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 $(A, f_1, \dots, f_k)$. Zbiór A nazywamy uniwersum lub dziedziną struktury. Mówimy, że dwie algebry $A = (A, f_1, \dots, f_k)$ i $B = (B, g_1, \dots, g_k)$ 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

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

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

$B = (B, g_1, \dots, g_k)$ jest podalgebrą $A = (A, f_1, \dots, f_k)$, 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 $f_1, \dots, f_k$. W takim przypadku B traktujemy jako strukturę będącą podstrukturą struktury A.

1.2 Grupy

Monoid to zbiór X z działaniem łącznym oraz elementem neutralnym. Liczby naturalne z dodawaniem są przykładem monoidu.

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 $gg^{-1} = g^{-1}g = e$

Grupa trywialna to zbiór z działaniem zawierający jedynie jego element neutralny: $\{e\}$.

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.

Jeśli działanie grupy jest przemienne, to nazywamy ją grupą abelową lub przemienną. Tak jak działanie w grupie oznaczamy zwykle przez $\cdot$, tak w grupie abelowej, aby podkreślić jego przemienność, działanie jest zwykle oznaczane przez +. Podobnie, potęgowanie w grupie abelowej nie oznaczamy x^n, a raczej nx.

Działanie w grupie możemy opisać za pomocą tabelki

$\star$	a_1	a_2	...	a_k
a_1	a_1a_1	a_1a_2	...	a_1a_k
a_2	a_2a_1	a_2a_2	...	a_2a_k
...				
a_k	a_ka_1	a_ka_2	...	a_ka_k

Jeżeli działanie jest przemienne, to oczywiście taka tabelka będzie symetryczna.

Grupę przemienną $G = \{e, a, b, c\}$ nazywamy grupą czwórkową Kleina [K_4]. Grupa izometrii własnych n-kąta foremnego [D_n] jest nazywana grupą dihedralną i nie jest ona grupą abelową. Jej podgrupą jest na przykład grupa obrotów własnych n-kąta foremnego [O_n].

Pierścieniem nazywamy zbiór X z dwoma działaniami, + i $\cdot$, z których $\cdot$ jest łączne, a + jest przemienne. W dodatku, $\cdot$ jest rozdzielne względem +:

$$(\forall\ x, y, z \in X)\ x \cdot (y + z) = x \cdot y + x \cdot z$$

Jeśli dodatkowo mnożenie w pierścieniu jest działaniem przemiennym, to taki pierścień nazywamy przemienny. Jeśli zaś istnieje element neutralny dla mnożenia, to jest on pierścieniem z jednością.

Pierścienie K, dla których $K \setminus \{0\}$ jest grupą przemienną względem mnożenia nazywamy ciałami. Najprostszym ciało są zbiory $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ze zwykłym dodawaniem i mnożeniem. Zbiór $\mathbb{Q}(i)$ wszystkich liczb zespolonych postaci $a + bi$ dla wymiernych a, b jest ciałem.

Niech $H \subseteq G$ dla pewnej grupy G. Mówimy, że H jest podgrupą grupy G [$H \leq G$], jeżeli H jest grupą względem działania z G (ograniczonego do H). Dodatkowo, jeśli $H \neq G$ to mówimy, że H jest podgrupą właściwą. Na przykład

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +).$$

Przy sprawdzaniu, czy dany zbiór H jest podgrupa G wystarczy sprawdzić, czy $(\forall\ x, y \in H)\ xy^{-1} \in H$.

Jeśli $a, b \in G$, to $(ab)^{-1} = b^{-1}a^{-1}$.

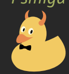
DOWÓD:

Chcemy sprawdzić, że $(b^{-1}a^{-1})ab = e$

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$$

a więc dostajemy to, czego się spodziewaliśmy.

i śmiga



Zdefiniujemy $a^{-n} = (a^{-1})^n$ i nie trudno pokazać, że też $a^{-n} = (a^n)^{-1}$. Dalej mamy $a^{n+m} = a^na^m$, a dla grupy przemiennej zachodzi $(ab)^n = a^nb^n$.

1.3 Grupa cykliczna

Rząd grupy to ilość jej elementów: $org(G) = |G|$. Dla każdego $g \in G$ definiujemy rząd elementu $ord(g) = N$ jako najmniejszą liczbę naturalną taką, że $g^N = e$. Znając pojęcie grup cyklicznych (niżej) możemy też podać równoważną definicję: $ord(g) = |\langle g \rangle|$.
Jeśli $ord(g) = n$ i weźmiemy N takie, że $g^N = e$, to mamy pewność, że $n|N$. Gdyby tak nie było, to mielibyśmy $N = kn + r$, $0 < r < n$ i

$$g^N = g^{kn+r} = g^{kn}g^r = (g^n)^kg^r = e^kg^r = g^r \neq e.$$

W takim razie dla $g, g^2, \dots, g^n$ są elementami parami różnymi i tworzą podgrupę grupy G.

Grupa cykliczna to grupa utworzona przez wzięcie wszystkich potęg $g \in G$: $H = \{g, g^1, \dots, g^{ord(g)}\}$, przy czym możemy mieć $ord(g) = \infty$. W takim przypadku dostajemy podgrupę nieskończoną. Dla grupy cyklicznej utworzonej przez g, ten element nazywamy generatorem. Zauważmy, że wszystkie grupy cykliczne sa abelowe.

Grupa zawierająca wszystkie liczby całkowite z dodawaniem jest grupą cykliczną generowaną przez 1 lub przez -1. Widzimy więc, że *generator grupy nie jest wyznaczony jednoznacznie*.

Dla $N \in \mathbb{N}$ definiujemy C_N jako liczby naturalne < N z dodawaniem modulo N. Zwykle oznaczamy ją $(\mathbb{Z}_N, +_N)$. Możemy pokazać, że każda grupa cykliczna skończona rzędu N jest izomorficzne z C_N, natomiast grupy cykliczne nieskończone są izomorficzne z C_∞.
Grupa $\mathbb{Z}_N* = (\mathbb{Z}_N*, \cdot)$ to grupa liczb naturalnych mniejszych niż N, które są z N względnie pierwsze. Działanie na tej grupie to mnożenie modulo N.

2 HOMOMORFIZMY

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

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.

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.

2.1 Rodzaje

2.2 Jądro, obraz

Dla danego homomorfizmu $f : G \to H$ definiujemy jądro $\text{Ker } f = \{g \in G \ : \ f(g) = e_H\}$ oraz obraz $\text{Im } f = \{f(g) \ : \ g \in G\}$. Z tych definicji wynika, że $\text{Ker } f \leq G$ oraz $\text{Im } f \leq H$.

Dla monomorfizmu $f : G \to H$ jądro jest trywialne $\ker f = \{e_G\}$. Gdyby tak nie było, to dla pewnego $e_G \neq g \in G$ mielibyśmy $f(g) = e_H$, a więc dla wszystkich innych $e_G \neq h \in G$

$$f(h) = e_H \cdot f(h) = f(g)f(h) = f(gh),$$

i jest $gh \neq h$ ale $f(h) = f(gh)$.

Jeśli $f : X \to Y$ jest epimorfizmem, to relacja $\sim$ określona na X przez

$$x \sim y \iff f(x) = f(y)$$

jest relacją równoważności, a jej klasy abstrakcji są włóknami funkcji f. Jeśli $K = \text{Ker } f$, to dla każdego $a \in X$ mamy $aK = Ka$ i warstwy K w X to włókna f.

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

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

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 Generatory

Jeśli mamy grupę G oraz jej podzbiór S, to mówimy, że S generuje grupę G, jeśli każdy element z G może być zapisany za pomocą skończenie wielu elementów z S i ich odwrotności. Wtedy elementy zbioru S to generatory grupy G. Jeżeli grupa G jest generowana przez skończony zbiór S, to G jest skończenie generowana. Dalej, jeśli $\phi : S \to G$ i $\mathrm{Im}(\phi)$ generuje G, to mówimy, że ϕ generuje G.

Niech S jest zbiorem, a F, G grupami. Jeśli istnieje różnowartościowa funkcja $f : S \to F$ generująca F, a $g : S \to G$ jest przekształceniem S w G, to widać, że istnieje dokładnie jeden homomorfizm $\psi : F \to G$:

$$\begin{tikzcd}
& G & \\
S \arrow[ur, "g"] \arrow[rr, "f"'] & & F \arrow[ul, "\psi"']
\end{tikzcd}$$

11.2 Własności

11.3 Przykłady

12 PIERŚCIENIE

12.1 Definicja

Pierścień $(R, +, \cdot)$ to zbiór z mnożeniem $\cdot$ oraz dodawaniem $+$ taki, że $(R, +)$ jest grupą przemienną, mnożenie jest łączne i posiada element neutralny. Dodatkowo, dodawanie jest dwustronnie rozdzielne względem mnożenia, czyli dla wszystkich $x, y, z \in A$ mamy

$$(x + y)z = xz + yz$$

Jeżeli w pierścieniu istnieje element neutralny 1 dla mnożenia $\cdot$ [jedność pierścienia], to jest on unikalny, a pierścień R dla którego to zachodzi jest nazywany pierścieniem z jednością. Dalej, jeśli mnożenie jest działaniem przemiennym, to R jest pierścieniem z jednością.

Grupa U zawierająca wszystkie elementy A takie, że istnieją ich odwrotności dla mnożenia nazywa się grupą multiplikatywną lub unit group of A. Czasem zapisujemy ją jako A^* i nazywamy grupą elementów, które są odwracalne. Jeżeli w pierścieniu A mamy $1 \neq 0$ i każdy jego element jest odwracalny, to A jest nazywamy pierścieniem z dzieleniem.

Podpierścień z jednością $R' \subseteq R$ jest pierścieniem względem działań z R, a w szczególności $1_{R'} = 1_R$.

Niech R będzie pierścieniem przemiennym z jednością (i tak będzie prawie zawsze), wtedy $R[X]$ to pierścień wielomianów zmiennej X nad R. Istnieje też pierścień formalnych szeregów potęgowych definiowany jako

$$R[[X]] := \{\sum_{i=0}^{\infty} a_i X^i \ : \ a_i \in R\}$$

z działaniami

$$\sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i$$

$$\left[\sum a_i X^i\right]\left[\sum b_i X^i\right] = \sum c_i X^i$$

gdzie $c_i = \sum_{n+k=i} a_n b_k$. Tutaj warto zaznaczyć, że $R[X] \subseteq R[[X]]$, bo ciągi $(0, \dots, 0, a_i, 0, \dots)$ zadają nam kolejne współczynniki wielomianu.
Na pierścieniu wielomianów możemy zdefiniować funkcję $\deg(w) : R[X] \to \mathbb{N}$, która wielomianowi przyporządkowuje jego stopień. Wtedy dla dowolnych $w, p \in R[X]$ zachodzą poniższe własności:

$$\deg(w \cdot p) \leq \deg(w) + \deg(p)$$

i zazwyczaj jest to równość, ale możemy trafić na wielomiany dziwne.

$$\deg(w + p) \leq \max(\deg(w), \deg(p)).$$

Dalej, łatwo zauważyć, że $R \subseteq R[X]$ jako zbiór wielomianów stopnia zerowego.

Kolejnym przykładem pierścienia jest R^X, czyli pierścień funkcji $X \to R$ dla R będącego pierścieniem. Dla dowolnych $f, g \in R^X$ definiujemy działania następująco:

$$(f + g)(x) = f(x) +_R g(x)$$

$$(f \cdot g)(x) = f(x) \cdot_R g(x)$$

Alternatywnie, możemy pierścień R^X zapisać jako produkt pierścieni z działaniami po osiach określonymi jak w przypadku produktów grup:

$$R^X = \prod_{x \in X} R_x$$

gdzie $R_x = R$.

Jeżeli X jest przestrzenią topologiczną, to przestrzeń $C(X)$ zawierająca funkcje ciągłe $X \to \mathbb{R}$ jest podpierścieniem pierścienia $\mathbb{R}^X$.

Jeżeli zajmiemy się na chwilę kategorią miary (lub miarą i całką, co kto woli), i rozważymy ciało zbiorów $\mathscr{C} \subseteq \mathscr{P}(X)$ z działaniami $\cap$ i $\triangle$, to również mamy pierścień. JEżeli teraz wprowadzimy pierścień Boole'a, czyli taki w którym $a^2 = a$, to możemy go utożsamić z pierścieniami tworzonymi na zbiorach potęgowych dowolnego zbioru X.

12.2 Dzielnik zera

12.3 Grupa elementów odwracalnych pierścienia

12.4 Dziedzina

12.5 Ciało