ZBIÓR LICZB WYMIERNYCH

Zbiór liczb wymiernych $\mathbb{Q}$ ma kilka różnych naturalnych struktur:

1. $(\mathbb{Q}, <)$ jest zbiorem liniowo uporządkowanym.
2. $(\mathbb{Q}, +)$ jest grupą przemienną.
3. $(\mathbb{Q}, +, \cdot, 0, 1)$ jest ciałem.

DEF. Częściowym porządkiem na zbiorze X nazywamy relację $\leq$ spełniającą warunki

(CP0) $x \leq x$, (zwrotność)

(CP1) $x \leq y$ i $y \leq z \Rightarrow x \leq z$, (przechodniość)

(CP2) $x \leq y$ i $y \leq x \Rightarrow x = y$, (antysymetria)

dla każdych $x, y, z \in X$.

Porządek $\leq$ nazywamy liniowym, jeśli

(PL) $(\forall x, y \in X)$ $x \leq y$ lub $y \leq x$.

Mając daną relację porządku $\leq$ definiujemy relację $<$ formułą

$$x < y \overset{df}{\iff} x \leq y \text{ oraz } x \neq y.$$

> $x \leq y$ czytamy „x mniejsze lub równe y"
>
> $x < y$ czytamy „x mniejsze od y"

Zachodzi równoważność

$$x \leq y \iff x < y \text{ lub } x = y.$$

Parę $(X, \leq)$, gdzie $\leq$ jest relacją częściowego porządku nazywamy zbiorem uporządkowanym. Jeżeli $\leq$ jest porządkiem liniowym, to $(X, \leq)$ nazywamy zbiorem liniowo uporządkowanym.

DEF. Niech $(X, \leq)$, $(Y, \leq)$ będą zbiorami uporządkowanymi. Odwzorowanie $f: X \to Y$ nazywamy rosnącym, jeśli

$$(\forall x_1, x_2 \in X) \quad x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2).$$

Piszemy wtedy $f: (X, \leq) \to (Y, \leq)$.

Odwzorowanie f nazywamy ściśle rosnącym, jeśli

$$(\forall x_1, x_2 \in X) \quad x_1 < x_2 \Rightarrow f(x_1) < f(x_2).$$

Piszemy wtedy $f: (X, <) \to (Y, <)$. Odwzorowanie rosnące różnowartościowe jest ściśle rosnące.

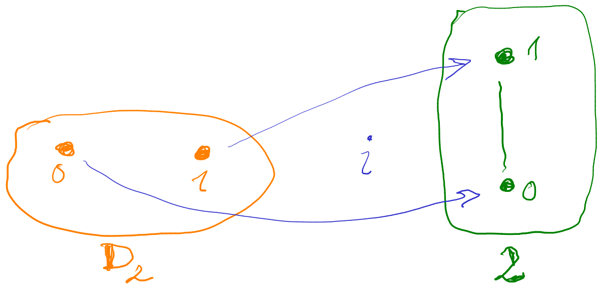
Odwzorowanie $f: X \to Y$ nazywamy izomorfizmem, jeśli f jest rosnące, f jest bijekcją oraz $f^{-1}: Y \to X$ jest rosnące. Piszemy wtedy $f: (X, \leq) \xrightarrow{\approx} (Y, \leq)$. Piszemy $(X, \leq) \approx (Y, \leq)$, jeśli istnieje izomorfizm $f: (X, \leq) \xrightarrow{\approx} (Y, \leq)$ i mówimy, że $(X, \leq)$, $(Y, \leq)$ są izomorficzne. Izomorfizm $f: (X, \leq) \xrightarrow{\approx} (X, \leq)$ nazywamy automorfizmem.

PRZYKŁAD 1 Niech $\mathbb{2} = (\{0,1\},\leq)$, gdzie $0 \leq 1$. Jest to jedyny, z dokładnością do izomorfizmu, zbiór liniowo uporządkowany 2-elementowy.

Dla $n\in\mathbb{N}$ niech $\mathbb{D}_n = (n, =)$, gdzie $n=\{0,1,\dots,n-1\}$. Jest to zbiór uporządkowany dyskretny.

Odwzorowanie identycznościowe $i: \mathbb{D}_2 \longrightarrow \mathbb{2}$ jest rosnącą bijekcją, ale nie jest izomorfizmem.

W $\mathbb{D}_2$ mamy $0 \not\leq 1$, $1\not\leq 0$, tymczasem $0<1$ w $\mathbb{2}$.



Zauważmy, że każde odwzorowanie $f:\mathbb{D}_n \longrightarrow (Y,\leq)$ jest ściśle rosnące.

DEF. Odwzorowanie (rosnące) $f:(X,\leq)\longrightarrow(Y,\leq)$ nazywamy zanurzeniem, jeśli jest izomorfizmem na obraz $(f[X],\leq)$. Równoważnie, f jest różnowartościowe oraz

$$(\forall x_1,x_2\in X)\qquad x_1\leq x_2 \iff f(x_1)\leq f(x_2).$$

DEF. Niech $\{(X_s,\leq_s)\}_{s\in S}$ będzie rodziną zbiorów uporządkowanych ($S\neq\emptyset$ zbiór indeksów). Produktem nazywamy zbiór uporządkowany

$$\left(\prod_{s\in S} X_s,\ \leq\right), \quad \text{gdzie} \quad x\leq y \overset{df}{\iff} (\forall s\in S)\ x(s)\leq_s y(s).$$

ILOCZYN KARTEZJAŃSKI

$$\prod_{s\in S}X_s = \left\{x\in \left(\bigcup_{s\in S} X_s\right)^S : (\forall s\in S)\ x(s)\in X_s\right\}.$$

Aksjomat wyboru mówi, że

$$\prod_{s\in S} X_s\neq\emptyset, \text{ o ile } (\forall s\in S)\ X_s\neq\emptyset.$$

Jeśli $X_s = X$ dla $s\in S$ to piszemy X^S zamiast $\prod_{s\in S} X_s$; zbiór uporządkowany $(X^S,\leq)$ nazywamy potęgą zbioru $(X,\leq)$.

$S=n$, to piszemy $X_0\times\dots\times X_{n-1}$ zamiast $\prod_{i\in n} X_i$

$$i\in n \Updownarrow i<n$$

FAKT 1 Produkt $\left(\prod_{s\in S}X_s,\leq\right)$ (rodziny) niepustych zbiorów uporządkowanych jest liniowo uporządkowany $\iff (\exists s_0\in S)$ X_{s_0} jest liniowo uporządkowany oraz $|X_s|=1$ dla $s\in S\setminus\{s_0\}$.

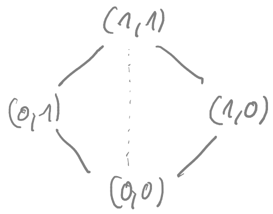
$$\prod_{s\in S}X_s=\emptyset \iff (\exists s_0\in S)\ X_{s_0}=\emptyset.$$

Dowód. ($\Longrightarrow$) Ustalmy $s_0\in S$; ustalmy $x_1,x_2\in X_{s_0}$. Niech $\bar{x}_1,\bar{x}_2\in\prod_{s\in S} X_s$ będą jakiekolwiek, spełniające $\bar{x}_1(s_0)=x_1$, $\bar{x}_2(s_0)=x_2$. Porządek $\leq$ na $\prod_{s\in S} X_s$ jest liniowy, zatem $\bar{x}_1\leq \bar{x}_2$ lub $\bar{x}_2\leq\bar{x}_1$. Stąd $\bar{x}_1(s_0)\leq \bar{x}_2(s_0)$ lub $\bar{x}_1(s_0)\geq \bar{x}_2(s_0)$, czyli $x_1\leq x_2$ lub $x_2\leq x_1$.

Przypuśćmy, że $s_0,s_1\in S$ są takie, że $s_0\neq s_1$ oraz $|X_{s_0}|>1$, $|X_{s_1}|>1$. Wybierzmy $a_{s_0}<_{s_0} b_{s_0}$ w X_{s_0} oraz $b_{s_1}<_{s_1} a_{s_1}$ w X_{s_1}.

Niech $a,b\in\prod_{s\in S}X_s$ będą takie, że $a(s_i)=a_{s_i}$, $b(s_i)=b_{s_i}$ dla $i=0,1$.
Wówczas $a\not\leqslant b$, bo $b(s_1)<_{s_1}a(s_1)$; $b\not\leqslant a$, bo $a(s_0)<_{s_0}b(s_0)$.
Sprzeczność, bo $\leqslant$ miałby być porządkiem liniowym.
($\Leftarrow$) Jeśli $|X_s|=1$ dla $s\in S\setminus\{s_0\}$, to $\left(\prod_{s\in S}X_s,\leqslant\right)\approx(X_{s_0},\leqslant_{s_0})$. ■

PRZYKŁAD 2 Zbiór uporządkowany $\mathbf{2}^2=\mathbf{2}\times\mathbf{2}$ wygląda następująco:

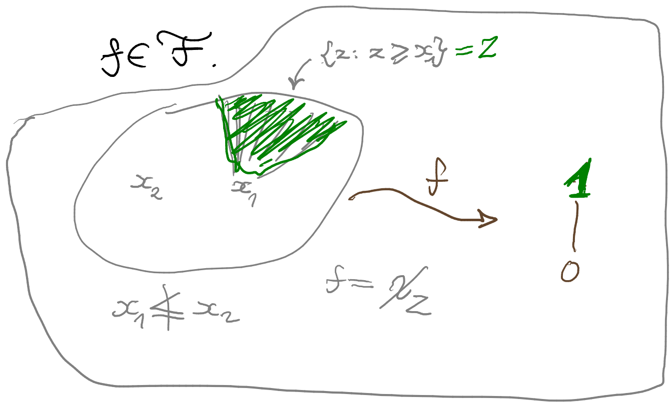


FAKT 2 Każdy zbiór uporządkowany zanurza się w potęgę $\mathbf{2}$.

DOWÓD (SZKIC) Ustalmy zbiór uporządkowany $(X,\leqslant)$ i rozważmy rodzinę $\mathcal{F}$ złożoną z wszystkich odwzorowań rosnących $f\colon(X,\leqslant)\longrightarrow\mathbf{2}$. Niech $\varphi\colon X\longrightarrow\mathbf{2}^{\mathcal{F}}$ będzie dane wzorem

$$\varphi(x)(f)=f(x),\qquad f\in\mathcal{F}.$$

Wówczas φ jest zanurzeniem. ■



DEF Zbiór liniowo uporządkowany przeliczalny $(X,\leqslant)$ nazywamy losowym, jeśli

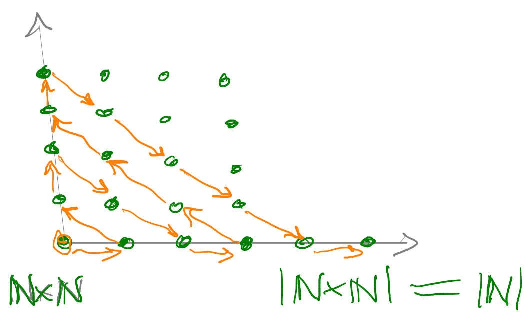
(1) $(\forall x\in X)(\exists y\in X)\ y<x$,

(2) $(\forall x\in X)(\exists z\in X)\ x<z$,

(3) $(\forall x_1,x_2\in X)\left[x_1<x_2\Rightarrow(\exists v\in X)\ x_1<v<x_2\right]$.

FAKT 3 $(\mathbb{Q},\leqslant)$ jest losowy.

Mamy surjekcję $f\colon\mathbb{Z}\times\mathbb{N}^+\longrightarrow\mathbb{Q}$,
$f(x,y)=\dfrac{x}{y}$.
Stąd $|\mathbb{Q}|\leqslant|\mathbb{Z}|\cdot|\mathbb{N}^+|=\aleph_0\cdot\aleph_0=\aleph_0$



FAKT 4 Niech $(X,\leqslant)$ będzie zbiorem liniowo uporządkowanym przeliczalnym. Wówczas $(X,\leqslant)$ jest losowy $\Longleftrightarrow$ dla każdego skończonego zbioru liniowo uporządkowanego $(F,\leqslant)$, jego podzbioru $F_0\subseteq F$, każde zanurzenie $g\colon(F_0,\leqslant)\longrightarrow(X,\leqslant)$ przedłuża się do zanurzenia $e\colon(F,\leqslant)\longrightarrow(X,\leqslant)$.

DOWÓD. ($\Leftarrow$) Z własności przedłużania wynika, że $|X|=\aleph_0$.

Ustalmy $x_0 < x_1$ w X. Niech $F = \{x_{-1}, x_0, x_{\frac{1}{2}}, x_1, x_2\}$, gdzie

$$x_{-1} < x_0 < x_{\frac{1}{2}} < x_1 < x_2 .$$

Niech $F_0 = \{x_0, x_1\}$. Wówczas zanurzenie tożsamościowe $e_0 : F_0 \longrightarrow X$ przedłuża się do zanurzenia $e : F \longrightarrow X$. Stąd $(\exists y, z, v)$ $y < x_1 < v < x_2 < z$.
To daje jednocześnie (1), (2), (3).

($\Longrightarrow$) Dzięki indukcji matematycznej możemy założyć, że $F = F_0 \cup \{v\}$.
Mamy trzy przypadki.

(1) $v = \min F$, tzn. $v < x$ dla $x \in F_0$.

Niech $x_0 = \min F_0$. Wówczas warunek (1) w definicji losowości daje $\bar{v} \in X$, $\bar{v} < e_0(x_0)$.
Definiując e wzorami $e(v) = \bar{v}$, $e|F_0 = e_0$, dostajemy zanurzenie $e : F \longrightarrow X$.

(2) $v = \max F$, tzn. $v > x$ dla $x \in F_0$.
Tak samo jak powyżej.

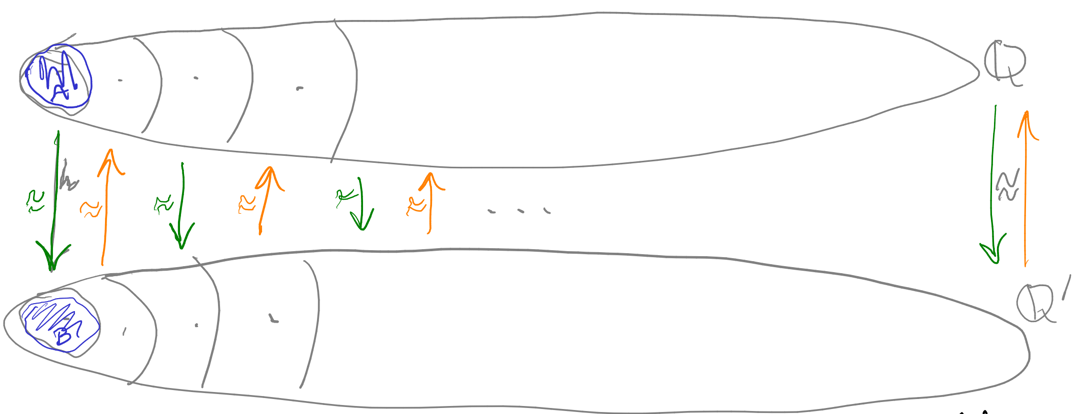
(3) $(\exists x_0, x_1 \in F_0)$ $x_0 < v < x_1$.
Warunek (3) w definicji losowości daje $\bar{v} \in X$, $e_0(x_0) < \bar{v} < e_0(x_1)$. Definiujemy $e(v) = \bar{v}$, $e|F_0 = e_0$. Jest to zanurzenie przedłużające e_0. ■

TWIERDZENIE 1 (CANTOR) (1) Zbiór liczb wymiernych $(\mathbb{Q}, \leq)$ jest jedynym z dokładnością do izomorfizmu zbiorem liniowo uporządkowanym losowym.

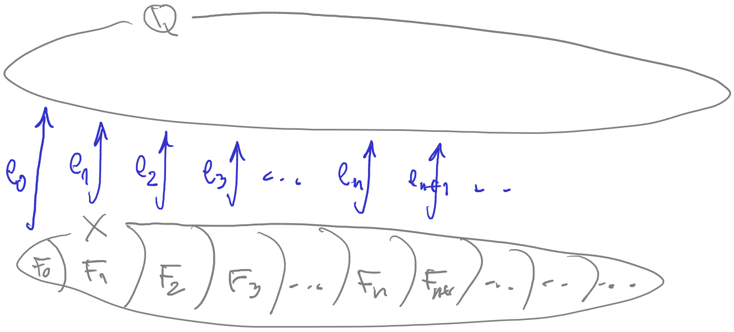
(2) Każdy przeliczalny zbiór liniowo uporządkowany zanurza się w $(\mathbb{Q}, \leq)$.

(3) Dla każdych zbiorów skończonych $A, B \subseteq \mathbb{Q}$, każdy izomorfizm $h : (A, \leq) \xrightarrow{\cong} (B, \leq)$ przedłuża się do automorfizmu $\tilde{h} : (\mathbb{Q}, \leq) \xrightarrow{\cong} (\mathbb{Q}, \leq)$. (tzn. $\tilde{h}|A = h$).

Tezy (1), (3) dowodzi się jednocześnie, używając argumentu „tam i z powrotem" (ang. back-and-forth argument).



Tezę (2) łatwo dowodzi się wykorzystując własność przedłużania oraz indukcję.



$$e = \bigcup_{n\in\mathbb{N}} e_n : (X,\leq) \longrightarrow (\mathbb{Q},\leq)$$

zanurzenie

DEF. Niech $(X,\leq)$, $(Y,\leq)$ będą zbiorami uporządkowanymi. Produktem leksykograficznym $(X,\leq)\cdot(Y,\leq)$ nazywamy zbiór uporządkowany $(X\times Y,\leq)$, gdzie $<$ jest zdefiniowana wzorem

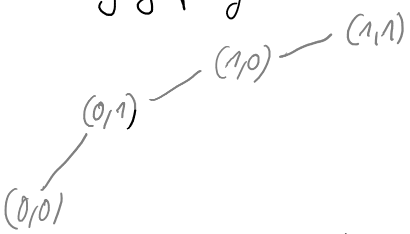
$$(x_0,y_0) < (x_1,y_1) \overset{df}{\iff} x_0<x_1 \text{ lub } \big(x_0=x_1 \text{ i } y_0<y_1\big).$$

Będziemy pisać $X\cdot Y$ zamiast $(X,\leq)\cdot(Y,\leq)$, o ile relacje porządku są wyznaczone w jasny sposób.

FAKT 5 Jeśli $(X,\leq)$, $(Y,\leq)$ są zbiorami liniowo uporządkowanymi, to $(X,\leq)\cdot(Y,\leq)$ jest zbiorem liniowo uporządkowanym.

DOWÓD. Ustalmy $(x_0,y_0),(x_1,y_1)\in X\times Y$, $(x_0,y_0)\neq(x_1,y_1)$.
Jeśli $x_0\neq x_1$, to albo $x_0<x_1$, co daje $(x_0,y_0)<(x_1,y_1)$, albo $x_1<x_0$, co daje $(x_1,y_1)<(x_0,y_0)$. Jeśli $x_0=x_1$, to albo $y_0<y_1$ i $(x_0,y_0)<(x_1,y_1)$, albo $y_1<y_0$ i $(x_1,y_1)<(x_0,y_0)$. $\blacksquare$

PRZYKŁAD 3 Produkt leksykograficzny $2\cdot 2$ wygląda następująco:

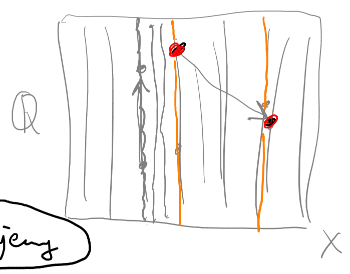


Poniższy fakt dowodzi tezę (2) Twierdzenia 1.

FAKT 6 Niech $(X,\leq)$ będzie zbiorem liniowo uporządkowanym niepustym przeliczalnym. Wówczas $(X,\leq)\cdot(\mathbb{Q},\leq)$ jest losowy. Ponadto, $(X,\leq)$ zanurza się w $(X,\leq)\cdot(\mathbb{Q},\leq)$.

DOWÓD. Niech $e: X\longrightarrow X\cdot\mathbb{Q}$ będzie dane wzorem $e(x)=(x,0)$. Jest to zanurzenie.
Pokażemy, że $X\cdot\mathbb{Q}$ jest losowy.
Ustalmy $(x_0,y_0)<(x_1,y_1)$.
Jeśli $x_0<x_1$, to

$$(x_0,y_0-1)<(x_0,y_0)<(x_0,y_0+1)<(x_1,y_1)<(x_1,y_1+1).$$



Jeśli $x_0=x_1$, to $y_0<y_1$, zatem

$$(x_0,y_0-1)<(x_0,y_0)<\left(x_0,\tfrac{y_0+y_1}{2}\right)<(x_1,y_1)<(x_1,y_1+1).$$

W obu przypadkach dostajemy losowość. $\blacksquare$

FAKT 7 Każda (nietrywialna) skończenie generowana podgrupa grupy $(\mathbb{Q},+)$ jest izomorficzna z $(\mathbb{Z},+)$.

Dowód. Ustalmy $\{0\} \neq H \leqslant \mathbb{Q}$, $H = \langle r_1, \dots, r_k \rangle$.

Niech q będzie wspólnym mianownikiem ułamków $r_1, \dots, r_k$.

To znaczy, $r_i = \dfrac{m_i}{q}$, $i = 1, \dots, k$, gdzie $m_1, \dots, m_k \in \mathbb{Z}$.

Tak więc
$$\{r_1, \dots, r_k\} \subseteq \tfrac{1}{q}\mathbb{Z} \approx \mathbb{Z},$$
a zatem $H \leqslant \frac{1}{q}\mathbb{Z}$. Każda nietrywialna podgrupa grupy $(\mathbb{Z},+)$ jest izomorficzna z $(\mathbb{Z},+)$. ■

> Grupa G jest cykliczna, jeśli $G = \{a^n : n \in \mathbb{Z}\}$ dla pewnego $a \in G$. Jeśli działanie to dodawanie $+$, to $G = \{na : n \in \mathbb{Z}\}$.

FAKT 8 Niech $H \leqslant G$ będą grupami cyklicznymi nieskończonymi. Wówczas każde zanurzenie $e_0 : H \longrightarrow \mathbb{Q}$ przedłuża się do zanurzenia $e : G \longrightarrow \mathbb{Q}$.

> $H \leqslant G$ oznacza „H jest podgrupą grupy G".

Dowód. Możemy założyć, że $G = \mathbb{Z}$, a zatem $H = k\mathbb{Z}$, gdzie $k \in \mathbb{N}^+$.

Zdefiniujmy $e : \mathbb{Z} \longrightarrow \mathbb{Q}$ wzorem

> $H \leqslant \mathbb{Z} \iff (\exists k \in \mathbb{N})\ H = k\mathbb{Z}$

$$e(n) = \frac{n}{k} e_0(k).$$

Mamy $e(n+m) = \dfrac{n+m}{k} e_0(k) = \dfrac{n}{k} e_0(k) + \dfrac{m}{k} e_0(k) = e(n) + e(m)$, zatem e jest homomorfizmem.

Ponadto $\ker(e) = \{0\}$, zatem e jest zanurzeniem. Oczywiście $e|_H = e_0$, bo

$$e(km) = \frac{km}{k} e_0(k) = m\, e_0(k) = e_0(km). \ ■$$

TWIERDZENIE 2 (1) Grupa $(\mathbb{Q},+)$ jest jedyną, z dokładnością do izomorfizmu, grupą przeliczalną mającą własność przedłużania z Faktu 8, w której każda podgrupa nietrywialna skończenie generowana jest izomorficzna z $(\mathbb{Z},+)$.

(2) Niech G będzie grupą przeliczalną, w której każda podgrupa nietrywialna skończenie generowana jest izomorficzna z $(\mathbb{Z},+)$. Wówczas istnieje zanurzenie $e : G \longrightarrow \mathbb{Q}$.

(3) Każdy izomorfizm pomiędzy skończenie generowanymi (cyklicznymi) podgrupami grupy $(\mathbb{Q},+)$ przedłuża się do automorfizmu grupy $(\mathbb{Q},+)$.

TWIERDZENIE 3 (1) Każdy zbiór przeliczalny (nieskończony) N ma własność przedłużania: $\forall F_0 \subseteq F$ skończone, $\forall e_0 : F_0 \xrightarrow{1-1} N$ $\exists\, e : F \xrightarrow{1-1} N$, $e|_{F_0} = F$

(2) Każdy zbiór przeliczalny (skończony lub nieskończony) ma odwzorowanie różnowartościowe w zbiór przeliczalny nieskończony N.

> $1-1$ oznacza „różnowartościowe"

(3) Każda bijekcja pomiędzy skończonymi podzbiorami zbioru nieskończonego N przedłuża się do permutacji zbioru N.

> Permutacja zbioru N to bijekcja $f : N \longrightarrow N$.