

# Algebra 1R

## Contents

<b>1</b>	<b>DEFINICJA GRUPY</b>	<b>3</b>
1.1	Działania, struktury	3
1.2	Grupy	3
1.3	Grupa cykliczna	4
<b>2</b>	<b>HOMOMORFIZMY</b>	<b>6</b>
2.1	Rodzaje	6
2.2	Jądro, obraz	6
2.3	Zasadnicze twierdzenie o homomorfizmie	6
<b>3</b>	<b>PERMUTACJE</b>	<b>7</b>
3.1	Transpozycje	7
3.2	Permutacje parzyste	7
<b>4</b>	<b>WARSTWY, DZIELNIK NORMALNY</b>	<b>8</b>
4.1	Warstwa, grupa ilorazowa	8
4.2	Orbita	8
4.3	Stabilizator	8
4.4	Orbit-stabilizer theorem	8
4.5	Dzielnik normalny	8
<b>5</b>	<b>PRODUKT PÓŁPROSTY</b>	<b>9</b>
5.1	Twierdzenie Lagrange'a	9
5.2	Produkt prosty	9
5.3	Produkt półprosty grup	9
<b>6</b>	<b>TWIERDZENIE SYLOWA</b>	<b>10</b>
6.1	I twierdzenie Sylowa	10
6.2	Twierdzenie Cauchy'ego	10
6.3	p-grupy Sylowa	10
6.4	Twierdzenia Sylowa	10
<b>7</b>	<b>KLASYFIKACJA MAŁYCH GRUP</b>	<b>11</b>
7.1	Grupy rzędu ???	11
<b>8</b>	<b>GRUPY TORSYJNE</b>	<b>12</b>
8.1	Torsje	12
8.2	Grupy torsyjne	12
8.3	Skończone grupy abelowe	12
<b>9</b>	<b>GRUPY ROZWIĄZALNE</b>	<b>13</b>
9.1	Komutator i komutant	13
9.2	Grupy rozwiązalne	13
9.3	Rozszerzenia grup rozwiązalnych	13
9.4	Używanie twierdzeń Sylowa	13
9.5	Grupy nilpotentne	13
<b>10</b>	<b>LEMAT O MOTYLU</b>	<b>14</b>
10.1	Ciąg kompozycyjny w grupie	14
10.2	Lemat motyla	14
10.3	Twierdzenie Schreiera	14

<b>11 GRUPY WOLNE</b>	<b>15</b>
11.1 Grupy wolne . . . . .	15
11.2 Własności . . . . .	15
11.3 Przykłady . . . . .	15
<b>12 PIERŚCIEŃ</b>	<b>16</b>
12.1 Definicja . . . . .	16
12.2 Dzielnik zera . . . . .	16
12.3 Grupa elementów odwracalnych pierścienia . . . . .	16
12.4 Dziedzina . . . . .	16
12.5 Ciało . . . . .	16

# 1 DEFINICJA GRUPY

## 1.1 Działania, struktury

DZIAŁANIE w zbiorze  $A$  to funkcja

$$\star : A \times A \rightarrow A$$

$$(x, y) \mapsto x \star y$$

Zwykle rozważamy działania binarne, ale działaniem może być funkcja z  $A^n$  w  $A$  (jak na przykład branie średniej arytmetycznej 3 liczb). Zdarza się też, że mamy działanie unarne, takie jak na przykład branie liczby przeciwnej do  $m \in \mathbb{Z}$ .

Działanie jest **łączne** [🇸🇪 *assosiative*], jeżeli

$$(\forall a, b, c \in A) a(bc) = (ab)c$$

a **przemienne** [🇸🇪 *commutative*], gdy

$$(\forall a, b \in A) ab = ba$$

Tutaj warto zaznaczyć, że jeśli działanie jest łączne dla 3 argumentów, to jest również łączne dla  $k$  argumentów. Dowód przez indukcję jest trywialny.

Algebrą nazywamy niepusty zbiór  $A$  ze wszystkimi działaniami na nim określonymi, to znaczy zestawienie  $(A, f_1, \dots, f_k)$ . Zbiór  $A$  nazywamy **uniwersum** lub dziedziną struktury. Mówimy, że dwie algebry  $A = (A, f_1, \dots, f_k)$  i  $B = (B, g_1, \dots, g_k)$  są **podobne**, jeśli dla każdego  $i \leq k$  arność (czyli liczba argumentów)  $f_i$  jest równa arności  $g_i$ , czyli liczbie  $l_i$ .

Dwie algebry są **izomorficzne**, jeżeli istnieje  $F : A \xrightarrow{1-1} B$  takie, że

$$(\forall i \leq k)(\forall a_1, \dots, a_{l_i} \in A) F(f_i(a_1, \dots, a_{l_i})) = g_i(F(a_1), \dots, F(a_{l_i}))$$

Struktury izomorficzne oznaczamy  $A \cong B$ . Warto zauważyć, że  $\cong$  ma *własności relacji równoważności*, to znaczy jest zwrotny, symetryczny i przechodni.

$B = (B, g_1, \dots, g_k)$  jest **podalgebrą**  $A = (A, f_1, \dots, f_k)$ , jeżeli

$$\hookrightarrow B \subseteq A$$

$$\hookrightarrow (\forall i \leq k) g_i = f_i|_B$$

Niech  $B \subseteq A$ , wtedy  $B$  jest uniwersum podstruktury struktury  $A$  z naturalnymi działaniami  $\iff B$  jest zamknięty na działania  $f_1, \dots, f_k$ . W takim przypadku  $B$  traktujemy jako strukturę będącą podstrukturą struktury  $A$ .

## 1.2 Grupy

**Monoid** to zbiór  $X$  z działaniem łącznym oraz elementem neutralnym. Liczby naturalne z dodawaniem są przykładem monoidu.

**Grupa** to struktura  $G = (G, \cdot)$  taka, że:

$$\hookrightarrow \cdot \text{ jest działaniem łącznym}$$

$$\hookrightarrow \text{ istnieje element neutralny } e \in G \text{ dla działania } \cdot$$

$$\hookrightarrow \text{ dla każdego } g \in G \text{ istnieje element odwrotny } g^{-1} \in G \text{ takie, że } gg^{-1} = g^{-1}g = e$$

Grupa trywialna to zbiór z działaniem zawierający jedynie jego element neutralny:  $\{e\}$ .

Tutaj warto zaznaczyć, że *element neutralny jest jedyny*. W przeciwnym przypadku istniałyby co najmniej dwa elementy neutralne  $e_1, e_2$ , ale wtedy

$$e_1 = e_1 \cdot e_2 = e_2.$$

Z łączności działania na grupie wynika, że dla każdego  $g \in G$  *istnieje co najwyżej jeden element odwrotny*. Gdyby  $x, y$  były dwoma elementami odwrotnymi do  $g$ , to

$$x = xe = x(gy) = (xg)y = ey = y,$$

co prowadzi do sprzeczności.

Jeśli działanie grupy jest przemienne, to nazywamy ją **grupą abelową** lub przemianą. Tak jak działanie w grupie oznaczamy zwykle przez  $\cdot$ , tak w grupie abelowej, aby podkreślić jego przemienność, działanie jest zwykle oznaczane przez  $+$ . Podobnie, potęgowanie w grupie abelowej nie oznaczamy  $x^n$ , a raczej  $nx$ .

Działanie w grupie możemy opisać za pomocą **tabelki**

$\star$	$a_1$	$a_2$	$\dots$	$a_k$
$a_1$	$a_1 a_1$	$a_1 a_2$	$\dots$	$a_1 a_k$
$a_2$	$a_2 a_1$	$a_2 a_2$	$\dots$	$a_2 a_k$
$\dots$				
$a_k$	$a_k a_1$	$a_k a_2$	$\dots$	$a_k a_k$

Jeżeli działanie jest przemienne, to oczywiście taka tabelka będzie symetryczna.

Grupę przemianą  $G = \{e, a, b, c\}$  nazywamy **grupą czwórkową Kleina**  $[K_4]$ . Grupa izometrii własnych  $n$ -kąta foremnego  $[D_n]$  jest nazywana grupą **dihedralną** i nie jest ona grupą abelową. Jej podgrupą jest na przykład **grupa obrotów własnych**  $n$ -kąta foremnego  $[O_n]$ .

**Pierścieniem** nazywamy zbiór  $X$  z dwoma działaniami,  $+$  i  $\cdot$ , z których  $\cdot$  jest łączne, a  $+$  jest przemienne. W dodatku,  $\cdot$  jest rozdzielne względem  $+$ :

$$(\forall x, y, z \in X) x \cdot (y + z) = x \cdot y + x \cdot z$$

Jeśli dodatkowo mnożenie w pierścieniu jest działaniem przemianym, to taki pierścień nazywamy **przemienny**. Jeśli zaś istnieje element neutralny dla mnożenia, to jest on **pierścieniem z jednością**.

Pierścień  $K$ , dla których  $K \setminus \{0\}$  jest grupą przemianą względem mnożenia nazywamy **ciałami**. Najprostszym ciałem są zbiory  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  ze zwykłym dodawaniem i mnożeniem. Zbiór  $\mathbb{Q}(i)$  wszystkich liczb zespolonych postaci  $a + bi$  dla wymiernych  $a, b$  jest ciałem.

Niech  $H \subseteq G$  dla pewnej grupy  $G$ . Mówimy, że  $H$  jest **podgrupą** grupy  $G$  [ $H \leq G$ ], jeżeli  $H$  jest grupą względem działania z  $G$  (ograniczonego do  $H$ ). Dodatkowo, jeśli  $H \neq G$  to mówimy, że  $H$  jest **podgrupą właściwą**. Na przykład

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +).$$

Przy sprawdzaniu, czy dany zbiór  $H$  jest podgrupą  $G$  wystarczy sprawdzić, czy  $(\forall x, y \in H) xy^{-1} \in H$ .

Jeśli  $a, b \in G$ , to  $(ab)^{-1} = b^{-1}a^{-1}$ .

**DOWÓD:**

Chcemy sprawdzić, że  $(b^{-1}a^{-1})ab = e$

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$$

a więc dostajemy to, czego się spodziewaliśmy.



Zdefiniujemy  $a^{-n} = (a^{-1})^n$  i nie trudno pokazać, że też  $a^{-n} = (a^n)^{-1}$ . Dalej mamy  $a^{n+m} = a^n a^m$ , a dla grupy przemiennej zachodzi  $(ab)^n = a^n b^n$ .

## 1.3 Grupa cykliczna

**Rząd grupy** to ilość jej elementów:  $\text{ord}(G) = |G|$ . Dla każdego  $g \in G$  definiujemy **rząd elementu**  $\text{ord}(g) = N$  jako najmniejszą liczbę naturalną taką, że  $g^N = e$ . Znając pojęcie grup cyklicznych (niżej) możemy też podać definicję:  $\text{ord}(g) = \langle g \rangle$ . Jeśli  $\text{ord}(g) = n$  i weźmiemy  $N$  takie, że  $g^N = e$ , to mamy pewność, że  $n|N$ . Gdyby tak nie było, to mielibyśmy  $N = kn + r$ ,  $0 < r < n$  i

$$g^N = g^{kn+r} = g^{kn} g^r = (g^n)^k g^r = e^k g^r = g^r \neq e.$$

W takim razie dla  $g, g^2, \dots, g^{n-1}$  są elementami parami różnymi i tworzą podgrupę grupy  $G$ .

**Grupa cykliczna** to grupa utworzona przez wzięcie wszystkich potęg  $g \in G$ :  $H = \{g, g^1, \dots, g^{\text{ord}(g)}\}$ , przy czym możemy mieć  $\text{ord}(g) = \infty$ . W takim przypadku dostajemy podgrupę nieskończoną. Dla grupy cyklicznej utworzonej przez  $g$ , ten element nazywamy **generatorem**. Zauważmy, że wszystkie grupy cykliczne są **abelowe**.

Grupa zawierająca wszystkie liczby całkowite z dodawaniem jest grupą cykliczną generowaną przez 1 lub przez  $-1$ . Widzimy więc, że generator grupy nie jest wyznaczony jednoznacznie.

Dla  $N \in \mathbb{N}$  definiujemy  $C_N$  jako liczby naturalne  $< N$  z dodawaniem modulo  $N$ . Zwykle oznaczamy ją  $(\mathbb{Z}_N, +_N)$ . Możemy pokazać, że każda grupa cykliczna skończona rzędu  $N$  jest izomorficzna z  $C_N$ , natomiast grupy cykliczne nieskończone są izomorficzne z  $C_\infty$ .

## 2 HOMOMORFIZMY

Jeżeli  $f : A \rightarrow B$  jest homomorfizmem struktur, to  $\text{Im}(f)$  jest podstrukturą  $B$ .

### SŁOWNICZEK:

- $\hookrightarrow$  epi-morfizm  $\rightarrow$  "na"
- $\hookrightarrow$  mono-morfizm  $\rightarrow$  1-1
- $\hookrightarrow$  izo-morfizm  $\rightarrow$  bijekcja
- $\hookrightarrow$  endo-morfizm  $\rightarrow$  w samego siebie
- $\hookrightarrow$  auto-morfizm  $\rightarrow$  endomorfizm który jest bijekcją.

Złożenie homomorfizmów jest homomorfizmem a odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

### DOWÓD:

Niech  $f : (X, \cdot) \rightarrow (Y, \circ)$  i  $g : (Y, \circ) \rightarrow (Z, \star)$  są homomorfizmami, a  $h(x) = g(f(x))$  jest ich złożeniem, to dla dowolnego  $a, b \in X$  mamy

$$h(a \cdot b) = g(f(a \cdot b)) = g(f(a) \circ f(b)) = g(f(a)) \star g(f(b)) = h(a) \star h(b)$$

więc  $h$  spełnia warunki homomorfizmu. Jeżeli  $f, g$  były epi, mono, ... morfizmami, to zachowanie odpowiednich własności wynika z własności składania funkcji różnowartościowych, na czy bijekcji.

Niech  $\phi : (X, \cdot) \xrightarrow[\text{na}]{1-1} (Y, \circ)$  będzie izomorfizmem. Chcemy pokazać, że  $\phi^{-1}$  jest homomorfizmem. Weźmy  $a, b \in Y$  i  $c, d \in X$  takie, że  $\phi(c) = a$  oraz  $\phi(d) = b$ . Wtedy

$$ab = \phi(c)\phi(d) = \phi(cd),$$

czyli

$$\phi^{-1}(ab) = cd,$$

a ponieważ  $\phi^{-1}(a) = c$  i  $\phi^{-1}(b) = d$ , to mamy

$$\phi^{-1}(ab) = cd = \phi^{-1}(a)\phi^{-1}(b).$$

Natomiast fakt, że  $\phi^{-1}$  jest bijekcją wynika z tego, że  $\phi$  jest bijekcją.

### 2.1 Rodzaje

### 2.2 Jądro, obraz

### 2.3 Zasadnicze twierdzenie o homomorfizmie









## 6 TWIERDZENIE SYŁOWA

### 6.1 I twierdzenie Sylowa

#### I twierdzenie Sylowa:

Jeżeli  $p$  jest liczbą pierwszą, a  $G$  jest grupą skończoną rzędu  $|G| = p^k m$  dla  $k \geq 1$  i  $p \nmid m$ , to istnieje podgrupa  $H \leq G$  mająca  $p^k$  elementów. Taka grupa nazywa się **podgrupą Sylowa**.

#### DOWÓD:

Niech  $G$  będzie grupą rzędu  $|G| = p^k m$  taką jak w twierdzeniu. Niech  $X$  będzie zbiorem wszystkich  $p^k$  elementowych podzbiorów grupy  $G$ . Możemy teraz określić działanie  $\psi$  grupy  $G$  na zbiór  $X$ . Jeśli  $H = \{h_1, \dots, h_{p^k}\} \in X$ , a  $g \in G$ , to

$$\psi(H) = \{gh_1, gh_2, \dots, gh_{p^k}\}.$$

Wiemy, że

$$\begin{aligned} |H| &= \binom{p^k m}{p^k} = \frac{(p^k m)!}{(p^k m - p^k)! (p^k)!} = \\ &= \frac{p^k m (p^k m - 1) \dots (p^k m - p^k + 1)}{(p^k)!} = \prod_{i=1}^{p^k} p^k m - i + 1 \end{aligned}$$

### 6.2 Twierdzenie Cauchy'ego

#### Twierdzenie Cauchy'ego:

Jeżeli liczba pierwsza  $p$  dzieli rząd grupy  $G$ , to  $G$  zawiera element rzędu  $p$ .

### 6.3 p-grupy Sylowa

### 6.4 Twierdzenia Sylowa











