WYKŁAD 11

Rozdział 14

Grupy

14.1 Automorfizmy

Definicja 14.1 (Grupa przekształceń (automorfizmów) obiektu)**.** Dla danego z obiektu kombinatorycznego S jego grupa przekształceń (symetrii, automorfizmów) $G = \mathrm{Aut}(S)$ powinna spełniać następująco warunki

- przekształcenie identycznościowe e jest w G
- jeśli $\varphi_1, \varphi_2 \in G$ to te przekształcenia można *złożyć* uzyskując $\varphi = \varphi_1 \circ \varphi_2 \in G$
- dla każdego $\varphi \in G$ istnieje φ^{-1} takie że $\varphi^{-1}\varphi = \varphi\varphi^{-1} = e$

Przykład 14.2. 1. kwadrat i jego obroty

2. kwadrat i jego symetrie
3. dwudziestościan foremny i jego obroty
4. macierz $n \times n$ i mnożenie przez macierze odwracalne
5. macierz $n \times n$ i mnożenie przez macierze odwracalne o wyznaczniku 1
6. macierz $n \times n$ i mnożenie przez macierze odwracalne o module wyznacznika równym 1
7. $\mathbb{Z}$ i dodawania elementów z $\mathbb{Z}$
8. $\mathbb{Z}_p$ i dodawanie elementów z $\mathbb{Z}_p$
9. $\mathbb{Z}_p \setminus \{0\}$ z mnożeniem przez niezerowe elementy w $\mathbb{Z}_p$
10. X i bijekcje z X w X
11. zbiór $\{1, 2, \ldots, n\}$ i jego permutacje
12. $2n$-kąt foremny i jego symetrie
13. $2n$-kąt foremny i jego obroty

14.2 Grupa

Definicja 14.3 (Grupa)**.** Zbiór $(G, \cdot)$, gdzie $\cdot : G \times G \to G$ jest działaniem dwuargumentowym jest *grupą*, gdy:

łączność działanie $\cdot$ jest łączne;

element neutralny istnieje element neutralny e taki że dla każdego $g \in G$ mamy $ge = eg = g$;

element odwrotny dla każdego $g \in G$ istnieje g^{-1} spełniający $g^{-1}g = gg^{-1} = e$.

Jeśli $\cdot$ jest przemienne, to mówimy o grupie *przemiennej* (*abelowej*).

Uwaga. Alternatywnie możemy zdefiniować grupę tak, że ma ona dodatkowo jedną operację unarną: $^{-1} : G \to G$ (branie elementu odwrotnego) oraz jedną stałą: e. Te operacje mają spełniać warunki podane w Definicji 14.3.

Lemat 14.4.

- *Element odwrotny w grupie G jest jedyny.*
- *Element prawostronnie odwrotny jest też lewostronnie odwrotny.*
- *Identyczność jest jedyna.*
- *Równanie $ax = b$ oraz $xa = b$ mają dokładnie jedno rozwiązanie.*

Przykład 14.5.
- $\{1, 3, 5, 7\}$ z mnożeniem mod 8 [Grupa Kleina]
- obroty kwadratu
- symetrie kwadratu
- obroty dwudziestościanu foremnego
- odwracalne macierze $n \times n$ (z mnożeniem)
- macierze $n \times n$ o wyznaczniku 1 (z mnożeniem)
- macierze $n \times n$ o module wyznacznika równym 1 (z mnożeniem)
- ortogonalne macierze $n \times n$ (z mnożeniem)
- $\mathbb{Z}$ z dodawaniem
- $\mathbb{Z}_n$ z dodawaniem modulo n
- $\mathbb{Z}_p \setminus \{0\}$ z mnożeniem (p — liczba pierwsza)
- bijekcje z X w X
- permutacje zbioru $\{1, 2, \ldots, n\}$
- obroty i symetrie $2n$-kąta foremnego
- obroty $2n$-kąta foremnego

14.2.1 Półgrupy

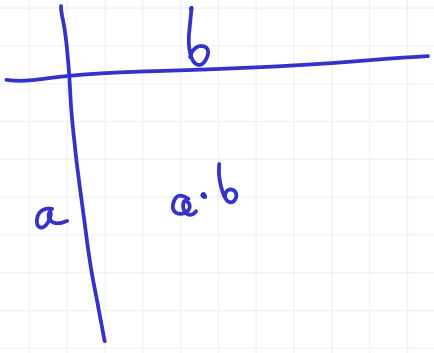
W ogólności rozważa się też monoidy (półgrupy), w których nie zakładamy istnienia elementu odwrotnego (elementu odwrotnego ani identyczności).

14.3 Tabelka działań (mnożenia)

Definicja 14.6 (Tabela działań)**.** *Tabela działań* dla grupy G podaje wprost wszystkie możliwe $|G|^2$ wyników mnożenia.

Przykład 14.7 (Tabela działań dla grupy Kleina).

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1



$g \cdot h = g' \cdot h$

$3 \cdot 3 = 3 \cdot 5$
$3x = 5$

Fakt 14.8. • *Każdy wiersz i każda kolumna w tabelce działań jest permutacją elementów z G.*

- *Dwa różne wiersze (dwie różne kolumny) są różne.*
- *Musi być dokładnie jeden wiersz (kolumna) w której permutacja jest identycznością.*

Definicja 14.9 (Iloczyn kartezjański grup; produkt prosty)**.** Dla grup G, H przez $G \times H$ oznaczamy grupę na zbiorze $G \times H$ i działaniu po współrzędnych

$$(g, h) \cdot (g', h') = (gg', hh') \ .$$

Definicję rozszerzamy naturalnie na iloczyn kartezjański dowolnej ilości grup.

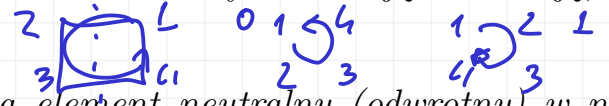
14.4 Homomorfizm, Izomorfizm

Definicja 14.10 (Homomorfizm, izomorfizm grup)**.** Operację $\varphi : \mathbb{G} \mapsto \mathbb{H}$ nazywamy *homomorfizmem grup*, jeśli zachowuje działanie grupowe, tj. $\varphi(ab) = \varphi(a)\varphi(b)$.

φ jest *izomorfizmem*, jeśli istnieje φ^{-1} które jest przekształceniem odwrotnym i homomorfizmem (w szczególności: φ, φ^{-1} są bijekcjami).

Przykład 14.11. • Izomorfizm: grupa Kleina oraz $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- Homomorfizm: macierze odwracalne rozmiaru $n \times n$ nad $\mathbb{F}$ $M \mapsto \det M$
- Homomorfizm: $\mathbb{Z}_2 \times \mathbb{Z}_2$ na pierwszą współrzędną.
- Homomorfizm: Macierze odwracalne w macierze o wyznaczniku ± 1: $\varphi(M) = M/|\det(M)|$.
- Homomorfizm: Macierze o wyznaczniku o module 1 w macierze o wyznaczniku 1: $\varphi(M) = M/\det(M)$.
- Homomorfizm: Obroty i symetrie kwadratu w $\mathbb{Z}_2$: czy zmieniają orientację, czy nie (tzn. symetrie w -1, obroty w 1).



Lemat 14.12. *Homomorfizm przeprowadza element neutralny (odwrotny) w neutralny (odwrotny).*

$x^2 = x$

G e $\qquad \varphi(e) \in H$

$\varphi(e)\cdot\varphi(e) = \varphi(e) \Rightarrow \varphi(e)$ – el. neutralny

$g,\ g^{-1}$ – $\qquad \varphi(g)^{-1} = \varphi(g^{-1})$

el. odwrotny do g to jedyny rozw. r.w. $g\cdot x = e$

g, g^{-1}, e

$e\cdot e = e \quad \rightarrow \quad \varphi(e)\varphi(e) = \underbrace{\varphi(e)}_{e_H}$

$g\cdot g^{-1} = e \quad \rightarrow \quad \varphi(g)\cdot\varphi(g^{-1}) = \varphi(e) = e_H$

$(\varphi(g))^{-1} = \varphi(g^{-1})$

14.5 Rząd elementu

Definicja 14.13 (Potęga, rząd)**.** Potęgą elementu a nazywamy dowolny element postaci a^n, gdzie $n \in \mathbb{Z}$. Dla $n = 0$ oznacza on e, dla $n > 1$: $a^n = \underbrace{a \cdot a \cdots a}_{n \text{ razy}}$, dla $n < 0$: $a^n = (a^{-1})^{-n}$.

Rząd elementu to najmniejsza dodatnia potęga n taka że $a^n = e$. Rząd elementu jest *nieskończony* (*nieokreślony*), jeśli nie ma takiego skończonego n.

Rząd grupy to ilość jej elementów (może, ale nie musi, być skończony).

Fakt 14.14. *Rząd a i rząd a^{-1} jest taki sam.*

Fakt 14.15. *W grupie skończonej każdy element ma rząd skończony.*

Lemat 14.16. *Jeśli $a \in G$ ma skończony rząd p, to $a^\ell = e \iff p|\ell$.*

$a^l = e$ $\quad$ $\text{rk}(a) = p$

$\Downarrow$

$p \mid l$ $\quad$ $(\ )(\ )(\ ) = e$

$e \quad e \quad c$

Zobaczmy, że n to najmniejsze l:

- $a^l = e$
- $p \nmid l$

1) $l < p$ $\quad$ $\lightning$ $\quad$ p to minimalne, t. że $a^p = e$

2) $l > p$ $\quad$ $l - p$

$a^l \cdot a^{-p} = a \cdot \ldots \cdot a \; a^{-1} \cdot \ldots \cdot a^{-1} = a^{l-p} = e$

$\uparrow e \quad \uparrow e \quad l \quad p$

$p \nmid l - p > 0$

$\lightning$

l to minimalne ($l - p$ też okr.)

W ogóle $\quad a^l = a^k \Rightarrow p \mid (l - k)$ $\quad l > k$

$a^{l-k} = e \quad p \mid l - k$

14.6 Podgrupy

Definicja 14.17 (Podgrupa)**.** H jest podgrupą G, co zapisujemy jako $H \leq G$, gdy $H \subseteq G$ oraz jest grupą.

Uwaga. Nie wystarczy, że $H \subseteq G$ i że jest zamknięta na działanie: może nie zawierać elementu odwrotnego! $\{1,2,3,\dots\} \subseteq \mathbb{Z}$ zam. na działanie

Uwaga. Dla alternatywnej definicji (z dodatkową operacją branie elementu odwrotnego oraz elementem neutralnym) już wystarczy, bo wtedy to są formalnie działania.

Przykład 14.18.
- Grupa obrotów $2n$ kąta w grupie symetrii $2n$ kąta.
- Dodawanie liczb parzystych w $\mathbb{Z}$.
- $\mathbb{Z}_2 \times \{0\}$ w $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- Macierze o wyznaczniku o module 1 w macierzach odwracalnych.
- Macierze o wyznaczniku 1 w macierzach odwracalnych.
- Macierze ortogonalne w macierzach odwracalnych.

Lemat 14.19. *W grupie skończonej G niepusty zbiór H jest podgrupą wtedy i tylko wtedy gdy jest zamknięty na działanie.*

W grupie, w której rząd każdego elementu jest skończony, niepusty podzbiór H jest podgrupą wtedy i tylko wtedy gdy jest zamknięty na działanie.

$H \subseteq G$ $\quad \cdot_H = \cdot_G \restriction_{H\times H}$

skoro H: zam. na działanie $\Rightarrow$ $\cdot_H$ jest dobrze określone

e, g^{-1}, $g, g^2, g^3, \dots, g^{p-1}, g^p = e$ jest $p = \mathrm{rk}(g)$

$g^{p-1} \cdot g = g^p = e$, $g^{p-1} = g^{-1}$

Definicja 14.20 (Generowanie)**.** Dla grupy G oraz zbioru $A \subseteq G$ podgrupa generowana przez A, oznaczana jako $\langle A \rangle$, to najmniejsza podgrupa G zawierająca A. W takim wypadku mówimy, że A to zbiór *generatorów* tej podgrupy.

$\mathbb{Z}$, $\langle 2, 4, 6, -8 \rangle = \langle$ liczby parz. $\rangle$

Przykład 14.21.
- $\mathbb{Z} = \langle 1 \rangle = \langle 3, 5 \rangle$
- $\mathbb{Z}_6 = \langle 1 \rangle = \langle 2, 3 \rangle$
- grupa obrotów kwadratu jest generowana przez obrót o 90^o
- grupa obrotów i symetrii kwadratu jest generowana przez obrót o 90^o i dowolną symetrię.

Fakt 14.22. $(x_1^{z_1} x_2^{z_2} \cdots x_k^{z_k})^{-1} = (x_k^{-1})^{z_k} (x_{k-1}^{-1})^{z_{k-1}} \cdots (x_1^{-1})^{z_1}$.

Definicja 14.23 (Postać zredukowana)**.** Niech $a_1, \ldots, a_k \in G$. O iloczynie $a_1^{\ell_1} a_2^{\ell_1} \cdots a_k^{\ell_k}$ mówimy, że jest w *postaci zredukowanej*, jeśli $a_i \notin \{a_{i+1}^{-1}, a_{i+1}\}$ dla każdego możliwego i oraz $\ell_i \neq 0$ dla każdego i.

Uwaga. Zauważmy, że jest możliwe, że zachodzą jakieś redukcje pomiędzy $a_i^{\ell_i}$ oraz $a_{i+1}^{\ell_{i+1}}$ czy możliwe jest wyrażenie jakiegoś podciągu w inny sposób.

Np. dla $a_1 = a^2$ oraz $a_2 = a^3$ ciąg $a_1^3 a_2^{-2}$ jest w postaci zredukowanej, pomimo tego, że $a_1^3 a_2^{-2} = e$.

Lemat 14.24. *Rozważmy ciągu elementów $a_1^{\ell_1} a_2^{\ell_1} \cdots a_k^{\ell_k}$ oraz następujące reguły przepisywania:*

- $a_i^{\ell_i} a_{i+1}^{\ell_{i+1}} \to a_i^{\ell_i + \ell_{i+1}}$, *jeśli* $a_i = a_{i+1}$
- $a_i^{\ell_i} a_{i+1}^{\ell_{i+1}} \to a_i^{\ell_i - \ell_{i+1}}$, *jeśli* $a_i = a_{i+1}^{-1}$
- $a_i^0 \to e$

Wtedy uzyskane końcowy ciąg $a_{i_1}^{\ell'_1} a_{i_2}^{\ell'_j} \cdots a_{i_j}^{\ell'_j}$:

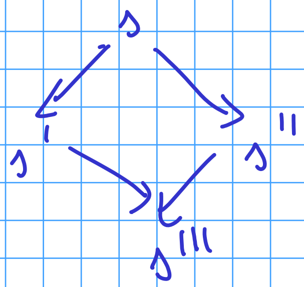
- *jest w postaci zredukowanej*
- *nie zależy od kolejności wykonania redukcji (utożsamiamy a^k z $(a^{-1})^{-k}$).*
- $a_1^{\ell_1} a_2^{\ell_2} \cdots a_k^{\ell_k} = a_{i_1}^{\ell'_1} a_{i_2}^{\ell'_2} \cdots a_{i_j}^{\ell'_j}$.

Ponadto, $a_{i_1}, a_{i_2}, \ldots, a_{i_j}$ jest podciągiem $a_1, a_2, \ldots, a_k$.

„nie zależy od kolejności redukcji"

- „się skończy" — maleje dł. $a_u^{l} \to 1$, $a_u^{l} a_{u'}^{l''} \to a_{u''}^{l''}$ (2 → 1)

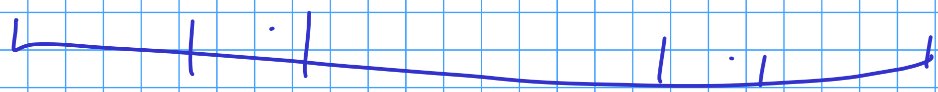
- konfluentny system przepisywania termów

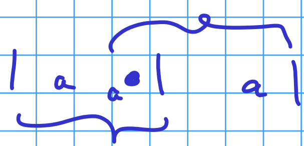


„Jeśli" $s \to s'$, $s \to s''$

$\exists s'''$: $s' \to s'''$, $s'' \to s'''$

- postać zredukowana jest jedyna





Lemat 14.25. *Dla zbioru generatorów X podgrupa $\langle X\rangle$ to dokładnie zbiór elementów postaci:*

$$\langle X\rangle = \{x_1^{z_1}x_2^{z_2}\cdots x_k^{z_k} \,:\, k\geq 0,\, x_1,\ldots,x_k\in X,\, z_1,\ldots,z_k\in\mathbb{Z}\}\ ,$$

bez zmniejszenia ogólności można dodatkowo założyć, że wszystkie elementy są w postaci zredukowanej.

14.7 Grupa cykliczna

Definicja 14.26 (Grupa cykliczna)**.** Grupa G jest *grupą cykliczną*, gdy $G=\langle\{a\}\rangle$ dla pewnego $a\in G$, tzn. jest generowana przez jeden element.

Uwaga. Grupa cykliczna nie musi być skończona: $\mathbb{Z}=\langle 1\rangle$. Dzieje się tak dlatego, że dla generatora dopuszczamy też ujemne potęgi.

Fakt 14.27. *Każda grupa cykliczna jest przemienna.*

$\langle g \rangle$ g^k

$g^k \cdot g^l = g \dots g \; g \dots g = g^{k+l} = g^l \cdot g^k$

Lemat 14.28. *Dla każdego $n < \infty$ wszystkie grupy cykliczne rzędu n są izomorficzne (z $(\mathbb{Z}_n, +)$). Wszystkie grupy cykliczne nieskończonego rzędu są izomorficzne (z $(\mathbb{Z}, +)$).*

$G \equiv H \equiv H' \Rightarrow G \equiv H'$

$\langle g \rangle \quad |G| = n \quad g^0, g^1, g^2, \ldots, g^{n-1}$

$\mathbb{Z}_n$

$0\ 1\ 2\ \ldots\ n-1$

$g^i \to i \in \mathbb{Z}_n$

zachowuje działanie

$g^i \cdot g^j = g^{i+j \bmod n}$

$i + j = i + j \bmod n$

$i + j > n$

$g^{i+j} \quad i+j > n$

$= g^{(i+j) \bmod n}$

$i+j = \not{0}\ \not{1}\ \not{2}\ \ldots\ \not{n}\ (i+j \bmod n)$

Lemat 14.29. *Podgrupa grupy cyklicznej jest cykliczna.*

14.8 Grupa wolna

Definicja 14.30 (Grupa wolna)**.** Niech $\Gamma^{-1} = \{a^{-1} : a \in \Gamma\}$ będzie rozłączne z Γ.

Grupa G o zbiorze generatorów Γ jest *wolna* (*wolnie generowana przez* Γ) jeśli dla dowolnego słowa $w \in (\Gamma \cup \Gamma^{-1})^*$ w postaci zredukowanej zachodzi

$$w =_G e \implies w = \varepsilon$$

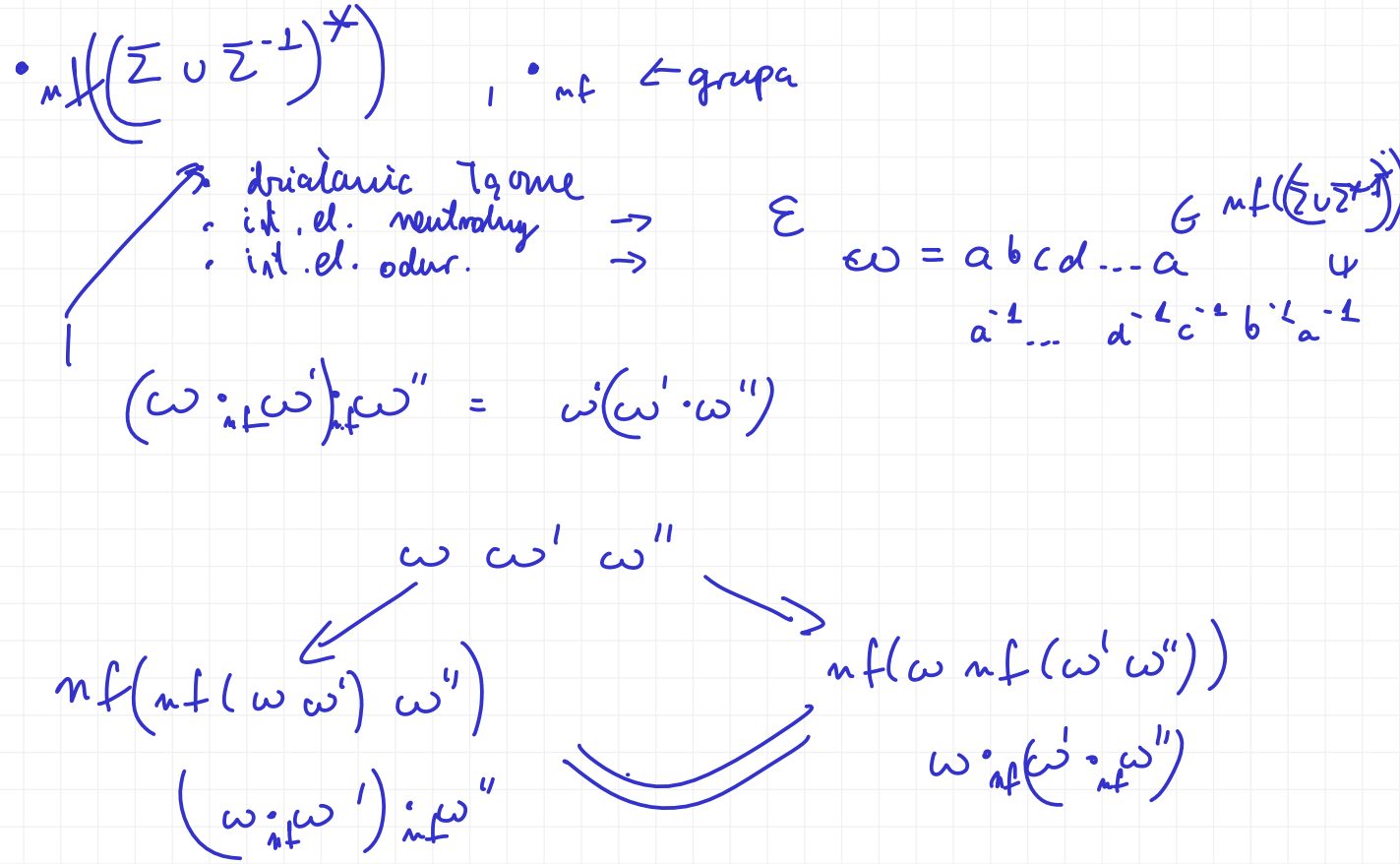
przy czym pierwsza równość oznacza równość w grupie, zaś druga równość słów w $(\Gamma \cup \Gamma^{-1})^*$.

Dla potrzeb tego rozdziału, poniżej $\mathrm{nf}(w)$ oznacza postać zredukowaną w.

Lemat 14.31 (Konstrukcja grupy wolnej)**.** *Niech Σ to zbiór różnych elementów (liter), $\Sigma^{-1} = \{a^{-1} : a \in \Sigma\}$ będzie rozłączny z Σ. Rozpatrzmy zbiór $\mathrm{nf}((\Sigma \cup \Sigma^{-1})^*)$ wszystkich słów zredukowanych z $(\Sigma \cup \Sigma^{-1})^*$. Mnożenie elementów $u \cdot w$ to postać zredukowana $\mathrm{nf}(uw)$ słowa uw.*

Tak zdefiniowana grupa jest grupą wolną (o generatorach Σ).

Każda grupa wolna jest izomorficzna z tak skonstruowaną grupą wolną.

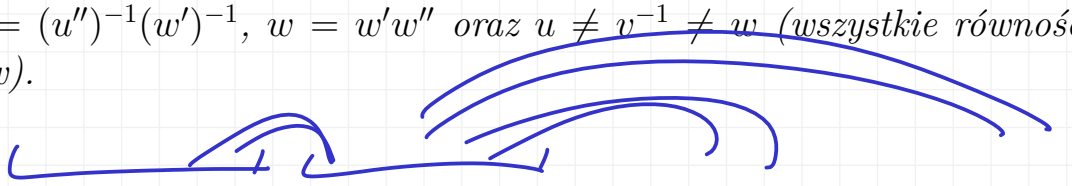


Twierdzenie 14.32 (Nielsen-Schreier). *Każda podgrupa grupy wolnej jest wolna.*

$H \leq G$ ← grupa wolna

$a b^3$ $b^{-1} a b^2$ $b^2 a$ $b^{-2} a^2 b$ wolna a, b

Lemat 14.33. *Niech $w_1, \dots, w_\ell \in (\Sigma \cup \Sigma^{-1})^*$ będą w postaci zredukowanej (jako słowa nad $\Sigma \cup \Sigma^{-1}$). Niech $w_1^{\ell_1} w_2^{\ell_2} \cdots w_n^{\ell_n}$ będzie w postaci zredukowanej oraz $\mathrm{nf}(w_1^{\ell_1} w_2^{\ell_2} \cdots w_n^{\ell_n}) = e$. Wtedy istnieją $u, v, w \in \{w_1, w_1^{-1}, \dots, w_\ell, w_\ell^{-1}\}$, takie że w uvw istnieje ciąg skróceń, który skraca całe v, tj. istnieją u', u'', w', w'' w postaci zredukowanej, takie że $u = u'u''$, $v = (u'')^{-1}(w')^{-1}$, $w = w'w''$ oraz $u \neq v^{-1} \neq w$ (wszystkie równości to równości słów).*

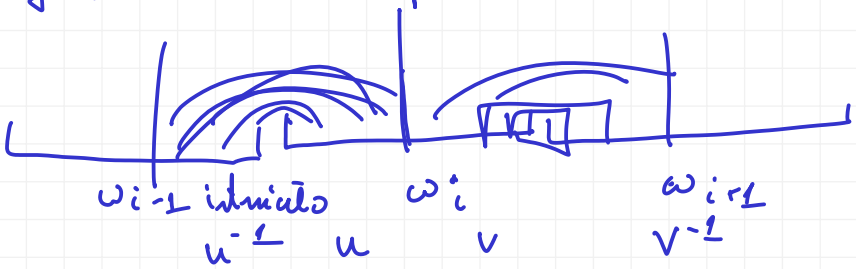


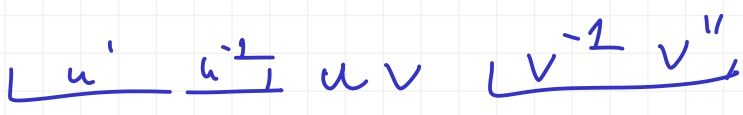
$w_{i-1} w_i w_{i+1}$

w_i skraca się w obrębie w_{i-1}, w_{i+1}

$w_1^{l_1} w_2^{l_2} \cdots w_n^{l_n}$

robimy skracanie krok po kroku, aż zniknie pierwsze w_i





$uv,\ v^{-1}v''$

$uv,\ uv''$

$|u| < |v|$

$|u| > |v|$

$u = v$

$u'\ u^{-1}$

$u'v$

Rozdział 15

Grupy permutacji

Definicja 15.1. Grupa permutacji S_n to zbiór wszystkich bijekcji ze zbior $\{1, 2, \ldots, n\}$ w siebie; operacją jest składanie funkcji, tj.

$$(\sigma' \cdot \sigma)(i) = \sigma'(\sigma(i)).$$

Permutacje zapisujemy jako dwuwierszową tabelkę:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

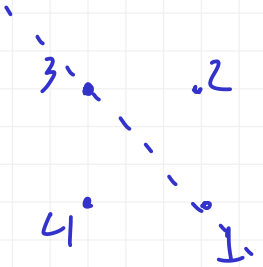
Przykład 15.2. Permutacje S_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Z takiej reprezentacji łatwo wyliczyć permutację odwrotną: wystarczy zamienić miejscami i przesortować kolumny.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$



Obroty i sym. hw.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Z dokładnością do izomorfizmu każda grupa jest grupą permutacji.

Twierdzenie 15.3 (Cayley). *Dla każdej grupy G (o n elementach) istnieje podgrupa S_n izomorficzna z G.*

$G \cong H \leq S_{|G|}$

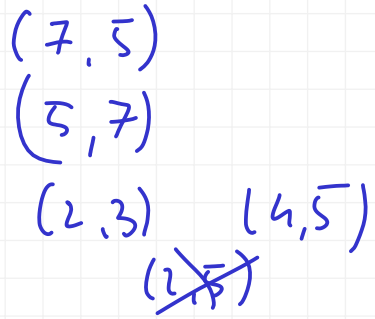
15.1 Rozkład permutacji na cykle

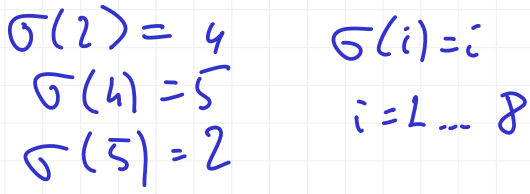
Definicja 15.4 (cykl). *Cykl* σ to taka permutacja, że istnieją elementy $a_1, \ldots, a_n$, że $\sigma(a_i) = a_{i+1}$ (gdzie $\sigma(a_n) = a_1$) a na innych elementach jest identycznością. Cykl taki zapisujemy jako $(a_1, a_2, \ldots, a_n)$. Elementy $\{a_1, \ldots, a_n\}$ to *dziedzina cyklu* lub *nośnik cyklu*, mówimy też o cyklu *na elementach* $\{a_1, \ldots, a_n\}$.

Długość cyklu $(a_1, \ldots, a_n)$ to n.

Cykle są *rozłączne*, gdy ich nośniki nie mają takich wspólnego elementu.

Transpozycja to cykl dwuelementowy. *Transpozycja elementów sąsiednich* to transpozycja postaci $(i, i+1)$.





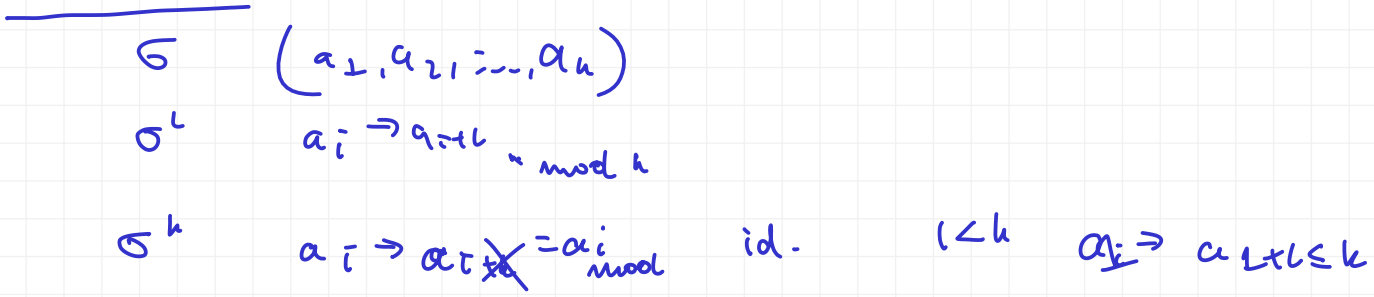
Lemat 15.5. *1. Rząd cyklu długości k to k.*

2. *Dla cyklu $(a_1, \ldots, a_n)$ permutacja odwrotna to $(a_1, \ldots, a_n)^{-1} = (a_n, a_{n-1}, \ldots, a_2, a_1) = (a_1, \ldots, a_n)^{n-1}$.*

3. *Jeśli $\{c_i\}_{i=1}^k$ są parami rozłącznymi cyklami, to $c_{i_1} c_{i_2} \cdots c_{i_k}$ jest tą samą permutacją, niezależnie od wyboru permutacji $i_1, \ldots, i_k$ liczb $1, \ldots, k$.*

4. *Jeśli $\{c_i\}_{i=1}^k$ są parami rozłącznymi cyklami, to rząd $c_1 \cdots c_k$ to* nww *rzędów poszczególnych cykli $c_1, \ldots, c_k$.*

5. *Jeśli $\sigma = c_1 c_2 \cdots c_k$, gdzie $c_1, \ldots, c_k$ są parami rozłącznymi cyklami , to $\sigma^{-1} = c_1^{-1} c_2^{-1} \cdots c_k^{-1}$.*



$c_1, c_2, \dots, c_l$ ← parami rozł.

$c_{i_1} \dots c_{i_l}(n)$ ← ta sama perm.

r $c(n)$

$c_{i_1} \dots c_{i_r} n'$

n'

2) $c_1, \dots, c_n$ ← cykle rozł

$$\mathrm{rk}(c_1 \cdot \dots \cdot c_n) = \mathrm{NWW}(\mathrm{rk}(c_1), \dots, \mathrm{rk}(c_n))$$

$$(c_1 \dots c_n)^l = (c_1 c_2 \dots c_n)(c_1 c_2 \dots c_n) \dots (c_1 \dots c_n)$$

$$\| \quad \underbrace{\quad c_1 \quad}\,\underbrace{\quad c_2 \quad}\,\underbrace{\quad c_3 \quad}\,\dots\,\underbrace{\quad c_n \quad}$$

$$c_1^l c_2^l \dots c_n^l$$

$l \leftarrow \mathrm{NWW}(\mathrm{rk}(c_1), \dots, \mathrm{rk}(c_n))$

$c_1^l \dots c_n^l = id$

$l' < l$ to l' nie jest wtedy $\mathrm{rk}(c_i)$

$c_i^{l'} \neq e$

$c_i^{l'}(n) = n' \neq n$

To nie jest identyczność

$(c_1 c_2 \dots c_n)^{-1}$

$c_1 \dots c_n c_n^{-1} c_{n-1}^{-1} \dots c_1^{-1} = e$

$c_1^{-1} c_2^{-1} \dots c_n^{-1}$

Twierdzenie 15.6. *1. Każda permutacja σ jednoznacznie (z dokładnością do kolejności cykli) rozkłada się na rozłączne cykle.*

- *2. Cykl długości k jest złożeniem $k-1$ transpozycji.*

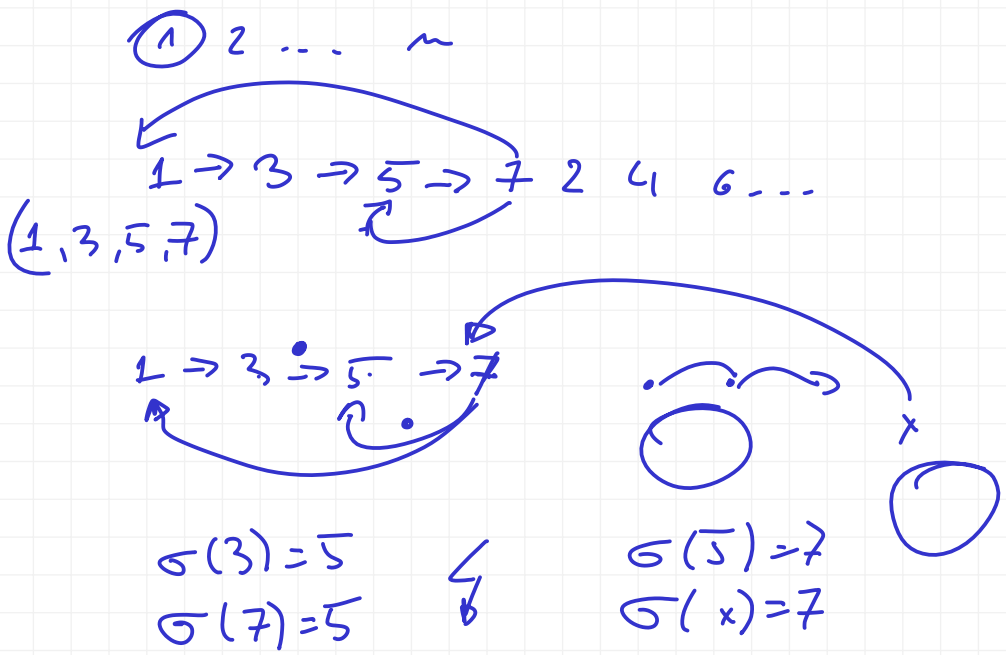
3. Każda transpozycja jest złożeniem nieparzystej liczby transpozycji elementów sąsiednich (niekoniecznie rozłącznych).

4. Każda permutacja da się przedstawić jako złożenie transpozycji (niekoniecznie rozłącznych).

5. Każda permutacja da się przedstawić jako złożenie transpozycji sąsiednich (niekoniecznie rozłącznych).

6. Grupa S_n jest generowana przez zbiór transpozycji (sąsiednich).

Ad 1



σ

$5 \to \sigma(5)$

$(i, \ldots, j)$ cykl dł. k to złożenie $(k-1)$ transpozycji

(1) lub $(i, i+1)$ 1

$(i, \ldots, j) = (i, i+1)(i+1, \ldots, j)$

$(i+1, \dots, j)(k) = k+1 \qquad (k \neq i,\ k \neq j)$

$(i, i+1)(k+1) = k+1$

$k+1 \notin \{i; i+1\}$

$(i+1, \dots, j)(i) = i \qquad (i, i+1)\, i = i+1$ ✓

$(i+1, \dots, j)(j) = i+1 \qquad (i, i+1)(i+1) = i$

tr. reciproc

$(i, j) = (i+1 \dots j)^{-1} (i \dots j)$

$j \to i$

$i \to i+1 \to j$