Mathematical Logic
Lecture 5
06.11.2023

Theorem 1 (characterization of injective functions).

Let $f: A \to B$ be a function. The following statements are equivalent:

(i) f is injective.

(ii) f is left-cancelable:

$$A' \underset{\beta}{\overset{\alpha}{\rightrightarrows}} A \xrightarrow{f} B$$

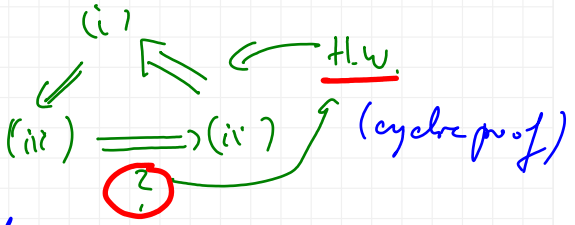
i.e. $\forall \alpha, \beta : A' \to A.$

$$f \circ \alpha = f \circ \beta \Longrightarrow \alpha = \beta$$

(iii) (Assume $A \neq \emptyset$) f has a left inverse (retraction):

$$A \xrightarrow{f} B \qquad \text{i.e. } \exists\, r : B \to A \text{ s.t. } r \circ f = \mathrm{id}_A$$
$$A \xleftarrow{r} B$$

(i) $\Longleftrightarrow$ (ii)
$\Uparrow$
(iii)



$$(p \to (q \to r)) \Longleftrightarrow (p \wedge q \to r)$$

Proof

(i) $\Rightarrow$ (ii) We assume that f is injective.

Let $\alpha, \beta : A' \to A$ such that $f \circ \alpha = f \circ \beta$.

We prove that $\alpha = \beta$.

Let $a' \in A'$. We know $(f \circ \alpha)(a') = (f \circ \beta)(a')$

hence: $f(\alpha(a')) = f(\beta(a')) \overset{f \text{ inj}}{\Longrightarrow} \alpha(a') = \beta(a')$.

So $\alpha = \beta$.

$$(p \to q) \Longleftrightarrow (\neg q \to \neg p)$$

contraposition.
proof by contradiction.

(ii) $\Rightarrow$ (i) We assume that f is not inj.

$\neg$(i) $\Rightarrow$ $\neg$(iii) So $\exists\, x_1, x_2 \in A$, $x_1 \neq x_2$ and $f(x_1) = f(x_2)$

We will prove that $\exists \alpha, \beta : A' \to A$ s.t.

$f \circ \alpha = f \circ \beta$ and $\alpha \neq \beta$.

$$\neg(p \to q) \Longleftrightarrow \neg(\neg p \vee q) \Longleftrightarrow p \wedge \neg q$$

Let $A' = \{x_1, x_2\}$. Let $\alpha, \beta : A' \longrightarrow A$

	x_1	x_2
$\alpha(x)$	x_1	x_2
$\beta(x)$	x_1	x_1

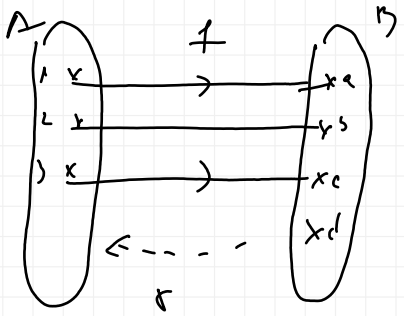
so $\alpha \neq \beta$.

$$\left.\begin{cases} (f\circ\alpha)(x_1) = f(\alpha(x_1)) = f(x_1) \\ (f\circ\alpha)(x_2) = f(\alpha(x_2)) = f(x_2) \end{cases}\right\} \Rightarrow f\circ\alpha = f\circ\beta.$$

$$\begin{cases} (f\circ\beta)(x_1) = f(\beta(x_1)) = f(x_1) \\ (f\circ\beta)(x_2) = f(\beta(x_2)) = f(x_1) = f(x_2) \end{cases}$$

(i) $\Rightarrow$ (iii) We assume that f is injective on $A \neq \emptyset$.

Example



$r(a) = 1$
$r(b) = 2$
$r(c) = 3$
$r(d) \in A$ so there are 3 possibly.
So f has 3 different retractions

We define $r : B \longrightarrow A$. Let $b \in B$.

- If $b \in \operatorname{Im} f$ then $\exists!\, a \in A$ s.t. $f(a) = b$.
  Define $r(b) = a$
- If $b \notin \operatorname{Im} f$ then $r(b)$ can be any element of A

We have $(r\circ f)(a) = r(f(a)) = r(b) = a$ $\forall a \in A$

$\Rightarrow r\circ f = 1_A$ $\qquad 1_A(a)$

(iii) $\Rightarrow$ (i) Let r be a left inverse of f.
We show that f is injective.

Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$.

We get $r(f(x_1)) = r(f(x_2)) \Rightarrow (r \circ f)(x_1) = (r \circ f)(x_2)$

By assumption we get $1(x_1) = 1(x_2)$, i.e. $x_1 = x_2$. ∎

Theorem 2 (characterization of surjective functions)

Let $f : A \to B$ be a function. The following statements are equivalent:

(i) f is surjective.

(ii) f is right-cancellable:

$$A \xrightarrow{f} B \underset{\beta}{\overset{\alpha}{\rightrightarrows}} B'$$

i.e. $\forall \alpha, \beta : B \to B'$

$\alpha \circ f = \beta \circ f \Rightarrow \alpha = \beta$

(iii) f has a right inverse (section):

$$A \underset{s}{\overset{f}{\leftrightarrows}} B$$

i.e. $\exists s : B \to A$ such that $f \circ s = 1_B$

Proof (i) $\Rightarrow$ (ii) Assume that f is surjective.

Let $\alpha, \beta : B \to B'$ such that $\alpha \circ f = \beta \circ f$.

We will prove that $\alpha = \beta$.

Let $b \in B$. Then $\exists a \in A$ such that $f(a) = b$.

We have $\alpha(b) = \alpha(f(a)) = (\alpha \circ f)(a) \overset{\text{hyp}}{=} (\beta \circ f)(a)$

$= \beta(f(a)) = \beta(b)$

Hence $\alpha = \beta$.

(ii) $\Rightarrow$ (i)

$\Leftrightarrow$

$\neg$(i) $\Rightarrow$ $\neg$(ii)

We assume that f is not surjective.

Hence $\exists\, b_0 \in B \setminus \mathrm{Im} f$, i.e.

$$f(a) \neq b_0 \quad \forall\, a \in A.$$

We want to find two functions $\alpha, \beta : B \to B'$ s.t.

$$\alpha \circ f = \beta \circ f \quad \text{and} \quad \alpha \neq \beta.$$

Let $B' := B$. Let $\alpha : B \to B$, $\alpha(b) = b \ \forall\, b \in B$.

Let $\beta : B \to B$, $\beta(b) = \begin{cases} b, & \text{if } b \neq b_0 \\ b_1 \neq b_0, & \text{if } b = b_0 \end{cases}$

Hence $\alpha \neq \beta$.

Now let $a \in A$: we have

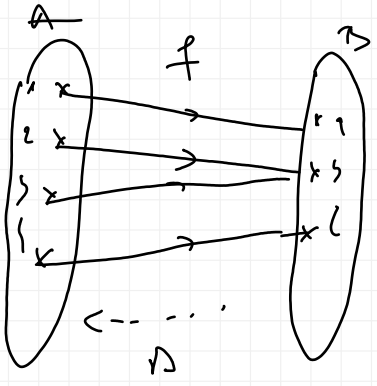
$$(\alpha \circ f)(a) = \alpha(f(a)) = f(a).$$

$$(\beta \circ f)(a) = \beta(f(a)) = f(a) \quad \text{because } f(a) \neq b_0$$

Hence $\alpha \circ f = \beta \circ f$

(i) $\Rightarrow$ (iii)

Exple:



$D(a) = 1$

$D(b)$ can be 2 or 3

$D(c) = 4$.

Assume that f is surjective. Let $b \in B$. We choose an element a s.t. $f(a) = b$ (we have $f^{-1}(b) = \emptyset$)

Define $D(b) = a$. We have:

$$(f \circ D)(b) = f(D(b)) = f(a) = b = 1_B(b)$$

Hence $f \circ D = 1_B$.

(iii) $\Rightarrow$ (i) Let $g: B \to A$ s.t. $f \circ g = \mathbb{1}_B$.

We prove that f is surjective.

Let $b \in B$. Let $a := g(b)$

We have $f(a) = f(g(b)) = (f \circ g)(b) \overset{\text{hypothesis}}{=} \mathbb{1}_B(b) = b$.

Thus $b \in \operatorname{Im} f$, hence f is surj. ∎

Theorem (characterization of bijective functions)

Let $f: A \to B$ be a function. Then:

f is bijective $\iff$ f is invertible (i.e. $\exists\, g: B \to A$ s.t. $g \circ f = \mathbb{1}_A$ and $f \circ g = \mathbb{1}_B$.)

Proof. "$\Rightarrow$". Assume that f is bijective. We want to find an inverse of f.

Let $b \in B$. Then $\exists!\, a \in A$ s.t. $f(a) = b$

We define $g(b) = a$.

We have: $(g \circ f)(a) = g(f(a)) = g(b) = a = \mathbb{1}_A(a)$

$(f \circ g)(b) = f(g(b)) = f(a) = b = \mathbb{1}_B(b)$

"$\Leftarrow$". g is a left inverse for $f \overset{\text{Thm 1}}{\Rightarrow} f$ is injective

g is a right inverse for $f \overset{\text{Thm}}{\Rightarrow} f$ is surjective.

Remarks 1) A bijective function has a unique inverse.

Indeed: if g_1, g_2 are inverses, then

$\mathbb{1}_A = g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2$

We denote the unique inverse of f by f^{-1}.

We have. $\boxed{f(x) = y \iff f^{-1}(y) = x}$

2) We know that any function f has the inverse relation $f^{-1} = (B, A, F^{-1})$, which is not a function in general. The above argument show that the rel f^{-1} is a function $\iff f$ is bijective

Homework: ex. 42 – 46, 51, 52

Equivalence relations

Def 1. A homogeneous relation $\rho = (A, A, R)$ is called an **equivalence relation** if:

Prerequisites:

(R) ρ is **reflexive**: $\forall x \in A \quad x \rho x$ (i.e. $1_A \subseteq \rho$)

not reflexive

ex d_1 $\perp$ d_2

because $d_1 \perp d_1$

(T) ρ **is transitive**: $\forall x, y, z \in A \quad x \rho y$ and $y \rho z \Rightarrow x \rho z$

(i.e. $x \rho \circ \rho z \Rightarrow x \rho z$

i.e. $\rho \circ \rho \subseteq \rho$)

(S) ρ is **symmetric**: $\forall x, y \in A \quad x \rho y \Rightarrow y \rho x$

(ρ is not sym: $\exists x, y \in A$ s.t. $x \rho y$ and $y \not\rho x$ | (i.e. $\rho = \bar{\rho}^{-1}$)

Examples 1). the equality relation on A: $1_A = (A, A, D_A)$ is equivalence

2). **Divisibility on $\mathbb{Z}$**: $a \mid b \overset{\text{def}}{\Leftrightarrow} \exists x \in \mathbb{Z}$ s.t. $b = ax$

Rem . $a \mid 0 \ \forall a \in \mathbb{Z}$ bc $0 = 0 \cdot a$

. in part $0 \mid 0$ (0 : 0 not defined)

. $0 \mid a \Leftrightarrow a = 0$

(R) $a \mid a$ ✓ bc $a = 1 \cdot a$

(T) assm $a \mid b$, $b \mid c$ so $\exists x, y \in \mathbb{Z}$ s.t. $b = ax$, $c = by$.

then $c = axy$ so $a \mid c$

(S) $a \mid b \overset{?}{\Rightarrow} b \mid a$ not in gen. eg $2 \mid 4$ and $4 \nmid 2$

3) The relation of <u>congruence modulo n</u> on $\mathbb{Z}$

Let $n \in \mathbb{N}$. We define the relation $\equiv (\mathrm{mod}\, n)$ on $\mathbb{Z}$:

If $a, b \in \mathbb{Z}$, then $a \equiv b (\mathrm{mod}\, n) \overset{\text{def}}{\iff} n \mid b-a$

e.g. $22 \equiv 57 (\mathrm{mod}\, 5)$

(R) $a \equiv a (\mathrm{mod}\, n) \iff n \mid a-a$ (true)

(T) $a \equiv b (\mathrm{mod}\, n)$, $b \equiv c (\mathrm{mod}\, n) \Longrightarrow$

$\Rightarrow n \mid b-a$, $n \mid c-b \Rightarrow n \mid (b-a)+(c-b)$

$\Rightarrow n \mid c-a \Rightarrow a \equiv c (\mathrm{mod}\, n)$

(S) $a \equiv b (\mathrm{mod}\, n) \Rightarrow n \mid b-a \Rightarrow n \mid a-b \Rightarrow b \equiv a (\mathrm{mod}\, n)$

Hence $\equiv (\mathrm{mod}\, n)$ is an equivalence relation on $\mathbb{Z}$.

<u>Def 2</u> Let A be a set. A subset $\Pi \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$

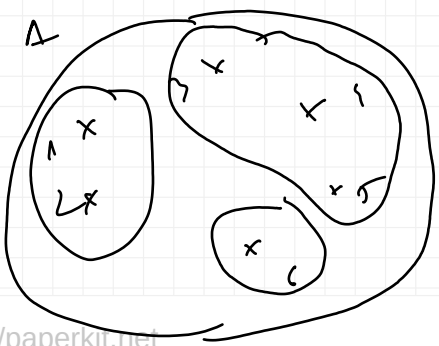
(i.e. Π is a set of nonempty subsets of A)

is called a <u>partition of A</u> if

$\forall x \in A \quad \exists! B \in \Pi$ such that $x \in B$

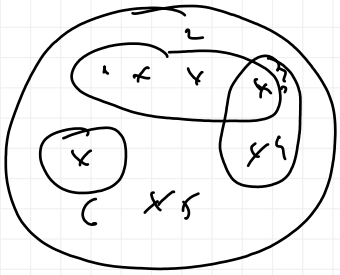
(i.e. any element of A belongs to exactly one class of the partition Π)

Equivalently, Π satisfies: $\begin{cases} (1) \bigcup_{B \in \Pi} B = A \\ (2) \forall B, B' \in \Pi,\ B \neq B' \Rightarrow B \cap B' = \emptyset \end{cases}$



$A = \{1, 2, 3, 4, 5, 6\}$

$\Pi = \{\{1,2\}, \{3,4,5\}, \{6\}\}$.



not a partition

$\Pi = \{\{1,2,3\}, \{3,4\}, \{6\}\}$

Theorem 1 Let Π be a partition of the set A.

We define on A the relation $\rho_\Pi = (A, A, R_\Pi)$ as follows:

$$\forall x, y \in A : \quad x \rho_\Pi y \overset{\text{def}}{\Longleftrightarrow} \exists B \in \Pi \text{ s.t. } x, y \in B.$$

Then: ρ_Π is an equivalence relation on A.

Example: in the previous example:

$$R_\Pi = \{(1,1), (2,2), (1,2), (2,1), (3,4), (3,3), (3,5), (4,4), (4,3), (4,5), (5,5), (5,3), (5,4), (6,6)\}$$

Homework: ex. 55 – 61