



1 Teoria grup

1.1 Grupy, pierścienie, ciała

Działanie na zbiorze X :

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

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

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

Element odwrotny do x to takie y , że $xy = yx = e$. Jeśli działanie jest łączne, 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 to niepusty zbiór z łącznym działaniem i elementem neutralnym (zwanym **jednością grupy**) oraz elementami odwrotnymi dla każdego elementu.

↪ **grupa abelowa** (przemienna) – 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*

PIERŚCIEN to niepusty zbiór X z dwoma działaniami $(\cdot, +, \text{mnożenie i dodawanie})$ 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 \star :

• **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 grupą, a e jej elementem neutralnym. Wówczas:

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

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

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

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

* 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

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

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** ($o(a) = \infty$).

↪ **grupa torsyjna** – wszystkie elementy mają rząd skończony

↪ **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

1.3 Permutacje :>

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

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

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

Mnozenie 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

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

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:

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

\Leftrightarrow rząd i indeks każdej podgrupy są dzielnikami rzędu grupy,

\Leftrightarrow jeśli rząd jest liczbą pierwszą, to grupa jest cykliczna

Twierdzenie Lagrange’a – dla skończonych $G > H$:

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

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 $f = \psi \circ \phi$

Jezeli $\emptyset \neq A \subseteq G$ oraz $G(A) < G$ to przekroj wszystkich podgrup G zawierajacych A , a $A \subseteq G_1 < G$, to $G(A) < G_1$.

Jezeli $K \triangleleft G$ i $H \triangleleft G$, to najmniejsza podgrupa G zawierajaca H i K pokrywa sie ze zbiorom

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

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

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

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

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

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

Drugie twierdzenie o izomorfizmach – jezeli $K \triangleleft G$ i $K < H < G$ i oznaczmy $\bar{H} = H/K$ oraz $\bar{G} = G/K$, to wtedy:

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

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

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

Jesli G to grupa abelowa, to dla kazdego g $\phi_g(x) = x$, a wiec ma ona jedynie idynty- cznosc.

Zbior wszystkich automorfizmow wewnetrznych grupy G oznaczamy $I(G)$ i tworzy on grupe ze skladaniem

Centrum grupy G $Z(G)$ to zbior $x \in G$ takich, ze dla dowolnego $y \in G$ $xy = yx$. Dla kazdego G $Z(G) \triangleleft G$

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

Jesli M to dowolny podzbior grupy G , to dla kazdego g takiego, ze $\phi_g \in I(G)$ zbiorem sprzezony do M nazywamy zbior

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

Jesli $M = \{x\}$, to M^g zawiera elementy sprze- zone z x .

Normalizator zbioru M :

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

Centralizator zbioru M :

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

Twierdzonka:

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

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

$$\hookrightarrow \text{dla } M \subseteq G \text{ ilosc zbiorow } M^g \text{ jest rowna } [G : N_G(M)].$$

Aby klasa elementow sprzezonych z $x \in G$ byla jednoelementowa wystarczy, zeby $x \in Z(G)$

Jesli G jest skonczone, to ilosc elemen- tow sprzezonych z zadany x jest dzielnikiem $|G|$.

p-grupa to grupa, w ktorej wszystkie ele- menty maja rzad p , gdzie p jest liczba pier- wsza. Jesli $|G| = p^n$ to G jest p -grupa.

Skonczone p -grupy maja **nietrywialne centrum**.

Jesli $|G| = p^2$, to G jest grupa abelowa.

1.5 Produkty grup

W zbiorze $A \times B = \{(a, b) : a \in A, b \in B\}$, gdzie A, B sa grupami, okreslmy

$$(a, b) \cdot (c, d) = (ac, bd)$$