$$\left|\frac{z_A-z_B}{z_A-z_C}\right| = \frac{AB}{AC} \text{ and } \arg\left(\frac{z_A-z_B}{z_A-z_C}\right) = (\overrightarrow{AC},\overrightarrow{AB}) \text{ (mod } 2\pi).$$

9- Show that if $n\in\mathbb{N}^*$, then the set S of the n^th roots of unity is a subgroup of $(\mathbb{C}^*,\times)$.

10- Solve in $\mathbb{C}$ the following equations :

(a) $z^2+15+8i = 0$; (b) $z^2-(2-i)z+3-i = 0$; (c) $(3-i)z^2+2(1-2i)z+3i-2 = 0$;

(d) $z^4 + \sqrt{2}\, z^2 + 1 = 0$; (e) $\left(\frac{z+1}{z-i}\right)^3 = \frac{\sqrt{3}+i}{\sqrt{3}-i}$, $z \neq i$; (f) $(z-1)^n = (z+1)^n$, $n \in \mathbb{N}^*$.

11- Calculate

(a) $x = \sum_{t=0}^{n} (i)^t$;

(b) the sum of all the nth roots of unity, for $n \geq 2$.

M1100

CHAPTER VII

POLYNOMIALS

Throughout this chapter the letter K denotes a field. The elements 0_K and 1_K are denoted 0 and 1 respectively. If $a\in K-\{0_K\}$, then a^{-1} is denoted $\frac{1}{a}$.

§ 7.1. DEFINITION AND OPERATIONS ON POLYNOMIALS.

Definition 1. We call **polynomial** with indeterminate x and coefficients in K, every expression f(x) of the form

$$f(x) = a_0+a_1x+\cdots+a_nx^n$$

where $a_0,a_1,...,a_n\in K$ and $n\in\mathbb{N}$ and where two expressions

$$f(x) = a_0+a_1x+\cdots+a_nx^n \text{ and } g(x) = b_0+b_1x+\cdots+b_mx^m$$

are **equal** and we write f(x) = g(x) if m = n and $a_i = b_i$, $\forall\ 1\le i\le n$. ■

If f(x) is a polynomial with indeterminate x and coefficients in K, we simply say that f(x) is a polynomial over K.

We denote by K[x] the set of all polynomials over K.

If we put $x^0=1$, we can write $a_0+a_1x+\cdots+a_nx^n = \sum_{i=0}^{n}a_ix^i$.

Also if we take $0x^i = 0$, for all $i\in\mathbb{N}$, then the polynomial $f(x) = \sum_{i=0}^{n}a_ix^i$, such that $a_0=a_1=\cdots=a_n=0$, is called **the zero polynomial** and denoted 0. Thus;

$$\sum_{i=0}^{n}a_ix^i = 0 \Leftrightarrow a_0=a_1=\cdots=a_n=0.$$

Definition 2. If $m\le n$ and $f(x) = \sum_{i=0}^{n}a_ix^i$ and $g(x) = \sum_{i=0}^{m}b_ix^i$ are two polynomials over K, then we define the **sum** f(x)+g(x) by:

$$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_nx^n.\ ■$$

Example: If $f(x) = 1+2x^2+3x^3+2x^5$ and $g(x) = -3+6x^2-5x^3+2x^4$, then

$$f(x)+g(x) = (1-3)+(2+6)x^2+(3-5)x^3+2x^4+2x^5 = -2+8x^2-2x^3+2x^4+2x^5.$$

7.1.1. K[x] is an abelian additive group with neutral element the zero polynomial and the opposite of every polynomial $f(x) = \sum_{i=0}^{n}a_ix^i$ is $-f(x) = \sum_{i=0}^{n}(-a_i)x^i$.

Proof: Easy enough. ■

Definition 3. If $\alpha\in K$ and $f(x) = \sum_{i=0}^{n} a_i x^i$, then we define $\alpha f(x)$ by $\alpha f(x) = \sum_{i=0}^{n}(\alpha a_i)x^i$. ■

7.1.2. The following hold, for all $\alpha,\beta\in K$ and $f(x),g(x)\in K[x]$:
(i) $(\alpha+\beta)f(x) = \alpha f(x)+\beta f(x)$;
(ii) $\alpha[f(x)+g(x)] = \alpha f(x)+ \alpha g(x)$;
(iii) $\alpha[\beta f(x)] = (\alpha\beta)f(x)$;
(iv) $1f(x)=f(x)$.

Proof: Easy. ■

Definition 4. If $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ are two polynomials over K, then we define $f(x)g(x)$ by $f(x)g(x) = \sum_{t=0}^{n+m} c_t x^t$, where $c_t = \sum_{i+j=t} a_i b_j$, $\forall 1\leq t\leq n+m$. ■

Thus if $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ and $f(x)g(x) = \sum_{t=0}^{n+m} c_t x^t$, then

$$c_0 = a_0 b_0 ,\ c_1 = a_0 b_1 + a_1 b_0 ,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

and

$$c_{n+m} = a_n b_m ,\ c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m \text{ and } c_{n+m-2} = a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m .$$

If we let $a_{n+1} = \cdots = a_{n+m} = 0$ and $b_{m+1} = \cdots = b_{n+m} = 0$, then

$$c_t = \sum_{i=0}^{t} a_i b_{t-i} ,\ \forall 1\leq t\leq n+m.$$

7.1.3. The multiplication of polynomials is commutative, associative has a neutral element the polynomial $f(x)=1$ and is distributive over the addition of polynomials. In particular $K[x]$ is a commutative unitary ring.

Proof: The proof is given in Appendix I. ■

§ 7.2. DEGREE OF A POLYNOMIAL.

Definition 5. Let $u = \sum_{i=0}^{n} a_i x^i \in K[x]-\{0\}$. We define the **degree** of u, written deg(u), to be the greatest integer t, such that $a_t \neq 0$. ■

Thus if $u\neq 0$ and $\deg(u)=n$, then $\exists a_0 ,a_1, \ldots,a_n \in K$, such that $a_n \neq 0$ and $u = \sum_{i=0}^{n} a_i x^i$.

Examples: Let $u = 3+x+x^2$ and $v = 2x-3x^3+x^5$. Then $\deg(u) = 2$ and $\deg(v) = 5$.

7.2.1. If u and v are two non-zero polynomials over K, then $uv\neq 0$ and

$$\deg(uv) = \deg(u)+\deg(v).$$

Proof: Let n = deg(u) and m = deg(v). Then u = $\sum_{i=0}^{n} a_i x^i$ and v = $\sum_{i=0}^{m} b_i x^i$, with $a_n \neq 0$ and $b_m \neq 0$. We have uv = $\sum_{t=0}^{n+m} c_t x^t$, with $c_{n+m} = a_n b_m$, hence $c_{n+m} \neq 0$ and so uv≠0 and deg(uv) = n+m = deg(u)+deg(v). ■

Corollary 7.2.1.1. Let u,v∈K[x]. If uv = 0, then u = 0 or v = 0.

Proof: Suppose that uv = 0. If u≠0 and v≠0, then uv≠0, by 7.2.1, a contradiction. Hence we must have u = 0 or v = 0. ■

Let u = $\sum_{i=0}^{n} a_i x^i$, with $a_n \neq 0$. Then a_n is called the **leading coefficient** of u and a_0 is called the **constant term** of u. If u=a_0, then u is called **a constant polynomial**. Thus; the constant polynomials are the elements of K.

A polynomial is called **monic** if its leading coefficient is 1.

7.2.2. Let u and v be two non-zero polynomials over K. Then we have
(i) if deg(u)>deg(v), then u-v≠0 and deg(u-v) = deg(u),
(ii) if deg(u) = deg(v) and u-v≠0, then deg(u-v)≤deg(u).
(iii) If c∈K and u-c≠0, then deg(u-c)=deg(u).

Proof: Let u = $\sum_{i=0}^{n} a_i x^i$ and v = $\sum_{i=0}^{m} b_i x^i$, with $a_n \neq 0$ and $b_m \neq 0$.

(i) Since m<n and u-v = $(a_0-b_0)+(a_1-b_1)x+\cdots+(a_m-b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_n x^n$, we then have that u-v≠0 and deg(u-v) = n = deg(u).

(ii) As n=m, then u-v=$(a_0-b_0)+(a_1-b_1)x+\cdots+(a_n-b_n)x^n$, and so deg(u-v)≤ n = deg(u).

(iii) We have u-c = $(a_0-c)+a_1x+\cdots+a_nx^n$, hence deg(u-c)=n=deg(u). ■

Corollary 7.2.2.1. Let u and v be two non-zero polynomials over K. If u-v≠0, then deg(u-v)≤max{deg(u),deg(v)}.

Proof: If deg(u)=deg(v), then deg(u-v)≤deg(u), by 7.2.2(ii), then the inequality is true in this case, because max{deg(u),deg(v)}=deg(u).
If deg(u)<deg(v), then deg(v) = max{deg(u),deg(v)}; but deg(u-v)=deg(v), by 7.2.2(i), hence the inequality is also true in this case.
If deg(u)>deg(v), then deg(u) = max{deg(u),deg(v)} and as deg(u-v)=deg(u), by 7.2.2(i), then the inequality is also true in this case. It follows that the inequality is always true. ■

7.2.3. (The Euclidian Division Algorithm). If u∈K[x] and v∈K[x]-{0}, then there exist two and only two polynomials q and r over K, such that
(i) u = qv+r,
(ii) r = 0 or [r≠0 and deg(r)<deg(v)].

Proof: **Existence:** If u = 0, then we take q = r = 0. Suppose that u≠0. If deg(u)<deg(v), we

take q = 0 and r = u. If deg(u)≥deg(v), we argue by induction on n = deg(u). For n = 0, we have deg(v)≤0, hence deg(v) = 0, and so u,v∈K. As v≠0, then u = $(uv^{-1})v$, and so we can take q = uv^{-1} and r = 0, whence the property is true for n = 0. Suppose that the property holds up to n-1 and let's show it for n. Let u= $\sum_{i=0}^{n} a_i x^i$ and v= $\sum_{i=0}^{m} b_i x^i$, with $a_n \neq 0$ and $b_m \neq 0$. As m≤n, then (n-m)∈ $\mathbb{N}$. Let

$$w = u-b_m^{-1} a_n x^{n-m} v.$$

If w = 0, then u = $b_m^{-1} a_n x^{n-m} v$, and so we take q = $b_m^{-1} a_n x^{n-m}$ and r = 0. Suppose that w≠0. Since u and $b_m^{-1} a_n x^{n-m} v$ have the same degree n and the same leading coefficient a_n, we then get that deg(w)≤n-1, hence $\exists q_0, r_0 \in K[x]$, such that

$$w = q_0 v+r_0 \text{ and } (r_0 = 0 \text{ or } [r_0 \neq 0 \text{ and } \deg(r_0)<\deg(v)])$$

by induction hypothesis. Then we take q = $q_0 + b_m^{-1} a_n x^{n-m}$ and r = r_0. Hence the property is true for n, and so it is true, ∀n∈ $\mathbb{N}$.

Uniqueness: Let q',r'∈K[x]-{0}, such that

$$u = q'v+r' \text{ and } (r' = 0 \text{ or } [r'\neq 0 \text{ and } \deg(r')<\deg(v)]).$$

We have u = qv+r, hence

$$r-r' = (q'-q)v.$$

Suppose that q'-q≠0. Then r-r'≠0, and so deg(r-r') = deg(q'-q)+deg(v), whence

$$\deg(r-r')\geq\deg(v).$$

If r=0, then deg(r-r')=deg(-r')=deg(r'), and so deg(r')≥deg(v), impossible. Similarly if r'=0, then deg(r)≥deg(v), which is impossible. Therefore r≠0 and r'≠0, and so

$$\deg(r-r')\leq \max\{\deg(r),\deg(r')\}<\deg(v),$$

by 7.2.2.1, impossible. It follows that q'-q=0, and so q=q'. This implies that r-r'=0, hence r=r', and so q=q' and r=r'. ■

The polynomials q and r obtained in 7.2.3 are respectively called the **quotient** and **the remainder** of the division of u by v.

Remark: In the proof of theorem 7.2.3, we have in fact given a practical method for calculating q and r. Here is an example explaining this method: Calculate q and r if u = $2x^4+2x+5$ and v = $3x^2+1$. Multiplying v by $\frac{2}{3}x^2$ (which is the result of the division of $2x^4$ by $3x^2$) and subtracting the result from u, we get

$$w = u-\frac{2}{3}x^2 v = 2x^4+2x+5-\frac{2}{3}x^2(3x^2+1) = -\frac{2}{3}x^2+2x+5. \quad (*)$$

Doing the same with w and v, that is multiplying v by $-\frac{2}{9}$ (which is the result of the division of $-\frac{2}{3}x^2$ by $3x^2$) and subtracting the result from w, we obtain

$$w' = w-(-\frac{2}{9}v) = -\frac{2}{3}x^2+2x+5-(-\frac{2}{9})(3x^2+1) = 2x+\frac{47}{9}. \quad (**)$$

Since deg(w')<deg(v), we then calculate u in terms of w' and v. By (*) and (**), we have u = $w+\frac{2}{3}x^2 v$ and w = $w'-\frac{2}{9}v$, hence u = $w'-\frac{2}{9}v+\frac{2}{3}x^2 v = (-\frac{2}{9}+\frac{2}{3}x^2)v+w'$, and so

$$q = -\frac{2}{9}+\frac{2}{3}x^2 \text{ and } r = w' = 2x+\frac{47}{9}.$$

These successive divisions by v can be represented by the following:

$$\begin{array}{rl|l}
 & 2x^4+2x+5 & 3x^2+1 \\ \cline{3-3}
- & 2x^4+\frac{2}{3}x^2 & \frac{2}{3}x^2-\frac{2}{9} \\ \cline{1-2}
 & -\frac{2}{3}x^2+2x+5 & \\
- & -\frac{2}{3}x^2-\frac{2}{9} & \\ \cline{1-2}
 & 2x+\frac{47}{9} &
\end{array}$$

7.2.4. Let $u \in K[x]$ and $v \in K[x]-\{0\}$ and let $s = \deg(v)$. If $r(x)$ denotes the remainder of the division of u by v, then $\exists a_0, a_1, ..., a_{s-1} \in K$, such that $r(x) = a_0+a_1x+\cdots+a_{s-1}x^{s-1}$.

Proof: If $r(x) = 0$, we take $a_0 = a_1 = \cdots = a_{s-1} = 0$. If $r(x) \neq 0$, let $t = \deg(r(x))$, then $\exists a_0, a_1, ..., a_t \in K$, such that $r(x) = a_0+a_1x+\cdots+a_tx^t$. Since $t < \deg(v) = s$, then $t \leq s-1$. If $t = s-1$, then there is nothing to prove and if $t < s-1$, we take $a_{t+1} = \cdots = a_{s-1} = 0$. ■

If $f(x) = \sum_{i=0}^{n} a_i x^i$ and $\alpha \in K$, then **the value of f(x) at x=α** is $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$.

7.2.5. If $u(x), v(x) \in K[x]$ and $\alpha \in K$, then
(i) if $f(x) = u(x)+v(x)$, then $f(\alpha) = u(\alpha)+v(\alpha)$,
(ii) if $f(x) = u(x)v(x)$, then $f(\alpha) = u(\alpha)v(\alpha)$,
(iii) if $\lambda \in K$ and $f(x) = \lambda u(x)$, then $f(\alpha) = \lambda u(\alpha)$.

Proof: The proof is easy. ■

Let $\alpha \in K$ and $f(x) \in K[x]$. We can directly calculate $f(\alpha)$, by simply replacing x by by α in $f(x)$. In 7.2.6, below we give **Horner's method**, which is a simple method that gives at the same time the value of $f(\alpha)$ and the quotient and the remainder of the division of $f(x)$ by $x-\alpha$.

7.2.6. (Horner's method): Let $f(x) = a_0+a_1x+\cdots+a_nx^n \in K[x]$. If $b_0, b_1, \ldots, b_n$ are elements of K, such that

$$b_n = a_n \text{ and } b_t = a_t + b_{t+1}\alpha, \text{ for all } 0 \leq t \leq n-1.$$

then the quotient $q(x)$ and the remainder $r(x)$ of the division of $f(x)$ by $x-\alpha$ are

$$q(x) = b_1+b_2x+\cdots+b_nx^{n-1} \text{ and } r(x) = f(\alpha) = b_0.$$

Proof: We simply verify that $f(x) = (x-\alpha)q(x)+b_0$, so that as $\deg(x-\alpha)=1$ and b_0 is constant, then $q(x)$ is the quotient and $r(x) = b_0$, by 7.2.3. As $f(x) = (x-\alpha)q(x)+b_0$, then

$f(\alpha) = b_0$, by 7.2.5, and so $r(x) = f(\alpha) = b_0$. ■

We have $b_n = a_n$ and to obtain $b_0, b_1, \ldots, b_{n-1}$ we use a table with n+1 columns and three rows. In the first row we start from left to right by putting a_n in the first box, a_{n-1} in the 2nd , and so on a_1 in the nth and a_0 in the last. In the first box of the 3rd row we put b_n, then in the 2nd row below a_{n-1}, we put $b_n\alpha$, and after that in the 3rd row under $b_n\alpha$, we put the sum $a_{n-1}+b_n\alpha$, which is the value of b_{n-1}. After obtaining b_{n-1}, we put $b_{n-1}\alpha$ in the 2nd row under a_{n-2} and then in the 3rd we put $a_{n-1}+b_{n-1}\alpha$, which is b_{n-2}, and so on we obtain $b_{n-1}, b_{n-2}, \ldots, b_1, b_0$ in the 3rd row. Here are two examples:

1) Let $f(x) = 3x^4-6x^2+8x-5$. Find f(-3) and the quotient and the remainder of the division of f(x) by x+3. Here $\alpha = -3$. We have

$a_4=3$	$a_3=0$	$a_2 = -6$	$a_1 = 8$	$a_0 = -5$
	$b_4\alpha= -9$	$b_3\alpha= 27$	$b_2\alpha= -63$	$b_1\alpha= 165$
$b_4=3$	$b_3=a_3+b_4\alpha= -9$	$b_2 = 21$	$b_1 = -55$	$b_0 = 160$

Therefore $q(x) = 3x^3-9x^2+21x-55$ and r(x) = f(-3) = 160.

2) Let $f(x) = 2x^5-3x^4+5x^3-8x+6$. Find f(4) and the quotient and the remainder of the division of f(x) by x-4. Here $\alpha = 4$. We have

2	-3	5	0	-8	6
	8	20	100	400	1568
2	5	25	100	392	1574

hence $q(x) = 2x^4+5x^3+25x^2+100x+392$ and r(x) = f(4) = 1574.

Remark: To calculate $b_n, b_{n-1}, b_{n-2}, \ldots, b_1, b_0$, we may simply use the program Excel or we may write a program giving them.

Definition 6. Let $u\in K[x]$ and $v\in K[x]-\{0\}$. We say that v **divides** u (or that u is **divisible by** v or that v is **a factor** of u) if $\exists w\in K[x]$, such that u = vw. ■

7.2.7. Let $u\in K[x]$ and $v\in K[x]-\{0\}$. Then v divides u if and only if the remainder of the division of u by v is zero.

Proof: Let r be the remainder and q the quotient of the division of u by v. Then u = qv+r.
N.C: Since v divides u, $\exists w\in K[x]$, such that u = vw.= wv+0, hence r = 0, by 7.2.3.
S.C: We have r = 0, hence u = qv, and so v divides u. ■

§ 7.3. ROOTS OF A POLYNOMIAL.

Definition 7. Let $f(x)\in K[x]$ and $\alpha\in K$. We say that α is a **root** of f(x) if $f(\alpha) = 0$. ■

7.3.1. If $f(x)\in K[x]$ and $\alpha\in K$, then α is a root of f(x) if and only if $(x-\alpha)$ divides f(x).

Proof: Let r(x) be the remainder and q(x) the quotient of the division of f(x) by $(x-\alpha)$. Then $f(x) = (x-\alpha)q(x)+r(x)$. Since $\deg(x-\alpha)=1$, $\exists a_0 \in K$, such that $r(x) = a_0$, by 7.2.4. We have $r(\alpha) = a_0$, hence $r(x) = r(\alpha)$, and so

$$\alpha \text{ is a root of } f(x) \Leftrightarrow f(\alpha) = 0 \Leftrightarrow r(\alpha) = 0 \Leftrightarrow r(x) = 0 \Leftrightarrow (x-\alpha) \text{ divides } f(x). \blacksquare$$

Corollary 7.3.1.1. If $b_1, b_2, ..., b_t \in K$ are pairwise distinct roots of a polynomial $f(x) \in K[x]$, then $(x-b_1)(x-b_2)...(x-b_t)$ divides $f(x)$.

Proof: We argue by induction on t. The property is true for t=1, by 7.3.1. Assume that it holds for (t-1) and let's show it for t. Since $b_1, b_2, ..., b_{t-1}$ are pairwise distinct roots of f(x), we then get from the hypothesis of induction that $(x-b_1)(x-b_2)...(x-b_{t-1})$ divides f(x), and so $\exists g(x) \in K[x]$, such that

$$f(x) = (x-b_1)(x-b_2)...(x-b_{t-1})g(x).$$

We have that b_t is a root of f(x), hence $f(b_t) = 0$, and so

$$(b_t - b_1)(b_t - b_2)...(b_t - b_{t-1})g(b_t) = 0.$$

Since $b_1, b_2, ..., b_{t-1}, b_t$ are pairwise distinct, we then have that $b_t \notin \{b_1, b_2, ..., b_{t-1}\}$, hence $(b_t - b_1)(b_t - b_2)...(b_t - b_{t-1}) \neq 0$, and so $g(b_t) = 0$. It follows that b_t is a root of g(x), hence $(x-b_t)$ divides g(x), by 7.3.1, and so $\exists h(x) \in K[x]$, such that $g(x) = (x-b_t)h(x)$. Therefore $f(x) = (x-b_1)(x-b_2)...(x-b_{t-1})(x-b_t)h(x)$, and so $(x-b_1)(x-b_2)...(x-b_{t-1})(x-b_t)$ divides f(x). Hence the property is true for t, and so it is true, $\forall t \geq 1$. ■

Corollary 7.3.1.2. If f(x) is a polynomial over K of degree $n \geq 1$, then f(x) has at most n pairwise distinct roots in K.

Proof: Suppose that the number of pairwise distinct roots of f(x) in K is $\geq n+1$. Let $b_1, b_2, ..., b_{n+1} \in K$ be pairwise distinct roots of f(x) in K. Then $(x-b_1)(x-b_2)...(x-b_{n+1})$ divides f(x), by 7.3.1, and so $\exists g(x) \in K[x]$, such that $f(x) = (x-b_1)(x-b_2)...(x-b_{n+1})g(x)$. We have that $n = \deg(f(x)) = \deg[(x-b_1)(x-b_2)...(x-b_{n+1})] + \deg(g(x)) \geq n+1$, a contradiction. Hence f(x) has at most n pairwise distinct roots in K. ■

§ 7.4. IRREDUCIBLE POLYNOMIAL.

Definition 8. Let $p(x) \in K[x]$. We say that p(x) is **irreducible** over K if p(x) is non-constant and cannot be factored into the product of two non-constant polynomials over K. ■

Thus if $p(x) \in K[x]$, then p(x) is **irreducible** over K if and only if
(i) $\deg(p) \geq 1$,
(ii) if $p(x) = f(x)g(x)$, where $f(x), g(x) \in K[x]$, then $\deg(f) = 0$ or $\deg(g) = 0$.

A polynomial which is not irreducible over K is called **reducible** over K.

If p(x) and f(x) are two polynomials over K, such that p(x) is irreducible over K and p(x) divides f(x), then p(x) is called **an irreducible factor** of f(x).

7.4.1. Every polynomial p(x) over K of degree 1 has a root in K and is irreducible over K.

Proof: We have $\deg(p) = 1$, hence $p(x) = ax+b$, for some $a, b \in K$, with $a \neq 0$, and so $\alpha = \dfrac{-b}{a}$ is a root of p(x). Suppose that p(x) is not irreducible over K. As p(x) is non-constant, then there exist two non-constant polynomial f(x) and g(x) in K[x], such that p(x)=f(x)g(x), We have deg(f)≥1 and deg(g)≥1, hence deg(f)+deg(g)≥2. But deg(f)+deg(g) = deg(p) = 1, by 7.2.1, a contradiction, and so p(x) is irreducible over K. ■

7.4.2 If $p(x)\in K[x]$ is irreducible over K and deg(p)≥2, then p(x) has no root in K.

Proof: Suppose that p(x) has a root $\alpha\in K$, then $(x-\alpha)$ divides p(x), by 7.3.1, and so $p(x)=(x-\alpha)g(x)$, for some $g(x)\in K[x]$. As p(x) is irreducible over K and $\deg(x-\alpha)=1$, then deg(g)=0, and so $\deg(p)=\deg(x-\alpha)+\deg(g)=1$, by 7.2.1, impossible. Hence p(x) has no root in K. ■

7.4.3. If $p(x)\in K[x]$ and $2\le\deg(p)\le3$, then p(x) is irreducible over K if and only if p(x) has no root in K.

Proof: **N.C:** By 7.4.2.
S.C: Suppose that p(x) is not irreducible, then $\exists f(x),g(x)\in K[x]$, such that

$$\deg(g)\neq0,\ \deg(h)\neq0 \text{ and } f(x)=g(x)h(x).$$

We have

$$\deg(f)\geq1,\ \deg(g)\geq1 \text{ and } \deg(f)+\deg(g)=\deg(p)\leq3$$

hence deg(f)=1 or deg(g)=1. If deg(f)=1, then f(x) has a root in K, by 7.4.1, and so p(x) has a root in K, a contradiction. Similarly if deg(g)=1, we get that p(x) has a root in K, which is impossible. Therefore p(x) is irreducible over K. ■

7.4.4. If $f(x)\in K[x]$ is of degree ≥1, then f(x) can be written as a product of a finite number of irreducible factors, that is there exists a finite number of irreducible polynomials over K, $p_1(x), p_2(x), \ldots, p_r(x)$, such that $f(x) = p_1(x)p_2(x)\ldots p_r(x)$.

Proof: We argue by induction on n=deg(f). For n=1, we have f(x) is irreducible over K, by 7.4.1, hence the property holds for n=1. Assume that it holds up to n-1 and let's prove it for n. If f(x) is irreducible, there is nothing to show, so suppose that f(x) is not irreducible over K, then $\exists g(x),h(x)\in K[x]$, such that

$$\deg(g)\neq0,\ \deg(h)\neq0 \text{ and } f(x)=g(x)h(x).$$

We have that deg(g)≥1, deg(h)≥1 and n=deg(f)=deg(g)+deg(h), by 7.2.1, hence deg(g)≤n-1 and deg(h)≤n-1, and so induction yields that there exists a finite number of irreducible polynomials over K, $u_1(x), u_2(x), \ldots, u_r(x), v_1(x), v_2(x), \ldots, v_s(x)$, such that

$$g(x) = u_1(x)u_2(x)\ldots u_r(x) \text{ and } h(x) = v_1(x)v_2(x)\ldots v_s(x).$$

As $f(x) = g(x)h(x) = u_1(x)u_2(x)\ldots u_r(x)v_1(x)v_2(x)\ldots v_s(x)$, then the property holds for n, and so it is true, for all n≥1. ■

§ 7.5. DERIVATIVE OF A POLYNOMIAL.

Definition 9. Let $f(x)=a_0+a_1x+\cdots+a_nx^n\in K[x]$. We define the **derivative** of f(x), denoted [f(x)]' by [f(x)]' = 0 if n = 0 and $[f(x)]' = a_1+2a_2x+\cdots+na_nx^{n-1}$, if n≥1. ■

Definition 10. Let $f(x)\in K[x]$ and $s\in\mathbb{N}$. We define **the sth derivative** (or **the derivative of order s**) of f(x), denoted $f^{(s)}(x)$ by $f^{(0)}(x) = f(x)$ and $f^{(s)}(x) = [f^{(s-1)}(x)]'$, if n≥1. ■

7.5.1. The following hold, for all $u(x),v(x),f(x)\in K[x]$ and $\alpha\in K$
(i) [u(x)+v(x)]' = [u(x)]'+[v(x)]',

(ii) $[\alpha u(x)]' = \alpha[u(x)]'$,
(iii) $[u(x)v(x)]' = [u(x)]'v(x)+u(x)[v(x)]'$,
(iv) if f(x) is constant, then $[f(x)]' = 0$.

Proof: Easy. ■

For each $f(x)\in K[x]$, set $f'(x) = [f(x)]'$, $f''(x) = f^{(2)}(x)$ and $f'''(x) = f^{(3)}(x)$.

7.5.2. (Taylor's Formula). If $f(x)\in K[x]-\{0\}$ is a polynomial of degree n and $\alpha\in K$, then

$$f(x) = f(\alpha)+\frac{(x-\alpha)}{1!}f'(\alpha)+\cdots+\frac{(x-\alpha)^n}{n!}f^{(n)}(\alpha).$$

Proof: The proof is given in Appendix I. ■

Definition 11. Let $f(x)\in K[x]$ and $\alpha\in K$. We say that α is a root of f(x) of **multiplicity** m if $(x-\alpha)^m$ divides f(x) and $(x-\alpha)^{m+1}$ does not divide f(x). ■

If α is a root of f(x) of multiplicity 1 (resp. 2,3, etc...), then we say that α is a **simple** (resp. **double**, **triple**, etc...) root of f(x).

Examples: Let $f(x)=(x-1)(x-4)^2(x-8)^5$. Then 8 is a root of f(x) of multiplicity 5, 1 is a simple root and 4 is a double root of f(x).

7.5.3. Let $f(x)\in K[x]-\{0\}$ be a polynomial of degree n and let $\alpha\in K$ and $m\in\mathbb{N}^*$, then $(x-\alpha)^m$ divides f(x) if and only if $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$.

Proof: **N.C:** We argue by induction on m. For m = 1, we have that $(x-\alpha)$ divides f(x), hence α is a root of f(x), by 7.3.1, and so $f(\alpha) = 0$ and the property is true for m = 1. Suppose that it is true for (m-1) and let's show it for m. We have that $(x-\alpha)^m$ divides f(x), hence $\exists v(x)\in K[x]$, such that $f(x) = (x-\alpha)^m v(x)$. Thus $f'(x) = m(x-\alpha)^{m-1}+(x-\alpha)^m v'(x)$, and so $(x-\alpha)^{m-1}$ divides $f'(x)$, whence $f'(\alpha) = (f')'(\alpha) = \cdots = (f')^{(m-2)}(\alpha) = 0$, by induction hypothesis. But $(f')'(\alpha) = f''(\alpha)$, …, $(f')^{(m-2)}(\alpha)=f^{(m-1)}(\alpha)$, hence

$$f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0.$$

Since $f(\alpha) = 0$, we get $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$, whence the property is true for m, and so it is true, $\forall m\in\mathbb{N}^*$.
S.C: By Taylor's formula, we have that

$$f(x) = f(\alpha)+\frac{(x-\alpha)}{1!}f'(\alpha)+\cdots+\frac{(x-\alpha)^n}{n!}f^{(n)}(\alpha).$$

If m>n, then $f(\alpha) = f'(\alpha) = \cdots = f^{(n)}(\alpha) = 0$, hence f(x) = 0, which is impossible, and so $m\leq n$. Since $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$, we then get that

$$f(x) = \frac{(x-\alpha)^m}{m!}f^{(m)}(\alpha)+\frac{(x-\alpha)^{m+1}}{(m+1)!}f^{(m+1)}(\alpha)+\cdots+\frac{(x-\alpha)^n}{n!}f^{(n)}(\alpha)$$

$$= (x-\alpha)^m\left[\frac{1}{m!}f^{(m)}(\alpha)+\frac{(x-\alpha)}{(m+1)!}f^{(m+1)}(\alpha)+\cdots+\frac{(x-\alpha)^{n-m}}{n!}f^{(n)}(\alpha)\right]$$

hence $(x-\alpha)^m$ divides f(x). ■

Corollary 7.5.3.1. Let $f(x)\in K[x]-\{0\}$ and let $\alpha\in K$ and $m\in\mathbb{N}^*$.Then α is a root of f(x) of multiplicity m if and only if $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ and $f^{(m)}(\alpha) \neq 0$.

Proof: **N.C:** Since $(x-\alpha)^m$ divides f(x), we then have $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$, by 7.5.3. If $f^{(m)}(\alpha) = 0$, then we obtain $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = f^{(m)}(\alpha) = 0$, hence $(x-\alpha)^{m+1}$ divides f(x), by 7.5.3, impossible, since $(x-\alpha)^{m+1}$ does not divide f(x). It follows that $f^{(m)}(\alpha) \neq 0$, and so $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ and $f^{(m)}(\alpha) \neq 0$.
S.C: We have $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$, hence $(x-\alpha)^m$ divides f(x), by 7.5.3. If $(x-\alpha)^{m+1}$ divides f(x), then $f^{(m)}(\alpha)=0$, impossible, since $f^{(m)}(\alpha) \neq 0$. Hence $(x-\alpha)^{m+1}$ does not divide f(x), and so α is a root of f(x) of multiplicity m. ■

7.5.4. Let $\alpha\in K$ and $f(x)\in K[x]$. If for each natural number t, we define $q_t(x)$ by $q_0(x) = f(x)$ and the inductive relation $q_{t+1}(x)$ is the quotient of the division of $q_t(x)$ by $x-\alpha$, then

$$f^{(t)}(\alpha) = t!q_t(\alpha), \text{ for all } t\geq 0.$$

Proof: The proof is given in Appendix I. ■

It follows from 7.5.4 that if $t\geq 0$, then by applying Horner's method successively to $q_0(x), q_1(x), \ldots, q_t(x)$, we get $f^{(s)}(\alpha)$, for all $0\leq s\leq t$. Thus if we retake the example 1) given after 7.2.6, where $f(x) = 3x^4 -6x^2 +8x-5$, we find that the quotient $q_1(x)$ of the division of f(x) by x+3 is $q_1(x) = 3x^3 -9x^2 +21x-55$. To find $f'(-3)$ we apply Horner's method to $q_1(x)$, then we get

3	-9	21	-55
	-9	54	-225
3	-18	75	-280

and so $q_2(x) = 3x^2 -18x+75$ and $f'(-3) = -280$.
Now to find $f''(-3)$ we apply Horner's method to $q_2(x)$, we get

3	-18	75
	-9	81
3	-27	156

and so $q_2(-3) = 156$ and $f''(-3) = 2!q_2(-3) = 2\times 156 = 312$.

§ 7.6. REAL AND COMPLEX POLYNOMIALS.

We call **real** (resp. **complex**) **polynomial** every polynomial over $\mathbb{R}$ (resp. $\mathbb{C}$). Since $\mathbb{R}\subseteq\mathbb{C}$, every real polynomial is a complex polynomial.

7.6.1. (The Fundamental Theorem of Algebra). If f(x) is a complex polynomial of degree $n\geq 1$, then f(x) has at least one root in $\mathbb{C}$.

Proof: To be admitted without proof. ■

Corollary 7.6.1.1. The following hold

(i) If f(x) is a complex polynomial of degree $n\geq 1$, then $\exists u,\alpha_1,\ldots,\alpha_n \in \mathbb{C}$, such that $f(x) = u(x-\alpha_1)\ldots(x-\alpha_n)$, that is every complex polynomial of degree $n\geq 1$ splits into a product of a constant and n linear factors over $\mathbb{C}$.

(ii) A non-constant complex polynomial p(x) is irreducible over $\mathbb{C}$ if and only if deg(p)=1.

Proof: (i) We proceed by induction on n. For n=1, we have f(x)=ax+b, for some $a,b\in\mathbb{C}$, with $a\neq 0$, and so putting $\alpha=\frac{-b}{a}$, we get $f(x)=a(x-\alpha)$, with $a,\alpha\in\mathbb{C}$, whence the property holds for n=1. Suppose that it holds up to n-1 and let's prove it for n. By 7.6.1, f(x) has a root $\alpha_1\in\mathbb{C}$. We have $x-\alpha_1$ divides f(x), by 7.3.1, hence $\exists g(x)\in\mathbb{C}[x]$, such that $f(x)=(x-\alpha_1)g(x)$. As

$$n = \deg(f) = \deg(x-a_1)+\deg(g) = 1+\deg(g)$$

then deg(g)=n-1, and so $\exists u,\alpha_2,\ldots,\alpha_n \in\mathbb{C}$, such that $g(x) = u(x-\alpha_2)\ldots(x-\alpha_n)$, by induction hypothesis. It follows that $f(x) = u(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$, hence the property holds for n, and so it is true, for all $n\geq 1$.

(ii) **N.C:** As $n=\deg(p)\geq 1$, then p(x) has a root in $\mathbb{C}$, by 7.6.1. We have p(x) is irreducible over $\mathbb{C}$, hence n=1, by 7.4.2.

S.C: By 7.4.1. ■

It follows that

(i) every complex polynomial of degree $n\geq 1$ has n roots in $\mathbb{C}$.

(ii) the irreducible polynomials over $\mathbb{C}$ are those of degree 1.

7.6.2. Let f(x) be a real polynomial and let $\alpha\in\mathbb{C}$. If α is a root of f(x), then so is the conjugate $\overline{\alpha}$ of α.

Proof: Since f(x) is a real polynomial, $\exists a_0,a_1,\ldots,a_n \in\mathbb{R}$, such that $f(x) = \sum_{t=0}^{n} a_t x^t$.

We have $f(\overline{\alpha}) = \sum_{t=0}^{n} a_t\overline{\alpha}^t = \sum_{t=0}^{n} \overline{a_t}\,\overline{\alpha^t} = \overline{\sum_{t=0}^{n} a_t\alpha^t} = 0$, hence $\overline{\alpha}$ is a root of f(x). ■

7.6.3. Let f(x), g(x) and h(x) be complex polynomials. If f(x)=g(x)h(x) and $f(x)\in\mathbb{R}[x]$ and $g(x)\in\mathbb{R}[x]-\{0\}$, then $h(x)\in\mathbb{R}[x]$.

Proof: By 7.2.3, $\exists q(x),r(x)\in\mathbb{R}[x]$, such that

$$f(x) = q(x)g(x)+r(x) \text{ and } (r(x) = 0 \text{ or } \deg(r)<\deg(g)).$$

Since $\mathbb{R}[x]\subseteq\mathbb{C}[x]$, $q(x),r(x)\in\mathbb{C}[x]$. But $h(x)\in\mathbb{C}[x]$ and $f(x) = h(x)g(x)$, hence $h(x) = q(x)$ and $r(x) = 0$, by 7.2.3, and so $h(x)\in\mathbb{R}[x]$. ■

Corollary 7.6.3.1. Let $f(x)\in\mathbb{R}[x]$. If $\alpha\in\mathbb{C}$ is a non-real root of f(x), then

(i) $(x-\alpha)(x-\overline{\alpha})\in\mathbb{R}[x]$,

(ii) $(x-\alpha)(x-\overline{\alpha})$ divides f(x) in $\mathbb{R}[x]$, that is $\exists g(x)\in\mathbb{R}[x]$, such that $f(x)=(x-\alpha)(x-\overline{\alpha})g(x)$.

Proof: (i) As $(x-\alpha)(x-\overline{\alpha}) = x^2-(\alpha+\overline{\alpha})x+\alpha\overline{\alpha}$ and $\alpha+\overline{\alpha}\in\mathbb{R}$ and $\alpha\overline{\alpha}\in\mathbb{R}$, then

$$(x-\alpha)(x-\overline{\alpha})\in\mathbb{R}[x].$$

(ii) Since $\alpha\notin\mathbb{R}$, $\overline{\alpha}\neq\alpha$, and so as $\overline{\alpha}$ is a root of f(x), by 7.6.2, then $(x-\alpha)(x-\overline{\alpha})$ divides f(x) in $\mathbb{C}[x]$, by 7.3.1.1, whence $\exists g(x)\in\mathbb{C}[x]$, such that $f(x) = (x-\alpha)(x-\overline{\alpha})g(x)$. We have that $(x-\alpha)(x-\overline{\alpha})\in\mathbb{R}[x]-\{0\}$, by (i), hence $g(x)\in\mathbb{R}[x]$, by 7.6.3. This completes (ii). ■

7.6.4. Every real polynomial of odd degree has at least one real root.

Proof: Let $m\in\mathbb{N}$, such that deg(f) = 2m+1. We argue by induction on m. For m=0, we have deg(f)=1, hence f(x) has a root in $\mathbb{R}$, by 7.4.1, and so the property holds for m=0. Suppose that it holds up to (m-1) and let's show it for m. Assume that f(x) has no real roots. We have that f(x) has roots in $\mathbb{C}$, by 7.6.1. Let $\alpha\in\mathbb{C}$ be such a root of f(x). Since $\alpha\notin\mathbb{R}$,

$$\exists g(x)\in\mathbb{R}[x], \text{ such that } f(x) = (x-\alpha)(x-\overline{\alpha})g(x)$$

by 7.6.3.1. Since $\deg(f) = \deg[(x-\alpha)(x-\overline{\alpha})]+\deg(g) = 2+\deg(g)$, we then get

$$\deg(g) = 2m+1-2 = 2(m-1)+1$$

and so g(x) has a root $\beta\in\mathbb{R}$, by induction hypothesis. As β is a root of f(x), then we have a contradiction to our assumption that f(x) has no real roots. Therefore the property is true for m, and so it is true, $\forall m\in\mathbb{N}$. ■

Corollary 7.6.4.1. If a real polynomial f(x) has no real roots, then its degree is even.

Proof: If the degree of f(x) is odd, then f(x) has at least one real root, impossible. Hence the degree of f(x) is even. ■

7.6.5. If $p(x)=ax^2+bx+c$ is a real polynomial of degree 2, then p(x) is irreducible over $\mathbb{R}$ if and only if $b^2-4ac<0$.

Proof: **N.C:** If $b^2-4ac\geq0$, then p(x) has a real root, and so p(x) is not irreducible over $\mathbb{R}$, by 7.4.2, a contradiction. Therefore $b^2-4ac<0$.

S.C: As $b^2-4ac<0$, then p(x) has no roots in $\mathbb{R}$, and so p(x) is irreducible over $\mathbb{R}$, by 7.4.3. ■

Corollary 7.6.5.1. The irreducible polynomials over $\mathbb{R}$ are those of degree 1 and those of the form ax^2+bx+c, with $a\neq0$ and $b^2-4ac<0$.

Proof: By 7.4.1 and 7.6.5, we have that every polynomial of degree 1 and every polynomial of the form ax^2+bx+c, with $a\neq0$ and $b^2-4ac<0$ are irreducible over $\mathbb{R}$.
Let $p(x)\in\mathbb{R}[x]$ be irreducible over $\mathbb{R}$. As $\deg(p)\geq1$, then p(x) has a root $\alpha\in\mathbb{C}$, by 7.6.1. If $\alpha\in\mathbb{R}$, then $x-\alpha$ divides p(x) in $\mathbb{R}[x]$, by 7.3.1, and so $\exists g(x)\in\mathbb{R}[x]$, such that $p(x)=(x-\alpha)g(x)$. But p(x) is irreducible over $\mathbb{R}$, and $\deg(x-\alpha)\neq0$, hence deg(g)=0, and so deg(p)=1. Assume that $\alpha\notin\mathbb{R}$, then $(x-\alpha)(x-\overline{\alpha})\in\mathbb{R}[x]$ and

$$\exists g(x)\in\mathbb{R}[x], \text{ such that } p(x)=(x-\alpha)(x-\overline{\alpha})g(x).$$

As p(x) is irreducible over $\mathbb{R}$ and $\deg[(x-\alpha)(x+\alpha)]\neq0$, then deg(g)=0, and so deg(p)=2. Therefore $\exists a,b,c\in\mathbb{R}$, such that $a\neq0$ and $p(x)=ax^2+bx+c$. But p(x) is irreducible over $\mathbb{R}$, hence $b^2-4ac<0$, by 7.6.5. Therefore p(x) is of the form ax^2+bx+c, with $a\neq0$ and $b^2-4ac<0$. This completes the proof of 7.5.6.1. ■

M1100

CHAPTER VII

EXERCISES

1- Calculate the remainder and the quotient of the division of f(x) by g(x) in the following cases:

(i) $f(x) = 2x^3-5x^2+2$ and $g(x) = x^2-3x+1$,

(ii) $f(x) = 5x^2+2x-1$ and $g(x) = x^3-x+2$,

(iii) $f(x) = 4x^6-2x^5+4x^3+2x^4-2x+6$ and $g(x) =3x^4-6x^2+8x-5$.

2- Find the conditions satisfied by the real numbers m, p and q, so that x^2+mx+1 divides x^3+px+q.

3- Let $a\in\mathbb{R}$ and $n\in\mathbb{N}^*$. Find the remainder of the division of $f(x) = (\cos a+x\sin a)^n$ by x^2+1.

4- Show that if j is a cube root of unity ≠1, then the polynomial

$$f(x) = x^4+2ix^3+jx^2-2ij^2x+j^2$$

is divisible by (x-j), (x+i) and (x-j)(x+i).

5- Using Horner's method find $f(\alpha)$ and the quotient and the remainder of the division of f(x) by $x-\alpha$, in the following cases:

(i) $f(x) = 2x^4-3x^3+2x^2-x-1$, for $\alpha = 2$.

(ii) $f(x) = x^5-3x^4+2x^3-5x^2+8$, for $\alpha = -3$.

Using the same method, find $f'(\alpha)$ and $f''(\alpha)$ in each case.

6- Show that 1-i is a root of $f(x) = x^6+(1+2i)x^4+(1+2i)x^2+2i$, then find the other roots.

7- Find the real numbers a and b, so that the real polynomial $f(x) = ax^{n+1}+bx^n+1$ is divisible by $(x-1)^2$.

8- Show that $(x-1)^3$ divides $f(x)=x^{2n}-nx^{n+1}+nx^{n-1}-1$, for all $n\geq2$.

9- Find a real polynomial f(x) of degree 5, such that f(x)+1 is divisible by $(x-1)^3$ and f(x)-1 is divisible by $(x+1)^3$.

10- Let $f(x) = 2x^5-12ix^4-23x^3+10ix^2-12x+8i$.

1- Show that 2i is a root of f(x) and find its order of multiplicity.

2- Give a factorization of f(x) over $\mathbb{C}$.

11- Let $f(x) = x^4-x^3+x^2+2$.

1- Show that 1+i is a root of f(x), then find the other roots.

2- Write f(x) as a product of irreducible factors over $\mathbb{C}$, then over $\mathbb{R}$.

12- Let f(x) = $x^4 + 3x^2 + 6x + 10$.

1- Find two real numbers a and b, such that f(x) = $(x^2 + a)^2 + (x - b)^2$.

2- Deduce a factorization of f(x) as a product of two complex polynomials each of degree 2.

3- Find the roots of f(x) in $\mathbb{C}$, and then write f(x) as a product of irreducible polynomials over $\mathbb{R}$.

APPENDIX I

PROOF OF SOME THEOREMS

2.4.6. If $f : A \longrightarrow B$ is a mapping, then

(i) f is injective if and only if there exists a mapping $g : B \longrightarrow A$, such that $g \circ f = id_A$.

(ii) f is surjective if and only if there exists a mapping $g : B \longrightarrow A$, such that $f \circ g = id_B$.

Proof: (i) **N.C:** Since $A \neq \varnothing$, $\exists a \in A$. Let g be the correspondence from B to A that associates every element x of f(A) with the elements y of A satisfying f(y)=x and associates every element of B-f(A) with the element a.

g is a mapping: Let $x \in B$. If $x \in f(A)$, then $\exists t \in A$, such that x=f(t), hence t is an image of x by g. if $x \notin f(A)$, then $x \in B\text{-}f(A)$, hence a is an image of x by g. Let y and y' be two images of x by g. If $x \in B\text{-}f(A)$, then y=a and y'=a, and so y = y' in this case. if $x \in f(A)$, then f(y)=x and f(y')=x, and so f(y)=f(y'), but f is injective, hence y = y'. Therefore every element x of B has a unique image under g, and so g is a mapping.

Let $t \in A$, then $f(t) \in f(A)$, hence g(f(t)) = t, and so $g \circ f(t) = g(f(t)) = t = id_A(t)$, $\forall t \in A$, whence $g \circ f = id_A$.

S.C: As $g \circ f$ is injective, then f is injective, by 2.4.3(ii)..

(ii) **N.C:** Consider the family $(f^{-1}(\{b\}))_{b \in B}$. As B is non-empty, then this family is non-empty. The sets in this family are non-empty and pairwise disjoint, because f is surjective and if $b,b' \in B$ and $b \neq b'$, then $f^{-1}(\{b\}) \cap f^{-1}(\{b'\}) = \varnothing$, for if $a \in f^{-1}(\{b\}) \cap f^{-1}(\{b'\})$, for some a, then $a \in f^{-1}(\{b\})$ and $a \in f^{-1}(\{b'\})$, and so f(a)=b and f(a)=b', whence b=b', which is impossible. It follows from the axiom of choice that there exists a set E, such that $E \cap f^{-1}(\{b\})$ is a singleton, for all $b \in B$. For each b in B, let

$$E \cap f^{-1}(\{b\}) = \{e_b\}.$$

Define $g : B \longrightarrow A$ by $g(b) = e_b$. We have

$$f \circ g(b) = f(g(b)) = f(e_b) = b = id_B(b), \text{ for all } b \in B, \text{ hence } f \circ g = id_B.$$

S.C: As $f \circ g$ is surjective, then f is surjective, by 2.4.3(iii). ■

3.1.4. If $A \approx B$ and $C \approx D$ and $A \cap C = B \cap D = \varnothing$, then $A \cup C \approx B \cup D$.

Proof: As $A \approx B$ and $C \approx D$, then there exist two bijections $f : A \longrightarrow B$ and $g : C \longrightarrow D$.

Let $h : A \cup C \longrightarrow B \cup D$ be the correspondence that associates every element x of $A \cup C$ with the elements y of $B \cup D$, satisfying

$$y = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in C. \end{cases}$$

h is a mapping: Let $x \in A \cup C$. Then $x \in A$ or $x \in C$. If $x \in A$, then f(x) is an image of x by h and if $x \in C$, then g(x) is an image of x by h.

Now let y and y' be two images of x by h. Then

y = f(x) or y = g(x)

and

$$y' = f(x) \text{ or } y' = g(x).$$

If $y\neq y'$, then

$$[y = f(x) \text{ and } y' = g(x)] \text{ or } [y = g(x) \text{ and } y' = f(x)]$$

which yields $x\in A$ and $x\in C$, and so $x\in A\cap C=\varnothing$, impossible. Hence $y=y'$, and so h is a mapping.

h injective: Let $x,y\in A\cup C$, such that $h(x)=h(y)$. Since $x,y\in A\cup C$, we get that ($x\in A$ or $x\in C$) and ($y\in A$ or $y\in C$), hence there are four cases to be tackled.

1st case: $x\in A$ and $y\in A$. Then $h(x)=f(x)$ and $h(y)=f(y)$, so that $f(x)=f(y)$, and so $x = y$.

2nd case: $x\in A$ and $y\in C$. We have $h(x)=f(x)$ and $h(y)=g(y)$, hence $f(x)=g(y)$, and so $f(x)\in B\cap D$, impossible. Therefore this case does not exist.

3rd case: $x\in C$ and $y\in A$. This case yields $f(x)\in B\cap D$, impossible, hence it does not exist.

4th case: $x\in C$ and $y\in C$. Then $h(x)=g(x)$ and $h(y)=g(y)$, and so $g(x)=g(y)$, whence $x = y$.

It follows that $x = y$ in every possible case, and so h is injective.

h surjective: Let $y\in B\cup D$. Then $y\in B$ or $y\in D$. If $y\in B$, then $\exists x\in A$, such that $y = f(x) = h(x)$, and if $y\in D$, then $\exists x\in C$, such that $y = g(x) = h(x)$. Therefore whenever $y\in B\cup D$, $\exists x\in A\cup C$, such that $y = h(x)$, and so h is surjective. Therefore h is bijective, and so $A\cup C\approx B\cup D$. ■

3.2.3. Let $n\geq 1$. If $x_1,\ldots, x_n$ are n pairwise distinct elements of $[1,n]$, then

$$[1,n]=\{x_1,\ldots,x_n\}.$$

Proof: We argue by induction on n. For n=1, we have $[1,n]=\{1\}$, and so as $x_1\in[1,n]$, then $x_1=1$, and hence $[1,n]=\{x_1\}$. Therefore the property holds for n=1. Assume that it holds up to n-1 and let's prove it for n. As $n\in[1,n]$, we then have two cases:

1st case: $n\in\{x_1,\ldots,x_n\}$. Then $\exists 1\leq t\leq n$, such that $n=x_t$. As $x_1,\ldots, x_n$ are pairwise distinct and $n=x_t$, then $x_s\neq n$, for all $s\neq t$. But $x_s\leq n$, hence $x_s\leq n-1$, for all $s\neq t$, and so $x_1,\ldots, x_{t-1}$, $x_{t+1},\ldots,x_n$ are n-1 pairwise distinct elements of $[1,n-1]$, whence

$$\{x_1,\ldots, x_{t-1},x_{t+1},\ldots,x_n\}=[1,n-1]$$

by induction hypothesis. It follows that

$$\{x_1,\ldots,x_n\}=\{x_1,\ldots, x_{t-1},x_{t+1},\ldots,x_n\}\cup\{ x_t\}=[1,n-1]\cup\{n\}=[1,n].$$

Therefore the property holds for n in this case.

2nd case: $n\notin\{x_1,\ldots,x_n\}$. Let $1\leq s\leq n$. Then $x_s\neq n$. But $x_s\leq n$, hence $x_s\leq n-1$, and so $x_s\in[1,n-1]$. This implies that $x_1,\ldots, x_{n-1}$ are n-1 pairwise distinct elements of $[1,n-1]$, whence

$$\{x_1,\ldots, x_{n-1}\}=[1,n-1]$$

by induction hypothesis. But $x_n\in[1,n-1]$, hence $x_n\in\{x_1,\ldots, x_{n-1}\}$, which contradicts the fact that $x_1,\ldots,x_n$ are pairwise distinct. Therefore this case does not occur.

It follows that the property holds for n, and so it is true, for all $n\geq 1$. ■

3.2.7. If A is a subset of a finite set E, then A is finite and $\text{card}(A)\leq\text{card}(E)$.

Proof: We argue by induction on $n=\text{card}(E)$. For n=0, we have $E=\varnothing$, by 3.2.4, and so $A=\varnothing$, whence A is finite and $\text{card}(A)=0\leq\text{card}(E)$. Therefore the property holds for n=0. Assume that it holds up to n-1 and let's prove it for n.

Let $f : E\longrightarrow[1,n]$ be a bijection and let $a\in E$, such that $f(a)=n$. Set $F=E-\{a\}$. Then

$$E=F\cup\{a\} \text{ and } F\cap\{a\}=\varnothing.$$

We have

$$[1, n]=f(E)=f(F)\cup f(\{a\})=f(F)\cup\{n\}.$$

As f is injective, then

$$f(F)\cap\{n\}=f(F)\cap f(\{a\})=f(F\cap\{a\})=f(\varnothing)=\varnothing$$

and so

$$f(F)=[1,n-1].$$

But $F\approx f(F)$, by 3.1.2, hence $F\approx[1,n-1]$, and so

F is finite of cardinal n-1.

We have $A\cap F$ is finite of cardinal $\leq n-1$, by induction hypothesis and also $A\cap\{a\}$ is finite of cardinal ≤ 1, because $A\cap\{a\}=\varnothing$ or $A\cap\{a\}=\{a\}$, and as

$$(A\cap F)\cap(A\cap\{a\})=A\cap(F\cap\{a\})=A\cap\varnothing=\varnothing$$

then we get from 3.2.6 that $(A\cap F)\cup(A\cap\{a\})$ is finite and

$$\mathrm{card}((A\cap F)\cup(A\cap\{a\}))=\mathrm{card}(A\cap F)+\mathrm{card}(A\cap\{a\})\leq n-1+1=n=\mathrm{card}(E).$$

But $A=A\cap E=A\cap(F\cup\{a\})=(A\cap F)\cup(A\cap\{a\})$, hence A is finite and $\mathrm{card}(A)\leq\mathrm{card}(E)$. Therefore the property holds for n, and so it is true, $\forall n\geq 0$. ■

4.1.1. If $n\geq 2$ and $a_1,a_2,....,a_n\in E$ and $*$ is associative and commutative, then

$$a_1*a_2*....*a_n = a_{i_1}*a_{i_2}*....*a_{i_n}, \text{ for all } \{i_1,i_2,...,i_n\} = \{1,2,...,n\}.$$

Proof: First we show by induction on n that

$$a_1*a_2*....*a_n = a_1*....*a_{i-1}*a_{i+1}*.....*a_n*a_i,\ \forall 1\leq i\leq n-1.\quad (1)$$

It is true for n = 2, because $a_1*a_2 = a_2*a_1$. Suppose that it is true up to (n-1) and let's show it for n. If i = n-1, then

$$\begin{aligned} a_1*a_2*....*a_n &= (a_1*a_2*....a_{n-2})*(a_{n-1}*a_n) \\ &= (a_1*a_2*....a_{n-2})*(a_n*a_{n-1}) \\ &= a_1*a_2*....a_{n-2}*a_n*a_{n-1}. \end{aligned}$$

Hence the property is true for i=n-1. If $i\neq n-1$, then we get $1\leq i\leq(n-1)-1$, and so

$$a_1*a_2*....*a_{n-1} = a_1*....*a_{i-1}*a_{i+1}*.....*a_{n-1}*a_i.$$

by induction hypothesis. This implies that

$$\begin{aligned} a_1*a_2*....*a_n &= (a_1*a_2*....*a_{n-1})*a_n \\ &= (a_1*....*a_{i-1}*a_{i+1}*.....*a_{n-1}*a_i)*a_n \\ &= (a_1*....*a_{i-1}*a_{i+1}*.....*a_{n-1})*(a_i*a_n) \\ &= (a_1*....*a_{i-1}*a_{i+1}*.....*a_{n-1})*(a_n*a_i) \\ &= a_1*....*a_{i-1}*a_{i+1}*.....*a_{n-1}*a_n*a_i. \end{aligned}$$

Therefore the property is true for all $1\leq i\leq n-1$.

Now we prove the theorem by induction on n, It is true for n=2, because $a_1*a_2 = a_2*a_1$. Suppose that it holds up to (n-1) and let's show it for n. Since $\{i_1,i_2,...,i_n\}=\{1,2,...,n\}$, there exists $1\leq s\leq n$, such that $n = i_s$. Then

$$\{i_1,...,i_{s-1},i_{s+1},...,i_n\} = \{1,...,(n-1)\}$$

and so induction yields that

$$a_1*a_2*....*a_{n-1} = a_{i_1}*....*a_{i_{s-1}}*a_{i_{s+1}}*.....*a_{i_n}.$$

But

$$a_{i_1}*a_{i_2}*....*a_{i_n} = a_{i_1}*....*a_{i_{s-1}}*a_{i_{s+1}}*.....*a_{i_n}*a_{i_s}$$

by (1), hence

$$a_{i_1}*a_{i_2}*....*a_{i_n} = a_1*a_2*....*a_{n-1}*a_{i_s} = a_1*a_2*....*a_{n-1}*a_n.$$

Therefore the property is true for n, and so it is true, for all n≥2. ■

<u>**6.1.1.**</u> The set K=$\mathbb{R}\times\mathbb{R}$, endowed with the following addition and multiplication

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

is a field, such that

(i) $0_K = (0,0)$; (ii) $1_K = (1,0)$; (iii) $-(a,b) = (-a,-b), \forall(a,b)\in K$;

(iv) if $(a,b)\in K-\{0_K\}$, then $(a,b)^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$.

<u>**Proof:**</u> <u>+ is associative:</u> Let $(a,b),(c,d),(x,y)\in K$, then

$$[(a,b)+(c,d)]+(x,y) = (a+c\ ,\ b+d)+(x,y) = ((a+c)+x\ ,\ (b+d)+y)) = (a+(c+x)\ ,\ b+(d+y))$$
$$= (a,b)+(c+x\ ,\ d+y) = (a,b)+[(c,d)+(x,y)]$$

and so + is associative.

<u>+ is commutative:</u> Let $(a,b),(c,d)\in K$, then

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

and so + is commutative.

<u>+ has a neutral element:</u> As $(0,0)\in K$ and + is commutative, then

$$(a,b)+(0,0) = (0,0)+(a,b) = (0+a\ ,\ 0+b) = (a,b)$$

for all $(a,b)\in K$, hence (0,0) is the neutral element for +.

<u>Every element (a,b) of K is invertible, for + :</u> As $(-a,-b)\in K$ and + is commutative, then

$$(a,b)+(-a,-b) = (-a,-b)+(a,b) = (-a+a\ ,\ -b+b) = (0,0)$$

hence (a,b) is invertible for + and $-(a,b)=(-a\ ,-b)$.

<u>× is associative:</u> Let $(a,b),(c,d),(x,y)\in K$, then

$$[(a,b)(c,d)](x,y) = (ac-bd\ ,\ ad+bc)(x,y) = ((ac-bd)x-(ad+bc)y\ ,\ (ac-bd)y+(ad+bc)x)$$
$$= (acx-bdx-ady-bcy\ ,\ acy-bdy+adx+bcx)$$

and

$$(a,b)[(c,d)(x,y)] = (a,b)(cx-dy\ ,\ cy+dx) = (a(cx-dy)-b(cy+dx)\ ,\ a(cy+dx)+b(cx-dy))$$
$$= (acx-ady-bcy-bdx\ ,\ acy+adx+bcx-bdy) = [(a,b)(c,d)](x,y)$$

and so × is associative.

<u>× is commutative:</u> Let $(a,b),(c,d)\in K$, then

$$(a,b)(c,d) = (ac-bd\ ,\ ad+bc) = (ca-db\ ,\ da+cb) = (c,d)(a,b)$$

and so × is commutative.

<u>× has a neutral element:</u> As $(1,0)\in K$ and × is commutative, then

$$(a,b)(1,0) = (1,0)(a,b) = (1\times a-0\times b\ ,\ 1\times b+0\times a) = (a,b)$$

for all $(a,b)\in K$, and so (1,0) is the neutral element for ×.

<u>Every non-zero element (a,b) of K is invertible for ×:</u> We have $(a,b)\neq(0,0)$, hence $a\neq0$ or $b\neq0$, and so $a^2+b^2\neq0$, whence $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})\in K$. As × is commutative, then

$$(a,b)(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})(a,b)$$
$$= (\frac{a^2}{a^2+b^2}+\frac{b^2}{a^2+b^2}\ ,\ \frac{ab}{a^2+b^2}+\frac{-ab}{a^2+b^2}) = (1,0)$$

and so (a,b) is invertible for × and $(a,b)^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$.

<u>× is distributive over +:</u> Let $(a,b),(c,d),(x,y)\in K$, then

$$[(a,b)+(c,d)](x,y) = (a+c\ ,\ b+d)(x,y) = ((a+c)x-(b+d)y\ ,\ (a+c)y+(b+d)x)$$
$$= (ax+cx-by-dy\ ,\ ay+cy+bx+dx)$$
$$= (ax-by\ ,\ ay+bx)+(cx-dy\ ,\ cy+dx)$$
$$= (a,b)(x,y)+(c,d)(x,y)$$

and so × is distributive on the right over +.
Now as × is commutative and distributive on the right over +, then

$$(a,b)[(c,d)+(x,y)] = [(c,d)+(x,y)](a,b) = (c,d)(a,b)+(x,y)(a,b) = (a,b)(c,d)+(a,b)(x,y)$$

and so × is distributive on the left over +. Therefore × is distributive over +, and so K is a field. ■

<u>7.1.3.</u> The multiplication of polynomials is commutative, associative has a neutral element the polynomial $f(x)=1$ and is distributive over the addition of polynomials. In particular $K[x]$ is a commutative unitary ring.

<u>Proof:</u> First, we show that if $\alpha,\beta,\gamma\in K$ and $r,s,t\in \mathbb{N}$, then

(a) $(\alpha x^t)(\beta x^r) = (\alpha\beta)x^{t+r}$ and

(b) $[(\alpha x^t)(\beta x^r)](\gamma x^s) = (\alpha x^t)[(\beta x^r)(\gamma x^s)] = (\alpha\beta\gamma)x^{t+r+s}$.

<u>Proof of (a):</u> We have $\alpha x^t = a_0 + a_1 x + \cdots + a_t x^t$ and $\beta x^r = b_0 + b_1 x + \cdots + b_r x^r$, with

$$a_0 = a_1 = ... = a_{t-1} = 0 \text{ and } a_t = \alpha \text{ and } b_0 = b_1 = ... = b_{r-1} = 0 \text{ and } b_r = \beta.$$

Hence $(\alpha x^t)(\beta x^r) = c_0 + c_1 x + \cdots + c_{t+r} x^{t+r}$, with $c_q = \sum\limits_{i+j=q} a_i b_j$, $\forall 1\leq q\leq t+r$.

Assume that $q<t+r$. Since $i+j=q$, we then have $i\neq t$ or $j\neq r$. But $1\leq i\leq t$ and $1\leq j\leq r$, hence $i\leq t-1$ or $j\leq r-1$, and so $a_i = 0$ or $b_j = 0$, which yields that $a_i b_j = 0$, whence $c_q = 0$. Therefore $c_q = 0$, $\forall q<t+r$, and so $(\alpha x^t)(\beta x^r) = c_{t+r} x^{t+r}$. As $c_{t+r} = a_t b_r = \alpha\beta$, then (a) holds.

<u>Proof of (b):</u> By (a), we have

$$[(\alpha x^t)(\beta x^r)](\gamma x^s)=[(\alpha\beta)x^{t+r}](\gamma x^s)=[(\alpha\beta)\gamma]x^{t+r+s}=(\alpha\beta\gamma)x^{t+r+s}$$

and

$$(\alpha x^t)[(\beta x^r)(\gamma x^s)]=(\alpha x^t)[(\beta\gamma)x^{r+s}]=[\alpha(\beta\gamma)]x^{t+r+s}=(\alpha\beta\gamma)x^{t+r+s}$$

hence $[(\alpha x^t)(\beta x^r)](\gamma x^s) = (\alpha x^t)[(\beta x^r)(\gamma x^s)] = (\alpha\beta\gamma)x^{t+r+s}$.

<u>× is commutative:</u> Let $u,v\in K[x]$ and put

$$u= \sum_{i=0}^{n} a_i x^i, v= \sum_{j=0}^{m} b_j x^j, uv= \sum_{t=0}^{n+m} c_t x^t \text{ and } vu= \sum_{t=0}^{m+n} d_t x^t,$$

with $c_t = \sum\limits_{i+j=t} a_i b_j$ and $d_t = \sum\limits_{j+i=t} b_j a_i$, $\forall 1\leq t\leq n+m$. As $a_i b_j = b_j a_i$, then $c_t = d_t$, for all $1\leq t\leq n+m$, and so $uv = vu$.

<u>× is distributive over +:</u> Let $u,v,w\in K[x]$ and put $u = \sum\limits_{i=0}^{n} a_i x^i$, $v = \sum\limits_{j=0}^{m} b_j x^j$ and $w = \sum\limits_{t=0}^{q} c_t x^t$.

Let $b_{m+1} = \cdots = b_{m+q} = 0$ and $c_{q+1} = \cdots = c_{m+q} = 0$, then

$$v= \sum_{t=0}^{m+q} b_t x^t, w= \sum_{t=0}^{m+q} c_t x^t \text{ and } v+w= \sum_{t=0}^{m+q} (b_t + c_t) x^t$$

and so $uv = \sum\limits_{r=0}^{n+(m+q)} \alpha_r x^r$, $uw= \sum\limits_{r=0}^{n+(m+q)} \beta_r x^r$ and $u(v+w) = \sum\limits_{r=0}^{n+(m+q)} \gamma_r x^r$.

We have

$$\gamma_r = \sum_{i+j=r} a_i (b_j + c_j) = \sum_{i+j=r} (a_i b_j + a_i c_j) = \sum_{i+j=r} a_i b_j + \sum_{i+j=r} a_i c_j = \alpha_r + \beta_r$$

so that $u(v+w) = uv+uw$, and so × is distributive on the left over +. As × is commutative, then $(u+v)w = w(u+v) = wu+wv = uw+vw$, and so × is distributive on the right over +, whence × is distributive over +.

× is associative: Let $u = \sum_{i=0}^{n} a_i x^i$, $v = \sum_{j=0}^{m} b_j x^j$ and $w = \sum_{t=0}^{q} c_t x^t$, then

$$(uv)w = [(a_0+a_1x+\cdots+a_nx^n)v]w = [a_0v+(a_1x)v+\cdots+(a_nx^n)v]w$$
$$= (a_0v)w+[(a_1x)v]w+\cdots+[(a_nx^n)v]w.$$

We have

$$[(a_ix^i)v]w = [(a_ix^i)(b_0+b_1x+\cdots+b_mx^m)]w = (a_ib_0x^i+a_ib_1x^{i+1}+\cdots+a_ib_mx^{i+m})w$$
$$= (a_ib_0x^i)w+(a_ib_1x^{i+1})w+\cdots+(a_ib_mx^{i+m})w$$

and

$$(a_ib_jx^{i+j})w = (a_ib_jx^{i+j})(c_0+c_1x+\cdots+c_qx^q)$$
$$= (a_ib_jx^{i+j})c_0+(a_ib_jx^{i+j})c_1x+\cdots+(a_ib_jx^{i+j})c_qx^q$$
$$= a_ib_jc_0x^{i+j}+a_ib_jc_1x^{i+j+1}+\cdots+a_ib_jc_qx^{i+j+q}$$
$$= (a_ix^i)[b_jc_0x^j+b_jc_1x^{j+1}+\cdots+b_jc_qx^{j+q}]$$
$$= (a_ix^i)[(b_jx^j)(c_0+c_1x+\cdots+c_qx^q)]$$
$$= (a_ix^i)[(b_jx^j)w]$$

hence

$$[(a_ix^i)v]w = (a_ib_0x^i)w+(a_ib_1x^{i+1})w+\cdots+(a_ib_mx^{i+m})w$$
$$= (a_ix^i)(b_0w)+(a_ix^i)[(b_1x)w]+\cdots+(a_ix^i)[(b_mx^m)w]$$
$$= (a_ix^i)[b_0w+(b_1x)w+\cdots+(b_mx^m)w]$$
$$= (a_ix^i)[(b_0+b_1x+\cdots+b_mx^m)w]$$
$$= (a_ix^i)[vw]$$

and so

$$(uv)w = (a_0v)w+[(a_1x)v]w+\cdots+[(a_nx^n)v]w = a_0[vw]+(a_1x)[vw]+\cdots+(a_nx^n)[vw]$$
$$= (a_0+a_1x+\cdots+a_nx^n)[vw] = u[vw].$$

× has a neutral element: We have u×1 = 1×u = u, for all u∈K[x], hence 1 is neutral for ×. Therefore K[x] is a unitary commutative ring ■

Before giving the proof of Taylor's Formula, we show the following Lemma:

Lemma 1: Let f(x)∈K[x]-{0} be a polynomial of degree n≥1. If

$$f(x) = (x-\alpha)v(x)+\beta$$

for some α,β∈K and v(x)∈K[x]-{0}, then $f^{(s)}(x) = sv^{(s-1)}(x)+(x-\alpha)v^{(s)}(x)$, $\forall 1\le s\le n$.

Proof: We argue by induction on s. For s = 1, we have

$$f'(x) = v(x)+(x-\alpha)v'(x) = 1v^{(0)}(x)+(x-\alpha)v^{(1)}(x) = 1v^{(1-1)}(x)+(x-\alpha)v^{(1)}(x)$$

hence the formula is true for s = 1. Suppose that it is true for (s-1) and let's show it for s. By induction hypothesis, we have $f^{(s-1)}(x) = (s-1)v^{(s-2)}(x)+(x-\alpha)v^{(s-1)}(x)$. Since $f^{(s)}(x) = [f^{(s-1)}(x)]'$, we then get

$f^{(s)}(x) = (s-1)[v^{(s-2)}(x)]'+v^{(s-1)}(x)+(x-\alpha)[v^{(s-1)}(x)]'$

$= (s\text{-}1)v^{(s-1)}(x)+v^{(s-1)}(x)+(x\text{-}\alpha)v^{(s)}(x)$
$= sv^{(s-1)}(x)+(x\text{-}\alpha)v^{(s)}(x)$
and so the formula is true for s. Therefore it is true, $\forall 1\leq s\leq n$. ■

Proof of Taylor's Formula: We argue by induction on n. For n = 0, we have f(x) is constant, hence f(x)=f(α), and so the formula is true for n=0. Assume that it holds up to n-1 and let's show it for n. Since α is a root of f(x)-f(α), (x-α) divides f(x)-f(α), by 7.3.2, and so $\exists v(x)\in K[x]$, such that

$$f(x)\text{-}f(\alpha)=(x\text{-}\alpha)v(x).$$

If v(x)=0, then f(x)=f(α), and so deg(f)=0, whence the formula is true in this case. Suppose that v(x)≠0, then f(x)-f(α)≠0, and so deg(f(x)-f(α))=deg(f(x)), by 7.2.2(iii). But

$$\deg(f(x)\text{-}f(\alpha)) = \deg[(x\text{-}\alpha)v(x)] = \deg[(x\text{-}\alpha)]+\deg(v) = 1+\deg(v)$$

by 7.2.1, hence deg(v)=deg(f)-1=n-1, and so the induction hypothesis yields that

$$v(x) = v(\alpha)+\frac{(x-\alpha)}{1!}v'(\alpha)+\cdots+\frac{(x-\alpha)^{n-1}}{(n-1)!}v^{(n-1)}(\alpha).$$

But $f^{(s)}(x) = sv^{(s-1)}(x)+(x\text{-}\alpha)v^{(s)}(x)$, by Lemma 1, hence $f^{(s)}(\alpha) = sv^{(s-1)}(\alpha)$, $\forall 1\leq s\leq n$, and so

$$f(x) = f(\alpha)+(x\text{-}\alpha)v(x) = f(\alpha)+(x\text{-}\alpha)[v(\alpha)+\frac{(x-\alpha)}{1!}v'(\alpha)+\cdots+\frac{(x-\alpha)^{n-1}}{(n-1)!}v^{(n-1)}(\alpha)]$$

$$= f(\alpha)+(x\text{-}\alpha)v(\alpha)+\frac{(x-\alpha)^2}{1!}v'(\alpha)+\cdots+\frac{(x-\alpha)^n}{(n-1)!}v^{(n-1)}(\alpha)$$

$$= f(\alpha)+(x\text{-}\alpha)\frac{f'(\alpha)}{1}+\frac{(x-\alpha)^2}{1!}\frac{f''(\alpha)}{2}+\cdots+\frac{(x-\alpha)^n}{(n-1)!}\frac{f^{(n)}(\alpha)}{n}$$

$$= f(\alpha)+\frac{(x-\alpha)}{1!}f'(\alpha)+\cdots+\frac{(x-\alpha)^n}{n!}f^{(n)}(\alpha).$$

Therefore the formula is true for n, and so it is true, $\forall n\geq 0$. ■

7.5.4. Let $\alpha\in K$ and $f(x)\in K[x]$. If for each natural number t, we define $q_t(x)$ by $q_0(x) = f(x)$ and the inductive relation $q_{t+1}(x)$ is the quotient of the division of $q_t(x)$ by x-α, then

$$f^{(t)}(\alpha) = t!q_t(\alpha), \text{ for all } t\geq 0.$$

Proof: We argue by induction on t. It is true for t=0, because $f^{(0)}(\alpha) = f(\alpha)= 0!q_0(\alpha)$. Suppose that the property holds up to t-1 and let's prove it for t. For each t≥0, let

$$u_t(x) = q_{t+1}(x) \text{ and } g(x) = u_0(x).$$

As $u_{t+1}(x)$ is the quotient of the division of $u_t(x)$ by x-α, then

$$g^{(t-1)}(\alpha) = (t\text{-}1)!u_{t-1}(\alpha)$$

by induction hypothesis. But f(x) = (x-α)g(x)+f(α), hence

$$f^{(t)}(\alpha) = tg^{(t-1)}(\alpha) = t[(t\text{-}1)!u_{t-1}(\alpha)] = t!q_t(\alpha)$$

by lemma 1. Therefore the property holds for t, and so it is true, for all t≥0. ■

References

[1] N. A. Cheaito, Introduction To Algebra, UL-FS1, 2018.

[2] N. A. Cheaito, Solved Problems In Algebra I, UL-FS1, 2018.

[3] C. El Bacha, Cours M1100, Algèbre I, UL-FS2, 2017.

[4] Paul R. Halmos, Naive Set Theory, New York, Springer Verlag, 1974.

[5] T. W. Hungerford, Algebra GTM, Springer, 1974.

[6] K, Jaber & A. Khatib, Math1100, UL-FS3, 2017.

[7] Jean-Louis Kirvine, Théorie des ensembles, Paris, Cassini, 2007.