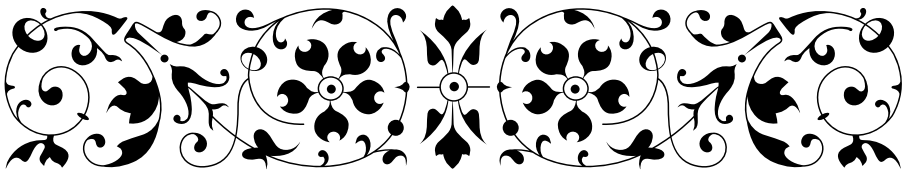
Szymoná Pawłá Zyguły

PODSTAWY ALGEBRY

ABSTRAKCYINEY,

ſporządzone dla ſtudentów kierunku Informatyka y Syſtemy Informacyine, ſpecyalność Proiektowanie Syſtemów CAD & CAM na Polytechnice Wárßáwſkiey, wydziale Mátemátyki y Náuk Informacyinych.

Z dla Boryſá Kurdká, Maxymilianá Michałá Czapſkiego, Zofii Anny Grabowſkiey, Piotrá Kucharczyká, Michałá Okurowſkiego, Filipá Łojká, i Miłoßá Damianá Sobczyká podziękowániami zá poprawki.



WÁRSZÁWÁ,

cum privilegio.

MM XX V.

Spis treści

1 Struktury algebraiczne. 5

1.1 Podstawowe struktury. 5

1.1.1 Złożone struktury. 7

1.1.2 Zadania. 8

1.2 Algebra Uniwersalna. 9

1.2.1 Podstawowe definicje. 10

1.2.2 Zadania. 11

1.3 Pewne definicje związane z algebrami. 12

1.3.1 Podalgebry. 12

1.3.2 Homomorfizmy. 12

1.3.3 Wolne algebry. 14

1.3.4 Zadania. 15

1.4 Kongruencje. 16

1.4.1 Zadania. 19

2 Przestrzenie liniowe. 21

2.1 Definicja przestrzeni liniowej i powiązane definicje. 21

2.1.1 Zadania. 21

2.2 Wartości własne macierzy. 21

2.2.1 Zadania. 24

2.3 Postać Jordana macierzy. 24

2.3.1 Zadania. 26

3 Teoria kategorii. 27

3.1 Wstęp. 27

3.1.1 Klasy. 27

3.1.2 Kategorie. 28

3.1.3 Diagramy. 29

3.1.4 Kilka podstawowych definicji. 30

3.1.5 Zadania. 31

3.2 Kategorie i język kategorii. 32

3.2.1 Zadania. 32

3.3 Różne konstrukcje kategoryczne. 32

3.3.1 Zadania. 32

3.4 Dualność i kilka innych pojęć. 32

3.4.1 Zadania. 32
3.5 Funktory. 32
3.5.1 Zadania. 32

Rozdział 1

Struktury algebraiczne.

Zajmiemy się teraz zdefiniowaniem tak zwanych **struktur algebraicznych**. Będą to zbiory z działaniami, które spełniają pewne własności. Znanym nam już przykładem—do którego jednak przejdziemy znacznie później—są przestrzenie liniowe.

W tekście zakładamy, że $0 \in \mathbb{N}$.

1.1 Podstawowe struktury.

Definicja 1.1.1. Magmą nazywamy parę $(A, \star)$, gdzie A jest zbiorem, a $\star : A^2 \to A$ jest dwuargumentową funkcją na A (nazywaną też działaniem). Działanie $\star$ na $x, y \in A$ zapisujemy $x \star y$.

Często magmę $(A, \star)$ będziemy utożsamiać ze zbiorem A i mówić, że A jest magmą. Podobny zabieg wykonamy dla wszystkich kolejnych definiowanych przez nas struktur.

Przykład 1.1.1. $(\mathbb{N}_+, +)$ (przez $\mathbb{N}_+$ rozumiemy dodatnie liczby naturalne) jest magmą.

Przykład 1.1.2. $(\mathbb{Z}, +)$ jest magmą.

Przykład 1.1.3. $(\mathbb{Q}_+, \div)$ (przez $\mathbb{Q}_+$ rozumiemy dodatnie liczby wymierne) jest magmą.

Definicja 1.1.2. Półgrupą nazywamy magmę $(A, \star)$, że działanie $\star$ jest łączne. To znaczy, że

$$\forall_{a,b,c \in A}\ a \star (b \star c) = (a \star b) \star c.$$

Przykład 1.1.4. $(\mathbb{N}_+, +)$ jest półgrupą.

Przykład 1.1.5. $(\mathbb{Z}, +)$ jest półgrupą.

Przykład 1.1.6. $(\mathbb{Q}_+, \div)$ *nie* jest półgrupą, ponieważ przykładowo

$$1 \div (2 \div 2) = 1 \neq \frac{1}{4} = (1 \div 2) \div 2.$$

Dzięki łączności, działania w półgrupach nie wymagają nawiasów. Przykładowo, jeśli $(A, \cdot)$ jest półgrupą i $a, b, c, d \in A$, to zapis

$$a \cdot b \cdot c \cdot d \tag{1.1}$$

jest jednoznaczny, bo

$$a \cdot (b \cdot (c \cdot d)) = (a \cdot b) \cdot (c \cdot d) = (a \cdot ((b \cdot c) \cdot d) = \dots \tag{1.2}$$

co niekoniecznie zachodzi w magmie. Własność tę można udowodnić indukcyjnie.

Jeśli w półgrupie działanie oznaczamy przez $\cdot$, to zwykle nie będziemy go zapisywać. To znaczy, zamiast pisać $x \cdot y$ będziemy pisać xy.

Definicja 1.1.3. Monoidem nazywamy trójkę $(A, \star, e)$, że $(A, \star)$ jest półgrupą, a $e \in A$ jest **elementem neutralnym** działania $\star$, t.j. takim, że

$$\forall_{x \in A}\ e \star x = x = x \star e. \tag{1.3}$$

Element e nazywamy zwykle **jednością**, **jedynką** lub **zerem**, zależnie od kontekstu. Jeśli element ten będzie wiadomy z kontekstu, to nie będziemy o nim wspominać

Przykład 1.1.7. $(\mathbb{Z}, +, 0)$ jest monoidem.

Przykład 1.1.8. $(\mathbb{N}_+, +)$ *nie* jest monoidem, bo nie jest trójką, tylko parą. Ale nawet gdybyśmy chcieli, to nie zrobimy z tego zbioru i działania monoidu, bo nie ma dodatniej liczby naturalnej n, że $n + a = a$ dla każdego $a \in \mathbb{N}_+$.

Przykład 1.1.9. Ciągi znaków (*stringi*) z operacją konkatenacji i pustym ciągiem tworzą monoid.

Przykład 1.1.10. $\left(\mathbb{R}^{2\times 2}, \cdot, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$ jest monoidem.

~~**Przykład 1.1.?** Monada jest monoidem w kategorii endofunktorów.~~

Jeśli ktoś kiedyś słyszał lub usłyszy o powyższym stwierdzeniu, często żartobliwie przytaczanym jako „proste" wytłumaczenie, czym jest monada, to zapewniam, że jest ono prawdziwe. Chodzi tam jednak o inny monoid, znacznie uogólniony w stosunku do naszego.

Definicja 1.1.4. Grupą nazywamy czwórkę $(A, \star, e, \mathrm{inv})$, że $(A, \star, e)$ jest monoidem, a $\mathrm{inv} : A \to A$ jest funkcją przypisującą każdemu elementowi jego **odwrotność**, to znaczy spełniającą warunek

$$\forall_{x \in A}\ x \star \mathrm{inv}(x) = e = \mathrm{inv}(x) \star x.$$

Podobnie jak w przypadku monoidu, jeśli jedność i funkcja odwrotności będzie oczywista, to nie będziemy o niej wspominać.

Przykład 1.1.11. Czwórka $(\mathbb{Q}, +, 0, (-\cdot))$, czyli liczby wymierne z dodawaniem, zerem i negacją, jest grupą.

Przykład 1.1.12. Używając uproszczonej terminologii, zbiór

$$\{A \in \mathbb{R}^{2\times 2} | \det(A) \neq 0\} \tag{1.4}$$

ze standardowym mnożeniem macierzy stanowi grupę.

Przykład 1.1.13. Zbiór $\mathbb{R}^{n\times n}$ dla ustalonego $n > 1$ nie stanowi grupy ze standardowym mnożeniem macierzy, gdyż nie każdy element ma odwrotność. Ten sam zbiór z dodawaniem macierzy jest już jednak grupą—odwrotnościami są negacje macierzy.

Przemienność.

Jeśli w którejś ze zdefiniowanych przez nas struktur działanie $\star$ jest przemienne, to znaczy

$$\forall_{x,y\in A}\ x \star y = y \star x, \tag{1.5}$$

to strukturę tę nazywamy przemienną. Mamy więc **przemienne magmy**, **przemienne półgrupy**, **przemienne monoidy** i **przemienne grupy**. Grupy przemienne nazywa się jednak zwykle **grupami abelowymi**, od nazwiska norweskiego matematyka Nielsa Henrika Abela, 1802–1829. „Abelowy" piszemy jednak z małej litery (z wyjątkiem początku zdania), gdyż jest to przymiotnik.

Przykład 1.1.14. $\mathbb{N}$ z dodawaniem jest półgrupą przemienną.

Przykład 1.1.15. $\mathbb{Q} \setminus \{0\}$ z mnożeniem jest grupą abelową.

Przykład 1.1.16. Zbiór ciągów znakowych z konkatenacją *nie* jest monoidem przemiennym—w konkatenacji kolejność ma znaczenie.

1.1.1 Złożone struktury.

Używając zdefiniowanych przez nas prostych struktur algebraicznych możemy definiować bardziej złożone, składające się z wielu działań (ale nadal tylko jednego zbioru).

Definicja 1.1.5. Pierścieniem nazywamy szóstkę $(P, +, 0, \mathrm{neg}, \cdot, 1)$, że $(P, +, 0, \mathrm{neg})$ jest grupą abelową, a $(P, \cdot, 1)$ jest monoidem, oraz zachodzą równania

$$\forall_{a,b,c\in P} a \cdot (b + c) = a \cdot b + a \cdot c \tag{1.6}$$

$$\forall_{a,b,c\in P} (a + b) \cdot c = a \cdot c + b \cdot c \tag{1.7}$$

W pierścieniu mamy już nie jedno, a dwa działania. Tworzą one niezależnie od siebie grupę abelową i monoid, ale dodatkowo łączy jest **rozdzielność**, czyli równania (1.6) i (1.7).

Przykład 1.1.17. Liczby całkowite z dodawaniem i mnożeniem tworzą pierścień. Jest to podstawowy przykład i inspiracja dla definicji pierścienia.

Przykład 1.1.18. Niech $P(\mathbb{R})$ będzie zbiorem wielomianów o współczynnikach z $\mathbb{R}$. Wtedy $P(\mathbb{R})$ z dodawaniem i mnożeniem wielomianów tworzy pierścień.

Dodatkowo możemy zdefiniować, że pierścień $(P, +, 0, \text{neg}, \cdot, 1)$ jest przemienny, jeśli działanie $\cdot$ jest przemienne. Przemienność $+$ jest natomiast wymagana już przez samą definicję pierścienia.

Definicja 1.1.6. Ciałem nazywamy siódemkę $(K, +, 0, \text{neg}, \cdot, 1, \text{inv})$, że $(K, +, 0, \text{neg}, \cdot, 1)$ jest pierścieniem, a $(K \setminus \{0\}, \cdot, 1, \text{inv})$ jest grupą abelową.

Przykład 1.1.19. $\mathbb{Q}$ z dodawaniem i mnożeniem tworzy ciało.

Przykład 1.1.20. $\mathbb{R}$ z dodawaniem i mnożeniem tworzy ciało.

Przykład 1.1.21. $\mathbb{Z}$ z dodawaniem i mnożeniem *nie* tworzy ciała—w liczbach całkowitych odwrotność względem mnożenia ma tylko 1.

1.1.2 Zadania.

Zadanie 1.1.1. Pokaż, że zbiór macierzy $\mathbb{R}^{2\times 2}$ z mnożeniem jest magmą, półgrupą, monoidem. Pokaż, że zbiór ten nie jest grupą.

Zadanie 1.1.2. Podaj przykład grupy, która nie jest przemienna.

Zadanie 1.1.3. Sprawdź, czy $(\mathbb{C}, +)$ jest grupą.

Zadanie 1.1.4. Czy $\mathbb{C}$ ze standardowym mnożeniem jest monoidem? Jeśli tak, to jaki jest element neutralny? Czy jest to grupa?

Zadanie 1.1.5. Niech A będzie dowolnym zbiorem. Które z definicji struktur algebraicznych spełnia zbiór funkcji $A \to A$ z operacją składania funkcji?

Zadanie 1.1.6. Sprawdź, które z definicji struktur algebraicznych spełnia zbiór ścieżek na płaszczyźnie (t.j. funkcji $[0, 1] \to \mathbb{R}^2$) z operacją łączenia ich swoimi końcami (tzn. dwie ścieżki możemy połączyć w jedną, wtedy i tylko wtedy gdy pierwsza kończy się tam, gdzie druga się zaczyna).

Zadanie 1.1.7. Udowodnij, że $\mathbb{R}^{2\times 2}$ ze standardowym dodawaniem i mnożeniem macierzy tworzy pierścień.

Zadanie 1.1.8. Zapisz definicję ciała, nie używając definicji pierścienia.

Zadanie 1.1.9. Udowodnij, że liczby zespolone $\mathbb{C}$ są ciałem.

Zadanie 1.1.10. Dlaczego zdefiniowaliśmy przemienne warianty każdej ze struktur, ale nie ciał?

Zadanie 1.1.11. Niech $(A, \cdot, e, \text{inv})$ będzie dowolną grupą. Udowodnij, że dla każdego $x \in A$ zachodzi $x^{-1^{-1}} = x$.

Zadanie 1.1.12. Niech $(A, \cdot, e)$ będzie dowolnym monoidem. Niech $y \in A$. Udowodnij, że jeśli dla każdego $x \in A$ zachodzi

$$yx = x, \tag{1.8}$$

lub

$$xy = x, \tag{1.9}$$

to $y = e$. Pokazuje to, że mając dane działanie, istnieje conajwyżej jeden element neutralny.

Zadanie 1.1.13. Niech $(A, \cdot, e, \mathrm{inv})$ będzie dowolną grupą. Niech $x \in A$. Udowodnij, że jeśli dla pewnego $y \in A$ zachodzi

$$yx = e, \tag{1.10}$$

lub

$$xy = e, \tag{1.11}$$

to $y = \mathrm{inv}(x)$. Pokazuje to, że mając dane działanie i element neutralny, dla każdego elementu istnieje conajwyżej jeden sposób zdefiniowania odwrotności.

1.2 Algebra Uniwersalna.

Wejdziemy teraz na nieco wyższy poziom abstrakcji. Szybko jednak zobaczymy, że znacząco ułatwi nam to posługiwanie się strukturami, które zdefiniowaliśmy.

Na czym polega problem? Poznane przez nas struktury algebraiczne wyglądają wszystkie bardzo podobnie. Mamy zbiór, pewne stałe i operacje wykonywane na tym zbiorze. Możemy się już domyślać, że będziemy mieli wiele bardzo podobnych twierdzeń i definicji dla każdej ze zdefiniowanych struktur.

Przykładowo, w algebrze występuje pojęcie **homomorfizmu**—funkcji $h : A \to B$ między dwoma strukturami tego samego typu (np. między dwoma grupami, dwoma monoidami itd.), które dodatkowo spełniają pewne warunki. Zwykle jednym z nich jest (jeśli $(A, \star, \dots)$ i $(B, \bullet, \dots)$ są jakimiś strukturami)

$$h(a \star b) = h(a) \bullet h(b). \tag{1.12}$$

Ale definicje homomorfizmów mają też więcej wymagań. W przypadku monoidów $(A, \star, e_A)$, $(B, \star, e_B)$ chcemy aby zachodziło też

$$h(e_A) = e_B. \tag{1.13}$$

W przypadku grup podobna własność musi zachodzić też dla odwracalności.

Najczęściej homomorfizmy definiuje się osobno dla każdej struktury. W trakcie studiów spotkaliśmy się już z przykładem homomorfizmu—mowa o przekształceniach liniowych (przestrzenie liniowe też są strukturą algebraiczną!). Nasuwa się jednak pytanie: czy nie dałoby się uogólnić tego, abyśmy mieli tylko jedną definicję? Chcielibyśmy mieć coś takiej postaci:

Definicja. **Homomorfizmem** struktur $(A, \dots)$ i $(B, \dots)$ nazywamy funkcję $h : A \to B$, spełniającą warunki …

Ciężko jednak powiedzieć, co należałoby wstawić w miejsce kropek, aby sformalizować tę definicję. Podobna sytuacja zajdzie, kiedy zechcemy zacząć definiować **podprzestrzenie liniowe**, **podgrupy**, **podciała**, **podmonoidy** itd. Definicje tych obiektów byłyby do siebie bardzo podobne. Jak jednak zawrzeć je wszystkie w jednej definicji? Odpowiedzi na te pytania dostarcza nam dziedzina algebry zwana *Algebrą Uniwersalną*.

1.2.1 Podstawowe definicje.

Definicja 1.2.1. Niech A będzie zbiorem. Mówimy, że funkcja $f : A^n \to A$ ma **arność** n (od końcówki *-arny*, a to z łacińskiej końcówki *-aris*, w analogii do bin*arny*, tern*arny*, itd.).

Ciekawa i przydatna własność zachodzi, gdy w powyższej definicji $n = 0$. Zbiór A^0 definiuje się jako zbiór jednoelementowy (co jest tym jednym elementem nie ma znaczenia). Funkcja $f : A^0 \to A$ jest więc funkcją ze zbioru jednoelementowego w zbiór A. Możemy więc na nią patrzeć jak na pojedynczą stałą (bo zbiór wartości też jest jednoelementowy).

Definicja 1.2.2. Algebrą nazywamy trójkę (Σ, α, E), gdzie

- Σ jest zbiorem, zwanym zbiorem **symboli**,
- $\alpha : \Sigma \to \mathbb{N}$ jest funkcją, która każdemu symbolowi przypisuje arność,
- E jest zbiorem równań używających zmiennych i symboli z Σ jako funkcji.

Parę (Σ, α) nazywamy **sygnaturą** algebry (Σ, α, E).

Definicja ta nie jest w pełni formalna (czym są „symbole"? czym są „zmienne"? co znaczy, że elementów Σ używamy jako funkcji? jak możemy czemuś, co nie jest funkcją, przypisać arność?). Sformalizowanie jej jednak wprowadziłoby więcej zamieszania niż pożytku, gdyż wymagałoby wprowadzenia mało istotnych, technicznych szczegółów. Zamiast tego przejdziemy do rozjaśniającego przykładu.

Przykład 1.2.1. Trójka (Σ, α, E), gdzie

- $\Sigma = \{f, g, e\}$,
- $\alpha : f \mapsto 2, g \mapsto 2, e \mapsto 0$,
- $E = \{g(x, y) = g(y, x), f(e, x) = x, f(x, e) = x\}$

jest algebrą.

Jak możemy interpretować, czym jest taka algebra? Jest to nic innego jak definicja pewnej struktury algebraicznej, gdzie mamy dwie operacje dwuargumentowe f, g i jedną wyróżnioną stałą e, że g jest przemienne, a e jest elementem neutralnym dla f.

Tłumacząc powyższy zapis na tradycyjną definicję, moglibyśmy napisać następująco.

Definicja 1.2.3. Gałganem nazywamy czwórkę (A, f, g, e), gdzie A jest zbiorem, $f, g : A^2 \to A$ są funkcjami dwuargumentowymi, $e \in A$ (lub, co w pewnym sensie jest równoważne, $e : \{0\} \to A$) i spełnione są następujące warunki:

- $\forall_{x \in A}\ f(e, x) = x$,
- $\forall_{x \in A}\ f(x, e) = x$,

- $\forall_{x,y\in A}\ g(x,y) = g(y,x)$.

Zwykle zapis będziemy jednak upraszczać, podając jednocześnie zbiór symboli Σ i funkcję α za jednym razem, n.p. w postaci

$$\Sigma = \{f^2, g^2, e\}, \tag{1.14}$$

t.j. podając w definicji symboli ich arność w indeksie górnym, i pomijając ją dla 0. Idąc tą konwencją będziemy też zamiast (Σ, α, E) pisać (Σ, E).

Algebry odpowiadają więc definicjom struktur. Co odpowiada jednak obiektom, spełniającym te definicje?

Definicja 1.2.4. Modelem algebry (Σ, α, E) nazywamy zbiór A (zwany **nośnikiem**), wraz z interpretacją symboli z Σ jako funkcje o arnościach definiowanych przez α i spełniających równania E.

Znowu nie jest to całkowicie formalna definicja, na nasze potrzeby jednak w pełni wystarczy.

Przykład 1.2.2. Zbiór $\mathbb{R}$ z działaniami $f(x,y) = x+y$, $g(x,y) = xy$ jest modelem gaugana.

Możemy teraz definiować nasze struktury w taki sam sposób jak gaugana.

Definicja 1.2.5. Monoidem nazywamy dowolny model algebry

$$(\{\star^2, e\}, \{x \star (y \star z) = (x \star y) \star z, x \star e = x, e \star x = x\}).$$

Ważne, aby rozróżniać teraz dwa pojęcia: algebrą jest *definicja* monoidu. Modelem algebry jest natomiast dowolny monoid, czyli obiekt, który spełnia tę definicję.

Algebra uniwersalna nie jest jednak taka uniwersalna, jak byśmy chcieli. Jedna z podanych przez nas w poprzedniej sekcji definicji nie stanowi algebry. Mowa tutaj o ciałach. Problemem jest to, że funkcja inv nie musi być określona dla elementu neutralnego dodawania w ciele. Jest to warunek, którego nie da się sformułować używając pojęcia algebry. Z tego powodu ciała będziemy musieli traktować osobno od pozostałych struktur.

1.2.2 Zadania.

Zadanie 1.2.1. Zapisz definicję magmy w postaci algebry.

Zadanie 1.2.2. Zapisz definicję półgrupy w postaci algebry.

Zadanie 1.2.3. Zapisz definicję grupy w postaci algebry.

Zadanie 1.2.4. Zapisz definicję grupy abelowej w postaci algebry.

Zadanie 1.2.5. Zapisz definicję pierścienia w postaci algebry.

1.3 Pewne definicje związane z algebrami.

Wprowadzimy teraz definicje, które dzięki pojęciu algebry będą miały sens dla wszystkich struktur, które są modelami algebr.

1.3.1 Podalgebry.

Definicja 1.3.1. Podmodelem modelu M algebry (Σ, E) nazywamy podzbiór $N \subseteq M$, który jest modelem algebry (Σ, E) z tymi samymi operacjami co M.

Przykład 1.3.1. $2\mathbb{N}$, czyli liczby parzyste naturalne stanowią podpółgrupę liczb naturalnych z dodawaniem.

Przykład 1.3.2. $\mathbb{Q}\backslash\{0\}$ stanowi podgrupę przemienną grupy przemiennej $\mathbb{R}\backslash\{0\}$ z mnożeniem.

1.3.2 Homomorfizmy.

Definicja 1.3.2. Niech $\mathfrak{A} = (\Sigma, E)$ będzie algebrą. **Homomorfizmem** (lub **morfizmem**) modeli $\mathfrak{A}$ nazywamy dowolną funkcję $h : A \to B$, gdzie A, B są dowolnymi modelami $\mathfrak{A}$, i dla każdego symbolu $f^n \in \Sigma$ o arności n, któremu w A odpowiada funkcja $f_A : A^n \to A$, a w B funkcja $f_B : B^n \to B$, zachodzi

$$\forall_{x_1,\ldots,x_n \in A}\ h(f_A(x_1, \ldots, x_n)) = f_B(h(x_1), \ldots, h(x_n)). \tag{1.15}$$

Przykład 1.3.3. Funkcja

$$f : \mathbb{Q} \to \mathbb{R},$$
$$f(x) = 5x,$$

jest homomorfizmem grup $\mathbb{Q}$ i $\mathbb{R}$ z dodawaniem. Rzeczywiście, dla każdych $x, y \in \mathbb{Q}$ mamy

$$5 \cdot (x + y) = 5x + 5y, \tag{1.16}$$
$$5 \cdot (-x) = -(5 \cdot x), \tag{1.17}$$
$$5 \cdot 0 = 5 \cdot 0. \tag{1.18}$$

Przykład 1.3.4. Funkcja

$$f : \mathbb{R}_+ \to \mathbb{R},$$
$$f(x) = \log(x)$$

jest homomorfizmem grup $\mathbb{R}_+$ z mnożeniem i $\mathbb{R}$ z dodawaniem. Rzeczywiście, dla każdych $x, y \in \mathbb{R}_+$ mamy

$$\log(x \cdot y) = \log(x) + \log(y), \tag{1.19}$$
$$\log(x^{-1}) = -\log(x), \tag{1.20}$$
$$\log(1) = 0. \tag{1.21}$$

Z pewnych niewyjaśnionych powodów, w przypadku homomorfizmów nie używa się pojęć takich jak iniekcja, bijekcja i surjekcja. Zamiast tych pochodzących z francuskiego wyrazów mamy greckie odpowiedniki.

Definicja 1.3.3. Homomorfizm nazywamy

- **epimorfizmem**, jeśli jest surjekcją,
- **monomorfizmem**, jeśli jest iniekcją,
- **izomorfizmem**, jeśli jest bijekcją,
- **endomorfizmem**, jeśli jego dziedzina i kodziedzina są równe, t.j. jest postaci $h : A \to A$,
- **automorfizmem**, jeśli jest endomorfizmem i izomorfizmem.

Lemat 1.3.1. Niech $\mathfrak{A} = (\Sigma, E)$ będzie algebrą. Niech A, B, C będą modelami $\mathfrak{A}$, a $h : A \to B$, $g : B \to C$ homomorfizmami tych modeli. Wtedy $g \circ h : A \to C$ jest homomorfizmem.

Dowód. Niech $f^n \in \Sigma$ będzie n-arnym symbolem, a f_A, f_B, f_C odpowiadającymi mu funkcjami w odpowiednio A, B, C. Mamy teraz dla dowolnych $x_1, \ldots, x_n \in A$

$$\begin{aligned}
(g \circ h)(f_A(x_1, \ldots, x_n)) &= && (1.22)\\
&= g(h(f_A(x_1, \ldots, x_n)) && (1.23)\\
&= g(f_B(h(x_1), \ldots, h(x_n))) && (1.24)\\
&= f_C(g(h(x_1)), \ldots, g(h(x_n)))) && (1.25)\\
&= f_C((g \circ h)(x_1), \ldots, (g \circ h)(x_n)))), && (1.26)
\end{aligned}$$

co pokazuje, że $(g \circ h)$ jest homomorfizmem. □

Lemat 1.3.2. Jeśli $h : A \to B$ jest izomorfizmem dwóch modeli algebry $\mathfrak{A} = (\Sigma, E)$, to funkcja odwrotna $h^{-1} : B \to A$ istnieje i też jest izomorfizmem.

Dowód. Istnienie h^{-1} i to, że jest bijekcją, jest oczywiste z faktu, że h jest bijekcją. Wystarczy więc pokazać, że h^{-1} jest homomorfizmem. Dla dowolnego symbolu $f^n \in \Sigma$ reprezentowanego przez funkcje $f_A : A^n \to A$ i $f_B : B^n \to B$, i dowolnych $x_1, \ldots, x_n \in B$ mamy

$$\begin{aligned}
h(f_A(h^{-1}(x_1), \ldots, h^{-1}(x_n))) &= && (1.27)\\
&= f_B(h(h^{-1}(x_1)), \ldots, h(h^{-1}(x_n))) && (1.28)\\
&= f_B(x_1, \ldots, x_n) && (1.29)\\
&= h(h^{-1}(f_B(x_1, \ldots, x_n))). && (1.30)
\end{aligned}$$

Ale ponieważ h jest iniekcją, to

$$f_A(h^{-1}(x_1), \ldots, h^{-1}(x_n)) = h^{-1}(f_B(x_1, \ldots, x_n)), \tag{1.31}$$

czyli h^{-1} jest homomorfizmem. □

Definicja 1.3.4. Mówimy, że modele A, B algebry (Σ, E) są **izomorficzne**, jeśli istnieje izomorfizm $f : A \to B$. Fakt ten zapisujemy $A \cong_f B$ lub po prostu $A \cong B$.

Jeśli dwa modele są izomorficzne, to w pewnym sensie są identyczne—różnią się tylko formą zapisu. Poza tym wszystkie algebraiczne własności, które zachodzą w jednym modelu, zachodzą też w drugim. W niektórych dziedzinach matematyki izomorficzne modele identyfikuje się tak bardzo, że zamiast używać znaku $A \cong B$ używa się zwykłej równości $=$. My jednak zostaniemy przy $\cong$.

Przykład 1.3.5. $\mathbb{R}$ z dodawaniem jest grupą abelową izomorficzną z grupą abelową $\mathbb{R}^{1\times 1}$ z dodawaniem macierzy. Izomorfizmem jest tu funkcja

$$f : \mathbb{R} \to \mathbb{R}^{1\times 1},$$
$$f(x) = [x].$$

Przykład 1.3.6. $\mathbb{Z}$ z dodawaniem (ozn. $\mathbb{Z}^+$) jako monoid nie jest izomorficzne z $\mathbb{Z}$ z mnożeniem (ozn. $\mathbb{Z}^*$) jako monoid.

Dowód. Przypuśćmy, że istnieje izomorfizm $f : \mathbb{Z}^+ \to \mathbb{Z}^*$. Istnieje więc też odwrotność tego izomorfizmu f^{-1}, która też jest izomorfizmem. Mamy zatem

$$f^{-1}(1) = 0 = 1 + (-1) = f^{-1}(f(1)) + f^{-1}(f(-1)) = f^{-1}(f(1) \cdot f(-1)). \quad (1.32)$$

Skoro f^{-1} jest izomorfizmem, to

$$1 = f(1) \cdot f(-1), \quad (1.33)$$

więc

$$f(1) = 1 = f(-1) \text{ lub } f(1) = -1 = f(-1). \quad (1.34)$$

Wtedy jednak korzystając z tego, że f jest izomorfizmem dostajemy $1 = -1$, co jest sprzecznością. □

1.3.3 Wolne algebry.

Definicja 1.3.5. Wolnym modelem algebry (Σ, E) generowanym przez zbiór G (tak zwany **zbiór generatorów**), nazywamy model algebry (Σ, E), którego nośnikiem jest zbiór wszystkich wyrażeń, które utworzyć możemy z elementów Σ i G, traktują elementy Σ jak funkcje z odpowiednimi arnościami. Dodatkowo, dwa wyrażenia uznajemy za równe, jeśli jedno możemy przekształcić w drugie używając równań z E.

Mówimy też, że model jest *nad zbiorem* G. Znowu nie jest to w pełni formalna definicja, jednak bardzo intuicyjnie oddająca istotę wolnych modeli. Definicja w pełni formalna wymagałaby albo wprowadzenia pewnych formalnych pojęć, których nie będziemy wprowadzać (np. ilorazy modeli przez podmodele), albo byłaby bardzo abstrakcyjna (pojęcie własności uniwersalnych).

Zwykle jako zbiór G bierze się pewne formalne symbole, czyli jakieś litery.

Przykład 1.3.7. Grupą wolną na zbiorze $\{a\}$ nazywamy grupę, której elementami są $e, a, a^{-1}, a^2, a^{-2}, \ldots$. Zachodzą w niej m.in. równości

$$aa^{-1} = e \tag{1.35}$$

$$eae = a \tag{1.36}$$

$$a^{-1}a = e \tag{1.37}$$

W pewnym sensie grupą wolną na zbiorze G jest najprostrza grupa, która zawiera całe G jako swoje elementy. Najprostsza, bo nie zachodzą w niej inne równania, niż te, które stanowią aksjomaty grupy, oraz te, które można z nich wyprowadzić. Podobnie jest dla innych struktur algebraicznych.

Przykład 1.3.8. $\mathbb{Z}$ wraz z dodawaniem stanowi wolną grupę przemienną nad zbiorem $\{1\}$.

Przykład 1.3.9. Zbiór skończonych ciągów liczb z $\mathbb{N}$ z konkatenacją stanowi wolny monoid nad $\mathbb{N}$.

Przykład 1.3.10. $\mathbb{Z}$ wraz z mnożeniem nie stanowi wolnej grupy przemiennej, bo dla dowolnego elementu x mamy

$$0x = 0 \tag{1.38}$$

czego nie możemy wyprowadzić z aksjomatów grupy przemiennej. Wystarczy podać grupę przemienną, w której nie ma elementu, który działa tak jak 0 w $\mathbb{Z}$ z mnożeniem. Jest nią przykładowo $\mathbb{Z}$ z dodawaniem.

1.3.4 Zadania.

Zadanie 1.3.1. Zapisz definicję homomorfizmu monoidów nie używając pojęć algebry uniwersalnej.

Zadanie 1.3.2. Zapisz definicję homomorfizmu grup nie używając pojęć algebry uniwersalnej.

Zadanie 1.3.3. Sprawdź, czy następujące funkcje

1. $f(x) = 2x$,
2. $g(x) = 2 + x$
3. $h(x) = x^2$,

są endomorfizmami w

1. monoidzie $\mathbb{Z}$ z mnożeniem,
2. grupie $\mathbb{Z}$ z dodawaniem.

Zadanie 1.3.4. Niech $(A,+),(B,\cdot)$ będą dowolnymi grupami. Udowodnij, że jeśli $f : A \to B$ jest funkcją spełniającą

$$f(x+y) = f(x) \cdot f(y) \tag{1.39}$$

dla każdych $x, y \in A$, to f jest homomorfizmem grup.

Zadanie 1.3.5. Udowodnij, że jeśli $\mathfrak{A}$ jest algebrą, a $\mathcal{A}$ zbiorem modeli $\mathfrak{A}$, to relacja $\cong$ na elementach $\mathcal{A}$ jest relacją równoważności.

Zadanie 1.3.6. Niech A będzie grupą abelową, a B dowolną grupą. Udowodnij, że jeśli $f : A \to B$ jest epimorfizmem, to B jest grupą abelową.

Zadanie 1.3.7. Udowodnij, że jeśli A, B są zbiorami i $|A| = |B|$, to grupa wolna nad A i grupa wolna nad B są izomorficzne.

1.4 Kongruencje.

Przejdziemy teraz do nieco bardziej abstrakcyjnego pojęcia, tak zwanych kongruencji. Mówiąc nieformalnie, są to relacje równoważności na modelach algebr, które są spójne ze strukturą tych modeli.

Definicja 1.4.1. Niech $\mathfrak{A} = (\Sigma, E)$ będzie algebrą, A modelem $\mathfrak{A}$, a $\sim$ dowolną relacją równoważności na A. Wtedy $\sim$ jest **kongruencją**, jeśli dla każdego symbolu $f^n \in \Sigma$, reprezentującej go funkcji $f : A^n \to A$ i

$$x_1, \ldots, x_n,\ y_1, \ldots, y_n \in A \tag{1.40}$$

zachodzi

$$x_1 \sim y_1, \ldots, x_n \sim y_n \implies f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n). \tag{1.41}$$

Czyli kongruencja jest relacją równoważności, która zachowuje równoważność przy nakładaniu funkcji reprezentujących symbole algebry.

Przykład 1.4.1. Rozważmy monoid ciągów znaków z konkatenacją. Relacja, która identyfikuje dwa ciągi, jeśli ich długość jest taka sama, jest kongruencją.

Przykład 1.4.2. Rozważmy $\mathbb{Z}$ jako pierścień z dodawaniem i mnożeniem. Dla dowolnej liczby $n \in \mathbb{N}$ relacja $\sim$ zdefiniowana przez warunek

$$\forall_{x,y\in\mathbb{Z}}\ x \sim y \iff x \mod n = y \mod n \tag{1.42}$$

jest kongruencją.

Twierdzenie 1.4.1. Niech $\mathfrak{A} = (\Sigma, E)$ będzie algebrą, A jej modelem i $\sim$ kongruencją na A. Wtedy $A/_\sim$ też jest modelem $\mathfrak{A}$.

Dowód. Musimy pokazać, że istnieją interpetacje symboli z Σ jako funkcje nad A z odpowiednimi arnościami, i że spełnione są przy tym wszystkie równania z E. Niech $f^n \in \Sigma$ będzie dowolnym symbolem arności n, któremu odpowiada funkcja f w A. Zdefiniujemy teraz odpowiadającą mu funkcję $f_\sim$ na $A/_\sim$ jako

$$f_\sim([x_1]_\sim, \ldots, [x_n]_\sim) = [f(x_1, \ldots, x_n)]_\sim. \tag{1.43}$$

Musimy jednak pokazać, że definicja $f_\sim$ jest niezależna od wybranych reprezentantów klas $[x_1]_\sim, \ldots, [x_n]_\sim$. Weźmy więc dowolne

$$x_1, \ldots, x_n,\ y_1, \ldots, y_n \in A \tag{1.44}$$

takie, że $x_i \sim y_i$ dla każdego $i = 1, \ldots, n$, czyli $[x_i]_\sim = [y_i]_\sim$. Mamy teraz

$$[f(x_1, \ldots, x_n)]_\sim = [f(y_1, \ldots, y_n)]_\sim, \tag{1.45}$$

ponieważ z definicji kongruencji mamy

$$x_1 \sim y_1, \ldots, x_n \sim y_n \implies f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n). \tag{1.46}$$

Oznacza to, że definicja $f_\sim$ nie jest zależna od wybranych reprezentantów klas $[x_1]_\sim, \ldots, [x_n]_\sim$, czyli poprawnie zdefiniowaliśmy funkcje na $A/_\sim$ odpowiadające symbolom z Σ.

Dowód, że funkcje te spełniają równania z E, pozostawiamy jako zadanie dla czytelnika (zad. 1.4.1–1.4.2). □

Definicja 1.4.2. Jądrem homomorfizmu $h : A \to B$ nazywamy relację określoną wzorem

$$x \equiv_h y \iff h(x) = h(y). \tag{1.47}$$

Definicja ta nie do końca zgadza się z tym, czego mogliśmy się kiedyś dowiedzieć. Czy jądrem nie powinien być zbiór miejsc zerowych? Dlaczego tutaj jest to relacja? Na te pytania odpowiemy niedługo.

Lemat 1.4.1. Niech $\mathfrak{A} = (\Sigma, E)$ będzie algebrą, a A, B jej modelami. Niech $h : A \to B$ będzie homomorfizmem. Wtedy jego jądro $\equiv_h$ jest kongruencją.

Dowód. Fakt, że $\equiv_h$ jest relacją równoważności, pozostawiamy dla czytelnika (zad. 1.4.3). Zakładając jego prawdziwość pokażemy, że $\equiv_h$ jest kongruencją.

Niech $f^n \in \Sigma$ będzie dowolnym symbolem arności n, a f_A, f_B odpowiadającymi mu funkcjami na odpowiednio A, B. Weźmy dowolne

$$x_1 \ldots, x_n,\ y_1, \ldots, y_n \in A \tag{1.48}$$

spełniające

$$x_1 \equiv_h y_1, \ldots, x_n \equiv_h y_n \tag{1.49}$$

Chcemy pokazać, że

$$f_A(x_1, \ldots, x_n) \equiv_h f_A(y_1, \ldots, y_n). \tag{1.50}$$

Z założenia i definicji jąda mamy

$$h(x_1) = h(y_1), \ldots, h(x_n) = h(y_n), \tag{1.51}$$

czyli

$$f_B(h(x_1), \ldots, h(x_n)) = f_B(h(y_1), \ldots, h(y_n)), \tag{1.52}$$

co z faktu, że h jest homorfizmem daje

$$h(f_A(x_1, \ldots, x_n)) = h(f_A(y_1, \ldots, y_n)), \tag{1.53}$$

co jest z definicji równoważne udowadnianej przez nas własności. □

Skoro jądro homomorfizmu $h : A \to B$ jest relacją równoważności, to dzieli ono A na klasy równoważności. Jeśli algebra, której A i B są modelami ma jakiś element e, który nazwać możemy jednością (czyli np. operujemy na monoidach, grupach, przestrzeniach liniowych), to jądrem możemy też nazywać klasę abstrakcji zawierającą ten element (co oznaczać będziemy przez $\operatorname{Ker} h$). Takie spojrzenie jest zgodne z tym, że jądro jest zbiorem „miejsc zerowych" homomorfizmu:

$$\begin{aligned} [e]_{\equiv_h} &= && (1.54)\\ &= \{x \in A | x \equiv_h e\} && (1.55)\\ &= \{x \in A | h(x) = h(e)\} && (1.56)\\ &= \{x \in A | h(x) = e\} && (1.57)\\ &= \operatorname{Ker} h. && (1.58) \end{aligned}$$

Pojęciem dualnym do jądra jest obraz homomorfizmu $\operatorname{Im} h$. Jest to nic innego, jak zbiór wartości. Obraz oczywiście nie musi być równy przeciwdziedzinie. Jeśli jest, to h jest epimorfizmem. Jak się okazuje, obrazy, podobnie jak jądra (zad. 1.4.4) są podmodelami.

Lemat 1.4.2. Niech $h : A \to B$ będzie homomorfizmem. Zbiór wartości $\operatorname{Im} h$ jest wtedy podmodelem B.

Dowód. Musimy pokazać, że funkcje na B odpowiadające symbolom z Σ możemy ograniczyć do $\operatorname{Im} h$, czyli że dla argumentów z $\operatorname{Im} h$ przyjmują wartości z $\operatorname{Im} h$. Niech więc $f^n \in \Sigma$ będzie n-arnym symbolem, a f_A, f_B odpowiadającymi mu funkcjami na odpowiednio A, B. Niech $y_1, \ldots, y_n \in \operatorname{Im} h$. Istnieją więc $x_1, \ldots, x_n \in A$, że

$$y_1 = h(x_1), \ldots, y_n = h(x_n). \tag{1.59}$$

Mamy więc

$$f_B(y_1, \ldots, y_n) = f_B(h(x_1), \ldots, h(x_n)) = h(f_A(x_1, \ldots, x_n)), \tag{1.60}$$

co znaczy, że $f_B(y_1, \ldots, y_n) \in \operatorname{Im} h$. □

Gotowi jesteśmy teraz, by zapostulować i udowodnić centralne twierdzenie tego skryptu, które mówi, jak dokładnie działają homomorfizmy.

Twierdzenie 1.4.2. Niech $h : A \to B$ będzie homomorfizmem. Wtedy

$$h_* : A/_{\equiv_h} \to \operatorname{Im} h, \tag{1.61}$$

zdefiniowany jako

$$h_*([x]_{\equiv_h}) = h(x), \tag{1.62}$$

jest izomorfizmem.

Dowód. Definicja h_* jest poprawna, t.j. nie zależy od wyboru reprezentanta klasy. Wynika to bezpośrednio z definicji jądra. Jeśli $x \equiv_h y$, to $h(x) = h(y)$.

Pokażemy, że h_* jest homomorfizmem. Jeśli $f^n \in \Sigma$ jest n-arnym symbolem i odpowiadają mu w $A, B, A/_{\equiv_h}, \operatorname{Im} h$ odpowiednio funkcje $f_A, f_B, f_{A/_{\equiv_h}}, f_{\operatorname{Im} h}$, to

$$\begin{aligned}
h_*(f_{A/_{\equiv_h}}([x_1]_{\equiv_h}, \ldots, [x_n]_{\equiv_h})) &= && (1.63)\\
(\text{definicja } A/_{\equiv_h} \text{ jako modelu}) \quad &= h_*([f_A(x_1, \ldots, x_n)]_{\equiv_h}) && (1.64)\\
(\text{definicja } h_*) \quad &= h(f_A(x_1, \ldots, x_n)) && (1.65)\\
(h \text{ jest homomorfizmem}) \quad &= f_B(h(x_1), \ldots, h(x_n)) && (1.66)\\
(h(x_i) \in \operatorname{Im} h) \quad &= f_{\operatorname{Im} h}(h(x_1), \ldots, h(x_n)) && (1.67)\\
(\text{definicja } h_*) \quad &= f_{\operatorname{Im} h}(h_*([x_1]_{\equiv_h}), \ldots, h_*([x_n]_{\equiv_h})), && (1.68)
\end{aligned}$$

czyli h_* jest homomorfizmem.

Pozostaje pokazać, że h_* jest bijekcją. Załóżmy, że $h_*([x]_{\equiv_h}) = h_*([y]_{\equiv_h})$. Czyli

$$h(x) = h_*([x]_{\equiv_h}) = h_*([y]_{\equiv_h}) = h(y). \tag{1.69}$$

Więc $x \equiv_h y$ i tym samym $[x]_{\equiv_h} = [y]_{\equiv_h}$, czyli h_* jest monomorfizmem. Załóżmy teraz, że $y \in \operatorname{Im} h$. Czyli istnieje $x \in A$, że $h(x) = y$. Mamy więc

$$h_*([x]_{\equiv_h}) = h(x) = y, \tag{1.70}$$

czyli h_* jest epimorfizmem. h_* jest więc izomorfizmem. □

1.4.1 Zadania.

Zadanie 1.4.1. Niech $\mathfrak{A} = (\Sigma, E)$ będzie dowolną algebrą. Niech A będzie modelem $\mathfrak{A}$, a $\sim$ kongruencją na A. Udowodnij, że jeśli $F : A^n \to A$ jest funkcją zdefiniowaną przez wyrażenie składające się ze zmiennych i funkcji odpowiadającym wyrażeniom z Σ, to możemy zdefiniować $F_\sim : (A/_\sim)^n \to A/_\sim$ jako

$$F_\sim([x_1], \ldots, [x_n]) = [F(x_1, \ldots, x_n)], \tag{1.71}$$

tzn., że definicja ta nie zależy od wyboru reprezentantów klas abstrakcji.

Podpowiedź: indukcja po wysokości drzewa wyrażenia, które definiuje F. Przypadek bazowy jest już rozważony w dowodzie twierdzenia 1.4.1

Zadanie 1.4.2. Używając wyniku zadania 1.4.1 udowodnij brakującą część dowodu twierdzenia 1.4.1

Zadanie 1.4.3. Udowodnij, że jeśli $h : A \to B$ jest homomorfizmem, to jego jądro $\equiv_h$ jest relacją równoważności (korzystając tylko z definicji jądra).

Zadanie 1.4.4. Niech $h : A \to B$ będzie homomorfizmem dwóch modeli pewnej algebry. Udowodnij, że $\operatorname{Ker} h$ jest podmodelem A.

Zadanie 1.4.5. Sformułuj i udowodnij przypadek szczególny twierdzenia 1.4.2 dla monoidów.

Rozdział 2

Przestrzenie liniowe.

Przejdziemy teraz do przestrzeni liniowych. Kiedyś będzie tu więcej tekstu.

2.1 Definicja przestrzeni liniowej i powiązane definicje.

Definicja 2.1.1. Niech V, W będą przestrzeniami liniowymi nad ciałem $\mathbb{K}$ oraz niech $f : V \to W$ będzie przekształceniem liniowym. Jądrem przekształcenia f nazywamy zbiór

$$\ker f = \{v \in V : f(v) = 0\}. \tag{2.1}$$

2.1.1 Zadania.

2.2 Wartości własne macierzy.

W tej sekcji zakładamy, że pracujemy nad ciałem $\mathbb{C}$.

Definicja 2.2.1. *Wektorem własnym* macierzy $A \in \mathbb{C}^{n\times n}$ nazywamy niezerowy wektor $v \in \mathbb{C}^{n\times 1}$ taki, że dla pewnego $\lambda \in \mathbb{C}$

$$Av = \lambda v. \tag{2.2}$$

λ nazywamy *wartością własną* odpowiadającą wektorowi własnemu v.

Załóżmy, że daną mamy macierz $A \in \mathbb{C}^{n\times n}$ i chcemy wyznaczyć jej wektory i wartości własne. Jak możemy to zrobić? Przekształćmy równanie definiujące te pojęcia.

$$Av = \lambda v, \tag{2.3}$$
$$\mathbf{0} = \lambda v - Av, \tag{2.4}$$
$$\mathbf{0} = \lambda I v - Av, \tag{2.5}$$
$$\mathbf{0} = (\lambda I - A)v. \tag{2.6}$$

Oznacza to, że v jest wektorem własnym macierzy A z odpowiadającą mu wartością własną λ wtedy i tylko wtedy, gdy $(\lambda I - A)v = \mathbf{0}$, czyli wtedy i tylko wtedy, gdy $v \in \ker(\lambda I - A)$.

Skoro interesują nas tylko takie v, które są niezerowe, to warunek ten może być spełniony wtedy i tylko wtedy, gdy jądro $\ker(\lambda I - A)$ jest nietrywialne. Zachodzi to dokładnie wtedy, gdy $A - \lambda I$ jest macierzą nieodwracalną, czyli

$$\det(\lambda I - A) = 0. \tag{2.7}$$

Aby wyznaczyć wartości własne A, musimy więc sprawdzić, dla jakich $\lambda \in \mathbb{C}$ spełnione jest równanie 2.7. Okazuje się to dość proste, gdyż zawsze jest to równanie wielomianowe (zadanie 2.2.1). Kiedy to ustalimy, wyznaczyć możemy $\ker(A - \lambda I)$. Każdy wektor w tej przestrzeni liniowej będzie wektorem własnym A. Wielomian, który pojawia się w tym równaniu, ma swoją specjalną nazwę.

Definicja 2.2.2. *Wielomianem charakterystycznym* macierzy $A \in \mathbb{C}^{n\times n}$ nazywamy wielomian

$$\chi_A(t) = \det(tI - A). \tag{2.8}$$

Definicja 2.2.3. Krotnością algebraiczną wartości własnej λ macierzy $A \in \mathbb{C}^{n\times n}$ nazywamy krotność pierwiastka λ wielomianu χ_A.

Przykład 2.2.1. Niech

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix}. \tag{2.9}$$

Wyznaczymy wartości własne macierzy A oraz ich krotności. Mamy

$$\chi_A(t) = \det \begin{bmatrix} t & -1 & 0 \\ 0 & t & -1 \\ -2 & 5 & t-4 \end{bmatrix} \tag{2.10}$$

$$= t(t(t-4)+5) - 2 \tag{2.11}$$

$$= t^3 - 4t^2 + 5t - 2 \tag{2.12}$$

$$= (t-1)^2(t-2). \tag{2.13}$$

Stąd wartościami własnymi macierzy A są 1 i 2. Wartość własna 1 ma krotność algebraiczną 2, a wartość własna 2 ma krotność algebraiczną 1.

Definicja 2.2.4. Macierz $A \in \mathbb{C}^{n\times n}$ nazywamy *diagonalizowalną*, jeśli istnieje macierz odwracalna $X \in \mathbb{C}^{n\times n}$ i macierz diagonalna $D \in \mathbb{C}^{n\times n}$, taka, że

$$A = XDX^{-1}. \tag{2.14}$$

Macierz X w powyższym równaniu traktujemy jako macierz zmiany bazy, a o macierzy D mówimy wtedy jako o postaci diagonalnej macierzy A. Dla danej macierzy A istnieć może wiele różnych postaci diagonalnych! Nie są one unikalne.

Macierz jest diagonalizowalna wtedy i tylko wtedy, gdy ma n wektorów własnych, których zbiór jest liniowo niezależny. Liczba ta jest zwana *krotnością geometryczną* wartości własnej.

Przykład 2.2.2. Macierz

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.15}$$

nie jest diagonalizowalna. Wyznaczmy jej wartości własne. Ponieważ A jest macierzą górnotrójkątną, to jej wartości własne leżą na diagonali (zadanie 2.2.3). Mamy

$$\chi_A(t) = (t-1)^4. \tag{2.16}$$

Jedyną wartością własną macierzy A jest więc 1, o krotności algebraicznej 4. Dalej

$$A - I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{2.17}$$

skąd

$$\ker(A-I) = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ 0 \\ 0 \end{bmatrix} : x_1, x_2 \in \mathbb{C} \right\} \implies \dim(\ker(A-I)) = 2. \tag{2.18}$$

Krotność geometryczna wartości własnej 1 jest więc równa 2, więc macierz A nie jest diagonalizowalna.

Przykład 2.2.3. Macierz

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} \tag{2.19}$$

jest diagonalizowalna. Ponieważ A jest macierzą górnotrójkątną (zob. zadanie 2.2.3), mamy

$$\chi_A(t) = (t-1)(t-2)^2(t-3). \tag{2.20}$$

Wartościami własnymi macierzy A są więc 1, 2 i 3. Ich krotności algebraiczne są równe odpowiednio 1, 2 i 1. Obliczmy krotność geometryczną wartości własnej 2. Mamy

$$A - 2I = \begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{2.21}$$

zatem

$$\ker(A-2I) = \left\{ \begin{bmatrix} x_1 \\ x_1 \\ x_3 \\ 0 \end{bmatrix} : x_1, x_3 \in \mathbb{C} \right\} \implies \dim(\ker(A-2I)) = 2. \tag{2.22}$$

Krotność geometryczna wartości własnej 2 jest więc równa 2, czyli jest równa jej krotności algebraicznej. Ponieważ pozostałe wartości własne mają krotność algebraiczną 1, to ich krotności geometryczne także są równe 1. W szczególności macierz A jest diagonalizowalna.

2.2.1 Zadania.

Zadanie 2.2.1. Niech $A \in \mathbb{C}^{n\times n}$ będzie macierzą. Udowodnij, że $\det(\lambda I - A)$ jest wielomianem z λ jako zmienną.

Zadanie 2.2.2. Niech $A \in \mathbb{C}^{n\times n}$ będzie macierzą. Udowodnij, że $\chi_A(t)$ jest wielomianem *monicznym*, czyli że jego wiodący współczynnik jest równy 1.

Zadanie 2.2.3. Udowodnij, że jeśli macierz $A \in \mathbb{C}^{n\times n}$ ma postać górnotrójkątną, to jej wartości własne są dokładnie elementami na jej diagonali, a ich krotności algebraiczne są liczbą ich wystąpień.

2.3 Postać Jordana macierzy.

W tej sekcji nadal zakładamy, że pracujemy nad ciałem $\mathbb{C}$.

Definicja 2.3.1. Dla dowolnego $m \in \mathbb{Z}_+$ i dowolnego $\lambda \in \mathbb{C}$ *klatką Jordana* nazywamy macierz $J_m(\lambda) \in \mathbb{C}^{m\times m}$ postaci

$$J_m(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & \vdots \\ 0 & 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & \dots & 0 & 0 & \lambda \end{bmatrix}. \tag{2.23}$$

Okazuje się, że nawet jeśli macierz nie jest diagonalizowalna, to zawsze można ją sprowadzić do postaci, która jest prawie diagonalna. Jednak nawet dla macierzy nad $\mathbb{R}$, ich postać Jordana może zawierać liczby zespolone. Postać ta nazywa się postacią Jordana macierzy.

Definicja 2.3.2. Mówimy, że macierz J jest w *postaci Jordana*, jeśli jest postaci

$$J = \begin{bmatrix} J_{m_1}(\lambda_1) & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & J_{m_2}(\lambda_2) & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & J_{m_r}(\lambda_r) \end{bmatrix}, \tag{2.24}$$

gdzie każdy blok $J_{m_i}(\lambda_i)$ jest klatką Jordana.

Postać normalna nie jest jednak unikalna! Kolejność klatek w macierzy jest dowolna—zmienia to tylko permutację wymiarów w bazie.

Istnieje algorytm wyznaczania postaci normalnej Jordana. Proces ten jest nieco bardziej złożony, niż proces wyznaczania macierzy diagonalnej.

1. oblicz wartości własne A: $\lambda_1, \ldots, \lambda_k$,
2. oblicz krotności algebraiczne $\lambda_1, \ldots, \lambda_k$ (krotności zer w wielomianie charakterystycznym A),
3. oblicz krotności geometryczne $\lambda_1, \ldots, \lambda_k$ (krotność geometryczna λ_i to $\dim(\ker(A-\lambda_i I))$),
4. (opcjonalnie) oblicz $\dim(\ker((A-\lambda_i I)^2)), \dim(\ker((A-\lambda_i I)^3)), \dim(\ker((A-\lambda_i I)^4)), \ldots$, aż wymiar przestanie się zmieniać.

Przykład 2.3.1. Wyznaczmy postać Jordana macierzy

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}. \tag{2.25}$$

Ponieważ A jest macierzą górnotrójkątną, jej wartościami własnymi są 1 i 2. Obie mają krotność algebraiczną 2. Mamy

$$A - I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{2.26}$$

zatem

$$\ker(A-I) = \left\{ \begin{bmatrix} x_1 \\ 0 \\ 0 \\ 0 \end{bmatrix} : x_1 \in \mathbb{C} \right\} \implies \dim(\ker(A-I)) = 1. \tag{2.27}$$

Podobnie

$$A - 2I = \begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{2.28}$$

skąd

$$\ker(A-2I) = \left\{ \begin{bmatrix} 0 \\ x_2 \\ 0 \\ 0 \end{bmatrix} : x_2 \in \mathbb{C} \right\} \implies \dim(\ker(A-2I)) = 1. \tag{2.29}$$

Krotności geometryczne obu wartości własnych są więc równe 1. Dla każdej z nich występuje zatem dokładnie jedna klatka Jordana. Ponieważ krotność algebraiczna każdej z nich jest równa 2, obie klatki mają rozmiar 2. Postać Jordana macierzy A jest więc równa

$$J = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}. \tag{2.30}$$

Przykład 2.3.2. Wyznaczmy postać Jordana macierzy

$$A = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}. \tag{2.31}$$

Ponieważ A jest macierzą górnotrójkątną, jej wartościami własnymi są 1 i 2. Ich krotności algebraiczne są równe odpowiednio 1 i 3. Aby ustalić postać Jordana dla wartości własnej 2, obliczmy jej krotność geometryczną. Mamy

$$A - 2I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{2.32}$$

zatem

$$\ker(A - 2I) = \left\{ \begin{bmatrix} x_1 \\ 0 \\ 0 \\ 0 \end{bmatrix} : x_1 \in \mathbb{C} \right\} \implies \dim(\ker(A - 2I)) = 1. \tag{2.33}$$

Krotność geometryczna wartości własnej 2 jest więc równa 1. Oznacza to, że dla wartości własnej 2 występuje dokładnie jedna klatka Jordana. Ponieważ jej rozmiar musi być równy krotności algebraicznej wartości własnej 2, ma ona rozmiar 3. Dla wartości własnej 1 mamy krotność algebraiczną 1, więc odpowiada jej jedna klatka rozmiaru 1. Postać Jordana macierzy A jest więc równa

$$J = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.34}$$

2.3.1 Zadania.

Rozdział 3

Teoria kategorii.

W tym rozdziale wspiemy się na nowe poziomy abstrakcji. Pojęcia takie jak grupa czy monoid powstały po to, by móc badać obiekty o podobnych cechach jednocześnie. Zamiast udowadniać twierdzenia osobno dla wielomianów i liczb nautralnych, można udowodnić je dla monoidu—i to wystarczy. W rozdziale 1 weszliśmy na wyższy poziom. Zamiast definiować dla każdej struktury algebraicznej z osobna homomorfizmy i jądra czy udowadniać o nich twierdzenia, zrobiliśmy to jednocześnie używając algebry uniwersalnej. Teoria kategorii jest bardzo podobnym pomysłem. Tym razem jednak zamiast uogólniać pojęcia na jakąś rodzinę struktur (jak poprzednio na wszystkie algebry), uogólnimy pojęcia na całe dziedziny matematyki.

3.1 Wstęp.

Zaczniemy od pewnych podstawowych definicji i wprowadzenia do pojęcia kategorii.

3.1.1 Klasy.

Zaczniemy od pewnego pojęcia pierwotnego, które będzie nam potrzebne. Pojęciem tym jest **klasa**. Klasą nazywamy dowolną kolekcję obiektów. Każdy zbiór tworzy klasę swoich elementów. Klasy są jednak ogólniejsze niż zbiory. Mówić będziemy m.in. o klasie wszystkich zbiorów, klasie wszystkich zbiorów nieskończonych czy skończonych, klasie wszyskich grup, klasie wszystkich przestrzeni liniowych... W ogólności bpojęcia tego będziemy używać zamiast zbioru, kiedy zbiory będą zbyt małe. Ale nam będzie potrzebny jakiś sposób „uchwycenia”wszystkich zbiorów.

Klasy dzielimy na dwa rodzaje: **zbiory** (które wszyscy wiedzą, czym są) i **klasy właściwe**. Klasy właściwe to klasy, które nie mogą być zbiorami, np. klasa wszystkich zbiorów. Jak wiadomo w końcu, zbiór wszystkich zbiorów nie istnieje.

3.1.2 Kategorie.

Definicja kategorii nie wymaga zbyt skomplikowanego aparatu. Pojęcie klasy jest jedynym, które będzie nam tu potrzebne. Przed przeczytaniem tej definicji należy wziąć jednak głęboki oddech. Swoje życie matematyczne możemy podzielić na dwa etapy: przed zrozumieniem kategorii, oraz po ich zrozumieniu. Powrotu już nie ma, a spojrzenie kategoryczne kategorycznie zmienia sposób myślenia o matematyce.

Definicja 3.1.1. Kategorią nazywamy parę klas (O, A), gdzie O jest klasą **obiektów**, a A **strzałek**. Spełniają one następujące warunki

- Dla każdej strzałki f istnieją obiekty $\mathrm{dom}(f)$ i $\mathrm{cod}(f)$ nazywane odpowiednio **dziedziną** i **kodziedziną** strzałki, co zapisujemy
$$f : \mathrm{dom}(f) \to \mathrm{cod}(f). \tag{3.1}$$
- Dla każdych dwóch strzałek f, g, spełniających
$$\mathrm{cod}(f) = \mathrm{dom}(g) \tag{3.2}$$
istnieje strzałka
$$g \circ f : \mathrm{dom}(f) \to \mathrm{cod}(g) \tag{3.3}$$
nazywana **złożeniem** strzałek f i g. $g \circ f$ zapisywać będziemy też jako gf.
- Dla każdego obiektu A istnieje strzałka
$$1_A : A \to A \tag{3.4}$$
nazywana strzałką **identycznościową**.
- Dla dowolnych trzech strzałek
$$f : A \to B, \tag{3.5}$$
$$g : B \to C, \tag{3.6}$$
$$h : C \to D, \tag{3.7}$$
spełniona jest własność łącznoci ze względu na składanie
$$h \circ (g \circ f) = (h \circ g) \circ f \tag{3.8}$$
- Dla dowolnej strzałki
$$f : A \to B \tag{3.9}$$
spełnione jest
$$f \circ 1_A = f = 1_B \circ f. \tag{3.10}$$

Definicję zaczeliśmy od czegoś, co na myśl przywodzi graf skierowany. Potem jednak zapis sugeruje, jakbyśmy działali na funkcjach oraz ich dziedzinach i kodziedzinach. A kończymy z czymś podobnym do monoidu—mamy łączność i identyczność. I rzeczywiście wszystkie te spojżenia są trafne. Przejdźmy jednak najpierw do konkretnych przykładów kategorii.

Przykład 3.1.1. Zbiory jako obiekty i funkcje jako strzałki tworzą kategorię. Rzeczywiście, wszystkie własności składania funkcji spełniają warunki, które spełniać muszą strzałki. Jako strzałkę identycznościową wystarczy wziąć funkcję identycznościową. Kategorię tę będziemy oznaczać przez **Set**.

Przykład 3.1.2. Przestrzenie liniowe jako obiekty i przekształcenia liniowe jako strzałki tworzą kategorię. Udowadnia się tego identycznie, jak w przypadku zbiorów i funkcji (bo w końcu przestrzenie liniowe to też zbiory, a przekształcenia liniowe to też funkcje). Kategorię tę będziemy oznaczać przez **Lin**.

Nie w każdej kategorii jednak strzałki muszą odpowiadać funkcjom.

Przykład 3.1.3. Zbiory jako obiekty i pary zbiorów (A, B), że $A \subseteq B$ jako strzałki tworzą kategorię. Rzeczywiście, każde zawieranie

$$A \subseteq B \tag{3.11}$$

możemy reprezentować przez strzałkę

$$(A, B) : A \to B, \tag{3.12}$$

a składanie strzałek i jego łączność jest możliwe ze względu na przechodniość relacji zawierania zbiorów. Strzałka identycznościowa istnieje, bo dla każdego zbioru A mamy

$$A \subseteq A. \tag{3.13}$$

O ile w powyższych przykładach obiekty zawsze były jakimiś zbiorami, to wcale nie jest to konieczne.

Przykład 3.1.4. Niech będzie dowolną relacją zwrotną i przechodnią na zbiorze A. Elementy A jako obiekty i pary (a, b), gdzie a b, tworzą kategorię. Dowodzi się tego podobnie co faktu, że zbiory i ich zawieranie tworzą kategorię.

Przykład 3.1.5. Klasy zdań matematycznych jako obiekty i dowody jako strzałki tworzą kategorię. Ograniczymi się do intuicyjnego wyjaśnienia. Każdy dowód ma pewne założenia i wnioski. Dowody można łączyć w ciągi dowodów, co jest oczywiście łączne. Dowód identycznościowy też jest dowodem $(t \implies t)$.

Dla dowolnych obiektów A, B klasę strzałek między A, B oznaczamy przez $\mathrm{Hom}(A, B)$.

Definicja 3.1.2. Kategorię nazywamy **małą**, jeśli jej obiekty i strzałki tworzą zbiór.

Definicja 3.1.3. Kategorię nazywamy **lokalnie małą**, jeśli dla każdych dwóch obiektów A, B $\mathrm{Hom}(A, B)$ jest zbiorem.

3.1.3 Diagramy.

Tutaj będą kiedyś rysunki.
WAŻNE TO OMÓWIĆ!

3.1.4 Kilka podstawowych definicji.

W tej sekcji zaczniemy powoli odkrywać, w jaki sposób kategorie pozwalają na uogólnianie definicji i twierdzeń na całe połacie matematyki.

Definicja 3.1.4. Obiektem początkowym kategorii nazywamy taki obiekt 0, że dla każdego obiektu A istnieje dokładnie jedna strzałka

$$\alpha_A : 0 \to A. \tag{3.14}$$

Przykład 3.1.6. W **Set** obiektem początkowym jest zbiór pusty. Rzeczywiście, dla każdego zbioru A istnieje dokładnie jedna funkcja

$$\alpha_A : \emptyset \to A, \tag{3.15}$$

która niczego nie mapuje.

Definicja 3.1.5. Obiektem końcowym kategorii nazywamy taki obiekt 1, że dla każdego obiektu B istnieje dokładnie jedna strzałka

$$\tau_A : A \to 1. \tag{3.16}$$

Przykład 3.1.7. W **Set** obiektem końcowym jest każdy zbiór jednoelementowy. Rzeczywiście, dla każdego zbioru A i zbioru jednoelementowego $\{x\}$ istnieje dokładnie jedna funkcja

$$\tau_A : A \to \{x\}, \tag{3.17}$$

którą możemy zdefiniować tylko na jeden sposób, t.j. dla każdego $a \in A$

$$\tau_A(a) = x. \tag{3.18}$$

Definicja 3.1.6. Strzałkę

$$f : A \to B \tag{3.19}$$

nazywamy **mono** lub **monomorfizmem**, jeśli dla dowolnych strzałek

$$g, h : C \to A, \tag{3.20}$$

że jeśli

$$fg = fh \tag{3.21}$$

to

$$g = h. \tag{3.22}$$

Przykład 3.1.8. W **Set** monomorfizmy to dokładnie iniekcje.

Najpierw pokażemy, że każdy monomorfizm to iniekcja. Niech $f : A \to B$ będzie dowolną funkcją mono. Niech $x, y \in B$. Załóżmy, że $f(x) = f(y)$. Chcemy pokazać, że $x = y$.

Zdefiniujmy

$$\chi_x : \{0\} \to A, \quad \chi_x(0) = x. \tag{3.23}$$
$$\chi_y : \{0\} \to A, \quad \chi_y(0) = y. \tag{3.24}$$

Mamy teraz

$$f(\chi_x(0)) = f(x) = f(y) = f(\chi_y(y)), \tag{3.25}$$

czyli

$$f\chi_x = f\chi_y. \tag{3.26}$$

Ponieważ f jest mono, to $\chi_x = \chi_y$. Więc $x = y$.

Teraz pokażemy, że każda iniekcja to monomorfizm. Niech $f : A \to B$ będzie dowolną iniekcją. Niech $g, h : C \to A$ będą dowolnymi funkcjami takimi, że

$$fg = fh \tag{3.27}$$

Pokażemy, że

$$g = h. \tag{3.28}$$

Weźmy dowolny $x \in C$. Ponieważ $fg = fh$, to

$$f(g(x)) = f(h(x)). \tag{3.29}$$

Ponieważ f jest iniekcją, to

$$g(x) = h(x). \tag{3.30}$$

Ponieważ x był dowolny, to

$$g = h \tag{3.31}$$

□

Definicja 3.1.7. Strzałkę

$$f : A \to B \tag{3.32}$$

nazywamy **epi** lub **epimorfizmem**, jeśli dla dowolnych strzałek

$$g, h : B \to C, \tag{3.33}$$

że jeśli

$$gf = hf \tag{3.34}$$

to

$$g = h. \tag{3.35}$$

Przykład 3.1.9. W **Set** epimorfizmy to dokładnie surjekcje.

3.1.5 Zadania.

Zadanie 3.1.1. Czy dowolny graf skierowany jest kategorią? Dlaczego?

Zadanie 3.1.2. Czy każda kategoria jest monoidem? Dlaczego? Czy każda mała kategoria jest monoidem?

Zadanie 3.1.3. Udowodnij, że jeśli $(A, \cdot, e)$ jest monoidem, to tworzy on kategorię z: A jako jedynym obiektem, elementami $a \in A$ jako strzałkami $a : A \to A$ i $\cdot$ jako składaniem strzałek.

Zadanie 3.1.4. Wskaż obiekty końcowe i początkowe w **Lin**. Pamiętaj, że nie ma czegoś takiego jak pusta przestrzeń liniowa.

Zadanie 3.1.5. Udowodnij, że w **Set** epimorfizmy to dokładnie surjekcje.

3.2 Kategorie i język kategorii.

3.2.1 Zadania.

3.3 Różne konstrukcje kategoryczne.

3.3.1 Zadania.

3.4 Dualność i kilka innych pojęć.

3.4.1 Zadania.

3.5 Funktory.

3.5.1 Zadania.

FINIS.

