Teoria ciała stałego
Cz. I

1. Elementy teorii grup

Grupy symetrii

def. Grupy

Zbiór (skończony lub nieskończony) elementów {g} tworzy grupę gdy:
- zdefiniowana operacja mnożenia (złożenia) $g_1g_2 = g_3 \in G$
- $(g_1g_2)g_3 = g_1(g_2g_3)$
- istnieje tylko jeden element tożsamościowy e, $eg = ge = g$
- każdy g posiada element odwrotny g^{-1} , $gg^{-1} = e$

grupy abelowe: $g_1g_2 = g_2g_1$ lub inaczej $[g_1 , g_2] = 0$

przykłady podstawowe

- **zbiór liczb [0,1] z dodawaniem zdef. jako**

  0+0->0
  0+1->1
  1+1->0

  tu e = 0 , 1 – jest odwrotnością dla siebie

zauważmy, że 0 i 1 możemy zastąpić dowolnymi symbolami
w szczególności zbiór [1, -1] ze zwykłym mnożeniem tworzy taką samą grupę (nierozróżnialną jeśli dodawanie zastąpimy mnożeniem)

- **zbiór [0,1] z mnożeniem – jako składaniem**
  nie jest grupą, gdyż nie istnieje element odwrotny do 0

ale samo „0” lub sama”1” z mnożeniem tworzą grupy jednoelementowe

- **grupa macierzy kwadratowych A o elementach rzeczywistych, rzędu *n* o det|A| ≠ 0, ze zwykłym mnożeniem macierzy** ***(nieskończona)***

- **zbiór {1,-1,i,-i} z mnożeniem**

ilość elementów, m = *rząd grupy*

Własności grup

g^n = ggg...g - n razy

dla grup skończonych, tworząc ciąg e, g, g^2, g^3, ...,g^n, ... pierwszym powtarzającym się elementem grupy będzie $e = g^m$

m – rząd elementu g (np. g^3 = ggg)

ciąg (zbiór) e, g, g^2, g^3, ...,g^{m-1} - nazywa się *okresem* elementu g

- **Okres elementu g tworzy *grupę cykliczną* (def.)**

- **Podzbiór G , będący grupą nazywa się *podgrupą***

- **Grupa *abelowa* : gh = hg (dla każdych h i g), ozn. [h,g]=0**

Warstwa:
Jesli H jest podgrupą G, to dla g ∈ G i g nie należącego do H, zbiór wszystkich hg lub gh (h ∈ H) tworzy warstwę Hg lub gH.

jest oczywiste, że żaden element warstwy nie należy do H, bo wówczas i g należałby do H – sprzeczność z założeniem **- dowód na ćwiczeniach.**

Tw. (Lagrange'a)
Rząd podgrupy jest dzielnikiem rzędu grupy

rząd G / rząd H = indeks podgrupy

inaczej:
liczba elementów w grupie jest wielokrotnością liczby elementów w podgrupie

dowód: **(na ćwiczenia)**

niech H będzie podgrupą G i niech $g \in G$,
biorąc g_2 nie należący ani do H ani do Hg, to wszystkie hg_2 są poza H i poza Hg,

(jeśli jakiś h_2g_2 należałby do Hg i byłby np. równy h_1g , to $h_2g_2 = h_1g$, a to oznacza, że $g_2=h_2^{-1}h_1g$, ale $h_2^{-1}h_1 \in H$, g_2 musiałby należeć do warstwy Hg – sprzeczność...)
zatem, ani H, ani Hg, ani Hg_2 nie mają wspólnych elementów;
powtarzając to aż wyczerpiemy wszystkie elementy G dostajemy podział G na rozłączne fragmenty

H, Hg, Hg_2, Hg_3, ..., Hg_{l-1} , l – liczba całkowita

ale każda warstwa ma tyle elementów ile wynosi rząd H (s), zatem

$$m = l\,s$$

(m – rząd G)

jeśli rząd grupy jest liczbą pierwszą to grupa nie ma podgrup

(za wyjątkiem podgrup *trywialnych*: e i G)

<u>def.</u>

g_1 i g_2 nazywają się sprzężonymi (równoważnymi) gdy istnieje taki $x \in G$, że

$$xg_1x^{-1} = g_2$$

sprzężenie (relacja równoważności) jest:
a) symetryczne (zwrotne**)**
b) przechodnie

elementy wzajemnie sprzężone tworzą <u>klasy</u>

(sprzęgający element x może być różny dla różnych par elementów)

każdy element grupy może należeć tylko do jednej klasy

niech liczba elementów w klasie = h_r ,
są to elementy gg_1g^{-1} dla ustalonego g_1 , nie wszystkie różne;

to każdy element klasy występuje w tak wygenerowanym zbiorze gg_1g^{-1} tę samą ilość razy:

$$h/h_r$$

(gdzie h=m)
(bez dowodu)

w grupach abelowych każda klasa składa się z jednego elementu

gdyż $xgx^{-1} = g$, **dla każdego x**

klasy (za wyjątkiem e) nie są podgrupami

def.
Podgrupa niezmiennicza lub *dzielnik normalny* grupy, to podgrupa R składająca się z pełnych klas grupy G

def.
Każda warstwa Rg stanowi element nowej grupy, zwanej *grupą ilorazową*
z mnożeniem zdefiniowanym jako $Rg_1 * Rg_2 = R(g_1g_2)$
(podgrupa R = Re stanowi element tożsamościowy grupy ilorazowej)

Izomorfizm

Dwie grupy G i H jednakowego rzędu są izomorficzne jeśli pomiędzy elementami tych grup istnieje wzajemnie jednoznaczne przyporządkowanie, takie, że

jeśli $g_1 \leftrightarrow h_1$ **i** $g_2 \leftrightarrow h_2 \Rightarrow g_1g_2 \leftrightarrow h_1h_2$.

Elementowi e odpowiada e, g^{-1} **odpowiada** h^{-1}

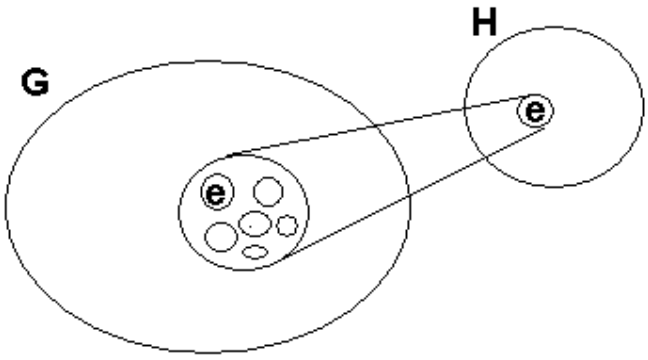
Homomorfizm

Grupa G jest *homomorficzna* do grupy H gdy każdemu elementowi G przyporządkowany jest jednoznacznie element

grupy H, ale jednemu elementowi z H może odpowiadać więcej niż jeden element z G

Homomorfizm nie jest symetryczny

Jądro homomorfizmu **J – te elementy w G, które odpowiadają elementowi e w H.**



Tw.
Jądro homomorfizmu jest *niezmienniczą podgrupą* grupy G

jądro: $e, e_1, e_2, e_3, ..., e_n$

dowód:
- oczywiście jądro jest grupą gdyż $e_i e_j$ też należy do jądra (w H: ee=e)

- dla $e_i \in J$, i $g \in G$, ge_ig^{-1} też należy do grupy, bo jeśli $g \leftrightarrow f$ to w H, $fef^{-1} = e$ (e - jest przemienny z każdym elementem z definicji) – zatem klasa każdego elementu e_i też należy do tej podgrupy.

---

zobaczmy czym jest w G zbór elementów, którym w H odpowiada f ,

niech g będzie jednym z takich elementów w G;
oczywiście cała warstwa podgrupy J tego elementu g (Jg) też odpowiada elementowi f (gdyż ef = f);

weźmy element g_1 (różny od g) ale też taki, że w H odpowiada mu f;
rozważmy $g_1 g^{-1}$, w H odpowiada mu $f f^{-1} = e$,
oznacza to, że $g_1 g^{-1} \in J$, a to oznacza
(*mnożąc obie strony przez g*) że $g_1 \in Jg$,
zatem liczba elementów, które w G odpowiadają f jest równa n – rzędowi J i wszystkie one tworzą warstwę.

Takie warstwy całkowicie wyczerpują G.

Pomiędzy elementami grupy H (homomorficznej do G) a warstwami w G (ze wzgl. na niezmienniczą podgrupę J), istnieje izomorfizm

Tzn. H jest izomorficzna z grupą ilorazową G

Podgrupa H, grupy G, nazywa się *centrum grupy G*, lub *abelowym dzielnikiem normalnym G*, gdy dla każdego $g \in G$ i $f \in H$ zachodzi $[f,g] = 0$

Iloczyn prosty grup

Jeśli $f \in H$ i $g \in G$, to pary elementów (f, g) tworzą nową grupę B z prawem mnożenia

$$(f_1 , g_1) (f_2 , g_2) = (f_1 f_2 , g_1 g_2)$$

$$B = H \times G$$

Liczba elementów w B – iloczyn liczb elementów

Liczba klas w B – iloczyn liczb klas H i G

Jeśli część wspólna H i G to tylko e i dla każdych g,h zachodzi $[h,g]=0$ => B można uważać za grupę o elementach fg

***Elementy tworzące grup skończonych*, a,b,c,...**

mówimy o nich
jeśli każdy element G można przedstawić w postaci iloczynu potęg tych elementów

relacje definiujące

$$a^p\, b^q\, c^r \ldots = e$$

zadanie elementów tworzących oraz relacji definiujących całkowicie określa grupę