Course 1: 04.10.2021

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. N. Both, S. Crivei, *Culegere de probleme de algebră*, Lito UBB Cluj-Napoca, 1996.
  2. G. Călugăreanu, *Lecţii de algebră liniară*, Lito UBB, Cluj-Napoca, 1995.
  3. S. Crivei, *Basic abstract algebra, Casa Cărţii de Ştiinţă*, Cluj-Napoca, 2002, 2003.
  4. J. Gilbert, L. Gilbert, *Elements of Modern Algebra*, PWS-Kent, 1992.
  5. W.J. Gilbert, W.K. Nicholson, *Modern Algebra with Applications*, John Wiley, 2004.
  6. P.N. Klein, *Coding the Matrix. Linear Algebra through Applications to Computer Science*, Newtonian Press, 2013.
  7. R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer-Verlag, 1998.
  8. I. Purdea, C. Pelea, *Probleme de algebră*, Eikon, Cluj-Napoca, 2008.

- **Course:**

  Course materials will be uploaded on the Microsoft Teams platform.

  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:**

  Problems for the next week will be uploaded on the Microsoft Teams platform after the course.

  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:**

  Partial exams in **Week 8** (Chapters 1-2) and **Week 14** (Chapters 3-4) (most likely on Saturday, November 20, 2021 and Saturday, January 15, 2022).

  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.

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.*

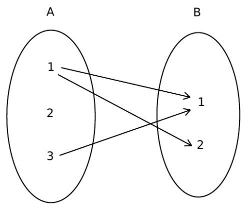
Definition 1.1.2 Let $r = (A, B, R)$ be a relation and let $X \subseteq A$. Then the set

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

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 One may represent relations (defined on finite sets) by diagrams. E.g., let $r = (A, B, R)$, where $A = \{1, 2, 3\}$, $B = \{1, 2\}$ and $R = \{(1, 1), (1, 2), (3, 1)\}$. As in the case of functions, 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. Also note that $r < 1 >= \{1, 2\} = r(A)$.



Example 1.1.4 (a) Let C be the set of all children and 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 $r < 1 >= [1, \infty)$ and $r([1, 2]) = [1, \infty)$.

(c) Examples from Number Theory and Geometry, e.g. divisibility on $\mathbb{N}$, parallelism of lines, perpendicularity of lines, congruence of triangles, similarity of triangles.

(d) Let A and B be two sets. Then the triples $o = (A, B, \emptyset)$ and $u = (A, B, A \times B)$ 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.

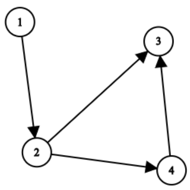
(f) Every function is a relation. Indeed, a function $f : A \to B$ is determined by its domain A, its codomain B and its graph

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

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



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

1.2 Functions

Definition 1.2.1 A relation $r = (A, B, R)$ is called a *function* if $\forall a \in A$, $|r < a > | = 1$.

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

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

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

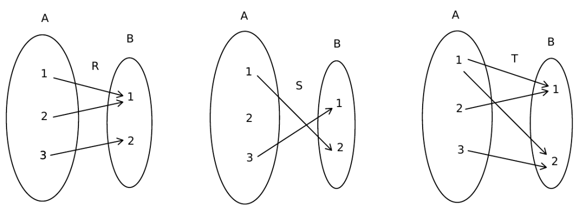
the *graph* of the function f. If $X \subseteq A$, then the relation class of X with respect to f, that is,

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

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

Example 1.2.3 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

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



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 $|t < 1 > | = 2$.

If A and B are 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 $B^n = \underbrace{B \times \cdots \times B}_{n \text{ times}} = \{(b_1, \ldots, b_n) \mid b_1, \ldots, b_n \in B\}$.

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

Homework: recall from High School the properties of injective, surjective and bijective functions.

1.3 Equivalence relations and partitions

Definition 1.3.1 A homogeneous relation $r = (A, A, R)$ on A is called:

- *reflexive* (r) if: $\forall x \in A$, $x\, r\, x$;
- *transitive* (t) if: $x, y, z \in A$, $x\, r\, y$ and $y\, r\, z \Longrightarrow x\, r\, z$;
- *symmetric* (s) if: $x, y \in A$, $x\, r\, y \Longrightarrow y\, r\, x$.
- *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 (r), (t) and (s), 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

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

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.

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_1 be the set of even integers and A_2 the set of odd integers. Then $\{A_1, A_2\}$ is a partition of $\mathbb{Z}$.

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

(d) Consider the intervals $A_n = [n, n+1)$ for $n \in \mathbb{Z}$. 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 $A/r = \{r<x>\mid x \in A\}$, 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*.

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

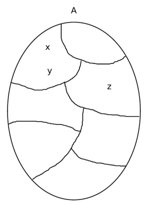
Theorem 1.3.6 *(i) Let $r \in E(A)$. Then*

$$A/r = \{r<x>\mid x \in A\} \in P(A).$$

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

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

Then $r_\pi \in E(A)$.



(iii) Let $F : E(A) \to P(A)$ be defined by $F(r) = A/r$, $\forall r \in E(A)$. Then F is a bijection, whose inverse is $G : P(A) \to E(A)$, defined by $G(\pi) = r_\pi$, $\forall \pi \in P(A)$.

Example 1.3.7 (a) Let $A = \{1,2,3\}$ and let r and s be the homogeneous relations on A with the graphs

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

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

$$A/r = \{r<a>\mid a \in A\} = \{\{1,2\},\{3\}\}.$$

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

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

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

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

where an equivalence class is denoted by $\widehat{x}$.

Extra: Relational database

Definition 1.3.8 A (finite) tuple $r = (A_1, \ldots, A_n, R)$, where $A_1, \ldots, A_n$ are sets and

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

is called an *(n-ary) relation.* The sets $A_1, \ldots, A_n$ 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 1.3.9 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 1.3.10 Some known relational database management systems are:

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