Historia, definicja grupy, rząd, potęga, rachunki, tabelki, przykłady, liczbowe, cykliczne, dihedralne, grupy permutacji warstwy, Lagrange,

Wykład 2 (cd)

Def. $H \leqslant G$ **podgrupa normalna**, jeśli $(\forall g \in G)\ \ gH = Hg$ piszemy $H \lhd G$ lub $H \trianglelefteq G$

Stw. $|G : H| = 2$, to $H \lhd G$

Ex. $A_n \lhd S_n$

Twierdzenie. $H \lhd G \iff g^{-1}Hg = H$ (dla każdego $g \in G$)
$\iff g^{-1}Hg \subseteq H$ (dla każdego $g \in G$)

Twierdzenie. Zbiór warstw G/H z działaniem $Ha \cdot Hb = H(ab)$ tworzy grupę zwaną **grupą ilorazową**.

Uwaga: poprawność definicji działania!

Def. $(G, \circ), (H, *)$ grupy, wtedy $f : G \to H$ nazywamy **homomorfizmem**, jeśli $f(a \circ b) = f(a) * f(b)$
dla wszystkich $a, b \in G$.
*Gdy oba działania oznaczymy znakiem mnożenia, to warunek ma postać: $f(a \cdot b) = f(a) \cdot f(b)$.

Stw. Homomorfizm zachowuje e oraz a^{-1}.

Def. Jądro Ker$f$, Obraz Imf, mono, epi, izo.

Stw. Ker$f \lhd G$

Stw. Obraz homomorficzny podgrupy (normalnej) jest podgrupą (normalną)

Stw. Przeciwobraz homom. podgrupy (normalnej) jest podgrupą (normalną)

Twierdzenie. Odwzorowanie $\kappa : G \to G/H : g \to Hg$ jest epimorfizmem, i zwane jest **epimorfizmem kanonicznym**.

Wn. Jądra $\longleftrightarrow$ podgrupy normalne

Wykład 3

Twierdzenie. (**o izomorfizmie**) Dla każdego homomorfizmu $f : G \to H$ istnieje dokładnie jeden izomorfizm $\phi : G/\mathrm{Ker}f \to \mathrm{Im}f$, taki że $f = \kappa \circ \phi$.

Wn. Wszystkie homomorfizmy wyznaczone są (z dokładnością do *izo*) przez epimorfizmy kanoniczne.

Wn. obrazy homomorficzne są izomorficzne z grupami ilorazowymi

Ex. $f : S_n \to C_2 = \{-1, 1\}$ parzystość

Ex. $\phi : \mathbb{Z} \to \mathbb{Z}_n$ reszta modulo n

Ex. $h : GL_n(\mathbb{R}) \to \mathbb{R}^* : M \to \det(M)$ (hom: Tw. Cauchy'ego)

*macierze nieosobliwe nad dowolnym ciałem $GL_n(K)$

Komutant grupy

Def. **Komutator** $[x, y] = x^{-1}y^{-1}xy$

Def. **Komutant** $[G, G] = \langle [x, y] : x, y \in G \rangle$ grupa generowana przez komut~~anty~~ ory

Stw. $[G, G] = \{[x_1, y_1][x_2, y_2] \dots [x_k, y_k] : x_i, y_i \in G, k \in \mathbb{N}\}$

Twierdzenie. $[G, G]$ jest podgrupą normalną G: $[G, G] \trianglelefteq G$

Centrum grupy

Def. $Z(G) = \{g \in G : (\forall x \in G)\ gx = xg\}$ **centrum grupy** G

Twierdzenie. $Z(G)$ jest podgrupą normalną G: $Z(G) \trianglelefteq G$

Klasyfikacja grup abelowych

Def. **Iloczynem prostym** grup G_1, G_2 nazywamy grupę na zbiorze $G_1 \times G_2$ z działaniem określonym "po osiach": $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$ (sprawdzić, że grupa)

Stw.. Iloczyn prosty grup abelowych jest grupą abelową.

W przypadku zapisu addytywnego mówimy o **sumie prostej** i używamy zapisu $G_1 \oplus G_2$.

Twierdzenie. $A, B \leqslant G$ abelowa, $A \cap B = \{0\} \implies \langle A \cup B \rangle \cong A \oplus B$.

* Uogólnienia: więcej składników, nieabelowe $A, B \triangleleft G$

Twierdzenie. Abelowa $|G| = mn$, $(m, n) = 1 \implies$ ist. $G_1, G_2 \leqslant G$ takie, że $G \cong G_1 \oplus G_2$, $|G_1| = m$, $|G_2| = n$.

Ex. $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$

Wykład 4 (*dodatkowy termin ???) czwartek.

ab

$p \mid |G| \Rightarrow \exists$ el $x \in G$ rzędu p.

Wn. abelowa $|G| = p_1^{k_1} \ldots p_m^{k_m}$ (p_i rożne liczby pierwsze), G rozkłada się na sumę prostą swoich podgrup $G \cong G_1 \oplus \ldots \oplus G_m$, gdzie $|G_i| = p_i^{k_i}$ (*p-grupy – definicja).

abelowa p-grupa, $|G| = p^k$??? $\mathbb{Z}_{p^k}$ $\quad \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{k}$ $(x_1, x_2, \ldots)$

Twierdzenie. abelowa $|G| = p^k$, $a \in G$ najwyższego rzędu $\implies$ $G \cong \langle a \rangle \oplus T$ dla pewnej $T \leqslant G$.
(*dowód indukcyjny pomijamy*).

$k = k_1 + k_2 + \ldots + k_s$

$\Downarrow$

Twierdzenie. Każda skończona grupa abelowa jest sumą prostą grup cyklicznych.

$\Downarrow$ (jednoznaczność?)

Ex. Grupy abelowe rzędu 16 ??? $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Działania grup na zbiorach

g-ust.

$\varphi_g(x) = g\cdot x$

$\varphi_g(x) = \varphi_g(y)$ 1-1

$g^{-1})\ g\cdot x = g\cdot y$

$x = y$

$\varphi_g(x) \stackrel{?}{=} y \in X$ na

$g\cdot x = y \quad x = g^{-1}\cdot y$

Def. Grupa G **działa** na zbiorze X, jeśli istnieje funkcja $\cdot : G \times X \to X$ spełniająca:

(1) $g \cdot (h \cdot x) = (gh) \cdot x$ dla wszystkich $g, h \in G, x \in X$,

(2) $e \cdot x = x$ dla wszystkich $x \in X$.

to jest równoważne (Stw):

Def 2. Istnieje homomorfizm $\phi : G \to Sym(X) : g \to \phi_g$

Dowód: $f(x\cdot y) = f(x)\cdot f(y)$

$\varphi(x\cdot y) = \varphi_x \circ \varphi_y \qquad (\varphi_x \circ \varphi_y)(z) = \varphi_x(\varphi_y(z)) = \varphi_x(y\cdot z) =$

$x\cdot y\cdot z$

L= $\varphi(x\cdot y) = \varphi_{x\cdot y}$

$\varphi_{x\cdot y}(z) = (x\cdot y)\cdot z = xyz.$

Def. Jeśli ϕ jest mono (1-1), to działanie **wierne** (*reprezentacja G jako grupy permutacji*)

X = zb. p. sześcianu

Uwaga: Oznaczenia multiplikatywne

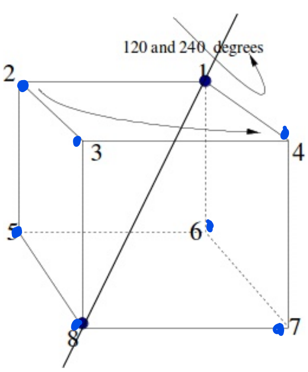
$X = \{1, 2, 3, 4, 5, 6\}$

Ex. Działanie C_3 na sześcian (obroty wokół przekątnej)

$C_3 = \{id, o120°, o240°\}$

(375)(246)

(357)(264)



$(1)\ (gh)\cdot x = ghx = g(hx)$

$gx = hx \mid x^{-1}$

$g = h$

Ex2. Działanie G na siebie ($X = G$) poprzez (lewe) translacje $\underbrace{g \cdot x}_{\varphi_g(x)} \stackrel{\text{def}}{=} gx$ (jest wierne).

$\varphi : G \to \cancel{G}\ \mathrm{Sym}(G) : g \to \varphi_g$

$\Downarrow$

Twierdzenie (Cayley'a) Każda grupa jest izomorficzna z pewną grupą permutacji. ($\leq \mathrm{Sym}(X)$)

po

$z = g\cdot x$

$g^{-1}z = x$

Def. W działaniu grupy G dla dowolnego elementu $x \in G$ definiujemy:

$\mathrm{Stab}(x) = \{g \in G : \ g \cdot x = x\}$ (**stabilizator** x)

$\mathrm{Orb}(x) = \{z \in X : \ z = g \cdot x, \ g \in G\}$ (**orbita** x)

podział X na orbity.

Stw. 1 Stab(x) jest podgrupą G .

$\to g_1, g_2 \in \mathrm{Stab}(x) \quad (g_1 g_2)\cdot x = g_1(g_2 x) = g_1\cdot x = x \Rightarrow g_1 g_2 \in \mathrm{Stab}(x)$

$\to g \in \mathrm{Stab}(x),\ g^{-1} \quad x = g^{-1}\cdot g\ (x) = g^{-1}(gx) = g^{-1}\cdot x$

$gh^{-1} \in G$

#warstw, $H = \mathrm{Stab}(x)$

Stw. 2 $|G : \mathrm{Stab}(x)| = |\mathrm{Orb}(x)|$.

D-d φ : zb.warstw $\to \mathrm{Orb}(x) : gH \to g\cdot x$

popr.def. (nie zależy od wyboru g) $\quad gH = g'H,\ g' = gh$

$gx \stackrel{?}{=} g'x \mid g'x = g\cdot \underset{\text{stab}}{h}\cdot x = g(hx) = gx$

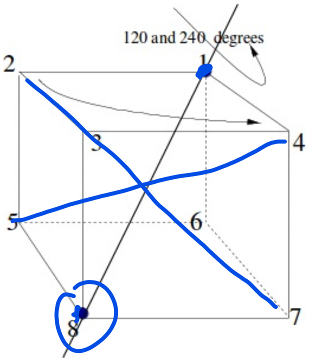
na-oczyw. 1-1 $\quad g\cdot H, g'H \wedge g\cdot x = g'x \Rightarrow gH \stackrel{?}{=} g'H$ stab

$\Rightarrow x = g^{-1}\cdot g'\cdot(x) \Rightarrow g^{-1}g' \in H$

$g^{-1}g' = h \quad g' \in gH$

Twierdzenie. $|G| = |\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)|$

Ex. Grupa obrotów sześcianu $|G| = ?$



$X = 8$

$|G| = |\mathrm{Stab}(8)| \cdot |\mathrm{Orb}(8)| =$

$= 3 \cdot 8 = \underline{\underline{24}}$

$G \leq S_8$

G działa na $\underline{X = \{\{1,8\},\{2,7\},\{5,4\},\{3,6\}\}}$

$\underbrace{G}_{24} \to \underbrace{S_4}_{24}$: $\Rightarrow G \cong \underline{S_4}$.

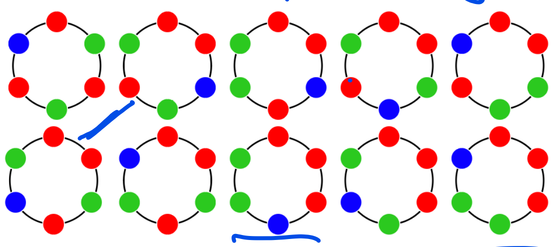
Twierdzenie (**Burnside'a**). Dla skończonej grupy G działającej na skończonym zbiorze X: Średnia ilość punktów stałych w permutacjach generowanych przez $g \in G$ równa jest ilości orbit w tym działaniu:

$$\#\mathrm{Orb} = \frac{1}{|G|} \sum_{g \in G} \underline{\mathrm{fix}(g)}$$

Zastosowania w kombinatoryce

$|X| = 60$

$6 \cdot \binom{5}{2} = 6 \cdot 10 = 60$



D_6

dihedralna

Ex. Ile jest różnych układów naszyjników złożonych z 6 koralików, każdy w jednym z trzech możliwych kolorów?

15

Grupa D_{15} — 15 obr, 15 odbić

orbit na zb $\boxed{3^{15}}$

3^{15}

$$\#\text{orb} = \frac{1}{|G|}\sum_{g\in G} \text{fix}(g) \to (\ )(\ )(\ )\ldots(\ )$$

odb $(2\,14)(3\,13)\ldots(\ )$ — 15

obr $(1\,2\,3\ldots 14)$ — 9

$(1\,4\,7\,10\,13)(2\ldots)(3\ldots)$ — 4

$(1\,6\,11)(\ )\ldots$ — 2

$$\frac{1}{30}\left(15\times 3^7 + 9\times 3^1 + 4\times 3^4 + 2\times 3^5\right)$$

Zastosowania działań grup w teorii grup

Grupa G działa na siebie przez sprzężenie: $g \cdot x \stackrel{\text{def}}{=} gxg^{-1}$

(moce orbit, stab=cent, wzór klas)

$|G| = |Z(G)| + \dfrac{|G|}{|C(x_1)|} + \ldots + \dfrac{|G|}{|C(x_r)|}$, gdzie $|C(x_i)| < |G|$ (wzór klas)

$\Downarrow$

Twierdzenie (**Sylowa**) $|G| = p^n m$, $n, m \geqslant 1$, p liczba pierwsza nie dzieląca m, wtedy G ma podgrupę P rzędu p^n (*p-podgrupy Sylowa*).

Podobnie:

- $\square$ G ma podgrupę rzędu p^i dla dowolnego $i \leqslant n$;
- $\square$ G ma element rzędu p (Tw. Cauchy'ego);
- $\square$ $|G| = p^n$ (p-grupa), to $p|Z(G)$;
- $\square$ $|G| = p^2$, to G abelowa.

TWIERDZENIE (**Sylowa**) (cd.)

(ii) Wszystkie p-podgrupy Sylowa są sprzężone ($P = gQg^{-1}$);

(iii) Liczba p-podgrup Sylowa N_p dzieli $|G|$ i $N_p \equiv 1 \pmod p$.

Def. **Grupa prosta** – nie ma nietrywialnych podgrup normalnych.

Twierdzenie. Wszystkie grupy A_n są proste dla $n \geqslant 5$.

TWIERDZENIE. **Klasyfikacja skończonych grup prostych**

- cykliczne C_p,
- alternujące A_n, $n \geqslant 5$,
- 16 nieskończonych rodzin grup typu Liego (w tym tzw. klasyczne: specjalne liniowe, projektywne, ortogonalne, symplektyczne, unitarne)
- 26 grup sporadycznych (od Mathieu groups $M_{11}, M_{12}, \ldots$ po tzw. „Monster group")

Dowód około: 10 000 stron, 500 artykułów, 100 autorów
w latach 1955-2004

1983 Gorenstein - szkic dowodu 2 tomy

2004 Aschenbacher - uzupełnienie 3 tom

dowody 2-giej i 3-ciej generacji

Historia: odkrywania grup (Mathieu 1861, k-tranzytywność),. . . ,
Monster – 1973 rzędu $\approx 8 \cdot 10^{53}$.

==

Grupy rozwiązalne

DEF. G **grupa rozwiązalna** – posiada „wieżę abelową", tzn.
ma podgrupy takie, że $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{e\}$ oraz G_i/G_{i+1} abelowe.
(„zbudowana z grup abelowych")