Algebra 1R

by a moron :3

21.03.2137

1 Teoria grup

1.1 Grupy, pierscienie, ciala

Dzialanie na zbiorze X:

$$\Phi : X \times X \to X,$$

zwykle zapisywane jako xy, $x \cdot y$, $x + y$.

Element neutralny – takie e, ze dla kazdego $x \in X$ ex = xe = x. Dzialanie ma co najwyzej jeden element neutralny.

Element odwrotny do x to takie y, ze xy = yx = e. Jesli dzialanie jest laczne, to ma co najwyzej jeden element odwrotny do danego x.

Homomorfizm algebry $\mathscr{X} = (X, \{\cdot\})$ na algebre $\mathscr{Y} = (Y, \{\circ\})$ nazywamy przeksztalcenie $f : X \to Y$ spelniajace dla kazdego $a, b \in X$

$$f(a \cdot b) = f(a) \circ f(b).$$

- monomorfizm – f jest 1-1
- epimorfizm – f jest "na"
- izomorfizm – f jest 1-1 i "na"
- endomorfizm – kiedy $\mathscr{Y} = \mathscr{X}$
- automorfizm – enodmorfizm bedacy izomorfizmem

Polgrupa to niepusty zbior z dzialaniem lacznym.

GRUPA to niepusty zbior z lacznym dzialaniem i elementem neutralnym (zwanym jednoscia grupy) oraz elementami odwrotnymi dla kazdego elementu.

$\hookrightarrow$ grupa abelowa (przemienna) – grupa z dzialaniem przemiennym

Zbior G z dzialaniem $\cdot$ jest grupa, jesli:

1. $(\forall\, a, b, c \in G)\ (ab)c = a(bc)$
2. $(\exists\, e \in G)(\forall\, a \in G)\ ea = ae = e$
3. $(\forall\, a \in G)(\exists\, b \in G)\ ab = ba = e$

*4. $(\forall\, a, b \in G)\ ab = ba$ w grupie *abelowej*

PIERSCIEN to niepusty zbior X z dwoma dzialaniami ($\cdot$, +, mnozenie i dodawanie) taki, ze:

1. zbior X z + jest grupa abelowa
2. $\cdot$ jest laczne
3. $(\forall\, x, y, z \in X)\ x \cdot (y + z) = x \cdot y + x \cdot z \wedge (x + y) \cdot z = x \cdot z + y \cdot z$

Kolejne dzikie nazwy $\star$:

$\star$ pierscien przemienny – jesli mnozenia jest przemienne

$\star$ pierscien z jednoscia – dla mnozenia istnieje element neutralny

CIALO to pierscien przemienny, ktory dla kazdego elementu $\neq 0$ ma element odwrotny

1.2 Wlasnosci

Niech G bedzie grupa, a e jej elementem neutralnym. Wowczas:

$\hookrightarrow$ $a, b \in G \implies (ab)^{-1} = b^{-1}a^{-1}$

$\hookrightarrow$ $a \in G$ i $n = 1, \ldots, n$ $a^{-n} = (a^n)^{-1} =^* (a^{-1})^n$

$\hookrightarrow$ dla $m, n \in \mathbb{Z}$ i $a \in G$ mamy $a^{mn} =^* (a^m)^n$

$\hookrightarrow$ dla G grupy abelowej i $n \in \mathbb{Z}$ $(ab)^n =^* a^n b^n$

* trzeba udowodnic, ale mi sie nie chce

$H \subseteq G$ jest podgrupa G, jesli jest grupa ze wzgledu na te same dzialania, czyli wystarczy, ze

$$(\forall\, a, b \in H)\ ab^{-1} \in H.$$

Jelsi $a \in G$ i istnieja $n \in \mathbb{N}$, $n \geq 1$, takie, ze $a^n = e$, to mowimy ze n jest rzedem elementu a ($n = o(a)$). Jesli takie n nie istnieja, to a ma rzad nieskonczony ($o(a) = \infty$).

$\hookrightarrow$ grupa torsyjna – wszystkie elementy maja rzad skonczony

$\hookrightarrow$ grupa beztorsyjna – wszystkie elementy maja rzad nieskonczony

Jesli $o(a) = n$ *oraz* $a^N = e$ *to* $n | N$, *fajny dowodzik, ale leniem jestem*

Grupa cykliczna to grupa zlozona z wszystkich poteg danego elementu a, natomiast a jest nazywane generatorem tej grupy

1.3 Permutacje :>

n-ta grupa symetryczna [S_n] - grupa wszystkich permutacji zbioru $X_n = \{1, \dots, n\}$. $|S_n| = n!$

Jesli $P \in S_n$ i dla $i = 1, \dots, n$ $P(i) = a_i$, to piszemy

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

Mnozenie permutacji:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} c_1 & c_2 & \dots & c_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} =$$

$$= \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

Zbior elementow niezmienniczych (fixpunktow) permutacji P to zbior $F(P) = \{k \in X_n : P(k) = k\}$. Jego dopelnienie oznaczamy $M(P) = S_n \setminus F(P)$.

Cykl k-elementowy C to permutacja taka, ze $C(a_1) = a_2$, $C(a_2) = a_3$, ..., $C(a_n) = a_1$. Cykl 2-elementowy to transpozycja. Cykle zapisujemy

$$(a_1, a_2, \dots, a_n)$$

Kazda permutacja jest iloczynem transpozycji.

Permutacje parzyste - iloczyn

$$\prod_{i<j}(a_j - a_i)$$

jest dodatni (gorny row to kolejne liczby naturalne, dolny to wyrazy). Pozostale permutacje sa nieparzyste.

Znak permutacji jest +1 gdzy permutacja jest parzysta i -1 wpp. Alternatywnie mozna zapisac (gorny row to b_k, a dolny to c_k)

$$\operatorname{sgn} P = \prod_{i<j}\frac{b_j - b_i}{c_j - c_i}$$

Dla dwoch dowolnych permutacji P_1, P_2 mamy

$$\operatorname{sgn} P_1P_2 = \operatorname{sgn} P_1 \cdot \operatorname{sgn} P_2$$

$$\operatorname{sgn} P_1^{-1} = \operatorname{sng} P_1 .$$

n-ta grupa alternujaca [A_n] - podgrupa S_n zlozona ze wszystkich parzystych permutacji.

1.4 Grupy ilorazowe B)

Prawostronna warstwa grupy G wzgledem jej podgrupy H wyznaczona przez $g \in G$ to zbior

$$gH = \{gh : h \in H\},$$

natomiast lewostronna warstwa to zbior

$$Hg = \{hg : h \in H\}.$$

Dla grup abelowych sa one rowne.

Dwa elementy $g_1, g_2 \in G$ wyznaczaja te sama warstwe prawostronna wzgledem H, gdy $g_1^{-1}g_2 \in H$, a te sama warstwe lewostronna, gdy $g_1g_2^{-1} \in H$.

Rzad grupy skonczonej G to ilosc jej elementow.

Indeks $[G : H]$ podgrupy H w grupie G to ilosc warstw w grupie G wzgledem H. Dla skonczonych grup mamy:

↪ $g \in G$ $o(g) | |G|$,

↪ rzad i indeks kazdej podgrupy sa dzielnikami rzedu grupy,

↪ jesli rzad jest liczba pierwsza, to grupa jest cykliczna

Twierdzenie Lagrange'a - dla skonczonych G > H:

$$|G| = [G : H] \cdot |H|.$$

Podgrupa H jest dzielnikiem normalnym grupy G [$H \triangleleft G$] jesli $(\forall g \in G)$ $gH = Hg$. Wystarczy, ze $(\forall g \in G)(\forall h \in H)$ $ghg^{-1} \in H$.

Niech $f : G_1 \to G_2$ bedzie homomorfizmem, a e_1, e_2 beda elementami neutralnymi grup odpowiednio G_1, G_2. Wtedy $f(e_1) = e_2$ oraz $f(g)^{-1} = f(g^{-1})$.

Obraz homomorfizmu $f : G_1 \to G_2$ jest podgrupa grupy G_2 [$\operatorname{Im} f < G_2$], natomiast jadro f jest dzielnikiem normalnym G_1 [$\operatorname{Ker} f \triangleleft G_1$].

Grupa ilorazowa to zbior wszyystkich warstw H/G, gdzie $H \triangleleft G$, z dzialaniem

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Odwzorowanie

$$\phi : G \to H$$
$$\phi(g) = gH$$

jest epimorfizmem (czesto nazywane kanonicznym homeomorfizmem G na H).

[!!!]Zasadnicze twierdzenie o homeomorfizmach dla grup – jesli $f : G \to G_1$ jest epimorfizmem oraz Ker $f = H$, natomiast $\phi : G \to G/H$ jest dzialaniem jak wyzej, to istnieje tylko jeden izomorfizm $\psi : G/H \to G_1$ taki, ze $f = \psi \circ \phi$

Jezeli $\emptyset \neq A \subseteq G$ oraz $G(A) < G$ to przekroj wszystkich podgrup G zawierajacych A, a $A \subseteq G_1 < G$, to $G(A) < G_1$.

Jezeli $K \lhd G$ i $H \lhd G$, to najmniejsza podgrupa G zawierajaca H i K pokrywa sie ze zbiorem

$$KH := \{kh : k \in K, h \in H\}$$

Pierwsze twierdzenie o izomorfizmach – jezeli $K \lhd G$ i $H \lhd G$, to

- $\hookrightarrow K < KH = HK < G$
- $\hookrightarrow H \cap K \lhd H$ i $K \lhd KH$
- $\hookrightarrow \phi : hK \to h(K \cap H)$ indukuje izomorfizm

$$HK/K \sim H/(H \cap K)$$

Drugie twierdzenie o izomorfizmach – jezeli $K \lhd G$ i $K < H < G$ i oznaczymy $\overline{H} = H/K$ oraz $\overline{G} = G/K$, to wtedy:

- $\hookrightarrow \overline{H} < \overline{G}$
- $\hookrightarrow \overline{H} \lhd \overline{G} \iff H \lhd G$

Automorfizm wewnetrzny grupy G wyznaczony przez g: $\phi_g(x) = g^{-1}xg$.
Jesli G to grupa abelowa, to dla kazdego g $\phi_g(x) = x$, a wiec ma ona jedynie identycznosc.
Zbior wszystkich automorfizmow wewnetrznych grupy G oznaczamy $I(G)$ i tworzy on grupe ze skladaniem

Centrum grupy G $[Z(G)]$ to zbior $x \in G$ takich, ze dla dowolnego $y \in G$ $xy = yx$. Dla kazdego G $Z(G) \lhd G$

Grupa $I(G)$ jest izomorficzna z $G/Z(G)$.

Jesli M to dowolny podzbior grupy G, to dla kazdego g takiego, ze $\phi_g \in I(G)$ zbiorem sprzezony do M nazywamy zbior

$$M^g = \{\phi_g(x) : x \in M\}$$

Jesli $M = \{x\}$, to M^g zawiera elementy sprzezone z x.
Normalizator zbioru M:

$$N_G(M) = \{g \in G : M^g = M\}$$

Centralizator zbioru M:

$$C_G(M) = \{g \in G : mg = gm, m \in M\}$$

Twierdzonka:

- $\hookrightarrow (\forall M \subseteq G)\ C_G(M) < N_G(M)\ (|M| = 1 \implies C_G(M) = N_G(M))$
- $\hookrightarrow Z(G) = C_G(G)$
- $\hookrightarrow$ dla $M \subseteq G$ ilosc zbiorow M^g jest rowna $[G : N_G(M)]$.

Aby klasa elementow sprzezonych z $x \in G$ byla jednoelementowa wystarczy, zeby $x \in Z(G)$

Jesli G jest skonczona, to ilosc elementow sprzezonych z zadanym x jest dzielnikiem $|G|$.

p-grupa to grupa, w ktorej wszystkie elementy maja rzad p, gdzie p jest liczba pierwsza. Jesli $|G| = p^n$ to G jest p-grupa.
Skonczone p=grupy maja nietrywialne centrum.
Jesli $|G| = p^2$, to G jest grupa abelowa.

1.5 Produkty grup

W zbiorze $A \times B = \{(a, b) : a \in A, b \in B\}$, gdzie A, B sa grupami, okreslmy

$$(a, b) \cdot (c, d) = (ac, bd)$$