Course 1

0.0 Coordinates

- **Structure:**

  Chapter 1: Preliminaries

  Chapter 2: Vector Spaces

  Chapter 3: Matrices and Linear Systems

  Chapter 4: Introduction to Coding Theory

- **Bibliography:**

  1. S. Crivei, *Basic Linear Algebra*, Presa Universitară Clujeană, Cluj-Napoca, 2022.

  2. W. J. Gilbert, W. K. Nicholson, *Modern Algebra with Applications*, John Wiley, 2004.

  3. J. S. Golan, *The Linear Algebra a Beginning Graduate Student Ought to Know*, Springer, Dordrecht, 2007.

  4. P. N. Klein, *Coding the Matrix. Linear Algebra through Applications to Computer Science*, Newtonian Press, 2013.

  5. R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer-Verlag, 1998.

  6. I. Purdea, C. Pelea, *Probleme de algebră*, Eikon, Cluj-Napoca, 2008.

  7. L. Robbiano, *Linear Algebra for Everyone*, Springer, Milan, 2011.

  8. G. Strang, *Linear Algebra and its Applications*, Brooks/Cole, 1988.

- **Course:**

  Course materials will be available in the *Algebra* course on the Moodle platform (https://moodle.cs.ubbcluj.ro/). Enrolment key: Algebra-IE-2022

  Students may get up to 1 bonus point from course projects to the final grade: up to 5 projects, each for 0.2 points [you will receive details in due time...].

- **Seminar:**

  Minimum attendance: 75% for seminar classes in order to be allowed to participate in the second partial exam.

  Problems for the next week will be available in the *Algebra* course on the Moodle platform.

  Students may get up to 0.5 bonus points from seminar to the final grade: 5 problems solved during the seminar, each for 0.1 points [you will receive details during seminars...].

- **Exam:**

  Written partial exams in Week 8 (Chapters 1-2) and Week 14 (Chapters 3-4).

  The final grade is computed as follows:

  $$G = 1 + P_1 + P_2 + B,$$

  where:

  G = the final grade

  P_1 = the grade from the first partial exam (max. 4)

  P_2 = the grade from the second partial exam (max. 5)

  B = bonus points from seminar or course (max. 1.5)

  Students may not pass the exam unless they participate in the second partial exam.

Computer Science topics using Linear Algebra

The Association for Computing Machinery (ACM) has developed the 2012 ACM Computing Classification System for the research topics in the field of Computer Science (`https://www.acm.org`) under the form of a multi-level tree. We mention some higher level branches of this tree in which Linear Algebra has important applications.

Networks

- Network architectures
  - Network design principles
- Network types
  - Public Internet

Theory of Computation

- Models of computation
  - Quantum computation theory
- Computational complexity and cryptography
  - Cryptographic protocols
- Randomness, geometry and discrete structures
  - Error-correcting codes
- Theory and algorithms for application domains
  - Machine learning theory

Mathematics of Computing

- Information theory
  - Coding theory
- Mathematical analysis
  - Mathematical optimization

Information Systems

- World Wide Web
  - Web searching and information discovery
- Information retrieval
  - Retrieval models and ranking

Security and Privacy

- Cryptography
  - Symmetric cryptography and hash functions
- Network security
  - Security protocols

Computing Methodologies

- Machine learning
  - Machine learning approaches
- Computer graphics
  - Image manipulation

Applied Computing

- Electronic commerce
  - Online banking
- Operations research
  - Decision analysis

Chapter 1 PRELIMINARIES

1.1 Relations

Definition 1.1.1 A triple $r = (A, B, R)$, where A, B are sets and

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

is called a *(binary) relation*.
The set A is called the *domain*, the set B is called the *codomain* and the set R is called the *graph* of the relation r.
If $A = B$, then the relation r is called *homogeneous*.
If $(a, b) \in R$, then we sometimes write $a\,r\,b$ and we say that *a has the relation r to b* or *a and b are related with respect to the relation r*.

Definition 1.1.2 Let $r = (A, B, R)$ be a relation and let $X \subseteq A$. Then the set

$$r(X) = \{b \in B \mid \exists x \in X : x\,r\,b\}$$

is called the *relation class of X with respect to r*. If $x \in X$, then we denote

$$r < x >= r(\{x\}) = \{b \in B \mid x\,r\,b\}.$$

Remark 1.1.3 (1) Let $r = (A, B, R)$ be a relation and let $X \subseteq A$. Notice that

$$r(X) = \bigcup_{x \in X} r < x > .$$

(2) As in the case of functions, if $A, B \subseteq \mathbb{R}$, then the graph of a relation $r = (A, B, R)$ may be represented as a subset of points of the real plane $\mathbb{R} \times \mathbb{R}$, whereas if A, B are any finite sets, then $r = (A, B, R)$ may be represented by a diagram consisting of two sets with elements and connecting arrows. For instance, let $r = (A, B, R)$, where $A = \{1, 2, 3\}$, $B = \{1, 2\}$ and

$$R = \{(1, 1), (1, 2), (3, 1)\}.$$

One may draw the two sets A and B, and arrows between the elements related by R, namely arrows from 1 to 1, from 1 to 2 and from 3 to 1.

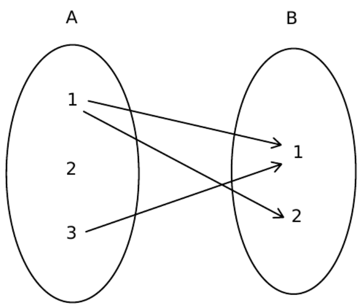

Figure 1.1: Diagram of a relation.

Also note that $r < 1 >= \{1, 2\} = r(A)$.

Example 1.1.4 (a) Let C be the set of all children and let P be the set of all parents. Then we may define the relation $r = (C, P, R)$, where

$$R = \{(c, p) \in C \times P \mid c \text{ is a child of } p\}.$$

(b) The triple $r = (\mathbb{R}, \mathbb{R}, R)$, where

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$$

is a homogeneous relation, called the *inequality relation* on $\mathbb{R}$. We have

$$r < 1 >= [1, \infty) = r([1, 2]).$$

(c) There are several examples from Number Theory, such as divisibility on $\mathbb{N}$ or on $\mathbb{Z}$, and Geometry, such as parallelism of lines, perpendicularity of lines, congruence of triangles, similarity of triangles.

(d) Let A and B be two sets. Then the triples

$$o = (A, B, \emptyset), \quad u = (A, B, A \times B)$$

are relations, called the *void relation* and the *universal relation* respectively.

(e) Let A be a set. Then the triple $\delta_A = (A, A, \Delta_A)$, where

$$\Delta_A = \{(a, a) \mid a \in A\}$$

is a relation called the *equality relation* on A.

(f) Every function is a relation. Indeed, a function $f : A \to B$ is determined by its domain A, its codomain B and its graph

$$G_f = \{(x, y) \in A \times B \mid y = f(x)\}.$$

Then the triple (A, B, G_f) is a relation.

(g) Every directed graph is a relation. Indeed, a directed graph (V, E) consists of a set V of vertices and a set E of directed edges ("arrows") between vertices. We may identify each directed edge with a pair in $V \times V$, where the first and the second component are respectively the starting and the ending vertex of that directed edge. Denote by P the set of those pairs. Then the triple (V, V, P) is a relation. For instance, the directed graph

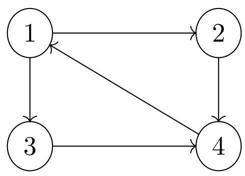

Figure 1.2: Directed graph.

may be seen as a relation (A, A, R), where $A = \{1, 2, 3, 4\}$ and

$$R = \{(1, 2), (1, 3), (2, 4), (3, 4), (4, 1)\}.$$

1.2 Functions

Definition 1.2.1 A relation $r = (A, B, R)$ is called a *function* if

$$\forall a \in A, \quad |r < a > | = 1,$$

that is, the relation class with respect to r of every $a \in A$ consists of exactly one element.

In other words, a relation r is a function if and only if every element of the domain has the relation r to exactly one element of the codomain.

In what follows, if $f = (A, B, F)$ is a function, we will mainly use the classical notation for a function, namely $f : A \to B$ or sometimes $A \xrightarrow{f} B$. The unique element of the set $f < a >$ will be denoted by $f(a)$. Then we have

$$(a, b) \in F \Longleftrightarrow f(a) = b.$$

In particular, from Definition 1.1.1 for a relation, we get the following corresponding notions for a function.

Definition 1.2.2 Let $f : A \to B$ be a function. Then A is called the *domain*, B is called the *codomain* and

$$F = \{(a, f(a)) \mid a \in A\}$$

is called the *graph* of the function f.

Example 1.2.3 (a) Let A be a set. Then the equality relation (A, A, Δ_A) is a function called the *identity function (map) on* A, that is denoted by $1_A : A \to A$ and is defined by $1_A(a) = a$, $\forall a \in A$.

(b) Let B be a set and let $A \subseteq B$. Then the relation (A, B, Δ_A) is a function called the *inclusion function of* A *into* B, that is denoted by $i : A \to B$ and is defined by $i(a) = a$, $\forall a \in A$.

(c) Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$ and let $r = (A, B, R)$, $s = (A, B, S)$, $t = (A, B, T)$ be the relations having the graphs

$$\begin{aligned} R &= \{(1, 1), (2, 1), (3, 2)\}, \\ S &= \{(1, 2), (3, 1)\}, \\ T &= \{(1, 1), (1, 2), (2, 1), (3, 2)\}. \end{aligned}$$

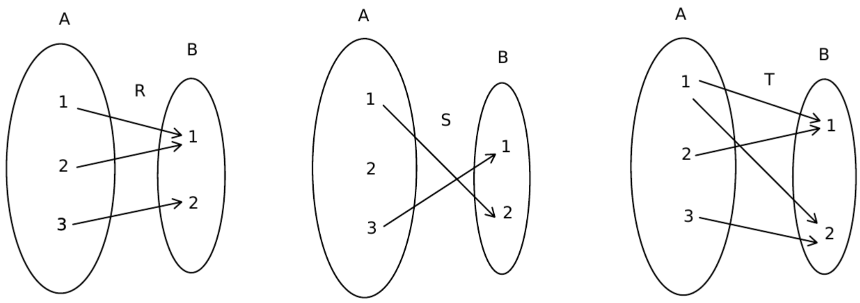

Figure 1.3: Diagrams of functions or relations.

Since $|r < a > | = 1$ for every $a \in A$, the relation r is a function. But s and t are not functions, because, for instance, we have $|s < 2 > | = 0$ and $|t < 1 > | = 2$.

Now we introduce a classical notation. Let A and B be two sets. Then we denote

$$B^A = \{f \mid f : A \to B \text{ is a function}\}.$$

If $|A| = n \in \mathbb{N}^*$, then the set B^A can be identified with the set $B^n = \underbrace{B \times \cdots \times B}_{n \text{ times}}$.

The notation is justified by the following nice result.

Theorem 1.2.4 *Let A and B be finite sets, say $|A| = n$ and $|B| = m$ $(m, n \in \mathbb{N}^*)$. Then*

$$|B^A| = m^n = |B|^{|A|}.$$

Definition 1.2.5 Let $f : A \to B$ be a function and let $X \subseteq A$.
We call the *image of* X *by* f the relation class of X with respect to f, that is,

$$f(X) = \{b \in B \mid \exists x \in X : x\, f\, b\} = \{f(x) \mid x \in X\}.$$

We denote $\mathrm{Im} f = f(A)$ and call it the *image of* f.

Homework: Recall the definitions and the properties of injective, surjective and bijective functions.

1.3 Equivalence relations and partitions

Recall that a relation $r = (A, B, R)$ is called *homogeneous* if $A = B$. Some special type of such relations is the subject of the present section.

Definition 1.3.1 A homogeneous relation $r = (A, A, R)$ on A is called:
(1) *reflexive* (r) if: $\quad \forall x \in A,\ x\,r\,x$.
(2) *transitive* (t) if: $\quad x, y, z \in A,\ x\,r\,y$ and $y\,r\,z \Longrightarrow x\,r\,z$.
(3) *symmetric* (s) if: $\quad x, y \in A,\ x\,r\,y \Longrightarrow y\,r\,x$.
A homogeneous relation $r = (A, A, R)$ is called an *equivalence relation* if r has the properties (r), (t) and (s).

Example 1.3.2 (a) The equality relation δ_A on a set A has all 3 properties, hence δ_A is an equivalence relation on A.

(b) The similarity of triangles is an equivalence relations on the set of all triangles.

(c) The inequality relation " $\leq$ " on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$ has (r) and (t), but not (s). Hence it is not an equivalence relation on the corresponding set.

(d) Let $n \in \mathbb{N}$ and let ρ_n be the relation defined on $\mathbb{Z}$ by

$$x\,\rho_n\,y \Longleftrightarrow x \equiv y \pmod{n},$$

that is, $n|(x-y)$ or equivalently for $n \neq 0$, x and y give the same remainder when divided by n. Then ρ_n is called the *congruence modulo* n and it has the properties (r), (t) and (s), hence it is an equivalence relation.

For $n = 0$, we have $x\,\rho_0\,y \Longleftrightarrow 0|x-y \Longleftrightarrow x = y$, hence $\rho_0 = \delta_{\mathbb{Z}} = (\mathbb{Z}, \mathbb{Z}, \Delta_{\mathbb{Z}})$.

For $n = 1$, we have $x\,\rho_1\,y \Longleftrightarrow 1|x-y$, which is always true, and thus $\rho_1 = u = (\mathbb{Z}, \mathbb{Z}, \mathbb{Z} \times \mathbb{Z})$.

Definition 1.3.3 Let A be a non-empty set. Then a family $(A_i)_{i \in I}$ of non-empty subsets of A is called a *partition* of A if:
(i) The family $(A_i)_{i \in I}$ covers A, that is,

$$\bigcup_{i \in I} A_i = A.$$

(ii) The A_i's are pairwise disjoint, that is,

$$i, j \in I, i \neq j \Longrightarrow A_i \cap A_j = \emptyset.$$

Example 1.3.4 (a) Let $A = \{1, 2, 3, 4, 5\}$ and $A_1 = \{1, 2, 3\}$, $A_2 = \{4\}$, $A_3 = \{5\}$. Then $\{A_1, A_2, A_3\}$ is a partition of A.

(b) Let A be a set. Then $\{\{a\} \mid a \in A\}$ and $\{A\}$ are partitions of A.

(c) Let A_1 be the set of even integers and A_2 the set of odd integers. Then $\{A_1, A_2\}$ is a partition of $\mathbb{Z}$.

(d) Consider the intervals

$$A_n = [n, n+1)$$

for every $n \in \mathbb{Z}$. Then the family $(A_n)_{n \in \mathbb{Z}}$ is a partition of $\mathbb{R}$.

Denote by $E(A)$ the set of all equivalence relations and by $P(A)$ the set of all partitions on a set A.

Definition 1.3.5 Let $r \in E(A)$.
The relation class $r < x >$ of an element $x \in A$ with respect to r is called the *equivalence class of x with respect to r*, while the element x is called a *representative* of $r < x >$.
The set

$$A/r = \{r < x >|\, x \in A\},$$

which is the set of all equivalence classes of elements of A with respect to r, is called the *quotient set of A by r*.

Definition 1.3.6 Let $\pi = (A_i)_{i \in I} \in P(A)$ and define the relation r_π on A by

$$x\, r_\pi\, y \Longleftrightarrow \exists i \in I : x, y \in A_i\,.$$

Then r_π is called the *relation associated to the partition π*.

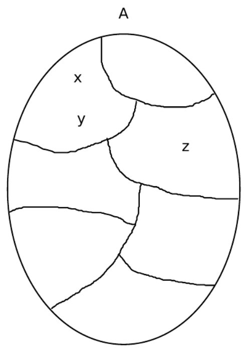

Figure 1.4: Relation associated to a partition.

The following theorem establishes the fundamental connection between equivalence relations and partitions.

Theorem 1.3.7 *(i) Let $r \in E(A)$. Then $A/r \in P(A)$.*
(ii) Let $\pi = (A_i)_{i \in I} \in P(A)$. Then $r_\pi \in E(A)$.
(iii) Let $F : E(A) \to P(A)$ be defined by

$$F(r) = A/r, \quad \forall r \in E(A).$$

Then F is a bijection, whose inverse is $G : P(A) \to E(A)$, defined by

$$G(\pi) = r_\pi, \quad \forall \pi \in P(A).$$

Example 1.3.8 (a) Consider the set A of all first-year students in Computer Science, and its partition, say $\pi = \{A_1, \dots, A_7\}$, where A_i denotes the set of all students in Group i for $i \in \{1, \dots, 7\}$. Then the equivalence relation r_π on A corresponding to the partition π is defined as follows: student $x \in A$ has relation r_π to student $y \in A$ if and only if students x and y are in the same group i.

(b) Let $A = \{1, 2, 3\}$ and let r and s be the homogeneous relations defined on A with the graphs

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}\,,$$
$$S = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}\,.$$

Then r is an equivalence relation, but s is not. The partition corresponding to r is

$$A/r = \{\{1,2\}, \{3\}\}\,.$$

(c) Consider the following families of sets:

$$\pi = \{\{1\}, \{2,3\}, \{4\}\},$$

$$\pi' = \{\{1,2\}, \{2,3\}, \{4\}\}.$$

Then π is a partition of $A = \{1,2,3,4\}$, but π' is not. The equivalence relation corresponding to π has the graph

$$R_\pi = \{(1,1), (2,2), (2,3), (3,2), (3,3), (4,4)\}\,.$$

(d) The congruence relation modulo n is an equivalence relation on $\mathbb{Z}$ and its corresponding partition is

$$\mathbb{Z}/\rho_n = \{\rho_n < x >| \; x \in \mathbb{Z}\} = \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\} = \{\widehat{x} \mid x \in \mathbb{Z}\}\,,$$

where an equivalence class is denoted by $\widehat{x}$. For $n \geq 2$, we denote

$$\mathbb{Z}_n = \mathbb{Z}/\rho_n = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}\,.$$

For $n = 0$ and $n = 1$, we have seen in Example 1.3.2 that $\rho_0 = \delta_{\mathbb{Z}}$ and $\rho_1 = u$, and we get

$$\mathbb{Z}/\rho_0 = \{\{x\} \mid x \in \mathbb{Z}\} \quad \text{and} \quad \mathbb{Z}/\rho_1 = \{\mathbb{Z}\}\,,$$

that are the two extreme partitions of $\mathbb{Z}$.

Extra: Relational database

Binary relations may be naturally generalized as follows.

Definition 1.3.9 A (finite) tuple

$$r = (A_1, \dots, A_n, R),$$

where $A_1, \dots, A_n$ are sets and

$$R \subseteq A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\},$$

is called an *(n-ary) relation*. The sets $A_1, \dots, A_n$ are called the *domains* of r, and the set R is called the *graph* of r. The number n is called the *degree (arity)* of r. A *relational database* is a (finite) set of relations.

Example 1.3.10 Consider the relation

$$student = (Integer, String, String, Integer, Student),$$

where

$$Student \subseteq Integer \times String \times String \times Integer$$

is given by the following table:

ID (Integer)	**Surname** (String)	**Name** (String)	**Grade** (Integer)
7	Ionescu	Alina	9
11	Ardelean	Cristina	10
23	Ionescu	Dan	7

Remark 1.3.11 Some known relational database management systems are:

- Oracle and RDB – Oracle
- SQL Server and Access - Microsoft