GRUPY I ICH ZASTOSOWANIA

PASJONACI MATEMATYKI

1. Definicje i przykłady

Motywacja:

(1) chcemy sformalizować koncept *symetrii*, łączący różne działy matematyki (teorię liczb, kombinatorykę, analizę, algebrę, ...), fizyki, chemii i innych nauk.
(2) Kryptografia: schemat El-Gamal.

Grupa to zbiór z „ładnym" działaniem. Zazwyczaj grupy powstają jako zbiory symetrii interesujących nas obiektów.

Definicja 1.1. Grupa to zbiór G wraz z działaniem $\star : G \times G \to G$ takim, że:

- (łączność) $(a \star b) \star c = a \star (b \star c)$,
- (istnienie eltu neutralnego) istnieje $e \in G$ takie, że $a \star e = e \star a = a$ dla każdego $a \in G$,
- (istnienie eltów przeciwnych) $\forall_{a \in G}\ \exists_b : a \star b = b \star a = e$.
  (b oznaczamy jako a^{-1})

Jeżeli $a \star b = b \star a$ to mówimy, że G jest **przemienna** (lub też **abelowa**). **Rząd grupy** to liczba jej elementów.

Przykład 1.2.

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, *ale nie* $(\mathbb{Z}, -)$,
- $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$ *nie są grupami.* $(\mathbb{R} \setminus \{0\}, \cdot)$ *jest grupą,*
- $(\mathbb{Z}/n, +_n)$, *gdzie* $\mathbb{Z}/n := \{0, 1, \ldots, n-1\}$ *oraz* $a +_n b := (a+b) \pmod n$ *(reszty z dzielenia przez n),*

  > $a \pmod n$ – *reszta z dzielenia a przez n (np.* $99 \pmod 5 = 4$*).*
  > *Piszemy* $a \equiv b \pmod n$*, jeżeli a oraz b dają tą samą resztę z dzielenia przez n (tzn.* $n | a - b$*).*

- $(\Phi(n), \cdot_n)$, *gdzie* $\Phi(n) := \{a \in \mathbb{Z}/n : NWD(a, n) = 1\}$ *oraz* $a \cdot_n b := (a \cdot b) \pmod n$.
  (np. $\Phi(9) = \{1, 2, 4, 5, 7, 8\}$ *oraz* $4^{-1} = 7$*, bo* $4 \cdot_9 7 = 1$*)*
- $\mathbb{Z}/2 \times \mathbb{Z}/2$*,*

- D_3 – *grupa "symetrii" trójkąta równobocznego:* $D_3 = \{O_{0^\circ}, O_{120^\circ}, O_{240^\circ}, s_A, s_B, s_C\}$. *Tabelka działania:*

$\circ$	O_{0°	O_{120°	O_{240°	s_A	s_B	s_C
O_{0°	O_{0°	O_{120°	O_{240°	s_A	s_B	s_C
O_{120°	O_{120°	O_{240°	O_{0°	s_C	s_A	s_B
O_{240°	O_{240°	O_{0°	O_{120°	s_B	s_C	s_A
s_A	s_A	s_C	s_B	O_{0°	O_{240°	O_{120°
s_B	s_B	s_A	s_C	O_{120°	O_{0°	O_{240°
s_C	s_C	s_B	s_A	O_{240°	O_{120°	O_{0°

- $S_n = \{$ *bijekcje* $f : \{1,\dots,n\} \to \{1,\dots,n\}\}$ *z działaniem składania. Przykład: w* S_5

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

  Grupa ta ma $n!$ *elementów.*

Definicja 1.3 (nieformalna)**.** G_1 i G_2 są **izomorficzne**, jeżeli są takie same po poprzestawianiu elementów.

Przykład 1.4.
(1) $\Phi(4) = \{1,3\}$, $\mathbb{Z}/2 = \{0,1\}$,
(2) $\mathbb{Z}/3 = \{0,1,2\}$, $\{e, r, r^2\}$,
(3) S_3, D_3.

Definicja 1.5. Rząd elementu $g \in G$:

$$ord(g) = \min\{n \geq 1 : g^n = e\}.$$

Przykłady:
- W $\mathbb{Z}$: $ord(n) = \infty$ dla $n \neq 0$.
- W $\mathbb{Z}/6$: $ord(4) = 3$, bo $4+4+4 = 12 \equiv 0 \pmod 6$.
- W $\Phi(7)$ mamy $ord(2) = 3$, bo $2^3 = 8 \equiv 1 \pmod 7$.
- W D_3: $ord(r) = 3$, $ord(s) = 2$.
- W S_4:

$$ord\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\right) = 4$$

Fakt 1.6.
(1) $ord(g) | \#G$
(2) $g^k = e$ *wtw gdy* $ord(g) | k$.

Dowód. (1) Udowodnimy później ogólniejszy fakt.
(2) jeżeli $ord(g) = n$, $k = K \cdot n$, to $g^k = (g^n)^K = e$.
Jeżeli $g^k = e$, to zapiszmy $k = qn + r$ dla $0 \leq r < n$. Wtedy:

$$g^r = e \cdot g^r = g^{qn+r} = g^k = e.$$

Z minimalności n dostajemy $r = 0$. □

Wniosek 1.7 (Małe Twierdzenie Fermata)**.** $p \in \mathbb{P}$, $p \nmid a \Rightarrow p | a^{p-1} - 1$
(tzn. $a^{p-1} \equiv 1 \pmod p$*).*

Dowód. $\Phi(p) = \{1,\dots,p-1\}$. Stąd $ord(a) | p-1 = |G|$, zatem $a^{p-1} \equiv 1 \pmod p$. □

2. Rzędy, podgrupy

Spójrzmy na obroty w D_3. Są one zamknięte ze względu na składanie, więc ich zbiór również tworzy grupę!

Definicja 2.1. Jeżeli $H \subset G$ spełnia:

- $e \in H$,
- $\forall_{a,b \in H}\, a \star b \in H$,
- $\forall_{a \in H}\, a^{-1} \in H$,

to mówimy, że H jest podgrupą G (zapisujemy: $H \leq G$).

Przykład 2.2.

- $\{0,3\} \leq \mathbb{Z}/6$,
- $5\mathbb{Z} \subset \mathbb{Z}$,
- $\{n \cdot \sqrt{2} : n \in \mathbb{Z}\} \subset \mathbb{R}$ *oraz* $\mathbb{Q} \subset \mathbb{R}$
- $\{e, r, r^2\}, \{e, s\} \subset D_3$,
- $S_{n-1} \leq S_n$

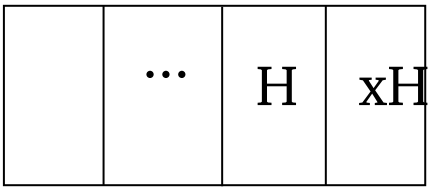
Definicja 2.3. Jeżeli $g \in G$ to zbiór $\langle g \rangle := \{g^k : k \in \mathbb{Z}\}$ jest podgrupą G (**podgrupa cykliczna generowana przez** g). Wtedy $|\langle g \rangle| = ord(g)$ oraz:

- $\langle g \rangle \cong \mathbb{Z}$, jeżeli $ord(g) = \infty$,
- $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\} \cong \mathbb{Z}/n$, jeżeli $ord(g) = n$.

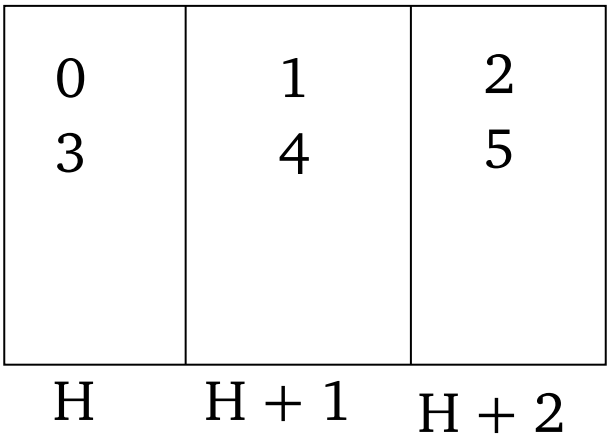
Uwaga 2.4. *Uwaga: okazuje się, że jeżeli H jest podgrupą grupy $\mathbb{R}$, to albo H jest cykliczna (jak np. $\{n \cdot \sqrt{2} : n \in \mathbb{Z}\}$), albo też jest gęsta jak $\mathbb{Q}$ (tzn. pomiędzy dowolnymi dwiema różnymi liczbami rzeczywistymi znajdziemy element tej grupy).*

Fakt 2.5. *Jeżeli $H \subset G$ jest podgrupą, to $|H| \,|\, |G|$.*

Dowód.



np.



□

Przykład 2.6. *(1)* $\mathbb{Z}/2 \times \mathbb{Z}/3$ *– mamy:*

$$1\cdot(1,1)=(1,1), 2\cdot(1,1)=(0,2), 3\cdot(1,1)=(1,0), 4\cdot(1,1)=(0,1), 5\cdot(1,1)=(1,2)$$

więc $ord((1,1))=6$ *oraz* $\mathbb{Z}/2\times\mathbb{Z}/3 \cong \mathbb{Z}/6$.

(2) $\Phi(7)=\{1,2,3,4,5,6\}$. *Mamy:*

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1,$$

zatem $\Phi(7)=\langle 5\rangle$*!*

Twierdzenie 2.7. *Jeżeli p jest liczbą pierwszą, to* $\Phi(p)$ *jest grupą cykliczną.*

Conjecture 2.8 (Artina)**.** 2 *jest generatorem dla nieskończenie wielu p.*

(prawdziwa przy założeniu Wielkiej Hipotezy Riemanna)

3. Działanie grupy na zbiorze

Definicja 3.1. Działanie grupy G na zbiorze X: działanie $\circ : G \times X \to X$ spełniające:

- $e \circ x = x$ dla każdego $x \in X$,
- $g \circ (h \circ x) = (g \star h) \circ x$.

Definicja 3.2. Orbita elementu $x \in X$:

$$Gx := \{g \circ x : g \in G\}.$$

Zbiór orbit: X/G.
Stabilizator elementu:

$$G_x := \{g \in G : g \circ x = x\}.$$

Zbiór punktów stałych elementu:

$$Fix(g) := \{x \in X : g \circ x = x\}.$$

Przykład 3.3.

(1) $G = D_3$*,* $X =$ *wierzchołki trójkąta równobocznego.*

$$GA = \{A,B,C\}, \quad G_A = \{O_{0^\circ}, s_A\}$$

(2) $G = \mathbb{R}$*,* $X = \mathbb{R}^2$*,* $\alpha \circ x :=$ *x obrócony o* α *stopni*

$$Fix(\alpha) = \{(0,0)\},\ Gx = O(x,|x|),\ G_x = 2\pi\mathbb{Z} \quad dla\ x \neq (0,0).$$

Zbiór orbit $\Leftrightarrow [0,\infty)$.

(3) $G = S_3$*,* $X =$

Twierdzenie 3.4 (orbit–stabilizer theorem)**.**

$$|G|/|G_x| = |Gx|$$

Dowód. $|G|/|G_x| \leftrightarrow g \cdot G_x \leftrightarrow g(x)$. □

Przykład 3.5. $G = D_3$*,* $X = \{A,B,C\}$*. Mamy:*

$$GA = \{A,B,C\}, G_A = \{id, s_A\}.$$

Zatem $|G|/|G_A| = 6/2 = 3 = GA$.

Twierdzenie 3.6 (lemat Burnside'a)**.**

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|.$$

Przykład 3.7. *Na ile sposobów można pokolorować krawędzie trójkąta równobocznego* 4 *kolorami? Dwa sposoby uznajemy za takie same, jeżeli stają się takie same po zastosowaniu pewnej symetrii trójkąta. Niech* $G = D_3$ *(grupa dihedralna), a* X *będzie zbiorem wszystkich możliwych sposobów pokolorowania trójkąta.*
Liczba wszystkich kolorowań to $|X| = 4^3 = 64$*. Chcemy znaleźć* $|X/G|$ *(liczbę orbit). Mamy:*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

Grupa ma $|G| = 6$ *elementów, więc musimy policzyć* $|Fix(g)|$ *dla każdego* $g \in G$*.*

- $|Fix(e)| = 64$.
- *Dla obrotów* O_{120° *i* O_{240° *każda krawędź przechodzi na inną, więc kolorowanie pozostaje niezmienione tylko wtedy, gdy wszystkie krawędzie mają ten sam kolor – są 4 takie kolorowania. Stąd* $|Fix(O_{120^\circ})| = |Fix(O_{240^\circ})| = 4$.
- *Dla odbić każda symetria zamienia dwie krawędzie miejscami, więc kolorowanie pozostaje niezmienione, gdy te dwie krawędzie mają ten sam kolor. Możemy wybrać kolor dla nieruchomej krawędzi (4 opcje) oraz wspólny kolor dla pozostałych dwóch (również 4 opcje), co daje* $|Fix(s_A)| = 16$ *itd.*

Podstawiając do wzoru Burnside'a:

$$\frac{64+4+4+16+16+16}{6} = 20$$