$A \neq \emptyset$

Def. 1.1.

(a) Działanie (domyślnie binarne) w zbiorze A:

funkcja $* : A \times A \longrightarrow A$

$(x, y) \longmapsto x * y$

k-arne
k-argumentowe : $f : A^k \longrightarrow A \quad k = 0, 1, 2, \ldots$

$(a_1, \ldots, a_k) \mapsto f(a_1, \ldots, a_k)$

gdy $k = 0$: stała $\in A$
(element)

(b) Struktura algebraiczna, algebra (ogólna):

$\mathcal{A} = (\underset{\substack{\neq \\ \emptyset}}{A}, \underbrace{f_1, \ldots, f_k}_{\text{działania w } A})$, $k \geq 0$

A ← universum, dziedzina struktury

(c) Algebry

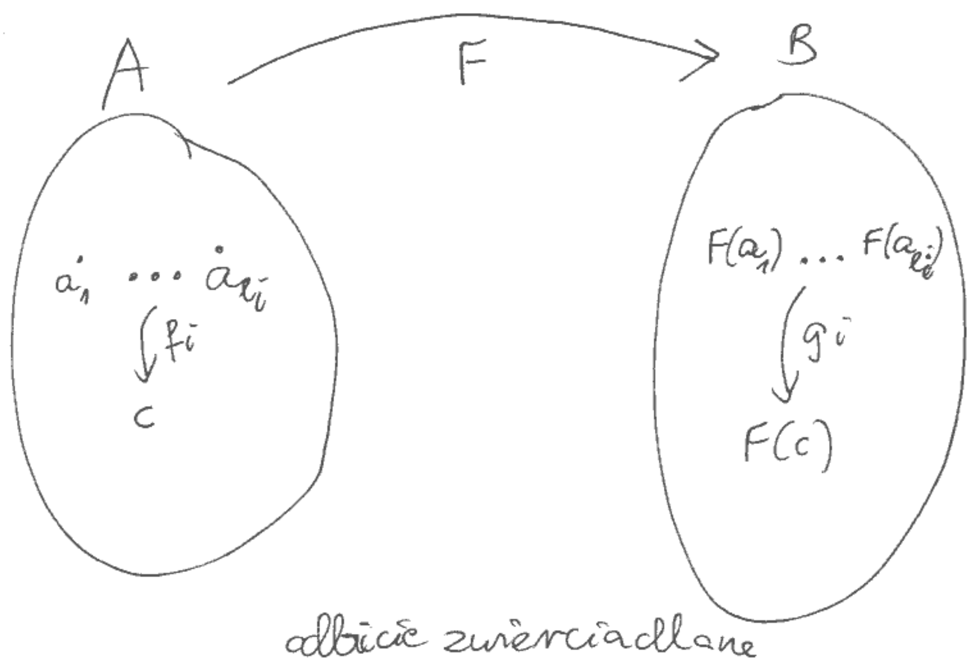
$\mathcal{A} = (A, f_1, \ldots, f_k)$, $\mathcal{B} = (B, g_1, \ldots, g_k)$ są <u>podobne</u>, gdy

arność(f_i) = arność(g_i) $(= l_i)$ dla $i \leq k$

$F : A \xrightarrow[\text{na}]{1-1} B$ jest <u>izomorfizmem</u> algebr $\mathcal{A}, \mathcal{B}$ gdy:

$(*)\ (\forall i = 1, 2, \ldots, k)\ (\forall a_1, \ldots, a_{l_i} \in A)\quad F(f_i(a_1, \ldots, a_{l_i})) =$

$= g_i(F(a_1), \ldots, F(a_{l_i}))$



odbicie zwierciadlane

$$\exists\, g_i(F(a_1),\dots,F(a_{l_i})) = F(c)$$

$$\Updownarrow \qquad \qquad \| \quad c = f_i(a_1,\dots,a_{l_i})$$

$$g_i(F(a_1),\dots,F(a_{l_i})) = F(f_i(a_1,\dots,a_{l_i})) \text{ jak w } (*)$$

Symbolicznie: $F : A \xrightarrow{\cong} B$

(d) $A \cong B$, gdy $\exists F \;\; F : A \xrightarrow{\cong} B$

struktury A i B są <u>izomorficzne</u>

$\cong$ ma własność relacji równoważności (zwrotna, symetryczna, przechodnia)

(e) $F : A \longrightarrow B$ jest <u>homomorfizmem</u>, gdy zachodzi $(*)$ z (c)

(f) Słowniczek:

epi — "na" (surjekcja)
mono — 1-1 (injekcja)
izo — bijekcja
endo — $(A, f_1, \ldots, f_k) = (B, g_1, \ldots, g_k)$
auto — endo + izo

morfizm = homomorfizm +

Def. 1.2

$\mathcal{B} = (B, g_1, \ldots, g_k)$ jest podstrukturą struktury $\mathcal{A} = (A, f_1, \ldots, f_k)$,
(podalgebrą)

gdy:

- $B \subseteq A$
- $(\forall i \leq k)\ g_i = f_i \restriction_B$

Uwaga 1.3. Załóżmy, że $B \subseteq A$. Wtedy (1) $\Longleftrightarrow$ (2), gdzie:

(1) B jest uniwersum podstruktury struktury $\mathcal{A}$
(z naturalnymi działaniami)

(2) B jest <u>zamknięty</u> na działania $f_1, \ldots, f_k$, <u>tzn</u>: (definicja)

$$(\forall i \leq k)(\forall \underbrace{b_1, \ldots, b_{l_i}}_{\bar{b}} \in B)\ f_i(\bar{b}) \in B$$

[Wtedy B traktujemy jako strukturę
$\parallel$
$(B, f_1|_B, \ldots, f_k|_B)$,]
podstrukturę struktury $\mathcal{A}$.

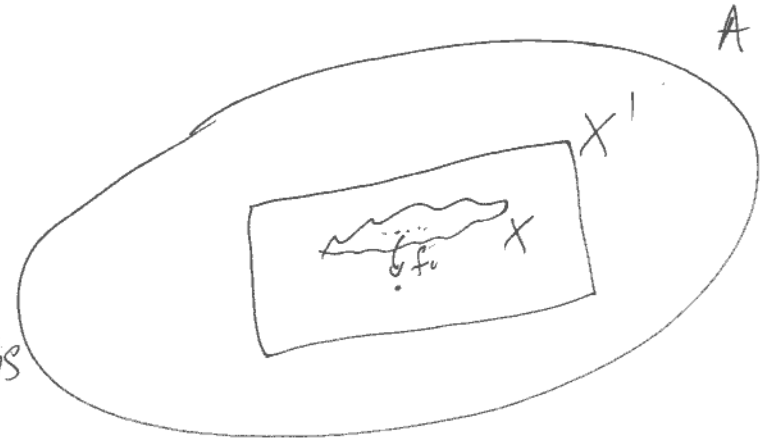
Uwaga 1.4.

Jeśli $F: \mathcal{A} \longrightarrow \mathcal{B}$ jest homomorfizmem struktur, to $Rng(F)$ jest podstrukturą $\mathcal{B}$.

$$\overset{\shortparallel}{Im}(F)$$

<u>Generowanie podstruktury</u> $\mathcal{A} = (A, f_1, \dots, f_k)$

Dla $\underset{\overset{\#}{\emptyset}}{X} \subseteq A$, $X' := X \cup \bigcup_{i=1}^{k} \{ f_i(a_1, \dots, a_{l_i}) : a_1, \dots, a_{l_i} \in X \}$



Iterujemy tę operację

$$\begin{cases} X^{(0)} := X \\ X^{(n+1)} := (X^{(n)})' , \quad n = 0, 1, 2, \dots \end{cases}$$

$$X = X^{(0)} \subseteq X^{(1)} \subseteq X^{(2)} \subseteq \dots$$

$$\langle X \rangle = \bigcup_{n=0}^{\infty} X^{(n)}$$

Uwaga 1.5. (definicja) (1) $\langle X \rangle$ jest najmniejszą podstrukturą struktury $\mathcal{A}$ zawierającą zbiór X, tzn: podstrukturą generowaną przez X w $\mathcal{A}$.

(2) Gdy $\langle X \rangle = \mathcal{A}$, mówimy, że X generuje $\mathcal{A}$, (jest zbiorem generatorów $\mathcal{A}$).

Przykład

$V = (V, +, r)_{r \in \mathbb{R}}$ przestrzeń liniowa nad $\mathbb{R}$

$B \subseteq V$.

Wtedy: B jest podstrukturą V (generowaną przez X)

$\Updownarrow$

B podprzestrzeń liniowa V (generowana przez X)

Metadefinicja

Własność algebraiczna struktury =

= własność niezmiennicza ~~na~~ ze względu na izomorfizmy.

Uwaga 1.6 (indukowanie struktury)

Zał. że $(A, \circ)$: struktura, B: zbiór i $F: A \xrightarrow[na]{1-1} B$.

Wtedy istnieje jedyne działanie $*$ w B takie, że

$$F: (A, \circ) \xrightarrow{\cong} (B, *)$$

(definicja) $*$ nazywamy działaniem indukowanym w zbiorze B przez F i $\circ$.

GRUPY.

Def. 1.7. Grupa to struktura $G = (G, \cdot)$ taka, że:

G1. działanie $\cdot$ jest łączne:

$$(\forall x, y, z \in G) \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$(xy)z = x(yz) \quad \cdot \text{ pomijamy}$$

G2. działanie $\cdot$ ma element neutralny w G:

$$(\exists e \in G)(\forall x \in G) \quad ex = xe = x$$

[wtedy e jest jedyny]

G3. Dla każdego $x \in G$ istnieje $x' \in G$ t. że

$$xx' = x'x = e$$

[wtedy x' jest jedyny dla danego x, nazywamy go elementem odwrotnym do x i oznaczamy przez x^{-1}]

Def. 1.8. Grupa G jest <u>abelowa</u> (przemienna), gdy działanie $\cdot$ jest przemienne, tzn. $(\forall x, y \in G) \quad xy = yx$

Def. 1.9. Rząd grupy $G = |G| =$ liczba elementów grupy G

<u>Notacja</u>. Gdy $\cdot$ łączne w A i $a_1, \dots, a_k \in A$, to

$$\prod_{i=1}^{k} a_i = a_1 \dots a_k$$

· Symbolem $+$ oznaczamy wyłącznie działanie przemienne. Jeśli dodatkowo jest łączne, to

$$\sum_{i=1}^{k} a_i \text{ oznacza } a_1 + \dots + a_k.$$

Pierwsze przykłady grup:

$(\mathbb{R}, +)$: addytywna grupa l. rzeczywistych
el. neutralny : 0
el. odwrotny do x : $-x$

~~$\mathbb{R}^* = \mathbb{R}$~~

$(\mathbb{R}^*, \cdot)$: multyplikatywna grupa l. rzeczywistych
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
el. neutralny : 1
el. odwrotny do x : x^{-1}.

Notacja grupowa

	multyplikatywna	addytywna
działanie grupowe	$\cdot$	$+$
el. neutralny	$e, 1$	0
element odwrotny do x (inverse)	x^{-1}	$-x$ (przeciwny)
odejmowanie		$x - y := x + (-y)$
{potęgowanie / krotność $n > 0$	$x^n = \overbrace{x \cdot \ldots \cdot x}^{n}$, $x^0 = 1$ $x^{-n} = \underbrace{x^{-1} \cdot \ldots \cdot x^{-1}}_{n}$ potęga $\overset{n}{x}$	$nx = \underbrace{x + \ldots + x}_{n}$, $0x = 0$ $(-n)x = \underbrace{(-x) + \ldots + (-x)}_{n}$ $\overset{n}{\text{krotność}}$ x
stosowalność	zawsze	tylko dla abelowych.

$*$: działanie w zbiorze skończonym $A = \{a_1, \dots, a_k\}$

tabelka $*$:

$*$	a_1	$\dots$	a_j	$\dots$	a_k
a_1			$\vdots$		
$\vdots$			$\vdots$		
a_i	$\dots$	$\dots$	$a_i * a_j$		
$\vdots$					
a_k					

Czasami traktujemy grupę $G = (G, \cdot)$ jak strukturę $G = (G, \cdot, {}^{-1}, e)$

działania: unarne (1-argumentowe), 0-argumentowe

Odtąd $G = (G, \cdot)$ zazwyczaj oznacza ~~gr~~ grupę.

Uwaga 1.10. Jeśli $F : (G, \cdot) \longrightarrow (A, *)$ jest homomorfizmem, to $F[G]$ jest grupą (jako podstruktura A), tzn: "homomorficzny obraz grupy jest grupą".

Def. 1.11. Załóżmy, że $H \subseteq G$. Mówimy, że H jest <u>podgrupą</u> grupy G, gdy H jest grupą względem działania $\cdot$ z G (ograniczonego do H).

Symbolicznie: $H < G$ — właściwa, gdy $H \neq G$; niewłaściwa, gdy $H = G$

(wtedy: G jest <u>nadgrupą</u> grupy H)

<u>Przykład</u> $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$

ale nieprawda, że $(\mathbb{N}, +) < (\mathbb{Z}, +)$, choć jest podstrukturą.

Uwaga 1.12.

(1) Jeśli $H < G$, to H jest podstrukturą grupy G.

(2) Załóżmy, że $\emptyset \neq H \subseteq G$. Wtedy : NWSR:

(a) $H < G$

(b) (i) H zamknięte na $\cdot$

(ii) $e \in H$

(iii) $(\forall x \in H)\ x^{-1} \in H$ (x^{-1} liczone w G)

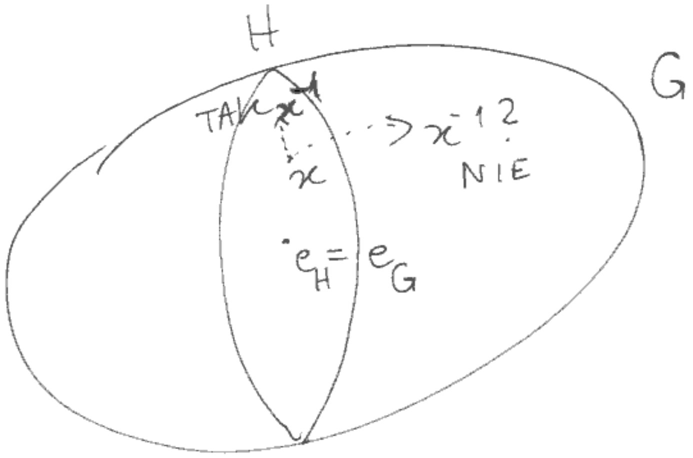
(c) $(\forall x, y \in H)\ xy^{-1} \in H$

(d) $(H, \cdot, ^{-1}, e)$ jest podstrukturą struktury $(G, \cdot, ^{-1}, e)$.

Wn. 1.13.

Gdy $H < G$, to (1) $e_H = e_G$

(2) $(\forall x \in H)$ x^{-1} liczone w G = x^{-1} liczone w H



Uwaga 1.14. W grupie $(G, \circ)$:

1. $e^{-1} = e$
2. $(a^{-1})^{-1} = a$
3. $(ab)^{-1} = b^{-1}a^{-1}$
4. $(a^n)^m = a^{nm}$
5. $a^n \cdot a^m = a^{n+m}$
6. Gdy $ab = ba$, to (tzn: a i b komutują, są przemienne)

$$(ab)^n = a^n b^n.$$

D-d: ćw.

Przykłady grup.

0. Grupa trywialna: $\{e\}$ $\quad ee = e$
1. $(\mathbb{R}^n, +)$, ogólniej: $(V, +)$, gdzie V: przestrzeń liniowa nad $\mathbb{R}$.
2. $(M_{m \times n}(\mathbb{R}), +)$, $m, n > 0$
3. Niech $X \subseteq \mathbb{R}^2$

$$G_X = \{ f : X \xrightarrow[\text{na}]{1-1} X : f \text{ izometria} \}.$$

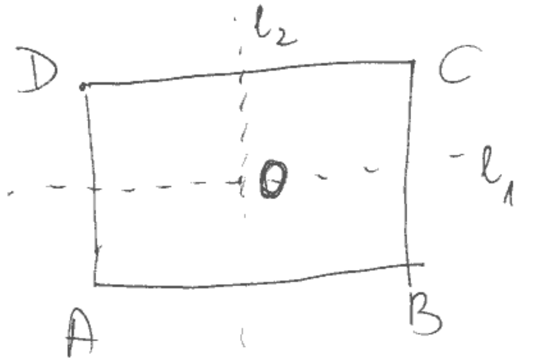
(zachowuje odległości)

grupa izometrii własnych zbioru (figury) X

- działanie: składanie funkcji
- el. neutralny ~~do f~~: id_X
- el. odwrotny do f: f^{-1}

Przykłady grup c.d.

3(a) $X = ABCD$ prostokąt niebędący kwadratem



G_X:

- $e = id_X$
- $a = S_{l_1}$ odbicie względem l_1
- $b = S_{l_2}$ — // — l_2
- $c = S_O$ — // — O

$G_X = \{e, a, b, c\}$

· G_X abelowa:
$$\left.\begin{aligned} a^2 &= b^2 = c^2 = e \\ ab &= ba = c \\ ca &= ac = b \\ bc &= cb = a \end{aligned}\right) \text{ćw.}$$

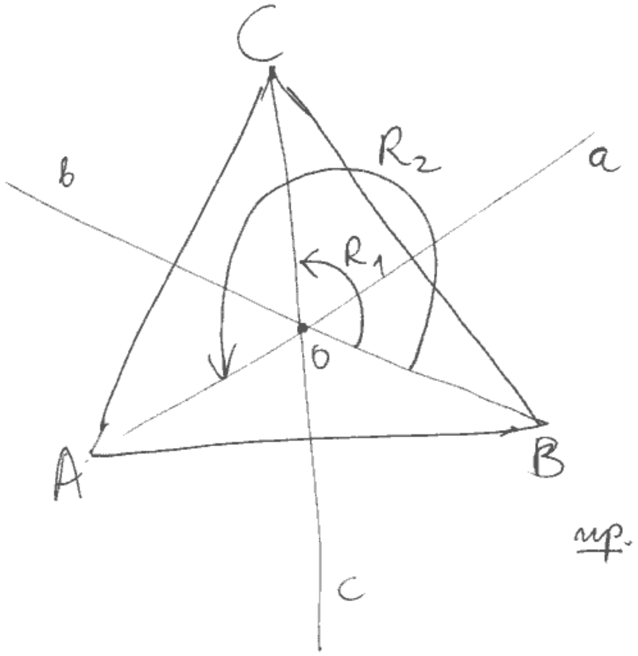
np.: $ab = c$, bo ~~dwie~~ funkcje po obu stronach równości zgadzają się na wierzchołkach A, B, C, D:

$$ab(A) = a(b(A)) = a(B) = C = c(A) \text{ itd.}$$

G_X nazywamy grupą czwórkową Kleina

ozn: $\mathbb{K}_4$.

3(b). $X = \Delta ABC$ równoboczny



$G_X = \{id, \underbrace{R_1, R_2}_{\text{obroty}}, S_a, S_b, S_c\}$

jak na rysunku wokół O.

nie jest abelowa:

np. $\underbrace{S_a \circ S_b}_{R_1}(A) = B$ $\quad$ $\underbrace{S_b \circ S_a}_{R_2}(A) = C$

$G_X > O_X = \{id, R_1, R_2\}$ $\quad$ X

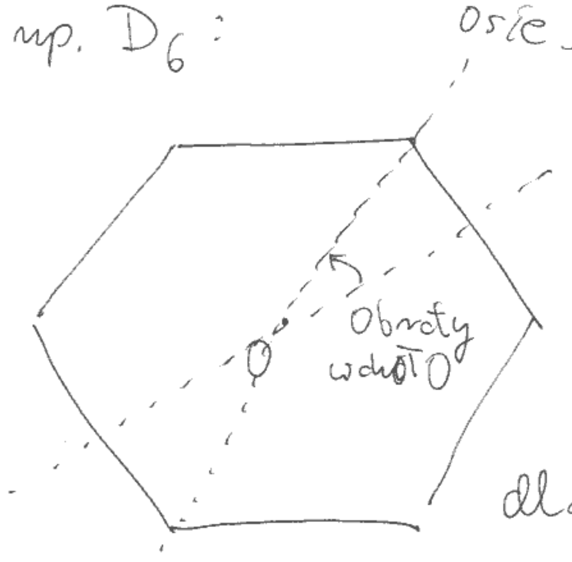
grupa obrotów własnych ΔABC

rzędu 3.

3(c). $X =$ n-kąt foremny, $n \geq 3$.

$D_n = G_X$: n-ta grupa dihedralna (w 3(b): D_3)

np. D_6:



$O_6 = \{\overset{id}{\overset{\shortparallel}{R_0}}, R_1, \dots, R_5\}$ obroty

$S_1, \dots, S_6$: odbicia

$D_6 = O_6 \cup \{S_1, \dots, S_6\}$

dla $n \geq 3$ D_n nieabelowa

$D_n > O_n$: grupa obrotów własnych n-kąta foremnego.

$n = 2$: D_2 : grupa izometrii własnych "2-kąta foremnego"

"2-kąt foremny":

$D_2 \cong K_4$: abelowa