Použitie Zornovej lemy

1 Ekvivalentné formy Axiómy výberu

Axióma výberu.

$(\forall \mathcal{S})[(\forall A \in \mathcal{S})(A \neq \emptyset) \wedge (\forall A \in \mathcal{S})(\forall B \in \mathcal{S})(A \neq B \Rightarrow A \cap B = \emptyset) \Rightarrow (\exists V)(\forall A \in \mathcal{S})(\exists x)(V \cap A = \{x\})]$

Pre každý systém neprázdnych po dvoch disjunktných množín existuje výberová množina, t.j. taká množina, ktorá má s každou z množín tohoto systému jednoprvkový prienik.

V praxi často používame rôzne tvrdenia, ktoré sú ekvivalentné s axiómou výberu. V tvrdení 2 je zozbieraných niekoľko výsledkov, ktoré sú len jednoduchým preformulovaním axiómy výberu, dôležitejšie (a často používané) sú však najmä ekvivalenty AC uvedené vo vete 3.

Asi sa oplatí aspoň stručne vysvetliť, čo rozumieme pod tým, že nejaké tvrdenie je *ekvivalentné s AC.* Je jasné, že nemá veľký zmysel hovoriť o tom, či niečo je ekvivalentné s AC, ak pracujeme v systéme, kde AC je jednou s axióm. Tvrdenie 2 a vetu 3 treba teda chápať tak, že je to tvrdenie v axiomatickom systéme, ktorý dostaneme po vynechaní axiómy výberu. Teda namiesto ZFC (čo je systém s ktorým obvykle pracujeme) ide v tomto prípade o výsledky v systéme ZF.[1]

Okrem iného to znamená, že ak by sme vytvorili axiomatický systém, kde by sme AC nahradili niektorým z jej ekvivalentov (napríklad ZF+ZL alebo ZF+WO), tak by sme dostali rovnako silný systém. Čiže v istom zmysle môžeme tieto ekvivalenty chápať priamo ako axiómy (ak už máme dokázanú vetu 3 alebo sme jej ochotní uveriť).

Definícia 1. Nech $\mathcal{S}$ je množina. Zobrazenie $f\colon \mathcal{S} \to \bigcup \mathcal{S}$ sa nazýva *selektor* alebo tiež *výberová funkcia* na množine $\mathcal{S}$, ak platí

$$(\forall x \in \mathcal{S}) f(x) \in x.$$

Pomenovanie výberová funkcia je pomerne prirodzené – je to funkcia, ktorá z každej množiny v $\mathcal{S}$ vyberá nejaký jej prvok.

Tvrdenie 2 (ZF). *Nasledujúce podmienky sú ekvivalentné* (*ako tvrdenia ZF*)*:*
(i) axióma výberu;
(ii) pre každý systém neprázdnych po dvoch disjunktných množín existuje selektor;
(iii) pre každý systém neprázdnych množín existuje selektor;
(iv) karteziánsky súčin ľubovoľného systému neprázdnych množín je neprázdny, t.j.

$$(\forall i \in I) X_i \neq \emptyset \qquad \Rightarrow \qquad \prod_{i \in I} X_i \neq \emptyset;$$

(v) ak R je relácia medzi množinami A a B taká, že pre každé $a \in A$ existuje $b \in B$ s vlastnosťou aRb, tak existuje funkcia $f\colon A \to B$ taká, že $f \subseteq R$;
(vi) ak $f\colon A \to B$ je surjekcia, tak existuje $g\colon B \to A$ také, že $f \circ g = id_B$.

Veta 3 (ZF). *Nasledujúce podmienky sú* (*ako tvrdenia systému ZF*) *ekvivalentné s axiómou výberu:*

[1] ZF je skratka pre Zermelov-Fraenkelov systém; ZFC označuje Zermelov-Fraenkelov systém s axiómou výberu.

(WO) *Na každej množine existuje dobré usporiadanie.*

(PM) *Pre každý reťazec v čiastočne usporiadanej množine* $(P, \leq)$ *existuje maximálny reťazec, ktorý ho obsahuje.*

(ZL) *Ak každý reťazec v čiastočne usporiadanej množine* $(P, \leq)$ *má horné ohraničenie, tak* $(P, \leq)$ *má maximálny prvok.*

Tvrdenie WO sa zvykne nazývať *princíp dobrého usporiadania,* PM je *princíp maximality* (alebo tiež Hausdorffov princíp maximality) a ZL sa zvyčajne volá *Zornova lema.*

Možno stojí za zmienku, že s použitím WO sa mnohé z dôkazov využívajúcich ZL dajú previesť na dôkazy pomocou transfinitnej indukcie. (Niekedy to ide jednoduchšie, niekedy ťažšie.)

2 Zornova lema

2.1 Konštrukcia maximálnych objektov

Jedno z typických použití Zornovej lemy je také, že čiastočné usporiadanie, s ktorým pracujeme, je inklúzia. Čiže ak sa o množine nejakých objektov podarí ukázať, že (spolu s čiastočným usporiadaním $\subseteq$) spĺňa predpoklady Zornovej lemy, máme zaručenú existenciu prvku tejto množiny, ktorý je maximálny vzhľadom na inklúziu.

Príklady takéhoto použitia Zornovej lemy:

- Každý vektorový priestor má bázu. (Pomocou ZL ukážeme, že existuje maximálna lineárne nezávislá množina. Potom overíme, že takáto množina musí tvoriť bázu.) [KT, Problem 14.6d]
- Každý centrovaný systém S je obsiahnutý v nejakom ultrafiltre. (Pomocou ZL ukážeme, že existuje maximálny centrovaný systém obsahujúci daný systém S. O ňom ukážeme, že už musí byť ultrafilter.)
- Každý vlastný ideál I v okruhu s jednotkou, je obsiahnutý v nejakom maximálnom ideále. (Pomocou ZL ukážeme, že existuje maximálny vlastný ideál obsahujúci I.) [KT, Problem 14.6b]
- Každý Hilbertov priestor má ortonormálnu bázu. (Z toho sa už dá odvodiť, že každý Hilbertov priestor je izomorfný s $\ell_2(M)$ pre nejakú množinu M.) Pozri napríklad [T, Proposition 1.4.18].
- Každé čiastočné usporiadanie má linearizáciu. (Maximálne čiastočné usporiadanie rozširujúce dané usporiadanie už bude lineárne.) Pozri napríklad [KT, Problem 14.8].
- Každý reťazec/antireťazec v čiastočne usporiadanej množine je obsiahnutý v maximálnom reťazci/antireťazci.
- Každý skoro disjunktný systém (AD-systém) je obsiahnutý v nejakom skoro maximálnom skoro disjunktnom systéme (MAD-systéme).

Ukážeme si aspoň niekoľko tvrdení podobného typu.

2.1.1 Minimálne prvoideály

S nasledujúcim tvrdením ste sa mohli stretnúť na predmete Vybrané kapitoly z algebry [G].

Tvrdenie 4. *Nech R je okruh, P je prvoideál v R. Potom P obsahuje minimálny prvoideál.*

Napríklad v okruhoch bez deliteľov nuly ľahko vidieť, že toto tvrdenie platí – minimálny ideál v takomto okruhu je (0).

Dôkaz. Stačí ukázať, že prienik reťazca prvoideálov je opäť prvoideál a potom použiť Zornovu lemu.

Ľahko sa ukážte, že ľubovoľný prienik ideálov je ideál.

Nech teraz $\{P_i; i \in I\}$ je nejaký reťazec prvoideálov. Nech $Q := \bigcap_{i\in I} P_i$. Ukážeme, že Q je prvoideál.

Každý ideál obsahuje nulu, takže $Q \neq \emptyset$.

Sporom. Nech by $xy \in Q$ a súčasne $x \notin Q$, $y \notin Q$. Teda existujú $i \in I$ a $j \in J$ tak, že $x \notin P_i$ a $y \notin P_j$. BUNV nech $P_i \subseteq P_j$. (Pretože pracujeme s reťazcom, niektorý z týchto prvoideálov musí byť podmnožinou druhého.) Potom ale máme $y \notin P_i$. Teda pre prvoideál P_i platí, $xy \in P_i$, $x \notin P_i$ a $y \notin P_i$, čo je spor. □

2.1.2 Nilradikál

Ešte spomenieme jeden pojem, ktorý je užitočný napríklad v komutatívnej algebre. Dôkazy týchto tvrdení môžete nájsť napríklad i v [Co] a [G]. Dôkazy, ktoré tu uvádzam, som prebral z [R, Proposition 1.9, Corollary 1.10].

Tvrdenie 5. *Nech R je komutatívny okruh s jednotkou. Nech $M \neq \emptyset$ je nejaká podmnožina R, ktorá je uzavretá na súčin. Nech I je ideál v R taký, že $I \cap M = \emptyset$. Potom existuje prvoideál P taký, že $P \supseteq I$ a $P \cap M = \emptyset$.*

Dôkaz. Nech P je maximálny (vzhľadom na inklúziu)[2] ideál v R s vlastnosťami $P \cap S = \emptyset$ a $P \supseteq I$. Existencia takéhoto ideálu vyplýva z Zornovej lemy. Stačí overiť, že zjednotenie reťazca takýchto ideálov má opäť uvedené vlastnosti. Je jasné, že zjednotenie neovplyvní disjunktnosť s M a ani to, či ideál obsahuje I. Zostáva teda overiť, že v KO s 1 je zjednotenie reťazca vlastných ideálov opäť ideál, čo je pomerne ľahké. (Označme Z zjednotenie reťazca vlastných ideálov. Žiadny z ideálov v reťazci nemôže obsahovať 1, lebo by to potom nebol vlastný ideál. Potom ani Z neobsahuje 1, čiže $Z \subsetneq R$. Ak x, y patria do Z, musia patriť do niektorého ideálu J v tomto reťazci, teda aj $x - y \in J \subseteq Z$. Takisto ak $x \in Z$ máme $x \in J$ pre nejaký ideál a potom pre ľubovoľné $a \in R$ platí $ax \in J \subseteq Z$.)[3]

Teraz pre ideál P ukážeme, že

$$a, b \notin P \Rightarrow ab \notin P.$$

Uvedomme si, čo nám o ideále P hovorí to, že je to maximálny ideál s uvedenou vlastnosťou. Ak $a \notin P$, tak najmenší ideál obsahujúci $P \cup \{a\}$ je

$$P + aR = \{p + ar; p \in P, r \in R\}.$$

Tento ideál už musí mať neprázdny prienik s množinou M. (Inak by sme dostali spor s maximalitou.)

Teda sme zistili, že ak $a \notin P$, tak existujú $p_1 \in P$ $r_1 \in R$ také, že $p_1 + ar_1 \in M$. Rovnaké zdôvodnenie nám dáva, že aj pre $b \notin P$ existujú $p_2 \in P$ a $r_2 \in R$ také, že $p_2 + br_2 \in M$. Potom aj súčin týchto prvkov je v M, teda dostávame

$$(p_1 + ar_1)(p_2 + br_2) = (p_1p_2 + p_1br_2 + p_2ar_1 + abr_1r_2) = p + abr,$$

kde $p \in P$ a $r \in R$.

Ak by platilo $ab \in P$, tak by tento prvok bol súčasne v P aj v M, čo by odporovalo predpokladu $P \cap M = \emptyset$; teda dostávame $ab \notin P$. □

[2] V celom tomto dôkaze sa slovo maximálny používa vo význame maximálny vzhľadom na inklúziu, nie maximálny ideál.

[3] Podobná argumentácia sa použije v dôkaze, že vlastný ideál v KO s 1 je obsiahnutý v nejakom maximálnom ideále.

Ak R je KO s 1, tak ideál

$$\mathrm{rad}(R) = \bigcap\{P; P \text{ je prvoideál v } R\}$$

sa nazýva *nilradikál* okruhu R. Ukážeme si, že nilradikál pozostáva presne z nilpotentných prvkov.

Veta 6. *Nech R je komutatívny okruh s jednotkou.*

Pre $x \in R$ existuje $n \in \mathbb{N}$ také, že $x^n = 0$ práve vtedy, keď x patrí do každého prvoideálu v R. Teda

$$\mathrm{rad}(R) = \{x \in R; x^n = 0 \text{ pre nejaké } n \in \mathbb{N}\}.$$

Dôkaz. $\boxed{\Rightarrow}$ Ak x je nilpotentný a P je ľubovoľný prvoideál v R tak z $x^n = 0 \in P$ dostávame $x \in P$.

$\boxed{\Leftarrow}$ Ak x nie je nilpotentný, tak $M = \{x^n; n \in \mathbb{N}\}$ je multiplikatívna množina a (0) je ideál disjunktný s M. Podľa predchádzajúceho tvrdenie potom existuje prvoideál taký, že $P \cap M = \emptyset$, špeciálne $x \notin P$. □

2.1.3 Alexandrova veta o subbáze

Pripomeňme, že ak $(X, \mathcal{T})$ je topologický priestor, tak systém otvorených množín $\mathcal{B}$ sa nazýva *báza* topológie $\mathcal{T}$, ak pre každé $x \in X$ a otvorené okolie $U \ni x$ existuje $B \in \mathcal{B}$ také, že $x \in B \subseteq U$. Ekvivalentne: Každá otvorená množina sa dá napísať ako zjednotenie množín z $\mathcal{B}$.

Systém otvorených množín $\mathcal{S}$ je *subbáza* pre $(X, \mathcal{T})$, ak konečné prieniky množín z $\mathcal{S}$ vytvoria bázu $(X, \mathcal{T})$.

Topologický priestor X je kompaktný, ak pre každé otvorené pokrytie existuje konečné podpokrytie. Nie je ťažké ukázať, že ak si zvolíme nejakú bázu $\mathcal{B}$, tak požiadavka aby existovalo konečné podpokrytie pre každé otvorené pokrytie pozostávajúce z bázových množín, je ekvivalentná s kompaktnosťou. (Čiže kompaktnosť stačí overovať pre pokrytia tvorené bázovými množinami.) Zaujímavé je, že rovnaké tvrdenie platí i pre subbázu. Tento výsledok sa nazýva Alexandrova veta o subbáze. Pozri napríklad [KT, Problem 14.9], [Ci, Lemma 4.4.4], [T, Theorem 1.8.9], [E, Problem 3.2.12].

Veta 7 (Alexander subbase theorem)**.** *Nech X je topologický priestor a $\mathcal{S}$ je jeho subbáza. Ak každé pokrytie $\mathcal{U} \subseteq \mathcal{S}$ má konečné podpokrytie, tak X je kompaktný.*

Dôkaz. Sporom. Nech X spĺňa uvedenú vlastnosť pre subbázu $\mathcal{S}$ a pritom nie je kompaktný.

To znamená, že existuje otvorené pokrytie, ktoré nemá konečné podpokrytie. Z Zornovej lemy vyplýva, že existuje aj maximálne pokrytie s touto vlastnosťou. Overme predpoklady Zornovej lemy. Nech $\mathcal{C}$ je reťazec takýchto pokrytí. Potom evidentne $\bigcup\mathcal{C}$ je tiež pokrytie. Ak by malo konečné podpokrytie, tak toto podpokrytie je už podpokrytím niektorého prvku z $\mathcal{C}$. (Vďaka konečnosti a tomu, že $\mathcal{C}$ je reťazec.)

Nech teda $\mathcal{C}$ je maximálne otvorené pokrytie, ktoré nemá konečné podpokrytie. Špeciálne to znamená, že ak pridáme ľubovoľnú otvorenú množinu U, tak $\mathcal{C} \cup \{U\}$ už bude mať pokrytie.

Uvažujme teraz systém $\mathcal{C} \cap \mathcal{S}$, t.j. zoberme len tie množiny z $\mathcal{C}$, ktoré patria do subbázy. Tento systém už nie je pokrytím – inak by mal konečné podpokrytie. Teda existuje $x \in X$, ktoré nie je pokryté žiadnou množinou z $\mathcal{C} \cap \mathcal{S}$.

Keďže $\mathcal{C}$ je pokrytie, bod x musí byť pokrytý nejakou množinou z $\mathcal{C}$, teda máme $x \in U \in \mathcal{C}$. Ďalej existujú $S_1, \dots, S_n$ také, že $x \in S_1 \cap \dots \cap S_n \subseteq U$.

Pretože bod x nie je pokrytý žiadnou množinou z $\mathcal{C} \cap \mathcal{S}$, máme $S_i \notin \mathcal{C}$ (pre $i = 1, \dots, n$). To ale znamená, že $\mathcal{C} \cup \{S_i\}$ už má nejaké konečné podpokrytie, čiže existuje konečný podsystém

$\mathcal{C}_i \subseteq C$ taký, že $\mathcal{C}_i \cup \{S_i\}$ pokrýva celé X. Posledná podmienka je ekvivalentná s tým, že $X \setminus S_i \subseteq \bigcup C_i$.

Potom ale dostaneme

$$X \setminus U \subseteq X \setminus \bigcap_{i=1}^{n} S_i = \bigcup_{i=1}^{n} (X \setminus S_i) \subseteq \bigcup_{i=1}^{n} \bigcup \mathcal{C}_i.$$

Teda

$$\mathcal{F} = \{U\} \cup \bigcup_{i=1}^{n} \mathcal{C}_i$$

je konečné podpokrytie pokrytia $\mathcal{C}$. $\square$

Z Alexandrovej vety o subbáze vieme ľahko dostať Tichonovovu vetu.

Veta 8 (Tichonov)**.** *Ľubovoľný súčin kompaktných priestorov je kompaktný.*

Dôkaz. Nech $\{X_i, i \in I\}$ je systém kompaktných priestorov. V priestore $X = \prod_{i \in I} X_i$ máme subbázu tvorenú množinami $p_i^{-1}(U)$ pre ľubovoľné $i \in I$ a ľubovoľnú otvorenú množinu U v X_i, kde $p_i \colon X \to X_i$ označuje projekciu na i-tu zložku. Chceme ukázať, že každé pokrytie množinami z tejto subbázy má konečné podpokrytie.

Nech teda $\mathcal{C}$ je ľubovoľné pokrytie subbázovými množinami. Označme

$$\mathcal{C}_i = \{U \subseteq X; p_i^{-1}(U) \in \mathcal{C}\}.$$

Ak pre niektoré $i \in I$ tvorí $\mathcal{C}_i$ pokrytie, tak má konečné podpokrytie $\mathcal{F}_i$ a

$$\{p_i^{-1}(U); U \in \mathcal{F}_i\}$$

je konečné podpokrytie pokrytia $\mathcal{C}$.

Zostáva teda možnosť, že pre žiadne $i \in I$ systém $\mathcal{C}_i$ nepokrýva X_i, čo znamená, že existuje $x_i \in X_i$, ktoré nie je pokryté systémom $\mathcal{C}_i$, t.j.

$$x_i \notin \bigcup \mathcal{C}_i.$$

Ukážeme, že táto možnosť vedie k sporu.

Definujme prvok $f \in X$ predpisom [4]

$$f(i) = x_i.$$

Potom $f \notin \bigcup \mathcal{C}$, čo znamená, že $\mathcal{C}$ nie je pokrytie. Skutočne, ak by f patrilo do nejakej množiny $p_i^{-1}(U)$ z $\mathcal{C}$, znamenalo by to, že $f(i) = x_i \in U$, čo je v spore s výberom x_i. $\square$

2.2 Hahn-Banachova veta

Ďalšia situácia, v ktorej sa často používa Zornova lema, je rozširovanie zobrazení s nejakou vlastnosťou z podmnožiny na celú množinu.

Čiastočne usporiadaná množina, s ktorou v takomto prípade pracujeme, je takáto: Je daná nejaká množina X a pracujeme so systémom

$$\mathcal{Z} = \{(f, A); A \subseteq M, f \text{ je zobrazenie definované na množine } A\}.$$

[4] Využívame AC – pre každé $i \in I$ sme vybrali jedno x_i.

(Prípadne môžeme pracovať s nejakým podsystémom $\mathcal{Z}$.) Na $\mathcal{S}$ sa dá zaviesť čiastočné usporiadanie

$$(f,A) \preceq (g,B) \qquad \Leftrightarrow \qquad A \subseteq B \wedge g|_A = f.$$

Stručne: $f \preceq g$ znamená, že g je rozšírením zobrazenia A.

Ľahko sa overí, že $\preceq$ je skutočne čiastočným usporiadaním.

Takýmto spôsobom sa dá napríklad ukázať, že v ZF platí (ZL)$\Rightarrow$(AC). Tu použijeme takéto usporiadanie na množine čiastočných selektorov. (T.j. na množine funkcií definovaných na podsystémoch $\mathcal{S}$ s vlastnosťou $f(x) \in x$.)

My si ako ilustráciu ukážeme Hahn-Banachovu vetu, ktorá je jeden z najčastejšie používaných výsledkov vo funkcionálnej analýze.[5]

Najprv zadefinujeme niektoré pojmy.

Definícia 9. Nech X je vektorový priestor a $f\colon X \to \mathbb{R}$ je funkcia.

(i) Funkcia f je *konvexná* ak pre ľubovoľné $x, y \in X$ a $\alpha \in (0,1)$ platí

$$f(\alpha x + (1-\alpha)y) \leq \alpha f(x) + (1-\alpha) f(y).$$

(ii) Funkcia f je *subaditívna,* ak pre ľubovoľné $x, y \in X$ platí

$$f(x+y) \leq f(x) + f(y).$$

(iii) Funkcia f je *pozitívne homogénna,* ak pre ľubovoľné $\alpha > 0$ a $x \in X$ platí $f(\alpha x) = \alpha f(x)$.

(iv) Funkcia f je *sublineárna,* ak je subaditívna a pozitívne homogénna

(v) Funkcia f je *polonorma,* ak je subaditívna a pre ľubovoľné $\alpha \in \mathbb{R}$, $x \in X$ platí $f(\alpha x) = |\alpha| f(x)$.

Môžeme si všimnúť, že definícia polonormy sa podobá na definíciu normy, iba sme z nej vynechali podmienku, že $f(x) = 0$ iba pre $x = 0$. Takisto je ľahko vidieť, že polonorma $\Rightarrow$ sublineárna $\Rightarrow$ konvexná.

Hahn-Banachova veta sa často nájdete sformulovanú pre polonormy alebo pre sublineárne funkcie. Tu uvedená formulácia s konvexnou funkciou je o čosi všeobecnejšia; v aplikáciach aj tak prakticky vždy budete pracovať s polonormou. Takisto sa obvykle neuvádza rozsah možných hodnôt takéhoto rozšírenia, hoci implicitne sa v dôkaze nachádza. Keďže občas môže byť možný rozsah hodnôt užitočný, doplnil som ho sem. (Formulácia s konvexnou funkciou je napríklad v [AB, Theorem 5.53])

Definícia 10. Nech $f, p\colon X \to \mathbb{R}$ a $M \subseteq X$. Hovoríme, že funkcia f je *majorizovaná funkciou p na množine M,* ak

$$(\forall M) f(x) \leq p(x).$$

Veta 11 (Hahn-Banach)**.** *Nech X je vektorový priestor a $p\colon X \to \mathbb{R}$ je konvexná funkcia. Nech M je podpriestor X a nech $f\colon M \to \mathbb{R}$ je lineárny funkcionál, ktorý je na M majorizovaný funkciou p. Potom existuje lineárna funkcia $\hat{f}$, ktorá je rozšírením f na celé X a je majorizovaná funkciou p na celom X.*

Navyše pre každé $x \in X$ existuje rozšírenie nadobúdajúce hodnotu $\hat{f}(x) = c$ práve vtedy, keď

$$\sup_{m \in M, \lambda > 0} \frac{f(m) - p(m - \lambda x)}{\lambda} \leq c \leq \inf_{m \in M, \mu > 0} \frac{p(m + \mu x) - f(m)}{\mu}. \qquad (1)$$ {EQRANGE}

[5]Spisovne je asi Hahnova-Banachova veta, ale ja si na to už asi nezvyknem.

V prípade, že p je kladne homogénna, možno vyjadrenie tohoto intervalu zjednodušiť na

$$\sup_{m\in M}[f(m)-p(m-x)] \le c \le \inf_{m\in M}[p(m+v)-f(m)].$$

Ak funkcie p a f navyše spĺňajú podmienku

$$(\forall x\in X)(\forall y\in M)p(x+y)=p(x)+f(y),$$

tak sa tento interval dá zjednodušiť na tvar

$$-p(-x)\le c\le p(x).$$

Plán dôkazu je takýto: Najprv ukážeme, že sa vždy dá urobiť rozšírenie o jednu dimenziu. Pomocou tohoto faktu a ZL to potom rozšírime na celý priestor. Rozšírenie o jeden rozmer dokážme a sformulujme ako samostatnú lemu.

Lema 12. *Nech X je vektorový a $p\colon X\to\mathbb{R}$ je konvexná funkcia. Nech M je podpriestor X a nech $f\colon M\to\mathbb{R}$ je lineárny funkcionál, ktorý je na M majorizovaný funkciou p. Nech ďalej $x\in X$.*

Potom existuje lineárne zobrazenie $\overline{f}\colon [M\cup\{x\}]\to\mathbb{R}$, ktoré je na podpriestore $[M\cup\{x\}]$ majorizované funkciou p.

Možné hodnoty, ktoré môže takéto rozšírenie nadobúdať v bode x, sú presne hodnoty z intervalu uvedeného v (1)*.*

Dôkaz. Máme danú lineárnu funkciu $f\colon M\to\mathbb{R}$, ktorú chcem rozšíriť na podpriestor

$$[M\cup\{x\}]=\{m+ax; m\in M, a\in\mathbb{R}\}.$$

Akonáhle si zvolíme hodnotu $\overline{f}(x)=c$, tak už je hodnota funkcie $\overline{f}$ jednoznačne určená pre všetky body z $[M\cup\{x\}]$, pre ľubovoľné $a\in\mathbb{R}$ totiž máme

$$f(m+ax)=f(m)+ac.$$

Zostáva nám zistiť, či existuje taká voľba c, aby bol funkcionál $\overline{f}$ majorizovaný funkciou p na celom podpriestore $[M\cup\{x\}]$.

Chceme teda, aby pre ľubovoľné $m\in M$, $a\in\mathbb{R}$ platilo

$$f(m+ax)=f(m)+ac\le p(m+ax).$$

Ak a je kladné, tak uvedená nerovnosť je ekvivalentná s

$$c\le\frac{p(m+ax)-f(m)}{a}.$$

Pre záporné a naopak dostávame

$$c\ge\frac{p(m+ax)-f(m)}{a}.$$

Zistili sme teda, že hodnota c musí nutne vyhovovať týmto nerovnostiam

$$\sup_{m\in M,\lambda>0}\frac{f(m)-p(m-\lambda x)}{\lambda}\le c\le\inf_{m\in M,\mu>0}\frac{p(m+\mu x)-f(m)}{\mu}. \qquad (2) \quad \{\texttt{EQLMRANGE}\}$$

Pomerne ľahko vidno, že voľba c vyhovujúceho nerovnostiam (2) už zabezpečí, že $\overline{f}$ bude majorizované funkciou p. Ak $a > 0$, tak

$$f(m + ax) = f(m) + ac \leq f(m) + a\frac{p(m + ax) - f(m)}{a} = p(m + ax).$$

Podobne pre $a < 0$ máme

$$f(m + ax) = f(m) + ac \leq f(m) + a\frac{p(m + ax) - f(m)}{a} = p(m + ax).$$

Zostáva nám teda len overiť, či je takáto voľba možná (či existuje aspoň jedno c v uvedenom intervale). Pýtame sa teda vlastne, či pre ľubovoľné $m, m' \in m$, $\lambda, \mu > 0$ platí

$$\frac{f(m) - p(m - \lambda x)}{\lambda} \leq \frac{p(m' + \mu x) - f(m')}{\mu}.$$

Táto nerovnosť je ekvivalentná s

$$f\left(\frac{1}{\mu}m' + \frac{1}{\lambda}m\right) = \frac{1}{\mu}f(m') + \frac{1}{\lambda}f(m) \leq \frac{p(m' + \mu x)}{\mu} + \frac{p(m - \lambda x)}{\lambda}.$$

Po vydelení tejto rovnosti kladným výrazom $\frac{1}{\mu} + \frac{1}{\lambda} = \frac{\mu+\lambda}{\mu\lambda}$ máme ekvivalentnú nerovnosť

$$\frac{f(\frac{1}{\mu}m + \frac{1}{\lambda}m')}{\frac{1}{\mu} + \frac{1}{\lambda}} = \frac{f(\frac{1}{\lambda}(m - \lambda x) + \frac{1}{\mu}(m' + \mu x))}{\frac{1}{\mu} + \frac{1}{\lambda}} \leq \frac{\frac{p(m'+\mu x)}{\mu} + \frac{p(m-\lambda x)}{\lambda}}{\frac{1}{\mu} + \frac{1}{\lambda}}$$

Ak označíme $\alpha = \frac{\frac{1}{\mu}}{\frac{1}{\mu}+\frac{1}{\lambda}} = \frac{\lambda}{\mu+\lambda}$, tak predošlá nerovnosť je ekvivalentná s nerovnosťou

$$f(\alpha(m' + \mu x) + (1 - \alpha)(m - \lambda x)) \leq \alpha p(m' + \mu x) + (1 - \alpha)p(m - \lambda x). \qquad (3)$$ {EQTREBA}

Pretože

$$\alpha(m' + \mu x) + (1 - \alpha)(m - \lambda x) = \frac{\lambda(m' + \mu x) + \mu(m - \lambda x)}{\mu + \lambda} = \frac{\lambda m' + \mu m}{\mu + \lambda}$$

je prvok z M, máme nerovnosť

$$f(\alpha(m' + \mu x) + (1 - \alpha)(m - \lambda x)) \leq p(\alpha(m' + \mu x) + (1 - \alpha)(m - \lambda x))$$

na základe predpokladu, že na podpriestore M je funkcia f majorizovaná funkciou p. Z konvexnosti funkcie p máme

$$p(\alpha(m' + \mu x) + (1 - \alpha)(m - \lambda x)) \leq \alpha p(m' + \mu x) + (1 - \alpha)p(m - \lambda x).$$

Z predošlých dvoch nerovností už vyplýva nerovnosť (3), ktorú sme chceli dokázať. □

Dôkaz Hahn-Banachovej vety. Budeme pracovať s množinou všetkých lineárnych rozšírení funkcie f, ktoré sú majorizované funkciou p. Čiastočné usporiadanie je

$$g \preceq h \Leftrightarrow h \text{ je rozšírením } g.$$

Ľahko sa overí, že ak systém funkcií $\{f_i; i \in I\}$ je reťazec v tejto čiastočne usporiadanej množine, tak

$$\hat{f} := \bigcup_{i \in I} f_i$$

je jeho horným ohraničením. Teda množina s ktorou pracujeme má maximálny prvok (podľa ZL).

Predchádzajúca lema zaručuje, že maximálne rozšírenie zobrazenia f už musí byť definované na celom X, inak by sa dalo rozšíriť na podpriestor dimenzie väčšej o 1. □

Literatúra

[AB] Charalambos D. Aliprantis and Kim C. Border. *Infinite Dimentional Analysis, A Hitchhiker's Guide*. Springer, Berlin, 3rd edition, 2006.

[Ci] Krzysztof Ciesielski. *Set Theory for the Working Mathematician*. Cambridge University Press, Cambridge, 1997. London Mathematical Society Student Texts 39.

[Co] Keith Conrad. Zorn's lemma. `http://www.math.uconn.edu/~kconrad/blurbs/`.

[E] Ryszard Engelking. *General Topology*. Heldermann Verlag, Berlin, 1989. Revised and completed edition, Sigma Series in Pure Mathematics, Vol. 6.

[G] Jaroslav Guričan. Vybrané kapitoly z algebry. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[KT] Péter Komjáth and Vilmos Totik. *Problems and Theorems in Classical Set Theory*. Springer, 2006. Problem Books in Mathematics.

[R] Miles Reid. *Undergraduate Commutative Algebra*. Cambridge University Press, Cambridge, 1995. London Mathematical Society Stuent Texts 29.

[T] Terence Tao. *An epsilon of room: pages from year three of a mathematical blog.*