







# 1 Teoria grup

## 1.1 Grupy, pierścienie, ciała

**Działanie** [🇬🇧 operation] na zbiorze  $X$ :

$$\Phi : X \times X \rightarrow X,$$

zwykle zapisywane jako  $xy$ ,  $x \cdot y$ ,  $x + y$ .

**Przykłady:**

↪ na dowolnym z  $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$  mamy dodawanie (+) i mnożenie (·)

↪ na  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{N}$  mamy  $\leq$  który daje działania:

$$a \vee b := \min a, b$$

$$a \wedge b := \max a, b$$

↪ np na  $\mathbb{R}$  możemy zdefiniować  $a * b := a + b^2$

↪ niech  $X$  będzie zbiorem, a  $X^X$  będzie zbiorem wszystkich funkcji  $X \rightarrow X$ , wtedy składanie funkcji jest działaniem określonym w  $X^X$ :

$$f \circ g \in X^X$$

**MOŻNA DOJEBAC GRAFIK KOMUTUJĄCY**

↪  $X$  – zbiór i niech  $\mathcal{P}(X)$  to zbiór wszystkich podzbiorów  $X$ , wtedy na  $\mathcal{P}(X)$  mamy działanie sumy [🇬🇧 union] i przekroju [🇬🇧 intersection]

↪ niech  $a, b \in X$ , wtedy mamy rzuty na osie:

$$a \downarrow b := a$$

$$a \uparrow b := b$$

↪ na zbiorze  $\mathbb{R} \cup \{\infty\}$  definiujemy ( $\forall a \in \mathbb{R} \cup \{\infty\}$ )  $a + \infty = \infty = \infty + a$  oraz ( $\forall a, b \in \mathbb{R}$ )  $a + b = a +_{\mathbb{R}} b$  (dodawanie w  $\mathbb{R}$ )

Prosty opis działań – niech  $*$  będzie działaniem określonym w  $A = \{a_1, \dots, a_n\}$ , to możemy dojebac tabelkę:

$*$	$a_1$	$a_2$	$\dots$	$a_n$
$a_1$	$a_1 * a_1$	$a_1 * a_2$	$\dots$	$a_1 * a_n$
$a_2$	$a_2 * a_1$	$a_2 * a_2$	$\dots$	$a_2 * a_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_n$	$a_n * a_1$	$a_n * a_2$	$\dots$	$a_n * a_n$

**Element neutralny** [🇬🇧 neutral element] – takie  $e$ , że dla każdego  $x \in X$   $ex = xe = x$ . Działanie ma co najwyżej jeden element neutralny.

**Element odwrotny** [🇬🇧 inverse element] do  $x$  to takie  $y$ , że  $xy = yx = e$ . Jeśli działanie jest łączne [🇬🇧 associative], to ma co najwyżej jeden element odwrotny do danego  $x$ .

**Homomorfizm** algebry  $\mathcal{X} = (X, \{\cdot\})$  na algebrę  $\mathcal{Y} = (Y, \{\circ\})$  nazywamy przekształcenie  $f : X \rightarrow Y$  spełniające dla każdego  $a, b \in X$

$$f(a \cdot b) = f(a) \circ f(b).$$

- **monomorfizm** –  $f$  jest 1-1
- **epimorfizm** –  $f$  jest "na"
- **izomorfizm** –  $f$  jest 1-1 i "na"
- **endomorfizm** – kiedy  $\mathcal{Y} = \mathcal{X}$
- **automorfizm** – endomorfizm będący izomorfizmem

**Polgrupa** to niepusty zbiór z działaniem łącznym.

**GRUPA** [🇬🇧 group] to niepusty zbiór z łącznym działaniem i elementem neutralnym (zwanym **jednością grupy**) oraz elementami odwrotnymi dla każdego elementu.

↪ **grupa abelowa** (przemienna) [🇬🇧 commutative group] – grupa z działaniem przemennym

Zbiór  $G$  z działaniem  $\cdot$  jest grupą, jeśli:

1. ( $\forall a, b, c \in G$ )  $(ab)c = a(bc)$
2. ( $\exists e \in G$ ) ( $\forall a \in G$ )  $ea = ae = e$
3. ( $\forall a \in G$ ) ( $\exists b \in G$ )  $ab = ba = e$
- \*4. ( $\forall a, b \in G$ )  $ab = ba$  w grupie *abelowej*

**Grupa przekształceń** [🇬🇧 transformation group] – niepusty podzbiór  $G \subseteq S_X$ , który jest:

- ↪ jest zamknięty na łączenie funkcji
- ↪ ( $\forall f \in G$ )  $f^{-1} \in G$

Pojęcie to wprowadził Galois ok 1830, gdzie  $X$  był zbiorem pierwiastków pewnego wielomianu.

**PIERŚCIEN** to niepusty zbiór  $X$  z dwoma działaniami ( $\cdot, +$ , mnożenie i dodawanie) taki, że:

1. zbiór  $X$  z  $+$  jest grupą abelową
2.  $\cdot$  jest łączne
3. ( $\forall x, y, z \in X$ )  $x \cdot (y + z) = x \cdot y + x \cdot z \wedge (x + y) \cdot z = x \cdot z + y \cdot z$

Kolejne dziwne nazwy  $*$ :

• **pierścien przemienny** – jeśli mnożenia jest przemienne

• **pierścien z jednością** – dla mnożenia istnieje element neutralny

**CIAŁO** to pierścien przemienny, który dla każdego elementu  $\neq 0$  ma element odwrotny

## 1.2 Własności

Niech  $G$  będzie grupa, a  $e$  jej elementem neutralnym. Wówczas:

$$\hookrightarrow a, b \in G \implies (ab)^{-1} = b^{-1}a^{-1}$$

$$\hookrightarrow a \in G \text{ i } n=1, \dots, n \quad a^{-n} = (a^n)^{-1} = (a^{-1})^n$$

$$\hookrightarrow \text{dla } m, n \in \mathbb{Z} \text{ i } a \in G \text{ mamy } a^{mn} = (a^m)^n$$

$$\hookrightarrow \text{dla } G \text{ grupy abelowej i } n \in \mathbb{Z} \quad (ab)^n = a^n b^n$$

\* trzeba udowodnić, ale mi się nie chce

$H \subseteq G$  jest **podgrupą**  $G$ , jeśli jest grupą ze względu na te same działania, czyli wystarczy, że

$$(\forall a, b \in H) ab^{-1} \in H.$$

## 1.3 Permutacje :>

**$n$ -ta grupa symetryczna**  $[S_n]$  – grupa wszystkich permutacji zbioru  $X_n = \{1, \dots, n\}$ .  $|S_n| = n!$

Jeśli  $P \in S_n$  i dla  $i = 1, \dots, n$   $P(i) = a_i$ , to piszemy

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

Mnożenie permutacji:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

**Zbiór elementów niezmienniczych** (fixpunktów) permutacji  $P$  to zbiór  $F(P) = \{k \in X_n : P(k) = k\}$ . Jego dopełnienie oznaczamy  $M(P) = S_n \setminus F(P)$ .

**Cykl  $k$ -elementowy**  $C$  to permutacja taka, że  $C(a_1) = a_2, C(a_2) = a_3, \dots, C(a_n) = a_1$ . Cykl 2-elementowy to **transpozycja**. Cykle zapisujemy

$$(a_1, a_2, \dots, a_n)$$

Jeśli  $a \in G$  i istnieją  $n \in \mathbb{N}, n \geq 1$ , takie, że  $a^n = e$ , to mówimy że  $n$  jest **rzędem elementu**  $a$  ( $n = o(a)$ ). Jeśli takie  $n$  nie istnieje, to  $a$  ma **rzad nieskończony** ( $o(a) = \infty$ ).

$\hookrightarrow$  **grupa torsyjna** – wszystkie elementy mają rząd skończony

$\hookrightarrow$  **grupa beztorsyjna** – wszystkie elementy mają rząd nieskończony

Jeśli  $o(a) = n$  oraz  $a^N = e$  to  $n|N$ , fajny dowódzik, ale leniem jestem

**Grupa cykliczna** to grupa złożona z wszystkich potęg danego elementu  $a$ , natomiast  $a$  jest nazywane **generatorem** tej grupy

Każda permutacja jest iloczynem transpozycji.

**Permutacje parzyste** – iloczyn

$$\prod_{i < j} (a_j - a_i)$$

jest dodatni (górny rząd to kolejne liczby naturalne, dolny to wyrazy). Pozostałe permutacje są **nieparzyste**.

**Znak permutacji** jest  $+1$  gdy permutacja jest parzysta i  $-1$  wpp. Alternatywnie można zapisać (górny rząd to  $b_k$ , a dolny to  $c_k$ )

$$\text{sgn } P = \prod_{i < j} \frac{b_j - b_i}{c_j - c_i}$$

Dla dwóch dowolnych permutacji  $P_1, P_2$  mamy

$$\text{sgn } P_1 P_2 = \text{sgn } P_1 \cdot \text{sgn } P_2$$

$$\text{sgn } P_1^{-1} = \text{sgn } P_1.$$

**$n$ -ta grupa alternująca**  $[A_n]$  – podgrupa  $S_n$  złożona ze wszystkich parzystych permutacji.

## 1.4 Grupy ilorazowe B)

**Prawostronna warstwa** grupy  $G$  względem jej podgrupy  $H$  wyznaczona przez  $g \in G$  to zbiór

$$gH = \{gh : h \in H\},$$

natomiast **lewostronna warstwa** to zbiór

$$Hg = \{hg : h \in H\}.$$

Dla grup abelowych są one równe.

Dwa elementy  $g_1, g_2 \in G$  wyznaczają tę samą warstwę prawostronną względem  $H$ , gdy  $g_1^{-1}g_2 \in H$ , a tę samą warstwę lewostronną, gdy  $g_1g_2^{-1} \in H$ .

**Rząd grupy** skończonej  $G$  to ilość jej elementów.



**Indeks**  $[G : H]$  podgrupy  $H$  w grupie  $G$  to ilość warstw w grupie  $G$  względem  $H$ . Dla skończonych grup mamy:

$$\hookrightarrow g \in G \text{ o}(g) \mid |G|,$$

$\hookrightarrow$  rząd i indeks każdej podgrupy są dzielnikami rzędu grupy,

$\hookrightarrow$  jeśli rząd jest liczbą pierwszą, to grupa jest cykliczna

**Twierdzenie Lagrange'a** – dla skończonych  $G \triangleright H$ :

$$|G| = [G : H] \cdot |H|.$$

Podgrupa  $H$  jest **dzielnikiem normalnym** grupy  $G$  [ $H \triangleleft G$ ] jeśli  $(\forall g \in G) gH = Hg$ . Wystarczy, że  $(\forall g \in G)(\forall h \in H) ghg^{-1} \in H$ .

Niech  $f : G_1 \rightarrow G_2$  będzie **homomorfizmem**, a  $e_1, e_2$  będą elementami neutralnymi grup odpowiednio  $G_1, G_2$ . Wtedy  $f(e_1) = e_2$  oraz  $f(g)^{-1} = f(g^{-1})$ .

Obraz homomorfizmu  $f : G_1 \rightarrow G_2$  jest **podgrupą grupy  $G_2$**  [ $\text{Im } f \triangleleft G_2$ ], natomiast jądro  $f$  jest **dzielnikiem normalnym  $G_1$**  [ $\text{Ker } f \triangleleft G_1$ ].

**Grupa ilorazowa** to zbiór wszystkich warstw  $H/G$ , gdzie  $H \triangleleft G$ , z działaniem

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Odwzorowanie

$$\phi : G \rightarrow H$$

$$\phi(g) = gH$$

jest **epimorfizmem** (często nazywane **kanonicznym homeomorfizmem  $G$  na  $H$** ).

**[!!!]Zasadnicze twierdzenie o homeomorfizmach dla grup** – jeśli  $f : G \rightarrow G_1$  jest epimorfizmem oraz  $\text{Ker } f = H$ , natomiast  $\phi : G \rightarrow G/H$  jest działaniem jak wyżej, to istnieje tylko jeden izomorfizm  $\psi : G/H \rightarrow G_1$  taki, że  $f = \psi \circ \phi$

Jeżeli  $\emptyset \neq A \subseteq G$  oraz  $G(A) \triangleleft G$  to przekroj wszystkich podgrup  $G$  zawierających  $A$ , a  $A \subseteq G_1 \triangleleft G$ , to  $G(A) \triangleleft G_1$ .

Jeżeli  $K \triangleleft G$  i  $H \triangleleft G$ , to najmniejsza podgrupa  $G$  zawierająca  $H$  i  $K$  pokrywa się ze zbiorem

$$KH := \{kh : k \in K, h \in H\}$$

**Pierwsze twierdzenie o izomorfizmach** – jeżeli  $K \triangleleft G$  i  $H \triangleleft G$ , to

$$\hookrightarrow K \triangleleft KH = HK \triangleleft G$$

$$\hookrightarrow H \cap K \triangleleft H \text{ i } K \triangleleft KH$$

$\hookrightarrow \phi : hK \rightarrow h(K \cap H)$  indukuje izomorfizm

$$HK/K \sim H/(H \cap K)$$

**Drugie twierdzenie o izomorfizmach** – jeżeli  $K \triangleleft G$  i  $K \triangleleft H \triangleleft G$  i oznaczymy  $\bar{H} = H/K$  oraz  $\bar{G} = G/K$ , to wtedy:

$$\hookrightarrow \bar{H} \triangleleft \bar{G}$$

$$\hookrightarrow \bar{H} \triangleleft \bar{G} \iff H \triangleleft G$$

**Automorfizm wewnętrzny** grupy  $G$  wyznaczony przez  $g$ :  $\phi_g(x) = g^{-1}xg$ .

Jeśli  $G$  to grupa abelowa, to dla każdego  $g$   $\phi_g(x) = x$ , a więc ma ona jedynie idynty-

czność. Zbiór wszystkich automorfizmów wewnętrznych grupy  $G$  oznaczamy  **$I(G)$**  i tworzy on grupę ze składaniem

**Centrum grupy  $G$**  [ $Z(G)$ ] to zbiór  $x \in G$  takich, że dla dowolnego  $y \in G$   $xy = yx$ . Dla każdego  $G$   $Z(G) \triangleleft G$

Grupa  $I(G)$  jest izomorficzna z  $G/Z(G)$ .

Jeśli  $M$  to dowolny podzbiór grupy  $G$ , to dla każdego  $g$  takiego, że  $\phi_g \in I(G)$  zbiorem **sprzeżony** do  $M$  nazywamy zbiór

$$M^g = \{\phi_g(x) : x \in M\}$$

Jeśli  $M = \{x\}$ , to  $M^g$  zawiera elementy sprzeżone z  $x$ .

**Normalizator** zbioru  $M$ :

$$N_G(M) = \{g \in G : M^g = M\}$$

**Centralizator** zbioru  $M$ :

$$C_G(M) = \{g \in G : mg = gm, m \in M\}$$

Twierdzonek:

$$\hookrightarrow (\forall M \subseteq G) C_G(M) \triangleleft N_G(M) \quad (|M| = 1 \implies C_G(M) = N_G(M))$$

$$\hookrightarrow Z(G) = C_G(G)$$

$$\hookrightarrow \text{dla } M \subseteq G \text{ ilość zbiorów } M^g \text{ jest równa } [G : N_G(M)].$$

Aby klasa elementów sprzeżonych z  $x \in G$  była jednoelementowa wystarczy, żeby  $x \in Z(G)$

Jeśli  $G$  jest skończona, to ilość elementów sprzeżonych z zadany  $x$  jest dzielnikiem  $|G|$ .

**p-grupa** to grupa, w której wszystkie elementy mają rząd  $p$ , gdzie  $p$  jest liczbą pierwszą. Jeśli  $|G| = p^n$  to  $G$  jest  $p$ -grupą.

Skończone  $p$ -grupy mają **nietrywialne centrum**.

Jeśli  $|G| = p^2$ , to  $G$  jest grupą abelową.



Listy zadań i cw po angielsku, wykład po polsku + terminologia ang; kolokwia po angielsku  
konsultacje: pon 11-13 (sala 502)  
kolokwia w trakcie konwersatorium

## 2 Wstęp

### 2.1 Działania

Działanie [🇬🇧 operation]

↪ np. dodawanie, mnożenie

↪ składanie funkcji

Formalnie, działaniem w dowolnym zbiorze  $X$  to dowolna funkcja  $\star : X \times X \rightarrow X$ . Dla dowolnych  $a, b \in X$  zamiast pisać  $\star((a, b))$ , używamy  $a \star b$ .

Przykłady:

↪ na dowolnym z  $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$  mamy dodawanie (+) i mnożenie (·)

↪ na  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{N}$  mamy  $\leq$  który daje działania:

$$a \vee b := \min a, b$$

$$a \wedge b := \max a, b$$

↪ np na  $\mathbb{R}$  możemy zdefiniować  $a \star b := a + b^2$

↪ niech  $X$  będzie zbiorem, a  $X^X$  będzie zbiorem wszystkich funkcji  $X \rightarrow X$ , wtedy składanie funkcji jest działaniem określonym w  $X^X$ :

$$f \circ g \in X^X$$

MOŻNA DOJEBAC GRAFIK KOMUTUJĄCY

↪  $X$  – zbiór i niech  $\mathcal{P}(X)$  to zbiór wszystkich podzbiorów  $X$ , wtedy na  $\mathcal{P}(X)$  mamy działanie sumy [🇬🇧 union] i przekroju [🇬🇧 intersection]

↪ niech  $a, b \in X$ , wtedy mamy rzuty na osie:

$$a \text{L} b := a$$

$$a \text{P} b := b$$

↪ na zbiorze  $\mathbb{R} \cup \{\infty\}$  definiujemy ( $\forall a \in \mathbb{R} \cup \{\infty\}$ )  $a + \infty = \infty = \infty + a$  oraz ( $\forall a, b \in \mathbb{R}$ )  $a + b = a +_{\mathbb{R}} b$  (dodawanie w  $\mathbb{R}$ )

Prosty opis działań – niech  $\star$  będzie działaniem określonym w  $A = \{a_1, \dots, a_n\}$ , to możemy dobrać tabelkę:

$\star$	$a_1$	$a_2$	$\dots$	$a_n$
$a_1$	$a_1 \star a_1$	$a_1 \star a_2$	$\dots$	$a_1 \star a_n$
$a_2$	$a_2 \star a_1$	$a_2 \star a_2$	$\dots$	$a_2 \star a_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_n$	$a_n \star a_1$	$a_n \star a_2$	$\dots$	$a_n \star a_n$

Sensowne działania to dla nas:

↪ działania **łączne**. Można by tutaj napisać literkową definicję, ale mi się nie chce

↪ istnieje **element neutralny**

↪ czasem istnieje **element odwrotny** do danego  $x$

.....

Niech  $S_X \subseteq X^X$  oznacza zbiór wszystkich bijekcji  $X \rightarrow X$

**Grupa przekształceń** [🇬🇧 transformation group] – niepusty podzbiór  $G \subseteq S_X$ , który jest:

↪ jest zamknięty na łączenie funkcji

↪ ( $\forall f \in G$ )  $f^{-1} \in G$

Pojęcie to wprowadził Galois ok 1830, gdzie  $X$  był zbiorem pierwiastków pewnego wielomianu.

Pare  $(G, \star)$  nazywamy **grupą** group, gdy  $\star$  jest działaniem określonym w  $G$  oraz zachodzi

↪ ( $\forall a, b, c \in G$ )  $a \star (b \star c) = (a \star b) \star c$ , czyli działanie jest **łączne** [🇬🇧 associative]

↪  $\star$  ma element neutralny [🇬🇧 neutral element]

↪  $\star$  ma element odwrotny [🇬🇧 inverse element] dla każdego elementu  $G$

### 2.2 Grupy