Pomocný text k 5. sérii

Báze a moduly

autor: *Tomáš Perutka*

V tomto studijňáku se trochu seznámíme s pojmy zmíněnými v nadpisu. Nejenže vám jejich znalost pomůže vyřešit příklady 1-4, ale jejich znalost je ve světě dnešní matematiky – a jejích aplikací – naprosto nezbytná. Pokud si tedy z toho textu něco zapamatujete a odnesete, neuděláte chybu!

Jelikož mezi čtenáři se nachází jak začátečníci (kteří žádný z pojmů v nadpisu ještě neznají), tak mírně pokročilí (kteří už o nich něco ví), snažili jsme se tento text napsat dvouúrovňově, aby něco dal oběma skupinám čtenářů.

R-moduly

Značení. *Napíšeme-li v následujícím textu R, bude to souhrnné označení pro číselné množiny $\mathbb{Z}$ a $\mathbb{R}$.* Pro pokročilé čtenáře podotýkám, že R ve skutečnosti může být libovolný komutativní okruh (tedy např. $\mathbb{Q}, \mathbb{C}$, okruh zbytkových tříd $\mathbb{Z}_m$ pro $m \in \mathbb{N}$, Gaussova čísla $\mathbb{Z}[i]$,...).

Všimněme si, že na každé ze zmíněných množin máme definované sčítání a násobení. Součin dvou prvků $x, y \in R$ budeme značit bez tečky jako xy. (Za chvíli uvidíme, že tečka bude vyhrazena na trochu jiný druh násobení.)

Co je to tedy R-modul? Je to množina M, jejíž prvky spolu umíme sčítat, a navíc je umíme násobit prvky z R. Trochu formálněji je to *komutativní grupa* vybavená *skalárním násobením* prvky z R. Hned si řekneme, co to znamená – nebojte se, není to nic těžkého, ač to tak může na první pohled vypadat. Vlastně to jen formalizuje věci, které už dávno znáte.

Když jste se například ve škole učili o celých nebo reálných číslech, jistě vám bylo řečeno (nebo jste si toho sami všimli), že jejich sčítání je komutativní a asociativní (tedy můžete prohodit pořadí sčítanců a při sčítání více čísel nezáleží, v jakém pořadí je sčítáte). Další pozoruhodná vlastnost sčítání v $\mathbb{Z}$ i $\mathbb{R}$ je to, že zde máme prvek 0, který „nic nedělá“: $0+x = x$ pro libovolné x. Dále pro každý prvek x máme opačný prvek $-x$, jejichž součtem je nula.

Mít na množině definovanou operaci, která splňuje tyto vztahy, je tak běžné, že proto matematici vymysleli speciální název:

Definice 1. O množině M řekneme, že je to komutativní grupa, pokud na ní máme definovanou operaci sčítání dvou prvků, která splňuje tyto podmínky:

1. operace je asociativní, tzn. pro každé $x, y, z \in M$ platí $(x + y) + z = x + (y + z)$,
2. operace je komutativní, tzn. pro každé $x, y \in M$ platí $x + y = y + x$,

3. existuje tzv. nulový (též neutrální) prvek, tedy prvek $0_M \in M$ takový, že pro každé $x \in M$ platí $0_M + x = x = x + 0_M$,

4. ke každému prvku můžeme nalézt prvek k němu inverzní, tedy pro každé $x \in M$ existuje $y \in M$ tak, že $x + y = 0_M = y + x$ (obvykle tento prvek značíme jako $-x$).

Definice 2. Nechť M je komutativní grupa. Řekneme, že M je R-modul, pokud existuje operace $R \times M \to M$, kterou zapisujeme jako $(r, m) \mapsto r \cdot m$ a říkáme jí skalární násobení, taková, že pro všechna $r, s \in R, m, n \in M$ platí:

1. $(rs) \cdot m = r \cdot (s \cdot m)$,

2. $(r + s) \cdot m = r \cdot m + s \cdot m$,

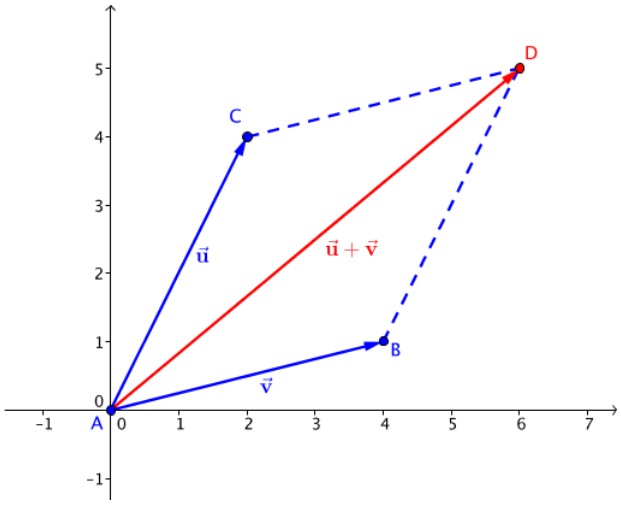
3. $r \cdot (m + n) = r \cdot m + r \cdot n$,

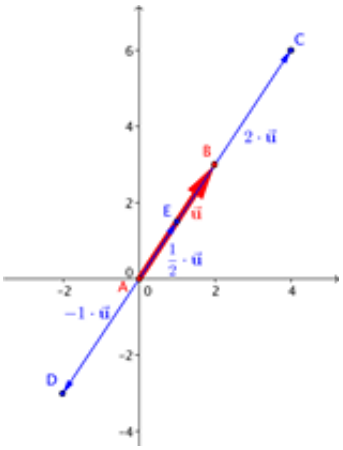
4. $1 \cdot m = m$.

Nyní je čas ukázat si několik příkladů toho, jak takový R-modul může vypadat.

Příklad 3. (jednoduchý a důležitý) $R^n = \{(a_1, ..., a_n) | a_1, ..., a_n \in R\}$ je R-modul. Komutativní grupu z této množiny dělá sčítání po složkách: $(a_1, ..., a_n) + (b_1, ..., b_n) \overset{\text{def}}{=} (a_1 + b_1, ..., a_n + b_n)$, nulový prvek je tvaru $0_{R^n} = (0, ..., 0)$ a opačný prvek si jistě domyslíte. Násobení prvkem $r \in R$ můžeme opět definovat po složkách: $r \cdot (a_1, ..., a_n) = (ra_1, ..., ra_n)$. Je jednoduché si ověřit, že všechny podmínky v definicích výše jsou splněny: využíváme toho, že sčítání i násobení v R je komutativní a asociativní a navíc tyto dvě operace splňují $r(s + t) = rs + rt, (s + t)r = sr + tr$ (distributivní zákony).

Nechť $R = \mathbb{R}$. Pak se na prvky $\mathbb{R}$-modulu $\mathbb{R}^n$ můžeme dívat jako na orientované úsečky vycházející z počátku souřadnicového systému (tedy z bodu $(0, ..., 0)$). Sčítání n-tic pak graficky vypadá tak, jak to známe ze středoškolské fyziky (viz obrázek). Násobení reálným číslem $c > 0$ pak vypadá tak, že úsečku $|c|$-krát prodloužíme (tedy pokud $|c| < 1$, tak vlastně zkracujeme). Pro $c < 0$ navíc ještě úsečku otočíme (viz obrázek).





Příklad 4. (trochu těžší, ale dost důležitý) Uvažujme soustavu lineárních rovnic (pro jednoduchost dvou rovnic o dvou neznámých, ale platí to i obecně)

$$a_{11}x + a_{12}y = 0,$$
$$a_{21}x + a_{22}y = 0,$$

kde koeficienty a_{ij} leží v R. Potom množina

$$M = \{(x, y) \in R^2 | x, y \text{ jsou řešením soustavy výše}\}$$

tvoří R-modul, opět vzhledem ke sčítání a násobením po složkách. Opravdu: uvědomme si, že pro řešení $(x_1, y_1), (x_2, y_2)$ rovnice výše dostaneme $a_{11}(x_1+x_2)+a_{12}(y_1+y_2) = (a_{11}x_1 + a_{12}y_1)+(a_{11}x_2+a_{12}y_2) = 0+0 = 0$, $a_{11}(rx_1)+a_{12}(ry_1) = r(a_{11}x_1+a_{12}y_1) = r \cdot 0 = 0$. Pro druhý řádek soustavy můžeme postupovat analogicky. Tedy M je na obě operace uzavřená (součet i násobek řešení je opět řešení). Navíc nulový prvek 0_M je řešení $x = y = 0$. Podmínky z definic se ověří stejně jako v předchozím příkladě.

Příklad 5. (ne tak důležitý, ale může se hodit) $\mathbb{R}$ je $\mathbb{Z}$-modul. Proč? Operace sčítání dělá z $\mathbb{R}$ komutativní grupu. Skalární násobení je v tomto případě běžné násobení dvou čísel. To jistě splňuje podmínky definice 2: (1) je asociativita násobení, (2) a (3) jsou distributivní zákony a (4) jistě platí.

V tomhle textu bohužel není moc prostoru na důkazy nějakých vět, ale jeden malý se nám sem vejde:

Tvrzení 6. Nechť M je R-modul, $m \in M$. Pak $0 \cdot m = 0_M$ a $(-1) \cdot m = -m$.

Důkaz. Všimněme si, že v první rovnosti máme dvě různé nuly, je to $0 \in R$ a $0_M \in M$. Využijeme druhé podmínky z definice: $0 \cdot m = (0 + 0) \cdot m = 0 \cdot m + 0 \cdot m$. Od obou stran této rovnosti můžeme odečíst výraz $0 \cdot m$ a dostáváme $0_M = 0 \cdot m$.

Nyní využijme této nově nabyté znalosti: $0_M = 0 \cdot m = (1+(-1)) \cdot m = 1 \cdot m+(-1) \cdot m = m + (-1) \cdot m$ (použili jsme podmínku (2) a potom (1) z definice 2). Tedy odečtením m od obou stran rovnosti opravdu dostáváme $(-1) \cdot m = -m$ a důkaz je hotov.

(pro velmi pokročilé) Díky tomuto můžeme ukázat, že na *každé* komutativní grupě M máme právě jednu strukturu $\mathbb{Z}$-modulu. Nechť $m \in M$. Jelikož podle podmínky (4) v

definici 2 platí $1 \cdot m = m$, máme z podmínky (2): $2 \cdot m = (1+1) \cdot m = 1 \cdot m + 1 \cdot m = m + m$. Indukcí dostaneme, že každé přirozené n nutně musí splňovat $n \cdot m = m + m + \cdots + m$ (sčítáme n-krát). Potom podle předchozího tvrzení máme $0 \cdot m = m$ a $(-n) \cdot m = ((-1) \cdot n) \cdot m = (-1) \cdot (n \cdot m) = -(n \cdot m)$. (Využili jsme tedy i podmínku 1 z def. 2.) Snadno se ověří, že takhle definované zobrazení splňuje podmínky z def. 2, a tedy M je $\mathbb{Z}$-modul. Vzhledem k tomu, jak jsme postupovali, je vidět, že jiné skalární násobení prvky ze $\mathbb{Z}$ na M definovat nelze.

Lineární závislost a nezávislost, báze

Představte si, že před sebou máte dlouhé nudné dopoledne a někdo vám dal na hraní prvky $x_1, ..., x_n$ nějakého R-modulu M. Jak se s nimi můžete zabavit? Můžete se snažit pomocí prvků, které máte k dispozici, vyrobit nové prvky modulu M. To lze udělat buď tím, že nějaké prvky sečtete, nebo tak, že je vynásobíte skalárem. Tyto dva postupy můžete libovolně kombinovat. To motivuje následující definici:

Definice 7. Nechť M je R-modul, $n \in \mathbb{N}$, $x_1, ..., x_n \in M$. Lineární kombinace prvků $x_1, ..., x_n$ je libovolný výraz ve tvaru $r_1 \cdot x_1 + \cdots + r_n \cdot x_n$ pro $r_1, ..., r_n \in R$. Množinu všech lineárních kombinací těchto prvků, tj. množinu $\{r_1 \cdot x_1 + \cdots + r_n \cdot x_n | r_1, ..., r_n \in R\}$ nazýváme lineární obal prvků $x_1, ..., x_n$.

Lineární kombinace je tedy způsob, jak ze zadaných prvků vytvářet nové prvky. Linární obal je potom množina všech prvků, které můžeme získat.

Příklad 8. Lineární obal prvků $(1, 0), (0, 1) \in R^2$ je celý R-modul R^2: opravdu, libovolný prvek $(r, s) \in R^2$ mohu napsat jako lineární kombinaci $r \cdot (1, 0) + s \cdot (0, 1)$.

Příklad 9. Uvažujme $\mathbb{R}$ jakožto $\mathbb{Z}$-modul (tj. máme povoleno násobit pouze celé číslo s reálným). Pak lineární obal prvků $1, \sqrt{2} \in \mathbb{R}$ obsahuje např. prvky $0, 42 + 2021\sqrt{2}, -5\sqrt{2}$. Neobsahuje ovšem např. reálná čísla $\sqrt{5}, \pi, \frac{\sqrt{2}}{68}$.

Pokud chceme zkoumat daný R-modul M, je tedy vzhledem k předcházejícím úvahám celkem logický postup zkusit najít nějakou skupinku prvků z M, jejichž lineárním obalem bude celé M. Tím se nám leccos zjednoduší, protože z konečného množství údajů (zadané prvky $x_1, ..., x_n$) získáme informace o všech prvcích v M (jsou tvaru $r_1 \cdot x_1 + \cdots + r_n \cdot x_n$) a těch jistě může být nekonečně mnoho. Vzpomeňte si na 5: takhle by nám stačilo nalézt konečně mnoho řešení naší soustavy rovnic a už bychom věděli, jak vypadají všechny!

Během tohoto postupu bychom měli dbát na efektivitu. Jistě, každý prvek v R^2 dostaneme jako lineární kombinaci prvků $(1, 0), (2, 3), (-19984126, 9279^{59489}), (0, 1)$, ale stejného výsledku dosáhneme i pomocí pouze prvního a posledního prvku z těchto čtyř (viz 10).

Tyto úvahy motivují následující definice:

Definice 10. Nechť M je R-modul, $n \in \mathbb{N}$, $x_1, ..., x_n \in M$. Řekneme, že prvky $x_1, ..., x_n$ generují M, pokud je jejich lineární obal roven M.

Tedy každý prvek z M dostaneme jako lineární kombinaci těch generujících.

Definice 11. Nechť M je R-modul, $n \in \mathbb{N}$, $x_1, ..., x_n \in M$. Řekneme, že prvky $x_1, ..., x_n$ jsou lineárně nezávislé, pokud jediná n-tice prvků $r_1, ..., r_n \in R$ splňující $r_1 \cdot x_1 + \cdots + r_n \cdot x_n = 0$ je $r_1 = \cdots = r_n = 0$. V opačném případě říkáme, že prvky $x_1, ..., x_n$ jsou lineárně závislé.

Tato definice se týká oné efektivity, o níž jsme mluvili výše. To, že jsou prvky linárně závislé, znamená, že je jich „moc". Prvky $(1,0), (2,3), (-2021, 9279^{59489}), (0,1)$ sice generují R^2, ale jsou lineárně závislé: to nám dokazuje např. lineární kombinace

$$2021 \cdot (1,0) + 0 \cdot (2,3) + 1 \cdot (-2021, 9279^{59489}) + (-9279^{59489}) \cdot (0,1) = (0,0).$$

Naopak prvky $(1,0), (0,1)$ jsou lineárně nezávislé: pokud pro nějaká $r, s \in R$ platí $r \cdot (1,0) + s \cdot (0,1) = (0,0)$, znamená to $(r,s) = (0,0)$, tedy $r = 0, s = 0$. To nás tedy přivádí až k naší finální definici:

Definice 12. Báze R-modulu M je n-tice prvků $x_1, ..., x_n \in M$ taková, že:

- $x_1, ..., x_n$ generují M,
- $x_1, ..., x_n$ jsou lineárně nezávislé.

Příklad 13. Prvky $(1,0), (0,1)$ tvoří bázi R-modulu R^2. Platnost obou podmínek v definici jsme již ověřili. Obecněji, R-modul R^n má vždy bázi skládající se z n různých n-tic, které mají na jedné pozici jedničku a na ostatních nulu.

Příklad 14. (pro pokročilé) $\mathbb{R}$ jakožto $\mathbb{Z}$-modul má nekonečnou bázi. $\mathbb{C}$ jakožto $\mathbb{R}$-modul má bázi $\{1, i\}$. (Pro experty: kvaterniony jakožto $\mathbb{R}$-modul mají bázi $\{1, i, j, k\}$)

Můžeme si dokázat následující jednoduché a pěkné tvrzení, které potvrzuje, že báze je efektivní způsob, jak vygenerovat všechny prvky z M:

Tvrzení 15. Nechť $x_1, ..., x_n$ tvoří bázi daného R-modulu M. Pak lze každý prvek $m \in M$ napsat jediným způsobem jako lineární kombinaci prvků této báze (až na pořadí sčítanců).

Důkaz. Jelikož se jedná o bázi, každý prvek z M lze napsat alespoň jedním způsobem jako lineární kombinace prvků $x_1, ..., x_n$. Dokážeme sporem, že takový zápis vždy existuje jediný. Nechť tedy $m \in M$, $r_1, ..., r_n, s_1, ..., s_n \in R$ tak, že $r_1x_1 + \cdots + r_nx_n = m = s_1x_1 + \cdots + s_nx_n$. Bez újmy na obecnosti předpokládejme, že $r_1 \neq s_1$. Potom ale dostáváme $(r_1 - s_1)x_1 + \cdots + (r_n - s_n)x_n = 0$. Jelikož $r_1 - s_1 \neq 0$, dostáváme spor s lineární nezávislostí prvků $x_1, ..., x_n$.

(pro mírně pokročilé) Všimněme si, že jsme použili kromě podmínek z definice 2 i dříve dokázané tvrzení, že $(-1) \cdot m = -m$: díky tomu $(-s) \cdot m = ((-1)s) \cdot m = (-1) \cdot (s \cdot m) = -s \cdot m$ a tedy opravdu dostaneme $(r_1x_1 + \cdots + r_nx_n) - (s_1x_+ \cdots + s_nx_n) = (r_1 - s_1)x_1 + \cdots + (r_n - s_n)x_n$.

Na závěr této sekce si řekneme jeden důležitý výsledek:

Nechť $R = \mathbb{R}$ (pro pokročilé: nechť R je těleso), M je $\mathbb{R}$-modul. Potom:

- každé dvě báze R-modulu M mají stejný počet prvků, který se označuje jako $\dim M$,

- každá lineárně nezávislá k-tice prvků splňuje $k \leq \dim M$,
- každá k-tice prvků pro $k > \dim M$ je lineárně závislá.

Číslo $\dim M$ se nazývá dimenze R-modulu M.

Varování a trocha terminologie. Pozor, v případě $R \neq \mathbb{R}$ (v případě, kdy R není těleso) může být situace o poznání složitější! Proto se také pro R-moduly, kde $R = \mathbb{R}$ (R je těleso), používá jiný název: *vektorové prostory*. To proto, že moduly nad $\mathbb{R}$ (tělesem) jsou o poznání jednodušší, a tedy byly studovány dříve než R-moduly pro $R = \mathbb{Z}$ (libovolný komutativní okruh); tím pádem se pro ně vžil jiný název.

Příklad 16. Dimenze $\mathbb{R}$-modulu $\mathbb{R}^n$ je rovna n, jelikož jsme v příkladě 15 našli n-prvkovou bázi. Totéž platí pro $\mathbb{Z}$-modul $\mathbb{Z}^n$: obecně může být sice komplikované pro $\mathbb{Z}$-moduly definovat dimenzi, ale $\mathbb{Z}^n$ je natolik slušně vychovaný, že to nečiní žádný problém.

Využití báze

Překvapivě často se v matematice i jejich aplikacích stane, že náš úkol je najít bázi nějakého R-modulu. Děje se to např. v teorii čísel, zpracování dat, nebo v teorii tzv. obyčejných diferenciálních rovnic. Děje se to rovněž v sérii Brkosu, jejíž řešení je nyní vaším úkolem.

Nejčastější případ, kdy hledáme bázi, nastává, kdy máme nějakou rovnici či soustavu rovnic. Ukažme si to na několika příkladech:

1. Hledáme celočíslená řešení rovnice $2x - 3y = 0$. Ta tvoří $\mathbb{Z}$-modul $M = \{(x, y) \in \mathbb{Z}^2 | 2x - 3y = 0\}$. Ukážeme, že každé dva nenulové prvky $(x_1, y_1), (x_2, y_2)$ tohoto $\mathbb{Z}$-modulu jsou lineárně závislé. Abychom viděli proč, uvědomme si, že $2x_1 = 3y_1, 2x_2 = 3y_2$. Proto tedy

$$\begin{aligned}(2y_2) \cdot (x_1, y_1) + (-2y_1) \cdot (x_2, y_2) &= (2x_1y_2, 2y_1y_2) + (-2x_2y_1, -2y_1y_2) \\ &= (3y_1y_2, 2y_1y_2) + (-3y_2y_1, -2y_1y_2) \\ &= (0, 0).\end{aligned}$$

Jelikož $2y_2 \neq 0, -2y_1 \neq 0$, dostáváme, že naše prvky jsou lineárně závislé.

Z toho můžeme odvodit, že M má jednoprvkovou bázi. Touto bází bude nějaký prvek $(x, y) \in M, x \neq 0, y \neq 0$ takový, že $|x| + |y|$ je co nejmenší. Ostatní prvky pak dostaneme lineární kombinací, v tomto případě jako násobek $c \cdot (x, y), c \in \mathbb{Z}$. Hledaný prvek báze je tedy $(3, 2)$ a jistě si ověříte, že každé řešení je opravdu tvaru $c \cdot (3, 2) = (3c, 2c)$.

Výsledek tohoto příkladu asi nebyl zas tak ohromující. Na závěr si tedy ukážeme něco o několik levelů náročnějšího.

2. (Pellova rovnice) Hledáme celočíselná řešení rovnice

$$x^2 - 2y^2 = 1.$$

Řekneme, že řešení této rovnice $(a, b) \in \mathbb{Z}^2$ je *minimální*, pokud $a \neq \pm 1, b \neq 0$ a $|a| + |b|\sqrt{2}$ je minimální mezi všemi řešeními kromě $(\pm 1, 0)$. Pomocí nikoli jednoduchých úvah o $\mathbb{Z}$-modulech a jejich bázích pak lze ukázat velice silné tvrzení: *každé další řešení (u, v) této rovnice splňuje $|u| + |v|\sqrt{2} = (|a| + |b|\sqrt{2})^n$ pro nějaké nezáporné celé číslo n.*

Minimální řešení ale v tomto případě najdeme velmi snadno: je tvaru $(a, b) = (3, 2)$. Tedy pouze z této informace jsme schopni pouhým umocňováním nalézt všechna řešení, např. $(u, v) = (3880899, 2744210)$ je řešení, které dostaneme umocněním $(3 + 2\sqrt{2})^9$.