Dodatek A

Celem dodatku jest przypomnienie podstawowych elementarnych pojęć matematycznych oraz wyjaśnienie ewentualnych wątpliwości co do terminologii i notacji stosowanych w podręczniku.

1. Zbiory

Przypomnimy podstawowe pojęcia teorii mnogości. Pojęcie „zbioru" oraz „należenie elementu do zbioru" są pojęciami pierwotnymi teorii mnogości. Zbiory oznaczamy z reguły dużymi literami np. X,Y,Z,A,B,C. Zdanie „element x należy do zbioru A", zapisujemy symbolicznie jako $x \in A$. Zdanie „element x nie należy do zbioru A", zapisujemy symbolicznie jako $x \notin A$.

Jeśli każdy element zbioru A jest elementem zbioru B, to mówimy, że A jest podzbiorem B lub B jest nadzbiorem A, co zapisujemy w postaci $A \subset B$. Symbol $\subset$ nazywamy *znakiem inkluzji*.

Niech A,B,X będą dowolnymi zbiorami takimi, że $A \subset X$ i $B \subset X$. W teorii mnogości, a ściślej, w jej dziale o nazwie *algebra zbiorów* wprowadza się działania dodawania zbiorów $A \cup B$, mnożenia: $A \cap B$, odejmowania: $A \setminus B$ oraz dopełnienia zbioru: $-A \overset{df}{=} X \setminus A$.

Niech X będzie dowolnym zbiorem niepustym. *Funkcją zdaniową* nazywamy wyrażenie $\varphi(x)$, w którym występuje zmienna x i które staje się zdaniem prawdziwym lub fałszywym, jeśli zamiast zmiennej x podstawimy dowolny element zbioru X.

Jeśli $\varphi(x)$ jest funkcją zdaniową to $\{x \in X;\ \varphi(x)\}$ jest z definicji zbiorem tych wszystkich elementów x zbioru X dla, których zdanie $\varphi(x)$ (jak mówimy czasem warunek $\varphi(x)$) jest prawdziwe.

By zdefiniować zbiór często po prostu wyliczamy jego elementy w nawiasach klamrowych. Np. $\{a,b,c\}$ oznacza zbiór złożony z 3 elementów a, b i c. Symbolem N oznaczamy zbiór liczb naturalnych $\{1,2,3,...\}$ a symbolem Z zbiór liczb całkowitych $\{...,-3,-2,-1,0,1,2,3,...\}$. Symbolem $<m,n>$ oznaczamy zbiór wszystkich liczb całkowitych większych równych m i mniejszych równych n.

2. Para uporządkowana

Niech a i b będą dowolnymi przedmiotami (czasem mówimy obiektami). *Parą uporządkowaną* nazywamy zbiór $\{a,\{a,b\}\}$. Parę uporządkowaną oznaczamy symbolem (a,b) przy czym a nazywa się pierwszą współrzędną (lub poprzednikiem) pary uporządkowanej (a,b) a b drugą współrzędną (lub następnikiem) pary uporządkowanej (a,b). Para uporządkowana umożliwia wprowadzenie pojęcia trójki uporządkowanej (czy ogólniej pojęcia n–tki uporządkowanej) jako pary uporządkowanej.

Trójkę uporządkowaną definiujemy rekurencyjnie jako $(a,b,c) \stackrel{df}{=} ((a,b),c)$, a *n-tkę uporządkowaną* jako $(x_1,x_2,...,x_n) \stackrel{df}{=} ((x_1,x_2,...,x_{n-1}),x_n)$.

Czasami nie precyzujemy jakie jest n w n-tce uporządkowanej i nazywamy taką n-tkę uporządkowaną układem uporządkowanym.

Przykład: Wiele pojęć matematycznych definiujemy jako pary uporządkowane np. liczba wymierna jest z definicji parą uporządkowaną liczb całkowitych. Liczba zespolona jest parą uporządkowaną liczb rzeczywistych. Automat skończony (będziemy mówić o atomatach skończonych w rozdziale 3) to piątka uporządkowana. Algebra Boole'a (będziemy mówić o algebrach Boole'a w rozdziale 2) to 6-stka uporządkowana. ■

Tak więc elementarne w swej treści pojęcie pary uporządkowanej i n-tki uporządkowanej jest użytecznym często wykorzystywanym pojęciem.

3. Relacja i relacja n-argumentowa, system relacyjny

Niech $X_1, X_2, ..., X_n$ będą zbiorami. *Relacja n-argumentowa* ($n \geq 2$) to dowolny podzbiór ρ produktu $X_1 \times X_2 \times ... \times X_n$. Jeśli n=2 to relację $\rho \subset X_1 \times X_2$ nazywamy relacją dwuargumentową lub krótko relacją i fakt , że $(x,y) \in \rho$ zapisujemy nieco krócej jako $x \rho y$. Jeśli $X_1 = X_2 = ... = X_n$ to relację n argumentowa nazywamy relacją w X.

System relacyjny to para uporządkowana (X, ρ) gdzie ρ jest relacją w X.
Dziedziną relacji $\rho \subset X_1 \times X_2$ nazywamy zbiór

$$\{x \in X_1; istnieje\ \ takie\ y \in X_2, ze\ (x,y) \in \rho\}$$

Przeciwdziedziną relacji $\rho \subset X_1 \times X_2$ nazywamy zbiór

$$\{y \in X_2; istnieje\ \ takie\ x \in X_2, ze\ (x,y) \in \rho\}$$

Relacja ρ w X jest *zwrotna,* jeśli dla każdego $x \in X$ spełniony jest warunek $x \rho x$.

Relacja ρ w X jest *przechodnia,* jeśli dla każdego $x, y, z \in X$ spełniony jest warunek

$$(x \rho y \ \wedge \ y \rho z) \Rightarrow (x \rho z).$$

Relacja ρ w X jest *symetryczna,* jeśli dla każdego $x, y \in X$ spełniony jest warunek

$$x \rho y \ \Rightarrow \ y \rho x$$

Relacja jest *antysymetryczna,* jeśli dla każdego $x, y \in X$ spełniony jest warunek

$$(x \rho y \ \wedge \ y \rho x) \Rightarrow (x \rho y)$$

Szczególnie ważne typy relacji to relacja funkcji czyli funkcja, relacja równoważności, relacja quasiporządku, relacja częściowego porządku i relacja liniowego porządku. Relacja funkcji omówiona jest w następnym punkcie (punkt 4).

Relacją quasiporządku w zbiorze X nazywamy relację zwrotną i przechodnią. Relacją quasiporządku oznaczamy najczęściej symbolem $\leq$.

Relacją porządku w zbiorze X nazywamy relację zwrotną, antysymetryczną i przechodnią. Relacją porządku oznaczamy podobnie jak relację quasiporządku najczęściej symbolem $\leq$.

Relacją liniowego porządku w zbiorze X nazywamy relację zwrotną, antysymetryczną i przechodnią (a więc relację porządku) spełniającą warunek dla każdego $x, y \in X$ mamy $x \leq y$ lub $y \leq x$, gdzie symbol $\leq$ oznacza relację liniowego porządku.

Niech X będzie dowolnym niepustym zbiorem. *Relacja równoważności* lub krótko *równoważność* w X, to relacja $\sim$ w X zwrotna, symetryczna i przechodnia. Relacja równoważności spełnia więc z definicji następujące warunki: dla każdego $a, b, c \in X$

- $a \sim a$ (zwrotność)
- jeśli $a \sim b$, to $b \sim a$ (symetryczność)
- jeśli $a \sim b$ i $b \sim c$, to $a \sim c$ (przechodniość).

Przykład: Przykładem relacji równoważności jest relacja przystawania liczb całkowitych modulo liczba $n \in N$. Mówimy, że dwie liczby całkowite $a, b \in Z$ przystają do siebie modulo m jeśli dają tę samą resztę z dzielenia przez m. Jeśli liczby $a, b \in Z$ przystają do siebie modulo n to fakt ten zapisujemy jako

$$a \equiv b \pmod{m}$$

i nazywamy kongruencją. ■

Twierdzenie (*zasada abstrakcji*): Dowolna relacja równoważności $\sim$ w zbiorze niepustym X wyznacza jednoznacznie rozbicie tego zbioru na parami rozłączne niepuste podzbiory $(K_t)_{t \in T}$ (które nazywamy klasami równoważności rozważanej relacji) w taki sposób, że dowolne dwa elementy $x, y \in X$ należą do tej samej klasy równoważności K_t wtedy i tylko wtedy, gdy $x \sim y$.

Z drugiej strony jeśli mamy rozbicie niepustego zbioru X na parami rozłączne niepuste podzbiory $(K_t)_{t \in T}$ to takie rozbicie wyznacza jednoznacznie relację równoważności w zbiorze X przy czy zdefiniowana jest ona tak:

$x \sim y$ wtedy i tylko wtedy, gdy istnieje takie $t \in T$, $x, y \in K_t$ ■

4. Funkcje

Niech X, Y będą ustalonymi zbiorami. *Funkcją* nazywamy dwuargumentową relację $f \subset X \times Y$ taką, że dla każdego $x \in X$ i dla każdego $x, y \in Y$ mamy

$$((x, y) \in f \wedge (x, z) \in f) \Rightarrow y = z$$

a ponadto dla każdego $x \in X$ istnieje $y \in Y$ takie, że $(x, y) \in f$. Zbiór X nazywamy dziedziną funkcji f lub zbiorem argumentów funkcji f a zbiór Y przeciwdziedziną funkcji f.

Jeśli dla każdego $y \in Y$ istnieje takie $x \in X$,że $(x, y) \in f$, to funkcję nazywamy "na" lub *suriekcją.*

Jeśli dla każdego $(x_1, y_1), (x_2, y_2) \in f$ zachodzi implikacja $(y_1 = y_2) \Rightarrow (x_1 = x_2)$, to funkcję f nazywamy *funkcją różnowartościową* lub *iniekcją.*

Fakt, że f jest funkcją z dziedziną X i przeciwdziedziną Y, zapisujemy jako $f : X \to Y$ lub $f : X \ni x \to y \in Y$. Jeśli $(x, y) \in f$, to x nazywamy *argumentem funkcji*, a y *wartością funkcji* i tradycyjnie zapisujemy ten fakt w postaci $f(x) = y$. Zapis $f(x)$ oznacza wartość funkcji, nie funkcję.

Funkcję (ang. function) nazywamy również inaczej *odwzorowaniem* (ang. mapping) lub *przekształceniem* (ang. transformation).

Niech $f : X \to Y$ będzie funkcją. Obraz zbioru $A \subset X$ przy odwzorowaniu f to z definicji podzbiór zbioru Y zdefiniowany jako $\{y \in Y;$ istnieje takie $x \in A, że\ f(x) = y\}$. Obraz zbioru A oznaczamy symbolem $f(A)$.

Przeciwobraz zbioru $B \subset Y$ przy odwzorowaniu f to z definicji podzbiór zbioru X zdefiniowany jako $\{x \in X;$ istnieje takie $y \in B, że\ f(x) = y\}$. Przeciwobraz zbioru A oznaczamy symbolem $f(A)$.

Funkcję określoną na zbiorze N nazywamy *ciągiem*, a określoną na Z *ciągiem dwustronnym*. Ciąg zapisujemy wyliczając jego kolejne elementy w postaci $a_1, a_2, a_3, ..., a_n, ...$ lub oznaczamy symbolem $(a_n)_{n=1}^{\infty}$ lub $(a_n)_{n \in N}$. Funkcję określoną na zbiorze <1,*m*>, gdzie $m \in Z$ nazywamy *ciągiem skończonym*.

5. Bijekcje, permutacje i inwolucje

Bijekcja to dowolne odwzorowanie różnowartościowe i "na". Jeśli A jest dowolnym niepustym zbiorem, to dowolna bijekcja $f : A \to A$ nazywa się *permutacją* zbioru A Najprostszą permutacją zbioru A jest tożsamość $id : A \to A$ zdefiniowana wzorem $id(x) = x$ dla każdego $x \in A$.

Zbiór wszystkich permutacji zbioru niepustego A stanowi (wraz z działaniem superpozycji funkcji) *grupę* (na ogół nieprzemienną). Elementem odwrotnym do danego elementu f jest funkcja odwrotna f^{-1}, a elementem jednostkowym jest tożsamość id: $A \to A$.

Jeśli A jest n-elementowym zbiorem skończonym, to liczba wszystkich różnych permutacji $f : A \to A$ jest równa $n!$

Z reguły mówiąc „permutacja", mamy na myśli skończony zbiór A. Wygodnie jest ponumerować elementy skończonego n – elementowego zbioru A liczbami ze zbioru <1,*n*> lub utożsamić zbiór A ze zbiorem liczb <1,*n*>.

Permutacje są bardzo często wykorzystywane w kryptografii (np. w szyfrach przestawieniowych permutacje są kluczami).

Tę samą permutację $f : A \to A$ można zdefiniować w różny sposób. Często stosowanym sposobem jest wpisywanie w nawiasach argumentów funkcji f wraz z wartościami funkcji według schematu:

$$f = \begin{pmatrix} 1 & 2 & 3 & n \\ f(1) & f(2) & f(3) & \ldots f(n) \end{pmatrix}$$

Przykład: Niech $A = \{1,2,3,4,5\}$. Odwzorowanie zdefiniowane tak $f(1) = 3$, $f(2) = 5$, $f(3) = 4, f(4) = 2, f(5) = 1$ jest permutacją. Można je zapisać jako

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \qquad (*)$$

Przy takim zapisie łatwo można znaleźć element odwrotny do f, czyli f^{-1}. Zamieniamy wiersze miejscami a następnie porządkujemy kolumny wg rosnącej współrzędnej , górnej współrzędnej. Uzyskujemy w tej sytuacji

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

■

Inwolucja to taka permutacja $f : A \to A$, że $f = f^{-1}$ lub co na jedno wychodzi $f \cdot f = id$, czyli $f(f(x)) = x$ dla każdego $x \in A$.

6. Działania i algebry

Niech A będzie niepustym zbiorem a n liczbą naturalną. Działanie n–argumentowe (lub operacja n-argumentowa) w zbiorze A, to dowolne odwzorowanie $f : \underbrace{A \times A \times \ldots \times A}_{n} \to A$. Element $f(a) \in A$ dla $a \in A^n$ nazywamy wynikiem tego działania.
Dodatkowo przez działanie 0 – argumentowe rozumiemy dowolny wyróżniony element zbioru A. Najczęściej mamy do czynienia z działaniami 0, 1 i 2 argumentowymi.
Mówimy, że podzbiór $B \subset A$ jest zamknięty ze względu na działanie $f : \underbrace{A \times A \times \ldots \times A}_{n} \to A$ jeśli dla każdego $(a_1, a_2, \ldots, a_n) \in B^n$ mamy $f(a_1, a_2, \ldots, a_n) \in B$.

Działania dwuargumentowe nazywamy krótko działaniami i oznaczamy zwykle takimi symbolami jak $+, \circ, \otimes, \oplus, /$ itp., a wynik działania na parze $(a_1, a_2) \in A^2$ oznaczamy symbolem $a_1 + a_2$, $a_1 \circ a_2$, $a_1 \otimes a_2$ itd.

Działanie dwuargumentowe $\circ$ nazywamy *przemiennym*, jeśli dla każdego $a, b \in A$ mamy

$$a \circ b = b \circ a$$

Działanie dwuargumentowe $\circ$ nazywamy *łącznym*, jeśli dla każdego $a, b, c \in A$ mamy

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Element $1 \in A$ nazywamy *elementem neutralnym* lub *jedynką* lub też *elementem jednostkowym* działania $\circ$ jeśli $1 \circ a = a \circ 1 = a$ dla każdego $a \in A$.

Fakt: Element jednostkowy ustalonego działania dwuargumentowego $\circ$ może być tylko jeden.
Dowód: Załóżmy, że istnieją dwa różne takie elementy. Prowadzi to do sprzeczności, a więc może istnieć tylko jeden element jednostkowy dla danego działania. ■

Działania zdefiniowane wyżej nazywają się również działaniami wewnętrznymi. Jeśli mamy dwa niepuste zbiory K i A to dowolne odwzorowanie $o_e : K \times A \to A$ nazywamy działaniem zewnętrznym.

Układ uporządkowany $(A, o_1, o_2, ..., o_n)$, gdzie A jest zbiorem, a $o_1, o_2, ..., o_n$ działaniami, nazywa się *algebrą*. Algebry nazywamy też "*algebrami ogólnymi* lub "*algebrami abstrakcyjnymi*". Z pojęciem algebry związane są ściśle pojęcia *podalgebry*, *homomorfizmu algebr* i *izomorfizmu algebr*.

Niech $(A, o_1, o_2, ..., o_n)$ będzie algebrą a zbiór $B \subset A$ niech będzie zamknięty ze względu na działania $o_1, o_2, ..., o_n$ oraz niech $o_i^{'} \overset{df}{=} o_i \big| B^{n_i}$ dla $i \in <1, n>$ (gdzie n_i jest liczbą argumentów działania o_i) . W tej sytuacji algebrę $(B, o_1^{'}, o_2^{'}, ..., o_n^{'})$ nazywamy *podalgebrą* algebry $(A, o_1, o_2, ..., o_n)$. Mówimy też często w uproszczeniu, że B jest podalgebrą algebry A.

Oczywiście każdy podzbiór $B \subset A$ zamknięty ze względu na działania $o_1, o_2, ..., o_n$ wyznacza podalgebrę algebry $(A, o_1, o_2, ..., o_n)$.

Niech będą dane 2 algebry $(A, o_1, o_2, ..., o_n)$ i $(A, o_1^{'}, o_2^{'}, ..., o_n^{'})$ tego samego typu tzn. takie, że dla każdego $i \in <1, n>$ liczby argumentów działania o_i oraz $o_i^{'}$ są jednakowe. Odwzorowanie $h : A_1 \to A_2$ nazywamy *homomorfizmem* algebr $(A, o_1, o_2, ..., o_n)$ i $(A, o_1^{'}, o_2^{'}, ..., o_n^{'})$ jeśli dla każdego $i \in <1, n>$ i dla każdego $(a_1, a_2, ..., a_{n_i}) \in A_1^{n_i}$ (gdzie n_i jest liczbą argumentów działania i) mamy

$$h(o_i(a_1, a_2, ..., a_{n_i})) = o_i^{'}(h(a_1), h(a_2), ..., h(a_{n_i}))$$

Szczególnymi przypadkami algebry są półgrupa, monoid, grupa, grupa abelowa, pierścień, ciało i algebra Boole'a, którą zajmiemy się szczegółowo w rozdziale 2.

Czasami wprowadza się (bardzo bliskie pojęciowo algebrze abstrakcyjnej, ale nieco ogólniejsze) pojęcie *struktury algebraicznej* jako n-tki uporządkowanej (w skład tej n-tki wchodzi rodzina zbiorów niepustych oraz rodzina działań wewnętrznych i zewnętrznych). Przykładem struktury algebraicznej jest przestrzeń liniowa $(V, K, +, \cdot)$, gdzie V jest zbiorem wektorów, K ciałem, plus oznacza dodawanie wektorów a kropka oznacza działanie mnożenia przez skalar.

Zbiór A z działaniem łącznym nazywa się *półgrupą*. Dokładniej jest to para uporządkowana (A, o_1) taka, że działanie $o_1 : A \times A \to A$ jest działaniem dwuargumentowym łącznym, tzn. dla każdego $a, b, c \in A$ mamy

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Półgrupę z jedynką nazywamy *monoidem*. Istnienie jedynki oznacza, że istnieje taki element $1 \in A$, że $1 \circ a = a \circ 1 = a$ dla każdego $a \in A$.

Fakt (który warto znać)**:** W dowolnej półgrupie $(A,\circ)$ wartość $(...((a_1 \circ a_2) \circ a_3) \circ ...a_{n-1}) \circ a_n$ dla $a_1, a_2, ..., a_n \in A$ nie zależy od rozmieszczenia nawiasów. Możemy więc pisać: $a_1 \circ a_2 \circ ... \circ a_n$.

Dowód: Dowód tego faktu jest indukcyjny. ■

7. Grupy

Monoid $(G,\circ)$ posiadający tę własność, że dla każdego $a \in A$ istnieje taki element $b \in A$, że $a \circ b = b \circ a = 1$ nazywamy *grupą*. Upraszczając mówimy, że G jest grupą.

Element b z powyższej definicji nazywamy elementem odwrotnym do a i oznaczamy symbolem a^{-1} tzn. $b = a^{-1}$.

Grupę nazywamy grupą skończoną jeśli ma skończoną liczbę elementów. Ilość elementów w grupie nazywamy *rzędem grupy* i oznaczamy symbolem $|G|$. Podzbiór grupy G, który jest grupą ze względu na to samo działanie grupowe nazywamy *podgrupą* grupy G.

Generator grupy to taki element $g \in G$, że $G = \{g^k;\ k \in N\}$

Grupy cykliczne to grupy mające generator.

Rząd elementu grupy to najmniejsza liczba naturalna taka , że $a^n = 1$

Jeśli działanie grupowe jest przemienne to taką grupę nazywamy *grupą abelową.*

Twierdzenie (Lagrange'a)**:**Dla grup skończonych rząd podgrupy jest dzielnikiem rzędu grupy.

Wniosek: Rząd elementu grupy jest dzielnikiem rzędu grupy.

Przykład: Zbiór liczb całkowitych Z z działaniem dodawania jako działaniem grupowym jest grupą abelową. Podobnie zbiór liczb Q wymiernych z dodawaniem, zbiór liczb rzeczywistych R z dodawaniem i zbiór liczb zespolonych C z dodawaniem są grupami apelowymi.

Przykład: Zbiór liczb $Z_n = \{0,1,2,...,n-1\}$ z działaniem dodawania modulo n jako działaniem grupowym jest grupą abelową. Jest to tzw. grupa reszt modulo n.

Przykład: Zbiór liczb $Z_p^* = \{1,2,..., p-1\}$, z działaniem mnożenia modulo p jest grupą apelową.

Przykład: Przykładem grupy nieabelowej jest $(S_n,\circ)$, gdzie S_n jest zbiorem wszystkich permutacji zbioru n elementowego a działanie "$\circ$" superpozycją odwzorowań.

Przykład: Zbiory Q\{0}, R\{0}, C\{0} z działaniem mnożenia liczb są grupami abelowymi. ■

Niech P będzie podgrupą grupy G. Jeśli $|P| = p^k$ dla pewnego $k \in N$ i liczby pierwszej p, to mówimy, że P jest p podgrupą grupy G. Każdą grupę mającą p^k elementów nazywamy p-grupą.

Jeśli $g \in G$ jest generatorem grupy G to liczbę $n \in N \cup \{0\}$ taką, że $g^n = a$, nazywamy *logarytmem dyskretnym* z a przy podstawie g i piszemy $\log_g a = n$.

8. Pierścienie

Niech w niepustym zbiorze P będą określone 2 działania, "+" i zwane odpowiednio dodawaniem i mnożeniem oraz niech będą wyróżnione 2 elementy 0 i 1 zwane *zerem* i *jedynką pierścienia*. Układ $(P,+,\cdot,0,1)$ czyli czwórkę uporządkowaną nazywamy *pierścieniem*, jeśli spełnione są dla każdego $a,b,c \in P$ następujące warunki:

1. $a+b=b+a$ (przemienność dodawania)
2. $a+(b+c)=(a+b)+c$ (łączność dodawania)
3. $a+0=0+a=a$ (0 jest elementem zerowym pierścienia)
4. dla każdego $a \in P$ istnieje $a' \in P$, że $a+a'=a'+a=0$ (istnienie elementu przeciwnego)
5. $a \cdot b = b \cdot a$ (przemienność mnożenia)
6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (łączność mnożenia)
7. $a \cdot 1 = 1 \cdot a = a$ (1 jest jedynką pierścienia)
8. $a(b+c) = a \cdot b + a \cdot c$ oraz $(b+c)a = ba + ca$ (rozdzielność mnożenia względem dodawania)

Ściślej, układ $(P,+,\cdot,0,1)$ spełniający powyższe warunki nazywamy zwykle *pierścieniem przemiennym z jednością*, a pierścieniem nazywa się układ $(P,+,\cdot,0)$ spełniający tylko warunki 1, 2, 3, 4, 7 i 8. Innymi słowy pierścień to grupa abelowa z mnożeniem spełniającym warunki 6 i 8.

Ponieważ w dalszym ciągu będziemy mieli do czynienia tylko z pierścieniami przemiennymi z jedynką będziemy je krótko nazywać pierścieniami.

Krótko: pierścieniem nazywamy algebrę $(P,+,\cdot,0)$ taką, że $(P,0,+)$ jest grupą abelową, a działanie mnożenia $\cdot : P \times P \to P$ jest łączne i rozdzielne względem dodawania (prawostronnie i lewostronnie), tzn. spełnione są aksjomaty grupy abelowej i następujące 2 warunki: $a(b+c) = a \cdot b + a \cdot c$ oraz $(b+c)a = ba + ca$ dla każdego $a,b,c \in P$.

Jeśli $a \cdot b = 0$ i $a,b \neq 0$ to a i b nazywamy *dzielnikami zera*.

Dziedzina całkowitości to pierścień bez dzielników 0.

Przykład: Zbiór liczb całkowitych Z ze zwykłymi działaniami dodawania i mnożenia jest pierścieniem (przemiennym z 1).

Przykład : Zbiór liczb $Z_m = \{0,1,...,m-1\}$ $(m \in N, m \geq 2)$ jest pierścieniem z działaniami sumy modulo m i mnożenia modulo m. Jest to tzw. pierścień reszt modulo m. Sumę modulo m oznaczamy symbolem $\oplus$ lub $\oplus_m$. Zapis $x \oplus_m y$ oznacza resztę z dzielenia zwykłej sumy $x + y$ liczb całkowitych przez m. Podobnie iloczyn modulo m oznaczamy symbolem $\otimes$ lub $\otimes_m$. Zapis $x \otimes_m y$ oznacza resztę z dzielenia zwykłego iloczynu liczb całkowitych przez m . Wprowadza się też często 2 zapisy na oznaczenie reszty z dzielenia przez liczby całkowitej x przez m : $x \pmod m$ oraz $[x]_m$. ■

9. Ciała, ciała skończone

W tym punkcie zdefiniujemy pojęcie ciała (ang. field, fran. le corp, nm. Korp) i omówimy podstawowe własności ciał. Ciała oznacza się z reguły symbolem K a tzw. ciała skończone o q elementach symbolem F_q lub $GF(q)$ (litera K sugeruje wykorzystanie francuskiej lub niemieckiej nazwy ciała, F nazwy angielskiej *a GF* jest skrótem od Galois field).

Ciało może mieć skończoną albo nieskończoną ilość elementów. Mówimy krótko "ciała skończone" i "ciała nieskończone". Szczególną uwagę zwrócimy na ciała skończone czyli ciała o skończonej ilości elementów. Szczególnie ważne są ciała skończone w kryptografii, kodach korekcyjnych i cyfrowym przetwarzaniu sygnałów. W niniejszym podrozdziale zostaną również omówione pierwiastki z jedności i pierwiastki pierwotne z jedności.

Pierścień przemienny z jednością $1 \neq 0$ spełniający warunek

$$\forall_{x \in K, x \neq 0} \; \exists_{y \in K} \; xy = 1$$

nazywa się *ciałem*.

Inaczej mówiąc ciało to z definicji taki pierścień przemienny z jednością $1 \neq 0$, w którym dla każdego niezerowego elementu istnieje element odwrotny. Jeśli ciało K ma skończoną ilość elementów, to nazywamy je ciałem skończonym, jeśli nieskończoną, to nazywamy je ciałem nieskończonym . Z definicji ciała wynika, że ciało ma co najmniej 2 elementy.

Niech K będzie ciałem. Podzbiór L ciała K nazywamy *podciałem* ciała K, jeśli $0,1 \in L$ i w podzbiorze L są wykonalne działania dodawania, odejmowania, mnożenia i dzielenia przez elementy różne od 0.

Przykład: Jeżeli p jest liczbą pierwszą to pierścień Z_p jest ciałem. Oczywiście jest to ciało skończone.

Przykład: Zbiór liczb wymiernych Q jest ciałem nieskończonym.

Przykład: Zbiór liczb rzeczywistych R jest ciałem nieskończonym. ■

Charakterystyka ciała to najmniejsza taka liczba $n \in N$, że $\underbrace{1+1+...+1}_{n} = 0$. Jeśli takiej liczby nie ma, to mówimy, ż ciało ma charakterystykę 0. Charakterystyka ciała jest liczbą pierwszą lub zerem. Charakterystyka ciała skończonego jest zawsze liczbą pierwszą. Ciało o charakterystyce 0 jest zawsze nieskończone.

Twierdzenie: Każde ciało skończone ma zawsze p^n elementów, tzn. dla każdego ciała skończonego istnieje taka liczba pierwsza p i naturalna $k \in N$, że liczba elementów ciała jest równa p^n. ■

Ciało skończone o $q = p^n$ elementach oznacza się symbolami F_q lub $GF(p^n)$.

Mówimy, że zbiór $L \subset K$ wraz z działaniami sumy i iloczynu jest *podciałem* ciała *K,* jeśli jest zamknięty ze względu na te działania. Z kolei ciało *K* nazywamy *rozszerzeniem* ciała *L* .

Ciało proste to takie ciało , które nie zawiera żadnego ciała właściwego.

Grupa addytywna ciała $(K,+,\cdot,0,1)$ to grupa $(K,+)$, a *grupa multiplikatywna ciała* to grupa $(K \setminus \{0\},\cdot)$.

Wielomian o współczynnikach w dowolnym ciele K definiujemy analogicznie, jak w przypadku ciała liczb rzeczywistych lub zespolonych. Zbiór wszystkich wielomianów wielomianów o współczynnikach w ciele K oznaczamy symbolem $K[x]$. Można pokazać, że ma on strukturę pierścienia przemiennego z jednością.

10. Przestrzenie liniowe

Pojęcie przestrzeni liniowej i bazy przestrzeni liniowej przyjmujemy za znane.

Przykład: Przestrzeń $\{0,1\}^n = Z_2^n$ jest przestrzenią liniową nad $Z_2 = \{0,1\}$. Ten istotny fakt wynika z ogólniejszego faktu następującego:

Fakt: Przestrzeń K^n z działaniami dodawania po współrzędnych i mnożeniem przez skalar po współrzędnych jest przestrzenią liniową nad *K*.

11. Odległość Hamminga

Żeby wyjaśnić czym jest odległość Hamminga wprowadzimy najpierw wprowadzić pojęcie przestrzeni metrycznej i produktu przestrzeni metrycznych.

Przestrzeń metryczna to para uporządkowana, (X,ρ) gdzie X jest niepustym zbiorem a ρ funkcją $\rho : X \times X \to R$ spełniającą dla każdego $x,y,z \in X$ następujące 3 warunki:

1. $\rho(x,y) = 0 \Leftrightarrow x = y$
2. $\rho(x,y) = \rho(y,x)$ (symetria)
3. $\rho(x,z) \le \rho(x,y) + \rho(y,z)$ (nierówność trójkąta lub tzw. warunek trójkąta)

Elementy zbioru X nazywamy *punktami*. Funkcja ρ nazywa się *metryką* (lub *odległością*) *przestrzeni X*, a wartość $\rho(x,y)$ *odległością punktów* $x,y \in X$. Z warunków 1, 2, 3 wynika, że metryka $\rho : X \times X \to R$ jest funkcją rzeczywistą nieujemną, zatem zawsze mamy $\rho : X \times X \to R^+$. Jeśli wiadomo, jaką metrykę rozważamy, to przestrzeń metryczną (X,ρ)

oznacza się dla uproszczenia pojedynczym symbolem X i mówi, że X jest przestrzenią metryczną.

Kulą otwartą o środku w punkcie $x \in X$ i promieniu $r \in R^+ \setminus \{0\}$ nazywamy zbiór $K(x,r) = \{y \in X; \rho(x,y) < r\}$, a *kulą domkniętą* zbiór $\overline{K(x,r)} = \{y \in X; \rho(x,y) \le r\}$.

Przykład: Zbiór liczb rzeczywistych R z funkcją $\rho : R \times R \to R^+$ zdefiniowaną wzorem : dla każdego $x, y \in R$, $\rho(x,y) = |y - x|$ jest przestrzenią metryczną.

Twierdzenie: Niech będzie danych n przestrzeni metrycznych (X_1, ρ_1), (X_2, ρ_2),..., ,(X_n, ρ_n). Rozważmy iloczyn kartezjański $X = X_1 \times X_2 \times ... \times X_n$ i zdefiniujmy funkcję $\rho : X \times X \to R^+$ następująco: dla każdego $x = (x_1, x_2, ..., x_n) \in X$ i każdego $y = (y_1, y_2, ..., y_n) \in X$

$$\rho(x,y) = \sum_{i=1}^{n} \rho_i(x_i, y_i) \qquad (1)$$

wówczas (X, ρ) jest przestrzenią metryczną.

Dowód: Dowód polega na sprawdzeniu własności 1, 2, 3 z definicji przestrzeni metrycznej. Szczegółowy dowód można znaleźć w pracy [2] (K.Maurin; Analiza).■

Przestrzeń (X, ρ) występującą w powyższym twierdzeniu nazywamy *iloczynem kartezjańskim* (lub *produktem kartezjańskim*) przestrzeni metrycznych (X_1, ρ_1), (X_2, ρ_2),...,(X_n, ρ_n).

Uwaga: Czasami definiujemy produkt przestrzeni metrycznych (X_1, ρ_1), (X_2, ρ_2),..., ,(X_n, ρ_n) jako parę uporządkowaną $(X, \tilde{\rho})$, gdzie funkcja $\tilde{\rho} : X \times X \to R^+$ jest zadana wzorem

$$\tilde{\rho}(x,y) = \left(\sum_{i=1}^{n} \rho_i(x_i, y_i)^2\right)^{1/2} \qquad (3)$$

Można wykazać, że funkcja $\tilde{\rho}$ jest metryką w zbiorze $X = X_1 \times X_2 \times ... \times X_n$. Obie metryki ρ i $\tilde{\rho}$ są równoważne w ty sensie, że dla dowolnego ciągu $(x_n)_{n=1}^{\infty}$ elementów przestrzeni X i dowolnego $x \in X$ mamy

$$\rho(x_n, x) \to 0 \text{ wtedy i tylko wtedy gdy } \tilde{\rho}(x_n, x) \to 0 \qquad (4)$$

Uwaga: Łatwo zauważyć, że jeśli (X_1, ρ_1), (X_2, ρ_2),..., ,(X_n, ρ_n) są przestrzeniami metrycznymi i $X_1 = X_2 = ... = X_n \overset{ozn}{=} Y$ to funkcja $\rho_s : Y \times Y \to R^+$ zdefiniowana wzorem: dla każdego $x, y \in Y$

$$\rho_s(x,y) = \sum_{i=1}^{n} \rho_i(x,y) \qquad (5)$$

jest metryką w Y. Mimo podobieństwa wzorów (1) i (5) definiują one zupełnie inne metryki

Przykład: Z twierdzenia 1 wynika, że R^n ($R^n = \underbrace{R \times R \times R ... \times R}_{n}$) z funkcją $\rho : R^n \times R^n \to R^+$ zdefiniowaną dla każdego $(x_1, x_2, ...x_n), (y_1, y_2, ..., y_n) \in R^n$ wzorem

$$\rho(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{6}$$

jest przestrzenią metryczną.■

W każdym niepustym zbiorze X można wprowadzić metrykę czyli jak mówimy zbiór X można zmetryzować, wprowadzają w nim tzw. metrykę dyskretną $\rho_d : X \times X \to R^+$ zdefiniowaną wzorem:

$$\rho_d(x, y) = \begin{cases} 1 & \text{gdy } x \neq y \\ 0 & \text{gdy } x = y \end{cases}$$

Sprawdzenie, że ρ_d jest metryką w X, jest bardzo proste. Tak zdefiniowana przestrzeń metryczna (X, ρ_d) nazywa się przestrzenią metryczną dyskretną.

Niech V będzie dowolnym ustalonym alfabetem. Wprowadźmy w tym alfabecie metrykę dyskretną $\rho_d : V \times V \to R^+$. Z twierdzenia 1 wynika, że funkcja $\rho_H : V^n \times V^n \to R^+$ zdefiniowana wzorem: dla każdego $x, y \in V^n$

$$\rho_H(x, y) = \sum_{i=1}^{n} \rho_d(x_i, y_i)$$

jest metryką nazywamy ją *metryką lub odległością Hamminga* w przestrzeni V^n (V^n jest to przestrzeń wszystkich słów o długości n nad alfabetem V). Najczęściej rozważamy metrykę Hamminga dla $V^n = \{0,1\}^n$. Oczywiście $\rho_H : V^n \times V^n \to N \cup \{0\}$ czyli ρ_H jest funkcją o wartościach w zbiorze liczb całkowitych nieujemnych.

Uwaga: Wartość $\rho_H(x, y) = \sum_{i=1}^{n} \rho_d(x_i, y_i)$ dla 2 słów $x, y \in V^n$ (czyli 2 słów o długości n nad alfabetem V) jest równa liczbie pozycji na, których słowa x i y się różnią. Jeśli np. przesyłamy słowo x przez kanał telekomunikacyjny i na wyjściu tego kanału otrzymujemy słowo y to $\rho_H(x, y)$ podaje liczbę błędów transmisji słowa x.

Przykład: Jeśli $V = \{0,1\}$ oraz x=01110000 i y=10001111 to odległość Hamminga tych 2 słów jest równa 8. ■

Wagą słowa binarnego z przestrzeni $\{0,1\}^n$ (lub ogólniej z $\{0,1\}^*$) nazywamy liczbą jedynek w tym słowie. W ten sposób definiujemy na $\{0,1\}^*$ funkcję $w : \{0,1\}^* \to N \cup \{0\}$. Oczywiście dla $a \in \{0,1\}^n$ mamy $w(a) = \rho_H(0, a)$ gdzie ρ_H jest metryką Hamminga. Można wyrazić metrykę Hamminga ρ_H w $\{0,1\}^n$ za pomocą funkcji wagi w.

Niech $x, y \in \{0,1\}^n$, $x = (x_1, x_2, ..., x_n)$, $y = (y_1, y_2, ..., y_n)$, wówczas mamy

$$\rho(x,y) \overset{df}{=} \sum_{i=1}^{n} \rho_d(x_i, y_i) = \sum_{i=1}^{n} w(x_i -_2 y_i) = w(x-y) = w(x+y)$$

gdzie $x_i -_2 y_i$ oznacza różnicę modulo 2, $x - y$ oznacza różnicę modulo 2 po współrzędnych a $x + y$ sumę modulo 2 po współrzędnych.

Przykład: Waga słowa 11111111 jest równa 8 tzn. w(11111111)=8, w(00)=0, w(001)=1. ■

12. Grafy

Graf (*nieskierowany*) to para uporządkowana (V, E), gdzie V jest dowolnym skończonym niepustym zbiorem tzw. zbiorem wierzchołków grafu a E skończoną rodziną nieuporządkowanych par elementów (niekoniecznie różnych) zbioru V, które to pary nazywają się krawędziami grafu.

Graf skierowany (nazywany też *digrafem*) to para uporządkowana (V, E), gdzie V jest dowolnym skończonym niepustym zbiorem tzw. zbiorem wierzchołków grafu a E skończoną rodziną par uporządkowanych elementów zbioru V, które to pary nazywają się krawędziami grafu.

Intuicyjnie jasne pojęcie grafu jest często wykorzystywane w teorii układów logicznych do opisu automatów skończonych, układów sekwencyjnych, a również w minimalizacji wyrażeń boolowskich.

Rząd wierzchołka v grafu to liczba krawędzi grafu schodzących się w danym wierzchołku.

Marszrutą w grafie nazywamy skończony ciąg krawędzi postaci $v_0v_1, v_1v_2, ..., v_{m-1}v_m$ wierzchołek v_0 nazywamy wierzchołkiem początkowym marszruty, a v_m wierzchołkiem końcowym marszruty.

Marszrutę, której wszystkie krawędzie są różne nazywamy *łańcuchem*.

Drogą nazywamy łańcuch, w którym wszystkie wierzchołki $v_0, v_1, v_2, ..., v_{m-1}, v_m$ są różne, za wyjątkiem być może v_0 i v_m.

Drogę zamkniętą zawierająca przynajmniej jedną krawędź nazywamy *cyklem*

Lasem nazywamy graf , który nie zawiera cykli

Las spójny nazywamy *drzewem*.

Korzeń to każdy wierzchołek drzewa o rzędzie większym od 1.

Liściem nazywamy każdy wierzchołek drzewa o rzędzie równym 1.