LINIOWA NIEZALEŻNOŚĆ, ROZPINANIE I BAZY

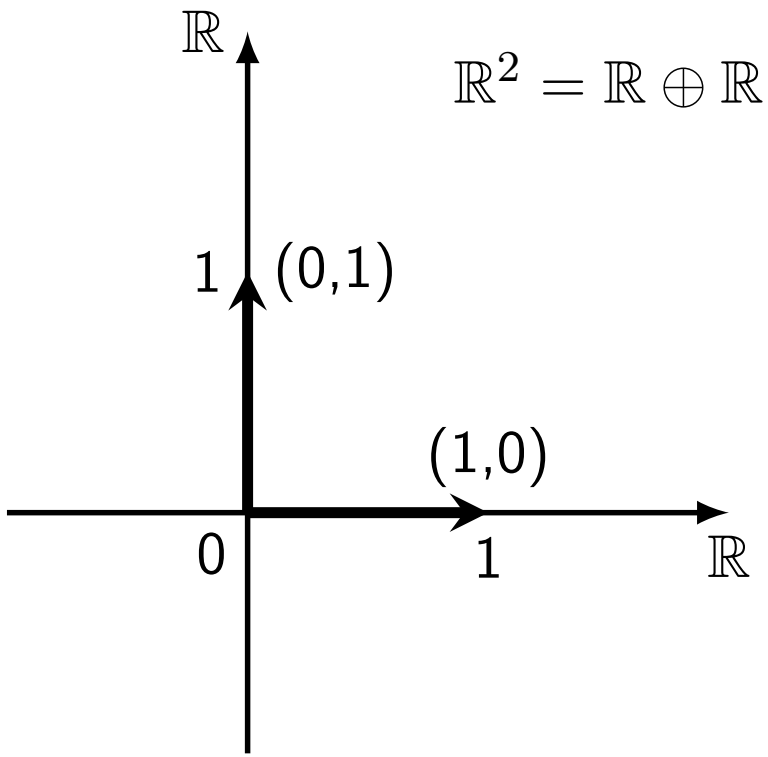
Piotr M. Hajac
Uniwersytet Warszawski

Wykład 10, 11.12.2013

Typeset by Jakub Szczepanik.

Geometryczne intuicje

Dla pierścienia $R = \mathbb{R}$ mamy geometryczną intuicję wprowadzanych pojęć:



Wektory $(1, 0)$ i $(0, 1)$:

1. są liniowo niezależne: $(1, 0) \neq r(0, 1)$,
2. rozpinają $\mathbb{R}^2$: $(a, b) = a(1, 0) + b(0, 1)$,
3. tworzą bazę $\mathbb{R}^2$: spełniają powyższe 2 warunki.

Wektory $(1, 2)$ i $(2, 4)$ nie są liniowo niezależne: $(2, 4) = 2(1, 2)$. Nie rozpinają też $\mathbb{R}^2$: $a(1, 2) + b(2, 4) = (a + 2b)(1, 2)$, a $(1, 1) \neq r(1, 2)$.

Liniowa niezależność

Definicja

Niech R będzie dowolnym pierścieniem, a M dowolnym lewym R-modułem. Niech $\emptyset \neq S \subseteq M$. Podzbiór S nazywamy liniowo niezależnym, a o jego elementach mówimy że są liniowo niezależne, wtedy i tylko wtedy gdy dla każdego skończonego podzbioru $I \subseteq S$:

$$\boxed{\sum_{m \in I} r_m m = 0 \quad \Longrightarrow \quad \forall\ m \in I :\ r_m = 0}\ .$$

Jeśli powyższa implikacja zachodzi dla skończonego zbioru I, to zachodzi też dla każdego podzbioru $J \subseteq I$:

$$\sum_{m \in J} r_m m = 0 \implies \sum_{m \in J} r_m m + \sum_{n \in I \setminus J} 0n = 0 \implies \underset{m \in J}{\forall} r_m = 0.$$

Dlatego, jeśli zbiór S jest skończony, wystarczy definiować liniową niezależność przez warunek

$$\sum_{m \in S} r_m m = 0 \quad \Longrightarrow \quad \forall\ m \in S : r_m = 0.$$

Rozpinanie

Jeżeli podzbiór S jest liniowo niezależny, to $0 \notin S$ lub $R = 0$.
Zbiory które nie są liniowo niezależne nazywamy liniowo zależnymi, a elementy zbiorów liniowo zależnych nazywamy liniowo zależnymi.

Definicja

Niech R będzie pierścieniem, M lewym R-modułem oraz $\emptyset \neq S \subseteq M$. Przestrzenią rozpinaną przez S nazywamy zbiór wszystkich skończonych kombinacji liniowych elementów S:

$$\operatorname{span}(S) := \left\{ \sum_{m \in S} r_m m \in M \;\middle|\; \begin{array}{c} \forall\ m \in S:\ r_m \in R, \\ \text{tylko skończona ilość } r_m \neq 0 \end{array} \right\} .$$

Podzbiór $\operatorname{span}(S)$ jest podmodułem M:

$$\sum_{m \in S} r_m m + \sum_{m \in S} s_m m = \sum_{m \in S} (r_m + s_m) m \in \operatorname{span}(S) ,$$

$$r \sum_{m \in S} r_m m = \sum_{m \in S} (r r_m) m \in \operatorname{span}(S) .$$

Pierścień jako lewy moduł nad sobą

Rozważmy pierścień R jako lewy moduł nad sobą. Wtedy

$$\mathrm{span}(\{r\}) = R \quad \Longleftrightarrow \quad \exists\ s \in R :\ sr = 1\,.$$

Istotnie, $1 \in R = \mathrm{span}(\{r\}) \Rightarrow \exists\ s \in R : sr = 1$. Z drugiej strony,

$$\exists\ s \in R : sr = 1 \quad \Longrightarrow$$
$$\forall\ r' \in R :\ r' = r'1 = r'(sr) = (r's)r \in \mathrm{span}(\{r\})\,.$$

Niech R będzie niezerowym pierścieniem bez dzielników zera. Wtedy jedyne lewo-odwracalne wielomiany w $R[\mathbb{N}]$ to $\alpha \in R \setminus \{0\}$. Zaiste, $\alpha \neq 0$ oraz

$$0 = \deg(1) = \deg(\beta * \alpha) = \deg(\beta) + \deg(\alpha)$$

implikuje $\alpha \in R \setminus \{0\}$. Zatem, rozważając $R[\mathbb{N}]$ jako lewy $R[\mathbb{N}]$-moduł, mamy

$$\forall\ n \in \mathbb{N} \setminus \{0\} :\ \mathrm{span}(\{x^n\}) \neq R[\mathbb{N}]\,.$$

$\mathbb{Q}$ jako $\mathbb{Z}$-moduł

Lemat

Rozważmy $\mathbb{Q}$ jako $\mathbb{Z}$-moduł. Podzbiór $\emptyset \neq S \subseteq \mathbb{Q}$ jest liniowo niezależny $\Leftrightarrow S = \{r\}$, gdzie $r \neq 0$.

Dowód: Zauważmy najpierw że $r \neq 0 \Leftrightarrow (nr = 0 \Rightarrow n = 0)$. Jeśli $\frac{p}{q}, \frac{p'}{q'} \in S$, $\frac{p}{q} \neq \frac{p'}{q'}$, to $qp'\frac{p}{q} + (-q'p)\frac{p'}{q'} = 0$, a nie jest prawdą że $qp' = -q'p = 0$, bo wtedy $\frac{p}{q} = 0 = \frac{p'}{q'}$, co przeczy $\frac{p}{q} \neq \frac{p'}{q'}$. ■

Lemat

Rozważmy $\mathbb{Q}$ jako $\mathbb{Z}$-moduł. Niech $\emptyset \neq S \subseteq \mathbb{Q}$. Wtedy, jeżeli $\mathrm{span}(S) = \mathbb{Q}$, to zbiór S nie jest skończony.

Dowód: Niech $S = \left\{\frac{p_1}{q_1}, ..., \frac{p_n}{q_n}\right\}$, gdzie wszystkie ułamki $\frac{p_i}{q_i}$ są w postaci względnie pierwszej (tzn. $\gcd(p_i, q_i) = 1$ i $q_i > 0$). Wtedy

$$x \in \mathrm{span}(S) \quad \Longrightarrow \quad x = \sum_{i=1}^{n} k_i \frac{p_i}{q_i} = \frac{\sum(...)}{q_1 q_2 ... q_n}.$$

Zatem $\forall\ x \in \mathrm{span}(S)$: mianownik x zapisanego w postaci względnie pierwszej jest $\leqslant q_1 q_2 ... q_n$. Stąd $\mathbb{Q} \ni \frac{1}{(q_1 ... q_n)+1} \notin \mathrm{span}(S)$. ■

Baza

Definicje

Niech R będzie dowolnym pierścieniem, a M dowolnym R-modułem. Niepusty podzbiór $B \subseteq M$ nazywamy bazą $M \Leftrightarrow$

1. B jest zbiorem liniowo niezależnym,
2. $\mathrm{span}(B) = M$.

Moduł nazywamy wolnym $\Leftrightarrow$ posiada bazę.

Twierdzenie

Modułem $\mathbb{Q}$ liczb wymiernych nie posiada bazy nad $\mathbb{Z}$ (nie jest modułem wolnym nad $\mathbb{Z}$).

Dowód: Żaden zbiór nie może być równocześnie jednoelementowy i nieskończony. ■

Elementarne fakty

1. Każdy pierścień R (nawet zerowy) jest wolnym R-modułem. Zbiór $\{1\}$ jest zawsze bazą R.

2. Dowolna suma prosta $\bigoplus_{i\in I} R$ jest wolnym R-modułem. Bazą (kanoniczną) jest zbiór

$$\{f_i \in \mathrm{Map}(I,R) \mid \forall\ i,j \in I : f_i(j) = \delta_{ij}\}\ ,$$

gdzie δ_{ij} jest deltą Kroneckera, tzn. $\boxed{\delta_{ij} = \begin{cases} 1 & \text{dla } i = j \\ 0 & \text{dla } i \neq j \end{cases}}$.

Jeśli $I = \mathbb{N}$, piszemy $f_i = (0,...,0,1,0,...)$. Jeśli $I = \{1,...,n\}$, piszemy $\bigoplus_{i\in I} R = R^n$. Moduł R^n jest prototypem modułu wolnego, a zbiór

$$\{(1,0,...,0),(0,1,0,...,0),...,(0,...,0,1)\}$$

prototypem bazy.

Twierdzenie o bazie

Twierdzenie

Jeśli M jest wolnym R-modułem z bazą B, to odwzorowanie

$$\bigoplus_{e\in B} R \ni f \overset{F_B}{\longmapsto} \sum_{e\in B} f(e)\, e \in M$$

jest izomorfizmem R-modułów.

Dowód: Odwzorowanie F_B jest ewidentnie liniowe. Skonstruujemy odwzorowanie odwrotne F_B^{-1}. Zauważmy że $\forall\ m \in M \setminus \{0\}$

$$\exists!\ \{r_1, ..., r_{N_m}\} \subseteq R \setminus \{0\}\,,\ \{e_1, ..., e_{N_m}\} \subseteq B :\ m = \sum_{k=1}^{N_m} r_k e_k\,.$$

Istotnie, przypuśćmy że mamy 2 rozkłady $m \neq 0$:

$$\sum_{e\in I} r_e\, e = m = \sum_{e'\in J} s_{e'}\, e'\,.$$

Dowód twierdzenia o bazie

Wtedy

$$0 = m - m = \sum_{k \in I \cap J} (r_k - s_k)\, k + \sum_{e \in I \setminus J} r_e\, e + \sum_{e' \in J \setminus I} (-s_{e'})\, e' \,.$$

Z liniowej niezależności wynika że

$$\forall\ k \in I \cap J :\ r_k = s_k \,, \quad \forall\ e \in I \setminus J :\ r_e = 0 \,, \quad \forall\ e' \in J \setminus I :\ s_{e'} = 0 \,.$$

Zatem, z założenia niezerowości współczynników, $I = J$ i rozkład $m \neq 0$ w bazie jest jednoznaczny. Jest też zawsze niezerowy, więc przypsując $0 \in M$ rozkład zerowy mamy jednoznaczność rozkładu w bazie dla wszystkich $m \in M$. Możemy więc zdefiniować

$$M \ni m \overset{F_B^{-1}}{\longmapsto} f_m \in \bigoplus_{e \in N} R, \quad \text{gdzie } \sum_{e \in B} f_m(e)\, e := m \,.$$

Jest oczywiste że $F_B \circ F_B^{-1} = \mathrm{id}$ i $F_B^{-1} \circ F_B = \mathrm{id}$. ■