Algebra 1R

Contents

1 DEFINICJA GRUPY

1.1 Działania, struktury

DZIAŁANIE w zbiorze A to funkcja

$$\star : A \times A \to A$$

$$(x, y) \mapsto x \star y$$

Zwykle rozważamy działania binarne, ale działaniem może być funkcją z A^n w A (jak na przykład branie średniej arytmetycznej 3 liczb). Zdarza się też, że mamy działanie unarne, takie jak na przykład branie liczby przeciwnej do $m \in \mathbb{Z}$.

Działanie jest łączne [assosiative], jeżeli

$$(\forall\ a, b, c \in A)\ a(bc) = (ab)c$$

a przemienne [commutative], gdy

$$(\forall\ a, b \in A)\ ab = ba$$

Tutaj warto zaznaczyć, że jeśli działanie jest łączne dla 3 argumentów, to jest również łączne dla k argumentów. Dowód przez indukcję jest trywialny.

Algebrą nazywamy niepusty zbiór A ze wszystkimi działaniami na nim określonymi, to znaczy zestawienie $(A, f_1, \ldots, f_k)$. Zbiór A nazywamy uniwersum lub dziedziną struktury. Mówimy, że dwie algebry $A = (A, f_1, \ldots, f_k)$ i $B = (B, g_1, \ldots, g_k)$ są podobne, jeśli dla każdego $i \leq k$ arność (czyli liczba argumentów) f_i jest równa arności g_i, czyli liczbie l_i.
Dwie algebry są izomorficzne, jeżeli istnieje $F : A \xrightarrow[\text{na}]{1-1} B$ takie, że

$$(\forall\ i \leq k)(\forall\ a_1, \ldots, a_{l_i} \in A)\ F(f_i(a_1, \ldots, a_{l_i})) = g_i(F(a_1), \ldots, F(a_{l_i}))$$

Struktury izomorficzne oznaczamy $A \cong B$. Warto zauważyć, że $\cong$ ma *własności relacji równoważności*, to znaczy jest zwrotny, symetryczny i przechodni.

SŁOWNICZEK:
- $\hookrightarrow$ epi-morfizm -> "na"
- $\hookrightarrow$ mono-morfizm -> 1-1
- $\hookrightarrow$ izo-morfizm -> bijeckja
- $\hookrightarrow$ endo-morfizm -> w samego siebie
- $\hookrightarrow$ auto-morfizm -> endomorfizm który jest bijekcją.

$B = (B, g_1, \ldots, g_k)$ jest podalgebrą $A = (A, f_1, \ldots, f_k)$, jeżeli
- $\hookrightarrow B \subseteq A$
- $\hookrightarrow (\forall\ i \leq k)\ g_i = f_i\restriction_B$

Niech $B \subseteq A$, wtedy B jest uniwersum podstruktury struktury A z naturalnymi działaniami $\iff$ B jest zamknięty na działania $f_1, \ldots, f_k$. W takim przypadku B traktujemy jako strukturę będącą podstrukturą struktury A.

Jeżeli $F : A \to B$ jest homomorfizmem struktur, to Im(F) jest podstrukturą B.

Złożenie homomorfizmów jest homomorfizmem a odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

DOWÓD:

Niech $f : (X, \cdot) \to (Y, \circ)$ i $g : (Y, \circ) \to (Z\star)$ są homomorfizmami, a $h(x) = g(f(x))$ jest ich złożeniem, to dla dowolnego $a, b \in X$ mamy

$$h(a \cdot b) = g(f(a \cdot b)) = g(f(a) \circ f(b)) = g(f(a)) \star g(f(b)) = h(a) \star h(b)$$

więc h spełnia warunki homomorfizmu. Jeżeli f, g były epi, mono, ... morfizmami, to zachowanie odpowiednich własności wynika z własności składania funkcji różnowartościowych, na czy bijekcji.

Niech $\phi : (X, \cdot) \xrightarrow[\text{na}]{1-1} (Y, \circ)$ będzie izomorfizmem. Chcemy pokazać, że ϕ^{-1} jest homomorfizmem. Weźmy $a, b \in Y$ i $c, d \in X$ takie, że $\phi(c) = a$ oraz $\phi(d) = b$. Wtedy

$$ab = \phi(c)\phi(d) = \phi(cd),$$

czyli

$$\phi^{-1}(ab) = cd,$$

a ponieważ $\phi^{-1}(a) = c$ i $\phi^{-1}(b) = d$, to mamy

$$\phi^{-1}(ab) = cd = \phi^{-1}(a)\phi^{-1}(b).$$

Natomiast fakt, że ϕ^{-1} jest bijekcją wynika z tego, że ϕ jest bijekcją.

1.2 Grupy

Grupa to struktura $G = (G, \cdot)$ taka, że:
- $\hookrightarrow$ $\cdot$ jest działaniem łącznym
- $\hookrightarrow$ istnieje element neutralny $e \in G$ dla działania $\cdot$
- $\hookrightarrow$ dla każdego $g \in G$ istnieje element odwrotny $g^{-1} \in G$ takie, że $gg^{-1} = g^{-1}g = e$

Tutaj warto zaznaczyć, że *element neutralny jest jedyny*. W przeciwnym przypadku istniałyby co najmniej dwa elementy neutralne e_1, e_2, ale wtedy

$$e_1 = e_1 \cdot e_2 = e_2.$$

Z łączności działania na grupie wynika, że dla każdego $g \in G$ *istnieje co najwyżej jeden element odwrotny*. Gdyby x, y były dwoma elementami odwrotnymi do g, to

$$x = xe = x(gy) = (xg)y = ey = y,$$

co prowadzi do sprzeczności.

1.3 Podgrupy

1.4 Grupa cykliczna

2 HOMOMORFIZMY

2.1 Rodzaje

2.2 Jądro, obraz

2.3 Zasadnicze twierdzenie o homomorfizmie

3 PERMUTACJE

3.1 Transpozycje

3.2 Permutacje parzyste

4 WARSTWY, DZIELNIK NORMALNY

4.1 Warstwa, grupa ilorazowa

4.2 Orbita

4.3 Stabilizator

4.4 Orbit-stabilizer theorem

4.5 Dzielnik normalny

5 PRODUKT PÓŁPROSTY

5.1 Twierdzenie Lagrange'a

5.2 Produkt prosty

5.3 Produkt półprosty grup

6 TWIERDZENIE SYLOWA

6.1 I twierdzenie Sylowa

I twierdzenie Sylowa:
Jeżeli p jest liczbą pierwszą, a G jest grupą skończoną rzędu $|G| = p^k m$ dla $k \geq 1$ i $p \nmid m$, to istnieje podgrupa $H \leq G$ mająca p^k elementów. Taka grupa nazywa się podgrupą Sylowa.

DOWÓD:

Niech G będzie grupą rzędu $|G| = p^k m$ taką jak w twierdzeniu. Niech X będzie zbiorem wszystkich p^k elementowych podzbiorów grupy G. Możemy teraz określić działanie ψ grupy G na zbiór X. Jeśli $H = \{h_1, \ldots, h_{p^k}\} \in X$, a $g \in G$, to

$$\psi(H) = \{gh_1, gh_2, \ldots, gh_{p^k}\}.$$

Wiemy, że

$$|H| = \binom{p^k m}{p^k} = \frac{(p^k m)!}{(p^k m - p^k)!(p^k)!} =$$
$$= \frac{p^k m(p^k m - 1)\ldots(p^k m - p^k + 1)}{(p^k)!} = \prod_{i=1}^{p^k} p^k m - i + 1$$

6.2 Twierdzenie Cauchy'ego

Twierdzenie Cauchy'ego:
Jeżeli liczba pierwsza p dzieli rząd grupy G, to G zawiera element rzędu p.

6.3 p-grupy Sylowa

6.4 Twierdzenia Sylowa

7 KLASYFIKACJA MAŁYCH GRUP

7.1 Grupy rzędu ???

8 GRUPY TORSYJNE

8.1 Torsje

8.2 Grupy torsyjne

8.3 Skończone grupy abelowe

9 GRUPY ROZWIĄZALNE

9.1 Komutator i komutant

9.2 Grupy rozwiązalne

9.3 Rozszerzenia grup rozwiązalnych

9.4 Używanie twierdzeń Sylowa

9.5 Grupy nilpotentne

10 LEMAT O MOTYLU

10.1 Ciąg kompozycyjny w grupie

10.2 Lemat motyla

10.3 Twierdzenie Schreiera

11 GRUPY WOLNE

11.1 Grupy wolne

11.2 Własności

11.3 Przykłady

12 PIERŚCIENIE

12.1 Definicja

12.2 Dzielnik zera

12.3 Grupa elementów odwracalnych pierścienia

12.4 Dziedzina

12.5 Ciało