Maciej Grzesiak

Podstawowe struktury algebraiczne

1. Wprowadzenie

Przedmiotem algebry było niegdyś przede wszystkim rozwiązywanie równań. Obecnie algebra staje się coraz bardziej nauką o systemach matematycznych. *System* bądź *struktura algebraiczna* to zbiór na elementach którego można wykonywać pewne działania, podlegające określonym regułom.
Można konstruować i badać różne takie systemy. Modelami dla nich są przeważnie systemy liczbowe. Jest widoczne, że system składający się z liczb naturalnych $\mathbb{N}$ z działaniami dodawania $+$ i mnożenia $\cdot$ ma inne własności niż np. system $\mathbb{Z}$ liczb całkowitych, $\mathbb{Q}$ liczb wymiernych czy $\mathbb{R}$ liczb rzeczywistych z tymi samymi działaniami. Wybierając podstawowe własności poszczególnych systemów (tak by z nich wynikały inne ich własności oraz by widoczne były różnice między poszczególnymi systemami) otrzymujemy pewien układ aksjomatów. Rozmaite układy aksjomatów stają się podstawą do definiowania różnych struktur algebraicznych.
Mówimy, że w zbiorze liczb X jest wykonalne dodawanie, jeśli dla każdej pary liczb $x_1, x_2 \in X$ ich suma $x_1 + x_2 \in X$.
Podobnie określamy w zbiorze X wykonalność odejmowania i mnożenia oraz dzielenia przez liczbę różną od zera.
Działania można wykonywać nie tylko na liczbach. Sprecyzujemy co to jest działanie w zbiorze (niekoniecznie liczbowym).

Definicja 1. *Działaniem* w zbiorze K nazywamy funkcję h, która każdej parze a, b elementów zbioru K przyporządkowuje pewien element tego samego zbioru: $h : K \times K \longrightarrow K$.

Na przykład dodawanie liczb rzeczywistych jest funkcją $+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ przyporządkowującą parze liczb x, y ich sumę $x + y$. Znak $+$ jest symbolem tego działania.

2. Ciała

Definicja 2. Każdy zbiór liczb, w którym są wykonalne cztery podstawowe działania arytmetyczne z wyjątkiem dzielenia przez 0 i który zawiera więcej niż jedną liczbę, nazywamy *ciałem liczbowym.*

Przykłady
1. Ciałami liczbowymi są $\mathbb{Q}$ i $\mathbb{R}$. Nie są ciałami $\mathbb{N}$ ani $\mathbb{Z}$.
1. Dla dowolnej liczby wymiernej dodatniej D nie będącej kwadratem liczby wymiernej zbiór

$$\{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

jest ciałem liczbowym.
Istnieje więc nieskończenie wiele ciał liczbowych.

Twierdzenie 1. *Każde ciało liczbowe K zawiera ciało liczb wymiernych.*

D o w ó d. K jest ciałem, więc zawiera liczbę $a \neq 0$. Z wykonalności dzielenia $a/a = 1 \in K$. Stąd na podstawie wykonalności dodawania $2 = 1 + 1 \in$, $3 = 2 + 1 \in K$ itd; ogólnie — $n \in K$ dla dowolnej liczby naturalnej n.

Z wykonalności odejmowania $1-1=0\in K$, a stąd dla dowolnego $n\in\mathbb{N}$, $-n\in K$. Z wykonalności dzielenia dla dowolnych liczb naturalnych n i m, $n/m\in K$, $-n/m\in K$, a więc $\mathbb{Q}\subset K$. ■
Zatem każde ciało liczbowe jest zbiorem nieskończonym.
Uogólnimy teraz pojęcie ciała liczbowego wychodząc z założenia, że najważniejsze są własności działań, a nie obiekty, na których działania są wykonywane.

Definicja 3. Niech będzie dany zbiór K mający co najmniej dwa elementy, w którym są określone dwa działania $\oplus$ i $\odot$ zwane odpowiednio dodawaniem i mnożeniem. Jeżeli dla dowolnych $x,y,z\in K$ i dla pewnych elementów $0,1\in K$ mamy:

1. $(x\oplus y)\oplus z=x\oplus(y\oplus z)$ (dodawanie jest łączne),
2. $x\oplus y=y\oplus x$ (dodawanie jest przemienne),
3. $0\oplus x=x\oplus 0=x$ (istnieje w K element zerowy 0),
4. $x\oplus(-x)=0$ (dla każdego elementu x istnieje element przeciwny $-x$),
5. $(x\odot y)\odot z=x\odot(y\odot z)$ (mnożenie jest łączne),
6. $x\odot y=y\odot x$ (mnożenie jest przemienne),
7. $1\odot x=x\odot 1=x$ (istnieje w K element jednostkowy $1\neq 0$),
8. $x\odot x^{-1}=x^{-1}\odot x=1$ (dla $x\neq 0$ istnieje element odwrotny x^{-1}),
9. $x\odot(y\oplus z)=x\odot y\oplus x\odot z$ (mnożenie jest rozdzielne względem dodawania),

to system $(K,\oplus,\odot)$ nazywamy *ciałem (abstrakcyjnym).*

Przykłady
1. Ciała liczbowe $\mathbb{Q}$, $\mathbb{R}$, $\{a+b\sqrt{D}:a,b\in\mathbb{Q}\}$ są oczywiście ciałami.
2. Zbiór $\mathbb{C}$ liczb zespolonych jest ciałem (z działaniami dodawania i mnożenia).
3. Niech p będzie liczbą pierwszą. Rozpatrzmy zbiór $\mathbb{Z}_p=\{0,1,2,\ldots,p-1\}$ możliwych reszt z dzielenia przez p. W zbiorze tym wprowadzimy działania *dodawania i mnożenia modulo p.* Określone są one następująco:

$$a+b=\text{ reszta z dzielenia zwykłej sumy przez } p,$$

$$a\cdot b=\text{ reszta z dzielenia zwykłego iloczynu przez } p.$$

Piszemy $a+b=c(\mathrm{mod}\,p)$. Na przykład:

$$2+2=1(\mathrm{mod}\,3),\ 2\cdot 2=1(\mathrm{mod}\,3),\ 3+4=2(\mathrm{mod}\,5),\ 3\cdot 2=1(\mathrm{mod}\,5).$$

Zbiory $\mathbb{Z}_p$ są skończone, więc można sporządzić dla nich kompletne tabelki działań. Przykładowo dla $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

oraz dla $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

Z tabel widzimy, że np. $-2=1(\mathrm{mod}\,3)$, $2^{-1}=2(\mathrm{mod}\,3)$.
4. Ciało funkcji wymiernych. *Funkcją wymierną* jednej zmiennej nazywamy iloraz dwóch wielomianów, tzn. funkcję postaci:

$$f(x)=\frac{a_0+a_1x+\cdots+a_nx^n}{b_0+b_1x+\cdots+b_mx^m}.$$

Zbiór wszystkich takich funkcji oznaczymy przez $\mathbb{R}(x)$. Zwykłe działania (dodawanie i mnożenie funkcji) określają w tym zbiorze strukturę ciała.

Definicja 4. Przekształcenie $f:K\longrightarrow K'$ odwzorowujące wzajemnie jednoznacznie ciało K na ciało K' i zachowujące działania, tj.:

$$f(a+b)=f(a)\oplus f(b),\quad f(ab)=f(a)\odot f(b)\text{ dla }a,b\in K,$$

nazywamy *izomorfizmem.* Ciała K i K' nazywają się *ciałami izomorficznymi.*

Przykłady.
1. Niech $K = K' = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Odwzorowanie $f : K \longrightarrow K'$ dane wzorem $f(a + b\sqrt{2}) = a - b\sqrt{2}$ jest izomorfizmem.
2. Niech $\mathbb{R}(x)$ i $\mathbb{R}(y)$ oznaczają ciała funkcji wymiernych zmiennej x i y odpowiednio. Przyporządkowanie:

$$\frac{a_0 + a_1x + \cdots + a_nx^n}{b_0 + b_1x + \cdots + b_mx^m} \longleftrightarrow \frac{a_0 + a_1y + \cdots + a_ny^n}{b_0 + b_1y + \cdots + b_my^m}$$

jest izomorfizmem.

3. Grupy

Definicja 5. Zbiór G z określonym na nim działaniem $\circ$ nazywamy *grupą*, gdy:
G1. $\forall_{x,y,z\in G}\ \ (x \circ y) \circ z = x \circ (y \circ z)$;
G2. $\exists_{e\in G}\ \ \forall_{x\in G}\ \ e \circ x = x \circ e = x$;
G3. $\forall_{x\in G}\ \ \exists_{x^{-1}\in G}\ \ x \circ x^{-1} = x^{-1} \circ x = e$.

Na ogół piszemy krócej ab zamiast $a \circ b$.
Ponieważ działanie jest łączne, więc $(ab)c = a(bc)$ można pisać po prostu jako abc. Z tego samego powodu iloczyn $a_1a_2 \ldots a_n$ można pisać bez nawiasów (ale nie można zmieniać kolejności). Jeśli $a_1 = a_2 = \ldots = a_n$, to taki iloczyn nazywamy $n-$tą potęgą i oznaczamy a^n. Określamy ponadto $a^0 = e$, $a^{-n} = (a^n)^{-1}$ lub $a^{-n} = (a^{-1})^n$.
Ćwiczenie. Wykazać, że dla $a \in G$, $m, n \in \mathbb{Z}$ $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Jeśli $a^n = e$ dla pewnego $n > 0$, to najmniejszą z liczb o tej własności nazywamy *rzędem elementu* a i oznaczamy $|a|$. Jeśli $a^n \neq e$ dla każdego $n > 0$, to $|a| = \infty$.
Jeśli grupa ma skończoną liczbę elementów, to nazywamy ją *grupą skończoną*. Liczbę elementów grupy nazywamy *rzędem grupy*; oznaczenie: $|G|$.
Ćwiczenie. Jeśli $a^n = e$, to n dzieli się przez $|a|$.

Jeżeli G spełnia oprócz G1—G3 jeszcze:

G4. $\forall_{x,y\in G}\ \ x \circ y = y \circ x$,

to nazywamy ją *grupą abelową*.
Tradycyjnie działanie w grupie abelowej oznaczamy $+$ i stosujemy następującą terminologię:

$\cdot$	$+$
mnożenie	dodawanie
iloczyn	suma
jedynka	zero
odwrotny	przeciwny
potęga	krotność
e lub 1	0
a^{-1}	$-a$
a^n	na

Przykłady.

1. Zbiór elementów dowolnego ciała rozpatrywany z dodawaniem tworzy grupę abelową, np. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

2. Zbiór elementów niezerowych dowolnego ciała rozpatrywany z mnożeniem tworzy grupę abelową, np. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$.

3. Zbiór $\mathbb{Z}$ z dodawaniem tworzy grupę abelową.

4. Zbiór $\mathbb{Z}_n$ reszt z dzielenia przez n z działaniem dodawania modulo n tworzy grupę abelową. Jest to grupa skończona rzędu n.

5. $\mathbb{Q}_p = \{\frac{m}{p^n} \ : \ m, n \in \mathbb{Z}\}$, gdzie p jest liczbą pierwszą, jest addytywną grupą abelową.

6. Zbiór $\mathbb{C}_n$ pierwiastków stopnia n z 1 jest grupą multiplikatywną skończoną rzędu n.
Przypomnienie. Pierwiastkami stopnia n z 1 są liczby

$$\varepsilon_k = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}, \qquad k = 0, 1, \ldots, n-1.$$

Można je zapisać w postaci wykładniczej:

$$\varepsilon_k = \mathrm{e}^{\mathrm{i}\,\frac{2k\pi}{n}}, \qquad k = 0, 1, \ldots, n-1$$

7. Niech Ω będzie zbiorem, a $S(\Omega)$ niech oznacza zbiór odwzorowań odwracalnych $\Omega \longrightarrow \Omega$. Zbiór $S(\Omega)$ z działaniem składania tworzy grupę.

8. W szczególności, gdy $\Omega = \{1, 2, \ldots, n\}$, to elementy zbioru $S(\Omega)$ nazywamy *permutacjami*, a $(S(\Omega), \circ)$ jest grupą permutacji n -elementowych. Nazywamy ją *grupą symetryczną* i oznaczamy S_n. Grupa S_n jest skończona i ma rząd $n!$, tj. $|S_n| = n!$. Dla $n > 2$ grupy S_n są nieabelowe.

9. Niech $\mathbb{K}$ będzie dowolnym ciałem. Zbiór macierzy nieosobliwych o wyrazach z $\mathbb{K}$ z działaniem mnożenia macierzy jest grupą. Oznaczamy ją $\mathbf{GL}(n, K)$ lub $\mathbf{GL}_n(K)$ i nazywamy *pełną grupą liniową*. Jedynką tej grupy jest macierz jednostkowa; elementem odwrotnym do macierzy $\mathbf{A}$ jest macierz odwrotna $\mathbf{A}^{-1}$.
W $\mathbf{GL}_n(K)$ można rozpatrywać następujące podzbiory:
a) $\mathbf{SL}_n(K) = \{\mathbf{A} \in \mathbf{GL}_n(K) : \det \mathbf{A} = 1\}$;
b) $\mathbf{D}_n(K) = \{\mathbf{A} \in \mathbf{GL}_n(K) : \mathbf{A}$ jest diagonalna$\}$;
c) $\mathbf{T}_n(K) = \{\mathbf{A} \in \mathbf{GL}_n(K) : \mathbf{A}$ jest górnotrójkątna$\}$;
d) $\mathbf{UT}_n(K) = \{\mathbf{A} \in \mathbf{T}_n(K) : \mathbf{A}$ ma jedynki na przekątnej $\}$.
Grupy te noszą nazwy: *specjalna grupa liniowa, grupa diagonalna, grupa trójkątna, grupa unitrójkątna.*

4. Pierścienie

Definicja 6. Niech P będzie zbiorem, w którym określone są działania $+$, $\cdot$ (dodawanie i mnożenie). Mówimy, że struktura $(P, +, \cdot)$ jest *pierścieniem*, jeżeli spełnione są następujące aksjomaty:
P1. $\forall x, y, z \in P \;\; (x + y) + z = x + (y + z)$;
P2. $\exists 0 \in P \;\; \forall x \in P \;\; 0 + x = x + 0 = x$;
P3. $\forall x \in P \;\; \exists - x \in P \;\; x + (-x) = (-x) + x = 0$;
P4. $\forall x, y \in P \;\; x + y = y + x$;
P5. $\forall x, y, z \in P \;\; (xy)z = x(yz)$;
P6. $\forall x, y, z \in P \;\; x(y + z) = xy + xz, \;\; (y + z)x = yx + zx$.
Pierścień, w którym dodatkowo spełniony jest:
P7. $\forall x, y \in P \;\; xy = yx$,
nazywamy *pierścieniem przemiennym.*

Jeśli ponadto:
P8. $\exists 1 \in P \;\; \forall x \in P \;\; x \cdot 1 = 1 \cdot x = x$,
to nazywamy go pierścieniem z jedynką.
W dalszym ciągu (poza przykładami) rozpatrujemy tylko pierścienie przemienne z jedynką.
Przykłady.
1. Zbiór liczb całkowitych ze zwykłymi działaniami dodawania i mnożenia $(\mathbb{Z}, +, \cdot)$ i elementami wyróżnionymi 0 i 1 jest pierścieniem przemiennym z jedynką.
2. $(\mathbb{Z}_n, +_n, \cdot_n)$ — zbiór reszt z dzielenia przez n z działaniami dodawania i mnożenia modulo n i elementami wyróżnionymi 0 i 1 jest także pierścieniem przemiennym z jedynką.
3. $(M_n(\mathbb{R}), +, \cdot)$ — zbiór macierzy kwadratowych stopnia n o elementach rzeczywistych z działaniami dodawania i mnożenia macierzy jest pierścieniem nieprzemiennym (ale z jedynką); zerem jest macierz zerowa, jedynką macierz jednostkowa I_n.

4. Zbiór funkcji ciągłych (rzeczywistych lub zespolonych) $C(a,b)$ ze zwykłymi działaniami dodawania i mnożenia funkcji jest pierścieniem przemiennym z jedynką, którą jest funkcja stała 1 (elementem zerowym jest funkcja stała 0).
Zadanie. Niech Ω będzie zbiorem niepustym, i niech $\mathcal{P}(\Omega)$ oznacza zbiór wszystkich podzbiorów zbioru Ω. Udowodnić, że zbiór $\mathcal{P}(\Omega)$ z działaniami:

$$A + B = (A \cup B) \setminus (A \cap B), \quad AB = A \cap B$$

jest pierścieniem z jedynką, w którym wszystkie niezerowe elementy grupy addytywnej są rzędu 2.
Poniższe własności mogą wydawać się oczywiste, ale warto zobaczyć jak wynikają one z aksjomatów pierścienia.

Lemat 1. *W dowolnym pierścieniu P: $0 \cdot b = b \cdot 0 = 0$ dla dowolnego $b \in P$.*

D o w ó d. $0 \cdot b = (0+0) \cdot b = 0 \cdot b + 0 \cdot b$, a stąd $0 \cdot b = 0$. □

Lemat 2. *W dowolnym pierścieniu P: $(-a)\cdot(-b) = a \cdot b$ dla dowolnych $a, b \in P$.*

D o w ó d. Ponieważ $a + (-a) = 0$, więc $0 = 0 \cdot (-b) = [a + (-a)](-b) = a(-b) + (-a)(-b)$. Ale także $a(-b) + ab = a[(-b) + b] = a \cdot 0 = 0$, więc $ab = (-a)(-b)$.
□

Definicja 7. Niech P będzie pierścieniem przemiennym z jedynką. Element $a \in P$, $a \neq 0$ nazywamy *dzielnikiem zera*, jeśli istnieje $b \in P$, $b \neq 0$ takie, że $ab = ba = 0$.

Przykłady.
1. W pierścieniu $\mathbb{Z}_6$ jest $2 \cdot 3 = 0$. Zatem elementy 2 i 3 są dzielnikami zera.
2. Niech $f \in C(0,1)$ będzie funkcją równą zero na przedziale $[a,b]$, gdzie $0 < a < b < 1$, zaś g dowolną niezerową funkcją równą 0 poza przedziałem $[a,b]$. Wtedy $f \cdot g = 0$, a więc takie funkcje są dzielnikami zera w pierścieniu $C(0,1)$.

Definicja 8. Pierścień przemienny z jedynką bez dzielników zera nazywamy *dziedziną całkowitości.*

Lemat 3. *Następujące warunki są równoważne:*
1. *P jest dziedziną całkowitości.*
2. *W P obowiązuje* prawo skracania*:*

$$ab = ac\ ,\ a \neq 0 \implies b = c.$$

D o w ó d. $(1) \Rightarrow (2)$: $ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b-c) = 0 \Rightarrow (a = 0 \vee b - c = 0) \Rightarrow b = c$.
$(2) \Rightarrow (1)$: niech $ab = 0$ i np. $a \neq 0$. Wtedy $ab = a \cdot 0$, więc $b = 0$. □
Przykłady.
1. $\mathbb{Z}$ jest dziedziną całkowitości.
2. $\mathbb{Z}_m$ jest dziedziną całkowitości $\Leftrightarrow$ m jest liczbą pierwszą.
D o w ó d. Różny od 0 element r pierścienia $\mathbb{Z}_m$ jest dzielnikiem zera wtedy i tylko wtedy, gdy istnieją liczby s i t $(0 < t < s \leqslant m-1)$ takie, że $rs = mt$. Jest to możliwe wtedy i tylko wtedy, gdy liczby r i m mają wspólny podzielnik większy od 1. Zatem dzielnikami zera w $\mathbb{Z}_m$ są wszystkie liczby różne od 0, mające z m wspólny podzielnik większy od 1. Stąd jeśli m jest liczbą pierwszą, to dzielników zera nie ma.
Pojęcie ciała pojawia się teraz jako szczególny przypadek pierścienia.

Definicja 9. *Ciało* jest to pierścień przemienny z jedynką, $1 \neq 0$, w którym elementy niezerowe tworzą grupę ze względu na mnożenie.

Przykłady. Zbiory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ze zwykłymi działaniami, zbiór $\mathbb{Z}_p$ dla liczb pierwszych p (z działaniami modulo p) tworzą ciała.
Każde ciało jest dziedziną całkowitości, ale nie na odwrót. Przykładem dziedziny całkowitości nie będącej ciałem jest *pierścień Gaussa*:

$$\mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z}\}.$$

Aby to wykazać przypuśćmy, że element $a+bi \in \mathbb{Z}[i]$ ma odwrotność, tj. istnieje taki element $c+di \in \mathbb{Z}[i]$, że $(a+bi)(c+di) = 1$. Wtedy także $|(a+bi)(c+di)|^2 = 1$, czyli

$$1 = |(a+bi)|^2 \cdot |(c+di)|^2 = (a^2+b^2)(c^2+d^2)$$

Liczby a, b, c, d są całkowite, więc musi być $a^2+b^2 = 1$, $c^2+d^2 = 1$. Stąd $a = \pm 1, b = 0$, lub $a = 0, b = \pm 1$. Zatem w $\mathbb{Z}[i]$ odwrotności mają tylko $1, -1, i, -i$.
Dzieleniem przez a nazywamy mnożenie przez element odwrotny do a; *ilorazem* $\frac{a}{b}$ nazywamy taki element x, że $bx = a$.

Lemat 4. *W dowolnym ciele wykonalne jest dzielenie (oprócz dzielenia przez 0) i jest ono jednoznaczne.*