PRZESTRZENIE WEKTOROWE

R-moduł M nazywamy przestrzenią wektorową $\iff$ R jest ciałem. Ciała typowo oznaczamy przez k a przestrzenie wektorowe przez V.

Twierdzenie: Każda przestrzeń wektorowa $V \neq 0$ nad dowolnym ciałem k zawsze posiada bazę.

Dowód: $V \neq 0 \implies \exists v \in V : v \neq 0$. Zbiór $\{v\}$ jest liniowo niezależny bo $(\alpha v = 0 \implies \alpha = 0) \iff \sim(\alpha \neq 0 \wedge \alpha v = 0)$ a z założenia że k jest ciałem mamy

$(\alpha \neq 0 \wedge \alpha v = 0) \implies 0 = \alpha^{-1} 0 = \alpha^{-1}(\alpha v)$

$= (\alpha^{-1}\alpha) v = 1 v = v$. Zatem zbiór wszystkich zbiorów liniowo niezależnych jest niepusty. Łatwo sprawdzić że spełnia on założenia lematu Kuratowskiego-Zorna (równoważnego pewnikowi wyboru) na mocy którego unioskujemy że istnieje zbiór liniowo niezależny B nie zawierający się w żadnym większym zbiorze liniowo niezależnym: ($B \subseteq B'$ i B' jest liniowo niezależny) $\Rightarrow$ $B' = B$. Korzystając z tego chcemy pokazać że $\operatorname{span}(B) = V$. Jest oczywiste że $\{0\} \cup B \subseteq \operatorname{span}(B)$, weźmy więc $0 \neq v_0 \notin B$. Wtedy zbiór $\{v_0\} \cup B$ jest liniowo zależny. Zatem

$$\exists \{v_1, \dots, v_n\} \subseteq B,\ \alpha_0, \dots, \alpha_n \in K : \sum_{i=0}^{n} \alpha_i v_i = 0$$

$$i\ \exists j \in \{0, \dots, n\} : \alpha_j \neq 0.$$ Stąd $\alpha_0 \neq 0$ bo inaczej, z liniowej niezależności zbioru $\{v_1, \dots, v_n\}$, mamy $\sum_{i=0}^{n} \alpha_i v_i = \sum_{i=1}^{n} \alpha_i v_i \Rightarrow$

$\alpha_1 = \dots = \alpha_n = 0$ co przeczy istnieniu $\alpha_j \neq 0$. Z założenia że K jest ciałem dostajemy więc $v_0 = \frac{-\alpha_1}{\alpha_0} v_1 + \dots + \frac{-\alpha_n}{\alpha_0} v_0 \in \operatorname{span}(B)$. ∎

Istnienie bazy jest podstawową własnością odróżniającą przestrzenie wektorowe od ogólnych modułów.

Wniosek: Ilość elementów każdego ciała skończonego $\mathbb{F}$ jest postaci p^n, gdzie p jest liczbą pierwszą a $n \in \in \mathbb{N} \setminus \{0\}$.

Dowód: Ze skończoności ciała wynika że istnieje najmniejsza liczba $p \in \mathbb{N} \setminus \{0,1\}$ taka że $p \cdot 1 = 0$. Liczba p musi być pierwsza bo inaczej z minimalności p i braku dzielników zera w ciele dostajemy sprzeczność:

$$0 = p \cdot 1 = \underbrace{(mm')}_{1<m,m'<p} \cdot 1 = \underbrace{(m \cdot 1)}_{\neq 0}\underbrace{(m' \cdot 1)}_{\neq 0}.$$

Dalej, $(\mathbb{Z}/p\mathbb{Z}) \cdot 1$ jest podciałem $\mathbb{F}$, więc $\mathbb{F}$ jest niezerową przestrzenią wektorową nad $\mathbb{Z}/p\mathbb{Z}$. Posiada zatem bazę B nad $\mathbb{Z}/p\mathbb{Z}$. Baza musi być skończona bo $\mathbb{F}$ jest skończone. Oznaczmy ilość elementów bazy przez n. Wtedy $\mathbb{F} \cong \bigoplus_{b \in B} (\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^n$. Stąd ilość elementów $\mathbb{F}$ to p^n. ■

Dlatego właśnie nie ma ciał np. 6-elementowych

<u>Twierdzenie</u>: Jeśli S jest liniowo niezależnym podzbiorem przestrzeni wektorowej V, to można go uzupełnić do bazy V.

<u>Dowód</u>: Tym razem stosujemy lemat Kuratowskiego – Zorna do rodziny wszystkich zbiorów liniowo niezależnych których podzbiorem jest S. Ta rodzina jest niepusta bo S do niej należy. Istnieje zatem największy zbiór liniowo niezależny $B \supseteq S$. Stąd, jeśli $0 \neq x \notin B$ to $\{x\} \cup B \supsetneq B \supseteq S$. Zatem zbiór $\{x\} \cup B$ jest liniowo zależny co, identycznie jak w twierdzeniu o istnieniu bazy, implikuje że $\operatorname{span}(B) = V$. Mamy zatem bazę zawierającą S. ∎

<u>Twierdzenie</u>: Jeśli V jest niezerową przestrzenią wektorową nad K i $\operatorname{span}(S) = V$, to z S można wybrać bazę V.

<u>Dowód</u>: Rozpatrzmy rodzinę wszystkich podzbiorów S rozpinających V. Jest ona niepusta bo należy do niej S. Znowu z lematu

Kuratowskiego - Zorna wnioskujemy że $\exists B \subseteq S : \mathrm{span}(B) = V$ oraz zachodzi $(B' \subseteq B \subseteq S$ i $\mathrm{span}(B') = V) \Rightarrow B' = B$.

Wystarczy teraz pokazać że B jest zbiorem liniowo niezależnym. Przypuśćmy że tak nie jest. Wtedy $\exists \{v_1, \ldots, v_n\} \subseteq B, \alpha_1, \ldots, \alpha_n \in k$:

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \text{ oraz } \exists j \in \{1, \ldots, n\} : \alpha_j \neq 0.$$

Jeśli $n=1$, to $\alpha_1 \neq 0$ i $\alpha_1 v_1 = 0$, skąd $v_1 = \alpha_1^{-1} \alpha_1 v_1 = 0$. Z założenia $V \neq 0$ i $\mathrm{span}(B) = V$ wiemy że $\phi \neq B \setminus \{0\}$. Zatem $\mathrm{span}(B \setminus \{0\}) = \mathrm{span}(B) = V$. W połączeniu z $B \setminus \{0\} \subsetneq B \subseteq S$ przeczy to minimalności B. Załóżmy teraz że $n > 1$. Wtedy

$$v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} \frac{-\alpha_i}{\alpha_j} v_i, \text{ skąd } \mathrm{span}(B \setminus \{v_j\}) = \mathrm{span}(B) = V.$$

Podobnie jak poprzednio, w połączeniu z $B \setminus \{v_j\} \subsetneq B \subseteq S$ otrzymujemy sprzeczność z minimalnością B. ∎ Tak więc baza to największy zbiór liniowo niezależny i najmniejszy zbiór rozpinający.

Lemat Steinitz'a: Jeśli przestrzeń wektorowa V nad k posiada bazę n-elementową B, to każda inna baza V też jest n-elementowa.

Dowód: Pokażemy najpierw że jeśli zbiór S posiada więcej niż n elementów to jest on liniowo zależny. Niech $\{v_1, \dots, v_{n+1}\} \subseteq S$ i $\sum_{i=1}^{n+1} \alpha_i v_i = 0$. Każdy wektor v_i zapiszmy

$$v_i = \sum_{j=1}^{n} \beta_{ij} e_j, \quad \text{gdzie } B = \{e_1, \dots, e_n\}.$$

Wtedy $0 = \sum_{i=1}^{n+1} \sum_{j=1}^{n} \alpha_i \beta_{ij} e_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n+1} \alpha_i \beta_{ij} \right) e_j$.

Z liniowej niezależności B, $\forall j \in \{1, \dots, n\}$: $\sum_{i=1}^{n+1} \alpha_i \beta_{ij} = 0$. Jeśli $\forall i,j: \beta_{ij} = 0$, to układ ma ewidentnie niezerowe rozwiązanie. Jeśli $\exists \beta_{kl} \neq 0$, to $\alpha_k = \sum_{\substack{i=1 \\ i \neq k}}^{n+1} \frac{-\beta_{il}}{\beta_{kl}} \alpha_i$ podstawiamy do pozostałych równań otrzymując układ n równań z $(n-1)$ niewiadomymi. Po $(n-1)$ krokach dostaniemy 1 równanie z 2 niewiadomymi, które zawsze ma niezerowe rozwiązanie. Zatem istnieje niezerowe rozwiązanie wyjściowego układu równań. Stąd S jest liniowo zależny, i nie jest bazą. Wreszcie jeśli S byłby bazą mniej niż n-elementową, to zbiór B byłby liniowo zależny co przeczy temu że jest bazą. ■