8.2 Pierścienie

Pierścieniem nazywamy algebrę z dodawaniem $+$ i mnożeniem $\cdot$, która z dodawaniem jest grupą przemienną, oraz w której są spełnione prawa łączności

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

i rozdzielności

$$(x + y) \cdot z = x \cdot z + y \cdot z \quad \text{oraz} \quad z \cdot (x + y) = z \cdot x + z \cdot y$$

Przykładem pierścienia jest zbiór liczb całkowitych ze zwykłymi działaniami, pierścień Z_n z dodawaniem i mnożeniem modulo n, zbiór liczb wymiernych ze zwykłymi działaniami. Pierścień R jest pierścieniem *z jednością*, jeżeli mnożenie w R ma element neutralny. Pierścień nazywamy *przemiennym*, jeżeli mnożenie w tym pierścieniu jest przemienne.

Element $a \neq 0$ (w pierścieniu R) jest *dzielnikiem zera*, jeżeli $a \cdot b = 0$ dla pewnego $b \neq 0$. Element $a \in R$ jest *odwracalny*, jeżeli $a \cdot b = b \cdot a = 1$ dla pewnego $b \in R$. Dzielniki zera nie są elementami odwracalnymi. Zero jest elementem odwracalnym tylko w pierścieniu, którego jedynym elementem jest 0. Wiemy też, że w pierścieniu zachodzą wzory $x \cdot 0 = 0 \cdot x = 0$.

Pierścień przemienny z jednością nazywamy *ciałem*, jeżeli $0 \neq 1$ i dla każdego niezerowego elementu w tym pierścieniu jest element odwrotny.

8.3 Produkt pierścieni

Przypuśmy, że R_1 i R_2 są pierścieniami. W produkcie $R_1 \times R_2$ definiujemy dodawanie i mnożenie

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2).$$

Zbiór $R_1 \times R_2$ z tymi działaniami nazywamy produktem (iloczynem) kartezjańskim pierścieni R_1 i R_2. Jeżeli pewna równość jest prawdziwa dla wszystkich elementów pierścieni R_1 i R_2, to jest też prawdziwa w produkcie $R_1 \times R_2$. Stąd wynika, że produkt kartezjański pierścieni jest pierścieniem.

Analogicznie definiujemy produkty większej liczby pierścieni $R_1 \times \ldots \times R_n$ albo $R \times \ldots \times R$.

Produkt ciał nie jest ciałem.

8.4 Szeregi formalne i wielomiany

Przypuśćmy, że R jest pierścieniem. Jeżeli $a_0, a_1, \ldots \in R$, to wyrażenie postaci

$$\sum_{i=0}^{\infty} a_i x^i$$

nazywamy szeregiem formalnym. Szereg formalny można też definiować jako ciąg $a_0, a_1, \ldots \in R$, ale ciąg ten powinien kojarzyć się z podanym wzorem.

W zbiorze szeregów formalnych definiujemy dodawanie i mnożenie przyjmując, że

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

oraz

$$(\sum_{i=0}^{\infty} a_i x^i) \cdot (\sum_{i=0}^{\infty} b_i x^i) = \sum_{i=0}^{\infty} (\sum_{j=0}^{i} a_j b_{i-j}) x^i.$$

Zbiór szeregów formalnych z tymi działaniami jest pierścieniem.

Pojęcie wielomianu można definiować na dwa sposoby. Są to albo szeregi formalne takie, że dla pewnej liczby naturalnej n i dla wszystkich $i > n$ mamy $a_i = 0$ albo też wielomiany definiuje się jako funkcje $f : R \to R$ określone wzorami postaci

$$f(x) = \sum_{i=0}^{n} a_i x^i. \tag{2}$$

W zbiorze liczb rzeczywistych mając wielomian-funkcję f zdefiniowaną wzorem (2) możemy jednoznacznie ustalić współczynniki $a_0, a_1, \ldots$. Podane definicje wielomianu nie są jednak równoważne. Inaczej jest, jeżeli rozważamy wielomiany o współczynnikach należących do ciała Z_p. Dla wszystkich x z tego ciała zachodzi wzór $x^p = x$. Funkcja $f : Z_p \to Z_p$ zdefiniowana wzorem $f(x) = x^p$ może też zostać zdefiniowana wzorem $f(x) = x$. Wobec tego, znając samą funkcją f nie potrafimy w tym przypadku odtworzyć wzoru, którym ta funkcja została określona.

Wielomiany rozumiane jako szeregi formalne tworzą podpierścień pierścienia szeregów formalnych. Także wielomiany rozumiane jako funkcje ze zwykłymi w takim przypadku działaniami tworzą pierścień.

8.5 Moduły

Przypuśmy, że R jest pierścieniem przemiennym z jednością. Zbiór M nazywamy *modułem* nad pierścieniem R, jeżeli

1. elementy M potrafimy dodawać i M z dodawaniem jest grupą przemienną,
2. jest określone mnożenie przekształcające $R \times M$ w M takie, że

$$(ab) \cdot x = a \cdot (b \cdot x)$$

$$(a + b) \cdot x = a \cdot x + b \cdot x$$

$$a \cdot (x + y) = a \cdot x + a \cdot y$$

$$1 \cdot x = x$$

dla wszystkich $a, b \in R$ oraz $x, y \in M$.

Moduły nad ciałami nazywamy *przestrzeniami liniowymi* lub *wektorowymi*.

8.5.1 Uwagi o definicji modułu

W literaturze często są podawane bardziej ogólne definicje modułów. Pojęcie modułu definiuje się dla dowolnych pierścieni, a nie tylko dla pierścieni przemiennych z jednością. W takim przypadku w definicji modułu pomija się warunek $1 \cdot x = x$. Przytoczona definicja odpowiada pojęciu modułu lewostronnego. Rozważa się też moduły prawostronne, w których jest określone mnożenie przekształcające $M \times R$ w M spełniające warunek

$$x \cdot (ab) = (x \cdot a) \cdot b$$

i równości analogiczne do podanych w rozdziale 8.5. Rozważane są też moduły (obustronne), które są jednocześnie lewo- i prawostronne. Nietrudno zauważyć, że w module lewostronnym nad pierścieniem przemiennym R można zdefiniować mnożenie z prawej strony przyjmując, że dla $x \in M$ i $a \in R$ mamy

$$x \cdot a = a \cdot x.$$

Moduł M z tak zdefiniowanym mnożeniem z prawej strony jest modułem prawostronnym, i w tym sensie jest też modułem obustronnym.

8.6 Przykłady modułów

Symbole R i R_1 będą oznaczać pierścienie przemienne z jednością.

- Dowolna grupa przemienna jest modułem nad pierścieniem liczb całkowitych, jeżeli dla $n \in N$, $n \neq 0$ przyjmiemy, że

$$n \cdot x = \underbrace{x + x + \ldots + x}_{n \text{ razy}},$$

$$(-n) \cdot x = \underbrace{(-x) + (-x) + \ldots + (-x)}_{n \text{ razy}},$$

$$0 \cdot x = 0.$$

- Jeżeli pierścień R_1 jest podpierścieniem pierścienia R_2, to R_2 jest modułem nad pierścieniem R_1 z mnożeniem (przekształcającym $R_1 \times R_2$ w R_2) zdefiniowanym jako zwykłe mnożenie w pierścieniu R_2 (ograniczone do sytuacji w których pierwszy argument należy do R_1). W szczególności, pierścień R jest modułem nad R, a także ciało liczb rzeczywistych jest przestrzenią liniową nad ciałem liczb wymiernych.

- Pierścień wielomianów o współczynnikach z R jest modułem nad pierścieniem R z mnożeniem

$$a \cdot \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} (a a_i) x^i.$$

- Jeżeli M jest podpierścieniem R i dla wszystkich $a \in R$ oraz $x \in M$ zachodzi warunek $ax \in M$, to M ze zwykłym mnożeniem z pierścienia R jest modułem. Moduły tej postaci nazywamy *ideałami* (w przypadku pierścieni przemiennych). Zauważmy, że nie każdy podpierścień jest modułem. Na przykład, Z jest podpierścieniem Q, ale nie jest modułem nad Q.

- Jeżeli $a_1, \ldots, a_n \in R$, to zbiór

$$\{x_1 a_1 + x_2 a_2 + \ldots + x_n a_n \mid x_1, x_2, \ldots, x_n \in R\}$$

z mnożeniem z pierścienia R jest ideałem. Zauważmy, że rozważany zbiór jest podpierścieniem R generowanym przez $a_1, \ldots, a_n$.

- Modułem jest zbiór $R^n = R \times \ldots \times R$ z działaniami

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

oraz

$$a \cdot (x_1, x_2, \ldots, x_n) = (a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n).$$

Elementy zbioru R^n nazywamy *wektorami* o współrzędnych należących do R.

- W zbiorze $R^X = \{f \mid f : X \to R\}$ definiujemy dodawanie oraz mnożenie przez element $a \in R$ przyjmując, że

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

oraz

$$(af)(x) = af(x).$$

Określona w ten sposób algebra jest modułem.

- Jeżeli $h : R_1 \to R_2$ jest homomorfizmem pierścieni, to

$$\{x \in R_1 \mid h(x) = 0\}$$

jest ideałem.

8.7 Podmoduły

Przyjmijmy, że M jest modułem nad R. Niepusty zbiór $X \subseteq M$ nazywamy *podmodułem* modułu M, jeżeli

1. $\vec{x} + \vec{y} \in X$ dla dowolnych $\vec{x}, \vec{y} \in X$,
2. $-\vec{x} \in X$ dla każdego $\vec{x} \in X$,
3. $a\vec{x} \in X$ dla wszystkich $\vec{x} \in X$ i $a \in R$.

Warto zauważyć, że warunki podane w definicji podmodułu można zastąpić jednym, stwierdzającym, że jeżeli $\vec{x}, \vec{y} \in X$ i $a, b \in R$, to $a\vec{x} + b\vec{y} \in X$.

Jeżeli R jest ciałem, to podmoduł nad R nazywamy *podprzestrzenią liniową* (lub wektorową) nad ciałem R.

Nietrudno sprawdzić, że podmoduł dowolnego modułu jest modułem. Tak więc podprzestrzeń liniowa dowolnej przestrzeni liniowej jest przestrzenią liniową.

Dla pierścienia R przykładami podmodułów są:

- zbiór
$$\{(x_1, \ldots, x_n) \in R^n : x_1 a_1 + \ldots + x_n a_n = 0\}$$
rozwiązań równania liniowego, jest to podmoduł R^n,
- zbiór
$$\{f : R \to R : \ f \text{ jest wielomianem}\},$$
jest to podmoduł modułu R^R,
- a także przekrój dowolnych podmodułów modułu M jest podmodułem M (a więc podmodułem jest także zbiór rozwiązań układu równań liniowych).

9.1 Moduły generowane przez zbiory

Przypuśćmy, że M jest modułem nad pierścieniem R. Zbiór

$$M' = \{\sum_{i=1}^{m} a_i \vec{x}_i : m \in N \wedge a_1, \ldots a_m \in R \wedge \vec{x}_1, \ldots \vec{x}_m \in X\}$$

jest podmodułem M i nazywamy go podmodułem *generowanym przez zbiór* X. Moduł M jest *generowany przez* X, jeżeli $M = M'$. Wyrażenie $\sum_{i=1}^{m} a_i \vec{x}_i$ nazywamy *kombinacją liniową* elementów $\vec{x}_1, \ldots \vec{x}_m$ o współczynnikach $a_1, \ldots a_m$. Zauważmy, że jeżeli $X = \{\vec{x}_1, \ldots \vec{x}_n\}$, to M' można zdefiniować wzorem

$$M' = \{\sum_{i=1}^{n} a_i \vec{x}_i : a_1, \ldots a_n \in R\}.$$

Moduł jest *skończenie generowalny*, jeżeli jest generowany przez pewien zbiór skończony.

Każdy pierścień R przemienny z jednością rozważany jako moduł nad R jest skończenie generowalny, gdyż jest generowany przez zbiór $\{1\}$. Moduł R^n też jest skończenie generowalny. Generują go wektory $\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (z i-tą współrzędną równą 1). Wynika to z oczywistego wzoru

$$(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i \vec{e}_i.$$

Z drugiej strony, skończenie generowalne przestrzenie liniowe nad ciałem liczb wymiernych są przeliczalne. Stąd wynika, że liczby rzeczywiste nie są skończenie generowalną przestrzenią liniową nad ciałem liczb wymiernych.

9.2 Zbiory liniowo niezależne

Niech M będzie modułem nad R. Zbiór $X \subseteq M$ jest *liniowo zależny*, jeżeli istnieją $a_1, \ldots, a_n \in R$ nie wszystkie równe 0 oraz parami różne elementy $\vec{x}_1, \ldots, \vec{x}_n \in X$ takie, że $\vec{0} = \sum_{i=1}^{n} a_i \vec{x}_i$. W przeciwnym razie zbiór X nazywamy *liniowo niezależnym*. Będziemy mówić o wektorach, że są liniowo zależne (niezależne), jeżeli zbiór tych wektorów jest liniowo zależny (lub odpowiednio: niezależny).

Lemat 9.1 *Następujące warunki są równoważne:*

1. *zbiór X jest liniowo niezależny, a więc dla dowolnych $a_1, \ldots, a_m \in R$ oraz parami różnych $\vec{x}_1, \ldots, \vec{x}_m \in X$, jeżeli $\sum_{i=1}^{m} a_i \vec{x}_i = \vec{0}$, to $a_1 = \ldots = a_m = 0$,*
2. *wektor $\vec{0}$ ma dokładnie jedno przedstawienie w postaci kombinacji liniowej wektorów ze zbioru X,*
3. *pewien wektor ma dokładnie jedno przedstawienie w postaci kombinacji liniowej wektorów ze zbioru X,*
4. *każdy element przestrzeni liniowej ma najwyżej jedno przedstawienie w postaci kombinacji liniowej wektorów ze zbioru X.*

Dowód. Warunek 2 jest wyrażonym innymi słowami warunkiem 1. Tak więc warunki 1 i 2 są równoważne. Jest też oczywiste, że warunek 2 implikuje warunek 3.

$(3 \Rightarrow 2)$. Przypuśćmy, że $\vec{x}_0$ ma dokładnie jedno przedstawienie w postaci kombinacji liniowej elementów X i $\vec{x}_0 = \sum_{i=1}^{m} b_i\vec{x}_i$ jest przedstawieniem tego wektora.

Dla dowodu nie wprost załóżmy, że $\vec{0}$ ma dwa przedstawienia, a więc ma także przedstawienie $\sum_{i=1}^{m} a_i\vec{x}_i = \vec{0}$ dla pewnych wektorów $\vec{x}_i \in X$ oraz współczynników $a_i \in R$ nie wszystkich równych 0. Można założyć, że w obu przedstawieniach występują te same elementy X, ponieważ takie przedstawienia można uzupełnić o dowolny wektor ze współczynnikiem 0 (nie rozróżniamy przedstawień różniących się iloczynami $0 \cdot \vec{x}$). Wtedy wzór

$$\vec{x}_0 = \vec{0} + \vec{x}_0 = \sum_{i=1}^{m} a_i\vec{x}_i + \sum_{i=1}^{m} b_i\vec{x}_i = \sum_{i=1}^{m}(a_i + b_i)\vec{x}_i$$

daje drugie przedstawienie wektora $\vec{x}_0$, a to przeczy wyborowi $\vec{x}_0$..

$(2 \Rightarrow 4)$. Jeżeli

$$\sum_{i=1}^{m} a_i\vec{x}_i = \vec{x} = \sum_{i=1}^{m} b_i\vec{x}_i$$

są różnymi przedstawieniami wektora $\vec{x}$, to wektor $\vec{0}$ można przedstawić jako

$$\sum_{i=1}^{m}(a_i - b_i)\vec{x}_i,$$

a więc w postaci kombinacji z niezerowymi współczynnikami.

Implikacja $(4 \Rightarrow 2)$ jest oczywista, ponieważ wektor $\vec{0}$ ma odpowiednie przestawienie. □

9.3 Baza modułu

Liniowo niezależmy zbiór generatorów modułu nazywamy *bazą*.

Łatwo podać przykłady baz. Zbiór $\{1\}$ jest bazą pierścienia R traktowanego jako moduł nad pierścieniem R. Wektory $\vec{e}_1, \ldots, \vec{e}_n$ tworzą bazę modułu R^n. Tę bazę R^n będziemy nazywać standardową. Jednak nie każdy moduł ma bazę. Jeżeli grupę Z_n z dodawaniem modulo n będziemy uważać za moduł nad pierścieniem liczb całkowitych, to z wzoru $(n+1) \cdot x = x$ otrzymamy, że dowolne przedstawienie w postaci kombinacji liniowej nie jest jednoznaczne, a więc żaden podzbiór Z_n nie jest liniowo niezależny. Ponadto, ten moduł jest generowany przez zbiór $\{1\}$, a więc jest skończenie generowalny. Zauważmy też, że sytuacja się zmienia, jeżeli pierścień Z_n uważamy za moduł nad nim samym. Wtedy Z_n ma bazę równą $\{1\}$.

W przypadku modułów, które niekoniecznie są przestrzeniami liniowymi, bazy nazywa się też zbiorami wolnych generatorów.

9.4 Bazy w przestrzeniach liniowych

Lemat 9.2 *W przestrzeni liniowej nad ciałem K, zbiór X jest liniowo zależny wtedy i tylko wtedy, gdy pewnego $\vec{x} \in X$ zachodzi wzór*

$$\vec{x} = \sum_{i=1}^{n} a_i\vec{x}_i$$

dla pewnych $x_1, \ldots, x_n \in X \setminus \{\vec{x}\}$ i pewnych $a_1, \ldots, a_n \in K$.

Dowód. Podany wzór oznacza, że $\vec{x}$ ma dwa przedstawienia w postaci kombinacji liniowej elementów zbioru X. Tak więc X jest liniowo zależny na mocy lematu 9.1 (ten fragment dowodu nie wymaga założenia, że K jest ciałem).

Jeżeli zbiór X jest liniowo zależny, to

$$\sum_{j=1}^{n} a_j\vec{x}_j = \vec{0}$$

dla pewnych parami różnych wektorów $\vec{x}_j \in X$ i współczynników $a_j \in K$, wśród których jest współczynnik $a_i \neq 0$. Wtedy

$$\vec{x}_i = \sum_{j \neq i} \frac{-a_j}{a_i}\vec{x}_j. \quad \square$$

Wniosek 9.3 *Minimalny zbiór generatorów przestrzeni liniowej jest bazą.*

Dowód. Przypuśćmy, że X jest minimalnym zbiorem generatorów i nie jest bazą. Wtedy X jest liniowo zależny i dla pewnego $\vec{x} \in X$, dla pewnych $x_1, \ldots, x_n \in X \setminus \{\vec{x}\}$ oraz $a_1, \ldots, a_n \in K$ mamy

$$\vec{x} = \sum_{i=1}^{n} a_i\vec{x}_i.$$

Z tego wzoru wynika jednak, że $X \setminus \{\vec{x}\}$ też jest zbiorem generatorów. Przeczy to minimalności zbioru X. □

Wniosek 9.4 *Każda skończenie generowalna przestrzeń liniowa ma bazę.*

Dowód. Bazą jest zbiór generatorów o najmniejszej liczbie elementów. □

Prawdziwe jest też ogólne twierdzenie o istnieniu bazy przestrzeni liniowej:

Twierdzenie 9.5 *Każda przestrzeń liniowa ma bazę.* □

Dowód tego twierdzenia wymaga skomplikowanych środków i został pominięty.

Twierdzenie 9.6 *Jeżeli V jest przestrzenią liniową i $X \subseteq V$, to następujące warunki są równoważne*

1. *X jest bazą*
2. *X jest maksymalnym zbiorem liniowo niezależnym.*
3. *X jest mininalnym zbiorem generatorów.*

Dowód. ($1 \Rightarrow 2$). Przypuśćmy, że X jest bazą i weźmy $\vec{x}_0 \notin X$. Ponieważ X jest zbiorem generatorów, więc $\vec{x}_0$ jest kombinacją wektorów z X. To jednak oznacza, że $\vec{x}_0$ ma dwa przedstawienia w postaci kombinacji liniowej elementów $X \cup \{\vec{x}_0\}$. Tak więc na podstawie lematu 9.1, zbiór $X \cup \{\vec{x}_0\}$ jest liniowo zależny. W ten sposób dowiedliśmy, że X jest maksymalnym zbiorem liniowo niezależnym.

($2 \Rightarrow 1$). Załóżmy teraz, że X jest maksymalnym zbiorem liniowo niezależnym Jeżeli $\vec{w} \notin X$, to zbiór $X \cup \{\vec{w}\}$ jest liniowo zależny. Podobnie jak w dowodzie lematu 9.2, znajdujemy przedstawienie

$$\vec{w} = \sum_{i=1}^{n} a_i \vec{x}_i$$

w postaci kombinacji liniowej elementów zbioru X. Także wektory $\vec{w} \in X$ są kombinacjami liniowymi elementów X. Tak więc każdy wektor $\vec{w}$ jest kombinacją liniową elementów X, czyli X jest zbiorem generatorów.

Z przedstawionego rozumowania wynika, że dwa pierwsze warunki z tezy są równoważne. Wobec wniosku 9.3, aby zakończyć dowód, wystarczy pokazać, że bazy są minimalnymi zbiorami generatorów.

($1 \Rightarrow 3$). Dla dowodu nie wprost załóżmy, że X jest bazą, $\vec{x}_0 \in X$ oraz zbiór $X \setminus \{\vec{x}_0\}$ generuje całą przestrzeń. Wtedy $\vec{x}_0$ jest kombinacją liniową elementów zbioru $X \setminus \{\vec{x}_0\}$. To jednak oznacza, że $\vec{x}_0$ ma dwa przedstawienia w postaci kombinacji liniowej elementów zbioru X. Z lematu 9.1 wynika, że X jest liniowo zależny, a to jest sprzeczne z założeniem. □

9.5 Lemat o wymianie i wymiar przestrzeni

Lemat 9.7 (lemat o wymianie) *Przypuśćmy, że wektory $\vec{u}_1, \ldots, \vec{u}_k, \vec{w}_1, \ldots, \vec{w}_m$ generują przestrzeń liniową V, a wektory $\vec{w}_1, \ldots, \vec{w}_m, \vec{w} \in V$ są liniowo niezależne. Wtedy istnieje indeks i, $1 \leqslant i \leqslant k$ taki, że wektory*

$$\vec{u}_1, \ldots, \vec{u}_{i-1}, \vec{u}_{i+1} \ldots \vec{u}_k, \vec{w}_1, \ldots, \vec{w}_m, \vec{w}$$

generują przestrzeń V.

Dowód. Z założenia o generowaniu V wynika, że

$$\vec{w} = \sum_{i=1}^{k} a_i \vec{u}_i + \sum_{j=1}^{m} b_j \vec{w}_j$$

dla pewnych współczynników $a_1, \ldots, a_k$ i $b_1, \ldots, b_m$. Gdyby wszystkie współczynniki $a_1, \ldots, a_k$ były równe 0, to wektor $\vec{w}$ byłby kombinacją liniową wektorów $\vec{w}_1, \ldots, \vec{w}_m$ i przeczyłoby to liniowej niezależnosci wektorów $\vec{w}_1, \ldots, \vec{w}_m, \vec{w}$. Niech i_0 będzie indeksem takim, że $a_{i_0} \neq 0$. Wtedy powyższy wzór można przekształcić do postaci

$$\vec{u}_{i_0} = \sum_{i \neq i_0} a_{i_0}^{-1} a_i \vec{u}_i + \sum_{j=1}^{m} a_{i_0}^{-1} b_j \vec{w}_j - a_{i_0}^{-1} \vec{w}.$$

Stąd wynika, że zbiór z tezy lematu dla $i = i_0$ pozwala na wygenerowanie wszystkich elementów zbioru generatorów przestrzeni V, i dlatego sam jest zbiorem generatorów. □

Wniosek 9.8 *W przestrzeni liniowej generowanej przez zbiór n elementowy każdy skończony zbiór liniowo niezależny jest zawarty n elementowym zbiorze generatorów.*

Dowód. Przypuśćmy, że wektory $\vec{u}_1, \ldots, \vec{u}_n$ generują przestrzeń liniową, a wektory $\vec{w}_1, \ldots, \vec{w}_m$ są liniowo niezależne. Każdy układ wektorów postaci $\vec{w}_1, \ldots, \vec{w}_i$ jest liniowo niezależny. Jeżeli lemat o wymianie zastosujemy kolejno dla $i = 1, \ldots, m$ i dla liniowo niezależnych wektorów $\vec{w}_1, \ldots, \vec{w}_i$, to skonstruujemy zbiór generatorów zawierający $\vec{w}_1, \ldots, \vec{w}_m$. Zauważmy, że za pomocą lematu o wymianie konstruujemy coraz to nowe zbiory generatorów nie zwiększając liczby elementów. □

Wniosek 9.9 *W przestrzeni liniowej generowanej przez zbiór n elementowy każdy zbiór liniowo niezależny jest skończony.* □

Wniosek 9.10 *W przestrzeni liniowej generowanej przez zbiór n elementowy każdy zbiór liniowo niezależny ma najwyżej n elementów.* □

Wniosek 9.11 *Każde dwie bazy skończenie generowalnej przestrzeni liniowej są równoliczne.* □

Wymiarem przestrzeni liniowej V nazywamy liczbę elementów (pewnej) bazy tej przestrzeni. Z wniosków 9.4 i 9.11 wynika, że pojęcie wymiaru jest dobrze zdefiniowane dla wszystkich skończenie generowalnych przestrzeni.

Wniosek 9.12 *W przestrzeni liniowej wymiaru n, każdy n elementowy zbiór generatorów i każdy n elementowy zbiór liniowo niezależny jest bazą.*

Dowód. Jest to wniosek z twierdzenia 9.6 i wniosku 9.10. □

Dla modułów też można wprowadzić pojęcie wymiaru. W tym przypadku nie zawsze istnieją bazy, ale można dowieść poniższe twierdzenie. Pomijamy uzasadnienie tego twierdzenia. Jest trudniejsze niż uzasadnienie analogicznej własności przestrzeni liniowych.

Twierdzenie 9.13 *Jeżeli moduł nad pierścieniem przemiennym (z jednością) ma skończoną bazę, to każde dwie bazy tego modułu są równoliczne.* □

Z lematu o wymianie wynika jeszcze następujący

Wniosek 9.14 *Podprzestrzeń skończenie generowalnej przestrzeni liniowej jest skończenie generowalna.*

Dowód. Przypuśćmy, że V' jest podprzestrzenią przestrzeni liniowej V. Wszystkie liniowo niezależne układy wektorów podprzestrzeni V' są też liniowo niezależne w przestrzeni V, a więc mają nie więcej niż n elementów dla pewnej liczby n. Wobec tego istnieje najliczniejszy układ liniowo niezależnych wektorów podprzestrzeni V'. Jest on oczywiście maksymalnym takim układem w tej podprzestrzeni i – na podstawie lematu 9.6 – jest bazą, a także zbiorem generatorów podprzestrzeni V'. □

9.6 Współrzędne wektora

Przypuśćmy, że $\vec{x} = (x_1, \ldots, x_n) \in R^n$. Wtedy elementy $x_1, \ldots, x_n \in K$ nazywamy współrzędnymi wektora $\vec{x}$, a dokładniej, x_i nazywamy i-tą współrzędną. Przypomnijmy, że $\vec{e}_i \in R^n$ jest wektorem $(0, \ldots, 1, \ldots, 0)$ z i-tą współrzędną równą 1 i pozostałymi równymi 0. Wiemy już, że wektory $\vec{e}_1, \ldots, \vec{e}_n$ tworzą tzw. standardową bazę modułu R^n. Oczywiście,

$$\vec{x} = \sum_{i=1}^{n} x_i \vec{e}_i.$$

Niech M będzie modułem nad pierścieniem R. Jeżeli układ $\vec{a}_1, \ldots, \vec{a}_n$ jest bazą modułu M i $\vec{x} \in M$, to $\vec{x}$ ma jednoznaczne przedstawienie postaci

$$\vec{x} = \sum_{i=1}^{n} y_i \vec{a}_i,$$

gdzie $\vec{a}_1, \ldots, \vec{a}_n \in X$ (patrz lemat 9.1). Element y_i z tego przedstawienia nazywamy i-tą współrzędną wektora $\vec{x} \in M$ w bazie $\vec{a}_1, \ldots, \vec{a}_n$.

Tak więc współrzędne wektora z modułu R^n są także jego współrzędnymi w bazie standardowej $\vec{e}_1, \ldots, \vec{e}_n$.

Lemat 9.15 *Jeżeli x_i i y_i są i-tymi współrzędnymi odpowiednio $\vec{x}$ i $\vec{y}$ w bazie $\vec{a}_1, \ldots, \vec{a}_n$, to $x_i + y_i$ jest i-tą współrzędną $\vec{x} + \vec{y}$, a ax_i jest i-tą współrzędną $a\vec{x}$ w tej bazie.*

Dowód. Jest to konsekwencja lematu 9.1. □

Pojęcie współrzędnych można w podobny sposób zdefiniować też dla baz nieskończonych.

9.7 Homomorfizmy i przekształcenia liniowe

Niech M_1 i M_2 będą modułami nad pierścieniem R. Funkcję $f : V_1 \to V_2$ nazywamy *homomorfizmem* (modułów), jeżeli spełnia wszystkie równości

$$f(a\vec{x} + b\vec{y}) = af(\vec{x}) + bf(\vec{y})$$

dla $\vec{x}, \vec{y} \in M_1$ oraz $a, b \in R$. Homomorfizmy modułów nazywamy też *funkcjami* lub *przekształceniami liniowymi*, zwłaszcza jeżeli ograniczamy się do przestrzeni liniowych. Homomorfizmy (funkcje liniowe) są addytywne: $f(\vec{x}+\vec{y}) = f(\vec{x})+f(\vec{y})$, oraz jednorodne: $f(a\vec{x}) = af(\vec{x})$, a także spełnią równość $f(\vec{0}) = \vec{0}$. Funkcje liniowe przyjmujące wartości w szczególnej przestrzeni liniowej jaką jest ciało R nazywamy funkcjonałami.

Zauważmy też, że homomorfizmy modułów są w szczególności homomorfizmami grup addytywnych modułów.

9.8 Pewien sposób definiowania homomorfizmów

Znając wartości homomorfizmu $f : M_1 \to M_2$ na zbiorze generatorów modułu M_1 potrafimy obliczyć jego wartości dla dowolnego elementu M_1. Jeżeli X jest zbiorem generatorów modułu M_1 i $\vec{x} \in M_1$, to aby obliczyć $f(\vec{x})$ najpierw przedstawiamy wektor $\vec{x}$ w postaci kombinacji liniowej generatorów $\vec{a}_1, \ldots, \vec{a}_n \in X$. Jeżeli

$$\vec{x} = \sum_{i=1}^{n} x_i \vec{a}_i,$$

to wartość $f(\vec{x})$ obliczamy zgodnie ze wzorem

$$f(\vec{x}) = f(\sum_{i=1}^{n} x_i \vec{a}_i) = \sum_{i=1}^{n} x_i f(\vec{a}_i).$$

Zachodzi więc następujący

Lemat 9.16 *Homomorfizmy przyjmujące te same wartości na zbiorze generatorów modułu są równe.* □

Dowolna baza jest zbiorem „wolnych” (albo „niepowiązanych”) generatorów. Konsekwencją tego jest możliwość dowolnego określania funkcji liniowych dla elementów bazy. Jeżeli X jest bazą przestrzeni M_1, a $f : X \to M_2$ jest dowolną funkcją przyjmującą wartości w module M_2, to istnieje homomorfizm $F : M_1 \to M_2$ taki, że $F(\vec{a}) = f(\vec{a})$ dla dowolnego $\vec{a} \in X$. Funkcję F definiujemy przyjmując, że

$$F(\vec{x}) = \sum_{i=1}^{n} x_i f(\vec{a}_i),$$

gdzie $x_1, \ldots, x_n$ są współrzędnymi wektora $\vec{x}$ w bazie X. Jest to poprawna definicja, gdyż współrzędne wektora w dowolnej bazie są wyznaczone jednoznacznie. Łatwo przekonać się, że jest to definicja funkcji liniowej.

Twierdzenie 9.17 *Każda funkcja określona na bazie modułu M_1 i przyjmująca wartości w module M_2 rozszerza się jednoznacznie do homomorfizmu określonego na M_1 i przyjmującego wartości w M_2.* □

10.1 Badanie podstawowych własności homomorfizmów

Mając homomorfizm zdefiniowany tak, jak to zostało opisane w rozdziale 9.8, łatwo można ustalić, czy jest on różnowartościowy lub typu „na".

Lemat 10.1 *Przypuśćmy, że X jest bazą modułu M_1 i $f : M_1 \to M_2$ jest homomorfizmem. Funkcja f jest typu „na" wtedy i tylko wtedy, gdy obraz $\vec{f}(X)$ jest zbiorem generatorów modułu M_2. Funkcja f jest różnowartościowa wtedy i tylko wtedy, gdy obraz $\vec{f}(X)$ jest liniowo niezależny.*

Dowód. Pierwsza część tezy wynika z wzoru

$$\sum_{i=1}^{n} x_i f(\vec{a}_i) = f(\sum_{i=1}^{n} x_i \vec{a}_i).$$

Dalej będziemy dowodzić tylko druga część.

Przypuśćmy najpierw, że funkcja f jest różnowartościowa i weźmy kombinację liniową wektorów z $\vec{f}(X)$ równą zero:

$$\vec{0} = \sum_{i=1}^{n} x_i f(\vec{a}_i) = f(\sum_{i=1}^{n} x_i \vec{a}_i).$$

Z różnowartościowości f i równości $f(\vec{0}) = \vec{0}$ wynika, że

$$\sum_{i=1}^{n} x_i \vec{a}_i = \vec{0},$$

a ponieważ wektory $\vec{a}_i$ należą do bazy X, więc $x_i = 0$ dla $i = 1, \ldots, n$. W ten sposób dowiedliśmy, że obraz $\vec{f}(X)$ jest liniowo niezależny.

Jeżeli natomiast funkcja f nie jest różnowartościowa, to istnieją dwie różne kombinacje liniowe wektorów z X przekształcane przez f na ten sam wektor $\vec{x}$. Tak więc

$$f(\sum_{i=1}^{n} x_i \vec{a}_i) = \vec{x} = f(\sum_{i=1}^{n} y_i \vec{a}_i)$$

dla różnych układów współczynników $x_1, \ldots, x_n$ i $y_1, \ldots, y_n$. Wtedy jednak wektor $\vec{x}$ ma różne przedstawienia

$$\sum_{i=1}^{n} x_i f(\vec{a}_i) = \vec{x} = \sum_{i=1}^{n} y_i f(\vec{a}_i)$$

w postaci kombinacji liniowej wektorów z $\vec{f}(X)$. Oznacza to, że $\vec{f}(X)$ jest liniowo zależny. □

10.2 Rola pojęcia wymiaru

Twierdzenie 10.2 *Każde dwa moduły wymiaru n nad dowolnym pierścieniem są izomorficzne, a więc istnieje różnowartościowa funkcja liniowa przekształcająca jeden z nich na drugi.*

Dowód. Przypuśćmy, że mamy moduły M_1 i M_2 oraz bazy $\vec{a}_1, \ldots, \vec{a}_n$ i $\vec{b}_1, \ldots, \vec{b}_n$ w tych modułach. Weźmy funkcję f taką, że $f(\vec{a}_i) = \vec{b}_i$ dla $i = 1, \ldots, n$. Na podstawie twierdzenia 9.17 funkcję f można rozszerzyć do funkcji liniowej $F : M_1 \to M_2$. Z lematu 10.1 wynika, że funkcja F jest różnowartościowa i typu „na". □

10.3 Obrazy homomorficzne modułów

Podobnie jak w przypadku homomorfizmów grup, jądrem przekształcenia liniowego (homomorfizmu) $f : M_1 \to M_2$ nazywamy zbiór

$$ker(f) = \{\vec{x} \in M_1 : f(\vec{x}) = \vec{0}\}.$$

Jądro przekształcenia liniowego jest zamknięte ze względu na mnożenie przez elementy pierścienia R oraz ze względu na dodawanie (zamkniętość ze względu na dodawanie wynika z teorii grup). Tak więc jądro jest podmodułem.

Z własności homomorfizmów grup wynika również następujący

Wniosek 10.3 *Przekształcenie liniowe jest różnowartościowe wtedy i tylko wtedy, gdy jego jądro jest jednoelementowe.* □

Rolę dzielników normalnych w teorii modułów pełnią podmoduły. W szczególności, mamy odpowiedniość między podmodułami modułu i jego obrazami homomorficznymi. Można się o tym przekonać odpowiednio uzupełniając konstrukcję ilorazową znaną z teorii grup.

Przypuśćmy, że I jest podmodułem modułu M nad pierścieniem R. Wtedy M jest grupą przemienną oraz I jest dzielnikiem normalnym M. Możemy więc utworzyć grupę ilorazową M/I (patrz rozdział 7.4). Grupa ta jest obrazem grupy addytywnej M wyznaczonym przez homomorfizm (grup) $\chi : M \to M/I$ zdefiniowany wzorem

$$\chi(x) = x + I = \{x + y \mid y \in I\}$$

(zauważmy, że teraz działanie grupowe oznaczamy symbolem $+$) i jest przemienna jako obraz homomorficzny grupy przemiennej. Oczywiście, I jest jądrem tego homomorfizmu (patrz rozdział 7.4).

W grupie M/I wzorem

$$a(x + I) = ax + I$$

definiujemy dodatkowo mnożenie przez elementy R. Wątpliwości może budzić poprawność tej definicji. Warunek $x + I = y + I$ jest jednak równoważny $x - y \in I$. Wobec tego, jeżeli $x + I = y + I$, to $x - y \in I$ oraz

$$a(x - y) = ax - ay \in I$$

(ponieważ I jest podmodułem). Stąd otrzymujemy, że $ax + I = ay + I$. Dowodzi to poprawności podanej definicji.

Wzór na mnożenie w M/I gwarantuje, że χ zachowuje także mnożenie przez elementy R i jest homomorfizmem modułu M na algebra M/I. Algebra ta jest więc modułem. W ten sposób dowiedliśmy

Twierdzenie 10.4 *Jeżeli I jest podmodułem modułu M, to istnieje homomorfizm (modułów) określony na M, którego jądrem jest I.* □

Zachodzi także

Twierdzenie 10.5 *Jeżeli dwa homomofizmy modułu M mają to samo jądro, to wyznaczone przez nie obrazy homomorficzne są izomorficzne.*

Dowód. Twierdzenie to dowodzimy tak, jak wniosek 7.4 dodatkowo sprawdzając, że skonstruowany izomorfizm grup zachowuje także mnożenie przez elementy pierścienia. □

Aby skonstruować przekształcenie liniowe przestrzeni V o jądrze równym podprzestrzeni V', możemy też skonstruować bazę X przestrzeni V zawierającą bazę podprzestrzeni V' (w przypadku przestrzeni skończonego wymiaru istnienie takiej bazy wynika z lematu o wymianie). Następnie definiujemy funkcję $f : X \to V$ przyjmując, że

$$f(\vec{x}) = \begin{cases} \vec{0} & \text{jeżeli } \vec{x} \in V', \\ \vec{x} & \text{w przeciwnym razie} \end{cases}$$

i rozszerzamy ją do przekształcenia liniowego F określonego na V. Jądrem przekształcenia F jest V'.

Dla przestrzeni skończonego wymiaru fakt, że jądro wyznacza obraz homomorficzny z dokładnością do izomorfizmu wynika też z następującego twierdzenia:

Twierdzenie 10.6 *Niech V_1 będzie przestrzenią liniową wymiaru n. Jeżeli funkcja liniowa $f : V_1 \to V_2$ przekształca V_1 na V_2, to przestrzeń V_2 jest skończenie generowalna i liczba n jest sumą wymiarów przestrzeni V_2 i jądra przekształcenia f.*

Dowód. Jeżeli X jest bazą przestrzeni V_1 i f jest typu „na", to $\vec{f}(X)$ jest zbiorem skończonym generującym V_2. Przestrzeń V_2 jest więc skończenie generowalna i ma skończoną bazę.

Niech $\vec{a}_1, \ldots, \vec{a}_m$ będzie bazą V_2. Dla $i = 1, \ldots, m$ weźmy wektor $\vec{b}_i \in V_1$ taki, że $f(\vec{b}_i) = \vec{a}_i$. Weźmy też bazę $\vec{c}_1, \ldots, \vec{c}_k$ jądra przekształcenia f. Zauważmy, że $\vec{b}_i \neq \vec{c}_j$, gdyż w przeciwnym razie $\vec{a}_i = f(\vec{b}_i) = f(\vec{c}_j) = \vec{0}$ i w bazie $\vec{a}_1, \ldots, \vec{a}_m$ znalazłby się wektor $\vec{0}$. Wobec tego, ciąg $\vec{b}_1, \ldots, \vec{b}_m, \vec{c}_1, \ldots, \vec{c}_k$ ma $m + k$ elementów. Pokażemy, że wektory z tego ciągu tworzą bazę przestrzeni V_1 i to zakończy dowód.

Najpierw dowiedziemy liniową niezależność tych wektorów. Przypuśćmy więc, że

$$\sum_{i=1}^{m} \beta_i \vec{b}_i + \sum_{i=1}^{k} \gamma_i \vec{c}_i = \vec{0}.$$

Wtedy

$$\vec{0} = f(\vec{0}) = f(\sum_{i=1}^{m} \beta_i \vec{b}_i + \sum_{i=1}^{k} \gamma_i \vec{c}_i) = \sum_{i=1}^{m} \beta_i f(\vec{b}_i) + \sum_{i=1}^{k} \gamma_i f(\vec{c}_i) = \sum_{i=1}^{m} \beta_i \vec{a}_i.$$

Ponieważ wektory $\vec{a}_1, \ldots, \vec{a}_m$ są bazą V_2, więc $\beta_i = 0$ dla $i = 1, \ldots, m$. Fakt ten implikuje dodatkowo, że

$$\sum_{i=1}^{k} \gamma_i \vec{c}_i = \vec{0}.$$

Jeżeli teraz skorzystamy z tego, że wektory $\vec{c}_1, \ldots, \vec{c}_k$ są liniowo niezależne, to otrzymamy, że także $\gamma_i = 0$ dla $i = 1, \ldots, k$ i w ten sposób zakończymy dowód niezależności.

Pokażemy jeszcze, że każdy wektor $\vec{x} \in V_1$ jest kombinacją liniową wektorów $\vec{b}_1, \ldots, \vec{b}_m$, $\vec{c}_1, \ldots, \vec{c}_k$. Przedstawmy $f(\vec{x})$ w postaci

$$f(\vec{x}) = \sum_{i=1}^{m} \beta_i \vec{a}_i = f(\sum_{i=1}^{m} \beta_i \vec{b}_i)$$

dla pewnych β_i. Stąd otrzymujemy, że

$$\vec{x} - \sum_{i=1}^{m} \beta_i \vec{b}_i$$

należy do jądra przekształcenia f i jest równy

$$\sum_{i=1}^{k} \gamma_i \vec{c}_i$$

dla pewnych γ_i. W ten sposób dowiedliśmy, że

$$\vec{x} = \sum_{i=1}^{m} \beta_i \vec{b}_i + \sum_{i=1}^{k} \gamma_i \vec{c}_i. \quad \square$$

10.4 Działania w zbiorze homomorfizmów

Przypuśćmy, że M_1 i M_2 są modułami nad pierścieniem R. Niech $L(M_1, M_2)$ oznacza zbiór wszystkich homomorfizmów (przekształceń liniowych) określonych w M_1 i przyjmujących wartości w M_2. Przekształcenia należące do $L(M_1, M_2)$ dodajemy i mnożymy przez elementy R w zwykły sposób:

$$(f_1 + f_2)(\vec{x}) = f_1(\vec{x}) + f_2(\vec{x})$$

oraz

$$(af)(\vec{x}) = af(\vec{x}).$$

Bez trudu dowodzimy, że oba te działania nie wyprowadzają poza $L(M_1, M_2)$. Stąd otrzymujemy, że zbiór $L(M_1, M_2)$ jest podmodułem modułu $M_2^{M_1}$ (patrz rozdział 8.6).

Wniosek 10.7 *Zbiór $L(M_1, M_2)$ z wyżej zdefiniowanymi działaniami jest modułem nad pierścieniem R.* □

10.5 Algebry

Słowo *algebra* oznacza także specyficzną algebrę. Przypuśćmy, że mamy dany przemienny pierścień R z jednością. Zbiór A, którego elementy potrafimy dodawać, mnożyć przez siebie i mnożyć przez elementy pierścienia R nazywamy *R-algebrą*, jeżeli

1. z dodawaniem i mnożeniem przez elementy R jest modułem nad R oraz
2. z dodawaniem i mnożeniem jest pierścieniem z jednością.

10.6 Złożenie homomorfizmów (funkcji liniowych)

Dla dowolnych przekształceń $f_1 \in L(M_2, M_3)$ i $f_2 \in L(M_1, M_2)$ w zwykły sposób definiujemy złożenie $f_1 f_2$ przyjmując, że

$$(f_1 f_2)(\vec{x}) = f_1(f_2(\vec{x})).$$

Oczywiście, składanie jest operacją łączną. Ponadto złożenie homomorfizmów jest homomorfizmem (a więc $f_1 f_2 \in L(M_1, M_3)$). Wynika to z następujących rachunków:

$$\begin{aligned}(f_1 f_2)(a\vec{x} + b\vec{y}) &= f_1(f_2(a\vec{x} + b\vec{y})) = f_1(af_2(\vec{x}) + bf_2(\vec{y})) = \\ &= af_1(f_2(\vec{x})) + bf_1(f_2(\vec{y})) = a(f_1 f_2)(\vec{x}) + b(f_1 f_2)(\vec{y}).\end{aligned}$$

Także bez trudu dowodzi się, że składanie jest rozdzielne względem dodawania. Jeżeli $f \in L(M_2, M_3)$ i $f_1, f_2 : M_1 \to M_2$, to dla dowolnego wektora $\vec{x} \in M_1$ zachodzą równości

$$\begin{aligned}(f(f_1 + f_2))(\vec{x}) &= f((f_1 + f_2)(\vec{x})) = f(f_1(\vec{x}) + f_2(\vec{x})) = f(f_1(\vec{x})) + f(f_2(\vec{x})) = \\ &= (ff_1)(\vec{x}) + (ff_2)(\vec{x}) = (ff_1 + ff_2)(\vec{x}),\end{aligned}$$

czyli $f(f_1 + f_2) = ff_1 + ff_2$ (zauważmy, że wykorzystaliśmy addytywność f).

Podobnie, jeżeli $f_1, f_2 : M_2 \to M_3$ i $f : M_1 \to M_2$, to dla dowolnego wektora $\vec{x} \in M_1$ zachodzą równości

$$\begin{aligned}((f_1 + f_2)f)(\vec{x}) &= (f_1 + f_2)(f(\vec{x})) = f_1(f(\vec{x})) + f_2(f(\vec{x})) = \\ &= (f_1 f)(\vec{x}) + (f_2 f)(\vec{x}) = (f_1 f + f_2 f)(\vec{x}),\end{aligned}$$

a więc mamy $(f_1 + f_2)f = f_1 f + f_2 f$ (ten wzór jest konsekwencją definicji sumy funkcji).

Jest oczywiste, że przekształcenie indentycznościowe I jest homomorfizmem, a więc $I \in L(M, M)$ dla dowolnego modułu M (oznaczenie I jest uproszczone, powinno zawierać także zawierać informacje o dziedzinie przekształcenia). Jeżeli $f : M_1 \to M_2$, a $I \in L(M_1, M_1)$, to $fI = f$. Jeżeli natomiast $f : M_1 \to M_2$ oraz $I \in L(M_2, M_2)$, to $If = f$.

Z przeprowadzonych rozważań wynika

Twierdzenie 10.8 *Jeżeli M jest modułem nad pierścieniem R, to zbiór $L(M, M)$ z dodawaniem, mnożeniem przez elementy R oraz z mnożeniem zdefiniowanym jako złożenie jest R-algebrą.* □

10.7 Macierze

Macierz o n kolumnach i m wierszach (albo o wymiarach $n \times m$, albo też o m wierszach długości n) możemy zdefiniować jako funkcję określoną w zbiorze $\{1, \ldots, m\} \times \{1, \ldots, n\}$. Jeżeli A jest taką funkcją oraz $A(i, j) = a_{i,j}$, to A przedstawiamy jako tablicę

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ & & \ddots & \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{bmatrix}.$$

Czasami wektory będzie wygodnie uważać za specyficzne macierze. W takiej sytuacji wektor $(x_1, x_2, \ldots, x_n)$ będziemy uważać za macierz jednokolumnową zgodnie ze wzorem

$$(x_1, x_2, \ldots, x_n) = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

W wielu książkach – przeciwnie – wektor $(x_1, x_2, \ldots, x_n)$ utożsamia się z macierzą $[x_1, x_2, \ldots, x_n]$.

10.8 Iloczyn skalarny

Przypuśćmy, że mamy wektory $\vec{x}, \vec{y} \in R^n$, $\vec{x} = (x_1, \ldots, x_n)$ i $\vec{y} = (y_1, \ldots, y_n)$. *Iloczynem skalarnym* wektorów $\vec{x}$ i $\vec{y}$ nazywamy skalar $\vec{x}\vec{y} \in R$ zdefiniowany wzorem

$$\vec{x}\vec{y} = \sum_{i=1}^{n} x_i y_i.$$

Iloczyn skalarny jest ważną funkcją. W szkole średniej podawana jest interpretacja geometryczna iloczynu skalarnego. Dla nas w tej chwili będzie to tylko wygodne oznaczenie.

Jest to funkcja liniowa względem każdej zmiennej:

$$\vec{x}(a\vec{y} + b\vec{z}) = a\vec{x}\vec{y} + b\vec{x}\vec{z} \text{ oraz } (a\vec{x} + b\vec{y})\vec{z} = a\vec{y}\vec{z} + b\vec{y}\vec{z}.$$

Funkcje o takich własnościach nazywamy *dwuliniowymi*. Ponadto, jeżeli mnożymy wektory o współrzędnych należących do pierścienia przemiennego, jest to funkcja *symetryczna*, czyli spełniająca równość $\vec{x}\vec{y} = \vec{y}\vec{x}$.

10.9 Macierz przekształcenia liniowego

Do końca wykładu 10 będziemy rozważać dwa moduły M_1 i M_2 nad pierścieniem R oraz bazy $\vec{a}_1, \ldots, \vec{a}_n$ modułu M_1 i $\vec{b}_1, \ldots, \vec{b}_m$ modułu M_2.

Przypuśćmy, że mamy przekształcenie liniowe $f : M_1 \to M_2$. Każdy z wektorów $f(\vec{a}_i) \in M_2$ przedstawiamy jako kombinację liniową wektorów $\vec{b}_1, \ldots, \vec{b}_m$. Jeżeli

$$f(\vec{a}_i) = \sum_{j=1}^{m} c_{j,i}\vec{b}_j.$$

to macierz

$$\begin{bmatrix} c_{1,1} & c_{1,2} & \ldots & c_{1,n} \\ c_{2,1} & c_{2,2} & \ldots & c_{2,n} \\ & & \ddots & \\ c_{m,1} & c_{m,2} & \ldots & c_{m,n} \end{bmatrix} \tag{3}$$

nazywamy *macierzą przekształcenia* f wyznaczoną przez bazy $\vec{a}_1, \ldots, \vec{a}_n$ oraz $\vec{b}_1, \ldots, \vec{b}_m$.

Zauważmy, że i-ta kolumna macierzy funkcji f zawiera współrzędne w bazie $\vec{b}_1, \ldots, \vec{b}_m$ wektora $f(\vec{a}_i)$, a więc znając ją potrafimy obliczyć $f(\vec{a}_i)$. Znając całą macierz przekształcenia f potrafi obliczyć wartości $f(\vec{a}_i)$ dla wektorów z bazy $\vec{a}_1, \ldots, \vec{a}_n$.

Niech $M_{n,m}$ oznacza zbiór macierzy o wyrazach z pierścienia R mających n kolumn i m wierszy. Dla $f \in L(M_1, M_2)$ przyjmijmy, że $\mu(f) \in M_{n,m}$ oznacza macierz przekształcenia f wyznaczoną przez ustalone bazy.

Lemat 10.9 *Funkcja μ, które przekształceniu liniowemu $f \in L(M_1, M_2)$ przyporządkowuje macierz $\mu(f)$ tego przekształcenia, przekształca $L(M_1, M_2)$ wzajemnie jednoznacznie na $M_{n,m}$.*

Dowód. Znając macierz przekształcenia znamy wartości przekształcenia dla argumentów należących do pewnej bazy. Stąd, na podstawie faktu 9.16 otrzymujemy, że istnieje najwyżej jedno przekształcenie o danej macierzy, a więc μ jest różnowartościowa. Korzystając z lematu 9.17 potrafimy skonstruować przekształcenie, którego macierzą jest dana macierz. W ten sposób dowodzimy, że μ jest typu „na". □

10.10 Macierz sumy przekształceń

Przypuśćmy, że mamy przekształcenia liniowe $f, g \in L(M_1, M_2)$. Niech

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} \\ & & \ddots & \\ \alpha_{m,1} & \alpha_{m,2} & \ldots & \alpha_{m,n} \end{bmatrix} \text{ i } B = \begin{bmatrix} \beta_{1,1} & \beta_{1,2} & \ldots & \beta_{1,n} \\ \beta_{2,1} & \beta_{2,2} & \ldots & \beta_{2,n} \\ & & \ddots & \\ \beta_{m,1} & \beta_{m,2} & \ldots & \beta_{m,n} \end{bmatrix} \tag{4}$$

będą odpowiednio macierzami przekształceń f i g (względem ustalonych baz). Znajdziemy macierz przekształcenia $f+g$. W tym celu musimy wyliczyć współrzędne wektorów $(f+g)(\vec{a}_i)$. Oczywiście,

$$f(\vec{a}_i) = \sum_{j=1}^{m} \alpha_{j,i}\vec{b}_j \text{ oraz } g(\vec{a}_i) = \sum_{j=1}^{m} \beta_{j,i}\vec{b}_j.$$

Wobec tego,

$$(f+g)(\vec{a}_i) = f(\vec{a}_i) + g(\vec{a}_i) = \sum_{j=1}^{m} \alpha_j\vec{b}_{j,i} + \sum_{j=1}^{m} \beta_{j,i}\vec{b}_j = \sum_{j=1}^{m} (\alpha_{j,i} + \beta_{j,i})\vec{b}_j.$$

Współrzędnymi $(f+g)(\vec{a}_i)$ są elementy $\alpha_{1,i} + \beta_{1,i}, \ldots, \alpha_{m,i} + \beta_{m,i}$, a więc przekształcenie $f+g$ ma macierz

$$\begin{bmatrix} \alpha_{1,1} + \beta_{1,1} & \alpha_{1,2} + \beta_{1,2} & \ldots & \alpha_{1,n} + \beta_{1,n} \\ \alpha_{2,1} + \beta_{2,1} & \alpha_{2,2} + \beta_{2,2} & \ldots & \alpha_{2,n} + \beta_{2,n} \\ & & \ddots & \\ \alpha_{m,1} + \beta_{m,1} & \alpha_{m,2} + \beta_{m,2} & \ldots & \alpha_{m,n} + \beta_{m,n} \end{bmatrix}.$$

10.11 Macierz iloczynu przekształcenia i skalaru

Przypuśćmy, że mamy przekształcenie liniowe $f \in L(M_1, M_2)$ o macierzy A z wzoru (4). Dla $c \in R$ znajdziemy macierz przekształcenia cf. Oczywiście,

$$(cf)(\vec{a}_i) = c(f(\vec{a}_i)) = c\sum_{j=1}^{m} \alpha_{j,i}\vec{b}_j = \sum_{j=1}^{m} (c\alpha_{j,i})\vec{b}_j.$$

Wobec tego, macierzą przekształcenia cf jest

$$\begin{bmatrix} c\alpha_{1,1} & c\alpha_{1,2} & \ldots & c\alpha_{1,n} \\ c\alpha_{2,1} & c\alpha_{2,2} & \ldots & c\alpha_{2,n} \\ & & \ddots & \\ c\alpha_{m,1} & c\alpha_{m,2} & \ldots & c\alpha_{m,n} \end{bmatrix}.$$

10.12 Dodawanie macierzy i mnożenie ich przez skalary

W zbiorze $M_{n,m}$ definiujemy działania tak, aby funkcja μ przyporządkowująca przekształceniu $f \in L(M_1, M_2)$ macierz $\mu(f)$ tego przekształcenia była izomorfizmem. Sumą $A + B$ macierzy A i B z wzoru (4) jest więc macierz

$$\begin{bmatrix} \alpha_{1,1} + \beta_{1,1} & \alpha_{1,2} + \beta_{1,2} & \ldots & \alpha_{1,n} + \beta_{1,n} \\ \alpha_{2,1} + \beta_{2,1} & \alpha_{2,2} + \beta_{2,2} & \ldots & \alpha_{2,n} + \beta_{2,n} \\ & & \ddots & \\ \alpha_{m,1} + \beta_{m,1} & \alpha_{m,2} + \beta_{m,2} & \ldots & \alpha_{m,n} + \beta_{m,n} \end{bmatrix},$$

a iloczynem cA macierzy A i skalaru c jest macierz

$$\begin{bmatrix} c\alpha_{1,1} & c\alpha_{1,2} & \ldots & c\alpha_{1,n} \\ c\alpha_{2,1} & c\alpha_{2,2} & \ldots & c\alpha_{2,n} \\ & & \ddots & \\ c\alpha_{m,1} & c\alpha_{m,2} & \ldots & c\alpha_{m,n} \end{bmatrix}.$$

Zbiór $M_{n,m}$ z tak zdefiniowanymi działaniami jest izomorficzny z $L(M_1, M_2)$ i jest modułem.

10.13 Współrzędne wartości przekształcenia

Znowu zakładamy, że mamy przekształcenia liniowe $f, g \in L(M_1, M_2)$. Niech A będzie macierzą przekształcenia f (patrz wzór (4)). Weźmy wektor $\vec{x} \in M_1$. Będziemy obliczać współrzędne wektora $f(\vec{x})$ w bazie $\vec{b}_1, \ldots, \vec{b}_m$.

Przypuśćmy, że wektor $\vec{x}$ ma w bazie $\vec{a}_1, \ldots, \vec{a}_n$ przedstawienie dane wzorem

$$\vec{x} = \sum_{i=1}^{n} x_i\vec{a}_i. \tag{5}$$

Wtedy

$$f(\vec{x}) = f(\sum_{i=1}^{n} x_i\vec{a}_i) = \sum_{i=1}^{n} x_i f(\vec{a}_i) = \sum_{i=1}^{n} x_i(\sum_{j=1}^{m} \alpha_{j,i}\vec{b}_j) = \sum_{j=1}^{m}(\sum_{i=1}^{n} x_i\alpha_{j,i})\vec{b}_j.$$

Tak więc $f(\vec{x})$ jest wektorem, który w bazie $\vec{b}_1, \ldots, \vec{b}_m$ ma współrzędne

$$\sum_{i=1}^{n} x_i\alpha_{1,i}, \ldots, \sum_{i=1}^{n} x_i\alpha_{m,i}.$$

Dalsze rozważania będziemy prowadzić przy dodatkowych założeniach, że $M_1 = R^n$ oraz $M_2 = R^m$. Będziemy też zakładać, że bazy $\vec{a}_1, \ldots, \vec{a}_n$ oraz $\vec{b}_1, \ldots, \vec{b}_m$ są bazami standardowymi. Założenia te nie są istotne. Ich przyjęcie jednak zdecydowanie uprości dalszy tekst. Nie będziemy musieli rozróżniać miedzy wektorem $\vec{x} \in M_1$ i ciągiem-wektorem $(x_1, x_2, \ldots, x_n) \in R^n$ jego współrzednych. Z przyjętych założeń wynika, że wzór (5) jest równoważny równości $\vec{x} = (x_1, x_2, \ldots, x_n)$.

Niech $\vec{\alpha}_i$ będzie i-tym wierszem macierzy przekształcenia f, a więc $\vec{\alpha}_i = (\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,n})$. Z przeprowadzonych rachunków wynika, że i-ta współrzędna wektora $f(\vec{x})$ jest równa iloczynowi skalarnemu $\vec{\alpha}_i\vec{x}$. Ponieważ założyliśmy, że rozważamy współrzędne w bazie standardowej, więc

$$f(\vec{x}) = (\vec{\alpha}_1\vec{x}, \vec{\alpha}_2\vec{x}, \ldots, \vec{\alpha}_m\vec{x}). \tag{6}$$

Z przedstawionych rozważań wynika, że każda funkcja liniowa przekształcająca R^n w R^m daje się zdefiniować wzorem postaci (6). Liniowość iloczynu skalarnego względem drugiego argumentu implikuje także, że każda funkcja zdefiniowana wzorem (6) jest liniowa.

10.14 Iloczyn macierzy: przypadek szczególny

Przypuśćmy, że mamy dwie macierze A i B. Iloczyn AB tych macierzy definiujemy tylko wtedy, gdy liczba kolumn (długość wierszy) macierz A jest równa liczbie wierszy (czyli długości kolumn) macierzy B. Teraz zajmiemy się przypadkiem, gdy B ma jedną kolumnę. Umówiliśmy się wcześmiej, że wektor $(x_1, x_2, \ldots, x_n)$ uważamy za jednokolumnową macierz, której kolejne wyrazy od góry są równe $x_1, x_2, \ldots, x_n$.

Niech A będzie macierzą z wzoru (4). Przyjmijmy, że $\vec{\alpha}_i = (\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,n})$ jest i-tym wierszem macierzy A. Weźmy też wektor $\vec{x} = (x_1, x_2, \ldots, x_n) \in R^n$. Iloczyn $A\vec{x}$ macierzy A i jednokolumnowej macierzy $\vec{x}$ definiujemy wzorem

$$A\vec{x} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} \\ & & \ddots & \\ \alpha_{m,1} & \alpha_{m,2} & \ldots & \alpha_{m,n} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \vec{\alpha}_1\vec{x} \\ \vec{\alpha}_2\vec{x} \\ \vdots \\ \vec{\alpha}_n\vec{x} \end{bmatrix}$$

(postać wzoru sugeruje, że A i $\vec{x}$ mają tyle samo wierszy, ale tak być nie musi).

Oczywistą konsekwencją przyjętej definicji jest wzór

$$f(\vec{x}) = A\vec{x}, \tag{7}$$

gdzie $f : R^n \to R^m$ jest funkcją liniową i A jest macierzą f wyznaczoną przez bazy standardowe. Łatwo też korzystając z dwuliniowości iloczynu skalarnego dowieść następujące wzory:

$$(A + B)\vec{x} = a\vec{x} = B\vec{x} \text{ oraz } A(\vec{x} + \vec{y}) = A\vec{x} + A\vec{y}.$$

10.15 „Łączenie" macierzy

Operacja „łączenia" jest uogólnieniem konkatenacji (łączenia) ciągów. Przypuśćmy, że mamy dwie macierze

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} \\ & & \ddots & \\ \alpha_{m,1} & \alpha_{m,2} & \ldots & \alpha_{m,n} \end{bmatrix} \text{ i } B = \begin{bmatrix} \beta_{1,1} & \beta_{1,2} & \ldots & \beta_{1,k} \\ \beta_{2,1} & \beta_{2,2} & \ldots & \beta_{2,k} \\ & & \ddots & \\ \beta_{l,1} & \beta_{l,2} & \ldots & \beta_{l,k} \end{bmatrix}.$$

Jeżeli macierze A i B mają tyle samo wierszy (jeżeli $m = l$), to możemy je połączyć i utworzyć macierz

$$[A\ B] = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} & \beta_{1,1} & \beta_{1,2} & \ldots & \beta_{1,k} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} & \beta_{2,1} & \beta_{2,2} & \ldots & \beta_{2,k} \\ & & \ddots & & & & & \\ \alpha_{m,1} & \alpha_{m,2} & \ldots & \alpha_{m,n} & \beta_{m,1} & \beta_{m,2} & \ldots & \beta_{m,k} \end{bmatrix}$$

W przypadku, gdy macierze A i B mają tyle samo kolumn (gdy $n = k$), to też możemy je połączyć tworząc macierz

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} \\ & & \ddots & \\ \alpha_{m,1} & \alpha_{m,2} & \ldots & \alpha_{m,n} \\ \beta_{1,1} & \beta_{1,2} & \ldots & \beta_{1,n} \\ \beta_{2,1} & \beta_{2,2} & \ldots & \beta_{2,n} \\ & & \ddots & \\ \beta_{l,1} & \beta_{l,2} & \ldots & \beta_{l,n} \end{bmatrix}.$$

Łatwy do sprawdzenia jest wzór

$$\begin{bmatrix} A \\ B \end{bmatrix}\vec{x} = \begin{bmatrix} A\vec{x} \\ B\vec{x} \end{bmatrix}.$$

10.16 Mnożenie macierzy

Zdefiniujemy teraz iloczyn AB dowolnych macierzy

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} \\ & & \ddots & \\ \alpha_{m,1} & \alpha_{m,2} & \ldots & \alpha_{m,n} \end{bmatrix} \text{ i } B = \begin{bmatrix} \beta_{1,1} & \beta_{1,2} & \ldots & \beta_{1,k} \\ \beta_{2,1} & \beta_{2,2} & \ldots & \beta_{2,k} \\ & & \ddots & \\ \beta_{n,1} & \beta_{n,2} & \ldots & \beta_{n,k} \end{bmatrix}$$

takich, że długość wierszy macierzy A jest równa długości kolumn macierzy B (wiersze macierzy A i kolumny macierzy B można mnożyć skalarnie). Przyjmijmy, że $\vec{\alpha}_i = (\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,n})$ jest i-tym wierszem macierzy A, a $\vec{\beta}_i = (\beta_{1,i}, \beta_{2,i}, \ldots, \beta_{n,i})$ – i-tą kolumną macierzy B. Iloczyn macierzy zdefiniujemy na trzy sposoby.

Po pierwsze chcemy, aby iloczyn macierzy miał własność

$$A[B_1\ B_2] = [AB_1\ AB_2]$$

dla dowolnych macierzy A, B_1 i B_2, gwarantujących wykonalność występujących w tym wzorze operacji. Wzór ten pozwala sprowadzić mnożenie macierzy do mnożenia macierzy przez macierz jednokolumnową i razem z definicją mnożenia przez pojedyńczą kolumnę można go uznać za definicję mnożenia dowolnych macierzy (patrz rozdział 10.14).

Posługując się „łączeniem" definicję *iloczynu macierzy* możemy wyrazić wzorem

$$AB = A[\vec{\beta}_1\ \vec{\beta}_2\ \ldots\ \vec{\beta}_k] = [A\vec{\beta}_1\ A\vec{\beta}_2\ \ldots\ A\vec{\beta}_k]. \tag{8}$$

Najczęściej *iloczyn* AB macierzy A o wymiarach $n \times m$ i macierzy B o wymiarach $k \times n$ definiujemy jako macierz o wymiarach $k \times m$, której wyraz $\gamma_{i,j}$ znajdujący się na przecięciu i-tego wiersza i j-tej kolumny jest dany wzorem

$$\gamma_{i,j} = \vec{\alpha}_i\vec{\beta}_j = \sum_{l=1}^{n} \alpha_{i,l}\beta_{l,j}.$$

Zakładając wykonalność odpowiednich operacji można dowieść następujące wzory:

1. $\begin{bmatrix} A \\ B \end{bmatrix} C = \begin{bmatrix} AC \\ BC \end{bmatrix}$.
2. $A(B + C) = AB + AC$ oraz $(A + B)C = AC + BC$.

11.1 Macierz złożenia przekształceń

Przypuśćmy, że mamy przekształcenia $f \in L(R^m, R^k)$ i $g \in L(R^n, R^m)$. Przyjmijmy, że A jest macierzą przekształcenia f, a B – macierzą przekształcenia g (dla uproszczenia załóżmy, że A i B są wyznaczone przez bazy standardowe). Znajdziemy macierz C złożenia fg.

Macierz przekształcenia g otrzymujemy obliczając wektory $g(\vec{e}_1), g(\vec{e}_2), \ldots, g(\vec{e}_n)$, przekształcając te wektory w jednokolumnowe macierze i łącząc te macierze. Tak więc

$$B = [g(\vec{e}_1)\ g(\vec{e}_2)\ \ldots\ g(\vec{e}_n)].$$

Podobnie

$$C = [(fg)(\vec{e}_1)\ (fg)(\vec{e}_2)\ \ldots\ (fg)(\vec{e}_n)].$$

Zauważmy, że zgodnie z definicją złożenia oraz wzorami (7) i (8)

$$C = [f(g(\vec{e}_1))\ f(g(\vec{e}_2))\ \ldots\ f(g((\vec{e}_n))] = [Ag(\vec{e}_1)\ Ag(\vec{e}_2)\ \ldots\ Ag((\vec{e}_n)] =$$
$$= A[g(\vec{e}_1)\ g(\vec{e}_2)\ \ldots\ g((\vec{e}_n)] = AB.$$

Lemat 11.1 *Macierzą złożenia przekształceń liniowych jest iloczyn macierzy tych przekształceń.* □

Wniosek 11.2 *Zbiór macierzy kwadratowych $M_{n,n}$ o wyrazach z pierścienia R z dodawaniem, mnożeniem i mnożeniem przez skalary należące do R jest R-algebrą izomorficzną z $L(R^n, R^n)$.* □

11.2 Macierze odwrotne

Zbiór macierzy kwadratowych $M_{n,n}$ o wyrazach z pierścienia R też jest pierścieniem z jednością. Jednością w tym pierścieniu jest macierz I, która na przekątnej ma wyrazy równe 1 (wyrazy postaci $a_{i,i} = 1$), a pozostałe wyrazy są równe 0. Łatwo sprawdza się, że $AI = IA = A$ dla dowolnej macierzy A.

Jeżeli macierz A ma w tym pierścieniu element odwrotny, to nazywamy go *macierzą odwrotną* i oznaczamy symbolem A^{-1}.

Lemat 11.3 *Przypuśćmy, że M jest modułem z n elementową bazą i A jest macierzą homomorfizmu $f : M \to M$. Macierz A jest odwracalna wtedy i tylko wtedy, gdy f jest izomorfizmem.* □

Lemat 11.4 *Jeżeli A i B są macierzami o wyrazach należących do ciała K, to następujące warunki są równoważne:*

1. *B jest macierzą odwrotna do A,*
2. *$AB = I$,*
3. *$BA = I$.*

Dowód. Lemat ten wynika z zadania 6 z listy 10. □

Najprostsza metoda znajdowanie macierzy odwrotnej polega na rozwiązywaniu równania $AX = I$.

11.3 Równania liniowe

Niech K będzie ciałem. *Równaniem liniowym* nazywamy równość postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

gdzie $a_1, a_2, \ldots, a_n, b \in K$, a $x_1, x_2, \ldots, x_n$ są zmiennymi o wartościach ze zbioru K.

Układem równań liniowych nazywamy kilka takich równości. Tak więc równości

$$\begin{array}{l} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n = b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,n}x_n = b_2, \\ \quad\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \ldots + a_{m,n}x_n = b_m \end{array} \tag{9}$$

tworzą układ m równań liniowych z n niewiadomymi.

Zbiór

$$\begin{array}{rl} \{(x_1, x_2, \ldots, x_n) \in K^n : & a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n = b_1 \wedge \\ & \wedge\, a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,n}x_n = b_2 \wedge \\ & \quad\vdots \\ & \wedge\, a_{m,1}x_1 + a_{m,2}x_2 + \ldots + a_{m,n}x_n = b_m\} \end{array}$$

nazywamy zbiorem rozwiązań układu (9), a jego elementy – rozwiązaniami tego układu. Będą nas interesować różne własności zbioru rozwiązań układu równań liniowych, a więc, czy jest niepusty (czy równanie ma chociaż jedno rozwiązanie, czyli problem niesprzeczności), jego struktura lub precyzyjny opis.

Macierz

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ & & \ddots & \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{bmatrix}$$

nazywamy *macierzą układu* (9), a macierz

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} & b_2 \\ & & \ddots & & \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} & b_m \end{bmatrix}$$

– jego *macierzą rozszerzoną* (o wektor wyrazów wolnych).

Przyjmijmy, że $\vec{\alpha}_i = (a_{i,1}, \ldots, a_{i,n})$ (tak więc $\vec{\alpha}_i$ jest i-tym wierszem macierzy układu (9)), $\vec{a}_j = (a_{1,j}, \ldots, a_{m,j})$ ($\vec{a}_j$ to j-ta kolumna) oraz $\vec{b} = (b_1, \ldots, b_m)$ ($\vec{b}$ jest kolumną wyrazów wolnych). Posługując się tymi oznaczeniami układowi równań (9) możemy nadać postać równania wektorowego

$$\vec{a}_1x_1 + \vec{a}_2x_2 + \ldots + \vec{a}_nx_n = \vec{b}.$$

Można też układowi (9) nadać postać o skróconym zapisie

$$\begin{array}{c} \vec{\alpha}_1\vec{x} = b_1, \\ \vec{\alpha}_2\vec{x} = b_2, \\ \vdots \\ \vec{\alpha}_m\vec{x} = b_m. \end{array}$$

Zdefiniujmy jeszcze funkcję $F : K^n \to K^m$ przyjmując, że

$$F(\vec{x}) = \begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ & & \ddots & \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}.$$

Oczywiście, F jest funkcją liniową i macierzą F wyznaczoną przez bazy standardowe jest macierz układu (9).

Nietrudno zauważyć, że

$$F(\vec{x}) = \begin{bmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \ldots + a_{m,n}x_n \end{bmatrix}$$

Lemat 11.5 *Wektor $\vec{x}$ spełnia układ* (9) *wtedy i tylko wtedy, gdy $F(\vec{x}) = \vec{b}$. Wobec tego zbiorem rozwiązań układu* (9) *jest $\{\vec{x} \in K^n : F(\vec{x}) = \vec{b}\}$* . □

11.4 Najprostsze własności

Lemat 11.6 *Jeżeli układ* (9) *ma dokładnie jedno rozwiązanie, to wektory $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ są liniowo niezależne. Jeżeli wektory $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ są liniowo niezależne, to układ* (9) *ma najwyżej jedno rozwiązanie.*

Dowód. Tezę dowodzonego lematu możemy wyprowadzić z lematu 9.1 posługując się postacią wektorową układu równań. □

11.5 Układy jednorodne

Układ (9) nazywamy *jednorodnym*, jeżeli $\vec{b} = \vec{0}$.

Lemat 11.7 *Przypuśćmy, że $F(\vec{c}) = \vec{b}$. Wtedy funkcja $p(\vec{x}) = \vec{x} + \vec{c}$ przekształca zbiór $\{\vec{x} \in K^n : F(\vec{x}) = \vec{0}\}$ wzajemnie jednoznacznie na zbiór $\{\vec{x} \in K^n : F(\vec{x}) = \vec{b}\}$ rozwiązań układu* (9).

Dowód. Funkcja p jest różnowartościowa na mocy prawa skracania. Przypuśćmy, że $F(\vec{x}) = \vec{0}$. Wtedy

$$F(p(\vec{x})) = F(\vec{x} + \vec{c}) = F(\vec{x}) + F(\vec{c}) = \vec{0} + \vec{b} = \vec{b}.$$

Jeżeli natomiast $F(\vec{x}) = \vec{b}$, to oczywiście $\vec{x}$ jest wartością $p(\vec{x} - \vec{c})$ oraz

$$F(\vec{x} - \vec{c}) = F(\vec{x}) - F(\vec{c}) = \vec{b} - \vec{(b)} = \vec{0}. \ \square$$

Z powyższego lematu wynika, że aby rozwiązać układ $F(\vec{x}) = \vec{b}$, trzeba znaleźć jedno rozwiązanie $\vec{c}$ tego układu i rozwiązać układ $F(\vec{x}) = \vec{0}$. Mając rozwiązanie układu $F(\vec{x}) = \vec{0}$, trzeba do każdego elementu tego rozwiązania dodać wektor $\vec{c}$ i w ten sposób otrzymamy rozwiązanie wyjściowego układu.

Z udowodnionego lematu wynika, że rozwiązywanie dowolnego układu równań liniowych sprowadza się do rozwiązywania układu jednorodnego. Zbiór rozwiązań jednorodnego układu $F(\vec{x}) = \vec{0}$ jest jądrem przekształcenia F.

Lemat 11.8 *Zbiór rozwiązań jednorodnego układu równań liniowych o n niewiadomych jest podprzestrzenią liniową przestrzeni K^n. W szczególności, wektor zerowy jest rozwiązaniem jednorodnego układu równań liniowych.* $\square$

11.6 Interpretacja geometryczna

Zbiory rozwiązań układu równań liniowych można opisać w języku geometrycznym. Jeżeli płaszczyznę utożsamimy z przestrzenią R^2, to podprzestrzeniami R^2 będą: zbiór, którego jedynym elementem jest początek układu współrzędnych $(\vec{0})$, proste przechodzące przez początek układu współrzędnych oraz cała płaszczyzna R^2. Tylko takie mogą być rozwiązania układu jednorodnego. Rozwiązaniami dowolnego układu są przesunięcia rozwiązań odpowiedniego układu jednorodnego, a więc dowolne punkty, dowolne proste oraz cała płaszczyzna. Rozwiązaniem może też być zbiór pusty. W przypadku układów równań z trzema zmiennymi, rozwiązaniami mogą być także dowolne płaszczyzny położone w przestrzeni (dla układów jednorodnych – zawierające $\vec{0}$) oraz cała przestrzeń R^3. Dla równań z większą liczbą niewiadomych sytuacja jest analogiczna.

11.7 Dopełnienie ortogonalne

Dla $X \subseteq K^n$ przyjmijmy, że

$$V_X = \{\sum_{i=1}^{k} v_i \vec{w_i} \in K^n : v_1, \ldots, v_k \in K \wedge \vec{w}_1 \ldots, \vec{w}_k \in X\}.$$

Zbiór V_X jest więc podprzestrzenią K^n generowaną przez X.

Przyjmijmy też, że

$$X^{\perp} = \{\vec{x} \in K^n : \forall \vec{a} \in X \ \vec{a}\vec{x} = 0\}.$$

Zbiór $X^{\perp}$ nazywamy *dopełnieniem ortogonalnym* X. Zauważmy, że jeżeli $X = \{\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_m\}$ i $\vec{b} = \vec{0}$, to $X^{\perp}$ jest zbiorem rozwiązań układu (9).

Wektory $\vec{a}$ i $\vec{x}$ nazywamy ortogonalnymi wtedy i tylko wtedy, gdy $\vec{a}\vec{x} = 0$. Te definicje wiążą się ze znaną ze szkoły charakteryzacją iloczynu skalarnego: iloczyn skalarny dwóch wektorów jest iloczynem długości tych wektorów i cosinusa kąta między wektorami. Stąd oczywiście wynika, że iloczyn skalarny dwóch niezerowych wektorów jest równy 0 wtedy i tylko wtedy, gdy cosinus kąta między wektorami jest równy 0, a więc, gdy wektory te są prostopadłe (ortogonalne).

Lemat 11.9 *Dopełnienie ortogonalne $X^{\perp}$ ma dla dowolnych $X, Y \subseteq K^n$ następujące własności:*

1. *jeżeli $X \subseteq Y$, to $Y^{\perp} \subseteq X^{\perp}$,*
2. *$X^{\perp} \subseteq V_X^{\perp}$, a więc także $X^{\perp} = V_X^{\perp}$,*
3. *$X^{\perp}$ jest podprzestrzenią liniową,*
4. *$V_X \subseteq (X^{\perp})^{\perp}$.*

Dowód. Punkt 1) jest oczywisty. Jeżeli wektory $\vec{x}$ i $\vec{y}$ są ortogonalne do $\vec{a}$, to oczywiście (wystarczy policzyć odpowiedni iloczyn) dowolna ich kombinacja liniowa też jest ortogonalna do $\vec{a}$. Stąd wynika punkt 3), a także pierwsza część punktu 2). Część druga punktu 2) wynika z części pierwszej i punktu 1).

Aby dowieść punkt 4) weźmy dowolny wektor $\vec{v} \in V_X$. Jeżeli $\vec{y}$ jest dowolnym wektorem ze zbioru $X^{\perp}$, to – na podstawie punktu 2) – $\vec{y} \in V_X^{\perp}$, a więc $\vec{y}\vec{v} = 0$. Tak więc zachodzi własność $\forall \vec{y} \in X^{\perp} \ \vec{y}\vec{v} = 0$. Własność ta oznacza, że $\vec{v} \in (X^{\perp})^{\perp}$. $\square$

11.8 Wymiar dopełnienia ortogonalnego

Niech $L(V, K)$ oznacza zbiór funkcjonałów (funkcji) liniowych określonych w zbiorze V i przyjmujących wartości w zbiorze K. Zbiór $L(V, K)$ z dodawaniem funkcji i mnożeniem funkcji przez skalar z ciała K, zdefiniowanymi w zwykły sposób jest przestrzenią liniową. Zauważmy, że

Lemat 11.10 *Jeżeli V jest przestrzenią wymiaru n, to przestrzeń $L(V, K)$ jest izomorficzna z przestrzenią K^n.*

Dowód. Weźmy bazę $\vec{a}_1, \ldots, \vec{a}_n$ przestzreni V i zdefiniujmy funkcję $\varphi : L(V, K) \to K^n$ przyjmując, że

$$\varphi(f) = (f(\vec{a}_1), \ldots, f(\vec{a}_n)).$$

Łatwo dowieść, że φ jest funkcją liniową. Z lematu 9.16 i twierdzenia 9.17 wynika, że φ jest izomorfizmem. $\square$

Lemat 11.11 *Jeżeli V jest przestrzenią wymiaru n, to przestrzeń $L(V, K)$ też jest wymiaru n.*

Dowód. Jest to oczywisty wniosek z poprzedniego lematu. $\square$

Lemat 11.12 *Jeżeli V jest podprzestrzenią K^n, to n jest sumą wymiarów przestrzeni V i dopełnienia ortogonalnego $V^\perp$.*

Dowód. Weźmy funkcję $\varphi : K^n \to L(V,K)$ taką, że

$$\varphi(\vec{a})(\vec{x}) = \vec{a}\vec{x}$$

(dla $\vec{x} \in V$ i $\vec{a} \in K^n$). Z dwuliniowości iloczynu skalarnego wynika, że funkcja φ przyjmuje wartości w zbiorze funkcjonałów $L(V,K)$, a także, że jest to funkcja liniowa.

Funkcja φ jest też typu „na", a więc jest epimorfizmem. Tak jest, ponieważ bazę przestrzeni V można rozszerzyć do bazy przestrzeni K^n (patrz lemat 9.7 o wymianie) i – w konsekwencji – każdy funkcjonał $f \in L(V,K)$ można rozszerzyć do funkcjonału $f' : K^n \to K$ (patrz twierdzenie 9.17). Z wzoru (6) otrzymujemy, że $f'(\vec{x}) = \vec{a}\vec{x}$ dla pewnego $\vec{a} \in K^n$. Tym bardziej $f(\vec{x}) = \vec{a}\vec{x}$.

Zauważmy, że zerem w przestrzeni $L(V,K)$ jest funkcja stale równa 0 i implikuje to, że dopełnienie ortogonalne przestrzeni V jest jądrem epimorfizmu φ.

Teraz wystarczy skorzystać z twierdzenia 10.6 i lematu 11.11. □

Wniosek 11.13 *Jeżeli V jest podprzestrzenią K^n, to $(V^\perp)^\perp = V$.*

Dowód. Tak jest, ponieważ przestrzenie V i $(V^\perp)^\perp$ są tego samego wymiaru i zachodzi zawieranie $V \subseteq (V^\perp)^\perp$. □

Wniosek 11.14 *Każda podprzestrzeń K^n jest zbiorem rozwiązań pewnego jednorodnego układu równań liniowych.* □

12.1 Suma prosta

Przestrzeń liniową V nazywamy *sumą prostą* podprzestrzeni $V_1, V_2 \subseteq V$, jeżeli każdy wektor $\vec{a} \in V$ ma jednoznaczne przedstawienie w postaci sumy $\vec{a} = \vec{x} + \vec{y}$ wektorów $\vec{x} \in V_1$ i $\vec{y} \in V_2$.

Lemat 12.1 *Przypuśćmy, że V_1 i V_2 są podprzestrzeniami przestrzeni liniowej V. Dowolny wektor $\vec{a} \in V$ ma najwyżej jedno przedstawienie w postaci sumy $\vec{x}+\vec{y}$ wektorów $\vec{x} \in V_1$ i $\vec{y} \in V_2$ wtedy i tylko wtedy, gdy $V_1 \cap V_2 = \{\vec{0}\}$.*

Dowód. Oczywiście, $\{\vec{0}\} \subseteq V_1 \cap V_2$. Jeżeli $\vec{a} \in V_1 \cap V_2$, to $\vec{a}$ można przedstawić w odpowiedniej postaci na dwa sposoby: $\vec{a} = \vec{0} + \vec{a} = \vec{a} + \vec{0}$. Jednoznaczność przedstawienia w tej postaci implikuje, że $vec a = \vec{0}$.

Załóżmy, że pewien wektor $\vec{a}$ ma przedstawienia

$$\vec{x}_1 + \vec{y}_1 = \vec{a} = \vec{x}_2 + \vec{y}_2$$

takie, że $\vec{x}_1, \vec{x}_2 \in V_1$ oraz $\vec{y}_1, \vec{y}_2 \in V_2$. Wtedy $\vec{x}_1 - \vec{x}_2 = \vec{y}_2 - \vec{y}_1 \in V_1 \cap V_2$ oraz $\vec{x}_1 - \vec{x}_2 = \vec{y}_2 - \vec{y}_1 = \vec{0}$. Wobec tego, te przedstawienia $\vec{a}$ są identyczne. □

Lemat 12.2 *Jeżeli V jest podprzestrzenią $\mathcal{R}^n$, to $V \cap V^\perp = \{\vec{0}\}$.*

Dowód. Jeżeli $\vec{x} \in V \cap V^\perp$, to iloczyn $\vec{x}\vec{x}$ wektorów $\vec{x} \in V$ i $\vec{x} \in V^\perp$ jest równy 0. Mamy więc

$$0 = \vec{x}\vec{x} = \sum_{i=1}^{n} x_i^2.$$

Ponieważ współrzędne x_i wektora $\vec{x}$ są liczbami rzeczywistymi, więc wszystkie są równe 0, a $\vec{x}$ jest wektorem zerowym. W ten sposób dowiedliśmy, że $V \cap V^\perp \subseteq \{\vec{0}\}$. Drugie zawieranie jest oczywiste. □

Lemat 12.3 *Jeżeli V jest podprzestrzenią $\mathcal{R}^n$, to każdy wektor $\vec{a} \in \mathcal{R}^n$ można przedstawić w postaci sumy $\vec{a} = \vec{x} + \vec{y}$ wektorów $\vec{x} \in V$ i $\vec{y} \in V^\perp$.*

Dowód. Bierzemy bazy $\vec{a}_1, \ldots, \vec{a}_m$ przestrzeni V oraz $\vec{b}_1, \ldots, \vec{b}_{n-m}$ przestrzeni $V^\perp$. To, że baza $V^\perp$ ma $n-m$ elementów wynika z lematu 11.12.

Układ $\vec{a}_1, \ldots, \vec{a}_m, \vec{b}_1, \ldots, \vec{b}_{n-m}$ jest liniowo niezależny. Aby się o tym przekonać załóżmy, że

$$\sum_{i=1}^{m} \alpha_i \vec{a}_i + \sum_{j=1}^{n-m} \beta_j \vec{b}_j = \vec{0}.$$

Wtedy

$$\sum_{i=1}^{m} \alpha_i \vec{a}_i = -\sum_{j=1}^{n-m} \beta_j \vec{b}_j \in V \cap V^\perp.$$

Z lematu 12.2 wynika, że obie strony równości są równe $\vec{0}$, a ponieważ są to kombinacje liniowe wektorów bazowych, więc ich współczynniki $\alpha_1 = \ldots = \alpha_m = \beta_1 = \ldots = \beta_{n-m} = 0$. Liniowa niezależność tego układu implikuje też, że składa się on z n elementów (w układzie liniowo niezależnym wektory nie mogą się powtarzać).

Teza lematu wynika stąd, że w przestrzeni n wymiarowej każdy n elementowy układ liniowo niezależny jest zbiorem generatorów. □

Twierdzenie 12.4 *Jeżeli V jest podprzestrzenią $\mathcal{R}^n$, to $\mathcal{R}^n$ jest sumą prostą V i $V^\perp$.*

Dowód. Jest to wniosek z lematów 12.1, 12.2 i 12.3. □

12.2 Operacje elementarne i równoważność wierszowa

Przypuśćmy, że mamy macierz A, której wierszami są wektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_m$. Będziemy rozważać następujące operacje na macierzy A, zwane *elementarnymi*:

1. zamiana dwóch wierszy macierzy A miejscami,
2. zastąpienia wiersza $\vec{\alpha}$ wektorem $c\vec{\alpha}$ dla $c \neq 0$,
3. dodanie do wiersza innego wiersza, a więc zastąpienie wiersza $\vec{\alpha}_i$ wektorem $\vec{\alpha}_i + \vec{\alpha}_j$.

Zauważmy, że jeżeli macierz B otrzymujemy z macierzy A wykonując operację elementarną, to także A można otrzymać z B wykonując najwyżej trzy operacje elemetarne. Jeżeli macierz B otrzymujemy zastępując wiersz $\vec{\alpha}_i$ wektorem $\vec{\alpha}_i + \vec{\alpha}_j$, to macierz A otrzymujemy mnożąc j-ty wiersz macierzy B przez -1, dodając go do i-tego wiersza, a następnie ponownie mnożąc j-ty wiersz przez -1. Dla pozostałych operacji jest oczywiste, że są odwracalne.

Macierze A i B są *równoważne wierszowo*, jeżeli jedną z nich można otrzymać z drugiej wykonując operacje elementarne.

Wniosek 12.5 *Relacja wierszowej równoważności macierzy jest relacją równoważności.* □

Lemat 12.6 *Wiersze macierzy równoważnych wierszowo generują tę samą podprzestrzeń.* □

Lemat 12.7 *Jeżeli macierze rozszerzone dwóch układów równań liniowych są wierszowo równoważne, to układy te są równoważne (a więc mają ten sam zbiór rozwiązań).* □

Zauważmy, że funkcje f_1, f_2 i f_3 definiowane wzorami

- $f_1(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_m) = (x_1, \ldots, x_j, \ldots, x_i, \ldots, x_m)$,
- $f_2(x_1, \ldots, x_i, \ldots, x_m) = (x_1, \ldots, cx_i, \ldots, x_m)$ (dla $(c \neq 0)$ oraz
- $f_3(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_m) = (x_1, \ldots, x_i + x_j, \ldots, x_j, \ldots, x_m)$

przekształcają K^m wzajemnie jednoznacznie na K^m i są liniowe. Zauważmy, że jeżeli macierz B otrzymujemy przez zamianę i-tego wiersza macierzy A z j-tym, to macierz B możemy też otrzymać zastępując każdą jej kolumnę $\vec{x}$ kolumną $f_1(\vec{x})$. Analogiczne własność ma miejsce dla pozostałych operacji elementarnych, a więc dla mnożenia wiersza i funkcji f_2 oraz dodawania wiersza i funkcji f_3.

Lemat 12.8 *Jeżeli macierze A i B są wierszowo równoważne, to istnieje różnowartościowe przekształcenie liniowe f przekształcające zbiór kolumn macierzy A na zbiór kolumn macierzy B. Wobec tego przestrzenie generowane przez kolumny macierzy równoważnych wierszowo mają ten sam wymiar.* □

12.3 Macierze zredukowane

Wyrazem kierunkowym wiersza macierzy nazywamy pierwszy niezerowy element tego wiersza. Oczywiście, wiersz zerowy nie ma wyrazu kierunkowego.

Macierz A o wyrazach $a_{i,j}$ (i to numer wiersza, a j to numer kolumny, w której znajduje się wyraz $a_{i,j}$) nazywamy *zredukowaną*, jeżeli

1. wyrazy kierunkowe wszystkich wierszy (o ile istnieją) są równe 1,
2. jeżeli $a_{i,j}$ jest wyrazem kierunkowym i-tego wiersza, to $a_{k,j} = 0$ dla $k < i$,
3. wyrazy kierunkowe są coraz dalej: jeżeli $a_{i,j}$ jest wyrazem kierunkowym i-tego wiersza, to $a_{k,l} = 0$ dla $k > i$ oraz $l \leqslant j$,
4. wiersze zerowe znajdują się na końcu macierzy (mają numery większe od numerów wierszy niezerowych).

Lemat 12.9 *Niezerowe wiersze macierzy zredukowanej są liniowo niezależne. Wymiar przestrzeni generowanej przez kolumny macierzy zredukowanej jest równy liczbie niezerowych wierszy tej macierzy.* □

Twierdzenie 12.10 *Każde dwie równoważne wierszowo macierze zredukowane (o określonych wymiarach) są identyczne.*

Dowód. Przypuśćmy, że mamy zredukowane, równoważne wierszowo macierze M_1 i M_2. Na mocy lematu 12.6, przestrzenie generowane przez wiersze tych macierzy są równe. W tej sytuacji z lematu 12.9 otrzymujemy, że macierzy M_1 i M_2 mają tyle samo wierszy niezerowych i tyle samo zerowych. Dalej będziemy zakładać, że nie mają wierszy zerowych.

Niech $\vec{w}_1$ i $\vec{w}_2$ będą ostatnimi wierszami macierzy M_1 i M_2, a t_1 i t_2 – indeksami wyrazów kierunkowych tych wierszy. Z wyboru wierszy i definicji macierzy zredukowanej wynika, że wyrazy kierunkowe pozostałych wierszy macierzy M_1 mają indeksy $< t_1$. Analogiczna własność jest prawdziwa dla M_2.

Załóżmy, że $t_1 < t_2$. Równość przestrzeni wierszy macierzy M_1 i M_2 implikuje, że $\vec{w}_2$ daje się przedstawić w postaci kombinacji liniowej wierszy $\vec{v}_1, \ldots, \vec{v}_m$ macierzy M_1, np.

$$\vec{w}_2 = \sum_{i=1}^{m} a_i \vec{v}_i. \tag{10}$$

Weźmy wiersz $\vec{v}_i$ i przyjmijmy, że jego wyraz kierunkowy znajduje się na pozycji t. Oczywiście $t \leqslant t_1 < t_2$. Implikuje to, że współrzędna o numerze t wektora w_2 jest równa 0. Z definicji macierzy zredukowanej wynika, że także współrzędne o numerze t pozostałych (o numerach $\neq i$) wierszy macierzy M_1 są równe 0. Oznacza to, że współrzędna o numerze t sumy

$$\sum_{i=1}^{m} a_i \vec{v}_i$$

jest równa a_i. Otrzymujemy więc, że $a_i = 0$, a ponieważ rozumowanie to możemy powtórzyć dla każdego wiersza macierzy M_1, więc $\vec{w}_2 = \vec{0}$. W ten sposób otrzymaliśmy sprzeczność.

W podobny sposób sprowadzamy do sprzeczności założenie, że $t_2 < t_1$. Tak więc dowiedliśmy, że $t_1 = t_2$.

Jeszcze raz skorzystamy z równości (10), ale dodatkowo przyjmijmy, że wiersz $\vec{v}_m$ jest ostatnim, a więc $\vec{v}_m = \vec{w}_1$. Podane rozumowanie pozwala teraz uzasadnić, że dla $i < m$ zachodzi równość $a_i = 0$. Porównując współrzędne obu stron wzoru (10) o numerach t_1 i korzystając dodatkowo z warunku, że wyrazy kierunkowe wierszy macierzy zredukowanej są równe jeden otrzymujemy, że $a_m = 1$. Oznacza to, że równość (10) redukuje się do równości $\vec{w}_2 = \vec{v}_m = \vec{w}_1$. Ostatnie wierszy macierzy M_1 i M_3 są więc identyczne.

Korzystając po raz trzeci z podobnego rozumowania pokazujemy, że wiersze macierzy M_1 różne od $\vec{w}_1$ i wiersze macierzy M_2 różne od $\vec{w}_2$ generują tę samą przestrzeń. Weźmy kombinację X wierszy M_1 różnych od $\vec{w}_1$. Współrzędna o numerze t_1 tej kombinacji jest równa 0. Kombinacja X daje się przedstawić jako kombinacja wierszy macierzy M_2. Na pozycji t_2 w tej kombinacji jest współczynnik przy wektorze $\vec{w}_2$, a więc współczynnik przy $\vec{w}_2$ jest równy 0. Oznacza to, że X jest kombinacją wierszy macierzy M_2 różnych od $\vec{w}_2$.

Aby dokończyć dowód wystarczy powołać się na zasadę indukcji matematycznej. □

12.4 Macierze zredukowane a układy równań liniowych

Układ równań liniowych czesto ma nieskończenie wiele rozwiązań. Polecenie rozwiązania takiego układu nie może więc być rozumiane jako polecenie wymienienia wszystkich jego rozwiązań (ciągów liczb spełniających układ). Jest rozumiane jako polecenie pewnego opisania zbioru wszystkich rozwiązań.

Zgodnie z lematem 11.7, zbiór rozwiązań układu równań liniowych można opisać podając jedno rozwiązanie i opisując zbiór rozwiązań odpowiadającego mu układu jednorodnego. Zbiór rozwiązań układu jenorodnego jest podprzestrzenią i może zostać opisany (niejednoznacznie) przez podanie zbioru generatorów lub bazy.

Polecenie rozwiązanie układu równań liniowych może też być rozumiane jako polecenia znalezienia tzw. rozwiązania parametrycznego, a więc układu równań liniowych szczególnej postaci, równoważnego danemu. Ten szczególny układ ma postać $\vec{x} = C\vec{y} + \vec{d}$, gdzie $\vec{x}$ i $\vec{y}$ są zmiennymi danego układu podzielonymi w pewien sposób na dwie części. Zauważmy, że mając dane parametryczne rozwiązanie łatwo podać jedno z rozwiązań układu (np. $\vec{x} = \vec{d}$ i $\vec{y} = \vec{0}$) oraz bazę zbioru rozwiązań odpowiedniego układu jednorodnego (bierzemy ciągi liczb złożone z $\vec{x} = C\vec{e}_i$ i $\vec{y} = \vec{e}_i$ dla wszystkich możliwych i).

Jeżeli macierz układu równań liniowych ma postać zredukowaną, to bez trudu można z niej odczytać parametryczne rozwiązanie układu.

Zauważmy jeszcze, że

$$[I\ A] \begin{bmatrix} -A \\ I \end{bmatrix} = [0]$$

Wzór ten pozwala znajdować bazę dopełnienia ortogonalnego podprzestrzeni generowanej przez wiersze macierzy $[I\ A]$ (symbole I w tym wzorze oznaczają macierze jednostkowe, ale mogą to być macierze o różnych wymiarach). Może też być wykorzystany przy szukaniu bazy zbioru rozwiązań jednorodnego układu równań liniowych.

12.5 Algorytm eliminacji Gaussa

Przypuśćmy, że mamy daną macierz A o wyrazach $a_{i,j}$ i wierszach $\vec{\alpha}_i$. Podany niżej algorytm nazywamy algorytmem *eliminacji Gaussa*.

1. Dla każdego k takiego, że $\vec{\alpha}_k \neq \vec{0}$:
   (a) znajdujemy numer l wyrazu kierunkowego wiersza $\vec{\alpha}_k$,
   (b) mnożymy wiersz $\vec{\alpha}_k$ przez $a_{k,l}^{-1}$ {wyraz kierunkowy wiersza $\vec{\alpha}_k$ staje się równy 1},
   (c) dla dowolnego $i \neq k$
   wiersz $\vec{\alpha}_i$ zastępujemy przez różnicę $\vec{\alpha}_i - a_{i,l}\vec{\alpha}_k$ {powodujemy, że l-tej kolumnie poza wierszem o numerze k są same zera},
2. przestawiamy wiersze zerowe za wiersze różne od zera,
3. porządkujemy wiersze ustawiając je według rosnących numerów wyrazów kierunkowych.

Lemat 12.11 *Algorytm eliminacji Gaussa przekształca dowolną macierz w równoważną jej wierszowo macierz zredukowaną.* □

Za pomocą tego algorytmu można rozwiązywać układy równań liniowych, przekształcać zbiór generatorów w bazę, badać liniową niezależność wektorów, obliczać wymiar przestrzeni mając zbiór jej generatorów, szukać bazy dopełnienia ortogonalnego, itp. Wiele zastosowań algorytmu eliminacji Gaussa jest zasygnalizowane na 12. liście zadań.

Zauważmy jeszcze, że z lematów 12.6, 12.8, 12.9 i 12.11 wynika

Lemat 12.12 *Dla dowolnej macierzy A, przestrzenie generowane przez wiersze macierzy A i przez jej kolumny mają ten sam wymiar.*

Dowód. Tak jest, ponieważ przekształcenia elementarne zachowują interesujące nas wymiary i pozwalają sprowadzić macierz do postaci zredukowanej, a dla macierzy zredukowanej wymiary te są identyczne. □

12.6 Twierdzenie Kroneckera-Capelliego

Rzędem macierzy nazywamy wymiar podprzestrzeni generowanej przez wiersze tej macierzy. Z lematu 12.12 wynika, że rząd macierzy możemy zdefiniować równoważnie jako wymiar przestrzeni generowanej przez kolumny.

Twierdzenie 12.13 (Kroneckera-Capelliego) *Układ równań liniowych ma rozwiązanie wtedy i tylko wtedy, gdy rząd macierzy tego układu jest równy rzędowi jego macierzy rozszerzonej.*

Dowód. Aby dowieść to twierdzenie, wystarczy układowi równań nadać postać wektorową i zauważyć, że układ równań liniowych ma rozwiązanie wtedy i tylko wtedy, gdy kolumna wyrazów wolnych jest kombinacją liniową kolumn macierzy badanego układu. □

Twierdzenie 12.14 *Układ równań liniowych z n niewiadomymi ma dokładnie jedno rozwiązanie wtedy i tylko wtedy, gdy rząd macierzy tego układu jest równy n.* □