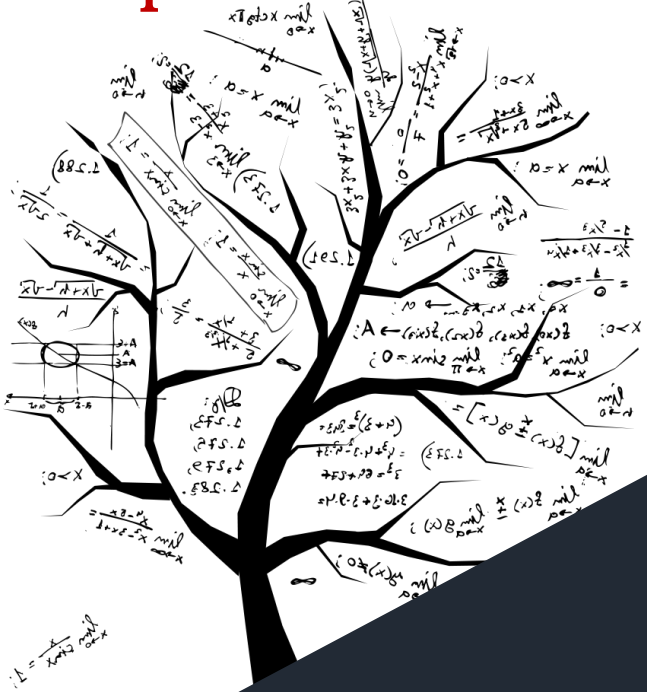
Lebanese University

Faculty of Sciences

Lebanese University
Faculty of Sciences

M1102
Algebra II

Department of Mathematics



Spring Semester

2018 - 2019

Preface

This book is designed to be compatible with the content of the course M1102 of the new curriculum at the faculty of sciences of the Lebanese University.

Ideas are presented in a clear style and the exercises were chosen delicately to deepen the understanding of the required concepts of each semester.

It is a ring in the chain of mathematical subjects required in our curriculum performed according to the new vision.

We hope the students find this text convenient with their understanding skills and enable them to go around elegantly between the ideas and the proofs presented.

Contents

Chapter 1

Binary relations

1.1 Definitions and Notations

After defining sets, collections of objects, it is important to study the kinds of binary relations which can exist between the elements of a set. So we are led to introduce an interesting notion in mathematics, the relations, which are the basic elements of quotient structures, in particular, those defined from $\mathbb{Z}$, and are strongly used in arithmetic and in other applications[1]. The binary relations between the elements of a set E and the elements of a set F may be viewed as properties defined on the set $E \times F$. We are limited in this chapter on binary relations defined on one set.

Definition 1.1.1. Let E be a non empty set and let (p) be a property defined on the set $E \times E$. (p) defines on E a binary relation R as follows: For every x and y in E, we say that x has a relation R with y, we write xRy, if and only if (x, y) verifies (p) in $E \times E$.

$$xRy \Leftrightarrow (x, y) \text{ verifies } (p).$$

The subset of $E \times E$, $\{(x, y); (x, y) \text{ verifies } (p)\}$, denoted by G_R, is said to be the graph of R. A more precise definition and details of graph are presented in chapter 2. We have:

$$xRy \Leftrightarrow (x, y) \in G_R$$

Remark 1.1.1. Two binary relations R and S defined on a set E are said to be equal, we write $R = S$, if they have the same graph. We have in this case the following equivalence:

$$xRy \Leftrightarrow xSy \ \forall x,\ y \in E.$$

[1] We use quotient structure of $\mathbb{Z}$ in the creation of advanced cryptographic systems.

A relation R defined on a set E is clearly defined on any part A of E. This is the restriction of R on A. The negation of R, denoted by $\not R$, is the relation defined on E by:

$$x \not R y \Leftrightarrow (x, y) \notin G_R \text{ for every } x, y \in E.$$

Example 1.1.1. 1. The equality (or the identity) defined trivially on a set. (This relation is not always obviously verified!)

$$\left(\sqrt{2}+\sqrt{3} = \sqrt{5+2\sqrt{6}}, \sqrt{2-\sqrt{3-x+\sqrt{2x+1+\sqrt{x^4}}}} = 0,\ x \leq 0.\right)$$

2. The usual order defined on $\mathbb{R}$. $\pi \leq 4$, $\sqrt{2} > 1$.

3. Let $p \in \mathbb{Z}$. We define on $\mathbb{Z}$ the binary relation R_p by:

$$x R_p y \Leftrightarrow p \text{ divides } x - y.$$

This is the congruence relation modulo p.

4. Let f be a mapping defined from a set E into a set F. We define on E the binary relation R_f by:

$$\forall x, y \in E;\ x R_f y \Leftrightarrow f(x) = f(y).$$

1.2 Properties

Definition 1.2.1. A relation R defined on a set E is said to be reflexive if xRx for every element x in E.

Example 1.2.1. The equality, the relations R_p and R_f defined in the above examples are reflexive. The relation $<$ (less than strictly) defined on $\mathbb{R}$ is not reflexive. It is a relation R verifying $x \not R x\ \forall x \in \mathbb{R}$. Such a relation is said to be antireflexive[2].

Exercise 1.2.1. R is a relation defined on a set E. We define the subset F of E formed by the elements $y \in E$ such that the elements $x \in E$ having relation with y are the elements verifying $x \not R x$. Show that $F = \emptyset$.

Definition 1.2.2. A relation R defined on a set E is said to be symmetric if for every elements x and y of E, we have $xRy \Rightarrow yRx$.

[2]Do not confuse between a non reflexive relation and an antireflexive one.

Example 1.2.2. The equality, the relation R_p and R_f are all symmetric. $\leq$ is not a symmetric relation.

Definition 1.2.3. A relation R defined on a set E is said to be antisymmetric if for every elements x and y of E, we have: (xRy and yRx) $\Rightarrow x = y$

Example 1.2.3. $\leq$ is an antisymmetric relation.

Remark 1.2.1. Note that a relation can be symmetric and antisymmetric at the same time. Also, it can be neither symmetric nor antisymmetric at the same time.

Definition 1.2.4. A relation R defined on a set E is said to be transitive if for every elements x, y and z of E, we have: xRy and $yRz \Rightarrow xRz$.

Remark 1.2.2. It is important to remark that transitivity does not give the sense of circulation, that is, we don't have: zRx instead of xRz in the definition. If we call a circular relation any relation R verifying xRy and $yRz \Rightarrow zRx$, we get the following fact:

Exercise 1.2.2. Let R be a reflexive relation. Then R is circular if and only if R is symmetric and transitive.

We treat in the sequel interesting families of relations, the order relations and the equivalence relations.

1.3 Order Relations

Definition 1.3.1. A relation$R$ defined on a set E is said to be an order relation if R is reflexive, antisymmetric and transitive.

Example 1.3.1. The relation $\leq$ defined on $\mathbb{R}$, the relation "division" defined on $\mathbb{N}$, the inclusion $\subseteq$ defined on the set of parts of a set E, are all order relations.

To simplify, an arbitrary order relation defined on a set is often denoted by $\leq$ if there is no any confusion. (Sometimes, we write $x < y$ to say that $x \leq y$ and $x \neq y$).

The couple $(E, \leq)$ denotes a set on which we define an order relation$\leq$, E is a set ordered by $\leq$. Two elements x and y of E are said to be comparable by $\leq$ if we have $x \leq y$ or $y \leq x$. If all the elements of E are pairwise comparable, $\leq$ is called a total order relation and E is totally ordered by $\leq$, otherwise, $\leq$ is called a partial order relation. We give essentially in this paragraph a collection of notions strongly used in any branch of the order relations theory.

Definition 1.3.2. Let E be a set endowed with an order relation $\leq$ and let a be an element of E.

(i) a is said to be maximal element (resp. minimal) in E if we have: $a \leq x \Rightarrow a = x$ (resp. $x \leq a \Rightarrow a = x$) for every $x \in E$.

(ii) a is said to be greatest element (resp. smallest element) if we have: $x \leq a$ (resp. $a \leq x$) for every $x \in E$.

Remark 1.3.1. A greatest element (resp. smallest element) of an ordered set E when it exists, is unique.

Obviously, a greatest element is maximal and a smallest element is minimal. The reciprocal is not true. These notions coincide in the case of a total order. To avoid confusion between these notions in the general case, we give the following example:

Example 1.3.2. Consider the set $P(E)$ ordered by inclusion where $E = \{1, 2, 3\}$. The parts $\{1, 2\}$, $\{2, 3\}$, $\{1, 3\}$ are the maximal elements in $\big(P(E) - \{E\}, \subseteq\big)$.

Remark 1.3.2. $(\mathbb{R}, \leq)$ has neither maximal element nor minimal element.

Definition 1.3.3. Let E be a set endowed with an order relation $\leq$ and let A be a part of E and a an element of E.

(i) a is said to be upper bound (resp. lower bound) of A in E if we have: $x \leq a$ (resp. $a \leq x$) for every $x \in A$.

(ii) a is said to be least upper bound (resp. greatest lower bound) if a is the smallest upper bound (resp. greatest lower bound).

Remark 1.3.3. The least upper bound (resp. greatest lower bound) of a part A is not necessarily an element of A. ($]1, 2[$ in $(\mathbb{R}, \leq)$.)

Definition 1.3.4. Let f be a mapping from an ordered set $(E, \leq)$ into another ordered set $(F, \leq)$.

(i) f is said to be an increasing mapping if we have:

$$x \leq y \Rightarrow f(x) \leq f(y) \ \forall x, y \in E.$$

(ii) f is said to be a decreasing mapping if:

$$x \leq y \Rightarrow f(y) \leq f(x) \ \forall x, y \in E.$$

(iii) f is said to be isomorphism if f is bijective and if:

$$x \leq y \Leftrightarrow f(x) \leq f(y)\ \forall x, y \in E.$$

Two ordered sets are said to be isomorphic if we may define an isomorphism between these two sets. It is possible in general to define many isomorphisms between two isomorphic ordered sets. An isomorphism defines so a sort of "superposition" between two given structures. This superposition is made in a unique way in the case of a well order relation. The notion of the well order relations is the first step towards the ordinals theory.

Definition 1.3.5. An order relation $\leq$ defined on a set E is said to be a well order relation if any non empty part of E has a smallest element. We say that E is well ordered.

Remark 1.3.4. Every well ordered relation is totally ordered. The converse is not true.

Example 1.3.3. The usual order of $\mathbb{N}$ is a well order (See 3).

Exercise 1.3.1. Show that the unique isomorphism from $(\mathbb{N}, \leq)$ into $(\mathbb{N}, \leq)$ is the identity.

Proposition 1.3.1. Let $(E, \leq)$ and $(F, \leq)$ be two isomorphic ordered sets. We suppose that E is well ordered. Then there exists a unique isomorphism from E into F.

Proof. Let f and g be two isomorphisms from E into F. We define $A = \{x \in E; f(x) \neq g(x)\}$. Suppose to the contrary that A is not empty. It admits then a smallest element, set a. We have: $f(a) \neq g(a)$. We suppose,without loss of generality, that $f(a) < g(a)$. g is surjective and $f(a) \in F$, then there exists $b \in E$ such that $g(b) = f(a)$. We have $g(b) = f(a) < g(a)$, then $b < a$ and then $b \notin A$, hence $f(b) = g(b)$. We get $f(b) = f(a)$, thus $b = a$ since f is injective. Consequently, $A = \emptyset$ and $f = g$. □

1.4 Equivalence Relations

Definition 1.4.1. A relation R defined on a set E is said to be an equivalence relation if R is reflexive, symmetric and transitive.

Exercise 1.4.1. Verify that R_p and R_f defined above, are equivalence relations.

A well illustration of the notion of an equivalence relation defined on a set is that of a school. The relation "be in the same class" is an equivalence relation defined on the set of students of this school. In fact, this relation is clearly reflexive, symmetric. If in addition, we know that two students a and b are in the same class and that b and c are in the same class also, we may deduce (by a subtle reasoning) that a, b and c are all in the same class, and then the relation is transitive. The class of a student a may be defined as the set of all students having relation with a. If we choose two arbitrary students, their classes are either equal or disjoint.By this relation, the set of students is partitioned into classes, the set of classes will be called the quotient set by the equivalence relation.To each student is associated a unique class, this correspondence is called the canonical surjection. Reciprocally, an arbitrary partition of the students into classes gives always the definition of of the equivalence relation: "be in the same class". These obvious remarks are all what we can say on an equivalence relation in general.

Definition 1.4.2. Let R be an equivalence relation defined on a non empty set E. For every $x \in E$, we define the equivalence class of x by:

$$\bar{x} = \{y \in E;\ xRy\}.$$

The set of the equivalence classes of the elements of E is said to be the quotient set of E by R. It is denoted by E/R.

Remark 1.4.1. $x \in \bar{x}$ for every $x \in E$ then $\bar{x} \neq \emptyset$. For every $y, z \in \bar{x}$, we have: yRz. In fact, we have: yRx and xRz then yRz. Similarly, if xRy then $\bar{x} = \bar{y}$. In fact, it is sufficient to show that $\bar{x} \subseteq \bar{y}$. Let $x \in \bar{x}$, we have zRx, but xRy, then zRy and $z \in \bar{y}$.

Exercise 1.4.2. Consider the relation R_f defined from a mapping f from E into F. Let $x \in E$. Show that $\bar{x} = f^{-1}(f(x))$.

Proposition 1.4.1. Let R be an equivalence relation defined on a non empty set E. For each $x, y \in E$, we have: $\bar{x} = \bar{y}$ or $\bar{x} \cap \bar{y} = \emptyset$.

Proof. Suppose that $\bar{x} \neq \bar{y}$. In this case, $\bar{x} \cap \bar{y} = \emptyset$, since otherwise, there exists $z \in \bar{x} \cap \bar{y}$ and we have: xRz and zRy, then xRy and $\bar{x} = \bar{y}$, a contradiction. □

Let I be a nonempty set. For all $i \in I$, we suppose that F_i is a well-defined set. The collection of sets F_i, $i \in I$, is said to be sa family of sets indexed by I and denoted by $F_{ii\in I}$.

Definition 1.4.3. Let E be a set, and let $(F_i)_{i\in I}$ be a family of subsets of E. $(F_i)_{i\in I}$ is said to be a partition of E if:

(a) $F_i \neq \emptyset$ for all $i \in I$.

(b) $F_i \cap F_j = \emptyset$ for all $i, j \in I$.

(c) $\cup_{i\in I} F_i = E$.

Corollary 1.4.1. Let R be an equivalence relation defined on a non empty set E. The family $\{\bar{x}\}_{x\in E/R}$ is a partition of E.

Proof. We may verify easily that this family satisfies the conditions of a partition, using the above proposition and the fact that $x \in \bar{x}$ for every $x \in E$. □

By the following proposition, we complete the proof of our remark that an equivalence relation defined on a set E is exactly a partition defined on the same set.

Proposition 1.4.2. Let E be a non empty set and let $\{F_i\}_{i\in I}$ be a partition of E. There exists an equivalence relation R defined on E such that the classes of R are exactly the members of the partition.

Proof. Let R be the relation defined on E by:

$$\forall x, y \in E;\ xRy \Leftrightarrow \exists i \in I \text{ such that } x, y \in F_i.$$

This relation is reflexive, symmetric. To verify that it is transitive, let x, y and z be three elements of E such that xRy and yRz. $\exists i, j \in I$ such that $x, y \in F_i$ and $y, z \in F_j$. Thus $y \in F_i \cap F_j$ and $F_i \cap F_j \neq \emptyset$, so $F_i = F_j$. Consequently, $x, y, z \in F_i$, and xRz. R is then an equivalence relation. Now, let's show that $E/R = \{F_i\}_{i\in I}$. Let $\bar{x} \in E/R$, $x \in E$, then $\exists i \in I$ such that $x \in F_i$. We have $\bar{x} = F_i$. In fact it is sufficient to to prove that $\bar{x} \subseteq F_i$, for this, let $y \in \bar{x}$. We have xRy, $\exists j \in I$ such that $x, y \in F_j$. Then, $x \in F_i \cap F_j$ and $F_i \cap F_j \neq \emptyset$, so $F_i = F_j$. Hence, $y \in F_i$ and so $\bar{x} \subseteq F_i$. In the other hand, for every $i \in I$, $F_i \neq \emptyset$, then $\exists x \in F_i$, we get $\bar{x} = F_i$. □

We end this paragraph by using equivalence relation in the establishment of a remarkable property, the canonical decomposition of a mapping.

Definition 1.4.4. Let R be an equivalence relation defined on a non empty set E. The canonical surjection defined by R is the mapping p which associates to each $x \in E$ its class $\bar{x} \in E/R$.

Proposition 1.4.3. Let f be a mapping defined from a set E into a set F. Then

$$\begin{aligned} \varphi : E/R_f &\mapsto f(E) \\ \bar{x} \quad &\mapsto \varphi(\bar{x}) = f(x) \end{aligned}$$

is a bijective mapping. Where R_f is the equivalence relation associated to f.

Proof. φ is well defined injective mapping. In fact, let $\bar{x}, \bar{y} \in E/R_f$. We have: $\bar{x} = \bar{y} \Leftrightarrow xR_fy \Leftrightarrow f(x) = f(y) \Leftrightarrow \varphi(\bar{x}) = \varphi(\bar{y})$. It is surjective by construction. Then φ is bijective. □

Proposition 1.4.4. (Canonical decomposition) Let f be a mapping from a set E into a set F. Then $f = i \circ \varphi \circ p$, where p is the canonical surjection, φ is the bijection defined in the above proposition, and i is the canonical injection from $f(E)$ into E. Moreover, if $f = i \circ \varphi' \circ p$, then $\varphi = \varphi'$.

Proof. Left to the reader. □

Exercises and Problems

1. Let E be a non-empty set and let F be an ordered set. Let Ω be the set of all mappings of E to F. Define on Ω the relation R by:

$$uRv \Leftrightarrow u(x) \leq v(x),\ \forall x \in E.$$

(a) Show that R is an ordering relation on Ω.

(b) Give an example of E and F, such that F is totally ordered but Ω is not totally ordered by R.

2. Let

$$A = \{x_n = \frac{2}{n} + (-1)^n;\ n \in \mathbb{N}^*\}.$$

Show that $Sup_{\mathbb{Q}}(A) = 2$ and $Inf_{\mathbb{Q}}(A) = -1$.

3. Does the set

$$B = \{x_n = \frac{2}{n};\ n \in \mathbb{N}^*\}$$

have a least upper bound or a greatest lower bound in $\mathbb{Q}^*$?

4. Let $E = \mathbb{N} - \{0, 1\}$ and let R be the ordering defined on E by

$$xRy \Leftrightarrow x\ divides\ y.$$

Show that E has no maximal elements and that every prime number is a minimal element of E.

5. Let $f : E \to F$ be a mapping of a set E to an ordered set F. Let R be the relation defined in E by

$$xRy \Leftrightarrow f(x) \leq f(y).$$

Show that:

(a) R is reflexive and transitive.

(b) R is an ordering relation on E if and only if f is injective.

6. Let $f : E \to F$ be a mapping from a set E to an ordered set F. Define on F the relation R by

$$xRy \Leftrightarrow \exists a \in E,\ \text{such that } x \leq f(a) \text{ and } f(a) \leq y.$$

(a) Show that R is antisymmetric and transitive.

(b) Prove that R is an ordering relation on F if and only if f is surjective.

7. Consider a mapping f of a set E to a set F. Let R be the relation defined on $P(E)$ by

$$ARB \Leftrightarrow A = f^{-1}(f(B)).$$

(a) Show that R is reflexive if and only if f is injective.

(b) Show that if $A, B \in P(E)$ and ARB, then $B \subseteq A$. Deduce that R is antisymmetric.

(c) Show that if $A, U \in P(E)$ and $A = f^{-1}(U)$, then ARA.

(d) Show that R is transitive.

(e) Deduce that if f is injective, then R is an ordering relation.

8. Let A be a set and E be a non-empty subset of $\mathcal{P}(A)$. Show that the relation R defined on E by

$$XRY \Leftrightarrow \text{there exists a bijection from } X \text{onto } Y$$

is an equivalence relation on E.

9. Let $f : \mathbb{R} \to \mathbb{R}$ be the mapping defined by

$$f(x) = 2x^2 - 3.$$

Let R_f be the equivalence relation associated with f. Find the classes $\overline{0}$ and $\overline{1}$.

10. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = x^2 - 2x + 3$, $\forall x \in \mathbb{N}$. Let R be the equivalence relation associated with f.

(a) Find the classes $\overline{0}$ and $\overline{1}$ modulo R.

(b) Find a if $\overline{a}$ is a singleton.

11. Let E and F be two sets and let R (resp. S) be an equivalence relation on E (resp. F). Let $p : E \to E/R$ (resp. $q : F \to F/S$) be the canonical surjection of E (resp. F) onto E/R (resp. F/R). Show that if $f : E \to F$ is a mapping of E to F, then the following properties are equivalent:

(a) There exists a mapping $g : E/R \to F/S$, such that $g \circ p = q \circ f$.

(b) The implication

$$xRy \to f(x)Sf(y)$$

is true, $\forall x, y \in E$.

12. A relation R on a set E is said to be **circular** if the following implication is true, $\forall a, b, c \in E$

$$[aRb \text{ and } bRc] \Rightarrow cRa.$$

Show that if R is reflexive and circular, then R is an equivalence relation on E. Is the converse true?

13. Let E be a non-empty set and let Δ be the diagonal of E^2, i.e

$$\Delta = \{(x, x); x \in E\}.$$

For each subset A of $E \times E$, set

$$A^{-1} = \{(x, y); (y, x) \in A\}$$

and

$$A \circ A = \{(x, y); \exists z \in E, \text{such that } (x, z) \in A \text{and } (z, y) \in A\}.$$

Let R be a binary relation on E and let G be the graph of R. Show that

(a) If R is reflexive and transitive, then $G \circ G = G$.

(b) R is an ordering relation on E if and only if

$$G \circ G = G \text{ and } G \cap G^{-1} = \Delta.$$

(c) R is an equivalence relation on E if and only if

$$G \circ G = G,\ G = G^{-1} \text{ and } Pr_1(G) = E.$$

14. Let R be the relation defined in $\mathbb{Q}$ by

$$xRy \Leftrightarrow (x - y) \in \mathbb{Z}.$$

Show that R is an equivalence relation on $\mathbb{Q}$ and find the class $\overline{0}$ modulo R.

15. Let P be the set of all the points $M(x, y)$ in the plane Oxy. Let R be the relation defined in P by

$$M(x, y)\ R\ M'(x', y') \Leftrightarrow x^2 + y^2 = x'^2 + y'^2.$$

(a) Show that R is an equivalence relation on P.

(b) Find the class modulo R of the point $A(a, b)$ of the plane.

16. In $\mathbb{R}^{*+}$, we define the relation R by

$$xRy \Leftrightarrow xln(y) = yln(x).$$

(a) Show that R is an equivalence relation.

(b) Describe the quotient set.

(c) find the canonical decomposition of the following mapping:

$$\begin{aligned} f : \mathbb{R}^{*+} &\mapsto \mathbb{R} \\ x \quad &\mapsto \frac{ln(x)}{x} \end{aligned}$$

17. A relation R defined on a set E is said to be connected if:

(a) $\forall x \in E;\ \exists u \in E$ such that xRy.

(b) R is symmetric.

(c) $\forall x, y, z \in E$ we have: xRy and $yRz \Rightarrow zRx$.

Show that R is an equivalence relation if and only if R is connected.

18. Let E be a set endowed with an equivalence relation R. Let f be a mapping defined from E into E such that $f(\bar{x}) \subseteq \bar{x}$ for every $x \in E$.

(a) Show that $xRf(x)$ for every $x \in E$.

(b) Show that $f(\bar{x}) \subseteq \bar{f(x)}$.

(c) Suppose that f is surjective.

i. Prove that $f(\bar{x}) = \bar{x}$.

ii. Deduce that the mapping

$$\begin{aligned} \varphi : E/R &\mapsto E/R \\ \bar{x} \quad &\mapsto \varphi(\bar{x}) = \bar{f(x)} \end{aligned}$$

is bijective.

19. Let f and g be two mappings defined from a set E into a set F such that $f(x) \neq g(x)$ for every $x \in E$. We define on E the relation R by $xRy \Leftrightarrow f(x) = g(y)$.

(a) A part L of E is said to be free if $x \not R y$ for every x and y in L.

i. Let $A \subseteq E$. Show that A is free if and only if $f(A) \cap g(A) = \emptyset$.

ii. Let $z \in F$ and let $A = f^{-1}(z)$. Show that A is a free part.

iii. Let $x, y, z \in E$ be such that xRz and yRz. Show that $\{x, y\}$ is a free part.

(b) A part C of E is said to be complete if $\{x, y\}$ is not free whenever x and y are two distinct elements of C. Let A be a complete part of E.

i. Let $x, y \in A$ be such that xRy. Show that $\forall z \in A$, we have yRz and zRx.

ii. Deduce that a complete part of E contains at most 3 elements.

20. Let $(E, \leq)$ be an ordered non empty set and let f be an increasing mapping from E to E verifying $x \leq f(x) = f(f(x))$ for every $x \in E$. Set $F = \{x \in E,\ x = f(x)\}$.

(a) Show that for every $x \in E$ the set $F_x = \{y \in F,\ x \leq y\}$ is not empty.

(b) Show that $f(x)$ is a smallest element of F_x.

(c) Let g be a mapping from E to E and let G be a part of E such that the set $G_x = \{y \in G,\ x \leq y\}$ is not empty for every $x \in E$ and admits $g(x)$ as smallest element.

i. Prove that $x \leq g(x)$ for every $x \in E$.

ii. Prove that $G = \{x \in E,\ x = g(x)\}$.

iii. Let $x, y \in G$ be such that $x \leq y$. Show that $G_y \subseteq G_y$. Deduce that g is increasing.

iv. Show that $\forall x \in E$ we have $g(g(x)) \subseteq G_x$. Deduce that $g(g(x)) = g(x)$.

Chapter 2

Relations and Graphs

2.1 Symmetric Relations

Many structures in many domains rise from symmetric relations. Some of these structures are deep and rich in theoretical mathematical properties, even though a symmetric relation in its own state is a simple concept.

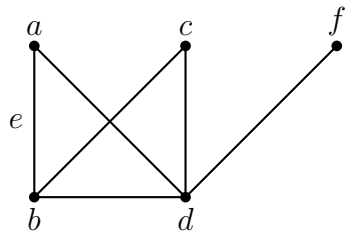
A very simple illustration of these structures is the friendship example: given a set V of persons, we define the symmetric relation R: "being a friend". At the first glance, V endowed with this relation is a very simple structure. But, through applying on it some tools from algebraic theories, the following elegant result, called the *friendship theorem*, emerges:

Theorem 2.1.1. If any two persons in V have exactly one common friend, then there is a person in V who is the friend of everyone in V.

Definition 2.1.1. Let R be a symmetric relation defined on a finite set V. V endowed with the relation R is said to be a graph. A graph is often denoted by the capital letter G. It is defined by the two sets: $V = V(G)$, called the set of vertices of G, and $E = E(G) = \{\{x, y\}; xRy\}$, called the set of edges of G. So a vertex v of G is simply an element of V, while an edge is a pair $\{x, y\} \subseteq V$ such that xRy. To simplify, we write $e = xy$ instead of $\{x, y\}$ where e is an edge of G.

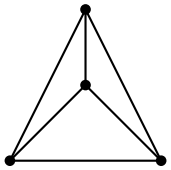
Graphs, in general, are supposed to be defined by antireflexive relations, that is $x\not{R}x\ \forall x \in V$. The order of a graph G, denoted by $v(G)$, is the number of its vertices and the size of G, denoted by $e(G)$, is the number of its edges. Graphs may be illustrated by points and lines.

Example 2.1.1. Given the graph G:



$V(G) = \{a, b, c, d, f\}$
$E(G) = \{ab, ad, bc, bd, cd, df\}$
$v(G) = 5$, $e(G) = 6$, $e = ab = ba$

Example 2.1.2. G is a complete graph if $xy \in E(G)\ \forall x, y \in V(G)$.



G=K_4

Definition 2.1.2. Let G be a graph. A graph H is said to be subgraph of G if

$$V(H) \subseteq V(G)$$
$$E(H) \subseteq E(G)$$

H is said to be an "induced subgraph of G" if

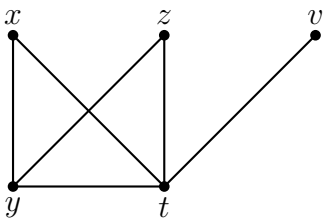
$$xy \in E(H) \Leftrightarrow xy \in E(G) \qquad \forall x, y \in V(H)$$

H is also called the subgraph of G induced by $A = V(H)$; we write:

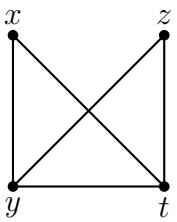
$$H =< A >$$

. H is said to be a "spanning subgraph of G" if $V(H) = V(G)$.

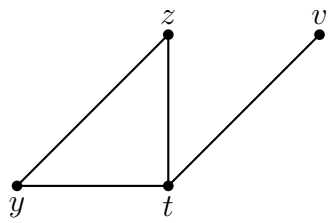
Example 2.1.3.



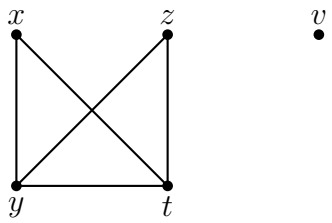
G



H: subgraph of G



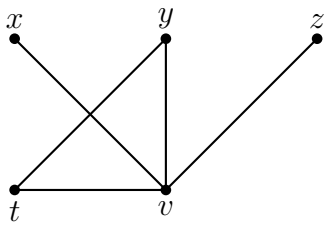
H_1: induced subgraph of G



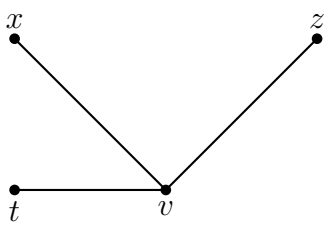
H_2: spanning subgraph of G

Notation 2.1.1. Let G be a graph, $v \in G$, $e = ab \in E(G)$. $G - v$ is the subgraph of G induced by $V(G) \setminus \{v\}$. $G - e$ is the subgraph of G obtained by deleting the edge e. Let $x, y \in G$ such that $xy \notin E(G)$, then $G + xy$ is the graph obtained from G by adding the edge xy.

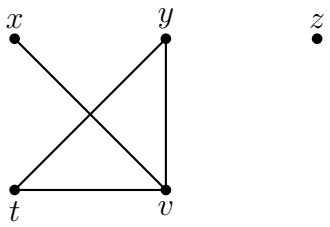
Example 2.1.4.



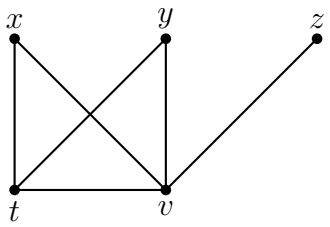
G



$G - y$



$G - vz$



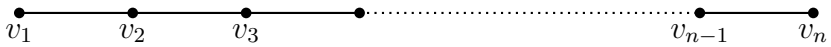
$G + xt$

Definition 2.1.3. A path $\mathcal{P}$ is a graph verifying:

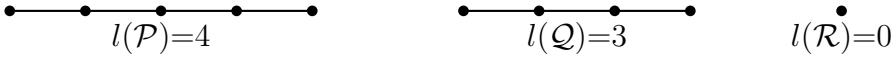
$$V(\mathcal{P}) = \{v_1, v_2, \ldots, v_n\}$$

$$E(\mathcal{P}) = \{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n\}$$

We write $\mathcal{P} = v_1v_2 \ldots v_{n-1}v_n$.



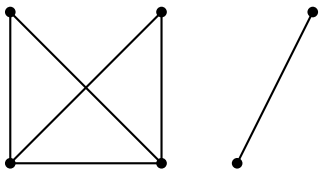
v_1 is the origin of $\mathcal{P}$ and v_n is its end. $\mathcal{P}$ is a v_1v_n-path. The length of a path is the number of its edges.



Definition 2.1.4. Let G be a graph. A path $\mathcal{P}$ in G is a subgraph of G. G is said to be connected if it contains an xy-path $\forall x, y \in V(G)$. A connected component of a graph G is an induced connected subgraph maximal with respect to the inclusion.

Definition 2.1.5. Let $x, y \in V(G)$. The distance between x and y in a connected graph G, denoted by $d(x, y)$, is the length of the shortest xy-path in G. The xy-path $\mathcal{P}$ such that $l(\mathcal{P}) = d(x, y)$ is called an xy-geodesic. The diameter of G is $d(G) = max\{d(x, y); x, y \in G\}$.

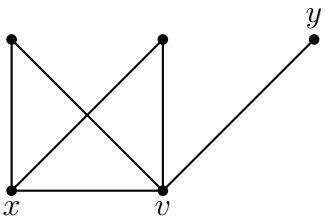
Example 2.1.5. Consider the following graph G:



Then,

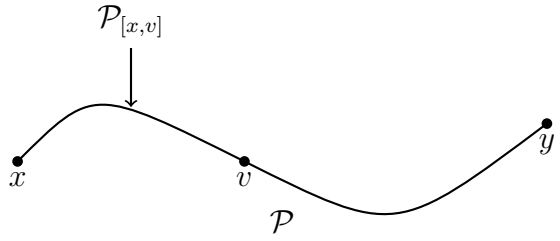
C_1: connected component of G C_2: connected component of G

Example 2.1.6. G is a connected graph:



$d(x, y) = 2$ and $(P) = xvy$ ia a geodesic in G. $d(G) = 2$.

Notation 2.1.2. Let $\mathcal{P}$ be an xy-path and $v \in \mathcal{P}$. $\mathcal{P}_{[x,v]}$ is the subpath of $\mathcal{P}$ of ends x and v.



Exercise 2.1.1. Let $\mathcal{P}$ be an xy-geodesic of a connected graph G ($x, y \in G$) and let $v \in \mathcal{P}$. Show that $\mathcal{P}_{[x,v]}$ is an xv-geodesic.

Exercise 2.1.2. Let G be a connected graph and let $x, y, z \in G$. Show that $d(x, y) \leq d(x, z) + d(z, y)$.

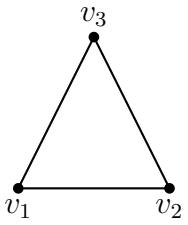
Definition 2.1.6. A cycle is a graph C verifying:

$$V(C) = \{v_1, v_2, \ldots, v_n\} \qquad n \geq 3$$

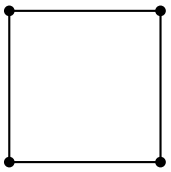
$$E(C) = \{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n, v_nv_1\}$$

We write $C = v_1v_2 \ldots v_n$. The length of C, $l(C)$, number of edges of C.

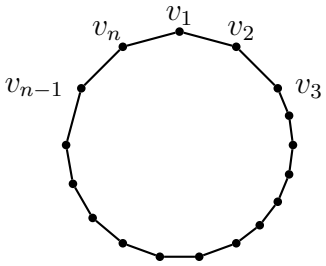
Example 2.1.7. C: triangle, $l(C) = 3$:



C: square, $l(C) = 4$:

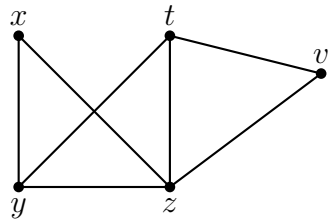


$l(C) = n$:



A cycle is said to be even if its length is even and odd if its length is odd.

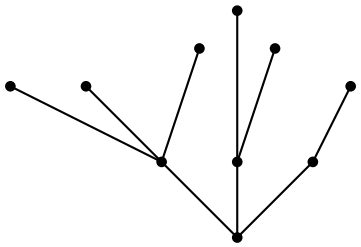
Definition 2.1.7. A cycle of a graph G is a subgraph of G which is a cycle.



G

$ytvz$ is a square in G, $xytvz$ is a cycle in G.

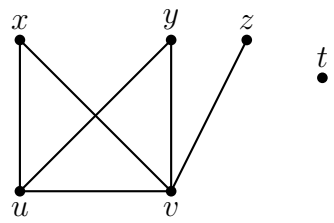
A connected graph without cycles is said to be a tree.



Tree

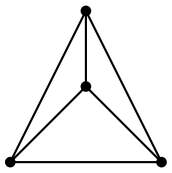
Definition 2.1.8. Let G be a graph and let $v \in G$. The neighborhood of v is the set $N(v) = \{x \in G; vx \in E(G)\}$. For more precision, we may write $N_G(v)$. The degree of v is $d(v) = d_G(v) = |N_G(v)|$. G is said to be regular or k-regular if $d(x) = k \ \forall x \in V(G)$.

Example 2.1.8.



G

$N(v) = \{u, x, y, z\}$, $d(v) = 4$
$N(t) = \emptyset$, $d(t) = 0$ (isolated vertex)



3-regular graph

Notation 2.1.3. G is a graph.
$\delta(G) = min\{d(v); v \in G\}$.
$\Delta(G) = max\{d(v); v \in G\}$.

Theorem 2.1.2. *(Euler,1736)* Let G be a graph. We have:

$$\sum_{v \in G} d_G(v) = 2e(G) \tag{i.2}$$

Proof. We argue by induction on $e(G)$. If $e(G) = 0$, then G has no edges and so $d(v) = 0\ \forall x \in G$, the equality (2.1) holds. Suppose that the equality holds for graphs of size s and suppose that $e(G) = s+1$. Let $e = xy \in E(G)$. Set $G' = G - e$. $e(G') = s$, then the equality (2.1) holds for G'. We have:

$$\begin{aligned}
&\sum_{v \in G'} d_{G'}(v) = 2e(G') \\
\Rightarrow &\sum_{v \neq xy} d_{G'}(v) + d_{G'}(x) + d_{G'}(y) = 2(e(G) - 1) \\
\Rightarrow &\sum_{\substack{v \in G \\ v \neq xy}} d_G(v) + (d_G(x) - 1) + (d_G(y) - 1) = 2e(G) - 2 \\
\Rightarrow &\sum_{v \in G} d_G(v) - 2 = 2e(G) - 2
\end{aligned}$$

Thus $\sum_{v \in G} d_G(v) = 2e(G)$. □

Corollary 2.1.1. Let G be a graph. Then $|\{v; d(v) \text{ is odd}\}|$ is even.

Proof. Remark that

$$\sum_{v \in G} d(v) = 2e(G) \quad \text{is even.}$$

So,

$$\sum_{\substack{v \in G \\ d(v)\ odd}} d(v) + \sum_{\substack{v \in G \\ d(v)\ even}} d(v) \quad \text{is even.}$$

Thus

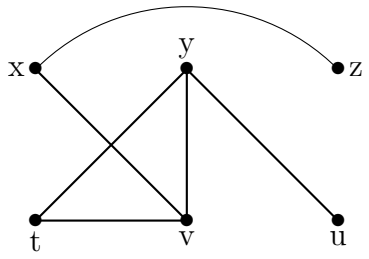
$$\sum_{\substack{v\in G \\ d(v)\ odd}} d(v) \quad \text{is even.}$$

Then $|\{v; d(v) \text{ is odd}\}|$ is even.

□

Definition 2.1.9. Let G be a graph. A subset $\zeta \subseteq V(G)$ is said to be stable if $xy \notin E(G)\ \forall x, y \in \zeta$. The stability of G is $\alpha(G) = max\{|\zeta|; \zeta \text{ stable in } G\}$. The chromatic number of G, denoted by $\chi(G)$, is the minimum number of stables in G whose union is $V(G)$. $\chi(G) = t$ means $\exists\ \zeta_1, \zeta_2, \ldots, \zeta_t$ stables in G such that $V(G) = \zeta_1 \cup \zeta_2 \cup \ldots \cup \zeta_t$ and t is minimal for this property.

Example 2.1.9.

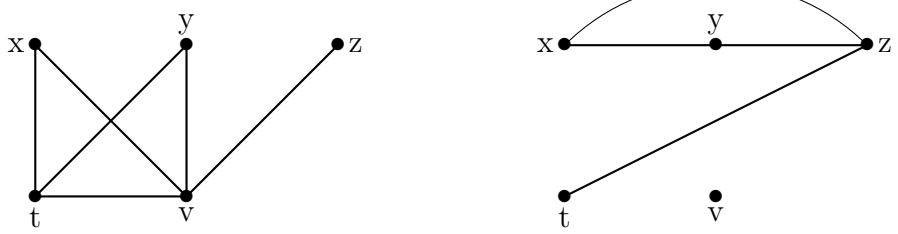


$*$ $\{x, y\}$ is a stable in G.
$*$ $\{t, z, u\}$ is a maximal stable in G.
$*$ $\alpha(G) = 3$.
$*$ $\chi(G) = 3$. $V(G) = S_1 \cup S_2 \cup S_3$, $S_1 = \{x, t\}$, $S_2 = \{y, z\}$, $S_3 = \{v, u\}$.
$*$ $\chi(G) \neq 2$.

Definition 2.1.10. Let G be a graph. The complement of G, denoted by $\bar{G}$, is the graph defined by:

$$V(\bar{G}) = V(G)$$
$$E(\bar{G}) = \{xy; xy \notin E(G)\}$$

Example 2.1.10.



G $\bar{\mathbf{G}}$

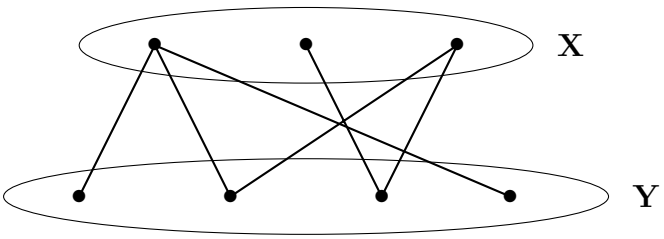
2.2 Bipartite graph

Definition 2.2.1. A graph G is said to be bipartite if:

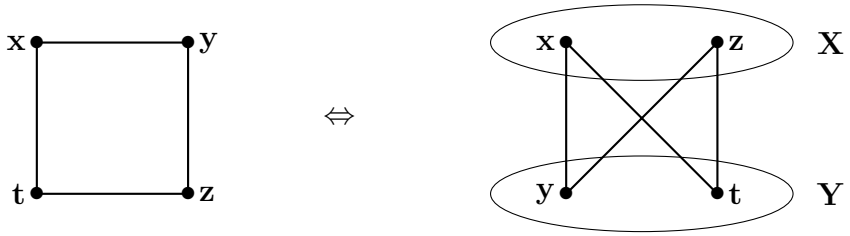
$$\begin{cases} V(G) = X \cup Y, \text{ where } X \text{ and } Y \text{ are disjoint.} \\ e \in E(G) \Leftrightarrow e = xy, \text{ with } x \in X,\ y \in Y \end{cases}$$

We write G=G(X,Y).
Remark: X and Y are stables; $\chi(G) \leq 2$.

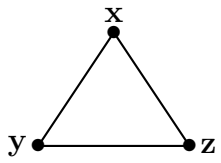
Example 2.2.1.



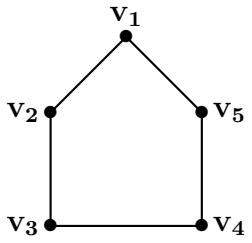
Remark 2.2.1.



G : bipartite



G is not bipartite



G is not bipartite

Proposition 2.2.1. An odd cycle is not bipartite.

Proof. Let $C = v_1 v_2 \dots v_{2p+1}$ be an odd cycle. Suppose to the contrary that C is bipartite and let X, Y be two stables such that $V(C) = X \cup Y$. Suppose, without loss of generality, that $v_1 \in X$. We have

$$v \in X \Rightarrow v_2 \in Y \Rightarrow v_3 \in X.$$

By induction, if $v_{2k-1} \in X$, then $v_{2k} \in Y$; and so $v_{2k+1} \in X$. Thus $v_1, v_{2p+1} \in X$ and $v_1 v_{2p+1} \in E(C)$. A contradiction. □

Remark 2.2.2. Let $G = G(X, Y)$ be a bipartite graph.

- Any subgraph of G is bipartite.
- $x \in X$, $y \in Y$, $xy \notin E(G)$; then $G' = G + xy$ is bipartite.
- $x \in X$, $y \in Y$, P is an xy-path, then $l(P)$ is odd.
- $e(G) = \sum_{x \in X} d(x) = \sum_{y \in Y} d(y)$.

Proposition 2.2.2. A graph G is bipartite if and only if any connected component of G is bipartite.

Proof. N.C. Suppose that G is bipartite; $G = G(X, Y)$ and let C be c.c. of G. We have $C = C(X \cap C, Y \cap C)$. So, C is bipartite.

S.C. Suppose that $C_1, C_2, \dots, C_s$ are the c.c. of G. Each one is bipartite. Set $C_i = C_i(X_i, Y_i)$. Then $X = \cup_{i=1}^{n} X_i$ and $Y = \cup_{i=1}^{n} Y_i$ are both stable and

$$V(G) = \cup_i V(C_i) = \cup_i (X_i \cup Y_i) = (\cup_i X_i)(\cup_i Y_i) = X \cup Y.$$

Then G is bipartite; $G = G(X, Y)$.

□

Theorem 2.2.1. [(König - 1928)] A connected graph G is bipartite if and only if it contains no odd cycle.

Admitted without proof.

Remark 2.2.3. Based on proposition 2.2.2, we may easily remark that an arbitrary graph is bipartite if and only if it contains no odd cycles.

Proposition 2.2.3. Let G be a k-regular bipartite graph $G = G(X, Y)$. Then $|X| = |Y|$.

Proof. We have

$$e(G) = \sum_{x \in X} d(x) = \sum_{y \in Y} d(y).$$

Then,

$$\sum_{x \in X} k = \sum_{y \in Y} k.$$

And so $k|X| = k|Y|$, $|X| = |Y|$. □

2.3 Digraphs

When a relation R is not symmetric, it defines what we call *oriented graph* or *digraph*. Pairs are replaced by couples, and edges become arcs.

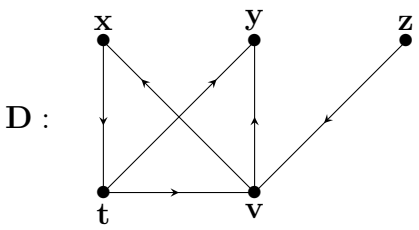
Definition 2.3.1. Let V be a finite set, and let R be an arbitrary relation defined on V. The set V endowed with the relation R is said to be a digraph. Thus a digraph D is defined by the sets:

$$\begin{cases} V = V(D) : \text{ the set of vertices of D} \\ E(D) = \{(x, y) \in V^2;\ xRy\} : \text{ the set of arcs of D} \end{cases}$$

The underlying graph of D, $G(D)$, is the graph obtained from D by ignoring the orientations of the arcs.

$$\begin{cases} V(G(D)) = V(D) \\ E(G(D)) = \{xy; (x, y) \in E(D) \text{ or } (y, x) \in E(D)\} \end{cases}$$

Example 2.3.1.



$V(D) = \{x, y, z, t, v\}$.
$E(D) = \{(x,t), (z,v), (t,y), (t,v), (v,x), (v,y)\}$.

Definition 2.3.2. Let D be a digraph, $v \in D$. The *out-neighborhood* of v is the set:

$$N^+(v) = \{x;\ (v,x) \in E(D)\}$$

The *out-degree* of v is $d^+(v) = |N^+(v)|$.

By a similar approach, we define the *in-neighbor* and the *in-degree* of v.

Remark 2.3.1.

- As we defined for graphs, similarly we define subgraphs, induced subgraphs and spanning subgraphs of a digraph D.
- The stability of a digraph D is the stability of its underlying graph $G(D)$. Also, $\chi(D) = \chi(G(D))$.
- A digraph D is connected if $G(D)$ is connected.
- An oriented path (resp. cycle) is a digraph whose underlying graph is a path (resp. cycle).

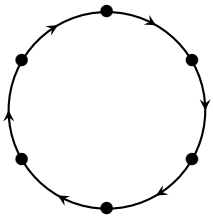
Definition 2.3.3. (i) A *directed path* P is a path verifying:

$$\begin{cases} V(P) = \{v_1, v_2, \ldots, v_n\} \\ E(P) = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n)\} \end{cases}$$

We write $P = v_1 v_2 \ldots v_n$. P is a $v_1 v_n$-directed path, $l(P) = n - 1$.

(ii) A *circuit* or a *directed cycle* C is a digraph verifying:

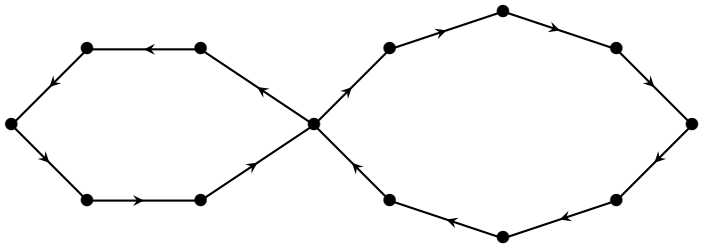
$$\begin{cases} V(C) = \{v_1, v_2, \ldots, v_n\} \\ E(C) = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n), (v_n, v_1)\} \end{cases}$$



We write $C = v_1v_2 \dots v_n$, $l(C) = n$.

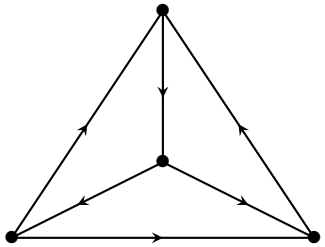
Definition 2.3.4. A digraph is said to be *strongly connected* or *strong* if $\forall x, y \in D$, D contains an xy-directed path.

Example 2.3.2. The digraph below is a strong digraph.



Definition 2.3.5. A tournament T is a digraph such that $\forall x, y \in V(T)$ we have $(x, y) \in E(T)$ or $(y, x) \in E(T)$. (It is not allowed that both (x, y) and (y, x) be in $E(T)$)

Example 2.3.3. T: Tournament



Proposition 2.3.1. Any tournament T contains a directed path passing through all the vertices of T.

Proof. Let $P = v_1v_2 \dots v_s$ be a longest directed path in T. If $s < v(T)$, then let $v \in T$ with $v \notin P$. If $(v, v_1) \in E(T)$, then $vv_1v_2 \dots v_s$ is a directed path longer than P; a contradiction. Then, $(v_1, v) \in E(T)$. Similarly, we show that $(v, v_s) \in E(T)$. So, $\exists\, i \in [1, s]$ such that $(v_i, v), (v, v_{i+1}) \in E(T)$. Thus, $v_1 \dots v_ivv_{i+1} \dots v_s$ is a directed path in T longer than P; a contradiction. $\square$

Exercises and Problems

1. Consider the graph defined by:

$$V(G) = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$$

$$E(G) = \{v_1v_3, v_1v_4, v_2v_3, v_2v_4, v_3v_4, v_4v_5, v_6v_7\}$$

(a) Draw G.

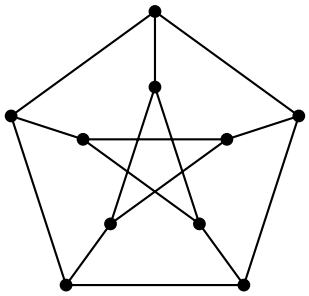
(b) Find $\delta(G)$, $\Delta(G)$, $\alpha(G)$, $d(G)$, $\chi(G)$.

(c) Is G connected? Find the connected components of G.

(d) Find a longest path of G.

(e) Find $x, y \in V(G)$ such that $xy \notin E(G)$ and $G' = G + xy$ verifies that G is connected and $\Delta(G') = \Delta(G)$. Show that $\delta(G') = \delta(G)$.

2. Given the Petersen graph:



G : Petersen graph

(a) Find the stability of G.

(b) Find the chromatic number of G.

(c) Find a longest cycle in G.

3. Let G be a connected graph. Let $x, y \in G$ such that $xy \in E(G)$ and $G' = G - xy$.

(a) Show that if G' is connected, then G has a cycle C containing xy.

(b) Show that if G' is disconnected, then G' contains exactly 2 distinct connected components, C_1 and C_2, such that $x \in C_1$ and $y \in C_2$.

4. Let G be a connected graph.

(a) Let $v \in G$ such that $d(v) = 1$. Show that $G' = G - v$ is connected.

(b) Suppose that G has no cycles. Let P be a longest path in G and let x be an end of P. Show that $d(x) = 1$.

(c) Deduce that G is a tree if and only if $v(G) = e(G) + 1$.

5. Let G be a connected graph with $\delta(G) \geq 2$.

(a) Show that $e(G) \geq v(G)$. Deduce that G contains a cycle.

(b) Show that G contains a cycle C with a vertex $v \in C$ such that $N(v) \subseteq C$.

6. Let G be a connected graph and let P be a longest path in G. Set $P = v_1 v_2 \dots v_n$.

(a) Show that $N(v_1) \subseteq P$, $N(v_n) \subseteq P$.

(b) Show that if $v_1 v_n \in E(G)$, then $v(G) = n$.

(c) Suppose that $v_1 v_n \notin E(G)$. Set

$$N(v_n) = \{v_{i_1}, v_{i_2}, \dots, v_{i_s}\};\ 2 < i_1 < i_2 < \dots < i_s \leq n-1$$

Set $X = \{v_{i_1+1}, v_{i_2+1}, \dots, v_{i_s+1}\}$. Show that if $N(v_1) \cap X \neq \emptyset$, then $v(G) = n$.

(d) Deduce that if $d(v_1) + d(v_n) \geq n$, then $v(G) = n$.

7. Let G be a connected graph.

(a) Let $S, S' \subseteq V(G)$, $S \cap S' = \emptyset$. Show that there is an xy-path P in G such that $P \cap S = \{x\}$ and $P \cap S' = \{y\}$.

(b) Two paths, P_1 and P_2, of G are said to be parallel if $P_1 \cap P_2 = \emptyset$. Let R be an xy-path such that $x \in P_1$ and $y \in P_2$ (P_1 and P_2 are two parallel paths of G). Show that $P_1 \cup R \cup P_2$ contains a path P such that $l(P) > l(P_1)$ and $l(P) > l(P_2)$.

(c) Deduce that two longest paths of G are not parallel.

8. Let G be a graph.

(a) Show that $v(G) \leq \alpha(G)\chi(G)$.

(b) Show that $e(G) \geq \delta(G)\alpha(G)$.

(c) Deduce that $\frac{v(G)}{\chi(G)} \leq \frac{e(G)}{\delta(G)}$.

9. Let G be a graph with $v \in G$.

(a) Show that $\alpha(G - v) \geq \alpha(G) - 1$.

(b) Show that $\chi(G-v) \geq \chi(G) - 1$.

(c) Show that:

$$\chi(G-v) = \chi(G) - 1 \Rightarrow d(v) \geq \chi(G) - 1.$$

10. Let G be a graph. Set $\omega(G) = max\{v(H)$; H is a complete subgraph of $G\}$.

(a) Show that $\omega(G) = \alpha(\bar{G})$ and $\alpha(G) = \omega(\bar{G})$.
Deduce that $v(G) \leq \chi(G)\chi(\bar{G})$.

(b) Let $v \in G$. Show that $d_G(v) + d_{\bar{G}}(v) = v(G) - 1$.

11. Let D be a diagraph. Suppose that D contains no circuits.

(a) Show that D contains a vertex v such that $d^+(v) = 0$. Show that $S = \{v; d^+(v) = 0\}$ is a stable.

(b) Let $v \in D$ and set $c(v) = max\{l(\mathcal{P})$; $\mathcal{P}$ is a divided path in D of origin $v\}$. Show that if $c(v) = c(v')$ then $vv' \notin E(G(D))$.

(c) Deduce that D contains a directed path $\mathcal{P}$ such that $l(\mathcal{P}) \geq \chi(D) - 1$.

12. Let T be a tournament of order $n \geq 4$.

(a) Show that T contains a non directed triangle.

(b) Show that if T is strong then it contains a circuit. Deduce that T contains a directed triangle.

13. Let H be a group of neutral element e. Let $a \neq e \in H$. We define a diagraph D by:

$$V(D) = H$$

$$(x, y) \in E(H) \Leftrightarrow y = ax$$

(a) Show that $d^+(v) = d^-(v) = 1\ \forall v \in G$.

(b) Show that any cycle in D is a circuit.

(c) Show that any cycle in D is of length p such that p is the order of a ($p = min\{m; a^m = e\}$).

(d) Deduce that $a^n = e$ where $n = |G|$.

Chapter 3

Complement on the Natural Integers and the Cardinals of Countable Sets

3.1 The Construction of $\mathbb{N}$

The mathematical teaching programs allow us to admit the existence of $\mathbb{N}$, the properties of the natural numbers and the classical operations defined on these numbers[1].

However, it is interesting to reintroduce $\mathbb{N}$ by a minimal number of axioms and establish then the fundamental properties of this set.

$\mathbb{N}$ is a non empty ordered set verifying the following axioms.

Axiom 3.1.1. ***(A_1)*** Any non empty part of $\mathbb{N}$ admits a smallest element.

The smallest element of $\mathbb{N}$ is denoted by the symbol 0 (called zero).

Axiom 3.1.2. ***(A_2)*** $\mathbb{N}$ has no greatest element.

Axiom 3.1.3. ***(A_3)*** Any element $a \neq 0$ of $\mathbb{N}$ has a predecessor a' (i.e. $a' < a$ and $a' \leq b \leq a \Rightarrow b = a'$ or $b = a^2$.

The set $\mathbb{N}$ may be introduced using another family of axioms, like Peano's axioms, the above axioms will be then simple consequences, they are chosen

[1]From Michel Queysanne: Algèbre (1^{er} cycle et classes préparatoires).

[2]We define the successor in the same way: a' is the successor of a if $a < a'$ and if $a \leq b \leq a'$ then $b = a'$ or $b = a$.

here for a simplification reason: these axioms permit us to present the induction as a proved fact. This notion may be presented as an axiom after defining the successor function $S(n)$ as follows:

Axiom 3.1.4. Let K be a set verifying:

1. $0 \in K$.
2. $n \in K \Rightarrow S(n) \in K$.

Then $K = \mathbb{N}$.

Induction is a fundamental principle justifying the apparent passage from particular to general in mathematics. It can be exposed in two forms:

Theorem 3.1.1. ***(First form)*** Let p be a property defined on $\mathbb{N}$ such that 0 verifies p and if k verifies p, then $k+1$ verifies p. Then p is true for every $n \in \mathbb{N}$.

Proof. We have to show that the set $A = \{k \in \mathbb{N}; k \text{ doesn't not verify } p\}$ is empty. Suppose to the contrary that $A \neq \emptyset$, then A admits a smallest element s by A_1. We have $s \neq 0$ since $0 \notin A$, then s admits a predecessor s'. We have $s' < s$, then $s' \notin A$ and then s' verifies p, thus by hypothesis $s = s' + 1$ verifies p, a contradiction. Then $A = \emptyset$. □

Theorem 3.1.2. ***(Second form)*** Let p be a property defined on $\mathbb{N}$ such that 0 verifies p and if s verifies p for every $s < k$, then k verifies p. Then p is true for every $n \in \mathbb{N}$.

Proof. A and s are defined as in the above theorem, for every $s' < s$, we have $s' \notin A$ and then s' verifies p, then by hypothesis s verifies p, a contradiction. So $A = \emptyset$. □

The induction principle is based then on the axiom of the smallest element satisfied in $\mathbb{N}$. It is also founded on what we call "mathematical definition". In fact, the ambiguity in the definition of many properties -in a mathematical point of view- raises up the belief that some of our fundamental logical laws are built over a weak base. The "sorites" are among the more ancient paradoxicons that go back to the Greek philosophers of the Megare school. These paradoxicons consist of proving that it is impossible to construct a handful of grains by adding one grain at a time. Other examples show in the same way that there are no rich men. In fact, a man possessing a franc is not rich and he will not be so if one franc is added. If we apply induction, we are forced to conclude that this man will remain poor no matter how many pieces of money

he receives. For certain, the same argument is valid for the example of grains.

Clearly, one of the pragmatic mean to destroy this argument is to unload containers full of grains. But this counter-example does not serve to discover the weak logical point in this reasoning.

The problem resides in the fact that we have no precise borders permitting to decide if something is a "handful" or not, if a man is rich or not, etc. Then, it is the mathematical ambiguity in the definitions of "handful", "rich", etc which leads to contradictory results[3] .

Finally, it remains to remark that the first step $'p(0)'$ must be carefully verified. To realize this see exercise 3 (A group of persons containing a woman contains only women).

3.2 Cardinal of a Finite Set

To simplify, the set $\{1, \ldots, n\}$ is denoted by $[1, n]$ for every $n \in \mathbb{N}^*$.

Proposition 3.2.1. Let m and n be two non zero positive integers. If there exists an injection from $[1, m]$ into $[1, n]$, then $m \leq n$.

Proof. We argue by induction on m; if $m = 1$, the inequality is trivial since $n \geq 1$. Suppose that the property holds for m and let's prove it for $m+1$ the successor of m. Let f be an injection from $[1, m+1]$ into $[1, n]$ (Note that $n > 1$ in this case, since otherwise $f(1) = f(m+1)$ and $1 \neq m+1$). Let s be the element of $[1, n]$ such that $f(m+1) = s$ and let φ the permutation $(s\ n)$ (if $s = n$, φ is the identical mapping), then $\varphi \circ f$ is an injection from $[1, m+1]$ into $[1, n]$ such that $\varphi \circ f(m+1) = n$, so the restriction of $f \circ \varphi$ on $[1, m]$ is an injection into $[1, n^*]$ where n^* is the predecessor of n, we deduce, by induction, that $m \leq n^*$ and consequently $m + 1 \leq n$. □

Corollary 3.2.1. If there exists a bijection from $[1, m]$ into $[1, n]$, then $m = n$.

Proposition 3.2.2. Let n be a non zero natural integer. Any injection from $[1, n]$ into $[1, n]$ is a bijection.

Proof. We argue by induction on n; if $n = 1$, the property is trivial. Suppose that the property holds for n and let's prove it for $n + 1$. Let f be the

[3]By Nicholas Falletta: The paradoxicons.

injection from $[1, n+1]$ into $[1, n+1]$. Let s be the element of $[1, n+1]$ such that $f(n+1) = s$ and let φ be the permutation $(s\ n+1)$ (if $s = n+1$, φ is then the identity mapping), then $\varphi \circ f$ is an injection from $[1, n+1]$ into $[1, n+1]$ such that $\varphi \circ f(n+1) = n+1$, then it is a bijection by induction hypothesis. We deduce that $\varphi \circ f$ is a bijection, then f is a bijection since φ is so ($f = \varphi^{-1} \circ (\varphi \circ f)$). □

Definition 3.2.1. A non empty set E is said to be finite of cardinal n (we write $card(E) = n$) if there exists a bijection from E into $[1, n]$ where $n \in \mathbb{N}^*$. A non finite set is said to be infinite. By definition $\emptyset$ is a finite set of cardinal zero, $card(\emptyset) = 0$.

Remark 3.2.1. The above definition is well justified, in fact, if there exist bijections from E to $[1, n]$ and $[1, m]$, then these two last sets are equipollent and $m = n$.

The verification of the following remarks is left to the reader:

Proposition 3.2.3. Let E and F be two given sets. We have:

1. If F is finite and $E \subseteq F$, then E is finite and $card(E) \leq card(F)$.
2. If E and F are finite, then $E \times F$ is finite and we have $card(E \times F) = card(E) \times card(F)$.
3. If E and F are finite and if $E \cap F = \emptyset$, then $E \cup F$ is finite and we have $card(E \cup F) = card(E) + card(F)$.

(To establish these three facts, argue by induction on the cardinal of F)

Exercise 3.2.1. Let E and F be two finite sets. Show that $card(E \cup F) = card(E) + card(F) - card(E \cap F)$.

Proposition 3.2.4. Let f be a bijection from a set E into a set F. If F is finite, then E is finite and we have $card(E) = card(F)$.

Proof. Set $card(F) = n$ and let φ be a bijection from F into $[1, n]$. $\varphi \circ f$ is a bijection from E into $[1, n]$ and then $card(E) = n = card(F)$. □

Remark 3.2.2. If f is injective, then $f : E \mapsto f(E)$ is bijective and we have $card(E) = card(f(E)) \leq card(F)$ since $f(E) \subseteq F$. If f is surjective, we may find a part A in E such that $f : A \mapsto F$ is a bijection. We have in this case $card(F) = card(A) \leq card(E)$.

Proposition 3.2.5. Let E of a finite set F such that $card(E) = card(F)$, then $E = F$.

Proof. It is sufficient to remark that the canonical injection $i : E \mapsto F$ is bijective. We have $E = i(E) = F$. Set $card(E) = card(F) = n$ and let φ (resp. φ') be a bijection from E (resp. F) in $[1, n]$. We have $\varphi' \circ i \circ \varphi^{-1}$ is an injection from $[1, n]$ into $[1, n]$, then it is a bijection and so i is a bijection. □

Corollary 3.2.2. Let E and F be two finite set such that $card(E) = card(F)$. For every mapping $f : E \mapsto F$ the following properties are equivalent:

1. f is injective.
2. f is surjective.
3. f is bijective.

Proof. If f is injective, then $f : E \mapsto f(E)$ is bijective and we have $card(f(E)) = card(E) = card(F)$, then $E = f(E)$ and f is bijective. If f is surjective, we may find a part A of E such that $f : A \mapsto F$ is a bijection. We have in this case $card(A) = card(F) = card(E)$, then $A = E$ and f is bijective. □

3.3 Countable sets

Definition 3.3.1. A set E is said to be countable if E is finite or E is equipollent to $\mathbb{N}$.

Remark 3.3.1. If a countable set E is equipollent to a set F, we write $E \sim F$, then F is countable.

As in the finite case, we are able to show that a subset of a countable set is countable, the intersection and union of 2 countable sets are countable. Moreover, we shall prove that the cartesian product of two countable sets is countable.

Proposition 3.3.1. Let B be an infinite subset of $\mathbb{N}$. Then B can be arranged into a strictly increasing sequence $(x_n)_{n\geq 0}$.

Proof. Let x_0 be the smallest element of B; it exists due to the axioms of $\mathbb{N}$. Suppose by induction that $x_0, \ldots, x_s$ are defined, $s \geq 0$. Since B is infinite, then $B - \{x_0, \ldots, x_s\} \neq \emptyset$. Let x_{s+1} be its smallest element. Then, the sequence is well defined and is obviously increasing. Set $H = \{x_n,\ n \geq 0\}$. Trivially, $H \subseteq B$. Conversely, let $m \in B$. If $m = 0$, then $m = x_1$ and so $m \in H$. Otherwise, $A = B \cap [1, m-1] \subseteq [1, m]$, then A is finite. Let x_k be the greatest element of A. We have $A = \{x_0, x_2, \ldots, x_k\}$. Since m is the smallest element of $B - A$, then $m = x_{k+1} \in B$. Thus $B \subseteq H$, and $B = H$. □

Corollary 3.3.1. Any subset of $\mathbb{N}$ is countable.

Proof. Let $B \subseteq \mathbb{N}$. If B is finite, then B is countable. If B is infinite, then $B = \{x_n,\ n \geq 0\}$ where $(x_n)_{n\geq 1}$ is strictly increasing. And so,

$$\begin{aligned} f :&\mathbb{N} \to B \\ &s \to f(s) = x_s. \qquad \text{is a bijection.} \end{aligned}$$

B is countable. □

Corollary 3.3.2. A set E is countable if there exists an injection from E to $\mathbb{N}$.

Proof. Let $f :\ E \to \mathbb{N}$ be an injective mapping. Then $E \sim f(E)$ which is countable. So, E is countable. □

Corollary 3.3.3. A subset E of a countable set F is countable.

Proof. Let

$$\begin{aligned} i_E : E &\to F \qquad\qquad ;\ f :\ F \to \mathbb{N} \quad \text{injection.} \\ x &\to i_E(x) = x. \end{aligned}$$

Then $f \circ i_E :\ E \to \mathbb{N}$ is an injective mapping. So, E is countable. □

Corollary 3.3.4. Let E be a countable set. Then for every set F we have: $E \cap F$ and $E - F$ are countable.

Proposition 3.3.2. Let E and F be two countable sets with $E \cap F = \emptyset$. Then $E \cup F$ is countable.

Proof. E and F are countable, then $\exists f :\ E \to \mathbb{N}$, $g :\ F \to \mathbb{N}$ which are injective. Define

$$\begin{aligned} \varphi : E \cup F &\to \mathbb{N} \\ x \to \varphi(x) &= \begin{cases} 2f(x) & \text{if } x \in E. \\ 2g(x) + 1 & \text{if } x \in F. \end{cases} \end{aligned}$$

We may easily verify that φ is injective. So, $E \cup F$ is countable. □

Remark 3.3.2. We conclude that the union of two arbitrary countable sets E and F is countable since $E \cup F = (E - F) \cup F$. Also, if $E_1, E_2, \ldots, E_n$ are countable sets, then $E_1 \cup \ldots \cup E_n$ is countable.

Proposition 3.3.3. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. Let

$$\begin{aligned} f : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a, b) &\to 2^a \times 3^b \end{aligned}$$

f is injective. In fact, let (a, b), $(a', b') \in \mathbb{N} \times \mathbb{N}$ such that $f(a, b) = f(a', b')$. We have:

$$f(a, b) = f(a', b') \Rightarrow 2^a 3^b = 2^{a'} 3^{b'}.$$

2^a divides $2^a 3^b = 2^{a'} 3^{b'}$ and $2^a \wedge 3^{b'} = 1 \Rightarrow 2^a$ divides $2^{a'}$. So, $a \leq a'$. Similarly, we show that $a' \leq a$. So $a = a'$. We prove by a similar way that $b = b'$. □

Corollary 3.3.5. The cartesian product of 2 countable sets is countable.

We prove now that the set $\mathbb{R}$ is not countable. For this, we prove first that $\mathcal{P}(\mathbb{N})$ is not countable.

Let $\chi = \{(x_n)_{n\geq 0};\ x_i \in \{0, 1\}\}$. $\forall A \subseteq \mathbb{N}$ we define the characteristic function of A by

$$\begin{aligned} \chi_A : \mathbb{N} &\to \{0, 1\} \\ t \to \chi_A(t) &= \begin{cases} 0 & if\ t \notin A. \\ 1 & if\ t \in A. \end{cases} \end{aligned}$$

Proposition 3.3.4. $\mathcal{P}(\mathbb{N}) \sim \chi$.

Proof. Define

$$\begin{aligned} \varphi :\ \mathcal{P}(\mathbb{N}) &\to \chi \\ A &\to \varphi(A) = (x_n)_{n\geq 0} \end{aligned}$$

where $x_n = \chi_A(n),\ \forall n \geq 0$.

- φ is injective: Let $A, A' \subseteq \mathbb{N}/\ \varphi(A) = \varphi(A')$. Set $\varphi(A) = (x_n)_{n\geq 0}$, $\varphi(A') = (x'_n)_{n\geq 0}$. We have:

  $$\varphi(A) = \varphi(A') \Rightarrow x_n = x'_n\ \forall n \geq 0.$$

  Let $t \in A$. We have $x_t = \chi_A(t) = 1$.

  $$x'_t = x_t = 1 \Rightarrow \chi_{A'}(t) = 1 \Rightarrow t \in A'$$

  So, $A \subseteq A'$. Similarly, $A' \subseteq A$. So, $A = A'$ and φ is injective.

- φ is surjective: Let $(x_n)_{n\geq 0} \in \chi$. Set $A = \{x_n;\ x_n = 1\}$. We have $A \subseteq \mathbb{N}$, and $\varphi(A) = (x_n)_{n\geq 0}$. φ is surjective.

Therefore, φ is bijective and $\mathcal{P}(\mathbb{N}) \sim \chi$. □

Theorem 3.3.1. $\mathcal{P}(\mathbb{N})$ is not countable.

Proof. Suppose to the contrary that $\mathcal{P}(\mathbb{N})$ is countable. Then χ is countable. Let $f : \mathbb{N} \to \chi$ be a bijection. Set $f(i) = (x_n^i)_{n\geq 0}$. Define $(u_n)_{n\geq 0}$ by:

$$u_i = 1 - x_i^i,\ i \geq 0.$$

Clearly $(u_n)_{n\geq 0} \in \chi$. Then $\exists\ s$ such that $f(s) = (u_n)_{n\geq 0}$. We have $f(s) = (x_n^s)_{n\geq 0} = (u_n)_{n\geq 0}$. So, $u_s = x_s^s$, a contradiction. □

Let $(x_n)_{n\geq 0} \in \chi$. We define the sequence:

$$s_i = 0, x_1 x_2 \dots x_i \quad i \geq 0.$$

This sequence of positive number is strictly increasing and bounded by 1. So, it converges in $\mathbb{R}$ to a limit s. We write: $s = 0, x_1 x_2 \dots x_n \dots$

Theorem 3.3.2. $\mathbb{R}$ is not countable.

Proof. Let

$$\begin{aligned} \varphi : \chi &\to \mathbb{R} \\ (x_n)_{n\geq}0 &\to \varphi((x_n)_{n\geq 0}) = 0, x_1 x_2 \dots x_n \dots \end{aligned}$$

φ is injective: Let $\varphi((x_n)_{n\geq 0}) = \varphi((x'_n)_{n\geq 0})$. Suppose to the contrary that $(x_n)_{n\geq 0} \neq (x'_n)_{n\geq 0}$ and let n_0 be the first integer such that $x_{n_0} \neq x'_{n_0}$. Suppose that $x_{n_0} = 0$, $x'_{n_0} = 1$.

$$\begin{aligned} 10^{n_0} \ .\ 0, x_1 x_2 \dots x_n \dots &= x_{n_0}, x_{n_0+1} \dots x_n \dots \\ 10^{n_0} \ .\ 0, x'_1 x'_2 \dots x'_n \dots &= x'_{n_0}, x'_{n_0+1} \dots \dots \end{aligned}$$

Then, $\varphi((x_n)_{n\geq 0}) \neq \varphi((x'_n)_{n\geq 0})$, a contradiction. So, $\varphi(\chi) \subseteq \mathbb{R}$ is equipollent to χ. So, it is not countable, then $\mathbb{R}$ is not countable. □

3.4 Combinatorial Analysis

Definition 3.4.1. Let E be a set of cardinal $n \geq 1$. For every $p \leq n$, a p-arrangement $(x_1, x_2, \ldots, x_p)$ of E is an ordered family formed by p elements of E pairwise distinct. The number of all p-arrangement of E depends only upon p and n. This number will be denoted by A_n^p. The n-arrangements are called the permutation of E, its number A_n^n is denoted by P_n.

Example 3.4.1. Let $E = \{1, 2, 3\}$. The 3-arrangements (permutations) of E are $(1, 2, 3), (2, 3, 1), (3, 1, 2), (1, 3, 2), (2, 1, 3), (3, 2, 1)$.

Notation 3.4.1. The number of parts of E formed by p elements is denoted by C_n^p.

In this section, we calculate A_n^p, P_n and C_n^p in terms of p and n.

Theorem 3.4.1. $A_n^p = \frac{n!}{(n-p)!}$.

Proof. A_n^p can be considered as the number of the p-arrangements of the set $E = \{1, 2, \ldots, n\}$. We establish the equality by induction on $p \leq n$. For $p = 1$, A_n^1 is the number of the elements of E, then $A_n^1 = n = \frac{n!}{(n-1)!}$. Suppose that the equality holds for $p < n$. Let H_k $(k = p, p+1)$ be the set of k-arrangements of E and let f be the surjective mapping associating to each element $(x_1, x_2, \ldots, x_p, x_{p+1})$ of H_{p+1} the element $(x_1, x_2, \ldots, x_p)$ of H_p. Consider the equivalence relation R_f. Let $\overline{z} \in H_{p+1}/R_f$, $z = (x_1, x_2, \ldots, x_p, x_{p+1})$, the only difference between two arbitrary elements of $\overline{z}$ is the $(p+1)^{th}$ element ($x_1, x_2, \ldots, x_p$ are fixed), then $card(\overline{z}) = n - p$. So $card(H_{p+1}) = card(H_{p+1}/R_f) \times (n - p)$ (The classes of R_f form a partition of H_{p+1}). But $card(H_{p+1}/R_f) = card(H_p)$ since H_{p+1}/R_f and H_p are equipollent (proposition 3.4.3). But $card(H_p) = A_n^p = \frac{n!}{(n-p)!}$ by the induction hypothesis. Consequently:

$$card(H_{p+1}) = card(H_p) \times (n - p) = \frac{n!}{(n-p)!} \times (n - p) = \frac{n!}{(n - (p+1))!}$$

□

Corollary 3.4.1. $P_n = n!$.

Proof. We have $P_n = A_n^n = \frac{n!}{(n-n)!} = n!$ $(0! = 1)$. □

Corollary 3.4.2. $C_n^p = \frac{n!}{p!(n-p)!}$.

Proof. Let S_p be the set of parts of $E = \{1, 2, \ldots, n\}$ formed by p elements and let f be the surjective mapping which associate to each element $(x_1, x_2, \ldots, x_p)$ of H_p the element $\{x_1, x_2, \ldots, x_p\}$ of S_p. We consider the equivalence relation R_f. Let $\overline{z} \in H_p/R_f$, $z = (x_1, x_2, \ldots, x_p)$, the elements of $\overline{z}$ are the permutations of the set $\{x_1, x_2, \ldots, x_p\}$, so $card(\overline{z}) = p!$. Thus $card(H_p) = card(H_p/R_f) \times p!$. But $card(H_p/R_f) = card(S_p)$ since H_p/R_f and S_p is equipollent (proposition 3.4.3). But $card(H_p) = A_n^p = \frac{n!}{(n-p)!}$. Consequently:

$$card(H_p) = card(S_p) \times p!$$

So

$$C_n^p = \frac{card(H_p)}{p!} = \frac{n!}{p!(n-p)!}$$

□

Exercises and Problems

1. Use induction to establish the following:

(a) $1 + \frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$; $n \geq 1$.

(b) $(1 + 2 + \ldots + n)^2 = 1^3 + 2^3 + \ldots + n^3$.

(c) $\left(\frac{n+1}{n}\right)^n \leq 3$.

2. Let E be a set of cardinal $n \geq 1$ and let $a \in E$.

(a) Find the number of parts of E containing a.

(b) Show that E is the union of its parts containing a if and only if $n \geq 3$.

3. Someone wants to show that if a group of persons contains a woman then it contains only women. He argues by induction as follows: If the group is formed by one person, the property is trivial. Suppose that we have n persons in the group, $n \geq 2$ and consider the parts of $n-1$ persons containing the woman of the group, by induction these parts contain only women. So the group itself contains only women. Is this argument true? Use the above exercise to justify your answer.

4. Let E be a finite set and let $F = E \cup \{a\}$ where $a \notin E$. We define the subset G of $P(F)$ by

$$G = \{X \in P(F) \text{ such that } a \in X\}$$

(a) Show that G and $P(E)$ form a partition of $P(F)$. Deduce that $card(P(F)) = card(P(E)) + card(G)$.

(b) We define the mapping f from $P(E)$ into G by:

$$\begin{aligned} f : P(E) &\mapsto G \\ X &\mapsto X \cup \{a\} \end{aligned}$$

Show that f is bijective. Deduce that $card(P(F)) = 2card(P(E))$.

(c) Conclude that if a set is of cardinal n, then its power set is of cardinal 2^n.

5. Show that if p is prime, then

(a) If p divides $a_1 \times a_2 \times \ldots \times a_n$, then $\exists 1 \leq i \leq n$ such that p divides a_i.

(b) If p divides a^n, where $n \in \mathbb{N}^*$, then p divides a.

(c) p divides p^n if and only if $n \geq 1$.

(d) p^t divides p^n if and only if $t \leq n$.

(e) If q is prime and q^t divides p^n, for some $t \in \mathbb{N}^*$, then $q = p$ and $t \leq n$.

6. Let $p_1, p_2, \ldots, p_r$ be pairwisely distinct prime numbers.

(a) Show that if q is a prime dividing $(p_1 \times p_2 \times \ldots \times p_r) + 1$, then $q \notin \{p_1, p_2, \ldots p_r\}$.

(b) Deduce that the set of prime numbers is infinite.

7. Let p be prime.

(a) Show that p is relatively prime with $s!$, for all $s \leq p - 1$.

(b) Deduce that p divides C_p^t, for all $1 \leq t \leq p - 1$.

8. Show that if p is prime, then p divides $n^p - n$, for every natural number n. (**Hint:** argue by induction on n and use exercise **7.**)

9. Show that if p is prime and p does not divide n, then p divides $n^{p-1} - 1$.

10. Let $n \geq 3$. Show that if p is a prime, such that $\sqrt{n} < p$ and every prime $\leq p$ does not divide n, then n is prime.

11. Let $n \geq 3$. Show that if p is a prime, such that every prime $\leq p$ does not divide n, and the quotient q of the division of n by p is $< p$, then n is prime.

12. Show that if $n \in \mathbb{N}$, then a and b are coprime in the following cases:

(a) $a = 3n + 2$ and $b = 2n + 1$.

(b) $a = 14n + 3$ and $b = 5n + 1$.

13. Let $a, b \in \mathbb{N}^*$. Show that if $\frac{a}{b} = \frac{\alpha}{\beta}$, where $\alpha \wedge \beta = 1$, then

$$a \wedge b = \frac{a}{\alpha} = \frac{b}{\beta} \text{and } a \vee b = a\beta = b\alpha.$$

Application: Compute $a \wedge b$ and $a \vee b$ in the following cases:

(a) $a = 18$ and $b = 42$.

(b) $a = 1224$ and $b = 216$.

14. Find the natural numbers x and y, satisfying

$$x^2 + y^2 = 25.$$

Deduce that we can find non-zero natural numbers x, y, and z, such that

$$x^2 + y^2 = z^2.$$

15. Show that if x and y are two natural numbers, such that 3 divides $x^2 + y^2$, then 3 divides x and y. Deduce that the equation $x^2 + y^2 = 7500000$ has no solution in $\mathbb{N}$.

16. Show that there exists no natural numbers x and y, such that x and y are non-zero and

$$x^3 + y^3 = 9^3.$$

Remark: This is a particular case of **Fermat's Last Theorem** which states that if n is any natural number, such that $n \geq 3$, then the equation

$$x^n + y^n = z^n$$

has no solutions for which x, y and z are non-zero natural numbers.
Pierre de Fermat, who lived from 1601 to 1665 was a French mathematician. He wrote in the margin of a notebook "I have found an admirable proof of this theorem, but the margin is too narrow to contain it." Mathematicians have been searching for this proof ever since. Using computers, they had proved the theorem for all $n \leq 30000$, but the year 1993 witnessed the end of this problem which had been facing mathematicians since the 17^{th} century, when **Professor Andrew Wiles**, who is a British mathematician at the University of Cambridge, announced a proof for Fermat's Last Theorem. He used ideas of many mathematicians, but one of the crucial ingredients was the work of the German mathematician **Dr.Matthias Flach** of Heidelberg University.

17. Show that if A and B are non-empty sets, then the following are equivalent:

(a) there exists an injection from A to B,

(b) there exists a surjection from B onto A.

Deduce that if A is countable and $f : A \to B$ is surjective, then B is countable.

18. Show that if A is a non-empty set, then A is countable if and only if there exists a surjection from $\mathbb{N}$ onto A.

19. Show that if $E_1, \ldots, E_n$ are countable sets, then so are the sets $E_1 \times \ldots \times E_n$ and $\cup_{i=1}^{n} E_i$.

20. Show that $\mathbb{Z}$ is infinitely countable and give a bijection from $\mathbb{Z}$ onto $\mathbb{N}$.

21. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by

$$f(m,n) = \frac{1}{2}(m+n+1)(m+n) + n.$$

(a) Show that if $m \geq 1$, then

$$f(m-1, n+1) = f(m,n) + 1, \ \textit{for all } n \in \mathbb{N}.$$

(b) Show that

$$2f(a,b) = (a+b+1)^2 + (b-a-1), \ \textit{for all } a, b \in \mathbb{N}.$$

(c) Let $a, b, n \in \mathbb{N}$, Show that if $a \neq 0$, then

i. if $a + b < n$, then

$$(a+b+1)^2 + (b-a) < (n+1)^2 + n,$$

ii. if $a + b > n$, then

$$(a+b+1)^2 - (n+1)^2 > n + a - b.$$

(d) Deduce that if $f(a,b) = f(0,n)$, where $a, b, n \in \mathbb{N}$, then $a = 0$ and $b = n$.

(e) Prove by induction on m that

$$f(a,b) = f(m,n) \Rightarrow a = m \text{ and } b = n.$$

where $m, n, a, b \in \mathbb{N}$. Deduce that f is injective.

(f) Show that if $b \in \mathbb{N}$ and $k = f(0,b)$, then $k + 1 = f(b+1, 0)$.

(g) Show by induction on k, where $k \in \mathbb{N}$, that $\exists m, n \in \mathbb{N}$, such that $f(m,n) = k$.

(h) Deduce that f is bijective.

22. Show that $\mathbb{Q}$ is countable.

23. Let A be a set.

(a) Show that if $f:\ A \to P(A)$ is a mapping and

$$B = \{x \in A;\ x \notin f(x)\}$$

then $B \neq f(a)$, for all $a \in A$.

(b) Deduce that there is no surjection from A onto $P(A)$.

24. A is said to be **uncountable** if it is not countable. Show that $P(\mathbb{N})$ is uncountable.

25. We admit that $\mathbb{R}$ is uncountable. Show that the set I of irrational numbers is uncountable.

26. Let n and k be non zero positive integers such that $k \leq 2n$.

(a) Show that $C_{2n}^{k+1} - C_{2n}^{k} = \frac{(2n-2k-1)}{(2n+1)} C_{2n+1}^{k+1}$. Deduce that $C_{2n}^{k} \leq C_{2n}^{k+1}$ if and only if $k < n$.

(b) Conclude that $C_{2n}^{k} \leq C_{2n}^{n}\ \forall\ k \leq 2n$.

(c) Using the binomial formula, calculate the expression

$$C_{2n}^{0} + C_{2n}^{1} + \ldots + C_{2n}^{2n}$$

Deduce that $\frac{4^n}{2n+1} \leq C_{2n}^{n}$.

27. Let f be a mapping defined from a set E into E such that $f(x) \neq x$ for every $x \in E$. Set $H = \{A \subseteq E,\ f(A) \cap A = \emptyset\}$.

(a) Let $(A_n)_n$ be an increasing sequence (for inclusion) of elements in H. Set $A = \bigcup_{n \geq 1} A_n$. Show that $A \in H$.

(b) Suppose that E is finite.

i. Show that H admits an element of maximal cardinal N.

ii. Let $z \in E$ such that $z \notin f(N)$ and set $L = N \cup \{z\}$. Show that $f(L) \cap L = \{f(z)\} \cap N$.

iii. Let $x \in E$ such that $x \notin f(N) \cup N$. Show that $f(x) \in N$. Deduce that $f(N) \cup N \in H$, where $f(N) \cup N$ is the complement of $f(N) \cup N$ in E.

iv. Conclude that there exists in E a subset F such that $card(F) \geq \frac{card(E)}{3}$ and $f(F) \cap F = \emptyset$.