Summary on Lecture 13, November 24, 2014

- **Cartesian products and relations.** We recall that a Cartesian product of two sets A and B is defined as

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

Examples: The Euclidian plane $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$, the Euclidian space $\mathbf{R}^3 = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$; the upper-right corner $\mathbf{R}_+ \times \mathbf{R}_+$; the integral latices:

$$\mathbf{Z} \times \mathbf{Z} \subset \mathbf{R} \times \mathbf{R}, \qquad \mathbf{Z}_+ \times \mathbf{Z}_+ \subset \mathbf{R}_+ \times \mathbf{R}_+.$$

There are the following properties of the Cartesian products:

Theorem. Let $A, B, C \subset \mathcal{U}$, where $\mathcal{U}$ be a "universe". Then

(a) $A \times \emptyset = \emptyset$;

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

(c) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

(d) $(B \cap C) \times A = (B \times A) \cap (C \times A)$;

(e) $(B \cup C) \times A = (B \times A) \cup (C \times A)$.

Exercise. Prove (a), (b) and (c).

Definition. A subset $\mathcal{R} \subset A \times B$ is called a *binary relation from A to B.* In the case when $A = B$, a subset $\mathcal{R} \subset A \times A$ is called a *binary relation on A.*

Let $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$ be finite sets. Then we can count how many binary relations $\mathcal{R} \subset A \times B$ do we have. Indeed, the set $A \times B$ has $m \cdot n$ elements, thus there are 2^{mn} subsets of $A \times B$ (or binary relations from A to B).

There are several very important relations in mathematics.

The equivalence relation. A binary relation $\mathcal{R}$ on A is an equivalence relation if it satisfies the following conditions:

(R) $(a,a) \in \mathcal{R}$ for all $a \in A$;

(S) If $(a,b) \in \mathcal{R}$ then $(b,a) \in \mathcal{R}$;

(T) If $(a,b) \in \mathcal{R}$ and $(b,c) \in \mathcal{R}$, then $(a,c) \in \mathcal{R}$.

The abbreviations (R), (S) and (T) stand for "reflexivity", "symmetry" and "transitivity", respectively. To simplify the notations, we denote by $a \sim b$ iff $(a,b) \in \mathcal{R}$, and $\mathcal{R}$ is an equivalence relation.

Important example.

- Let $n > 1$ be a positive integer. We define the equivalence relation $a \sim_n b$ iff $a - b$ is divisible by n. Clearly, $a \sim_n b$ when a and b have the same remainders: $(a \ \mathsf{DIV}\ n) = (a \ \mathsf{DIV}\ n)$. Then we can put together all integers in n different classes:

$$\mathbf{0} := \{0, \pm n, \pm 2 \cdot n, \ldots\}, \quad \mathbf{1} := \{1, 1 \pm n, 1 \pm 2 \cdot n, \ldots\}, \quad \mathbf{2} := \{2, 2 \pm n, 2 \pm 2 \cdot n, \ldots\},$$
$$\mathbf{3} := \{3, 3 \pm n, 3 \pm 2 \cdot n, \ldots\}, \ \cdots, (\mathbf{n-1}) := \{(n-1), (n-1) \pm n, (n-1) \pm 2 \cdot n, \ldots\}.$$

We see that $\mathbf{Z} = \mathbf{0} \cup \mathbf{1} \cup \mathbf{2} \cup \cdots \cup (\mathbf{n-1})$. The set of classes $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, (\mathbf{n-1})\}$ is denoted by $\mathbf{Z}/n$. See Lecture 11 for the addition and multiplication tables when $n = 5, 6$.

We say that subsets $\{A_i\}_{i\in I}$, $A_i \subset A$ form a *partition of* A iff

(1) $A = \bigcup_i A_i$,

(2) $A_i \cap A_j = \emptyset$ if $i \neq j$.

Let $\sim$ be an equivalence relation on A. Then we denote by $[a]$ the set

$$[a] := \{ \ a' \in A \mid a \sim a' \ \}.$$

We denote the set $\{ \ [a] \mid a \in A \ \}$ by $[A]$. **Lemma 1.** Let $\sim$ be an equivalence relation on A. The following assertions are equivalent:

(1) $a \sim a'$,

(2) $[a] = [a']$,

(3) $[a] \cap [a'] \neq \emptyset$.

Proof. $(1) \to (2)$. We assume that $a \sim a'$. If $a_1 \in [a]$, then $a_1 \sim a$. Since $a_1 \sim a$ and $a \sim a'$, then $a_1 \sim a'$ by transitivity. If $a_1' \in [a']$, then $a_1' \sim a'$. By the symmetry, $a \sim a'$ implies $a' \sim a$. Then $a_1' \sim a'$ and $a' \sim a$ imply that $a_1' \sim a$ by transitivity.

$(2) \to (3)$ We assume that $[a] = [a']$. In particular, $a \in [a]$ by reflexivity. Then $a \in [a']$. Thus $a \in [a] \cap [a']$, i.e., $[a] \cap [a'] \neq \emptyset$.

$(3) \to (1)$ We assume that $[a] \cap [a'] \neq \emptyset$, then we find $a_1 \in [a]$ and $a_1 \in [a']$. This means that $a_1 \sim a$ and $a_1 \sim a'$. By symmetry, $a_1 \sim a$ implies that $a \sim a_1$. Then, since $a \sim a_1$ and $a_1 \sim a'$, transitivity implies that $a \sim a'$. □

Theorem 1. (1) Let $\sim$ be an equivalence relation on A, where $A \neq \emptyset$. Then the set $[A]$ is a partition of A.

(2) Let $\{A_i\}_{i\in I}$ be a partition of A. Then A_i are equivalence classes of the following equivalence relation:

$$a \sim a' \ \text{ if and only if there exists } i \in I \text{ such that } a, a' \in A_i$$

Exercise. Prove Theorem 1.

Partial order relation. Let $A = \mathbf{Z}_+$, $\mathbf{Z}$ or $A = \mathbf{R}$. We define a partial order relation

$$\mathcal{R} := \{ \ (a, b) \mid a \leq b \ \} \subset A \times A.$$

Consider the case $A = \mathbf{Z}_+$. We define the same partial order recursively as follows:

(B) $1 \leq 1$

(R) If $a \leq b$, then $a \leq b + 1$, and $a + 1 \leq b + 1$.

- **Back to functions** $f : A \to B$. Recall that a function (or a map) $f : A \to B$ means that each $a \in A$ it is assigned a value $f(a) \in B$. The set A is called the *domain* of f, and B is the *target* (or *codomain*). The element $b = f(a)$ is the *image* of a; then for an element b the set $f^{-1}(b) = \{ \ a \in A \mid f(a) = b \ \}$ is called the *inverse image of* b. The set

$$\Gamma(f) = \{ \ (a, b) \mid f(a) = b \ \} \subset A \times B$$

is called the *graph of* $f : A \to B$. The set $f(A) \subset B$ is called a *range* of f.

Two functions $f, g : A \to B$ are *equal* iff $f(a) = g(a)$ for every element $a \in A$.

Exercises.

(1) $f : \mathbf{R} \to \mathbf{Z}$ is given as $f(x) = \lfloor x \rfloor$. Give a graph of f.

(2) $f : \mathbf{R} \to \mathbf{R}$ is given as $f(x) = x^{2015} + 1$. Find the range of f.

We already have seen many example of functions. Let $\mathcal{F}(A, B)$ be the set of functions $f \to B$. For two finite sets $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$ we have seen that $|\mathcal{F}(A, B)| = n^m$.

We say that a function $f : A \to B$ is *one-to-one* iff $f(a) = f(a')$ implies that $a = a'$, i.e., no two elements in A have the same image in B. Let $\mathcal{F}^{\text{one-to-one}}(A, B)$ be the set of one-to-one functions $f : A \to B$. Now we assume that A and B are finite sets with $|A| = m$ and $|B| = n$.

Question: What is the size of the set $\mathcal{F}^{\text{one-to-one}}(A, B)$?

Clearly, if $|A| > |B|$, we do not have any one-to-one function $f : A \to B$. Indeed, then we do not have enough different values to assign for all elements of A.

To answer the question, we assume that $m \leq n$.

Exercise.

(3) Prove that $|\mathcal{F}^{\text{one-to-one}}(A, B)| = n(n-1) \cdots (n-m+1)$.

Recall that a function $f : A \to B$ is *onto* iff $f(A) = B$. Let $\mathcal{F}^{\text{onto}}(A, B) \subset \mathcal{F}(A, B)$ be the set of all functions $f : A \to B$ which are onto.

Question: What is the size of the set $\mathcal{F}^{\text{onto}}(A, B)$?

We already know that (see Lecture 8):

$$|\mathcal{F}^{\text{onto}}(A, B)| = \sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m.$$

Now we can think about this fact as follows. We have m (indistinguishable) objects and n numbered containers. Then we have $\sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m$ ways to put m (indistinguishable) objects into n numbered containers, so that no container would be empty.

Then we can remove the numbers from our "containers", and we conclude that there are

$$S(m, n) = \frac{1}{n!} \sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m \tag{1}$$

ways to put m (indistinguishable) objects into n (indistinguishable) containers, so that no container would be empty. The number $S(m, n)$ is called a *Stirling number of the second kind.*