UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA

BAKALÁŘSKÁ PRÁCE

Abstraktní derivace

Katedra algebry a geometrie
Vedoucí bakalářské práce: **RNDr. Pavel Ludvík, Ph.D.**
Vypracoval: **Jakub Baloun**
Studijní program: B0541A170020 Matematika
Studijní obor: Matematika
Forma studia: prezenční
Rok odevzdání: 2024

BIBLIOGRAFICKÁ IDENTIFIKACE

Autor: Jakub Baloun

Název práce: Abstraktní derivace

Typ práce: Bakalářská práce

Pracoviště: Katedra algebry a geometrie

Vedoucí práce: RNDr. Pavel Ludvík, Ph.D.

Rok obhajoby práce: 2024

Abstrakt: Abstraktní derivace jakožto zobrazení definované na okruhu, které je aditivní a splňuje pravidlo o derivaci součinu (neboli tzv. Leibnizovu formuli), je základním pojmem diferenciální algebry. V této práci je pojem derivace ještě poněkud zobecněn – je od ní požadována pouze platnost Leibnizovy formule. Cílem je prozkoumat vlastnosti takto definovaných zobrazení a nalézt souvislosti s jinými pojmy abstraktní algebry. Ukazuje se, že na spoustu známých vlastností běžných derivací na prostorech funkcí lze pohlížet jako na konsekvence pravidla o derivaci součinu. V práci jsou přirozeně zobecněny některé základní pojmy z diferenciálního počtu a je zkonstruováno několik příkladů abstraktních derivací. Tato zobrazení jsou zkoumána na různých strukturách (číselné obory, obory integrity s jednoznačným rozkladem, zobecněné asociativní algebry). Např. teorie tzv. lineárních derivací na zobecněných asociativních algebrách je pak aplikována na řešení ryze analytické úlohy, které by v mnoha případech bez tohoto algebraického přístupu bylo velice komplikované. Díky tomuto zobecnění pojmu derivace lze o množině všech derivací na dané struktuře dokázat některé zajímavé strukturální vlastnosti a také souvislosti s algebraickou strukturou homomorfismů jistých multiplikativních a aditivních grup.

Klíčová slova: abstraktní derivace, Leibnizova formule, logaritmická derivace, moduly nad okruhy, diferenciální algebra

Počet stran: 89

Počet příloh: 0

Jazyk: český

BIBLIOGRAPHICAL IDENTIFICATION

Author: Jakub Baloun

Title: Abstract derivation

Type of thesis: Bachelor's

Department: Department of Algebra and Geometry

Supervisor: RNDr. Pavel Ludvík, Ph.D.

The year of presentation: 2024

Abstract: The abstract derivation as a map defined on a ring that is additive and satisfies the product rule (or the so-called Leibniz formula) is a fundamental concept of differential algebra. In this paper, the notion of derivative is still somewhat generalized – only the validity of Leibniz's formula is assumed. The aim is to investigate the properties of mappings defined in this way and to find connections with other notions of abstract algebra. It turns out that many well-known properties of usual derivations on function spaces can be viewed as consequences of the product rule. In the paper, some basic notions of differential calculus are generalized and several examples of abstract derivations are constructed. These representations are studied on various structures (number fields, unique factorization domains, generalized associative algebras). For example, the theory of so-called linear derivations on generalized associative algebras is then applied to the solution of a purely analytic problem, which in many cases would be very complicated without this algebraic approach. Due to this generalization of the notion of derivation, it is possible to show some interesting structural properties about the set of all derivations on a given structure, as well as connections with the algebraic structure of certain homomorphisms of multiplicative and additive groups.

Key words: abstract derivation, Leibniz formula, logarithmic derivation, modules over rings, differential algebra

Number of pages: 89

Number of appendices: 0

Language: Czech

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně pod vedením pana RNDr. Pavla Ludvíka, Ph.D. a všechny použité zdroje jsem uvedl v seznamu literatury.

V Olomouci dne ....

podpis

Obsah

Poděkování

Rád bych touto cestou vyjádřil poděkování panu RNDr. Pavlovi Ludvíkovi, Ph.D. za jeho cenné rady, doporučení, věcné připomínky a vstřícnost při vedení mé bakalářské práce.

Úvod

Čtenář je jistě velmi dobře obeznámen s pojmy derivace funkce jedné proměnné a směrová a parciální derivace funkce více proměnných stejně tak jako se základními vlastnostmi těchto stěžejních pojmů matematické analýzy. Uveďme kupříkladu některé z nich:[1]

(*i*) aditivita:

$$D(f+g) = Df + Dg,$$

(*ii*) homogenita:

$$D(\alpha f) = \alpha Df,$$

(*iii*) pravidlo o derivaci součinu (tzv. *Leibnizova formule*):

$$D(fg) = (Df)g + fDg,$$

(*iv*) *řetízkové pravidlo* (anglicky *chain rule*) pro derivaci funkcí jedné proměnné:

$$D(f \circ g) = \Big((Df) \circ g\Big)Dg.^2$$

V této práci bude klíčovým pojmem Leibnizova formule uvedená v bodě (*iii*). Budeme se totiž zabývat právě zobrazeními splňujícími tento vztah.

Je určitě žádoucí, aby derivace funkcí byly jen speciálními případy takových zobrazení. To nás dovádí k tomu, abychom se zamysleli nad strukturami, na kterých jsou tyto diferenciální operátory definovány. Pro jednoduchost se nyní zaměřme na derivaci funkcí jedné proměnné. Přirozeným kandidátem na definiční obor tohoto operátoru je množina $\mathcal{C}^1(\Omega)$, kde $\Omega \subseteq \mathbb{R}$ je otevřená, tj. množina právě všech spojitě diferencovatelných funkcí $\Omega \to \mathbb{R}$. Tento operátor budeme značit $\frac{\mathrm{d}}{\mathrm{d}x}$. Pak je zřejmé, že

$$\frac{\mathrm{d}}{\mathrm{d}x} : \mathcal{C}^1(\Omega) \to \mathcal{C}(\Omega).$$

[1] D zde značí libovolný z výše uvedených operátorů, f, g jsou funkce, $\alpha \in \mathbb{R}$.

[2] Zde je důležité uprozornit na to, jakým způsobem definujeme skládání zobrazení. Ať A, B, C jsou neprázdné množiny a $g : A \to B$ a $f : B \to C$ jsou zobrazení množin. Pak *složením zobrazení* f a g (v tomto pořadí) rozumíme zobrazení $f \circ g$ definované předpisem

$$(f \circ g)(x) = f\big(g(x)\big),\ x \in A.$$

$f \circ g$ je tedy zobrazení z A do C.

Není těžké ověřit, že množiny $\mathcal{C}^1(\Omega)$ a $\mathcal{C}(\Omega)$ tvoří spolu se sčítáním a násobením funkcí unitární okruhy, kde nulovým prvkem je konstantní funkce $x \mapsto 0, x \in \Omega$ (tuto funkci budeme nadále označovat $\mathfrak{o}_\Omega$) a jednotkovým prvkem je konstatní funkce $x \mapsto 1, x \in \Omega$ (podobně tuto funkci budeme značit symbolem $\mathfrak{1}_\Omega$). Zjevně taky $\mathcal{C}^1(\Omega) \subseteq \mathcal{C}(\Omega)$,[3] a proto $\mathcal{C}^1(\Omega)$ je unitárním podokruhem[4] unitárního okruhu $\mathcal{C}(\Omega)$. Dostáváme tak, že definiční obor operátoru $\frac{\mathrm{d}}{\mathrm{d}x}$ je unitárním podokruhem jeho oboru hodnot (nebo, chcete-li, jeho obrazu). Tuto skutečnost ještě poněkud zobecníme.

Uvážíme-li dvě komutativní tělesa T_1 a T_2 taková, že $T_1 \subseteq T_2$, tj. T_1 je podtěleso T_2, pak lze T_2 chápat jako vektorový prostor nad tělesem T_1, ve kterém násobení skalárem z T_1 je totožné s násobením v tělese T_2.[5] Zobecněním vektorových prostorů nad komutativními tělesy jsou tzv. *moduly nad unitárními okruhy*, se kterými se ještě blíže seznámíme v kapitole 1. Máme-li tedy dva unitární okruhy R_1 a R_2 takové, že $R_1 \subseteq R_2$ (tedy R_1 je unitárním podokruhem unitárního okruhu R_2, přitom je zřejmé, že jednotkový prvek v R_1 je tentýž jako v R_2), pak lze zcela analogicky jako u těles R_2 chápat jako modul nad okruhem R_1 (násobení prvku z R_2 skalárem z R_1 je právě násobení v R_2). Protože okruhy obecně nemají komutativní násobení, tak nemusí pro všechny $r_1 \in R_1$ a $r_2 \in R_2$ platit $r_1 r_2 = r_2 r_1$. Z tohoto je zřejmé, že pro nás bude mít význam rozlišovat mezi násobením prvků modulu skalárem z okruhu zleva a zprava. Moduly, ve kterých bude definováno násobení skalárem zleva, resp. zprava, pak budeme nazývat *levými*, resp. *pravými*, moduly. Moduly, které budou současně levými i pravými moduly, budeme nazývat *bimoduly* (vizte definice 1.1, 1.3 a 1.4).

Z těchto úvah plyne, že $\mathcal{C}(\Omega)$ lze chápat (mimo nadokruh[6] $\mathcal{C}^1(\Omega)$) také jako bimodul nad unitárním okruhem $\mathcal{C}^1(\Omega)$. Operátor $\frac{\mathrm{d}}{\mathrm{d}x}$ tedy zobrazuje okruh $\mathcal{C}^1(\Omega)$ do bimodulu $\mathcal{C}(\Omega)$ nad okruhem $\mathcal{C}^1(\Omega)$.[7] V Leibnizově formuli

$$\frac{\mathrm{d}}{\mathrm{d}x}(fg) = \frac{\mathrm{d}f}{\mathrm{d}x}g + f\frac{\mathrm{d}g}{\mathrm{d}x}$$

člen $\frac{\mathrm{d}f}{\mathrm{d}x}g$ tedy chápeme jako skalární násobek prvku $\frac{\mathrm{d}f}{\mathrm{d}x}$ skalárem g zprava a člen $f\frac{\mathrm{d}g}{\mathrm{d}x}$ chápeme jako skalární násobek prvku $\frac{\mathrm{d}g}{\mathrm{d}x}$ skalárem f zleva. V tomto případě násobení skalárem zleva a zprava vyjde nastejno, neboť okruhy $\mathcal{C}^1(\Omega)$ a $\mathcal{C}(\Omega)$ jsou komutativní. Obecně ale na tomto pořadí bude záležet!

Nyní již můžeme přistoupit k onomu zobecnění operátoru $\frac{\mathrm{d}}{\mathrm{d}x}$. *Derivací* budeme v tomto textu rozumět každé zobrazení $D : R \to M$, kde M je bimodul nad okruhem R (budeme též používat obrat „M je R-bimodul“), splňující Leibnizovu formuli

$$\forall r, s \in R : D(rs) = (Dr)s + rDs.^8$$

Další vlastnosti v tomto textu po derivaci požadovat nebudeme, resp. bude-li dané zobrazení splňovat nějakou další vlastnost, vysloveně na to upozorníme (např. derivace, které budou splňovat podmínku aditivity

$$\forall r, s \in R : D(r + s) = Dr + Ds,$$

[3] Má-li funkce $f : \Omega \to \mathbb{R}$ vlastní derivaci v bodě $a \in \Omega$, pak je v a spojitá.

[4] Unitárním podokruhem rozumíme takový podokruh, který obsahuje jednotkový prvek.

[5] Formálně násobení skalárem je právě násobení na T_2 zúžené na množinu $T_1 \times T_2$.

[6] Je-li S podokruhem okruhu R, říkáme též, že R je nadokruhem S.

[7] Uvědomme si, že skaláry, nad kterými je bimodul $\mathcal{C}(\Omega)$ uvažován, jsou funkce z $\mathcal{C}^1(\Omega)$!

[8] Protože při aplikaci operátoru A na funkci f je zvykem vynechávat závorku, tj. místo $A(f)$ se užívá zkráceného zápisu Af, budeme stejnou konvenci používat i pro derivace.

budeme nazývat aditivní derivace).

V této práci bude naším cílem ukázat, že

- některé známé vlastnosti derivací funkcí lze chápat jako důsledky pravidla o derivaci součinu,
- pokusíme se nalézt další příklady těchto zobecněných derivací,
- budeme se zabývat vlastnostmi derivací, které budou definovány na těch algebraických strukturách, na které budeme klást i další dodatečné předpoklady (mimo požadavků na strukturu okruhu a bimodulu),
- a budeme zkoumat algebraické struktury, které tyto derivace samy tvoří.

Kapitola 1

Moduly nad okruhy

V první kapitole připomeneme definice levého a pravého modulu a bimodulu nad okruhy a uvedeme si jejich základní vlastnosti, které budeme v tomto textu využívat. Jak už bylo zmíněno v úvodu, moduly jsou pouhým zobecněním vektorových prostorů, a proto v nich lze zavést zcela analogické pojmy tak, jak je známe z teorie vektorových prostorů. Definice pojmů báze, řád, homomorfismus modulů atd. stejně tak jako jejich vlastnosti uvedeme v dodatku této práce (strana 81), aby zbytečně neodváděly naši pozornost od hlavní problematiky, kterou se v tomto textu budeme zabývat. Využijeme-li v našich úvahách nějaký pojem z teorie modulů či jistou vlastnost modulů z dodatku, odkážeme na definici či větu, která o tomto pojednává.

Nyní již můžeme přistoupit k definici levého modulu nad okruhem.

Definice 1.1 (levého modulu). Ať $(R, +, \cdot)$ je unitární okruh s jednotkovým prvkem[a] 1. Pak *levým R-modulem*, též *levým modulem nad R*, rozumíme komutativní grupu $(M, \oplus)$ spolu s levou akcí $\odot : R \times M \to M$ splňující

(i) $\forall r, s \in R\ \forall m \in M : (rs) \odot m = r \odot (s \odot m)$,

(ii) $\forall r, s \in R\ \forall m \in M : (r + s) \odot m = (r \odot m) \oplus (s \odot m)$,

(iii) $\forall r \in R\ \forall m, n \in M : r \odot (m \oplus n) = (r \odot m) \oplus (r \odot n)$,

(iv) $\forall m \in M : 1 \odot m = m$.

Prvky R budeme nazývat *skaláry*.

[a] Jednotkový prvek budeme taky zkráceně nazývat jednotkou.

Poznámka 1.2. Povšimněme si, že je-li R tělesem, pak definice levého R-modulu splývá s definicí vektorového prostoru nad R.

Párovým pojmem k levému modulu bude pravý modul, kde namísto násobení prvků z M skaláry z R zleva je budeme násobit zprava.

Definice 1.3 (pravého modulu). Ať $(R, +, \cdot)$ je unitární okruh s jednotkou 1. Pak *pravým R-modulem*, též *pravým modulem nad R*, rozumíme komutativní grupu $(M, \oplus)$ spolu s pravou akcí $\odot : M \times R \to M$ splňující

(*i*) $\forall r, s \in R\ \forall m \in M : m \odot (rs) = (m \odot r) \odot s$,

(*ii*) $\forall r, s \in R\ \forall m \in M : m \odot (r + s) = (m \odot r) \oplus (m \odot s)$,

(*iii*) $\forall r \in R\ \forall m, n \in M : (m \oplus n) \odot r = (m \odot r) \oplus (n \odot r)$,

(*iv*) $\forall m \in M : m \odot 1 = m$.

Prvky R budeme nazývat *skaláry*.

Z úvah provedených v úvodu práce je zřejmé, že budeme potřebovat násobit prvky modulu skaláry zleva i zprava, přitom v obecnosti nemusí jít o tytéž prvky, přesněji nemusí platit výrok

$$\forall r \in R\ \forall m \in M : r \odot m = m \odot r. \tag{1.1}$$

Moduly, které budou levými i pravými moduly současně, budeme nazývat bimoduly. Pokud bude splněna podmínka 1.1, budeme mluvit o symetrických modulech. Vizte následující definici.

Definice 1.4 (bimodulu). Ať $(R, +_R, \cdot_R)$ a $(S, +_S, \cdot_S)$ jsou unitární okruhy. Pak *R-S-bimodulem*, též *bimodulem nad okruhy R a S*, rozumíme komutativní grupu $(M, \oplus)$, která

- spolu s levou akcí $\odot_R : R \times M \to M$ tvoří levý R-modul,
- spolu s pravou akcí $\odot_S : M \times S \to M$ tvoří pravý S-modul,
- a navíc platí

$$\forall r \in R\ \forall m \in M\ \forall s \in S : (r \odot_R m) \odot_S s = r \odot_R (m \odot_S s). \tag{1.2}$$

Je-li $(M, \oplus)$ spolu s levou akcí $\odot_1 : R \times M \to M$ a pravou akcí $\odot_2 : M \times R \to M$ R-R-bimodulem, pak ho nazýváme pouze *R-bimodulem* nebo *bimodulem nad okruhem R*. Sjednocení akcí $\odot_1$ a $\odot_2$ budeme značit pouze $\odot$. R-bimodul M nazveme *symetrický*, jestliže platí výrok (1.1).

Značení 1.5.

- Jelikož nemůže dojít k záměně operací $\odot$ z definic 1.1, 1.3, 1.4 s běžným násobením v okruhu, budeme pro $r \in R$ a $m \in M$ nadále místo $r \odot m$, resp. $m \odot r$, používat značení $r \cdot m$ nebo rm, resp. $m \cdot r$ nebo mr. Analogicky budeme pro $m, n \in M$ namísto $m \oplus n$ psát $m + n$.
- Vždy budeme operace sčítání a násobení v okruhu značit po řadě $+$ a $\cdot$. Proto se nadále na okruh (a tedy i na obor integrity nebo těleso) budeme odkazovat pouze pomocí jeho nosiče, tj. množiny jeho prvků bez operací. Tj. místo $(R, +, \cdot)$ budeme psát pouze R (tak, jak jsme již činili v úvodu této práce).

- Pro odlišení budeme nulový prvek M značit symbolem o a nulový prvek R budeme značit symbolem 0. Jednotku R budeme vždy značit symbolem 1.

Poznámka 1.6. Na symetrický R-bimodul M lze také pohlížet jako na levý R-modul, ve kterém pro $r \in R$ a $m \in M$ definujeme $mr \coloneqq rm$ (příp. symetricky jako na pravý R-modul, ve kterém analogicky dodefinujeme levou akci pomocí pravé). Všechny pojmy zavedené pro levé moduly i jejich vlastnosti (vizte dodatek) se tedy přirozeně přenesou i do symetrických bimodulů.

Uveďme si lemma popisující základní vlastnosti bimodulů.

Lemma 1.7. *Ať R je unitární okruh, M je R-bimodul, $r \in R$ a $m \in M$. Pak*

(i) $0m = o \quad \& \quad m0 = o,$

(ii) $ro = o \quad \& \quad or = o,$

(iii) $(-r)m = r(-m) = -rm \quad \& \quad m(-r) = (-m)r = -mr.$

Důkaz.

(*i*) Z vlastnosti (*ii*) definice 1.1 dostáváme

$$0m = (0 + 0)m = 0m + 0m,$$

z čehož máme $0m = o$ (stačí k oběma stranám rovnosti přičíst $-0m$). Analogicky se pomocí bodu (*ii*) definice 1.3 dokáže $m0 = o$.

(*ii*) Z vlastnosti (*iii*) definice 1.1 dostáváme

$$ro = r(o + o) = ro + ro,$$

z čehož analogicky předchozímu bodu dostáváme $ro = o$. Opět se $or = o$ dokáže obdobně.

(*iii*) Z bodu (*i*) tohoto lemmatu a z bodu (*ii*) definice 1.1 máme

$$0 = 0m = \Big(r + (-r)\Big)m = rm + (-r)m,$$

z čehož dostáváme $(-r)m = -rm$. Podobně z bodu (*ii*) tohoto lemmatu a z (*iii*) definice 1.1 dostaneme $r(-m) = -rm$. Analogicky se dokáže

$$m(-r) = (-m)r = -mr.$$

■

V úvodu práce jsme uvedli, že na nadokruh unitárního okruhu lze také pohlížet jako na modul nad tímto okruhem. Nyní si tuto skutečnost formálně dokážeme.

Lemma 1.8. *Ať S je unitárním podokruhem unitárního okruhu R. Pak R tvoří nad S bimodul.*

Důkaz. Ověřme, že R je levý S-modul. Zvolme $s_1, s_2 \in S \subseteq R$ a $r_1, r_2 \in R$ libovolně a ověřme platnost 4 axiomů z definice 1.1 levého modulu. Z vlastností sčítání a násobení v R jistě platí

(i) $(s_1 s_2) r_1 = s_1 (s_2 r_1)$,

(ii) $(s_1 + s_1) r_1 = s_1 r_1 + s_2 r_1$,

(iii) $s_1 (r_1 + r_2) = s_1 r_1 + s_1 r_2$,

(iv) $1 r_1 = r_1$,

takže R je opravdu levým S-modulem. Podobně bychom ukázali, že R je i pravým S-modulem.

Nyní jen stačí ověřit podmínku v definici 1.4 bimodulu, tj. že pro každé $s_1, s_2 \in S \subseteq R$ a každé $r \in R$ platí

$$(s_1 r) s_2 = s_1 (r s_2).$$

Tato vlastnost ale plyne z asociativity násobení v R. Tímto jsme ukázali, že R je opravdu bimodulem nad podokruhem S. ■

Poznámka 1.9. Protože R je triviální podokruhem unitárního okruhu R, s ohledem na lemma 1.8 lze na R pohlížet též jako na bimodul sám nad sebou. Akce $\odot$ je totožná s násobením v R.

Zbylé pojmy spojené s moduly nad okruhy, které v této práci budeme používat, zavedeme a také dokážeme jejich základní vlastnosti v dodatku této bakalářské práce na straně 81.

Kapitola 2

Studium derivací

V této kapitole budeme symbolem R vždy rozumět unitární okruh s jednotkou 1 a symbolem M budeme vždy označovat R-bimodul. Budeme-li po M požadovat, aby byl symetrický, upozorníme na to.

2.1. Definice derivace a příklady derivací

Nyní jsme vybaveni vším potřebným, abychom mohli definovat slíbenou zobecněnou derivaci. Vizte následující definici.

Definice 2.1 (derivace, [1, Definition 186]). (R, M)-*derivací* rozumíme každé zobrazení $D : R \to M$ splňující *Leibnizovu formuli*

$$\forall r, s \in R : D(rs) = (Dr)s + rDs.$$

Pro $r \in R$ nazýváme Dr *derivací* r. Platí-li $M = R$, mluvíme pouze o R-*derivaci* nebo o *derivaci na* R. Množinu všech (R, M)-derivací, resp. R-derivací, značíme $\mathfrak{Der}(R, M)$, resp. $\mathfrak{Der}(R)$.

Je-li navíc D aditivní, tj. platí-li

$$\forall r, s \in R : D(r + s) = Dr + Ds,$$

mluvíme o *aditivní derivaci*. Množinu všech aditivních (R, M)-derivací, resp. aditivních R-derivací, značíme $\mathfrak{Der}_+(R, M)$, resp. $\mathfrak{Der}_+(R)$.

Poznámka 2.2. V případě symetrických bimodulů lze Leibnizovu formuli zapsat též ve tvaru

$$D(rs) = sDr + rDs,$$

čehož budeme někdy využívat.

Poznámka 2.3. Bude-li jasné, nad kterými strukturami je daná (R, M)-derivace uvažována, budeme ji nazývat pouze derivací. V celém textu tedy derivacemi budeme rozumět právě zobrazení splňující Leibnizovu formuli. Budeme-li mít na mysli běžnou derivaci funkcí z $\mathcal{C}^1(\Omega)$, kde $\Omega \subseteq \mathbb{R}$ je otevřená, (vizte příklad 2.6), budeme vždy pro tento operátor používat symbol $\frac{\mathrm{d}}{\mathrm{d}x}$.

Ukažme si nyní několik příkladů zobrazení, která jsou derivacemi ve smyslu definice 2.1.

Příklad 2.4. Ať R je unitární okruh a M je R-bimodul. Pak zobrazení

$$\begin{aligned} O_{R,M} : R &\to M, \\ r &\mapsto o, \end{aligned}$$

je aditivní (R, M)-derivací. To je vidět triviálně, neboť pro libovolné $r, s \in R$ máme

$$O_{R,M}(r+s) = o = o + o = O_{R,M}r + O_{R,M}s$$

a

$$O_{R,M}(rs) = o = os + ro = (O_{R,M}r)s + rO_{R,M}s.$$

Toto zobrazení budeme nazývat *triviální* (R, M)*-derivací*. Pro triviální derivaci $R \to R$ budeme namísto $O_{R,R}$ psát jen O_R. Bude-li zřejmé, na kterých strukturách je tato derivace definovaná, budeme dolní index vynechávat. Triviální derivaci tedy někdy budeme značit pouze symbolem O.

Uvědomme si, že role bimodulu M zde spočívá pouze v určení nulového prvku o.

Příklad 2.5. Uvažme komutativní unitární okruh R. Pak zobrazení

$$\cdot' : R[x] \to R[x]^{9}$$

definované předpisem

$$R \ni a \mapsto 0 \qquad \text{a} \qquad \sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=1}^{n} k a_k x^{k-1} \quad (n \in \mathbb{N} \text{ a existuje } i \in \widehat{n},^{10} \text{ že } a_i \neq 0)$$

je aditivní $R[x]$-derivací. Proč? Z algebry je známo, že $R[x]$ je komutativním unitárním okruhem s jednotkou 1, a tedy požadavky na strukturu definičního oboru zobrazení $\cdot'$ jsou splněny.

Dále ověřme aditivitu. Ať tedy $n, m \in \mathbb{N}_0$, $a_0, \ldots, a_n, b_0, \ldots, b_m \in R$ a bez újmy na obecnosti ať $n \leq m$. Pak

$$\begin{aligned} \left(\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{m} b_k x^k\right)' &\overset{\text{(a)}}{=} \left(\sum_{k=0}^{n} (a_k + b_k) x^k + \sum_{k=n+1}^{m} b_k x^k\right)' \\ &\overset{\text{(b)}}{=} \sum_{k=1}^{n} k(a_k + b_k) x^{k-1} + \sum_{k=n+1}^{m} k b_k x^{k-1} \\ &\overset{\text{(a)}}{=} \sum_{k=1}^{n} k a_k x^{k-1} + \sum_{k=1}^{m} k b_k x^{k-1} \overset{\text{(b)}}{=} \left(\sum_{k=0}^{n} a_k x^k\right)' + \left(\sum_{k=0}^{m} a_k x^k\right)', \end{aligned}$$

[9] Je-li R komutativní unitární okruh, pak symbolem $R[x]$ značíme množinu všech polynomů $p(x)$ s neznámou x a s koeficienty v R, tj. výrazy ve tvaru

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k,$$

kde pro $k = 0, \ldots, n$ je $a_k \in R$.

[10] Pro $n \in \mathbb{N}$ symbolem $\widehat{n}$ budeme nadále označovat množinu $\{1, \ldots, n\}$. Po množinu $\widehat{n} \cup \{0\}$ budeme používat symbol $\widehat{n}^0$.

kde (a) plyne z definice sčítání polynomů a (b) plyne z definice zobrazení $\cdot'$.[11]

Leibnizovu formuli ověříme matematickou indukcí podle n, tj. podle stupně prvního z polynomů[12]. Ať $n \in \{-1, 0\}$, tj. $p(x) = a_0$, kde $a_0 \in R$ (včetně případu $a_0 = 0$). Počítejme:

$$\left(a_0 \sum_{l=0}^{m} b_l x^l\right)' = \left(\sum_{l=0}^{m} a_0 b_l x^l\right)' = \sum_{l=1}^{m} l a_0 b_l x^{l-1} = 0 \cdot \sum_{l=0}^{m} b_l x^l + a_0 \sum_{l=1}^{m} l b_l x^{l-1}$$
$$= a_0' \sum_{l=0}^{m} b_l x^l + a_0 \left(\sum_{l=0}^{m} b_l x^l\right)'.$$

Předpokládejme nyní, že Leibnizova formule platí pro $n - 1, n \in \mathbb{N}$, a ukážeme platnost pro n:

$$\left(\left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{l=0}^{m} b_l x^l\right)\right)' = \left(\left(\sum_{k=0}^{n-1} a_k x^k + a_n x^n\right)\left(\sum_{l=0}^{m} b_l x^l\right)\right)'$$
$$\overset{(a)}{=} \left(\left(\sum_{k=0}^{n-1} a_k x^k\right)\left(\sum_{l=0}^{m} b_l x^l\right) + a_n x^n \left(\sum_{l=0}^{m} b_l x^l\right)\right)'$$
$$\overset{(b)}{=} \left(\left(\sum_{k=0}^{n-1} a_k x^k\right)\left(\sum_{l=0}^{m} b_l x^l\right)\right)' + \left(a_n x^n \sum_{l=0}^{m} b_l x^l\right)'$$
$$\overset{(c)}{=} \left(\sum_{k=0}^{n-1} a_k x^k\right)' \left(\sum_{l=0}^{m} b_l x^l\right) + \left(\sum_{k=0}^{n-1} a_k x^k\right)\left(\sum_{l=0}^{m} b_l x^l\right)' + \left(\sum_{l=0}^{m} a_n b_l x^{n+l}\right)'$$
$$\overset{(d)}{=} \left(\sum_{k=1}^{n-1} k a_k x^{k-1}\right)\left(\sum_{l=0}^{m} b_l x^l\right) + \left(\sum_{k=0}^{n-1} a_k x^k\right)\left(\sum_{l=1}^{m} l b_l x^{l-1}\right)$$
$$+ \sum_{l=1}^{m} (n+l) a_n b_l x^{n+l-1}$$
$$= \left(\sum_{k=1}^{n-1} k a_k x^{k-1}\right)\left(\sum_{l=0}^{m} b_l x^l\right) + \left(\sum_{k=0}^{n-1} a_k x^k\right)\left(\sum_{l=1}^{m} l b_l x^{l-1}\right)$$
$$+ n a_n x^{n-1} \sum_{l=1}^{m} b_l x^l + a_n x^n \sum_{l=1}^{m} l b_l x^{l-1}$$
$$= \left(\sum_{k=1}^{n} k a_k x^{k-1}\right)\left(\sum_{l=0}^{m} b_l x^l\right) + \left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{l=1}^{m} l b_l x^{l-1}\right)$$
$$\overset{(d)}{=} \left(\sum_{k=0}^{n} a_k x^k\right)' \left(\sum_{l=0}^{m} b_l x^l\right) + \left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{l=0}^{m} b_l x^l\right)',$$

[11] Pro úplnost uveďme, že je-li $n = m$, pak součty

$$\sum_{k=n+1}^{m} b_k x^k \qquad \text{a} \qquad \sum_{k=n+1}^{m} k b_k x^{k-1}$$

chápeme jako nulové polynomy.

[12] Je-li polynom $p(x)$ ve tvaru

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

kde $a_0, \ldots, a_n \in R, a_n \neq 0$, pak číslo n nazýváme stupněm polynomu $p(x)$ a značíme jej $\deg p(x)$. Stupeň nulového polynomu, tj. polynomu $p(x) = 0$, pokládáme roven -1.

kde (a) plyne z distributivity násobení vůči sčítání, (b) plyne z již dokázané aditivity $\cdot'$, (c) plyne z indukčního předpokladu a (d) plyne z definice $\cdot'$.

Příklad 2.6. Ať $\emptyset \neq \Omega \subseteq \mathbb{R}$ je otevřená množina. Pak zobrazení

$$\frac{\mathrm{d}}{\mathrm{d}x} : \mathcal{C}^1(\Omega) \to \mathcal{C}(\Omega),$$
$$f \mapsto \frac{\mathrm{d}f}{\mathrm{d}x},$$

kde

$$\frac{\mathrm{d}f}{\mathrm{d}x}(x) = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h}, \ x \in \Omega,$$

je aditivní $(\mathcal{C}^1(\Omega), \mathcal{C}(\Omega))$-derivací. (Připomeňme, že pro funkce $f \in \mathcal{C}^1(\Omega)$ tato limita existuje pro každé $x \in \Omega$.) Aditivita a platnost Leibnizovy formule je zřejmá (to již víme z úvodního kurzu matematické analýzy). V úvodu práce jsme si uvědomili, že $\mathcal{C}^1(\Omega)$ a $\mathcal{C}(\Omega)$ jsou komutativními unitárními okruhy s jednotkou $\mathbb{1}_\Omega$ a že $\mathcal{C}^1(\Omega)$ je podokruhem okruhu $\mathcal{C}(\Omega)$. S ohledem na lemma 1.8 a na komutativitu násobení funkcí tak dostáváme, že $\mathcal{C}(\Omega)$ je symetrickým $\mathcal{C}^1(\Omega)$-bimodulem.

Příklad 2.7. Uvažme otevřenou množinu $\emptyset \neq \Omega \subseteq \mathbb{R}^N$, $N \in \mathbb{N}$, $N \geq 2$, a množinu $\mathcal{C}^1(\Omega)$.[13] Ať je dán libovolný vektor $\boldsymbol{\nu} \in \mathbb{R}^N \setminus \{\mathbf{0}\}$.[14] Pak směrová derivace

$$\frac{\partial}{\partial \boldsymbol{\nu}} : \mathcal{C}^1(\Omega) \to \mathcal{C}(\Omega)$$

definovaná tradičním způsobem

$$\frac{\partial f}{\partial \boldsymbol{\nu}}(\mathbf{x}) = \lim_{h\to 0} \frac{f(\mathbf{x} + h\boldsymbol{\nu}) - f(\mathbf{x})}{h}, \ \mathbf{x} \in \Omega,$$

je aditivní $(\mathcal{C}^1(\Omega), \mathcal{C}(\Omega))$-derivací. Uvědomme si, že tato limita pro funkce $\mathcal{C}^1(\Omega)$ existuje pro každé $\mathbf{x} \in \Omega$.[15] Z matematické analýzy víme, že $\frac{\partial}{\partial \boldsymbol{\nu}}$ je aditivní a splňuje Leibnizovu formuli. Podobnými úvahami, jako jsme provedli v úvodu práce a v předešlém příkladě 2.6, lze dojít k tomu, že $\mathcal{C}(\Omega)$ je symetrickým $\mathcal{C}^1(\Omega)$-bimodulem.

Je taky jasné, že všechny parciální derivace jsou aditivními $(\mathcal{C}^1(\Omega), \mathcal{C}(\Omega))$-derivacemi, neboť parciální derivace podle $x_i, i \in \widehat{N}$, není ničím jiným než směrovou derivací ve směru i-tého vektoru kanonické báze $\mathbb{R}^N$, tj. vektoru $\mathbf{e}_i = (\delta_{1i}, \ldots, \delta_{Ni})^{\mathrm{T}}$.[16]

[13] Množinou $\mathcal{C}^1(\Omega)$, kde $\Omega \subseteq \mathbb{R}^N$, rozumíme množinu všech funkcí $f : \Omega \to \mathbb{R}$, které mají spojité všechny parciální derivace prvního řádu na Ω.

[14] Symbolem $\mathbf{0}$ značíme nulový prvek $\mathbb{R}^N$, tj. nulový vektor $\mathbf{0} = (0, \ldots, 0)^{\mathrm{T}}$.

[15] Funkce $f \in \mathcal{C}^1(\Omega)$ má na Ω totální diferenciál, a tedy na Ω existuje ∇f (vizte např. [6, Věta 2.93]). Z matematické analýzy je pro funkce mající totální diferenciál znám vztah pro výpočet směrové derivace právě pomocí gradientu:

$$\frac{\partial f}{\partial \boldsymbol{\nu}} = \nabla f \cdot \boldsymbol{\nu} = \sum_{i=1}^{N} \frac{\partial f}{\partial x_i} \nu_i,$$

kde $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_N)^{\mathrm{T}} \in \mathbb{R}^N \setminus \{\mathbf{0}\}$ (vizte např. [6, Věta 2.96]). Dostáváme tak, že limita uvedená v definici směrové derivace existuje pro všechna $\mathbf{x} \in \Omega$ a je rovna právě $\nabla f(\mathbf{x}) \cdot \boldsymbol{\nu}$.

[16] Symbol δ_{ij} zde značí tzv. *Kroneckerovo delta*, které je definováno takto:

$$\delta_{ij} = \begin{cases} 1 & \text{pro } i = j \\ 0 & \text{pro } i \neq j \end{cases}$$

Příklad 2.8. Ať $\emptyset \neq \Omega \subseteq \mathbb{R}^N, N \in \mathbb{N}$, $N \geq 2$, je otevřená množina. Pak zobrazení $\nabla : \mathcal{C}^1(\Omega) \to \mathcal{C}(\Omega, \mathbb{R}^N)$[17] s předpisem

$$f \mapsto \nabla f = \begin{pmatrix} \frac{\partial f}{\partial x_1} \\ \vdots \\ \frac{\partial f}{\partial x_N} \end{pmatrix}$$

je aditivní $(\mathcal{C}^1(\Omega), \mathcal{C}(\Omega, \mathbb{R}^N))$-derivací. Nejdříve ověříme, že $\mathcal{C}(\Omega, \mathbb{R}^N)$ je bimodulem nad okruhem $\mathcal{C}^1(\Omega)$. Nyní již ale nelze použít stejný argument jako v příkladech 2.6 a 2.7, neboť $\mathcal{C}(\Omega, \mathbb{R}^N)$ netvoří okruh (vektorové funkce neumíme násobit). Je ale snadné si uvědomit, že $\mathcal{C}(\Omega, \mathbb{R}^N)$ tvoří spolu se sčítáním vektorových funkcí komutativní grupu. Levou akci definujeme přirozeným způsobem:

$$f \begin{pmatrix} g_1 \\ \vdots \\ g_N \end{pmatrix} \coloneqq \begin{pmatrix} fg_1 \\ \vdots \\ fg_N \end{pmatrix}, \quad f \in \mathcal{C}^1(\Omega), \begin{pmatrix} g_1 \\ \vdots \\ g_N \end{pmatrix} \in \mathcal{C}(\Omega, \mathbb{R}^N).$$

Jistě se jedná o zobrazení $\mathcal{C}^1(\Omega) \times \mathcal{C}(\Omega, \mathbb{R}^N) \to \mathcal{C}(\Omega, \mathbb{R}^N)$ (součiny fg_i na jednotlivých složkách jsou funkce z $\mathcal{C}(\Omega)$). Pravou akci definujeme pomocí levé akce tak, jak je uvedeno v poznámce 1.6. Pak už je jen mechanickou záležitostí ověření platnosti axiomů (i) až (iv) uvedených v definicích 1.1 a 1.3 a podmínky (1.2) uvedené v definici 1.4. Dostáváme tak, že $\mathcal{C}(\Omega, \mathbb{R}^N)$ je opravdu $\mathcal{C}^1(\Omega)$-bimodulem, který je symetrický.

Zřejmě je ∇ aditivní operátor. Stačí už jen ověřit, že je splněna Leibnizova formule. Volme proto funkce $f, g \in \mathcal{C}^1(\Omega)$ libovolně a počítejme:

$$\nabla(fg) = \begin{pmatrix} \frac{\partial}{\partial x_1}(fg) \\ \vdots \\ \frac{\partial}{\partial x_N}(fg) \end{pmatrix} = \begin{pmatrix} \frac{\partial f}{\partial x_1} g + f \frac{\partial g}{\partial x_1} \\ \vdots \\ \frac{\partial f}{\partial x_N} g + f \frac{\partial g}{\partial x_N} \end{pmatrix} = g \begin{pmatrix} \frac{\partial f}{\partial x_1} \\ \vdots \\ \frac{\partial f}{\partial x_N} \end{pmatrix} + f \begin{pmatrix} \frac{\partial g}{\partial x_1} \\ \vdots \\ \frac{\partial g}{\partial x_N} \end{pmatrix} = g \nabla f + f \nabla g.$$

Příklad 2.9 ([1, Exercise 38]). Ať R je libovolný unitární okruh a M je R-bimodul. Zvolme pevné $m \in M$. Pak zobrazení $D_m : R \to M$ definované

$$D_m r = [r, m] = rm - mr, \quad r \in R,$$

je aditivní (R, M)-derivací. Toto zobrazení nazýváme *vnitřní derivací na okruhu R určenou prvkem m*. Množinu všech vnitřních (R, M)-derivací značíme $\mathfrak{ID}\mathfrak{er}(R, M)$. Ukažme, že se jedná o aditivní (R, M)-derivaci. Zvolme $r, s \in R$ libovolně a nejdříve dokažme platnost Leibnizovy formule:

$$\begin{aligned} D_m(rs) &= rsm - mrs = (rms - mrs) + (rsm - rms) \\ &= (rm - mr)s + r(sm - ms) = (D_m r)s + r D_m s. \end{aligned}$$

Nyní ukažme aditivitu:

$$\begin{aligned} D_m(r + s) &= (r + s)m - m(r + s) = rm + sm - mr - ms \\ &= (rm - mr) + (sm - ms) = D_m r + D_m s. \end{aligned}$$

Všimněme si, že je-li M symetrický bimodul, pak pro libovolné $m \in M$ je D_m triviální derivací O.

[17] Symbol $\mathcal{C}(\Omega, \mathbb{R}^N)$ zde značí množinu všech spojitých vektorových funkcí $\mathbf{f} : \Omega \to \mathbb{R}^N$.

Poznámka 2.10. V kapitole 4 se budeme dále zabývat tzv. *aritmetickými derivacemi*, které, jak uvidíme, budou derivacemi ve smyslu definice 2.1, které nebudou aditivní. To ospravedlňuje, proč v definici derivace požadujeme pouze platnost Leibnizovy formule.

2.2. Vlastnosti derivací

V této sekci se zaměříme na vlastnosti (R, M)-derivací. Jinými slovy ukážeme si, které známé vztahy lze chápat jako důsledky Leibnizovy formule (v některých případech budeme po derivaci požadovat i aditivitu). Často se budeme inspirovat vlastnostmi derivace $\frac{\mathrm{d}}{\mathrm{d}x}$ z příkladu 2.6. Např. z matematické analýzy víme, že funkcemi, jejichž derivace je nulová, jsou právě funkce konstantní. To nás inspiruje k zavedení nového pojmu *konstanta okruhu vzhledem k derivaci* v následující definici.

Definice 2.11 (jádra derivace, [1, Definition 187]). Ať D je (R, M)-derivace. Pak *jádrem* D rozumíme množinu

$$\operatorname{Ker} D = \Big\{ r \in R \;\Big|\; Dr = o \Big\}.$$

Prvky $\operatorname{Ker} D$ budeme nazývat *konstanty okruhu* R *vzhledem k derivaci* D.

Poznámka 2.12. Pokud bude z kontextu zřejmé, s jakou derivací pracujeme a na jakém okruhu je tato derivace definovaná, budeme prvky jádra této derivace nazývat pouze konstanty.

Příklad 2.13. Jádrem triviální derivace O z příkladu 2.4 je zřejmě celý okruh, na kterém je derivace O definována.

Příklad 2.14. Ať $\emptyset \neq \Omega \subseteq \mathbb{R}$ je otevřená množina. Jádrem derivace $\frac{\mathrm{d}}{\mathrm{d}x}$ z příkladu 2.6 je množina

$$\operatorname{Ker} \frac{\mathrm{d}}{\mathrm{d}x} = \Big\{ f \in \mathcal{C}^1(\Omega) \;\Big|\; \exists c \in \mathbb{R} \;\; \forall x \in \Omega : f(x) = c \Big\},$$

tedy množina právě všech konstantních funkcí na Ω.

Příklad 2.15. Pro konvexní[18] otevřenou množinu $\emptyset \neq \Omega \subseteq \mathbb{R}^N, N \in \mathbb{N}$, $N \geq 2$, a $\boldsymbol{\nu} \in \mathbb{R}^N \setminus \{\mathbf{0}\}$ je jádrem derivace $\frac{\partial}{\partial \boldsymbol{\nu}}$ z příkladu 2.7 množina funkcí $f \in \mathcal{C}^1(\Omega)$, které jsou konstantní na množinách

$$\Omega_{\mathbf{x}} = \{ \mathbf{y} \in \Omega \mid \exists h \in \mathbb{R} : \mathbf{y} = \mathbf{x} + h\boldsymbol{\nu} \}, \;\; \mathbf{x} \in \Omega,$$

Proč? Ať $f \in \mathcal{C}^1(\Omega)$ je taková funkce. Volme $\mathbf{x} \in \Omega$ libovolně. Pak jistě pro všechna h z nějakého redukovného okolí $\mathcal{R}(0)$ máme $f(\mathbf{x} + h\boldsymbol{\nu}) = f(\mathbf{x})$, a tedy

$$\frac{\partial f}{\partial \boldsymbol{\nu}}(\mathbf{x}) = \lim_{h \to 0} \frac{f(\mathbf{x} + h\boldsymbol{\nu}) - f(\mathbf{x})}{h} = 0.$$

[18] Konvexní množinou v $\mathbb{R}^N$ rozumíme takovou podmnožinu $\Omega \subseteq \mathbb{R}^N$, že s každými dvěma body z Ω se v ní nacházejí také všechny body na úsečce se zvolenými krajními body.

Nyní naopak ať $\frac{\partial f}{\partial \boldsymbol{\nu}} = 0$ na Ω. Zvolme $\mathbf{x} \in \Omega$ libovolně. Dále ať $\mathbf{y} \in \Omega_{\mathbf{x}}$, tj. existuje $h > 0$ takové, že $\mathbf{y} = \mathbf{x} + h\boldsymbol{\nu} \in \Omega$. Protože Ω je konvexní, tak

$$\left\{\mathbf{x} + th\boldsymbol{\nu} \;\middle|\; t \in [0,1]\right\} \subseteq \Omega$$

a z věty o střední hodnotě pro směrovou derivaci (vizte např. [6, Věta 2.77]) existuje $\theta \in (0,1)$, že

$$f(\mathbf{y}) - f(\mathbf{x}) = f(\mathbf{x} + h\boldsymbol{\nu}) - f(\mathbf{x}) = \frac{\partial f}{\partial (h\boldsymbol{\nu})}(\mathbf{x} + \theta h\boldsymbol{\nu}) = h\frac{\partial f}{\partial \boldsymbol{\nu}}(\mathbf{x} + \theta h\boldsymbol{\nu}) = 0$$

Odtud

$$f(\mathbf{y}) = f(\mathbf{x}),$$

tedy f je na $\Omega_{\mathbf{x}}$ konstantní. Protože $\mathbf{x} \in \Omega$ bylo voleno libovolně, jsme tímto hotovi.[19]

Příklad 2.16. Jádrem vnitřní derivace $D_m : R \to M$, kde $m \in M$, z příkladu 2.9 je množina

$$\operatorname{Ker} D_m = \{r \in R \mid rm = mr\}.$$

Následující věta nám říká, které prvky okruhu R jsou konstantami vůči všem (R, M)-derivacím.

Věta 2.17 ([1, Theorem 84]). *Ať $D \in \mathfrak{Der}(R, M)$. Pak $0, 1, -1 \in \operatorname{Ker} D$.*

Důkaz. $0 \in \operatorname{Ker} D$, protože

$$D(0) = D(0 \cdot 0) = D(0)0 + 0D(0) \overset{(*)}{=} o,$$

kde v $(*)$ bylo využito lemmatu 1.7.

Dále

$$D(1) = D(1 \cdot 1) = D(1)1 + 1D(1) = 2D(1).$$

Odtud $D(1) = o$, a tedy $1 \in \operatorname{Ker} D$.

Konečně $-1 \in \operatorname{Ker} D$, protože

$$o = D(0) = D(1 - 1) = D(1)(-1) + 1D(-1) = D(-1).$$

■

Poznámka 2.18. Z věty 2.17 ihned plyne, že pokud je $R \neq \{0\}$, pak žádná (R, M)-derivace není injektivní.

[19] Uvědomme si, že existenci $h > 0$ splňující výše uvedené zaručuje předpoklad o otevřenosti množiny Ω. Protože $f \in \mathcal{C}^1(\Omega)$, tak směrová derivace $\frac{\partial f}{\partial \boldsymbol{\nu}}$ existuje ve všech bodech úsečky

$$\left\{\mathbf{x} + th\boldsymbol{\nu} \;\middle|\; t \in [0,1]\right\}.$$

Předpoklady věty o střední hodnotě pro směrovou derivaci jsou splněny, a výše provedné úvahy jsou tedy korektní.

Přirozeně se nabízí otázka, zda inverze konstant (pokud existují) nejsou náhodou také konstantami. Odpověď přináší následující věta.

Věta 2.19 ([1, Theorem 84]). *Ať $D \in \mathfrak{Der}(R, M)$ a $r \in R^{\times}$.*[a] *Pak platí $r \in \operatorname{Ker} D$, právě když $r^{-1} \in \operatorname{Ker} D$.*

[a] Symbolem $R^{\times}$ značíme množinu všech invertibilních prvků z okruhu R, tj. prvků $r \in R$, ke kterým existuje inverzní prvek $r^{-1} \in R$ vůči násobení.

Důkaz. Zvolme $r \in R^{\times}$ libovolně, tj. existuje r^{-1}. V prvním kroku předpokládejme, že r je konstanta, tj. $Dr = o$. Ukážeme, že i r^{-1} je konstanta. Využitím věty 2.17 máme

$$\begin{aligned} o = r^{-1}o = r^{-1}D(1) = r^{-1}D(rr^{-1}) &= r^{-1}\Big((Dr)r^{-1} + rDr^{-1}\Big) \\ &= r^{-1}rDr^{-1} = Dr^{-1}, \end{aligned}$$

tedy $r^{-1} \in \operatorname{Ker} D$.

Je-li naopak r^{-1} konstanta, pak z předchozího plyne, že i $(r^{-1})^{-1} = r$ je konstanta, čímž je věta dokázána. ∎

Pro derivaci $\frac{\mathrm{d}}{\mathrm{d}x}$ z příkladu 2.6 jistě platí

$$\frac{\mathrm{d}}{\mathrm{d}x}(\alpha f) = \alpha \frac{\mathrm{d}f}{\mathrm{d}x},$$

kde $\alpha \in \mathbb{R}$ a $f \in \mathcal{C}^1(\Omega)$. Tento vztah lze také přeformulovat takto:

$$\frac{\mathrm{d}}{\mathrm{d}x}\Big((\alpha \mathbb{1}_{\Omega})f\Big) = (\alpha \mathbb{1}_{\Omega})\frac{\mathrm{d}f}{\mathrm{d}x}.$$

Tentokrát jsou totiž $\alpha\mathbb{1}_{\Omega}$ i f prvky $\mathcal{C}^1(\Omega)$, přitom $\alpha\mathbb{1}_{\Omega}$ je konstantou okruhu $\mathcal{C}^1(\Omega)$ vzhledem k derivaci $\frac{\mathrm{d}}{\mathrm{d}x}$. Stejnou vlastnost lze z Leibnizovy formule odvodit i pro (R, M)-derivace.

Věta 2.20 ([1, page 242]). *Ať $D \in \mathfrak{Der}(R, M)$, $r \in R$, $s \in \operatorname{Ker} D$. Pak platí*

(i) $D(sr) = sDr$,

(ii) $D(rs) = (Dr)s$.

Důkaz. Zvolme $r \in R$ a $s \in \operatorname{Ker} D$ a ukažme platnost (i):

$$D(sr) \overset{\text{(a)}}{=} (Ds)r + sDr \overset{\text{(b)}}{=} sDr,$$

kde v (a) byla použita Leibnizova formule a v (b) bylo využito toho, že $s \in \operatorname{Ker} D$, a lemmatu 1.7. (ii) se dokáže analogicky. ∎

Poznámka 2.21. Uvědomme si, že pokud je r konstantou okruhu R vzhledem k derivaci D, tak i $-r$ je konstantou. Z věty 2.20 totiž dostáváme

$$D(-r) = D\Big((-1)r\Big) = (-1)Dr = o.$$

S ohledem na větu 2.19 tedy dostáváme, že jádro derivace je uzavřené na opačné prvky a inverze (pokud k dané konstantě inverze existuje).

Povšimněme si, že jsme tímto zároveň určili vztah pro derivování opačných prvků

$$D(-r) = -Dr. \tag{2.1}$$

Z algebry je známo, že je-li $\varphi : R \to S$ homomorfismus okruhů R a S, pak $\operatorname{Ker}\varphi$ je ideálem v R (vizte např. [4, page 89]). Z příkladu 2.13 víme, že jádrem triviální derivace $O_{R,M}$ je celý okruh R, což je triviální ideál v R. Následující věta pojednává o struktuře jader netriviálních aditivních derivací.

Věta 2.22. *Ať D je netriviální aditivní (R, M)-derivace. Pak $\operatorname{Ker} D$ je unitární podokruh R, který není ideálem v R.*

Důkaz. Nejdříve ukažme, že $\operatorname{Ker} D$ je unitární podokruh R. Zřejmě $\operatorname{Ker} D \subseteq R$ a $1 \in \operatorname{Ker} D$ (věta 2.17). Dokážeme, že $\operatorname{Ker} D$ je podgrupa grupy $(R, +)$, tj. že pro libovolné $r, s \in \operatorname{Ker} D$ je $r - s \in \operatorname{Ker} D$. Zvolme proto $r, s \in \operatorname{Ker} D$ libovolně. Pak

$$D(r - s) \overset{\text{(a)}}{=} Dr + D(-s) \overset{\text{(b)}}{=} Dr - Ds = o - o = o,$$

kde v (a) byla využita aditivita D a rovnost (b) plyne z věty 2.20. Nyní ukažme uzavřenost na násobení:

$$D(rs) = (Dr)s + rDs = o + o = o,$$

a proto $rs \in \operatorname{Ker} D$. Celkem je tedy $\operatorname{Ker} D$ unitárním podokruhem R.

Nyní pro spor předpokládejme, že $\operatorname{Ker} D$ je ideál v R. Volme $r \in R$ libovolně. Protože $1 \in \operatorname{Ker} D$, tak $r = 1r \in \operatorname{Ker} D$, tj. $R = \operatorname{Ker} D$. To by ale znamenalo, že $D = O_{R,M}$, což je spor s tím, že D je netriviální derivace. ■

Poznámka 2.23. Vidíme, že pokud D není aditivní derivací, $\operatorname{Ker} D$ nemusí být podokruhem R. Příkladem může být jádro aritmetické $\mathbb{Z}$-derivace (vizte poznámku 4.5).

Leibnizova formule nám říká, jak vypadá derivace součinu dvou prvků z okruhu. Patrně ale půjde odvodit vztah pro derivaci součinu libovolného konečného počtu prvků z R. Právě ten nám představí následující věta.

Věta 2.24. *Ať $D \in \mathfrak{Der}(R, M)$. Pak pro každé $r_1, \ldots, r_k \in R$ platí*

$$D\left(\prod_{i=1}^{k} r_i\right) = \sum_{i=1}^{k} r_1 \cdots r_{i-1}(Dr_i)r_{i+1} \cdots r_k.$$

Důkaz. Budeme postupovat matematickou indukcí. Pro $k = 1$ je platnost triviální a pro $k = 2$ dostáváme Leibnizovu formuli. Předpokládejme, že věta platí pro $k \geq 2$. Ukážeme, že platí i pro $k + 1$:

$$D\left(\prod_{i=1}^{k+1} r_i\right) = D\left(\left(\prod_{i=1}^{k} r_i\right) r_{k+1}\right) \overset{\text{(a)}}{=} D\left(\prod_{i=1}^{k} r_i\right) r_{k+1} + \left(\prod_{i=1}^{k} r_i\right) Dr_{k+1}$$
$$\overset{\text{(b)}}{=} \left(\sum_{i=1}^{k} r_1 \cdots r_{i-1}(Dr_i)r_{i+1}\cdots r_k\right) r_{k+1} + r_1 \cdots r_k Dr_{k+1}$$
$$= \sum_{i=1}^{k+1} r_1 \cdots r_{i-1}(Dr_i)r_{i+1}\cdots r_{k+1},$$

kde v kroku (a) byla použita Leibnizova formule a v kroku (b) byl použit indukční předpoklad. ■

Další vlastnost plynoucí z Leibnizovy formule je n-tá derivace součinu rs pro $r, s \in R$. Pokud ale budeme chtít počítat násobné derivace, budeme se muset omezit pouze na R-derivace. Navíc budeme požadovat aditivitu D. Vizte následující větu.

Věta 2.25. *Ať $D \in \mathfrak{Der}_+(R)$ a $r, s \in R$. Pak pro každé $n \in \mathbb{N}_0$ platí*

$$D^n(rs) = \sum_{k=0}^{n} \binom{n}{k} D^{n-k} r D^k s.^a$$

[a] Symbolem D^n rozumíme

$$D^n = \begin{cases} \mathrm{id}_R, & n = 0 \\ D \circ D^{n-1}, & n \in \mathbb{N} \end{cases}$$

Důkaz. V prvé řadě má levá strana rovnosti smysl, neboť D je zobrazení z R do R. Postupujme matematickou indukcí. Pro $n = 0$ tvrzení platí triviálně a pro $n = 1$ máme Leibnizovu formuli. Předpokládejme, že věta platí pro $n \geq 1$. Ukážeme, že platí i pro $n + 1$:

$$D^{n+1}(rs) = D\big(D^n(rs)\big) \overset{\text{(a)}}{=} D\left(\sum_{k=0}^{n} \binom{n}{k} D^{n-k} r D^k s\right) \overset{\text{(b)}}{=} \sum_{k=0}^{n} \binom{n}{k} D\big(D^{n-k} r D^k s\big)$$
$$\overset{\text{(c)}}{=} \sum_{k=0}^{n} \binom{n}{k} \big(D^{n-k+1} r D^k s + D^{n-k} r D^{k+1} s\big)$$
$$= \sum_{k=0}^{n} \binom{n}{k} \big(D^{n+1-k} r D^k s\big) + \sum_{k=0}^{n} \binom{n}{k} \big(D^{n-k} r D^{k+1} s\big)$$
$$= (D^{n+1}r)s + \sum_{k=1}^{n} \binom{n}{k} \big(D^{n+1-k} r D^k s\big) + \sum_{k=1}^{n} \binom{n}{k-1} \big(D^{n+1-k} r D^k s\big) + r D^{n+1} s$$
$$= (D^{n+1}r)s + \sum_{k=1}^{n} \binom{n+1}{k} \big(D^{n+1-k} r D^k s\big) + r D^{n+1} s$$
$$= \sum_{k=0}^{n+1} \binom{n+1}{k} D^{n+1-k} r D^k s,$$

kde v (a) bylo využito indukčního předpokladu, v (b) aditivity D a v (c) Leibnizovy formule. ■

Známým vztahem z matematické analýzy je derivace podílu dvou funkcí:

$$\frac{\mathrm{d}}{\mathrm{d}x}\frac{f}{g} = \frac{1}{g^2}\left(\frac{\mathrm{d}f}{\mathrm{d}x}g - f\frac{\mathrm{d}g}{\mathrm{d}x}\right), \quad f, g \in \mathcal{C}^1(\Omega),\ g \neq 0 \text{ na } \Omega.$$

Jeho analogii pro (R, M)-derivace nám představí následující věta.

Věta 2.26 (o derivaci podílu, [1, Theorem 86]). *Ať $D \in \mathfrak{Der}(R, M)$, $r \in R$ a $s \in R^\times$. Pak*

$$D(rs^{-1}) = \Big(D(r)s - rs^{-1}(Ds)s\Big)s^{-2}.$$

Pokud navíc $sDs = (Ds)s$,[a] platí

$$D(rs^{-1}) = \Big((Dr)s - r(Ds)\Big)s^{-2}.$$

[a]Budeme říkat, že s a Ds komutují.

Důkaz. Zvolme $r \in R$ a $s \in R^\times$ libovolně. Nejdříve s využitím Leibnizovy formule a věty 2.17 dostáváme

$$o = D(1) = D(ss^{-1}) = (Ds)s^{-1} + sDs^{-1},$$

z čehož využitím (iii) lemmatu 1.7 dostáváme $D(s^{-1}) = -s^{-1}(Ds)s^{-1}$. Dále

$$\begin{aligned} D(rs^{-1}) &= (Dr)s^{-1} + rDs^{-1} = (Dr)s^{-1} - rs^{-1}(Ds)s^{-1} \\ &= (Dr)ss^{-2} - rs^{-1}(Ds)ss^{-2} = \Big((Dr)s - rs^{-1}(Ds)s\Big)s^{-2}. \end{aligned}$$

Pokud s a Ds komutují, pak

$$\Big((Dr)s - rs^{-1}(Ds)s\Big)s^{-2} = \Big((Dr)s - rs^{-1}sDs\Big)s^{-2} = \Big((Dr)s - rDs\Big)s^{-2}.$$

■

Poznámka 2.27. V důkazu věty 2.26 jsme také odvodili vztah pro derivaci s^{-1} (pokud $s \in R^\times$):

$$Ds^{-1} = -s^{-1}(Ds)s^{-1}.$$

Pokud navíc s a Ds komutují, vztah se zjednoduší na

$$Ds^{-1} = -s^{-2}Ds.$$[20]

Následující věta nám představí variantu řetízkového pravidla pro aditivní (R, M)-derivace.

Věta 2.28 (polynomiální řetízkové pravidlo, [1, Theorem 87]). *Ať $D \in \mathfrak{Der}_+(R, M)$, $r \in R$ a $p(x) \in (\operatorname{Ker} D)[x]$. Pokud r a Dr komutují, pak platí*

$$Dp(r) = p'(r)Dr,$$

kde $p'(r)$ značí prvek okruhu R, který vznikne dosazením r do derivace $p'(x)$ polynomu $p(x)$ definované v příkladu 2.5.

[20]Srovnejte tento vztah s derivací složené funkce $\frac{1}{f}$ pro $f \in \mathcal{C}^1(\Omega)$, $f \neq 0$ na Ω.

Důkaz. Označme $p(x) = \sum_{k=0}^{n} a_k x^k$. Z aditivity D a z toho, že $p(x) \in (\operatorname{Ker} D)[x]$, tj. pro všechna $k \in \widehat{n}^0$ platí $a_k \in \operatorname{Ker} D$, dostáváme $Dp(r) = \sum_{k=0}^{n} a_k Dr^k$. Je proto zřejmé, že stačí ukázat platnost vztahu

$$Dr^n = nr^{n-1}Dr$$

pro libovolné $n \in \mathbb{N}$ (platí totiž $(r^n)' = nr^{n-1}$). Budeme postupovat matematickou indukcí. Pro $n = 1$ vztah zřejmě platí. Předpokládejme nyní, že vztah platí pro nějaké $n \in \mathbb{N}$. Ukážeme platnost pro $n + 1$:

$$\begin{aligned} Dr^{n+1} = D(r^n r) = (Dr^n)r + r^n Dr &\overset{\text{(a)}}{=} nr^{n-1}(Dr)r + r^n Dr \\ &\overset{\text{(b)}}{=} nr^{n-1}rDr + r^n Dr = nr^n Dr + r^n Dr = (n+1)r^n Dr, \end{aligned}$$

přitom v (a) jsme využili indukčního předpokladu a v (b) jsme využili skutečnosti, že r a Dr komutují. ■

V důkazu předešlé věty jsme odvodili, že pro $n \in \mathbb{N}$ a $r \in R$ takové, že r a Dr komutují, platí

$$Dr^n = nr^{n-1}Dr.$$

Uvědomme si, že tento vztah platí i pro derivace, které nejsou aditivní (v důkazu jeho platnosti se totiž nijak nevyužila aditivita D). Dokonce lze dokázat jeho platnosti i pro libovolnou celočíselnou mocninu prvku r. Vizte následující větu.

Věta 2.29 ([1, Corollary 41]). *Ať $D \in \mathfrak{Der}(R, M)$ a $r \in R^\times$. Pokud r a Dr komutují, pak pro libovolné $n \in \mathbb{Z}$ platí*

$$Dr^n = nr^{n-1}Dr.$$

Důkaz. Patnost pro $n \in \mathbb{N}$ je vidět z důkazu věty 2.28. Pro $n = 0$ máme

$$Dr^0 = D(1) = o = 0r^{-1}Dr,$$

protože $1 \in \operatorname{Ker} D$ (věta 2.17). Zbývá nám ukázat platnost pro $n < 0$. Z poznámky 2.27 plyne $Dr^{-1} = -r^{-2}Dr$. Odtud

$$\begin{aligned} Dr^n &= D(r^{-1})^{-n} = -n(r^{-1})^{-n-1}Dr^{-1} = \left(-n(r^{-1})^{-n-1}\right)(-r^{-2}Dr) \\ &= nr^{n+1-2}Dr = nr^{n-1}Dr. \end{aligned}$$

■

Kapitola 3

Podílové rozšíření derivace

V této kapitole bude naším cílem z derivace $D : R \to M$ definované na oboru integrity[21] R zkonstruovat derivaci $D^* : Q(R) \to Q(M)$ definovanou na podílovém tělese $Q(R)$ oboru integrity R takovou, že $D^*|_R = D$.[22] Množina $Q(M)$ pak bude vektorový prostor nad podílovým tělesem $Q(R)$ takový, že $M \subseteq Q(M)$. Této konstrukce využijeme např. při rozšiřování aritmetické derivace definované na oboru integrity $\mathbb{Z}$ na aritmetickou derivaci definovanou na $\mathbb{Q} = Q(\mathbb{Z})$ (více v kapitole 4).

V této kapitole budeme symbolem R rozumět obor integrity a symbolem M budeme značit symetrický R-bimodul.

3.1. Konstrukce podílového tělesa oboru integrity

Nejdříve připomeňme konstrukci podílového tělesa oboru integrity[23] R (nebudeme procházet všechny detaily, neboť tato konstrukce je dobře známá ze základního kurzu algebry; vizte např. [5, Section 5.7]). Uvažme množinu $R \times (R \setminus \{0\})$, na které definujeme relaci $\sim$ takto:

$$(r, s) \sim (u, v) \qquad \overset{\text{def}}{\iff} \qquad rv = su,$$

kde $r, s, u, v \in R, s, v \neq 0$. Ukáže se, že $\sim$ je relace ekvivalence na $R \times (R \setminus \{0\})$ (k důkazu je potřeba komutativita násobení a skutečnost, že v R nejsou netriviální dělitelé nuly, což je zajištěno tím, že R je obor integrity). Lze tedy definovat

[21] Oborem integrity rozumíme takový komutativní unitární okruh R, ve kterém neexistují netriviální dělitelé nuly, tj. prvky $r \in R \setminus \{0\}$ takové, že

$$\exists s \in R \setminus \{0\} : rs = 0.$$

[22] Obor integrity R tedy chápeme jako podmnožinu $Q(R)$ (vizte dále).

[23] Tuto konstrukci lze obecně provést nad libovolným komutativním okruhem R, ve kterém nejsou netriviální dělitelé nuly, tj. R nemusí obsahovat jednotku. Protože ale derivaci definujeme na unitárním okruhu, pak se opravdu v této práci stačí zabývat konstrukcí podílového tělesa oboru integrity. Navíc díky tomu, že jsme v R vybaveni jednotkou 1, využijeme zjednodušeného zápisu některých tříd v $Q(R)$. Např. namísto třídy $[(rs, s)]_\sim$, kde $r, s \in R, s \neq 0$, lze psát $[(r, 1)]_\sim$.

faktorovou množinu[24]

$$Q(R) := R \times \Big(R \setminus \{0\}\Big)\Big/\!\sim$$

a na ní operace sčítání a násobení následovně:

$$[(r,s)]_\sim + [(u,v)]_\sim = [(rv+su, sv)]_\sim \qquad \text{a} \qquad [(r,s)]_\sim [(u,v)]_\sim = [(ru, sv)]_\sim.^{25}$$

Tyto operace jsou definovány korektně, tj. že nezáleží na volbě reprezentantů tříd. Nyní si stačí uvědomit, že

- nulovým prvkem $Q(R)$ je třída $[(0,1)]_\sim$,
- jednotkovým prvkem $Q(R)$ je třída $[(1,1)]_\sim$,
- opačným prvkem k třídě $[(r,s)]_\sim \in Q(R)$ je třída $[(-r,s)]_\sim$,
- inverzním prvkem k třídě $[(r,s)]_\sim \in Q(R)$, kde $r \neq 0$, je třída $[(s,r)]_\sim$,
- komutativita a asociativita sčítání a násobení na $Q(R)$ plyne z odpovídajících vlastností sčítání a násobení v oboru integrity R a
- distributivita násobení vzhledem ke sčítání lze také dokázat.

Celkem je tedy $Q(R)$ komutativním tělesem.

Nyní ukážeme, že existuje vnoření $\nu : R \hookrightarrow Q(R)$[26] oboru integrity R do komutativního tělesa $Q(R)$. Definujme ν předpisem

$$\nu(r) = [(r,1)]_\sim, \quad r \in R.$$

Ukážeme, že se opravdu jedná o vnoření.

(i) Dokažme injektivitu ν. Ať tedy $r, s \in R$ jsou takové, že $\nu(r) = \nu(s)$, tj. $[(r,1)]_\sim = [(s,1)]_\sim$. Odtud $(r,1) \sim (s,1)$, a to podle definice relace $\sim$ znamená $r1 = 1s$, tj. $r = s$.

---

[24]Faktorovou množinou na množině R podle relace ekvivalence $\sim$ definované na R rozumíme množinu všech tříd ekvivalence prvků z R podle relace $\sim$ a značíme ji symbolem $R/\sim$. Třídou prvku $r \in R$ podle relace $\sim$ rozumíme množinu

$$[r]_\sim = \{s \in R \mid r \sim s\}.$$

Takže

$$R/\sim = \big\{[r]_\sim \;\big|\; r \in R\big\}.$$

[25]Definice těchto operací jsou inspirovány sčítáním a násobením zlomků z $\mathbb{Q}$. Představíme-li si totiž třídy $[(r,s)]_\sim$ a $[(u,v)]_\sim$ po řadě jako zlomky $\frac{r}{s}$ a $\frac{u}{v}$, pak

$$\frac{r}{s} + \frac{u}{v} = \frac{rv+su}{sv} \qquad \text{a} \qquad \frac{r}{s} \cdot \frac{u}{v} = \frac{ru}{sv}.$$

[26]Vnořením okruhů rozumíme libovolný injektivní homomorfismus okruhů. Je-li f injektivní zobrazení z A do B, budeme tuto skutečnost zapisovat $f : A \hookrightarrow B$.

(ii) Ukažme, že ν je homomorfismus R do $Q(R)$. Jistě $\nu(1) = [(1,1)]_\sim$ je jednotkou $Q(R)$. Dále ukažme, že ν zachovává součet. Zvolme proto $r, s \in R$ libovolně a počítejme

$$\nu(r+s) = [(r+s,1)]_\sim = [(r,1)]_\sim + [(s,1)]_\sim = \nu(r) + \nu(s).$$

Nakonec ukažme, že ν zachovává i násobení:

$$\nu(rs) = [(rs,1)]_\sim = [(r,1)]_\sim[(s,1)]_\sim = \nu(r)\nu(s).$$

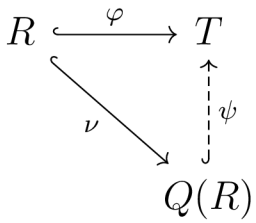
V dalším kroku zrotožníme prvek $r \in R$ a třídu $\nu(r) = [(r,1)]_\sim$ a přeznačíme třídy $[(r,s)]_\sim \in Q(R)$ na „zlomky“ $\frac{r}{s}$. Po tomto ztotožení tedy lze psát $R \subseteq Q(R)$.

Shrňme získaný výsledek do věty.

Věta 3.1. *Každý obor integrity lze vnořit do komutativního tělesa.*

Definice 3.2. Ať R je obor integrity. Pak komutativní těleso $Q(R)$ definované výše nazýváme *podílové těleso oboru integrity* R. Vnoření $\nu : r \mapsto \frac{r}{1} = [(r,1)]_\sim$ nazýváme *kanonické vnoření* R *do* $Q(R)$.

Poznámka 3.3. Podílové těleso $Q(R)$ oboru integrity R je nejmenším komutativním tělesem, do kterého lze R vnořit. Přesněji: Existuje-li vnoření $\varphi : R \hookrightarrow T$, kde T je komutativní těleso, pak existuje vnoření $\psi : Q(R) \hookrightarrow T$ takové, že $\psi \circ \nu = \varphi$, neboli následující diagram komutuje:



Odtud taky plyne, že je-li R komutativním tělesem, pak $Q(R) \cong R$.

3.2. Konstrukce podílového vektorového prostoru symetrického bimodulu

Nyní se pokusme rozšířit R-bimodul M na vektorový prostor $Q(M)$ nad tělesem $Q(R)$ takový, že M půjde do $Q(M)$ vnořit. V tomto odstavci budeme pracovat se symetrickým R-bimodulem M, tj. s bimodulem, ve kterém je $rm = mr$ pro každé $r \in R$ a $m \in M$. Ve struktuře $Q(M)$ pak budeme mít formálně definovány dvě akce – levou i pravou. Ty ale budou dávat odpovídajícím si dvojicím stejné výsledky, přesněji $tv = vt$ pro $t \in Q(R)$ a $v \in Q(M)$. Na $Q(M)$ tedy opravdu budeme moct pohlížet jako na vektorový prostor nad komutativním tělesem, ve kterém je obecně formálně definovaná jen levá akce. Při jeho konstrukci se budeme inspirovat postupem konstrukce podílového tělesa $Q(R)$. Protože tato konstrukce ale není tak známá, jako konstrukce podílového tělesa oboru integrity, budeme v tomto odstavci postupovat poněkud precizněji.

Protože chceme zkonstruovat vektorový prostor, jistě musí platit následující: je-li $m \in M$, pak $tm \in Q(M)$ pro každé $t \in Q(R)$ (budeme chtít, aby $M \subseteq Q(M)$). Protože $Q(R)$ je podílové těleso R, tak t lze psát ve tvaru $\frac{r}{s}$, kde $r, s \in R$, $s \neq 0$. $Q(M)$ tedy musí obsahovat prvky ve tvaru $\frac{r}{s}m$. Přirozeně budeme chtít, aby

$$\frac{r}{s}m = \frac{rm}{s}.^{27}$$

Toto jsou prvky, které budeme k prvkům z M chtít „přidat“ (a budeme doufat, že to postačí). Protože $rm \in M$, stačí se dokonce omezit jen prvky ve tvaru $\frac{m}{r}$, kde $m \in M$ a $r \in R \setminus \{0\}$. Vezměme tedy množinu $M \times (R \setminus \{0\})$ a na ní definujme relaci $\sim_M$ takto:

$$(m, r) \sim_M (n, s) \qquad \overset{\text{def}}{\iff} \qquad sm = rn.$$

Ukažme, že se jedná o relaci ekvivalence. Volme $m, n, p \in M$ a $r, s, t \in R \setminus \{0\}$ libovolně.

(i) $\sim_M$ je reflexivní, neboť $(m, r) \sim_M (m, r)$, právě když $rm = rm$, a to jistě platí.

(ii) $\sim_M$ je taky relace symetrická. To plyne přímo z definice a ze symetrice relace „být rovno“, tj. relace $=$.

(iii) Ať $(m, r) \sim_M (n, s)$ a $(n, s) \sim_M (p, t)$, tj. $sm = rn$ a $tn = sp$. Odtud pak $stm = rtn = rsp$, z čehož máme $tm = rp$, tj. $(m, r) \sim_M (p, t)$. Relace $\sim_M$ je proto tranzitivní.

Dokázali jsme, že $\sim_M$ je relací ekvivalence na $M \times (R \setminus \{0\})$, a lze tedy faktorizovat. Označme

$$Q(M) \coloneqq M \times (R \setminus \{0\}) / \sim_M . \tag{3.1}$$

Definujme sčítání na $Q(M)$:

$$[(m, r)]_{\sim_M} + [(n, s)]_{\sim_M} \coloneqq [(sm + rn, rs)]_{\sim_M} \tag{3.2}$$

a násobení tříd z $Q(M)$ skalárem z $Q(R)$:

$$\frac{u}{v}[(m, r)]_{\sim_M} \coloneqq [(um, vr)]_{\sim_M}, \tag{3.3}$$

$r, s, u, v \in R, r, s, v \neq 0, m, n \in M$. Uvědomíme-li si, že třída $[(m, r)]_{\sim_M}$ představuje zlomek „$\frac{m}{r}$“, přesněji prvek „$\frac{1}{r} \cdot m$“, pak je jasné, proč tyto operace zavádíme právě tímto způsobem. Ukažme, že tyto definice jsou korektní, tj. že nezáleží na volbě reprezentantů tříd. Ať tedy $(m, r) \sim_M (m', r')$, $(n, s) \sim_M (n', s')$, $\frac{u}{v} = \frac{u'}{v'}$, tj. $r'm = rm'$, $s'n = sn'$ a $u'v = uv'$.

(i) Ověřme korektnost sčítání. Platí

$$[(m', r')]_{\sim_M} + [(n', s')]_{\sim_M} = [(s'm' + r'n', r's')]_{\sim_M}.$$

[27] Tento zápis chápeme zatím jako symbolický. Takové operace totiž definované ještě nemáme.

Chceme ukázat, že $(s'm' + r'n', r's') \sim_M (sm + rn, rs)$, tj. $rs(s'm' + r'n') = r's'(sm + rn)$. Roznásobením dostaneme

$$rss'm' + rr'sn' = r'ss'm + rr's'n.$$

Tato rovnost ale plyne ze skutečnosti, že $r'm = rm'$ a $s'n = sn'$. Tím je korektnost sčítání dokázána.

(ii) Nyní se zabývejme ověřením koreknosti levé akce. Platí

$$\frac{u'}{v'}[(m', r')]_{\sim_M} = [(u'm', v'r')]_{\sim_M}.$$

Analogicky bodu (i) lze ze skutečnosti $r'm = rm'$ a $u'v = uv'$ ukázat, že $(u'm', v'r') \sim_M (um, vr)$.

Nyní bude naším cílem dokázat, že $Q(M)$ spolu se sčítáním tříd a násobením tříd skalárem z $Q(R)$ tvoří vektorový prostor nad komutativním tělesem $Q(R)$. Pro větší přehlednost nejdříve dokažme pomocné lemma.

Lemma 3.4. *Ať $Q(R)$ je podílové těleso oboru integrity R, M je symetrický R-bimodul a $Q(M)$ je definováno v* (3.1)*. Pak $Q(M)$ tvoří spolu se sčítáním tříd definovaným v* (3.2) *komutativní grupu s nulovým prvkem $[(o, 1)]_{\sim_M}$. Opačným prvkem k třídě $[(m, r)]_{\sim_M} \in Q(M)$ je třída $[(-m, r)]_{\sim_M}$.*

Důkaz. Jistě je + operací na $Q(M)$, takže $(Q(M), +)$ je grupoid. Komutativita a asociativita sčítání v $Q(M)$ plyne z komutativity a asociativity sčítání v M a násobení v R. Opravdu pro $m, n, p \in M$ a $r, s, t \in R \setminus \{0\}$ platí

$$\begin{aligned}[(m, r)]_{\sim_M} + [(n, s)]_{\sim_M} &= [(sm + rn, rs)]_{\sim_M} = [(rn + sm, sr)]_{\sim_M} \\ &= [(n, s)]_{\sim_M} + [(m, r)]_{\sim_M}\end{aligned}$$

a

$$\begin{aligned}\Big([(m, r)]_{\sim_M} + [(n, s)]_{\sim_M}\Big) + [(p, t)]_{\sim_M} &= [(sm + rn, rs)]_{\sim_M} + [(p, t)]_{\sim_M} \\ &= \Big[\Big(t(sm + rn) + rsp, (rs)t\Big)\Big]_{\sim_M} = [(tsm + rtn + rsp, rst)]_{\sim_M} \\ &= \Big[\Big(stm + r(tn + sp), r(st)\Big)\Big]_{\sim_M} = [(m, r)]_{\sim_M} + [(tn + sp, st)]_{\sim_M} \\ &= [(m, r)]_{\sim_M} + \Big([(n, s)]_{\sim_M} + [(p, t)]_{\sim_M}\Big).\end{aligned}$$

Ukažme, že $[(o, 1)]_{\sim_M}$ je nulový prvek $(Q(M), +)$:

$$[(m, r)]_{\sim_M} + [(o, 1)]_{\sim_M} = [(1m + ro, 1r)]_{\sim_M} = [(m, r)]_{\sim_M},$$

což spolu s komutativitou dává požadovaný výsledek.

Konečně dokažme, že k třídě $[(m, r)]_{\sim_M}$ je opačným prvkem třída $[(-m, r)]_{\sim_M}$ (s ohledem na komutativitu operace + stačí opět počítat součet pouze „v jednom pořadí“):

$$[(m,r)]_{\sim_M} + [(-m,r)]_{\sim_M} = \Big[\Big(rm + (-rm), r^2\Big)\Big]_{\sim_M} = [(o,r^2)]_{\sim_M} = [(o,1)]_{\sim_M},$$

protože $1o = r^2 o$, a tedy $(o, r^2) \sim_M (o, 1)$. Tím je lemma dokázáno. ■

Nyní můžeme přejít k důkazu skutečnosti, že $Q(M)$ s výše uvedenými operacemi opravdu tvoří vektorový prostor nad tělesem $Q(R)$ (vizte následující větu).

Věta 3.5. *Ať $Q(R)$ je podílové těleso oboru integrity R, M je symetrický R-bimodul a $Q(M)$ je definováno v* (3.1)*. Pak $Q(M)$ tvoří spolu se sčítáním tříd definovaný v* (3.2) *a násobením tříd skalárem z $Q(R)$ definovaným v* (3.3) *vektorový prostor nad tělesem $Q(R)$. Zobrazení*

$$\begin{aligned} \nu : M &\to Q(M), \\ m &\mapsto [(m,1)]_{\sim_M} \end{aligned}$$

je vnoření bimodulu M do vektorového prostoru $Q(M)$.

Důkaz. Z lemmatu 3.4 již víme, že $(Q(M), +)$ je grupa. Stačí ukázat platnost čtyř axiomů vektorového prostoru (vizte body (i) až (iv) níže). Volme třídy $[(m,r)]_{\sim_M}$, $[(n,s)]_{\sim_M} \in Q(M)$ a zlomky $\frac{u}{v}$, $\frac{x}{y} \in Q(R)$ libovolně a počítejme:

(i)

$$\begin{aligned} \left(\frac{u}{v} + \frac{x}{y}\right)[(m,r)]_{\sim_M} &= \frac{uy + vx}{vy}[(m,r)]_{\sim_M} = [(uym + vxm, vyr)]_{\sim_M} \\ &= [(um, vr)]_{\sim_M} + [(xm, yr)]_{\sim_M} \\ &= \frac{u}{v}[(m,r)]_{\sim_M} + \frac{x}{y}[(m,r)]_{\sim_M}, \end{aligned}$$

(ii)

$$\begin{aligned} \frac{u}{v}\Big([(m,r)]_{\sim_M} + [(n,s)]_{\sim_M}\Big) &= \frac{u}{v}[(sm + rn, rs)]_{\sim_M} = [(usm + urn, vrs)]_{\sim_M} \\ &= [(um, vr)]_{\sim_M} + [(un, vs)]_{\sim_M} \\ &= \frac{u}{v}[(m,r)]_{\sim_M} + \frac{u}{v}[(n,s)]_{\sim_M}, \end{aligned}$$

(iii)

$$\begin{aligned} \left(\frac{u}{v}\frac{x}{y}\right)[(m,r)]_{\sim_M} &= \frac{ux}{vy}[(m,r)]_{\sim_M} = [(uxm, vyr)]_{\sim_M} = \frac{u}{v}[(xm, yr)]_{\sim_M} \\ &= \frac{u}{v}\left(\frac{x}{y}[(m,r)]_{\sim_M}\right) \end{aligned}$$

(iv)

$$1 \cdot [(m,r)]_{\sim_M} = \frac{1}{1} \cdot [(m,r)]_{\sim_M} = [(m,r)]_{\sim_M}.$$

Čtveřice $(Q(M), +, Q(R), \cdot)$ je tedy vektorovým prostorem.

V druhé části ukážeme, že zobrazení $\nu : m \mapsto [(m,1)]_{\sim_M}$ je vnořením M do $Q(M)$.

(i) Nejdříve ukážeme, se jedná o homomorfismus. Volme proto $m, n \in M$ a $r \in R$ libovolně. Pak

$$\nu(m+n) = [(m+n,1)]_{\sim_M} = [(m,1)]_{\sim_M} + [(n,1)]_{\sim_M} = \nu(m) + \nu(n)$$

a

$$\nu(rm) = [(rm,1)]_{\sim_M} = \frac{r}{1}[(m,1)]_{\sim_M} = r\nu(m).$$

(ii) Nyní ukážeme, že ν je injektivní zobrazení. Ať tedy pro $m, n \in M$ platí $\nu(m) = \nu(n)$, tj. $[(m,1)]_{\sim_M} = [(n,1)]_{\sim_M}$. Pak $(m,1) \sim_M (n,1)$, a to podle definice relace $\sim_M$ znamená $1m = 1n$, neboli $m = n$.

Tím je věta dokázána. ■

Anologicky jako při konstrukci podílového tělesa oboru integrity nyní ztožníme prvky $m \in M$ a třídy $\nu(m) = [(m,1)]_{\sim_M}$. Tím docílíme toho, že $M \subseteq Q(M)$. Dále přeznačíme třídy $[(m,r)]_{\sim_M}$ na „zlomky“ $\frac{m}{r}$. Operace definované v (3.2) a v (3.3) lze pak přepsat do tvaru

$$\frac{m}{r} + \frac{n}{s} = \frac{sm+rn}{rs} \qquad \text{a} \qquad \frac{u}{v}\frac{m}{r} = \frac{um}{vr},$$

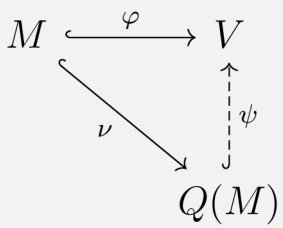
$m, n \in M, u, v, r, s \in R, r, s, v \neq 0$.

Takto zkonstruovaný vektorový prostor $Q(M)$ bude mít i svůj název. Vizte následující definici.

Definice 3.6. Ať $Q(R)$ je podílové těleso oboru integrity R, M je symetrický R-bimodul. Pak vektorový prostor $Q(M)$, o kterém pojednává věta 3.5, nazýváme *podílový vektorový prostor R-bimodulu M*. Vnoření ν, které je zmíněno v téže větě, nazýváme *kanonické vnoření M do $Q(M)$*.

Zabývejme se nyní minimalitou konstrukce $Q(M)$. Následující věta nám říká, že podílový vektorový prostor je nejmenším vektorovým prostorem, do kterého lze bimodul M vnořit.

Věta 3.7. *Ať $Q(R)$ je podílové těleso oboru integrity R, $Q(M)$ je podílový vektorový prostor symetrického R-bimodulu M a ν je kanonické vnoření M do $Q(M)$. Dále ať existuje vnoření $\varphi : M \hookrightarrow V$ bimodulu M do vektorového prostoru V nad podílovým tělesem $Q(R)$. Pak existuje vnoření $\psi : Q(M) \hookrightarrow V$ takové, že $\psi \circ \nu = \varphi$, neboli následující diagram komutuje:*



Důkaz. Ukážeme, že zobrazení $\psi : Q(M) \to V$ definované předpisem

$$\psi\left(\frac{m}{r}\right) = \frac{1}{r}\varphi(m)$$

je hledané vnoření.

(i) Nejdříve ukažme, že se jedná o homomorfismus. Volme proto $\frac{m}{r}, \frac{n}{s} \in Q(M)$ a $\frac{u}{v} \in Q(R)$ libovolně. Pak máme

$$\begin{aligned}\psi\left(\frac{m}{r}+\frac{n}{s}\right) = \psi\left(\frac{sm+rn}{rs}\right) &= \frac{1}{rs}\varphi(sm+rn) \overset{\text{(a)}}{=} \frac{1}{rs}\Big(\varphi(sm)+\varphi(rn)\Big) \\ &\overset{\text{(b)}}{=} \frac{1}{rs}\varphi(sm)+\frac{1}{rs}\varphi(rn) \overset{\text{(a)}}{=} \frac{1}{r}\varphi(m)+\frac{1}{s}\varphi(n) \\ &= \psi\left(\frac{m}{r}\right)+\psi\left(\frac{n}{s}\right),\end{aligned}$$

kde (a) plyne ze skutečnosti, že φ je homomorfismus a (b) plyne z faktu, že V je vektorový prostor. Dále

$$\psi\left(\frac{u}{v}\frac{m}{r}\right) = \psi\left(\frac{um}{vr}\right) = \frac{1}{vr}\varphi(um) \overset{\text{(a)}}{=} \frac{u}{vr}\varphi(m) = \frac{u}{v}\psi\left(\frac{m}{r}\right),$$

kde (a) opět plyne z faktu, že φ je homomorfismus.

(ii) V druhém kroku ukážeme, že ψ je injektivní zobrazení. Ať tedy $\psi\left(\frac{m}{r}\right) = \psi\left(\frac{n}{s}\right)$, tj. $\frac{1}{r}\varphi(m) = \frac{1}{s}\varphi(n)$. Odtud $s\varphi(m) = r\varphi(n)$, z čehož užitím skutečnosti, že φ je homomorfismus, máme $\varphi(sm) = \varphi(rn)$. Protože φ je injektivní, tak $sm = rn$. To ale znamená, že $(m, r) \sim_M (n, r)$, a proto $\frac{m}{r} = \frac{n}{s}$.

Dokázali jsme, že ψ je vnoření $Q(M)$ do V. Navíc $\psi \circ \nu = \varphi$. Totiž pro $m \in M$ máme

$$(\psi \circ \nu)(m) = \psi\Big(\nu(m)\Big) = \psi\left(\frac{m}{1}\right) = \frac{1}{1}\varphi(m) = \varphi(m).$$

■

Poznámka 3.8. Jak víme z poznámky 1.9, okruh R lze chápat jako bimodul sám nad sebou. Protože v oboru integrity je násobení komutativní, lze jej chápat jako symetrický bimodul (násobení skaláry v R jakožto bimodulu je právě násobení v R jakožto oboru integrity). Lze tedy zkonstruovat jednak podílové těleso $Q(R)$ oboru integrity R, jednak podílový vektorový prostor R jakožto symetrického R-bimodulu, který také značíme $Q(R)$. Otázkou je, zda je mezi těmito strukturami nějaký rozdíl. Není těžké si uvědomit, že kontrukce podílového vektorového prostoru s konstrukcí podílového tělesa v tomto případě splývá. Odtud lze na $Q(R)$ pohlížet oběma způsoby – jako na podílové těleso oboru integrity R nebo jako na vektorový prostor nad tělesem $Q(R)$.

3.3. Podílové rozšíření derivace

Nyní se zabývejme rozšířením (R, M)-derivace D, kde R je obor integrity a M je symetrický R-bimodul, na derivaci $D^* : Q(R) \to Q(M)$. Patrně bude existovat

jediný způsob, jak tuto derivaci definovat, a to sice pomocí vztahu o derivaci podílu z věty 2.26. Nepřekvapí nás tedy následující věta.

Věta 3.9. *Ať $Q(R)$ je podílové těleso oboru integrity R, $Q(M)$ je podílový vektorový prostor symetrického R-bimodulu M a D je (R,M)-derivace. Pak zobrazení*

$$\begin{aligned} D^* :\ Q(R) &\to Q(M), \\ \frac{r}{s} &\mapsto \frac{sDr - rDs}{s^2} \end{aligned}$$

je jedinou $(Q(R),Q(M))$-derivací takovou, že $D^*|_R = D$.

Důkaz. Protože obraz třídy $\frac{r}{s} \in Q(R)$ v zobrazení D^* je definován pomocí jejího reprezentanta, tj. dvojice $(r,s) \in R \times (R \setminus \{0\})$, musíme nejdříve ověřit korektnost definice D^*. Volme proto dvě dvojice $(r,s),(u,v) \in R \times (R \setminus \{0\})$ takové, že $\frac{r}{s} = \frac{u}{v}$, tj. $ru = sv$. Chceme ukázat, že

$$\frac{sDr - rDs}{s^2} = \frac{vDu - uDv}{v^2}.$$

Tuto rovnost upravujme:

$$\begin{aligned} sv^2Dr - rv^2Ds &= s^2vDu - s^2uDv \\ sv^2Dr + s^2uDv &= s^2vDu + rv^2Ds \\ sv^2Dr + s(su)Dv &= s^2vDu + (rv)vDs \\ sv^2Dr + s(rv)Dv &= s^2vDu + (su)vDs \\ sv(vDr + rDv) &= sv(sDu + uDs) \\ D(rv) &= D(su), \end{aligned}$$

kde výrazy na posledním řádku jsou si rovny, neboť $rv = su$. Stačí si už jen uvědomit, že v každém kroku byly použity ekvivalentní úpravy. Lze tedy postupovat zpětným chodem, tj. začít s rovností $D(rv) = D(su)$, ze které pak plynou řádky výše, a tedy finálně i rovnost

$$\frac{sDr - rDs}{s^2} = \frac{vDu - uDv}{v^2}.$$

kterou jsme chtěli dokázat.[28] Jistě taky $D^*(\frac{r}{s}) \in Q(M)$ pro každé $\frac{r}{s} \in Q(R)$. Dostáváme tak, že D^* je korektně definované zobrazení $Q(R) \to Q(M)$.

V druhém kroku ukážeme, že se jedná o $(Q(R),Q(M))$-derivaci tak, že dokážeme platnost Leibnizovy formule:

[28] Byl volen tento méně formální „obrácený“ postup důkazu, aby jednotlivé kroky byly jasnější.

$$
\begin{aligned}
D^*\left(\frac{r}{s}\frac{u}{v}\right) = D^*\left(\frac{ru}{sv}\right) &= \frac{svD(ru) - ruD(sv)}{(sv)^2} \\
&= \frac{usvDr + rsvDu - ruvDs - rusDv}{s^2v^2} \\
&= \frac{uv(sDr - rDs) + rs(vDu - uDv)}{s^2v^2} \\
&= \frac{u(sDr - rDs)}{s^2v} + \frac{r(vDu - uDv)}{sv^2} = \frac{u}{v}\frac{sDr - rDs}{s^2} + \frac{r}{s}\frac{vDu - uDv}{v^2} \\
&= \frac{u}{v}D^*\left(\frac{r}{s}\right) + \frac{r}{s}D^*\left(\frac{u}{v}\right).
\end{aligned}
$$

Dalším krokem bude ukázat, že $D^*|_R = D$. Zvolme $r \in R$ libovolně a počítejme

$$
D^*r = D^*\left(\frac{r}{1}\right) = \frac{1Dr - rD1}{1^2} = \frac{Dr}{1} = Dr,
$$

protože $D1 = o$ (1 je konstanta vůči libovolné derivaci – věta 2.17).

Na závěr dokážeme, že taková $(Q(R), Q(M))$-derivace s vlastností $D^*|_R = D$ je jediná. Ať i $\widehat{D}$ je $(Q(R), Q(M))$-derivace taková, že $\widehat{D}|_R = D$, a volme $\frac{r}{s} \in Q(R)$ libovolně. Pak lze psát

$$
\frac{r}{s} = \frac{r}{1}\frac{1}{s} = rs^{-1}, \tag{3.4}
$$

kde inverze s^{-1} je chápána v $Q(R)$, nikoliv v R (s totiž nemusí být invertibilní v R). Pak ale z věty 2.26 máme

$$
\widehat{D}\left(\frac{r}{s}\right) = \widehat{D}(rs^{-1}) = (s\widehat{D}r - r\widehat{D}s)s^{-2} \overset{(*)}{=} \frac{sDr - rDs}{s^2} = D^*\left(\frac{r}{s}\right),
$$

kde $(*)$ plyne z předpokladu $\widehat{D}|_R = D$ a z faktu, že

$$
(s\widehat{D}r - r\widehat{D}s, s^2) \sim_M \Big((s\widehat{D}r - r\widehat{D}s)s^{-2}, 1\Big)
$$

znamená rovnost

$$
s\widehat{D}r - r\widehat{D}s = s^2s^{-2}(s\widehat{D}r - r\widehat{D}s),
$$

která zjevně platí. Tímto je důkaz věty u konce. ■

Takto zkonstruovaná derivace bude mít svůj název, který se tyčí v názvu této kapitoly (vizte následující definici).

Definice 3.10. Ať $Q(R)$ je podílové těleso oboru integrity R, $Q(M)$ je podílový vektorový prostor symetrického R-bimodulu M a D je (R, M)-derivace. Pak zobrazení $D^* : Q(R) \to Q(M)$ definované ve větě 3.9 nazýváme *podílové rozšíření derivace* D a tuto skutečnost zapisujeme následovně: $D^* = Q(D)$.

Poznámka 3.11. Je-li M symetrický bimodul nad oborem integrity R, pak z věty 3.9 ihned dostáváme, že zobrazení

$$
Q : \mathfrak{Der}(R, M) \to \mathfrak{Der}\Big(Q(R), Q(M)\Big),
$$

které derivace D přiřadí své podílové rozšíření $Q(D)$, je injektivní. Totiž pokud $Q(D_1) = Q(D_2)$, pak

$$D_1 = Q(D_1)|_R = Q(D_2)|_R = D_2.$$

Odtud taky

$$|\mathfrak{Der}(R, M)| \leq \Big|\mathfrak{Der}\Big(Q(R), Q(M)\Big)\Big|.$$

Kapitola 4

Derivace na číselných oborech

4.1. Aritmetické derivace

V této kapitole představíme, jak je uvedeno v poznámce 2.10, příklady neaditivních derivací, a to sice tzv. *aritmetické derivace*, které budou definovány na některých číselných oborech. Budeme se přitom inspirovat článkem [7]. Začneme definicí aritmetické derivace na $\mathbb{Z}$, což je s ohledem na definici 2.1 nejmenší číselný obor, na kterém lze derivaci definovat ($\mathbb{N}$ totiž není okruhem). Pro tento účel nejdříve zavedeme novou notaci. Označme $\mathbb{P}$ množinu všech prvočísel, kterou oindexujme následovně:

$$\mathbb{P} = \{p_i \mid i \in \mathbb{N}\}.$$

Pro jednoduchost ať $p_1 < p_2 < p_3 < \dots$, tj. $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ atd. Rozklad přirozených čísel na součin prvočísel pak budeme zapisovat jako součin

$$\prod_{i\in\mathbb{N}} p_i^{\alpha_i},$$

kde jen konečně mnoho z $\alpha_i \in \mathbb{N}_0$ je nenulových. Ten, byť se jeví jako nekonečný, je ve skutečnosti konečný. Kdykoliv tedy napíšeme, že n má prvočíselný rozklad $\prod_{i\in\mathbb{N}} p_i^{\alpha_i}$, budeme vždy implicitně předpokládat, že jen konečně mnoho z α_i je nenulových. Tato notace bude velice výhodná v této i v následující kapitole 5 o konstrukci derivace na oboru integrity s jednoznačným rozkladem.

Dříve, než přistoupíme k definici již avizované aritmetické derivace, dokážeme následující větu.

Věta 4.1. *Existuje jediná $\mathbb{Z}$-derivace D splňující*

$$\forall p \in \mathbb{P} : D(p) = 1.^a \tag{4.1}$$

[a] V této kapitole budeme pro derivace na číselných oborech namísto Dn používat (pro obrazy čísel v zobrazení přirozenější) zápis $D(n)$.

Důkaz. Ať D je $\mathbb{Z}$-derivace splňující podmínku (4.1). Důkaz jednoznačnosti provedeme tak, že nalezneme její explicitní předpis. Z věty 2.17 ihned dostáváme, že $D(0) = 0$. Derivaci záporných čísel lze převést na derivaci kladných čísel pomocí vztahu (2.1), tj. pro $n \in \mathbb{N}$ máme

$$D(-n) = -D(n). \tag{4.2}$$

Stačí tedy nalézt obrazy všech přirozených čísel. Využijeme přitom skutečnosti, že každé takové číslo n (včetně čísla 1, kde v tomto případě pokládáme všechna $\alpha_i = 0$) lze jednoznačně (až na pořadí) rozložit na součin prvočísel

$$n = \prod_{i \in \mathbb{N}} p_i^{\alpha_i},$$

S ohledem na věty 2.24 a 2.29, na komutativitu násobení přirozených čísel a na definiční podmínku (4.1) derivace D lze provést následující výpočet:

$$\begin{aligned} D(n) = D\left(\prod_{i \in \mathbb{N}} p_i^{\alpha_i}\right) &= \sum_{i \in \mathbb{N}} D(p_i^{\alpha_i}) \prod_{j \in \mathbb{N} \setminus \{i\}} p_j^{\alpha_j} = \sum_{i \in \mathbb{N}} \alpha_i p_i^{\alpha_i - 1} D(p_i) \prod_{j \in \mathbb{N} \setminus \{i\}} p_j^{\alpha_j} \\ &= \sum_{i \in \mathbb{N}} \alpha_i p_i^{\alpha_i - 1} \prod_{j \in \mathbb{N} \setminus \{i\}} p_j^{\alpha_j} = \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i} \prod_{j \in \mathbb{N}} p_j^{\alpha_j} = n \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i}. \end{aligned}$$

(Uvědomme si, že pokud pro nějaké $i \in \mathbb{N}$ je $\alpha_i = 0$, pak i člen $\alpha_i p_i^{\alpha_i - 1}$ má smysl a je roven 0.) Derivace D má tedy tento předpis:

- $D(0) = 0$ a
- je-li $n \in \mathbb{Z} \setminus \{0\}$, kde $|n|$ má prvočíselný rozklad $\prod_{i \in \mathbb{N}} p_i^{\alpha_i}$, pak

$$D(n) = n \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i}.^{29} \tag{4.3}$$

Existenci ukážeme tak, že o zobrazení definovaném právě odvozeným předpisem ukážeme, že je $\mathbb{Z}$-derivací splňující podmínku (4.1). Pro každé prvočíslo p dostaneme

$$D(p) = p \cdot \frac{1}{p} = 1.$$

Nyní volme dvě celá čísla m a n. Je-li alespoň jedno z nich 0, pak

$$D(mn) = D(0) = 0 = nD(m) + mD(n).$$

Ať jsou tedy obě nenulová a $|m|$ a $|n|$ mají po řadě prvočíselné rozklady $\prod_{i \in \mathbb{N}} p_i^{\alpha_i}$ a $\prod_{j \in \mathbb{N}} p_j^{\beta_j}$. Pak

$$|mn| = \left(\prod_{i \in \mathbb{N}} p_i^{\alpha_i}\right) \left(\prod_{j \in \mathbb{N}} p_j^{\beta_j}\right) = \prod_{i \in \mathbb{N}} p_i^{\alpha_i + \beta_i},$$

[29] Pro $n < 0$ opravdu dostaneme stejnou formuli jako pro derivaci kladných přirozených čísel. Platí totiž

$$D(n) = -D(|n|) = -|n| \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i} = n \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i}.$$

Dále si uvědomme, že tímto předpisem je definováno zobrazení $\mathbb{Z} \to \mathbb{Z}$. Totiž pro všechna $i \in \mathbb{N}$ taková, že $\alpha_i \neq 0$, platí $p_i \mid n$, a tedy $n \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i} \in \mathbb{Z}$. To ostatně plane i z rovnosti

$$n \sum_{i \in \mathbb{N}} \frac{\alpha_i}{p_i} = \sum_{i \in \mathbb{N}} \alpha_i p_i^{\alpha_i - 1} \prod_{j \in \mathbb{N} \setminus \{i\}} p_j^{\alpha_j}.$$

a odtud

$$D(mn) = mn \sum_{i\in\mathbb{N}} \frac{\alpha_i + \beta_i}{p_i} = n\left(m \sum_{i\in\mathbb{N}} \frac{\alpha_i}{p_i}\right) + m\left(n \sum_{i\in\mathbb{N}} \frac{\beta_i}{p_i}\right) = nD(m) + mD(n).$$

Vidíme tedy, že zobrazení D definované předpisem (4.3) je $\mathbb{Z}$-derivací, čímž je věta dokázána. ■

Nyní již můžeme přistoupit k definici nového pojmu.

Definice 4.2. $\mathbb{Z}$-derivaci, o které pojednává věta 4.1, budeme nazývat *aritmetickou $\mathbb{Z}$-derivaci* a budeme ji značit $D_{\mathbb{Z}}$.

Poznámka 4.3. Povšimněme si toho, že $D_{\mathbb{Z}}$ není aditivní derivací. Například

$$1 = D_{\mathbb{Z}}(2) = D_{\mathbb{Z}}(1+1) \neq D_{\mathbb{Z}}(1) + D_{\mathbb{Z}}(1) = 0 + 0 = 0.$$

Příklad 4.4. Vztah (4.3) nám nabízí velice efektivní způsob výpočtu $D_{\mathbb{Z}}(n)$ pro $n \in \mathbb{Z}$. Pro ilustraci si ukažme, jak bychom spočítali např. derivaci čísla 12:

$$D_{\mathbb{Z}}(12) = 12\left(\frac{2}{2} + \frac{1}{3}\right) = 16.$$

Kdybychom tuto formuli neznali, museli bychom opakovaně rozkládat na součin a aplikovat Leibnizovu formuli, dokud bychom nedospěli k derivacím prvočísel. Např.

$$\begin{aligned} D_{\mathbb{Z}}(12) = D_{\mathbb{Z}}(3\cdot 4) &= 4D_{\mathbb{Z}}(3) + 3D_{\mathbb{Z}}(4) = 4 + 3D_{\mathbb{Z}}(2\cdot 2) \\ &= 4 + 3\Big(2D_{\mathbb{Z}}(2) + 2D_{\mathbb{Z}}(2)\Big) = 4 + 3(2+2) = 16. \end{aligned}$$

Poznámka 4.5. Podívejme se na to, jak vypadá jádro $D_{\mathbb{Z}}$. Pro $n \neq 0$ takové, že $|n|$ má prvočíselný rozklad $\prod_{i\in\mathbb{N}} p_i^{\alpha_i}$, platí

$$D_{\mathbb{Z}}(n) = n \sum_{i\in\mathbb{N}} \frac{\alpha_i}{p_i} = 0,$$

právě když pro všechna $i \in \mathbb{N}$ je $\alpha_i = 0$. To ale znamená, že $n \in \{-1, 1\}$. Proto $\operatorname{Ker} D_{\mathbb{Z}} = \{-1, 0, 1\}$, což není podokruh $\mathbb{Z}$!

Nyní rozšíříme aritmetickou $\mathbb{Z}$-derivaci na množinu racionálních čísel $\mathbb{Q}$. Z teoretické aritmetiky víme, že $\mathbb{Q}$ je definováno jako podílové těleso oboru integrity $\mathbb{Z}$. Nepřekvapí nás tedy následující definice.

Definice 4.6. *Aritmetickou $\mathbb{Q}$-derivací* rozumíme podílové rozšíření derivace $D_{\mathbb{Z}}$ a značíme ji $D_{\mathbb{Q}}$, tedy $D_{\mathbb{Q}} = Q(D_{\mathbb{Z}})$.

Z kapitoly 3 víme, že se jedná o jedinou $\mathbb{Q}$-derivaci takovou, že $D_{\mathbb{Q}}|_{\mathbb{Z}} = D_{\mathbb{Z}}$.

Podobně, jako jsme využitím rozkladu na součin prvočísel nalezli předpis pro artimetickou $\mathbb{Z}$-derivaci, můžeme nalézt podobnou formuli pro derivaci $D_{\mathbb{Q}}$ (vizte následující větu).

Věta 4.7. *Ať m, $n \in \mathbb{Z}\setminus\{0\}$ a $|m|$ a $|n|$ mají po řadě prvočíselné rozklady $\prod_{i\in\mathbb{N}} p_i^{\alpha_i}$ a $\prod_{i\in\mathbb{N}} p_i^{\beta_i}$. Pak platí*

$$D_{\mathbb{Q}}\left(\frac{m}{n}\right) = \frac{m}{n}\sum_{i\in\mathbb{N}}\frac{\alpha_i - \beta_i}{p_i}. \tag{4.4}$$

Důkaz. Platnost vztahu (4.4) plyne z následujícího výpočtu (m a n jsou jako z tvrzení věty):

$$D_{\mathbb{Q}}\left(\frac{m}{n}\right) = \frac{nD_{\mathbb{Z}}(m) - mD_{\mathbb{Z}}(n)}{n^2} = \frac{m}{n}\sum_{i\in\mathbb{N}}\frac{\alpha_i}{p_i} - \frac{m}{n}\sum_{i\in\mathbb{N}}\frac{\beta_i}{p_i} = \frac{m}{n}\sum_{i\in\mathbb{N}}\frac{\alpha_i - \beta_i}{p_i}.$$

■

Poznámka 4.8. Uvědomme si, že věta 4.7 lze též zformulovat následovně: Ať $q \neq 0$ je libovolné racionální číslo a

$$|q| = \prod_{i\in\mathbb{N}} p_i^{\alpha_i},$$

kde $\alpha_i \in \mathbb{Z}$ a jen konečně mnoho z nich je nenulových.[30] Pak platí

$$D_{\mathbb{Q}}(q) = q\sum_{i\in\mathbb{N}}\frac{\alpha_i}{p_i},$$

což působí jako identický vztah s (4.3). Rozdíl je v tom, že nyní připouštíme i záporná α_i.

4.2. Zobecnění aritmetických derivací

Ve větě 4.1 jsme ukázali, že existuje jediná derivace na $\mathbb{Z}$ splňující podmínku

$$\forall p \in \mathbb{P} : D(p) = 1.$$

Ukažme si její zobecněnou verzi.

Věta 4.9. *Ať $(d_i)_{i\in\mathbb{N}}$ je libovolná posloupnost celých čísel. Pak existuje jediná $\mathbb{Z}$-derivace D splňující*

$$\forall i \in \mathbb{N} : D(p_i) = d_i. \tag{4.5}$$

Důkaz. Budeme postupovat analogicky jako při důkazu věty 4.1.

Začneme jednoznačností. Předpokládejme, že taková derivace D existuje. Pak jistě $D(0) = 0$ a $D(-n) = -D(n)$ pro $n \in \mathbb{N}$. Pro přirozené číslo n s prvočíselným rozkladem $\prod_{i\in\mathbb{N}} p_i^{\alpha_i}$ dostáváme

[30] Je zřejmé, že každé kladné racionální číslo lze právě jedním způsobem psát v tomto tvaru.

$$D(n) = D\left(\prod_{i\in\mathbb{N}} p_i^{\alpha_i}\right) = \sum_{i\in\mathbb{N}} D(p_i^{\alpha_i}) \prod_{j\in\mathbb{N}\setminus\{i\}} p_j^{\alpha_j} = \sum_{i\in\mathbb{N}} \alpha_i p_i^{\alpha_i-1} D(p_i) \prod_{j\in\mathbb{N}\setminus\{i\}} p_j^{\alpha_j}$$
$$= \sum_{i\in\mathbb{N}} \alpha_i d_i p_i^{\alpha_i-1} \prod_{j\in\mathbb{N}\setminus\{i\}} p_j^{\alpha_j} = \sum_{i\in\mathbb{N}} \frac{\alpha_i d_i}{p_i} \prod_{j\in\mathbb{N}} p_j^{\alpha_j} = n \sum_{i\in\mathbb{N}} \frac{\alpha_i d_i}{p_i}.$$

Tímto jsme ukázali jednoznačnost.

Nyní je potřeba o zobrazení D, které je definováno následujícím způsobem:

- $D(0) = 0$,
- je-li $n \in \mathbb{Z}\setminus\{0\}$, kde $|n|$ má prvočíselný rozklad $\prod_{i\in\mathbb{N}} p_i^{\alpha_i}$, pak

$$D(n) = n \sum_{i\in\mathbb{N}} \frac{\alpha_i d_i}{p_i}, \tag{4.6}$$

ukázat, že se jedná o $\mathbb{Z}$-derivaci, což by se udělalo zcela analogicky jako při důkazu věty 4.1. ■

Poznámka 4.10. Analogický vztah jako (4.4) lze odvodit i pro podílové rozšíření $\mathbb{Z}$-derivace D splňující podmínku (4.5). Tento předpis odvodíme obecně na libovolném oboru integrity s jednoznačným rozkladem v poznámce 5.3.

Důsledkem věty 4.9 je následující tvrzení.

Důsledek 4.11. *Mezi množinou $\mathbb{Z}^{\mathbb{N}}$[a] všech posloupností celých čísel a množinou $\mathfrak{Der}(\mathbb{Z})$ existuje bijekce a pro mohutnost množiny $\mathfrak{Der}(\mathbb{Z})$ platí*

$$|\mathfrak{Der}(\mathbb{Z})| = \mathfrak{c}.$$[b]

[a] Jsou-li A a B množiny, pak symbolem A^B rozumíme množinu všech zobrazení $f : B \to A$. Pro její mohutnost platí $|A^B| = |A|^{|B|}$.

[b] $\mathfrak{c}$ zde značí *mohutnost kontinua*, tj. mohutnost množiny $\mathbb{R}$, pro kterou platí $\mathfrak{c} = 2^{\aleph_0}$, kde $\aleph_0 = |\mathbb{N}|$.

Důkaz. Z věty 4.9 plyne, že mezi posloupnostmi celých čísel a $\mathbb{Z}$-derivacemi je jednoznačná korespondence. Proto zobrazení

$$\mathfrak{Der}(\mathbb{Z}) \to \mathbb{Z}^{\mathbb{N}},$$
$$D \mapsto \big(D(p_i)\big)_{i\in\mathbb{N}}$$

je bijekcí uvedených množin, a tedy $|\mathfrak{Der}(\mathbb{Z})| = |\mathbb{Z}^{\mathbb{N}}|$. Stačí ukázat, že $|\mathbb{Z}^{\mathbb{N}}| = \mathfrak{c}$. Platí $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$. Z kardinální aritmetiky dostáváme

$$|\mathbb{Z}^{\mathbb{N}}| = |\mathbb{Z}|^{|\mathbb{N}|} = \aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0\aleph_0} = 2^{\aleph_0} = \mathfrak{c} = |\mathbb{R}|.$$[31]

Triviálně taky $2^{\aleph_0} \leq \aleph_0^{\aleph_0}$, a tedy z Cantorovy-Bernsteinovy věty máme $|\mathbb{Z}^{\mathbb{N}}| = \mathfrak{c}$ (vizte [3, 1.6 Cantor-Bernstein Theorem]). ■

[31] Na tomto místě využíváme platnosti hypetézy kontinua.

Poznámka 4.12. Z důsledku 4.11 a z poznámky 3.11 ihned vyplývá, že

$$|\mathfrak{Der}(\mathbb{Q})| \geq \mathfrak{c}.$$

V závěru této kapitoly ukážeme, že na $\mathbb{Z}$ neexistuje žádná netriviální aditivní derivace.

Věta 4.13. *Jedinou aditivní $\mathbb{Z}$-derivací je triviální derivace $O_{\mathbb{Z}}$.*

Důkaz. Z příkladu 2.4 víme, že $O_{\mathbb{Z}}$ je aditivní $\mathbb{Z}$-derivace. Pro spor předpokládejme, že D je libovolná netriviální aditivní $\mathbb{Z}$-derivace. Pak existuje $p \in \mathbb{P}$, že $D(p) \neq 0$. Kdyby totiž pro všechna $p \in \mathbb{P}$ platilo, že $D(p) = 0$, pak bychom s ohledem na větu 4.9 dostali, že $D = O$. Z aditivity D plyne

$$0 \neq D(p) = D\left(\sum_{i=1}^{p} 1\right) = \sum_{i=1}^{p} D(1) = 0,$$

a to je spor. Neexistuje tedy žádná netriviální aditivní $\mathbb{Z}$-derivace. ■

Kapitola 5

Derivace na oboru integrity s jednoznačným rozkladem

V kapitole 4 jsme téměř všechny vlastnosti aritmetických derivací odvodili z faktu, že každé přirozené číslo lze jednoznačně rozložit na součin prvočísel. Patrně tedy půjde konstrukce těchto derivací zobecnit na libovolné obory integrity s jednoznačným rozkladem.

Připomeňme proto nejdříve několik základních pojmů z teorie dělitelnosti v oborech integrity. V této kapitole bude R značit libovolný obor integrity s jednotkou 1.

(*i*) Řekneme, že *prvek* $r \in R$ *dělí prvek* $s \in R$, značíme $r \mid s$, jestliže existuje prvek $t \in R$ takový, že $s = rt$.

(*ii*) Prvek $r \in R$ nazveme *asociovaný s prvkem* $s \in R$, píšeme $r \parallel s$, jestliže $r \mid s$ a současně $s \mid r$ (jelikož je $\parallel$ relací ekvivalence na R, budeme také užívat obrat „prvky r a s jsou asociované“).

(*iii*) Prvky asociované s jednotkovým prvkem 1 nazýváme *jednotky dělení*.[32] Přímo z definice plyne, že jednotky dělení jsou právě invertibilní prvky R. Proto budeme pro množinu všech jednotek dělení R používat symbol $R^\times$.

(*iv*) Platí, že nenulové prvky r a s jsou asociované, právě když existuje jednotka dělení e taková, že $s = re$. Proč? Pokud $r \parallel s$, pak existují u, $v \in R$ takové, že $s = ru$ a $r = sv$. Odtud ovšem $r = ruv$, a tedy $1 = uv$, neboli u a v jsou jednotky dělení. Naopak ať $s = re$ pro nějakou jednotku dělení e. Ihned vidíme, že $r \mid s$. Protože existuje e^{-1}, tak $r = se^{-1}$, tj. $s \mid r$. Celkem tedy $r \parallel s$.

(*v*) Prvek $r \in R \setminus (\{0\} \cup R^\times)$ (tj. $r \neq 0$ a r není není jednotkou dělení) nazveme *ireducibilní*, jestliže pro libovolné $s \in R$ platí implikace

$$s \mid r \quad \Rightarrow \quad s \parallel 1 \text{ nebo } s \parallel r.$$

(*vi*) Prvek $p \in R \setminus (\{0\} \cup R^\times)$ nazveme *prvočinitel*, jestliže pro každé r, $s \in R$ platí implikace

$$p \mid rs \quad \Rightarrow \quad p \mid r \text{ nebo } p \mid s.$$

[32] Zde by stačilo říct, že jednotky dělení jsou právě ty prvky, které dělí jednotkový prvek R. Ten totiž dělí všechny prvky R.

(*vii*) Obor integrity R nazveme *oborem integrity s jednoznačným rozkladem*, jestliže pro libovolný prvek $r \in R \setminus (\{0\} \cup R^\times)$ platí: Jsou-li

$$r = \prod_{i=1}^{m} x_i \qquad \text{a} \qquad r = \prod_{j=1}^{n} y_j$$

dva rozklady r na součin ireducibilních prvků, pak $m = n$ a existuje permutace $\pi \in S_m$[33] taková, že

$$\forall i \in \widehat{m} : x_i \parallel y_{\pi(i)}.$$

(*viii*) Každý prvočinitel je ireducibilní, ale naopak to obecně neplatí. V oborech integrity s jednoznačným rozkladem ovšem platí i obrácená implikace, tj. mezi prvočiniteli a ireducibilními prvky není potřeba rozlišovat.

Jednotkami dělení v $\mathbb{Z}$ jsou právě 1 a -1. Vidíme tedy, že asociované jsou vždy dvojice čísel n a $-n$. Všchny ireducibilní prvky v $\mathbb{Z}$ (a tedy i všichni prvočinitelé[34]) jsou prvky $\mathbb{P} \cup (-\mathbb{P})$, tedy čísla ve tvaru $\pm p$, kde $p \in \mathbb{P}$. Pro rozklad přirozeného čísla na součin ireducibilních prvků jsme používali pouze prvočísla, tj. pouze kladné ireducibilní prvky. V podstatě jsme si z každé třídy rozkladu množiny $\mathbb{P} \cup (-\mathbb{P})$ podle relace $\parallel$ pevně zvolili jednoho reprezenta (v našem případě vždy kladné číslo) a pomocí nich jsme tvořili rozklady celých čísel. Pokud $n \in \mathbb{Z} \setminus \{0\}$ bylo takové, že $|n|$ mělo prvočíselný rozklad $\prod_{i \in \mathbb{N}} p_i \alpha_i$, pak

- $n = \prod_{i \in \mathbb{N}} p_i \alpha_i$ v případě $n > 0$ a
- $n = -\prod_{i \in \mathbb{N}} p_i \alpha_i$ v případě $n < 0$.

Tento postup půjde zobecnit pro libovolné obory integrity s jednoznačným rozkladem (vizte následující lemma).

[33] Symbolem S_m značíme množinu všech permutací na množině $\widehat{m}$.

[34] $\mathbb{Z}$ je oborem integrity hlavních ideálů, a tedy i oborem integrity s jednoznačným rozkladem (důkaz vizte např. v [5, Theorem 5.16.7]). Takže pojmy ireducibilní prvek a prvočinitel v tomto případě splývají.

Oborem integrity hlavních ideálů rozumíme takový obor integrity R, ve kterém je každý ideál hlavní, tj. je-li $I \subseteq R$ ideál, pak existuje $r \in R$ takové, že

$$I = \langle r \rangle = \{nr \mid n \in \mathbb{Z}\}.$$

Lemma 5.1. *Ať Y je množina všech ireducibilních prvků v oboru integrity R s jednoznačným rozkladem a $\{X_i \mid i \in I\}$ je systém všech tříd rozkladu Y podle relace $\parallel$,*[a] *tj.*

$$Y \Big/ \parallel = \{X_i \mid i \in I\}.$$

Dále ať je pro každé $i \in I$ z třídy X_i pevně vybrán ireducibilní prvek x_i.[b] *Pak každy prvek $r \in R$ lze jednoznačně (až na pořadí) vyjádřit ve tvaru*

$$r = e \prod_{i \in I} x_i^{\alpha_i},$$

kde $e \in R^\times$ a jen konečně mnoho z $\alpha_i \in \mathbb{N}_0$ je nenulových.

[a] Přesněji podle relace $\parallel$ zúžené na množinu $Y \times Y$.
[b] Povšimněme si, že je zde použit axiom výběru.

Důkaz. Volme $r \in R$ libovolně a označme jeho rozklad na součin ireducibilních prvků

$$\prod_{j=1}^{n} y_j^{\beta_j}.$$

Protože pro každé $j \in \widehat{n}$ je $y_j \in Y$, tak existuje index $i_j \in I$, že $y_j \in X_{i_j}$, tj. $y_j \parallel x_{i_j}$.[35] Odtud existuje $e_{i_j} \in R^\times$, že $y_j = e_{i_j} x_{i_j}$, a tedy

$$r = \prod_{j=1}^{n} y_j^{\beta_j} = \prod_{j=1}^{n} e_{i_j}^{\beta_j} x_{i_j}^{\beta_j} = \left(\prod_{j=1}^{n} e_{i_j}^{\beta_j} \right) \left(\prod_{j=1}^{n} x_{i_j}^{\beta_j} \right).$$

Protože součin jednotek dělení je opět jednotka dělení, tak $\prod_{j=1}^{n} e_{i_j}^{\beta_j} = e$ pro některé $e \in R^\times$. Nyní v součinu $\prod_{j=1}^{n} x_{i_j}^{\beta_j}$ sjednotíme stejná x_{i_j} pod jednu mocninu α_i[36] a doplníme ty prvky z x_i, $i \in I$ (opatřené mocninou $\alpha_i = 0$), které se v něm nenachází. Dostaneme tak, že

$$r = e \prod_{i \in I} x_i^{\alpha_i}.$$

Nyní určíme jednoznačnost. Protože R je obor integrity s jednoznačným rozkladem, tak je rozklad na součin ireducibilních prvků

$$r = \prod_{j=1}^{n} y_j^{\beta_j}$$

jednoznačný až na pořadí a asociovanost, a to právě ve smyslu bodu (*vii*) úvodu této kapitoly. To znamená, že pro každé y_j je výše vybraný prvek x_{i_j} asociovaný

[35] Povšimněme si, že pro $j, k \in \widehat{n}$, $j \neq k$, může platit $x_{i_j} = x_{i_k}$. V rozkladu

$$r = \prod_{j=1}^{n} y_j^{\beta_j}$$

totiž může pro $j \neq k$ nastat tato situce: $y_j \neq y_k$ a zároveň $y_j \parallel y_k$.

[36] Přesněji jsou-li $j_1, \ldots, j_k \in \widehat{n}$ taková, že $x_{i_{j_1}} = \cdots = x_{i_{j_k}} = x_i$ pro některé $i \in I$, pak pro příslušnou mocninu α_i při x_i platí $\alpha_i = \beta_{i_{j_1}} + \cdots + \beta_{i_{j_k}}$.

s y_j určen jednoznačně. Stačí ověřit, že pokud lze r vyjádřit následujícími dvěma způsoby:

$$r = e_1 \prod_{i\in I} x_i^{\alpha_i} \qquad \text{a současně} \qquad r = e_2 \prod_{i\in I} x_i^{\alpha_i},$$

kde e_1 a e_2 jsou jednotky dělení a jen konečně mnoho z α_i je nenulových, pak $e_1 = e_2$. To vyplyne z následujícího výpočtu:

$$0 = r - r = e_1 \prod_{i\in I} x_i^{\alpha_i} - e_2 \prod_{i\in I} x_i^{\alpha_i} = (e_1 - e_2) \prod_{i\in I} x_i^{\alpha_i}.$$

Protože $\prod_{i\in I} x_i^{\alpha_i} \neq 0$, tak $e_1 = e_2$. ■

Než přistoupíme k definici derivace na oboru integrity s jednoznačným rozkladem, předpokládejme (stejně jako v lemmatu 5.1), že máme pro každé $i \in I$ pevně vybrán prvek x_i z každé třídy X_i rozkladu množiny Y všech ireducibilních prvků R podle relace $\|$. Předpis zobrazení D v následující větě je inspirován předpisem $\mathbb{Z}$-derivace z věty 4.9.

Věta 5.2. *Ať je pro každé $i \in I$ pevně zvolem prvek $d_i \in R$. Pak zobrazení D, které každému $r \in R$ ve tvaru*

$$r = e \prod_{i\in I} x_i^{\alpha_i},$$

kde $e \in R^\times$ a jen konečně mnoho z $\alpha_i \in \mathbb{N}_0$ je nenulových, přiřadí prvek

$$Dr = e \sum_{i\in I} \alpha_i d_i x_i^{\alpha_i - 1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j}, \tag{5.1}$$

kde pro $i \in I$ takové, že $\alpha_i = 0$, pokládáme

$$\alpha_i d_i x_i^{\alpha_i - 1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j} = 0,$$

je R-derivací splňující

$$\forall i \in I : Dx_i = d_i. \tag{5.2}$$

Důkaz. S ohledem na lemma 5.1 je D korektně definované zobrazení $R \to R$. Platnost podmínky (5.2) je zřejmá z předpisu D. Ukažme, že platí Leibnizova formule. Volme r, $s \in R$, jejichž rozklady jsou

$$r = e_1 \prod_{i\in I} x_i^{\alpha_i} \qquad \text{a} \qquad s = e_2 \prod_{i\in I} x_i^{\beta_i},$$

e_1, $e_2 \in R^\times$ a jen konečně mnoho z α_i i z β_i je nenulových. Protože

$$rs = e_1 e_2 \prod_{i\in I} x_i^{\alpha_i + \beta_i},$$

přitom z lemmatu 5.1 plyne, že je tento rozklad jednoznačný, dostáváme

$$
\begin{aligned}
D(rs) &= e_1 e_2 \sum_{i\in I} (\alpha_i+\beta_i) d_i x_i^{\alpha_i+\beta_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j+\beta_j} \\
&= \left(e_2 \prod_{i\in I} x_i^{\beta_i}\right)\left(e_1 \sum_{i\in I} \alpha_i d_i x_i^{\alpha_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j}\right) \\
&\qquad + \left(e_1 \prod_{i\in I} x_i^{\alpha_i}\right)\left(e_2 \sum_{i\in I} \beta_i d_i x_i^{\beta_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\beta_j}\right) \\
&= sDr + rDs.
\end{aligned}
$$

Tím je důkaz věty u konce. ■

Poznámka 5.3. Derivaci D z věty 5.2 lze (stejně jako $D_{\mathbb{Z}}$) rozšířit na podílové těleso oboru integrity R. Označme si její podílové rozšíření D^*, tj. $D^* = Q(D)$. Pak obraz zlomku $\frac{r}{s}$, kde $r,\, s \in R\setminus\{0\}$ mají po řadě rozklady $e_1 \prod_{i\in I} x_i^{\alpha_i}$ a $e_2 \prod_{i\in I} x_i^{\beta_i}$ vyhovující předpokladům věty 5.2, v zobrazení D^* je

$$
\begin{aligned}
D^*\left(\frac{r}{s}\right) &= \frac{sDr - rDs}{s^2} \\
&= \frac{1}{e_2^2 \prod_{i\in I} x_i^{2\beta_i}} \left(\left(e_2 \prod_{i\in I} x_i^{\beta_i}\right)\left(e_1 \sum_{i\in I} \alpha_i d_i x_i^{\alpha_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j}\right) \right. \\
&\qquad \left. - \left(e_1 \prod_{i\in I} x_i^{\alpha_i}\right)\left(e_2 \sum_{i\in I} \beta_i d_i x_i^{\beta_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\beta_j}\right) \right) \\
&= \frac{e_1}{e_2} \sum_{i\in I} (\alpha_i-\beta_i) d_i x_i^{\alpha_i-\beta_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j-\beta_j} = \frac{e_1}{e_2} \prod_{j\in I} x_j^{\alpha_j-\beta_j} \sum_{i\in I} \frac{(\alpha_i-\beta_i)d_i}{x_i} \\
&= \frac{r}{s} \sum_{i\in I} \frac{(\alpha_i-\beta_i)d_i}{x_i},
\end{aligned}
$$

což je vztah skoro identický s (4.7) (jen zde v součtu navíc vystupují členy d_i, které předepisují hodnoty derivací zvolených ireducibilních prvků x_i – v případě $D_{\mathbb{Q}}$ platilo, že $D_{\mathbb{Q}}(p) = 1$ pro každé $p \in \mathbb{P}$).

V podílovém tělese $Q(R)$ lze také zjednodušit předpis (5.1), provedeme-li následující výpočet:

$$
Dr = e \sum_{i\in I} \alpha_i d_i x_i^{\alpha_i-1} \prod_{j\in I\setminus\{i\}} x_j^{\alpha_j} = e \prod_{j\in I} x_j^{\alpha_j} \sum_{i\in I} \frac{\alpha_i d_i}{x_i} = r \sum_{i\in I} \frac{\alpha_i d_i}{x_i}.
$$

[37]

Povšimněte si, že tato formule má smysl pouze v $Q(R)$, i když zobrazení D je z R do R. Protože podílové těleso $Q(R)$ oboru integrity R existuje vždy, je tento předpis korektní.

V důkazu věty 4.9 je při předepsání obrazů prvočísel ukázána existence a jednoznačnost $\mathbb{Z}$-derivace mající na $\mathbb{P}$ právě tyto obrazy. Platí totéž i pro derivaci D, o které pojednává věta 5.2? Při důkazu věty 4.9 jsme postupovali tak, že z podmínky $D(p_i) = d_i$, $i \in \mathbb{N}$, kde d_i jsou libovolně, ale pevně zvolená celá čísla, jsme jednoznačně odvodili předpis takové derivace. Volme stejnou strategii i v tomto případě. Ať

[37] Srovnejte tento vztah s (4.6).

$r \in R$ je jako v tvrzení věty 5.2 a D je R-derivace, která splňuje podmínku (5.2). S ohledem na větu 2.24 dostáváme

$$\begin{aligned} Dr = D\left(e\prod_{i\in I} x_i^{\alpha_i}\right) &= (De)\prod_{i\in I} x_i^{\alpha_i} + e\sum_{i\in I}\alpha_i x_i^{\alpha_i-1}(Dx_i)\prod_{j\in I\setminus\{i\}} x_j^{\alpha_j} \\ &= (De)\prod_{i\in I} x_i^{\alpha_i} + e\sum_{i\in I}\alpha_i d_i x_i^{\alpha_i-1}\prod_{j\in I\setminus\{i\}} x_j^{\alpha_j}, \end{aligned}$$

což obecně nemusí vyjít stejně, jako předpis D z věty 5.2. Pouze pokud platí $De = 0$ pro každé $e \in R^\times$, dostáváme (5.1). Lze tedy říci, že existuje jediná derivace na R splňující

- $Dx_i = d_i$ pro každé $i \in I$ a
- $De = 0$ pro každé $e \in R^\times$.

V tuto chvíli se nabízejí tři zajímavé otázky o derivacích na oboru integrity R s jednoznačným rozkladem, které ovšem v této práci nezodpovíme:

(*i*) Existují další možnosti (mimo výše uvedenou) jak předepsat obrazy jednotek dělení, které nejsou 1 a -1 (ty jsou totiž konstantami vůči všem derivacím), R-derivace tak, aby splňovala podmínku (5.2)?

(*ii*) Pokud ano, je tato derivace tímto předepsáním jednoznačně určená?

(*iii*) Lze tímto způsobem zkonstruovat všechny R-derivace? [38]

[38] Pokud bychom takto dovedli charakterizovat každou derivaci z množiny $\mathfrak{Der}(R)$, patrně by šla její mohutnost vyjádřit pomocí mohutností množin R a $R^\times$ (podobně jako jsme určili mohutnost množiny $\mathfrak{Der}(\mathbb{Z})$ při důkazu důsledku 4.11).

Kapitola 6

Algebraické struktury derivací

V důsledku 4.11 o mohutnosti množiny $\mathfrak{Der}(\mathbb{Z})$ jsme viděli, že zobrazení splňujících Leibnizovu formuli může na dané struktuře existovat mnoho. Pokud je M bimodul nad unitárním okruhem R (opět v této kapitole symboly R a M budeme rozumět právě tyto struktury), pak $O \in \mathfrak{Der}_+(R, M)$ a $D_m \in \mathfrak{Der}_+(R, M)$ pro libovolné $m \in M$ (připomeňme, že symbolem D_m značíme tzv. vnitřní (R, M)-derivaci určenou prvkem m – vizte příklad 2.9). Vidíme, že množina $\mathfrak{Der}_+(R, M)$ (a tedy i $\mathfrak{Der}(R, M)$) je vždy neprázdná. Patrně má tedy smysl zabývat se algebraickými strukturami, jejichž nosičem bude množina $\mathfrak{Der}(R, M)$, příp. $\mathfrak{Der}_+(R, M)$ (včetně případů, kdy $R = M$). K tomuto účelu zavedeme nové operace mezi derivacemi v následující definici.

Definice 6.1.

(i) *Součtem (R, M)-derivací D_1 a D_2* rozumíme zobrazení $D_1 + D_2 : R \to M$ definované vztahem

$$\forall r \in R : (D_1 + D_2)(r) = D_1 r + D_2 r.$$

(ii) *Komutátorem R-derivací D_1 a D_2* rozumíme zobrazení $[D_1, D_2] : R \to R$ definované vztahem

$$\forall r \in R : [D_1, D_2](r) = (D_1 \circ D_2)(r) - (D_2 \circ D_1)(r) = D_1(D_2 r) - D_2(D_1 r).$$

(iii) Ať $t \in R$. Pak *Levým*, resp. *pravým*, *t-násobkem (R, M)-derivace D* rozumíme zobrazení $tD : R \to M$, resp. $Dt : R \to M$, definované vztahem

$$\forall r \in R : (tD)(r) = tDr, \quad \text{resp.} \quad \forall r \in R : (Dt)(r) = (Dr)t.$$

Značení 6.2. Pro R-derivace D_1 a D_2 a prvek $r \in R$ budeme častěji namísto $(D_1 \circ D_2)(r)$ nebo $D_1(D_2 r)$ používat zkrácený zápis $D_1 D_2 r$. Definiční vztah komutátoru R-derivací se tak zjednoduší na

$$[D_1, D_2](r) = D_1 D_2 r - D_2 D_1 r.$$

Protože máme definovaný i součet R-derivací, lze psát

$$[D_1, D_2] = D_1 D_2 - D_2 D_1,$$ [39]

kde symbolem $-D_2 D_1$ značíme zobrazení $r \mapsto -D_2 D_1 r$ (později uvídíme, že se bude jednat o opačný prvek k $D_2 D_1$ v komutativní grupě $(\mathfrak{Der}(R, M), +)$).

Tímto jsme zadefinovali nová zobrazení $+, [\cdot, \cdot]$ a $\cdot$, na jejichž vstupech jsou derivace. Otázkou je, zda i jejich výstupy jsou opět derivace, tj. zda splňují Leibnizovu formuli. Následující lemma nám říká, za jakých předpokladů opravdu součtem a komutátorem derivací a t-násobkem derivace bude opět derivace.

Lemma 6.3.

(i) *Ať $D_1, D_2 \in \mathfrak{Der}(R, M)$. Pak i $D_1 + D_2 \in \mathfrak{Der}(R, M)$. Jsou-li navíc D_1 a D_2 aditivní, pak i $D_1 + D_2$ je aditivní.*

(ii) *Ať $D_1, D_2 \in \mathfrak{Der}_+(R)$. Pak i $[D_1, D_2] \in \mathfrak{Der}_+(R)$.*

(iii) *Ať $D \in \mathfrak{Der}(R, M)$ a $t \in Z(R)$[a]. Pak i $tD, Dt \in \mathfrak{Der}(R, M)$. Je-li navíc D aditivní, pak i tD a Dt jsou aditivní.*

[a] Symbolem $Z(R)$ značíme tzv. *centrum okruhu* R, tj. množinu

$$Z(R) = \{r \in R \mid \forall s \in R : rs = sr\}.$$

Důkaz: Zvolme r, $s \in R$, D_1, D_2, $D \in \mathfrak{Der}(R, M)$, $t \in Z(R)$ a r, $s \in R$ libovolně a dokažme postupně body (i), (ii) a (iii).

(i) Ukažme platnost Leibnizovy formule:

$$\begin{aligned}(D_1 + D_2)(rs) &= D_1(rs) + D_2(rs) \overset{(*)}{=} (D_1 r)s + rD_1 s + (D_2 r)s + rD_2 s \\ &= (D_1 r + D_2 r)s + r(D_1 s + D_2 s) \\ &= (D_1 + D_2)(r)s + r(D_1 + D_2)(s),\end{aligned}$$

kde v $(*)$ bylo využito Liebnizovy formule. Pokud jsou navíc D_1 a D_2 aditivní, dostáváme

$$\begin{aligned}(D_1 + D_2)(r + s) &= D_1(r + s) + D_2(r + s) = D_1 r + D_1 s + D_2 r + D_2 s \\ &= (D_1 + D_2)(r) + (D_1 + D_2)(s),\end{aligned}$$

čímž jsme dokázali aditivitu $D_1 + D_2$.

(ii) Ukažme nejdříve aditivitu $[D_1, D_2]$:

$$\begin{aligned}[D_1, D_2](r + s) &= D_1 D_2(r + s) - D_2 D_1(r + s) \\ &\overset{(*)}{=} D_1(D_2 r + D_2 s) - D_2(D_1 r + D_1 s) \\ &\overset{(*)}{=} D_1 D_2 r + D_1 D_2 s - D_2 D_1 r - D_2 D_1 s \\ &= [D_1, D_2](r) + [D_1, D_2](s),\end{aligned}$$

[39] Přesněji $[D_1, D_2] = D_1 D_2 + (-D_2 D_1)$.

kde v rovnostech $(*)$ bylo využito aditivity D_1 a D_2. Nyní ukažme platnost Leibnizovy formule:

$$\begin{aligned}
[D_1, D_2](rs) &= D_1D_2(rs) - D_2D_1(rs) \\
&\overset{(a)}{=} D_1\Big((D_2r)s + rD_2s\Big) - D_2\Big((D_1r)s + rD_1s\Big) \\
&\overset{(b)}{=} D_1\Big((D_2r)s\Big) + D_1\Big(rD_2s\Big) - D_2\Big((D_1r)s\Big) - D_2\Big(rD_1s\Big) \\
&\overset{(a)}{=} (D_1D_2r)s + D_2rD_1s + D_1rD_2s + rD_1D_2s \\
&\qquad - (D_2D_1r)s - D_1rD_2s - D_2rD_1s - rD_2D_1s \\
&= (D_1D_2r - D_2D_1r)s + r(D_1D_2s - D_2D_1s) \\
&= [D_1, D_2](r)s + r[D_1, D_2](s),
\end{aligned}$$

kde v (a) bylo využitu Leibnizovy formule a v (b) bylo využito aditivity D_1 a D_2.

(iii) Začněme s důkazem platnosti Leibnizovy formule pro zobrazení tD:

$$\begin{aligned}
(tD)(rs) = tD(rs) &\overset{(a)}{=} t\Big((Dr)s + rDs\Big) = t(Dr)s + trDs \overset{(b)}{=} t(Dr)s + rtDs \\
&= (tD)(r)s + r(tD)(s),
\end{aligned}$$

kde v (a) bylo využito Liebnizovy formule a v (b) bylo využito předpokladu $t \in Z(R)$. Nyní předpokládejme, že D je aditivní, a ukažme aditivitu tD:

$$(tD)(r+s) = tD(r+s) = t(Dr + Ds) = tDr + tDs = (tD)(r) + (tD)(s).$$

Analogicky postupujeme i při důkazu Leibnizovy formule a aditivity Dt. ■

Poznámka 6.4. Uvědomme si, že pokud je R komutativní okruh, pak jsou tD i Dt (R, M)-derivacemi pro libovolné $t \in R$ a $D \in \mathfrak{Der}(R, M)$.

Věta 6.5. *$\mathfrak{Der}(R, M)$ tvoří spolu se sčítáním derivací komutativní grupu.*

Důkaz. Ukážeme, že jsou splněny všechny definiční podmínky komutativní grupy.

- Uzavřenost $\mathfrak{Der}(R, M)$ na sčítání derivací plyne z bodu (i) lemmatu 6.3, takže $\mathfrak{Der}(R, M)$ spolu se sčítáním derivací tvoří grupoid.
- Asociativita a komutativita sčítání derivací plyne z asociativity a komutativity sčítání v bimodulu M.
- Nulovým prvkem $\mathfrak{Der}(R, M)$ je zřejmě nulová derivace $O_{R,M}$.
- Opačným prvkem k $D \in \mathfrak{Der}(R, M)$, pokud existuje, musí zřejmě být zobrazení $-D : R \to M$ definované předpisem

$$(-D)(r) = -Dr, \quad r \in R.$$

Protože $-1 \in Z(R)$, z bodu (iii) lemmatu 6.3 plyne, že i $-D$ je (R, M)-derivací. ■

Věta 6.6. *Ať M je bimodul nad komutativním unitárním okruhem R. Pak $\mathfrak{Der}(R, M)$ tvoří spolu s násobením derivací prkvy z R (levým i pravým) bimodul nad okruhem R.*

Důkaz. Z věty 6.5 víme, že $(\mathfrak{Der}(R, M), +)$ je komutativní grupa. Protože R je komutativní okruh, tak $tD, Dt \in \mathfrak{Der}(R, M)$ pro libovolné $t \in R$ a $D \in \mathfrak{Der}(R, M)$ (vizte poznámku 6.4). Stačí tedy ověřit platnost podmínek (i) až (iv) definic levého a pravého R-modulu (tj. definic 1.1 a 1.3) a podmínky (1.2) v definici bimodulu (tj. v definici 1.4). Zvolme $t, s \in R$ a $D, D_1, D_2 \in \mathfrak{Der}(R, M)$ a ověřme platnost podmínek v definici levého modulu (pro pravý modul bychom postupovali analogicky). Pro libovolně $r \in R$ máme

(i) $\Big((ts)D\Big)(r) = tsDr = \Big(t(sD)\Big)(r),$

(ii) $\Big((t+s)D\Big)(r) = (t+s)Dr = tDr + sDr = (tD)(r) + (sD)(r),$

(iii) $\Big(t(D_1 + D_2)\Big)(r) = t(D_1 + D_2)(r) = tD_1r + tD_2r = (tD_1)(r) + (tD_2)(r),$

(iv) $(1D)(r) = 1Dr = Dr.$

Nakonec ověřme platnost podmínky (1.2) v definici bimodulu:

$$\Big((tD)s\Big)(r) = (tD)(r)s = (tDr)s = t\Big((Dr)s\Big) = t(Ds)(r) = \Big(t(Ds)\Big)(r).$$

■

V kapitole 8 ukážeme, že množina tzv. *lineárních derivací* spolu s komutátorem $[\cdot, \cdot]$ tvoří tzv. *zobecněnou Lieovu algebru*. Nejdříve se ale v následující kapitole budeme zabývat derivacemi na *zobecněných asociativních algebrách*, kde si také pojem lineární derivace zadefinujeme.

Kapitola 7

Derivace na zobecněné asociativní algebře

V této kapitole se budeme zabývat derivacemi na tzv. *zobecněné asociativní algebře*, která bude levým modulem nad okruhem, který sám o sobě bude mít strukturu unitárního okruhu. Budeme přitom využívat pojmy definované v dodatku této práce.

Přistupme k definici nového pojmu.

Definice 7.1. Ať A je neprázdná množina, R je unitární okruh a jsou dány operace

$$+ : A \times A \to A, \quad \circ : A \times A \to A \quad \text{a} \quad \cdot : R \times A \to A.$$

Platí-li, že

(i) A tvoří spolu s operacemi $+$ a $\cdot$ levý R-modul,

(ii) A tvoří spolu s operacemi $+$ a $\circ$ unitární okruh a

(iii) $\forall a, b \in A \; \forall r \in R : r \cdot (a \circ b) = (r \cdot a) \circ b = a \circ (r \cdot b)$ (kompatibilita $\cdot$ s $\circ$),

pak A spolu s uvedenými operacemi $+, \circ, \cdot$ nazveme *levou zobecněnou*[a] *asociativní algebrou nad unitárním okruhem* R. Je-li R komutativním tělesem, pak A nazýváme *lineární algebrou nad* R. *Řádem algebry* A rozumíme řád A jakožto levého R-modulu. Je-li operace $\circ$ komutativní, pak algebru A nazýváme komutativní.

[a] Běžně se totiž asociativní algebra definuje nad komutativním okruhem.

Poznámka 7.2. Neřekneme-li jinak, nadále v této kapitole budeme symbolem R rozumět unitární okruh a symbolem A levou zobecněnou asociativní algebru nad R.

Poznámka 7.3. Analogicky lze zavést i tzv. *pravou zobecněnou asociativní algebru nad okruhem*. Její definice by se lišila pouze v bodě (i), kde bychom namísto levý modul psali pravý modul, a v bodě (iii), kde bychom prvky z A násobili skalárem zprava namísto zleva. Protože se těmito pravými zobecněnými asociativními algebrami zabývat nebudeme, kdykoliv zmíníme zobecněnou asociativní algebru nad okruhem, budeme jí rozumět levou algebru. Dokonce budeme zobecněnou asociativní

algebru nazývat pouze asociativní algebrou, příp. jen R-algebrou či algebrou. Kdykoliv budeme chtít zdůraznit, že daná R-algebra je definovaná nad komutativním okruhem, vysloveně na to upozorníme.

Poznámka 7.4. Jelikož nemůže dojít k nedorozumění, budeme nadále pro $a, b \in A$ a $r \in R$ místo $a \circ b$, resp. $r \cdot a$, psát pouze ab, resp. ra. Nulový prvek A budeme značit o, jednotkový prvek A budeme značit e.

Poznámka 7.5. Je-li B podmodulem modulu A a současně i podokruhem okruhu A, budeme B nazývat podalgebrou R-algebry A.

Poznámka 7.6. Bází R-algebry A rozumíme libovolnou bázi A jakožto R-modulu.

Z (ii) definice 7.1 ihned dostáváme, že je-li A algebrou nad okruhem R, pak zobrazení $D : A \to A$ splňující Leibnizovu formuli je A-derivací. Struktura algebry (konkrétně existence skalárního násobku) nám umožňuje zcela přirozeně zavést nový pojem.

Definice 7.7. A-derivaci D nazveme *lineární derivací*, pokud je aditivní a splňuje podmínku homogenity

$$\forall a \in A \; \forall r \in R : D(ra) = rDa. \tag{7.1}$$

Množinu všech lineárních A-derivací značíme $\mathfrak{Der}_\lambda(A)$.

Poznámka 7.8. A-derivaci D, která splňuje podmínku (7.1) budeme nazývat homogenní derivace. Tedy každá lineární derivace je derivací homogenní.

Následující věta nám představuje jednodušší kritérium pro to, aby aditivní A-derivace byla derivací lineární.

Věta 7.9. *Aditivní A-derivace D je lineární derivací, právě když*

$$\forall r \in R : D(re) = o.$$

Důkaz. Pokud je derivace D lineární, pak z věty 2.17 pro libovolné $r \in R$ dostáváme

$$D(re) = rDe = o.$$

Ukažme, že je platnost tohoto vztahu dokonce postačující podmínkou pro to, aby aditivní derivace D byla lineární. Z Leibnizovy formule máme pro libovolné $r \in R$ a $a \in A$

$$D(ra) = D\Big((re)a\Big) = D(re)a + reDa = D(re)a + rDa.$$

Odtud, pokud platí $D(re) = o$, dostáváme $D(ra) = rDa$. ∎

Poznámka 7.10. Povšimněte si, že jádro lineární derivace vždy obsahuje všechny skalární násobky jednotky e.

Z definice lineární derivace okamžitě plyne platnost následující věty.

Věta 7.11. *Lineární A-derivace je endomorfismem na R-modulu A.*

Poznámka 7.12. Zdůrazněme, že lineární A-derivace obecně není endomorfismem na asociativní algebře A. Totiž takový endomorfismus je mimo uzavřenosti na sčítání a na skalární násobek také uzavřený na násobení na A, tj.

$$\forall a, b \in A : \varphi(ab) = \varphi(a)\varphi(b),$$

a jednotku zobrazuje na jednotku, tj. $\varphi(e) = e$. To zřejmě nesplňuje žádná A-derivace (mimo triviální situaci, kdy $A = \{o\}$ – v tomto jako v jediném případě platí $e = o$). Abychom se vyhli nedorozumění, množinu všech endomorfismů na R-modulu A budeme značit $\mathfrak{End}_{\mathrm{mod}}(A)$, zatímco množinu všech endomorfismů na asociativní algebře A budeme značit $\mathfrak{End}_{\mathrm{alg}}(A)$. Platí tedy $\mathfrak{End}_{\mathrm{alg}}(A) \subseteq \mathfrak{End}_{\mathrm{mod}}(A)$.

Z poznámky 9.35 víme, že $\mathfrak{End}_{\mathrm{mod}}(A)$ tvoří spolu se sčítáním endomorfismů a násobením endomorfismů skalárem z R modul nad R. Zahrneme-li do této struktury navíc skládání endomorfismů, pak $\mathfrak{End}_{\mathrm{mod}}(A)$ bude se sčítáním a skládáním endomorfismů a násobením endomorfismů skalárem z R tvořit asociativní algebru nad R (stačí si uvědomit, že skládání je asociativní operace uzavřená na $\mathfrak{End}_{\mathrm{mod}}(A)$ a id_A je jednotkou v okruhu $(\mathfrak{End}_{\mathrm{mod}}(A), +, \circ)$).

Definice 7.13. Ať $D \in \mathfrak{Der}(A)$ a $r \in R$. Pak *(skalárním) r-násobkem derivace D* budeme rozmět zobrazení označované rD a definované vztahem

$$\forall a \in A : (rD)(a) = rDa.$$

Poznámka 7.14. Povšimněme si, že skalární násobek derivace D na R-algebře A není totéž co levý násobek derivace D definovaný v 6.1. Byť jejich definiční vztahy působí identicky, tyto pojmy se liší tím, že skalární násobek rD derivace D je definovaný pro $r \in R$, zatímco levý a-násobek D, tj. aD, je definován pro $a \in A$. Mezi nimi je ovšem tento vztah: $rD = (re)D$ (nalevo od rovnosti máme skalární r-násobek a na pravé straně již máme levý re-násobek definovaný v 6.1).

Není těžké ověřit, že rD je pro libovolné $r \in R$ A-derivací. Stačí provést následující výpočet (a, $b \in A$):

$$(rD)(ab) = rD(ab) = r(Da)b + raDb = (rD)(a)b + a(rD)(b)$$

Poznámka 7.15. Pokud je D navíc lineární A-derivací, pak z věty 7.11 je i endomorfismem modulu A. Přitom skalární násobek endomorfismů je již definovaný (vizte poznámku 9.35). Naštěstí obě tyto definice splývají.

Věta 7.16. *Ať A je asociativní algebra konečného řádu nad okruhem R a $\mathcal{B} = (e_1, \ldots, e_k)$ je bází A. Pokud pro endomorfismus $\delta \in \mathfrak{End}_{\mathrm{mod}}(A)$ a pro každé $i, j \in \widehat{k}$ platí*

$$\delta(e_i e_j) = \delta(e_i)e_j + e_i\delta(e_j),$$

pak δ je lineární A-derivací.

Důkaz. Pro $a, b \in A$ označme $[a]_{\mathcal{B}} = (a_1, \ldots, a_k)^{\mathrm{T}}$ a $[b]_{\mathcal{B}} = (b_1, \ldots, b_k)^{\mathrm{T}}$. Pak máme

$$\delta(ab) = \delta\left(\Big(\sum_{i=1}^{k} a_i e_i\Big)\Big(\sum_{j=1}^{k} b_j e_j\Big)\right) \overset{\text{(a)}}{=} \delta\left(\sum_{i=1}^{k}\sum_{j=1}^{k}(a_i b_j)(e_i e_j)\right) \overset{\text{(b)}}{=} \sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j \delta(e_i e_j),$$

kde (a) plyne z toho, že A je algebra a (b) plyne z faktu, že δ je endomorfismus modulu A. Dále

$$\delta(a)b = \delta\left(\sum_{i=1}^{k} a_i e_i\right)\left(\sum_{j=1}^{k} b_j e_j\right) = \left(\sum_{i=1}^{k} a_i \delta(e_i)\right)\left(\sum_{j=1}^{k} b_j e_j\right) = \sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j \delta(e_i) e_j$$

a analogicky

$$a\delta(b) = \left(\sum_{i=1}^{k} a_i e_i\right)\delta\left(\sum_{j=1}^{k} b_j e_j\right) = \sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j e_i \delta(e_j).$$

Pro to, aby endomorfismus δ byl lineární derivací, stačí dokázat platnost Leibnizovy formule

$$\delta(ab) = \delta(a)b + a\delta(b),$$

což využitím vztahů výše znamená

$$\begin{aligned}\sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j \delta(e_i e_j) &= \sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j \delta(e_i) e_j + \sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j e_i \delta(e_j) \\ &= \sum_{i=1}^{k}\sum_{j=1}^{k} a_i b_j \Big(\delta(e_i) e_j + e_i \delta(e_j)\Big).\end{aligned}$$

Odtud je zřejmé, že pokud pro každé $i, j \in \widehat{k}$ platí

$$\delta(e_i e_j) = \delta(e_i) e_j + e_i \delta(e_j),$$

pak je δ lineární A-derivací. ■

Věta 7.17. *Množina všech lineárních derivací $\mathfrak{Der}_\lambda(A)$ tvoří spolu se sčítáním derivací a násobením derivací skaláry z R podmodul modulu $\mathfrak{End}_{\mathrm{mod}}(A)$.*

Důkaz. Jistě $\mathfrak{Der}_\lambda(A) \subseteq \mathfrak{End}_{\mathrm{mod}}(A)$. Stačí tedy ukázat, že pro D, D_1, $D_2 \in \mathfrak{Der}_\lambda(A)$ a $r \in R$ platí, že derivace $D_1 - D_2$ a rD jsou lineární. Užitím bodů (i) a (iii) lemmatu 6.3 dostáváme, že z aditivity D_1 a D_2 plyne aditivita $D_1 - D_2$. Stačí už jen ukázat homogenitu $D_1 - D_2$. Zvolme proto $a \in A$ libovolně a počítejme:

$$(D_1 - D_2)(ra) \overset{\text{(a)}}{=} D_1(ra) - D_2(ra) \overset{\text{(b)}}{=} rD_1 a - rD_2 a = r(D_1 - D_2)(a),$$

kde (a) plyne z definice sčítání derivací a (b) plyne z homogenity D_1 a D_2. Dostali jsme, že $\mathfrak{Der}_\lambda(A)$ je uzavřená na odčítání derivací, tj. $\mathfrak{Der}_\lambda(A)$ je podgrupou aditivní grupy $\mathfrak{End}_{\mathrm{mod}}(A)$.

Dokažme uzavřenost $\mathfrak{Der}_\lambda(A)$ na skalární násobek. Zvolme $D \in \mathfrak{Der}_\lambda(A)$ a $s \in R$. Nejprve ukážeme, že sD je aditivní:

$$(sD)(a+b) \overset{\text{(a)}}{=} sD(a+b) \overset{\text{(b)}}{=} sDa + sDb \overset{\text{(a)}}{=} (sD)(a) + (sD)(b),$$

kde (a) plyne z definice sD a (b) plyne z aditivity D. Nyní ukážeme homogenitu:

$$(sD)(ra) \overset{\text{(a)}}{=} sD(ra) \overset{\text{(b)}}{=} rsDa \overset{\text{(a)}}{=} r(sD)(a),$$

kde (a) plyne z definice sD a (b) plyne z homogenity D a z komutativity R. Dostáváme tak, že $sD \in \mathfrak{Der}_\lambda(A)$.

Tímto je důkaz věty u konce. ■

Poznámka 7.18. Jelikož je lineární derivace D endomorfismem na modulu A, lze jí, pokud je A řádu $k \in \mathbb{N}$, v dané bázi $\mathcal{B}$ v souladu s definicí 9.36 přiřadit matici $\mathbf{D} \in \mathcal{M}_k(R)$,[40] pro kterou platí (vizte větu 9.37)

$$[Da]_\mathcal{B} = \left([a]_\mathcal{B}^{\mathrm{T}}\mathbf{D}^{\mathrm{T}}\right)^{\mathrm{T}} \quad \text{nebo ekvivalentně} \quad [Da]_\mathcal{B}^{\mathrm{T}} = [a]_\mathcal{B}^{\mathrm{T}}\mathbf{D}^{\mathrm{T}}, \quad a \in A.$$

Pokud je R komutativní okruh, pak se tento vztah zjednoduší na

$$[Da]_\mathcal{B} = \mathbf{D}[a]_\mathcal{B}.$$

Tato matice vypadá v bázi $\mathcal{B} = (e_1, \ldots, e_k)$ následovně:

$$\mathbf{D} = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1k} \\ d_{21} & d_{22} & \cdots & d_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ d_{k1} & d_{k2} & \cdots & d_{kk} \end{pmatrix}, \quad \text{kde} \quad [De_i]_\mathcal{B} = \begin{pmatrix} d_{1i} \\ \vdots \\ d_{ki} \end{pmatrix}, i = 1, \ldots, k.$$

Příklad 7.19. Uvažme modul M polynomů stupně nejvýše $n \in \mathbb{N}$ na komutativním unitárním okruhem R, který je podmodulem asociativní algebry $R[x]$.[41] Nyní zúžíme derivaci $\cdot'$ definovanou v příkladu 2.5 na modul M, označíme toto zobrazení D (tj. $D = \cdot'|_M$) a v modulu M zvolíme bázi $\mathcal{B} = (1, x, x^2, \ldots, x^n)$. Povšimněme si, že D není derivací ve smyslu definice 2.1, neboť M netvoří okruh! Zobrazení D je ale endomorfismem na modulu M, takže mu lze v bázi $\mathcal{B}$ přiřadit matici, na kterou můžeme pohlížet jako na matici derivace – ta totiž bude mít tu zásadní vlastnost, že díky ní budeme moci derivování polynomů z M převést na maticové násobení. Zřejmě platí

$$D1 = 0 \quad \text{a} \quad Dx^k = kx^{k-1} \text{ pro } k \in \widehat{n}.$$

V souřadnicích pak

$$[D1]_\mathcal{B} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{a} \quad [Dx^k]_\mathcal{B} = \begin{pmatrix} \delta_{1k}k \\ \vdots \\ \delta_{nk}k \end{pmatrix}, k \in \widehat{n}.$$

Odtud matice D v bázi $\mathcal{B}$ vypadá následovně:

[40] Symbolem $\mathcal{M}_k(R)$ rozumíme množinu všech čtvercových matic $k \times k$ nad okruhem R

[41] Již víme, že $R[x]$ tvoří unitární okruh. Budeme-li se na $R[x]$ dívat jako na algebru nad okruhem R, není těžké si uvědomit, že $R[x]$ opravdu bude asociativní algebrou nad R ve smyslu definice 7.1.

$$\mathbf{D} = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & n \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Věta 7.20. *Ať A je asociativní algebra řádu $k \in \mathbb{N}$ nad okruhem R. Pak asociativní algebra $\mathfrak{End}_{\mathrm{mod}}(A)$ spolu se sčítáním a skládáním endomorfismů a násobením endomorfismů skalárem je izomorfní asociativní algebře $\mathcal{M}_k(R)$ čtvercových matic řádu k nad okruhem R spolu se sčítáním a násobením matic a násobením matic skalárem.*

Důkaz. Zvolme si libovolnou bázi $\mathcal{B} = (e_1, \ldots, e_k)$ v A. Ukažme, že zobrazení

$$\Gamma_{\mathcal{B}} : \mathfrak{End}_{\mathrm{mod}}(A) \to \mathcal{M}_k(R),$$

které endomorfismu $\varphi \in \mathfrak{End}_{\mathrm{mod}}(A)$ přiřadí jeho matici v bázi $\mathcal{B}$, je izomorfismem asociativních algeber. Nejdříve ukažme, že se jedná o bijekci.

$(i)_B$ V prvním kroku dokažme injektivitu $\Gamma_{\mathcal{B}}$. Ať $\varphi, \psi \in \mathfrak{End}_{\mathrm{mod}}(A)$ jsou endomorfismy takové, že $\Gamma_{\mathcal{B}}(\varphi) = \Gamma_{\mathcal{B}}(\psi)$. To ale znamená $[\varphi(e_i)]_{\mathcal{B}} = [\psi(e_i)]_{\mathcal{B}}$ pro každé $i \in \widehat{k}$. Z věty 9.38 pak máme $\varphi = \psi$.

$(ii)_B$ Nyní ukažme surjektivitu $\Gamma_{\mathcal{B}}$. Zvolme matici $\mathbf{A} \in \mathcal{M}_k(R)$ libovolně. Pak pro endomorfismus φ takový, že $[\varphi(e_i)]_{\mathcal{B}} = (a_{1i}, \ldots, a_{ki})^{\mathrm{T}}, i \in \widehat{k}$, platí, že $\Gamma_{\mathcal{B}}(\varphi) = \mathbf{A}$ (jeho existence opět plyne z věty 9.38).

Nyní přejdeme k důkazu skutečnosti, že $\Gamma_{\mathcal{B}}$ je homomorfismem algeber, tj. že zachovává všechny operace na $\mathfrak{End}_{\mathrm{mod}}(A)$.

$(i)_H$ Nejdříve se podívejme na obraz součtu endomorfismů a násobku endomorfismu skalárem. Označme $\mathbf{A}$ a $\mathbf{B}$ matice po řadě endomorfismů $\varphi, \psi \in \mathfrak{End}_{\mathrm{mod}}(A)$. Zvolme navíc $r \in R$ libovolně. Matice endomorfismu $\varphi + \psi$ je $\mathbf{A} + \mathbf{B}$ a matice endomorfismu $r\varphi$ je $r\mathbf{A}$.[42] Máme tedy

$$\Gamma_{\mathcal{B}}(\varphi + \psi) = \Gamma_{\mathcal{B}}(\varphi) + \Gamma_{\mathcal{B}}(\psi) \qquad \text{a} \qquad \Gamma_{\mathcal{B}}(r\varphi) = r\Gamma_{\mathcal{B}}(\varphi).$$

$(ii)_H$ Konečně ukažme, že $\Gamma_{\mathcal{B}}$ převádí skládání endomorfismů na násobení matic. Ať matice $\mathbf{A}$ a $\mathbf{B}$ jsou stejné jako výše. Zvolme si libovolný prvek $a \in A$. Pak využitím věty 9.37 máme

$$\Big[(\varphi \circ \psi)(a)\Big]_{\mathcal{B}}^{\mathrm{T}} = \Big[\varphi\Big(\psi(a)\Big)\Big]_{\mathcal{B}}^{\mathrm{T}} = \Big[\psi(a)\Big]_{\mathcal{B}}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}} = [a]_{\mathcal{B}}^{\mathrm{T}} \mathbf{B}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}} = [a]_{\mathcal{B}}^{\mathrm{T}} (\mathbf{AB})^{\mathrm{T}}.$$

Odtud $\Gamma_{\mathcal{B}}(\varphi \circ \psi) = \Gamma_{\mathcal{B}}(\varphi)\Gamma_{\mathcal{B}}(\psi)$.

[42] Toto je známý fakt z úvodních kurzů lineární algebry pro endomorfismy na vektorových prostorech, ovšem zcela pochopitelně lze totéž dokázat i pro endomorfismy na asociativních algebrách.

Celkem tedy dostáváme, že $\Gamma_{\mathcal{B}}$ je izomorfismus asociativních algeber $\mathfrak{End}_{\mathrm{mod}}(A)$ a $\mathcal{M}_k(R)$. ■

Poznámka 7.21. Z věty 7.17 víme, že $\mathfrak{Der}_\lambda(A)$ tvoří podmodul $\mathfrak{End}_{\mathrm{mod}}(A)$, přitom $\mathfrak{End}_{\mathrm{mod}}(A) \cong \mathcal{M}_k(R)$ (je-li A řádu k). Odtud existuje vnoření $\mathfrak{Der}_\lambda(A)$ do $\mathcal{M}_k(R)$,[43] tj. $\mathfrak{Der}_\lambda(A)$ je izomorfní jistému podmodulu $\mathcal{M}_k(R)$.

Nyní využijeme poznámky 7.21 a maticového násobení k určení předpisu n-té derivace některých v jistém smyslu „pěkných“ funkcí (v jakém smyslu uvidíme později). Dále k tomu využijeme větu 9.40. Budeme řešit následující úlohu: Ať f je funkce z $\mathcal{C}^\infty(\Omega)$[44], kde $\Omega \subseteq \mathbb{R}$ je otevřená množina. Určete předpis $f^{(n)}$ pro libovolné $n \in \mathbb{N}$.

Postupovat budeme takto:

1. Určíme lineárně nezávislé funkce $f_1, \ldots, f_k$ takové, že

   $$f, f_1', \ldots, f_k' \in \langle f_1, \ldots, f_k \rangle.$$

   Takové funkce zřejmě nelze nalézt vždy. Při označení $\mathcal{F} = (f_1, \ldots, f_k)$ máme, že $\langle \mathcal{F} \rangle$ je $\frac{\mathrm{d}}{\mathrm{d}x}$-invariantní podprostor $\mathcal{C}^\infty(\Omega)$ (věta 9.40), z čehož plyne, že $f^{(n)} \in \langle \mathcal{F} \rangle$ pro libovolné $n \in \mathbb{N}$.

2. Určíme $[f]_{\mathcal{F}}, [f_1]_{\mathcal{F}}, \ldots, [f_k]_{\mathcal{F}}$ a matici $\mathbf{D}$ derivace $\frac{\mathrm{d}}{\mathrm{d}x}$ v bázi $\mathcal{F}$.[45]

3. Určíme $\mathbf{D}^n$ pro libovolné $n \in \mathbb{N}$ buď

   - přímo (pokud to lze), nebo
   - převodem na Jordanův kanonický tvar.

4. Vypočítáme souřadnice $f^{(n)}$ v bázi $\mathcal{F}$ pomocí matice $\mathbf{D}$ takto:

   $$[f^{(n)}]_{\mathcal{F}} = \mathbf{D}^n [f]_{\mathcal{F}}.$$

   Při označení

   $$[f^{(n)}]_{\mathcal{F}} = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

   je hledaná funkce ve tvaru

   $$f^{(n)} = \sum_{i=1}^{k} a_i f_i.$$

Tento postup si ukažme na následujících dvou příkladech:

[43] Toto vnoření přiřazuje ve zvolené bázi každé lineární derivaci její matici, tj. jedná se o zobrazení $\Gamma_{\mathcal{B}}$ zúžené na množinu $\mathfrak{Der}_\lambda(A)$.

[44] Symbolem $\mathcal{C}^\infty(\Omega)$ značíme množinu takových funkcí $f : \Omega \to \mathbb{R}$, které mají na Ω spojité derivace všech řádů. Je známou skutečností, že tato množina spolu se sčítáním funkcí a násobením funkcí reálnými čísly tvoří vektorový prostor. Tohoto faktu budeme využívat.

[45] Přesněji matici derivace $\frac{\mathrm{d}}{\mathrm{d}x}$ zúžené na $\langle \mathcal{F} \rangle$.

Příklad 7.22. Určete předpis $f^{(n)}$, kde

$$f(x) = e^x(\sin x + \cos x),\ x \in \mathbb{R}\,.$$

Řešení. Budeme postupovat podle bodů 1–4:

1. Nejdříve si přepišme předpis f takto:

$$f(x) = e^x \sin x + e^x \cos x.$$

Určeme f':

$$f'(x) = e^x \sin x + e^x \cos x + e^x \cos x - e^x \sin x = 2e^x \cos x.$$

To nás dovádí k tomu, abychom zvolili $f_1(x) = e^x \sin x$ a $f_2(x) = e^x \cos x$. Pak totiž $f,\ f_1',\ f_2' \in \langle f_1, f_2\rangle$, protože

$$\begin{aligned} f_1'(x) &= \quad e^x \sin x + e^x \cos x, \\ f_2'(x) &= -e^x \sin x + e^x \cos x. \end{aligned}$$

2. Označme $\mathcal{F} = (f_1, f_2)$ a určeme souřadnice f_1 a f_2:

$$[f_1']_{\mathcal{F}} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad [f_2']_{\mathcal{F}} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

Ihned taky vidíme, že $f = f_1'$, a tedy $[f]_{\mathcal{F}} = [f_1']_{\mathcal{F}} = (1,1)^{\mathrm{T}}$. S ohledem na poznámku 7.18 má matice $\mathbf{D}$ derivace $\frac{\mathrm{d}}{\mathrm{d}x}$ v bázi $\mathcal{F}$ tvar

$$\mathbf{D} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

3. Určíme $\mathbf{D}^n$ pomocí převodu $\mathbf{D}$ na Jordanův kanonický tvar. Nejdříve určíme spektrum matice $\mathbf{D}$.[46] Charakteristický polynom matice $\mathbf{D}$ má tvar

$$\det(\mathbf{D} - \lambda\mathbf{I}) = \begin{vmatrix} 1-\lambda & -1 \\ 1 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 + 1 = \lambda^2 - 2\lambda + 2.$$

Vyřešením kvadratické rovnice $\lambda^2 - 2\lambda + 2 = 0$ dostaneme 2 komplexně sdružená vlastní čísla

$$\lambda_1 = 1 + \mathrm{i} \quad \text{a} \quad \lambda_2 = 1 - \mathrm{i}\,.$$

Odtud $\operatorname{Spec}\mathbf{D} = \{1+\mathrm{i}, 1-\mathrm{i}\}$. Protože $\mathbf{D}$ je matice typu 2×2 a má dvě různá vlastní čísla, musí být Jordanův tvar matice $\mathbf{D}$ (až na pořadí diagonálních prvků) následující diagonální matice:

$$\mathbf{J} = \begin{pmatrix} 1+\mathrm{i} & 0 \\ 0 & 1-\mathrm{i} \end{pmatrix}.$$

Nyní určíme vlastní vektory příslušící jednotlivým vlastním číslům jako řešení homogenní soustavy lineárních rovnic

$$(\mathbf{D} - \lambda_j\mathbf{I})\mathbf{x} = \mathbf{o}, \quad j = 1, 2.$$

[46] Spektrem matice $\mathbf{D}$ rozumíme množinu všech jejích vlastních čísel, kterou značíme $\operatorname{Spec}\mathbf{D}$.

(*i*) Nejdříve najdeme vlastní podprostor[47] $\mathbf{N}_{1+\mathrm{i}}$ matice $\mathbf{D}$ příslušící vlastnímu číslu $\lambda_1 = 1+\mathrm{i}$ jako řešení homogenní soustavy rovnic o matici

$$\mathbf{D} - (1+\mathrm{i})\mathbf{I} = \begin{pmatrix} -\mathrm{i} & -1 \\ 1 & -\mathrm{i} \end{pmatrix} \sim \begin{pmatrix} \mathrm{i} & 1 \\ 0 & 0 \end{pmatrix}.$$

Platí tedy

$$\mathbf{N}_{1+\mathrm{i}} = \left\langle \begin{pmatrix} 1 \\ -\mathrm{i} \end{pmatrix} \right\rangle.^{48}$$

(*ii*) Nyní nalezneme vlastní podprostor $\mathbf{N}_{1-\mathrm{i}}$ jako řešení homogenní soustavy rovnic o matici

$$\mathbf{D} - (1-\mathrm{i})\mathbf{I} = \begin{pmatrix} \mathrm{i} & -1 \\ 1 & \mathrm{i} \end{pmatrix} \sim \begin{pmatrix} \mathrm{i} & -1 \\ 0 & 0 \end{pmatrix}.$$

Vidíme, že

$$\mathbf{N}_{1-\mathrm{i}} = \left\langle \begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix} \right\rangle.$$

Z lineární algebry víme, že matice $\mathbf{D}$ lze vyjádřit jako součin $\mathbf{D} = \mathbf{AJA}^{-1}$, kde $\mathbf{A}$ je regulární matice, jejíž sloupce jsou (pokud existují) lineárně nezávislé vlastní vektory. V našem případě má tedy matice $\mathbf{A}$ tvar

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ -\mathrm{i} & \mathrm{i} \end{pmatrix}.$$

Dále

$$\mathbf{A}^{-1} = \frac{1}{2}\begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix}.$$

Přímým výpočtem lze ověřit, že opravdu $\mathbf{D} = \mathbf{AJA}^{-1}$. Nyní tohoto rozkladu využijeme pro určení $\mathbf{D}^n$:

$$\begin{aligned}
\mathbf{D}^n = (\mathbf{AJA}^{-1})^n &= \underbrace{\mathbf{AJA}^{-1}\mathbf{AJA}^{-1}\cdots\mathbf{AJA}^{-1}}_{n\text{-krát}} = \mathbf{AJ}^n\mathbf{A}^{-1} \\
&= \begin{pmatrix} 1 & 1 \\ -\mathrm{i} & \mathrm{i} \end{pmatrix} \begin{pmatrix} 1+\mathrm{i} & 0 \\ 0 & 1-\mathrm{i} \end{pmatrix}^n \left(\frac{1}{2}\begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix} \right) \\
&= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -\mathrm{i} & \mathrm{i} \end{pmatrix} \begin{pmatrix} (1+\mathrm{i})^n & 0 \\ 0 & (1-\mathrm{i})^n \end{pmatrix} \begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} (1+\mathrm{i})^n + (1-\mathrm{i})^n & \mathrm{i}(1+\mathrm{i})^n - \mathrm{i}(1-\mathrm{i})^n \\ -\mathrm{i}(1+\mathrm{i})^n + \mathrm{i}(1-\mathrm{i})^n & (1+\mathrm{i})^n + (1-\mathrm{i})^n \end{pmatrix}.
\end{aligned}$$

[47] Vlastním podprostorem $\mathbf{N}_\lambda$ matice $\mathbf{D}$ příslušící vlastnímu číslu λ rozumíme množinu všech vlastních vektorů $\mathbf{D}$ příslušící λ spolu s nulovým vektorem $\mathbf{0}$ (vlastní vektory totiž chápeme jako vektory nenulové.

[48] Symbolem

$$\left\langle \begin{pmatrix} 1 \\ -\mathrm{i} \end{pmatrix} \right\rangle$$

zde značíme podprostor $\mathbb{R}^2$ generovaný vektorem $(1, -\mathrm{i})^{\mathrm{T}}$ tak, jak jsme jej zavedli pro podmoduly generované množinou. Chápeme jej však stejně jako tradičně užívaný zápis

$$\mathbf{N}_{1+\mathrm{i}} = \operatorname{span}\left\{ \begin{pmatrix} 1 \\ -\mathrm{i} \end{pmatrix} \right\}.$$

4. Určeme souřadnice $f^{(n)}$:

$$\begin{aligned}[f^{(n)}]_{\mathcal{F}} = \mathbf{D}^n[f]_{\mathcal{F}} &= \frac{1}{2}\begin{pmatrix}(1+\mathrm{i})^n + (1-\mathrm{i})^n & \mathrm{i}(1+\mathrm{i})^n - \mathrm{i}(1-\mathrm{i})^n \\ -\mathrm{i}(1+\mathrm{i})^n + \mathrm{i}(1-\mathrm{i})^n & (1+\mathrm{i})^n + (1-\mathrm{i})^n\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}(1+\mathrm{i})^n + \mathrm{i}(1+\mathrm{i})^n + (1-\mathrm{i})^n - \mathrm{i}(1-\mathrm{i})^n \\ -\mathrm{i}(1+\mathrm{i})^n + (1+\mathrm{i})^n + \mathrm{i}(1-\mathrm{i})^n + (1-\mathrm{i})^n\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}(1+\mathrm{i})^{n+1} + (1-\mathrm{i})^{n+1} \\ (1+\mathrm{i})^n(1-\mathrm{i}) + (1-\mathrm{i})^n(1+\mathrm{i})\end{pmatrix}.\end{aligned}$$

Jednotlivé souřadnice si ještě zjednodušme tak, aby v nich nevystupovala komplexní čísla. Využijeme přitom goniometrického tvaru komplexního čísla a Moivreovy věty. Zřejmě platí

$$1 \pm \mathrm{i} = \sqrt{2}\left(\cos\left(\pm\frac{\pi}{4}\right) + \mathrm{i}\sin\left(\pm\frac{\pi}{4}\right)\right) = \sqrt{2}\left(\cos\frac{\pi}{4} \pm \mathrm{i}\sin\frac{\pi}{4}\right).$$

Z Moievrovy věty pro libovolné $k \in \mathbb{N}$ plyne

$$(1 \pm \mathrm{i})^k = 2^{\frac{k}{2}}\left(\cos\frac{k\pi}{4} \pm \mathrm{i}\sin\frac{k\pi}{4}\right).$$

První složka vektoru $[f^{(n)}]_{\mathcal{F}}$ lze vyjádřit ve tvaru

$$\begin{aligned}\frac{1}{2}\left((1+\mathrm{i})^{n+1} + (1-\mathrm{i})^{n+1}\right) &= 2^{\frac{n-1}{2}}\Bigg(\cos\frac{(n+1)\pi}{4} + \mathrm{i}\sin\frac{(n+1)\pi}{4} \\ &\qquad + \cos\frac{(n+1)\pi}{4} - \mathrm{i}\sin\frac{(n+1)\pi}{4}\Bigg) \\ &= 2^{\frac{n+1}{2}}\cos\frac{(n+1)\pi}{4}.\end{aligned}$$

Podobně druhá složka $[f^{(n)}]_{\mathcal{F}}$ lze po úpravě vyjádřit ve tvaru

$$\frac{1}{2}\Big((1+\mathrm{i})^n(1-\mathrm{i}) + (1-\mathrm{i})^n(1+\mathrm{i})\Big) = 2^{\frac{n}{2}}\left(\cos\frac{n\pi}{4} + \sin\frac{n\pi}{4}\right).$$

Celkem dostáváme, že předpis funkce $f^{(n)}$ je pro libovolné $n \in \mathbb{N}$ následující:

$$f^{(n)}(x) = 2^{\frac{n+1}{2}}\cos\left(\frac{(n+1)\pi}{4}\right)e^x\sin x + 2^{\frac{n}{2}}\left(\cos\frac{n\pi}{4} + \sin\frac{n\pi}{4}\right)e^x\cos x,\ x \in \mathbb{R}.$$

○

Příklad 7.23. Určete předpis n-té derivace funkce

$$f(x) = x^k e^x,\ x \in \mathbb{R}, k \in \mathbb{N}.$$

Řešení.

1. Určeme derivaci f:
$$f'(x) = x^k e^x + k x^{k-1} e^x.$$
Pokud označíme $f_0(x) = f(x) = x^k e^x$ a $f_1(x) = x^{k-1} e^x$, pak $f, f' \in \langle f_0, f_1 \rangle$. Funkce f_0, f_1 je potřeba ještě doplnit funkcemi
$$f_i(x) = x^{k-i} e^x, \ i = 2, \dots, k,$$
aby platilo $f_i' \in \langle f_0, \dots, f_k \rangle$ pro všechna $i \in \widehat{k}^0$, neboť
$f_i'(x) = x^{k-i} e^x + (k-i) x^{k-i-1} e^x$ pro $i \in \{0, \dots, k-1\}$ a $f_k'(x) = (e^x)' = e^x$.

2. Označme $\mathcal{F} = (f_0, \dots, f_k)$ a určeme souřadnice $f, f_0', \dots, f_k'$ v bázi $\mathcal{F}$:
$$[f]_{\mathcal{F}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ [f_0']_{\mathcal{F}} = \begin{pmatrix} 1 \\ k \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ [f_1']_{\mathcal{F}} = \begin{pmatrix} 0 \\ 1 \\ k-1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ \dots \ , \ [f_k']_{\mathcal{F}} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$
Matice derivace $\frac{\mathrm{d}}{\mathrm{d}x}$ v bázi $\mathcal{F}$ má pak tvar
$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ k & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & k-1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}.$$

3. V dalším kroku opět určíme Jordanův kanonický tvar matice $\mathbf{D}$. Protože matice $\mathbf{D}$ je v dolním trojúhelníkovém tvaru, jejím charakteristickým polynomem je
$$\det(\mathbf{D} - \lambda \mathbf{I}) = (1 - \lambda)^n,$$
a tedy $\operatorname{Spec} \mathbf{D} = \{1\}$. Ihned vidíme, že vlastní podprostor $\mathbf{N}_1$ je jednodimenzionální (matice $\mathbf{D} - \mathbf{I}$ má totiž hodnost k). Není těžké si uvědomit, že matice $(\mathbf{D} - \mathbf{I})^2$ bude mít hodnost $k-1$, matice $(\mathbf{D} - \mathbf{I})^3$ bude mít hodnost $k-2$ atd., obecně matice $(\mathbf{D} - \mathbf{I})^j$, $j \in \widehat{k}$, bude mít hodnost $k - j + 1$. V takovém případě musí matice $\mathbf{D}$ mít tento Jordanův kanonický tvar:
$$\mathbf{J} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

Nyní nalezneme regulární matici $\mathbf{A} \in \mathcal{M}_k(\mathbb{R})$ takovou, že $\mathbf{D} = \mathbf{AJA}^{-1}$. Ta bude sestavená z lineárně nezávislých adjungovaných vektorů matice $\mathbf{D}$.[49] Nejdříve nalezneme adjungovaný vektor řádu 1, což je vlastní vektor matice $\mathbf{D}$ příslušící vlastnímu číslu $\lambda = 1$, jako řešení homogenní soustavy rovnic o matici

$$\mathbf{D} - \mathbf{I} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ k & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & k-1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 2 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

Dostáváme např. tento vlastní vektor:

$$\mathbf{a}_1 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Adjungovaný vektor $\mathbf{a}_2$ řádu 2, který tedy bude lineárně nezávislý s vektorem $\mathbf{a}_1$, nalezneme jako řešení nehomogenní soustavy rovnic $(\mathbf{D} - \mathbf{I})\mathbf{a}_2 = \mathbf{a}_1$, tj.

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ k & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & k-1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 2 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{21} \\ \vdots \\ a_{2,k+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Z ní dostáváme $a_{2i} = 0$ pro $i < k$ a $a_{2k} = 1$ ($a_{2,k+1}$ může být libovolné – volme např. $a_{2,k+1} = 0$). Máme tedy adjungovaný vektor $\mathbf{a}_2 = (0, \ldots, 0, 1, 0)^{\mathrm{T}}$. Adjungovaný vektor $\mathbf{a}_3$ řádu 3 najdeme jako řešení soustavy $(\mathbf{D} - \mathbf{I})\mathbf{a}_3 = \mathbf{a}_2$. Tím je například vektor

$$\mathbf{a}_3 = \frac{1}{2} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

[49] Adjungovaným vektorem řádu $m \in \widehat{k+1}$ matice $\mathbf{D}$ příslušící vlastnímu číslu λ rozumíme vektor $\mathbf{a} \in \mathbb{R}^{k+1}$ splňující

$$(\mathbf{D} - \lambda\mathbf{I})^m \mathbf{a} = \mathbf{0} \quad \text{a zároveň} \quad (\mathbf{D} - \lambda\mathbf{I})^{m-1} \mathbf{a} \neq \mathbf{0}.$$

Analogicky lze zjistit adjungované vektory všech řádů:

$$\mathbf{a}_4 = \frac{1}{3!}\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ 0\\ 0\end{pmatrix},\ \mathbf{a}_5 = \frac{1}{4!}\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ 0\\ 0\\ 0\end{pmatrix},\ \ldots\ \ \mathbf{a}_{k+1} = \frac{1}{k!}\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Z nich nyní sestavíme regulární matici

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & \cdots & 0 & \frac{1}{k!} \\ 0 & 0 & \cdots & \frac{1}{(k-1)!} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \frac{1}{1!} & \cdots & 0 & 0 \\ \frac{1}{0!} & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Snadno se ověří, že

$$\mathbf{A}^{-1} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0! \\ 0 & 0 & \cdots & 1! & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & (k-1)! & \cdots & 0 & 0 \\ k! & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Platí $\mathbf{D} = \mathbf{A}\mathbf{J}\mathbf{A}^{-1}$, a tedy i $\mathbf{D}^n = \mathbf{A}\mathbf{J}^n\mathbf{A}^{-1}$ (vizte předchozí příklad). Nyní využijeme znalosti mocniny Jordanovy buňky řádu $k+1$, kterou je vlastně naše matice $\mathbf{J}$:

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}^n = \begin{pmatrix} \lambda^n & \binom{n}{1}\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots & \binom{n}{k}\lambda^{n-k} \\ 0 & \lambda^n & \binom{n}{1}\lambda^{n-1} & \cdots & \binom{n}{k-1}\lambda^{n-k+1} \\ 0 & 0 & \lambda^n & \cdots & \binom{n}{k-2}\lambda^{n-k+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^n \end{pmatrix}.$$

Pro $\lambda = 1$ máme

$$\mathbf{J}^n = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{k} \\ 0 & 1 & \binom{n}{1} & \cdots & \binom{n}{k-1} \\ 0 & 0 & 1 & \cdots & \binom{n}{k-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Odtud

$$\mathbf{D}^n = \begin{pmatrix} 0 & 0 & \cdots & 0 & \frac{1}{k!} \\ 0 & 0 & \cdots & \frac{1}{(k-1)!} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \frac{1}{1!} & \cdots & 0 & 0 \\ \frac{1}{0!} & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{k} \\ 0 & 1 & \binom{n}{1} & \cdots & \binom{n}{k-1} \\ 0 & 0 & 1 & \cdots & \binom{n}{k-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 & 0! \\ 0 & 0 & \cdots & 1! & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & (k-1)! & \cdots & 0 & 0 \\ k! & 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \cdots & 0 & 0 & \frac{1}{k!}\binom{n}{0} \\ 0 & \cdots & 0 & \frac{1}{(k-1)!}\binom{n}{0} & \frac{1}{(k-1)!}\binom{n}{1} \\ 0 & \cdots & \frac{1}{(k-2)!}\binom{n}{0} & \frac{1}{(k-2)!}\binom{n}{1} & \frac{1}{(k-2)!}\binom{n}{2} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{1}{0!}\binom{n}{0} & \cdots & \frac{1}{0!}\binom{n}{k-2} & \frac{1}{0!}\binom{n}{k-1} & \frac{1}{0!}\binom{n}{k} \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 & 0! \\ 0 & 0 & \cdots & 1! & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & (k-1)! & \cdots & 0 & 0 \\ k! & 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{k!}{k!}\binom{n}{0} & 0 & 0 & \cdots & 0 \\ \frac{k!}{(k-1)!}\binom{n}{1} & \frac{(k-1)!}{(k-1)!}\binom{n}{0} & 0 & \cdots & 0 \\ \frac{k!}{(k-2)!}\binom{n}{2} & \frac{(k-1)!}{(k-2)!}\binom{n}{1} & \frac{(k-2)!}{(k-2)!}\binom{n}{0} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{k!}{0!}\binom{n}{k} & \frac{(k-1)!}{0!}\binom{n}{k-1} & \frac{(k-2)!}{0!}\binom{n}{k-2} & \cdots & \frac{0!}{0!}\binom{n}{0} \end{pmatrix}.$$

4. Nyní už jen určíme souřadnice $f^{(n)}$ v bázi $\mathcal{F}$:

$$[f^{(n)}]_{\mathcal{F}} = \mathbf{D}^n[f]_{\mathcal{F}} = \begin{pmatrix} \frac{k!}{k!}\binom{n}{0} & 0 & 0 & \cdots & 0 \\ \frac{k!}{(k-1)!}\binom{n}{1} & \frac{(k-1)!}{(k-1)!}\binom{n}{0} & 0 & \cdots & 0 \\ \frac{k!}{(k-2)!}\binom{n}{2} & \frac{(k-1)!}{(k-2)!}\binom{n}{1} & \frac{(k-2)!}{(k-2)!}\binom{n}{0} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{k!}{0!}\binom{n}{k} & \frac{(k-1)!}{0!}\binom{n}{k-1} & \frac{(k-2)!}{0!}\binom{n}{k-2} & \cdots & \frac{0!}{0!}\binom{n}{0} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{k!}{k!}\binom{n}{0} \\ \frac{k!}{(k-1)!}\binom{n}{1} \\ \frac{k!}{(k-2)!}\binom{n}{2} \\ \vdots \\ \frac{k!}{0!}\binom{n}{k} \end{pmatrix}.$$

Předpis n-té derivace funkce f je tedy

$$f^{(n)}(x) = k! \left(\sum_{j=0}^{k} \binom{n}{j} \frac{x^{k-j}}{(k-j)!} \right) e^x, \ x \in \mathbb{R}.$$

○

Kapitola 8

Lieova algebra derivací

V tomto odstavci se budeme zabývat další algebraickou strukturou, kterou derivace tvoří, a to sice Lieovou algebrou. Běžně se Lieova algebra definuje jako vektorový prostor s tzv. *Lieovou závorkou* (vizte níže). Protože se snažíme o co největší zobecnění, má pro nás význam zabývat se zobecněnou Lieovou algebrou jako levým modulem nad unitárním okruhem. Zřejmě každá Lieova algebra jakožto vektorový prostor je zobecněnou Lieovou algebrou (vizte poznámku 1.2).

Definice 8.1. Ať M je levý modul nad unitárním okruhem R a $[\cdot,\cdot]^a$ je bilineární zobrazení[b] na M splňující

(i) $\forall m \in M : [m,m] = o$ (alternativita),

(ii) $\forall m,n,p \in M : \big[m,[n,p]\big]+\big[n,[p,m]\big]+\big[p,[m,n]\big] = o$ (Jacobiho identita).

Pak M spolu se zobrazením $[\cdot,\cdot]$ nazveme *zobecněnou Lieovou algebrou nad unitárním okruhem R.*

[a] Toto zobrazení se nazývá *Lieova závorka.*

[b] Bilineárním zobrazením na modulu M nad unitárním okruhem R rozumíme zobrazení $\varphi : M \times M \to M$ splňující

(i) $\forall m,n,p \in M : \varphi(m+n,p) = \varphi(m,p)+\varphi(n,p) \quad \& \quad \varphi(m,n+p) = \varphi(m,n)+\varphi(m,p),$

(ii) $\forall m,n \in M\ \forall r \in R : \varphi(rm,n) = r\varphi(m,n) \quad \& \quad \varphi(m,rn) = r\varphi(m,n).$

Příklad 8.2. Mějme A asociativní algebru[50] nad unitárním okruhem R a $[\cdot,\cdot]$ komutátor na A, tj. zobrazení

$$[a,b] = ab - ba, \quad a,b \in A.$$

Ukažme, že $[\cdot,\cdot]$ je bilineárním zobrazením na A. zvolme $a,b,c \in A$ a $r \in R$ libovolně. Pak máme

(i)
$$[a+b,c] = (a+b)c - c(a+b) = ac + bc - ca - cb = [a,c] + [b,c].$$

Podobně bychom ukázali i $[a,b+c] = [a,b] + [a,c]$.

[50] Strukturu algebry zde potřebujeme, abychom uměli násobit prvky z A. Jak ale víme, tak algebra nad unitárním okruhem R je sama o sobě R-modulem (vizte definici 7.1).

(*ii*)

$$[ra, b] = (ra)b - b(ra) = rab - rba = r[a, b].$$

Opět by se $[a, rb] = r[a, b]$ ukázalo analogicky.

Nyní vyslovíme hlavní a jedinou větu této kapitoly.

Věta 8.3. *Ať A je algebra nad unitárním okruhem R. Pak $\mathfrak{Der}_\lambda(A)$ tvoří spolu s komutátorem $[\cdot, \cdot]$ zobecněnou Lieovu algebru nad R.*

Důkaz. Nejdříve si uvědomme, že $\mathfrak{Der}_\lambda(A)$ tvoří podmodul levého modulu $\mathfrak{End}_{\mathrm{mod}}(A)$ (věta 7.17), a tedy na $\mathfrak{Der}_\lambda(A)$ lze pohlížet také jako na levý modul nad R. Z lemmatu 6.3 víme, že komutátor $[\cdot, \cdot]$ je binární operace na $\mathfrak{Der}_+(A)$. Ukážeme, že $[\cdot, \cdot]$ je uzavřený na $\mathfrak{Der}_\lambda(A)$. Z aditivity lineárních A-derivací D_1 a D_2 plyne aditivita $[D_1, D_2] \in \mathfrak{Der}_+(A)$. Stačí tedy ukázat, že $[D_1, D_2]$ je homogenní derivace, tj. pro každé $r \in R$ a $a \in A$ platí

$$[D_1, D_2](ra) = r[D_1, D_2](a).$$

Počítejme:

$$[D_1, D_2](ra) = D_1D_2(ra) - D_2D_1(ra) \overset{(*)}{=} rD_1D_2a - rD_2D_1a = r[D_1, D_2](a),$$

kde $(*)$ plyne z linearity D_1 a D_2.

Nyní dokážeme vlastnostmi (*i*) a (*ii*) z definice 8.1.

(*i*) Nejdříve dokažme alternativitu. Pro $D \in \mathfrak{Der}_\lambda(A)$ platí $[D, D] = D^2 - D^2 = O$, kde O je nulová derivace, což je nulový prvek modulu $\mathfrak{Der}_\lambda(A)$, a to jsme chtěli.

(*ii*) V druhém kroku dokážeme, že platí Jacobiho identita. Zvolme libovolné lineární A-derivace D_1, D_2 a D_3 a počítejme:

$$\begin{aligned}
&\Big[D_1, [D_2, D_3]\Big] + \Big[D_2, [D_3, D_1]\Big] + \Big[D_3, [D_1, D_2]\Big] \\
&\quad = D_1[D_2, D_3] - [D_2, D_3]D_1 + D_2[D_3, D_1] \\
&\qquad - [D_3, D_1]D_2 + D_3[D_1, D_2] - [D_1, D_2]D_3 \\
&\quad = D_1D_2D_3 - D_1D_3D_2 - D_2D_3D_1 + D_3D_2D_1 + D_2D_3D_1 - D_2D_1D_3 \\
&\qquad - D_3D_1D_2 + D_1D_3D_2 + D_3D_1D_2 - D_3D_2D_1 - D_1D_2D_3 + D_2D_1D_3 \\
&\quad = O,
\end{aligned}$$

kde např. $D_1[D_2, D_3]$ zde pochopitelně značí zobrazení $D_1 \circ [D_2, D_3]$.

V definici 8.1 po Lieově závorce požadujeme bilinearitu. Dokažme ji tedy pro komutátor na $\mathfrak{Der}_\lambda(A)$.[51]

[51] Uvědomme si, že nelze použít argument, že bilinearita komutátoru plyne z příkladu 8.2. V něm jsme totiž dokázali, že každý komutátor na algebře A je bilineární zobrazení na A, ovšem $\mathfrak{Der}_\lambda(A)$ není algebrou! Důkaz se každopádně povede analogicky.

(i) Nejdříve dokažme aditivitu v prvním argumentu. Pro libovolné $r \in R$ platí

$$\begin{aligned}[D_1 + D_2, D_3](r) &= (D_1 + D_2)D_3 r - D_3(D_1 r + D_2 r) \\ &\overset{(*)}{=} D_1 D_3 r + D_2 D_3 r - D_3 D_1 r - D_3 D_2 r \\ &= [D_1, D_3](r) + [D_2, D_3](r),\end{aligned}$$

kde krok $(*)$ plyne z aditivity D_3 a z definice součtu derivací $D_1 + D_2$. Aditivita v druhém argumentu by se dokázala analogicky.

(ii) Nyní ukažme homogenitu v prvním argumentu. Pro r, $s \in R$ máme

$$\begin{aligned}[sD_1, D_2](r) &= (sD_1)D_2 r - \Big(D_2(sD_1)\Big)(r) \overset{(*)}{=} sD_1 D_2 r - sD_2 D_1 r \\ &= \Big(s[D_1, D_2]\Big)(r),\end{aligned}$$

kde $(*)$ plyne z definice skalárního násobku sD_1 a z homogenity D_2. Opět by se homogenita v druhém argumentu dokázala analogicky.

Víme tedy, že komutátor $[\cdot, \cdot]$ je bilineární zobrazení na $\mathfrak{Der}_\lambda(A)$, které splňuje vlastnosti (i) a (ii) definice 8.1 zobecněné Lieovy algebry. Celkem je tedy $\mathfrak{Der}_\lambda(A)$ spolu s komutátorem $[\cdot, \cdot]$ zobecněnou Lieovou algebrou nad okruhem R. ■

Kapitola 9

Logaritmická derivace

V této kapitole se budeme zabývat tzv. *logaritmickými derivacemi*. Uvidíme, že tato zobrazení budou mít důležitý význam při zkoumání vlastností aditivní grupy derivací definovaných na tělese. Nejdříve ale motivujme definici tohoto nového pojmu. Ta je inspirovaná derivací složené funkce $\ln f$ pro $f \in \mathcal{C}^1(\Omega)$, $f > 0$ na otevené množině Ω. Totiž využitím pravidla o derivaci složené funkce máme

$$\frac{\mathrm{d}}{\mathrm{d}x} \ln f = \frac{1}{f} \frac{\mathrm{d}f}{\mathrm{d}x}.$$

V tomto odstavci se budeme zabývat (R, M)-derivacemi, které jsou definované na komutativním unitárním okruhu R (proč předpokládáme komutativitu násobení uvidíme později). Protože ale v R-bimodulu M obecně neplatí, že $rm = mr$ pro každé $m \in M$ a $r \in R$, rozlišíme tzv. levou a pravou logaritmickou derivaci. Vizte následující definici.

Definice 9.1. Ať M je bimodul nad komutativním unitárním okruhem R a D je (R, M)-derivace. Pak zobrazení označované ${}_D\mathrm{ld}$, resp. ld_D, a definované předpisem

$${}_D\mathrm{ld}(r) = r^{-1}Dr, \quad r \in R^\times,$$

resp.

$$\mathrm{ld}_D(r) = (Dr)r^{-1}, \quad r \in R^\times,$$

nazýváme *levou*, resp. *pravou*, *logaritmickou derivací indukovanou derivací* D.

Poznámka 9.2. Uvědomme si, že pokud je M symetrickým R-bimodulem, pak ${}_D\mathrm{ld} = \mathrm{ld}_D$. V takovém případě, bude-li zřejmé, která derivace indukuje danou logaritmickou derivaci, se také místy uchýlíme k úspornějšímu značení ld namísto ${}_D\mathrm{ld}$, resp. ld_D.

Poznámka 9.3. Je-li M vektorovým prostorem nad komutativním tělesem R, pak je ${}_D\mathrm{ld}(r) = \mathrm{ld}_D(r)$ definováno pro všechna $r \in R \setminus \{0\}$.

Příklad 9.4. Ať R je komutativní unitární okruh, M je R-bimodul a $m \in M$. Nalezněme předpis levé, resp. pravé, logaritmické derivace indukované vnitřní derivací $D_m \in \mathfrak{IDer}(R, M)$, kterou označíme ${}_m\mathrm{ld}$, resp. ld_m. Pro libovolné $r \in R^\times$ pak máme

$${}_m\mathrm{ld}(r) = (D_m r)r^{-1} = (rm - mr)r^{-1} = rmr^{-1} - m.$$

Symetricky pro pravou logaritmickou derivaci dostáváme

$$\mathrm{ld}_m(r) = r^{-1}D_m r = r^{-1}(rm - mr) = m - r^{-1}mr.$$

Odtud ${}_m\mathrm{ld} : r \mapsto rmr^{-1} - m$ a $\mathrm{ld}_m : r \mapsto m - r^{-1}mr$.

V následující větě si uvedeme základní vlastnosti logaritmických derivací.

Věta 9.5. *Ať M je bimodul nad komutativním unitárním okruhem R a D je (R, M)-derivace. Pak pro levou a pravou logaritmickou derivaci indukovanou derivací D platí*

(i) ${}_D\mathrm{ld}(1) = o = \mathrm{ld}_D(1)$,

(ii) $\forall r \in R^\times : {}_D\mathrm{ld}(-r) = {}_D\mathrm{ld}(r) \quad \& \quad \mathrm{ld}_D(-r) = \mathrm{ld}_D(r)$,

(iii) $\forall r \in R^\times : {}_D\mathrm{ld}(r^{-1}) = -\mathrm{ld}_D(r) \ \& \ \mathrm{ld}_D(r^{-1}) = -{}_D\mathrm{ld}(r)$,

(iv) $\forall r \in R^\times : r\,{}_D\mathrm{ld}(r) = \mathrm{ld}_D(r)r$.

Je-li navíc $rm = mr$ pro libovolné $r \in R^\times$ a $m \in M$, pak platí

(v) $\forall r, s \in R^\times : {}_D\mathrm{ld}(rs) = {}_D\mathrm{ld}(r) + {}_D\mathrm{ld}(s) \ \& \ \mathrm{ld}_D(rs) = \mathrm{ld}_D(r) + \mathrm{ld}_D(s)$,

(vi) $\forall r, s \in R^\times : {}_D\mathrm{ld}\,(rs^{-1}) = {}_D\mathrm{ld}(r) - \mathrm{ld}_D(s)$
$\& \quad \mathrm{ld}_D\,(rs^{-1}) = \mathrm{ld}_D(r) - {}_D\mathrm{ld}(s)$.

Důkaz. Důkaz (i) až (iii) provedeme pouze pro levé logaritmické derivace (pro pravé by se postupovalo symetricky).

Vlastnost (i) plyne z následujícího (jistě $1 \in R^\times$):

$${}_D\mathrm{ld}(1) = 1^{-1}D1 = 1o = o.$$

Zvolme $r \in R^\times$ libovolně a dokažme (ii). Platí

$${}_D\mathrm{ld}(-r) = (-r)^{-1}D(-r) \overset{(*)}{=} r^{-1}Dr = {}_D\mathrm{ld}(r),$$

kde $(*)$ plyne z toho, že $(-r)^{-1} = -r^{-1}$ a ze vztahu (2.1).

Ukažme (iii):

$${}_D\mathrm{ld}(r^{-1}) = (r^{-1})^{-1}Dr^{-1} \overset{(*)}{=} r\Big(-r^{-1}(Dr)r^{-1}\Big) = -(Dr)r^{-1} = \mathrm{ld}_D\, r,$$

kde $(*)$ plyne z z poznámky 2.27 o derivaci inverzních prvků.

Vlastnost (iv), která popisuje vztah mezi ${}_D\mathrm{ld}$ a ld_D, dokážeme následovně:

$$r\,{}_D\mathrm{ld}(r) = rr^{-1}Dr = Dr = (Dr)r^{-1}r = \mathrm{ld}_D(r)r.$$

Nyní navíc předpokládejme, že $rm = mr$ pro libovolné $r \in R^\times$ a $m \in M$, a dokažme (v) (opět pouze pro levé logaritmické derivace). Volme proto navíc $s \in R^\times$ libovolně a počítejme:

$${}_D\mathrm{ld}(rs) = (rs)^{-1}D(rs) \overset{(a)}{=} r^{-1}s^{-1}\Big((Dr)s + rDs\Big) \overset{(b)}{=} r^{-1}Dr + s^{-1}Ds = {}_D\mathrm{ld}(r) + {}_D\mathrm{ld}(s),$$

kde (a) plyne z komutativity násobení v okruhu R a (b) z dodatečného předpokladu $rm = mr$ pro $r \in R^\times$ a $m \in M$.

Konečně vlastnost (vi) okamžitě vyplývá z vlastností (iii) a (v). ■

Poznámka 9.6. Vlastnost (iv) věty 9.5 lze přeformulovat taky tak, že pro libolné $r \in R^\times$ platí

$$ {}_D\mathrm{ld}(r) = r^{-1}\,\mathrm{ld}_D(r)r, \quad \text{resp.} \quad \mathrm{ld}_D(r) = r\,{}_D\mathrm{ld}(r)r^{-1}. $$

Nadále se budeme zabývat jen symetrickými bimoduly M nad komutativním unitárním okruhem R. V takovém případě je pak dodatečná podmínka $rm = mr$ pro $r \in R^\times$ a $m \in M$ uvedená ve větě 9.5 triviálně splněna. Povšimněme si, že logaritmická derivace převadí násobení prvků z R na sčítání prvků z M. Dále si uvědomme, že $R^\times$ je podmonoidem[52] komutativního monoidu $(R \setminus \{0\}, \cdot)$. Opravdu $1 \in R^\times$ a jsou-li $r, s \in R^\times$, tak i $rs \in R^\times$, neboť $(rs)^{-1} = r^{-1}s^{-1}$. Protože navíc každý prvek $R^\times$ má inverzi (a ta jistě leží v $R^\times$), tak $(R^\times, \cdot)$[53] je komutativní grupa. Platí tedy následující věta.

Věta 9.7. *Ať M je symetrický bimodul nad komutativním unitárním okruhem R a D je (R, M)-derivace. Pak logaritmická derivace ld_D je homomorfismem grup $(R^\times, \cdot)$ a $(M, +)$.*

Poznámka 9.8. Z věty 9.7 také plyne, že pokud je R komutativním tělesem, tak ld_D je homomorfismus grup $(R \setminus \{0\}, \cdot)$ a $(M, +)$.

Vidíme tedy, že každá derivace definovaná na komutativním okruhu indukuje nějaký homomorfismus multiplikativní grupy $(R^\times, \cdot)$ do aditivní grupy $(M, +)$. Přirozeně se nabízí otázka, zda každý takový homomorfismus grup indukuje nějakou derivaci. Protože se jedná o homomorfismy právě těchto výše uvedných grup (ne tedy libovolných grup), je jasné, že problémové budou ty okruhy, ve kterých je $R^\times$ „moc malá“ množina, tj. hodně prvků z R nemá inverzi. Logaritmická derivace je totiž definovaná pouze na invertibilních prvcích, a tedy derivaci indukovanou tímto homomorfismem bychom museli na neinvertibilních prvcích dodefinovat (ideálně nějakým přirozeným způsobem). Tímto se budeme zabývat až v závěru této kapitoly.

Omezme se proto v tomto smyslu na nejjednodušší situaci, tj. na homomorfismy grup $(T^\times, \cdot)$ a $(V, +)$, kde V je vektorový prostor nad komutativním tělesem T. Pak totiž $T^\times = T \setminus \{0\}$. Vezměme libovolný homomorfismus $\lambda : T^\times \to V$ a definujme zobrazení $D_\lambda : T \to V$ předpisem

$$ D_\lambda t = \begin{cases} t\lambda(t), & t \in T^\times \\ o, & t = 0 \end{cases} $$

Následující věta říká, že takto definované zobrazení bude (T, V)-derivací.

[52] Podmonoidem monoidu $(A, \cdot)$ s neutrálním prvkem e rozumíme podmnožinu $B \subseteq A$, pro kterou je splněno

(i) $e \in B$,

(ii) $\forall a, b \in B : ab \in B$.

[53] Přesněji $(R^\times, \cdot|_{R^\times})$ je komutativní grupa.

Věta 9.9. *Ať V je vektorový prostor nad komutativním tělesem T a λ je homomorfismus grup $(T^\times, \cdot)$ a $(V, +)$. Pak zobrazení $D_\lambda : T \to V$ definované předpisem*

$$D_\lambda t = \begin{cases} t\lambda(t), & t \in T^\times \\ o, & t = 0 \end{cases}$$

je (T, V)-derivací.

Důkaz. Ukážeme, že D_λ splňuje Leibnizovu formuli. Rozlišme následující případy:

(*i*) Ať $t, s \in T^\times$. Pak

$$D_\lambda(ts) = ts\lambda(ts) = t\lambda(t)s + ts\lambda(s) = sD_\lambda t + tD_\lambda s.$$

(*ii*) Bez újmy na obecnosti ať $t = 0$. Pak

$$D_\lambda(ts) = D_\lambda 0 = o = so + 0D_\lambda s = sD_\lambda t + tD_\lambda s.$$

Tím je důkaz věty u konce. ■

Takto definovaná derivace bude mít svůj název. Vizte následující definici.

Definice 9.10. Ať V je vektorový prostor nad komutativním tělesem T a λ je homomorfismus grup $(T^\times, \cdot)$ a $(V, +)$. Pak derivaci $D_\lambda : T \to V$ definovanou ve větě 9.9 nazýváme *derivací indukovanou homomorfismem* λ.

Věta 9.9 nám dává návod, jak na daném komutativním unitárním okruhu nalézt nějakou derivaci. Tento postup si ukažme na následujícím příkladě.

Příklad 9.11. Uvažme komutativní těleso reálných čísel $\mathbb{R}$. Chceme najít nějakou derivaci $\mathbb{R} \to \mathbb{R}$. S ohledem na větu 9.9 stačí najít nějaký homomorfismus grup $(\mathbb{R}\setminus\{0\}, \cdot)$ a $(\mathbb{R}, +)$ ($\mathbb{R}$ lze chápat jako jednodimenzionální vektorový prostor nad tělesem $\mathbb{R}$). Takovým homomorfismem může být kupříkladu funkce

$$\lambda(x) = \ln|x|, \ x \in \mathbb{R}\setminus\{0\}.$$

Ověřme, že se opravdu jedná o homomorfismus. Zvolme $x, y \in \mathbb{R}\setminus\{0\}$ libovolně. Pak platí

$$\lambda(xy) = \ln|xy| = \ln(|x||y|) = \ln|x| + \ln|y| = \lambda(x) + \lambda(y),$$

a to jsme chtěli. Dle věty 9.9 je funkce $D_\lambda : \mathbb{R} \to \mathbb{R}$ definovaná předpisem

$$D_\lambda(x) = \begin{cases} x\ln|x|, & x \in \mathbb{R}\setminus\{0\} \\ 0, & x = 0 \end{cases}$$

$\mathbb{R}$-derivací. Opravdu platí Leibnizova formule:

$$D_\lambda(xy) = xy\ln|xy| = xy\ln(|x||y|) = xy\ln|x| + xy\ln|y| = y\,D_\lambda\,x + x\,D_\lambda\,y.$$

Povšimněme si, že tato derivace není aditivní. To je vidět z následujícího výpočtu (e zde značí Eulerovo číslo):

$$D_\lambda(e+e) = D_\lambda(2e) = 2e\ln(2e) = 2e(\ln 2 + 1) \neq 2e = e\ln e + e\ln e = D_\lambda\, e + D_\lambda\, e.$$

Příklad 9.12. V předešlém příkladě jsme našli derivaci na $\mathbb{R}$. Inspirujme se jím pro nalezení „další“ derivace (jiné než $\frac{\mathrm{d}}{\mathrm{d}x}$ nebo $\frac{\partial}{\partial \boldsymbol{\nu}}$) na prostoru funkcí. Označme $\mathcal{F}(\Omega)$ množinu všech funkcí $f : \Omega \to \mathbb{R}$, kde $\emptyset \neq \Omega \subseteq \mathbb{R}^N, N \in \mathbb{N}$. Je zřejmé, že $\mathcal{F}(\Omega)$ tvoří spolu se sčítáním funkcí a násobením funkcí komutativní unitární okruh s jednotkou $\mathbb{1}_\Omega$, a proto každé zobrazení $\mathcal{F}(\Omega) \to \mathcal{F}(\Omega)$ splňující Leibnizovu formuli je $\mathcal{F}(\Omega)$-derivací. Definujme operátor $D : \mathcal{F}(\Omega) \to \mathcal{F}(\Omega)$, který funkci f přiřadí funkci s předpisem[54] (srovnejte s předpisem $\mathbb{R}$-derivace v předchozím příkladě 9.11)

$$Df(\mathbf{x}) = \begin{cases} f(\mathbf{x})\ln|f(\mathbf{x})|, & \mathbf{x} \in \Omega \setminus f^{-1}(\{0\}) \\ 0, & \mathbf{x} \in f^{-1}(\{0\}) \end{cases}$$

Ukážeme, že se opravdu jedná o $\mathcal{F}(\Omega)$-derivaci. Volme proto dvě funkce $f, g \in \mathcal{F}(\Omega)$ libovolně a ukažme platnost Leibnizovy formule. Pro $\mathbf{x} \in \Omega \setminus (f^{-1}(\{0\}) \cup g^{-1}(\{0\}))$ máme

$$\begin{aligned} D(fg)(\mathbf{x}) &= f(\mathbf{x})g(\mathbf{x})\ln|f(\mathbf{x})g(\mathbf{x})| = f(\mathbf{x})g(\mathbf{x})\ln|f(\mathbf{x})| + f(\mathbf{x})g(\mathbf{x})\ln|g(\mathbf{x})| \\ &= g(\mathbf{x})Df(\mathbf{x}) + f(\mathbf{x})Dg(\mathbf{x}). \end{aligned}$$

Toto ostatně plyne i z příkladu 9.11, neboť sčítání a násobení funkcí je definováno bodově. Nyní ať $\mathbf{x} \in f^{-1}(\{0\}) \cup g^{-1}(\{0\})$, tj. $f(\mathbf{x}) = 0$ nebo $g(\mathbf{x}) = 0$. Pak i $f(\mathbf{x})g(\mathbf{x}) = 0$ a

$$D(fg)(\mathbf{x}) = 0 = g(\mathbf{x})Df(\mathbf{x}) + f(\mathbf{x})Dg(\mathbf{x}).$$

Tato derivace není aditivní, neboť není aditivní ani $\mathbb{R}$-derivace z příkladu 9.11.

Nyní si uvědomme, že jsme zkonstruovali netriviální derivaci (tj. zobrazení, které splňuje Leibnizovu formuli) funkcí, která jistě není tatáž jako běžná derivace (ta je totiž aditivní). Přesněji je-li $\Omega \subseteq \mathbb{R}^N$ otevřená množina, pak

$$D|_{\mathcal{C}^1(\Omega)} \neq \frac{\mathrm{d}}{\mathrm{d}x} \quad \text{pro } N = 1 \qquad \text{a} \qquad D|_{\mathcal{C}^1(\Omega)} \neq \frac{\partial}{\partial \boldsymbol{\nu}},\ \boldsymbol{\nu} \in \mathbb{R}^N \setminus \{\mathbf{0}\}, \quad \text{pro } N > 1.$$

Víme tedy, že každé derivaci $T \to V$, kde V je vektorový prostor nad komutativním tělesem T, přísluší nějaký homomorfismus grup $(T^\times, \cdot)$ a $(V, +)$ (věta 9.7), ale taky každý homomorfismus grup $(T^\times, \cdot)$ a $(V, +)$ indukuje nějakou derivaci $T \to V$ (věta 9.9). Naskýtá se přirozená otázka, zda je tato korespondence jednoznačná, tj. zda mezi množinou homomorfismů $\mathfrak{Hom}(T^\times, V)$ výše uvedených grup a množinou derivací $\mathfrak{Der}(T, V)$ existuje bijekce. Ptejme se proto, zda zobrazení $\mathfrak{Hom}(T^\times, V) \to \mathfrak{Der}(T, V)$, které homomorfismu λ přiřadí derivaci D_λ indukovanou homomorfismem λ, je bijekcí.

[54] Symbolem $f^{-1}(\{0\})$ značíme množinu všech $\mathbf{x} \in \Omega$ takových, že $f(\mathbf{x}) = 0$.

(*i*) Ukažme, že je injektivní. Zvolme proto dva homomorfismy $\lambda, \mu \in \mathfrak{Hom}(T^\times, V)$ takové, že $D_\lambda = D_\mu$. Pro každé $t \in T$ tedy platí $D_\lambda t = D_\mu t$, což využitím definice derivace indukované homomorfismem grup znamená

$$t\lambda(t) = t\mu(t) \quad \text{pro} \quad t \neq 0.$$

Odtud

$$t\Big(\lambda(t) - \mu(t)\Big) = o.$$

Protože $t \neq 0$, tak $\lambda(t) = \mu(t)$ pro všechna $t \in T^\times$, a tedy $\lambda = \mu$.

(*ii*) V druhém kroku ukážeme, že se jedná o surjekci. Zvolme libovolnou derivaci $D \in \mathfrak{Der}(T, V)$ a ať ld_D je logaritmická derivace indukovaná D. Pak

$$D_{\mathrm{ld}_D} t = \begin{cases} tt^{-1}Dt = Dt, & t \neq 0 \\ o, & t = 0 \end{cases}$$

tj. $D_{\mathrm{ld}_D} = D$, a tedy našli jsme homomorfismus, který indukuje D.

Zobrazení $\lambda \mapsto D_\lambda$ je proto bijekcí $\mathfrak{Hom}(T^\times, V)$ na $\mathfrak{Der}(T, V)$. Ve (*ii*) jsme taky ukázali

$$D_{\mathrm{ld}_D} = D,$$

pro libovolnou derivaci $D \in \mathfrak{Der}(T, V)$. Podobně pro libovolný homomorfismus $\lambda \in \mathfrak{Hom}(T^\times, V)$ platí

$$\mathrm{ld}_{D_\lambda} = \lambda.$$

Opravdu pro každé $t \in T^\times$ máme

$$\mathrm{ld}_{D_\lambda}(t) = t^{-1} D_\lambda t = t^{-1} t\lambda(t) = \lambda(t).$$

Nyní ukážeme, že zobrazení $\lambda \mapsto D_\lambda$ je dokonce izomorfismem grup $\mathfrak{Hom}(T^\times, V)$ a $\mathfrak{Der}(T, V)$. Zde je ale potřeba upřesnit, jaké operace definované na těchto nosičích máme na mysli. Grupu $\mathfrak{Der}(T, V)$ chápeme jako aditivní grupu, tj. operací na $\mathfrak{Der}(T, V)$ je sčítání derivací z definice 6.1. Na $\mathfrak{Hom}(T^\times, V)$ definujeme násobení homomorfismů takto:

$$(\lambda\mu)(t) = \lambda(t) + \mu(t), \ t \in T^\times. \tag{9.1}$$

Ukažme, že $\mathfrak{Hom}(T^\times, V)$ spolu s touto operací tvoří komutativní grupu.

(*i*) V prvním kroku ukažme komutativitu. Zvolme proto $\lambda, \mu \in \mathfrak{Hom}(T^\times, V)$ a $t \in T^\times$ a počítejme:

$$(\lambda\mu)(t) = \lambda(t) + \mu(t) = \mu(t) + \lambda(t) = (\mu\lambda)(t),$$

tedy komutativita násobení homomofimů plyne z komutativity sčítání na V.

(*ii*) Asociativita násobení na $\mathfrak{Hom}(T^\times, V)$ podobně jako v (*i*) plyne z asociativity sčítání na V.

(*iii*) Jednotkou v $\mathfrak{Hom}(T^\times, V)$ je homomorfimsus $\iota : t \mapsto o$.

(*iv*) Inverzí k $\lambda \in \mathfrak{Hom}(T^\times, V)$ je homomorfismus $\lambda^{-1} : t \mapsto -\lambda(t),\ t \in T^\times$.

Stačí ukázat, že zobrazení $\lambda \mapsto D_\lambda$ zachovává výše uvedené grupové operace. Zvolme dva libovolné homomorfismy $\lambda, \mu \in \mathfrak{Hom}(T^\times, V)$ a $t \in T^\times$ a počítejme:

$$D_{\lambda\mu}t = t(\lambda\mu)(t) = t\lambda(t) + t\mu(t) = D_\lambda t + D_\mu t.$$

Pro $t = 0$ dostáváme

$$D_{\lambda\mu}0 = o = D_\lambda 0 + D_\mu 0.$$

Odvodili jsme tak platnost následující věty.

Věta 9.13. *Ať V je vektorový prostor nad komutativním tělesem T. Pak multiplikativní grupa všech homomorfismů multiplikativní grupy $T^\times$ do aditivní grupy V spolu s násobení homomorfismů definovaným v* (9.1) *je izomorfní aditivní grupě všech (T, V)-derivací spolu se sčítáním derivací, tj. platí*

$$\Big(\mathfrak{Hom}(T^\times, V), \cdot\Big) \cong \Big(\mathfrak{Der}(T, V), +\Big).$$

Příslušným izomorfismem je zobrazení

$$\begin{aligned} \mathfrak{Hom}(T^\times, V) &\to \mathfrak{Der}(T, V) \\ \lambda &\mapsto D_\lambda \end{aligned}$$

Poznámka 9.14. Věta 9.13 nám říká, že struktura derivací definovaných jako zobrazení komutativního tělesa T do vektorového prostoru V nad tělesem T je jen kopií struktury homomorfismů multiplikativní grupy $T^\times$ do aditivní grupy V.

Věta 9.13 má i ryze algebraický důsledek:

Důsledek 9.15. *Ať V je vektorový prostor nad komutativním tělesem T charakteristiky různé od 2. Pak neexistuje vnoření multiplikativní grupy $(T^\times, \cdot)$ do aditivní grupy $(V, +)$.*

Důkaz. Ať λ je libovolný homomorfismus grup $(T^\times, \cdot)$ a $(V, +)$. Z odvození věty 9.13 plyne, že $\lambda = \mathrm{ld}_{D_\lambda}$, kde D_λ je (T, V)-derivace indukovaná homomorfismem λ. Pro $t \in T^\times$ lze tedy psát

$$\lambda(t) = t^{-1} D_\lambda t.$$

Z věty 2.17 víme, že $D_\lambda 1 = o = D_\lambda(-1)$, a tedy

$$\lambda(1) = 1 D_\lambda 1 = o = -1 D_\lambda(-1) = \lambda(-1).$$

Protože $\operatorname{char} T \neq 2$, tak $1 \neq -1$. Totiž pokud by $1 = -1$, tak máme

$$0 = 1 - 1 = 1 + 1 = 2 \cdot 1,$$

a tedy $\operatorname{char} T = 2$, což je spor. Proto λ není injektivní homomorfismus. ∎

Poznámka 9.16. Z důsledku 9.15 taky plyne, že neexistuje vnoření multiplikativní grupy $(T, \cdot)$ do aditivní grupy $(T, +)$ (T chápeme jako vektorový prostor nad T).

Následující věta říká, jakou vlastnost má logaritmická derivace indukovaná aditivní (R, M)-derivací.

Věta 9.17. *Ať R je unitární okruh, M je symetrický R-bimodul, D je aditivní (R, M)-derivace a* ld *je logaritmická derivace indukovaná derivací D. Pak platí*

$$\forall r, s \in R^\times : (r+s)\,\mathrm{ld}(r+s) = r\,\mathrm{ld}(r) + s\,\mathrm{ld}(s).$$

Důkaz. Ať jsou splněny předpoklady tvrzení. Pak platí

$$(r+s)\,\mathrm{ld}(r+s) = D(r+s) = Dr + Ds = r\,\mathrm{ld}(r) + s\,\mathrm{ld}(s).$$

■

Příklad 9.18. Ilustrujme platnost věty 9.17 na příkladě. Ať $\Omega \subseteq \mathbb{R}$ je otevřená množina. Pak předpis logaritmická derivace $\mathrm{ld} = \mathrm{ld}_{\frac{\mathrm{d}}{\mathrm{d}x}}$ příslušící aditivní derivaci $\frac{\mathrm{d}}{\mathrm{d}x} : \mathcal{C}^1(\Omega) \to \mathcal{C}(\Omega)$ vypadá následovně:

$$\mathrm{ld}(f) = \frac{1}{f}\frac{\mathrm{d}f}{\mathrm{d}x}, \quad f \in \mathcal{C}^1(\Omega), f \neq 0 \text{ na } \Omega.$$

Totiž množina $\{f \in \mathcal{C}^1(\Omega) \mid f \neq 0 \text{ na } \Omega\}$ je právě $\mathcal{C}^1(\Omega)^\times$.

Volme nyní funkce $f, g \in \mathcal{C}^1(\Omega), f, g \neq 0$ na Ω, libovolně a ilustrujme platnost vztahu ve větě 9.19:

$$(f+g)\,\mathrm{ld}(f+g) = (f+g)\frac{1}{f+g}\left(\frac{\mathrm{d}f}{\mathrm{d}x} + \frac{\mathrm{d}g}{\mathrm{d}x}\right) = \frac{\mathrm{d}f}{\mathrm{d}x} + \frac{\mathrm{d}g}{\mathrm{d}x} = f\,\mathrm{ld}\,f + g\,\mathrm{ld}\,g.$$

Pokud je D (T, V)-derivace, kde V je vektorový prostor nad komutativním tělesem T, pak platí i obrácená implikace k implikaci uvedené ve větě 9.17. Vizte následující větu.

Věta 9.19. *Ať V je vektorový prostor nad komutativním tělesem T. Pak (T, V)-derivace je aditivní, právě když jí indukovaná logaritmická derivace* ld *splňuje podmínku*

$$\forall t, s \in T^\times : (t+s)\,\mathrm{ld}(t+s) = t\,\mathrm{ld}(t) + s\,\mathrm{ld}(s).$$

Důkaz. Volme libovolnou (T, V)-derivaci D a ať ld je logaritmická derivace jí indukovaná. Předpokládejme, že ld splňuje podmínku

$$\forall t, s \in T^\times : (t+s)\lambda(t+s) = t\lambda(t) + s\lambda(s).$$

Pak máme

$$D(t+s) = (t+s)\,\mathrm{ld}(t+s) = t\,\mathrm{ld}(t) + s\,\mathrm{ld}(s) = D_{\mathrm{ld}}\,t + D_{\mathrm{ld}}\,s,$$

a tedy D je aditivní (T, V)-derivace. ■

Jak bylo slíbeno výše, zabývejme se nyní otázkou, zda lze každým homomorfismem $\lambda : R^\times \to M$, kde M je symetrický bimodul nad komutativním unitárním okruhem R, indukovat nějakou (R, M)-derivaci. Inspirujme se definicí D_λ v případě, kdy M byl vektorový prostor nad komutativním tělesem R, a položme

$$D_\lambda r = \begin{cases} r\lambda(r), & r \in R^\times \\ o, & r \in R \setminus R^\times \end{cases}$$

Chtěli bychom, aby takto definované zobrazení splňovalo Leibnizovu formuli. Případ $r,\ s \in R^\times$ již vlastně máme vyřešený (v důkazu věty 9.9 jsme v bodě (i) nijak nevyužili faktu, že T je těleso). Bez újmy na obecnosti ať $r \notin R^\times$. Pak i $rs \notin R^\times$. Kdyby totiž existoval prvek $t \in R$ takový, že $(rs)t = 1$, s ohledem na asociativitu násobení by to znamenalo, že $r^{-1} = st$. Ovšem my předpokládáme, že r inverzi nemá! Platí tedy $D_\lambda(rs) = o$. Chceme ukázat, že i

$$sD_\lambda r + rD_\lambda s = o.$$

Protože $r \notin R^\times$, tak $D_\lambda r = o$. Pokud by i $s \notin R^\times$, Leibnizova formule platí. Zbývá nám případ $r \notin R^\times$ a $s \in R^\times$. Z předpisu D_λ máme

$$rD_\lambda s = rs\lambda(s).$$

Protože $s \in R^\times$, tak

$$rs\lambda(s) = o, \qquad \text{právě když} \qquad r\lambda(s) = o.$$

Dostáváme tak, že výše definované zobrazení D_λ je (R, M)-derivací, právě když pro homomorfismus λ platí

$$\forall r \in R \setminus R^\times\ \forall s \in R^\times : r\lambda(s) = o. \tag{9.2}$$

V tuto chvíli se nabízejí další otázky, na které již v této práci nezbylo místo:

(i) Existuje nějaký homomorfismus $\lambda : R^\times \to M$ splňující podmínku (9.2)?

(ii) Lze obrazy neinvertibilních prvků z R v zobrazení D_λ dodefinovat nějakým jiným způsobem tak, aby D_λ byla (R, M)-derivace?

Závěr

Základní motivací pro tuto práci bylo prozkoumat vlastnosti zobrazení splňujících pouze a jenom Leibnizovu formuli.

V kapitole 2 se povedlo definovat abstraktní derivaci ve velice obecné formě, a to včetně požadavků na algebraické struktury, na kterých je toto zobrazení definováno. I v této zobecněné verzi se povedlo s pomocí [1, Chapter 4] ukázat několik známých vlastností derivací z diferenciálního počtu. Na ty lze tedy pohlížet jako na důsledky platnosti Leibnizovy formule (jak bylo předsevzato v úvodu této práce).

V téže kapitole bylo představeno několik základních příkladů derivací (včetně běžných derivací na prostorech funkcí) a v kapitole 4 se uvedly první příklady neaditivních derivací na číselných oborech. Ukázalo se tak, že pojem neaditivní derivace není prázdný. Naopak takových derivací může existovat mnoho (např. všech $\mathbb{Z}$-derivací je přesně tolik, kolik je reálných čísel, přitom z nich je jen jediná aditivní – je jí triviální derivace $O_{\mathbb{Z}}$). Konstrukce derivací na číselných oborech byla přirozeně zobecněna na libovolné obory integrity s jednoznačným rozkladem v kapitole 5. Ukázalo se tak, že na každém oboru integrity s jednoznačným rozkladem existuje nějaká derivace, a je dokonce znám její předpis. Ve stejné kapitole vyvstaly některé v této práci nezodpovězené otázky, a to sice zda existuje ještě další způsob (mimo ten, který je uveden v závěru kapitoly 5), jak předepsat obrazy jednotek dělení různých od 1 a -1 a pevně zvolených zástupců tříd vzájemně asociovaných ireducibilních prvků tak, aby daná derivace měla na těchto prvcích předepsané obrazy, a zda lze tímto způsobem zkonstruovat každou derivaci na oboru integrity s jednoznačným rozkladem. V kladném případě by patrně šel (podobně jako u $\mathbb{Z}$-derivací) charakterizovat počet aditivních derivací na této struktuře. V kapitole 3 bylo dále představeno jednoznačné rozšíření každé derivace definované na oboru integrity na podílové těleso tohoto oboru integrity, tzv. podílové rozšíření derivace.

Mimo derivace na oborech integrity s jednoznačným rozkladem byly také zkoumány derivace na zobecněných asociativních algebrách (tj. na asociativních algebrách obecně i nad nekomutativními okruhy) v kapitole 7. Největší zřetel byl brán na lineární derivace, na které lze pohlížet jako na zobrazení, která jsou současně derivacemi i endomorfismy na modulech. Díky této skutečnosti lze derivování prvků převést na maticové násobení, čehož bylo využito při řešení úlohy o nalezení explicitního předpisu libovolné derivace některých nekonečně spojitě diferencovatelných funkcí.

V kapitole 6 byly na množině derivací zavedeny nové operace, s nimiž tato množina tvořila některé algebraické struktury:

- aditivní grupa $\mathfrak{Der}(R, M)$ spolu se sčítáním derivací,
- R-bimodul $\mathfrak{Der}(R, M)$ spolu s násobením derivací prvky z okruhu R a

- zobecněná Lieova algebra lineárních derivací $\mathfrak{Der}_\lambda(A)$ na algebře A spolu s komutátorem $[\cdot,\cdot]$.

V kapitole 9 o logaritmické derivaci byla ukázána úzká souvislost mezi aditivní grupou derivací a multiplikativní grupou homomorfismů z multiplikativní grupy okruhu do aditivní grupy modulu nad tímto okruhem. Konkrétně pro derivace definované jako zobrazení z komutativního tělesa T do vektorového prostoru V nad tělesem T byl nalezen izomorfismus grupy $(\mathfrak{Hom}(T^\times, V), \cdot)$ na grupu $(\mathfrak{Der}(T, V), +)$. Nevyřešenou otázkou je, zda lze podobnou souvislost mezi výše uvedenými grupami derivací a homomorfismů nalézt i v případě obecnějších struktur, tj. modulů nad obory integrity či dokonce obecně nad libovolnými okruhy.

Dodatek

V dodatku této práce, jak bylo avizováno v úvodu kapitoly 1 o modulech nad okruhy, uvedeme další pojmy, které lze definovat v levých modulech, a ukážeme jejich základní vlastnosti. S ohledem na poznámku 1.6 lze přirozeně tyto pojmy převést i do symetrických bimodulů. V bimodulech, které nejsou symetrické, bychom museli rozlišovat mezi „levými a pravými variantami“ (např. levá a pravá báze bimodulu). Protože v tomto textu takové pojmy užívat nebudeme, omezíme se pouze na levé moduly. Nebude-li řečeno jinak, budeme R-modulem vždy myslet levý R-modul. Symbolem R budeme nadále značit unitární okruh a jednotku budeme značit 1. Symbolem M budeme rozumět modul nad R.

Následující definice a věty jsou inspirované definicemi a větami z [2], které jsou sice původně vysloveny, příp. dokázány pro vektorové prostory nad komutativními tělesy, ovšem lze je přirozeně zobecnit i na R-moduly tak, jak učiníme na následujících stranách.

Definice 9.20. Ať $r_1, \dots, r_k \in R$ a $m_1, \dots, m_k \in M$. Pak prvek

$$r_1 m_1 + \cdots + r_k m_k = \sum_{i=1}^{k} r_i m_i$$

nazýváme *lineární kombinací prvků* $m_1, \dots, m_k$.

Definice 9.21. O prvcích $m_1, \dots, m_k \in M$ řekneme, že jsou *lineárně nezávislé*, jestliže platí implikace

$$\sum_{i=1}^{k} r_i m_i = o \quad \Rightarrow \quad \forall i \in \widehat{k} : r_i = 0.$$

V opačném případě prvky $m_1, \dots, m_k$ nazýváme *lineárně závislé*.

Definice 9.22. Podmnožinu $N \subseteq M$ nazveme *podmodulem modulu* M, jestliže

(i) N je podgrupa $(M, +)$ a

(ii) $\forall r \in R \; \forall m \in N : rm \in N$.

Poznámka 9.23. Podmínka (i) definice 9.22 je ekvivalentní podmínce

$$\forall m, n \in N : m - n \in N.$$

Věta 9.24. *Ať $\{M_i \mid i \in I\}$ je libovolný systém podmodulů R-modulu M. Pak i $\bigcap_{i\in I} M_i$ je podmodulem M.*

Důkaz. Z algebry je známo, že průnik libovolného systému podgrup je opět podgrupa – podmínka (i) definice 9.22 je tedy splněna.[55] Ukažme, že platí (ii). Zvolme $r \in R$ a $m \in \bigcap_{i\in I} M_i$ libovolně. Pak $m \in M_i$ pro všechna $i \in I$. Protože M_i jsou podmoduly, tak i $rm \in M_i$ pro všechna $i \in I$, a tedy $rm \in \bigcap_{i\in I} M_i$. ■

Definice 9.25. Ať $N \subseteq M$. Pak *podmodulem generovaným množinou N* rozumíme průnik všech podmodulů modulu M, které N obsahují. Značíme jej $\langle N\rangle$. Množinu N nazýváme *generátorem podmodulu* $\langle N\rangle$.

Poznámka 9.26. Definice 9.25 nám říká, že $\langle N\rangle$ je nejmenší podmodul modulu M, ve kterém je N obsaženo.

Značení 9.27. Pro konečné množiny $N = \{m_1, \ldots, m_k\}$ budeme nadále místo $\langle\{m_1, \ldots, m_k\}\rangle$ psát pouze $\langle m_1, \ldots, m_k\rangle$.

Věta 9.28. *Ať $N \subseteq M$.*

(i) Je-li $N = \emptyset$, pak $\langle N\rangle = \{o\}$.

(ii) Je-li $N \neq \emptyset$, pak $\langle N\rangle = \left\{ \sum_{i=1}^{k} r_i n_i \;\middle|\; r_i \in R, n_i \in N, i \in \widehat{k} \right\}$.

Důkaz. (i) je triviální, neboť každý podmodul obsahuje o. Dokažme (ii), tj. předpokládáme $N \neq \emptyset$. Označme si

$$P = \left\{ \sum_{i=1}^{k} r_i m_i \;\middle|\; r_i \in R, m_i \in N, i \in \widehat{k} \right\}.$$

(a) V prvním kroku ukážeme, že P je podmodul M. Zvolme si $m, n \in P$ libovolně. Pak lze psát

$$m = \sum_{i=1}^{k} r_i m_i \qquad \text{a} \qquad n = \sum_{j=1}^{l} s_j n_j,$$

kde pro $i \in \widehat{k}$ a $j \in \widehat{l}$ jsou r_i, $s_j \in R$ a m_i, $n_j \in N$. Pak ale

$$m - n = \sum_{i=1}^{k} r_i m_i - \sum_{j=1}^{l} s_j n_j = \sum_{i=1}^{k} r_i m_i + \sum_{j=1}^{l} (-s_j) n_j \in P.$$

Dále ať $r \in R$ je libovolné. Pak

$$rm = r \sum_{i=1}^{k} r_i m_i = \sum_{i=1}^{k} (r r_i) m_i \in P.$$

Tímto jsou splněny podmínky (i) a (ii) definice 9.22, a tedy P je podmodul M. Jistě taky $N \subseteq P$.

[55] Důkaz by se vedl podobně jako důkaz (ii), jen bychom ukázali, že $m - n \in \bigcap_{i\in I} M_i$ pro libovolné $m, n \in \bigcap_{i\in I} M_i$, což téměř ihned plyne z toho, že M_i je grupou pro libovolné $i \in I$.

(b) V druhém kroku ukážeme, že P je nejmenší podmodul M obsahující N (ve smyslu definice 9.25). Ať Q je libovolný podmodul M obsahující N. Zvolme $m_1, \ldots, m_k \in N \subseteq Q$ a $r_1, \ldots, r_k \in R$. Protože Q je podmodul M, tak $r_i m_i \in Q$ pro všechna $i \in \widehat{k}$. Odtud taky $\sum_{i=1}^{k} r_i m_i \in Q$. Proto $Q \subseteq P$, a tedy $\langle N \rangle = P$. ■

Definice 9.29. M nazveme *modulem konečného řádu*, jestliže existuje konečná množina $N \subseteq M$ taková, že $\langle N \rangle = M$.[a] V opačném případě říkáme, že M je *modulem nekonečného řádu*. Je-li M modulem konečného řádu, pak minimální počet lineárně nezávislých prvků z M, které M generují, nazýváme *řádem modulu* M a značíme jej $\operatorname{rank} M$.

[a] Konečnou množinou rozumíme i $\emptyset$. Tedy triviální modul $\{o\}$ je konečného řádu (konkrétně řádu 0).

Poznámka 9.30. Povšimněme si, že řád modulu je přímou analogií k dimenzi vektorového prostoru.

Definice 9.31. Ať M je R-modul konečného řádu a $e_1, \ldots, e_k \in M$. Jsou-li

(*i*) $e_1, \ldots, e_k$ lineárně nezávislé a

(*ii*) $\langle e_1, \ldots, e_k \rangle = M$,

pak k-tici $\mathcal{B} = (e_1, \ldots, e_k)$ budeme nazývat *bází modulu* M. Pro modul generovaný množinou bázových vektorů $\{e_1, \ldots, e_k\}$, tj. pro modul $\langle e_1, \ldots, e_k \rangle$, budeme používat zápis $\langle \mathcal{B} \rangle$.[a]

[a] Protože $\mathcal{B}$ je uspořádaná k-tice prvků z M a nikoliv podmnožina M, tak zápis $\langle \mathcal{B} \rangle$ nemá smysl, dokud jej zvlášť nezadefinujeme.

Věta 9.32. *Ať $\mathcal{B}$ je libovolná báze modulu M. Pak každý prvek z M lze jednoznačně vyjádřit jako lineární kombinace prvků báze $\mathcal{B}$.*

Důkaz. Označme $\mathcal{B} = (e_1, \ldots, e_k)$ a zvolme $m \in M$ libovolně. Ať lze m vyjádřit ve tvaru $\sum_{i=1}^{k} m_i e_i$ a zároveň ve tvaru $\sum_{i=1}^{k} n_i e_i$ ($m_i, n_i \in R$ pro $i \in \widehat{k}$). Ukažme, že pro všechna $i \in \widehat{k}$ platí $m_i = n_i$. Máme

$$o = m - m = \sum_{i=1}^{k} m_i e_i - \sum_{i=1}^{k} n_i e_i = \sum_{i=1}^{k} (m_i - n_i) e_i.$$

Protože $e_1, \ldots, e_k$ jsou lineárně nezávislé, tak $m_i - n_i = o$ pro všechna $i \in \widehat{k}$. Odtud máme požadovaný výsledek. ■

Definice 9.33. Ať M je R-modul konečného řádu a $\mathcal{B} = (e_1, \ldots, e_k)$ je jeho libovolná báze. Pokud $m \in M$ lze vyjádřit ve tvaru

$$\sum_{i=1}^{k} m_i e_i,$$

kde $m_1, \ldots, m_k \in R$, pak sloupcový vektor $(m_1, \ldots, m_k)^{\mathrm{T}}$ nazýváme *vektorem souřadnic prvku m v bázi $\mathcal{B}$* a značíme jej $[m]_{\mathcal{B}}$. Skaláry $m_1, \ldots, m_k$ nazýváme *souřadnice prvku m v bázi $\mathcal{B}$*.

Definice 9.34. Ať M a N jsou R-moduly. Zobrazení $\varphi : M \to N$ nazveme *homomorfismem modulů M a N*, pokud zachovává součet a skalární násobek, tj. pokud

(*i*) $\forall m, n \in M : \varphi(m + n) = \varphi(m) + \varphi(n)$,

(*ii*) $\forall m \in M\ \forall r \in R : \varphi(rm) = r\varphi(m)$.

Homomorfismus $\varphi : M \to M$ nazýváme *endomorfismus na modulu M*. Množinu všech endomorfismů na modulu M značíme $\mathfrak{End}(M)$.

Poznámka 9.35. Pokud definujeme sčítání endomorfismů a násobení endomorfismů skalárem bodově, tj. pro $\varphi, \psi \in \mathfrak{End}(M)$ a $r \in R$ definujeme

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \quad \text{a} \quad (r\varphi)(m) = r\varphi(m), \quad m \in M,$$

pak $\mathfrak{End}(M)$ spolu s těmito operacemi tvoří levý R-modul. Stačí jen mechanicky ověřit platnost definičních podmínek (včetně podmínek pro strukturu aditivní grupy) levého modulu z definice 1.1.

Definice 9.36. Ať M a N jsou R-moduly konečného řádu, $\mathcal{B} = (e_1, \dots, e_k)$ ($\operatorname{rank} M = k$) a $\mathcal{C}$ jsou báze po řadě modulů M a N, $\operatorname{rank} N = l$ a $\varphi : M \to N$ je homomorfismus modulů M a N. Označme pro $i \in \widehat{k}$

$$[\varphi(e_i)]_{\mathcal{C}} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{li} \end{pmatrix}.$$

Pak matici

$$\mathbf{A} = (a_{ij})_{i,j=1}^{l,k} = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{l1} & \cdots & a_{lk} \end{pmatrix} \in \mathcal{M}_{l\times k}(R)^a$$

nazveme *maticí homomorfismu φ v bázích $\mathcal{B}$ a $\mathcal{C}$*. Je-li φ endomorfismus na M a $\mathbf{A}$ je jeho matice v bázích $\mathcal{B}$ a $\mathcal{B}$, pak pouze říkáme, že $\mathbf{A}$ je *maticí φ v bázi $\mathcal{B}$*.

[a] Symbolem $\mathcal{M}_{l\times k}(R)$ značíme množinu všech matic řádu $l \times k$ nad okruhem R. Povšimněme si, že zde obecně pracujeme s nekomutativním okruhem, nad kterým se obvykle matice neuvažují. S těmito maticemi budeme pracovat zcela analogicky, jako se pracuje s maticemi nad komutativními okruhy s tím rozdílem, že při jejich násobení, které samo o sobě není komutativní, ještě budeme muset dbát na pořadí násobení jejich prvků. Máme-li tedy matice $\mathbf{A} = (a_{ij}) \in \mathcal{M}_{k\times l}(R)$, $\mathbf{B} = (b_{ij}) \in \mathcal{M}_{l\times m}(R)$, pak jejich součinem v uvedeném pořadí rozumíme matici $\mathbf{AB} \in \mathcal{M}_{k\times m}(R)$ mající na pozici $(i,j) \in \widehat{m} \times \widehat{k}$ prvek

$$\sum_{p=1}^{l} a_{ip} b_{pj},$$

přitom musíme dbát na pořadí součinů $a_{ip}b_{pj}$. Tento součet tedy nelze psát např. takto:

$$\sum_{p=1}^{l} b_{pj} a_{ip}!$$

Věta 9.37. *Ať M a N jsou R-moduly konečného řádu, $\mathcal{B}$ a $\mathcal{C}$ jsou báze po řadě modulů M a N, $\varphi : M \to N$ je homomorfismus a $\mathbf{A}$ je jeho matice v bázích $\mathcal{B}$ a $\mathcal{C}$. Pak pro každé $m \in M$ platí*

$$[\varphi(m)]_{\mathcal{C}} = \left([m]_{\mathcal{B}}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}}\right)^{\mathrm{T}}.$$

Pokud je R komutativní okruh, pak se vztah zjednoduší na

$$[\varphi(m)]_{\mathcal{C}} = \mathbf{A}[m]_{\mathcal{B}}.$$

Důkaz. Označme si prvky bází $\mathcal{B}$ a $\mathcal{C}$ následovně:

$$\mathcal{B} = (e_1, \dots, e_k) \qquad \text{a} \qquad \mathcal{C} = (\widetilde{e}_1, \dots, \widetilde{e}_l)$$

Dále ať $[m]_{\mathcal{B}} = (m_1, \dots, m_k)^{\mathrm{T}}$, $[\varphi(m)]_{\mathcal{C}} = (\widetilde{m}_1, \dots, \widetilde{m}_l)^{\mathrm{T}}$ a $\mathbf{A} = (a_{ij})_{i,j=1}^{l,k}$. Protože φ

je homomorfismus[56], platí

$$\varphi(m) = \varphi\left(\sum_{i=1}^{k} m_i e_i\right) = \sum_{i=1}^{k} m_i \varphi(e_i) = \sum_{i=1}^{k} m_i \sum_{j=1}^{l} a_{ji} \widetilde{e}_j = \sum_{j=1}^{l} \left(\sum_{i=1}^{k} m_i a_{ji}\right) \widetilde{e}_j,$$

tedy pro všechna $j \in \widehat{l}$ máme

$$\widetilde{m}_j = \sum_{i=1}^{k} m_i a_{ji}. \tag{9.3}$$

Počítejme nyní $([m]_{\mathcal{B}}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}})^{\mathrm{T}}$. Nejdříve

$$[m]_{\mathcal{B}}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}} = (m_1, \ldots, m_k) \begin{pmatrix} a_{11} & \cdots & a_{l1} \\ \vdots & \ddots & \vdots \\ a_{1k} & \cdots & a_{lk} \end{pmatrix} = \left(\sum_{i=1}^{k} m_i a_{1i}, \ldots, \sum_{i=1}^{k} m_i a_{li}\right).$$

Transponujme:

$$\left([m]_{\mathcal{B}}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}}\right)^{\mathrm{T}} = \begin{pmatrix} \sum_{i=1}^{k} m_i a_{1i} \\ \vdots \\ \sum_{i=1}^{k} m_i a_{li} \end{pmatrix}.$$

Porovnáním se vztahem (9.3) dostáváme požadovaný výsledek. Pokud je R navíc komutativním okruhem, pak zřejmě $([m]_{\mathcal{B}}^{\mathrm{T}} \mathbf{A}^{\mathrm{T}})^{\mathrm{T}} = \mathbf{A}[m]_{\mathcal{B}}$. ■

Věta 9.38 (o určenosti homomorfismu). *Ať M a N jsou R-moduly konečného řádu. Pak ke každé bázi $\mathcal{B} = (e_1, \ldots, e_k)$ modulu M a každé uspořádáné k-tici $(n_1, \ldots, n_k)$ prvků z N existuje jediný homomorfismus $\varphi : M \to N$ takový, že*

$$\forall i \in \widehat{k} : \varphi(e_i) = n_i.$$

Důkaz. Ať báze $\mathcal{B}$ a k-tice $(n_1, \ldots, n_k)$ jsou voleny jako v tvrzení a definujme zobrazení $\varphi : M \to N$ podmínkou

$$\forall m_1, \ldots, m_k \in R : \varphi\left(\sum_{i=1}^{k} m_i e_i\right) = \sum_{i=1}^{k} m_i n_i.$$

Zřejmě takto definované zobrazení splňuje podmínku

$$\forall i \in \widehat{k} : \varphi(e_i) = n_i.$$

[56] Indukcí lze totiž z vlastnosti $\varphi(m+n) = \varphi(m) + \varphi(n)$, $m, n \in M$, odvodit

$$\varphi\left(\sum_{i=1}^{k} m_i\right) = \sum_{i=1}^{k} \varphi(m_i), \quad m_1, \ldots, m_k \in M.$$

(*i*) V prvním kroku ukážeme, že se jedná o homomorfismus. Volme $m, \widetilde{m} \in M$ libovolně a označme $[m]_{\mathcal{B}} = (m_1, \ldots, m_k)^{\mathrm{T}}$ a $[\widetilde{m}]_{\mathcal{B}} = (\widetilde{m}_1, \ldots, \widetilde{m}_k)^{\mathrm{T}}$. Pak

$$\begin{aligned}\varphi(m + \widetilde{m}) &= \varphi\left(\sum_{i=1}^{k} m_i e_i + \sum_{i=1}^{k} \widetilde{m}_i e_i\right) = \varphi\left(\sum_{i=1}^{k} (m_i + \widetilde{m}_i) e_i\right) = \sum_{i=1}^{k} (m_i + \widetilde{m}_i) n_i \\ &= \sum_{i=1}^{k} m_i n_i + \sum_{i=1}^{k} \widetilde{m}_i n_i = \varphi(m) + \varphi(\widetilde{m}).\end{aligned}$$

Volme navíc $r \in R$ a počítejme:

$$\varphi(rm) = \varphi\left(r \sum_{i=1}^{k} m_i e_i\right) = \varphi\left(\sum_{i=1}^{k} r m_i e_i\right) = \sum_{i=1}^{k} r m_i n_i = r \sum_{i=1}^{k} m_i n_i = r\varphi(m).$$

Máme tedy, že φ je homomorfismus modulů.

(*ii*) V druhém kroku ukážeme, že je takto definovaný homomorfismus jediný. Uvažme navíc homomorfmus $\psi : M \to N$ splňující podmínku

$$\forall i \in \widehat{k} : \psi(e_i) = n_i.$$

Opět ať $[m]_{\mathcal{B}} = (m_1, \ldots, m_k)^{\mathrm{T}}$ je libovolný pevně zvolený prvek M. Pak máme

$$\psi(m) = \psi\left(\sum_{i=1}^{k} m_i e_i\right) \overset{(*)}{=} \sum_{i=1}^{k} m_i \psi(e_i) = \sum_{i=1}^{k} m_i n_i = \varphi(m),$$

kde $(*)$ plyne z toho, že ψ je homomorfismus. Máme tedy $\varphi = \psi$. ■

Definice 9.39. Ať φ je endomorfismus na M. Podmodul N modulu M nazveme *φ-invariantní*, jestliže

$$\forall m \in N : \varphi(m) \in N.$$

Věta 9.40. *Ať φ je endomorfismus na M. Podmodul $\langle m_1, \ldots, m_k \rangle$ je φ-invariantní, právě když*

$$\forall i \in \widehat{k} : \varphi(m_i) \in \langle m_1, \ldots, m_k \rangle.$$

Důkaz. Přímá implikace je triviální. Ukažme, že pokud platí

$$\forall i \in \widehat{k} : \varphi(m_i) \in \langle m_1, \ldots, m_k \rangle,$$

pak je $\langle m_1, \ldots, m_k \rangle$ φ-invariantní podmodul M. Označme pro $i \in \widehat{k}$

$$\varphi(m_i) = \sum_{j=1}^{k} s_{ij} m_j$$

(takové skaláry $s_{ij} \in R$ jistě existují, protože $\varphi(m_i) \in \langle m_1, \ldots, m_k \rangle$ pro všechna $i \in \widehat{k}$) a zvolme $m \in \langle m_1, \ldots, m_k \rangle$ libovolně. Pak existují $r_1, \ldots, r_k \in R$, že

$$m = \sum_{i=1}^{k} r_i m_i.$$

Dále z předpokladu a z toho, že φ je endomorfismus, dostáváme

$$\begin{aligned} \varphi(m) = \varphi\left(\sum_{i=1}^{k} r_i m_i\right) = \sum_{i=1}^{k} a_i \varphi(m_i) = \sum_{i=1}^{k} a_i \left(\sum_{j=1}^{k} s_{ij} m_j\right) \\ = \sum_{j=1}^{k} \left(\sum_{i=1}^{k} a_i s_{ij}\right) m_j \in \langle m_1, \ldots, m_k \rangle. \end{aligned}$$

■

Literatura

[1] GARCÍA-PACHECO, Francisco Javier. *Abstract calculus: A categorical approach.* Boca Raton: CRC Press, 2022. ISBN 9780367762209.

[2] HORT, Daniel a Jiří RACHŮNEK. *Algebra I.* Olomouc: Univerzita Palackého, 2003. ISBN 80-244-0631-4.

[3] HRBACEK, Karel a Thomas JECH. *Introduction to set theory.* 3rd ed., rev. and expanded. New York: Marcel Dekker, 1999. ISBN 0-8247-7915-0.

[4] LANG, Serge. *Algebra.* Third Edition. New Haven: Springer, 2005. ISBN 978-1-4612-6551-1.

[5] PALEY, Hiram. *A first course in abstract algebra.* Third Edition. International Thomson Publishing, 1966. ISBN 0-03-054965-5.

[6] TOMEČEK, Jan. *Matematická analýza 2.* Olomouc: Univerzita Palackého, 2020. ISBN 978-80-244-5853-3.

[7] UFNAROVSKI, Victor a Bo ÅHLANDER. *How to differentiate a number.* Journal of Integer Sequences [online]. 2003, (03.3.4), 24 [cit. 2024-04-25]. Dostupné z: `http://eudml.org/doc/54388`