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.

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

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.

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 $\mathbb{Q}(\sqrt{3})$ 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.

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

1.3 Grupa cykliczna

Rząd grupy to ilość jej elementów: $\text{org}(G) = |G|$. Dla każdego $g \in G$ definiujemy rząd elementu $\text{ord}(g) = N$ jako najmniejszą liczbę naturalną taką, że $g^N = e$. Znając pojęcie grup cyklicznych (niżej) możemy też podać równoważną definicję: $\text{ord}(g) = |\langle g \rangle|$.

Jeśli $\text{ord}(g) = n$ 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

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

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

Grupa cykliczna to grupa utworzona przez wzięcie wszystkich potęg $g \in G$: $H = \{g, g^1, \ldots, g^{ord(g)}\}$, 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 ϕ : (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 ϕ(c) = a oraz ϕ(d) = b. Wtedy

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

czyli

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

a ponieważ ϕ^{-1}(a) = c i ϕ^{-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 Ker f = {g $\in$ G : f(g) = e_H} oraz obraz Im f = {f(g) : g $\in$ G}. Z tych definicji wynika, że Ker f $\leq$ G oraz 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 = 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

5 PRODUKT PÓŁPROSTY

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

9 GRUPY ROZWIĄZALNE

10 LEMAT O MOTYLU

11 GRUPY WOLNE

11.1 Grupy wolne

11.2 Własności

11.3 Przykłady

12 PIERŚCIENIE