Okruhy a moduly

sbírka příkladů

Francírek Pavel
Hulík Ondřej
Janík Tomáš
Sotáková Jana
Suchánek Radek

19. února 2015

Obsah

Úvod

zde bude popis textu LaTeXu vyrobeno v

Tým autorů

1. Moduly, podmoduly, homomorfismy modulů, faktorové moduly

Definice 1.1 (Levý modul)**.** Levým R-modulem nebo levým modulem nad R nazveme množinu M se strukturou abelovské grupy, na níž má okruh R akci (tj. zobrazení $R \times M \to M$), tzv. skalární násobení, splňující $\forall r, s \in R$, $\forall m, n \in M$ následující podmínky:

(i) $(rs)m = r(sm)$

(ii) $(r + s)m = rm + sm$

(iii) $r(m + n) = rm + rn$.

(iv) $1m = m$.

Analogicky zavedeme pravé R-moduly (pravé moduly nad R) změnou podmínek na akci R na M.

Definice 1.2 (Pravý modul)**.** Pravým R-modulem nebo také pravým modulem nad R nazveme množinu M se strukturou abelovské grupy, na níž má okruh R akci (tj. zobrazení $M \times R \to M$), tzv. skalární násobení, splňující $\forall r, s \in R$, $\forall m, n \in M$ následující podmínky:

(i) $m(rs) = (mr)s$

(ii) $m(r + s) = mr + ms$

(iii) $(m + n)r = mr + nr$.

(iv) $m1 = m$.

Nyní uvažujme dva okruhy R, S.

Definice 1.3 (Bimodul)**.** Abelovskou grupu M nazveme R-S-bimodulem, jestliže M má strukturu levého R-modulu a zároveň pravého S-modulu a navíc splňuje $\forall r \in R, s \in S, m \in M$ následující podmínku:

$$r(ms) = (rm)s.$$

Bude-li z kontextu jasné, jaký modul je uvažován, budeme ve většině případů daný modul označovat pouze M. Bude-li však třeba, levé R-moduly budeme značit takto: ${}_RM$, pravé R-moduly označíme takto: M_R a R-S-bimoduly budeme psát tímto způsobem: ${}_RM_S$

Příklad 1.4.

1. Každý okruh je modulem sám nad sebou. Akce $R \times R \to R$ je dána násobením v okruhu $s_1 \cdot s_2 = s_1 s_2$.
2. Moduly nad okruhem celých čísel $\mathbb{Z}$ jsou přesně abelovské grupy.
3. Moduly nad tělesem $\mathbb{K}$ jsou přesně vektorové prostory.
4. Uvažujme vektorový prostor V dimenze n nad tělesem $\mathbb{K}$ a okruh čtvercových matic $\mathrm{Mat}_n(\mathbb{K}$. Pokud ve V zvolíme bázi, můžeme prvky tohoto prostoru chápat jako sloupce a (přirozeným způsobem) definovat levou akci $\mathrm{Mat}_n(\mathbb{K})$ na V jako násobení matice a vektoru. Tedy V je (levý) $\mathrm{Mat}_n(\mathbb{K})$-modul.
5. Podobně na duálním prostoru k V, $V^* = \{\alpha \colon V \to \mathbb{K} \mid \alpha \textit{ lineární}\}$ (tj. vektorovém prostoru všech jedna forem na V) máme pravou akci matic, kterou při zvoleném souřadnicovém vyjádření můžeme chápat jako násobení řádku maticí. Tedy V^* je (pravým) $\mathrm{Mat}_n(\mathbb{K})$ modulem.

6. Uvažujme hladkou varietu M. Pak prostor $\Gamma(TM)$ všech hladkých vektorových polí na této varietě je $C^\infty(M)$ modulem, kde $C^\infty(M)$ značí okruh všech hladkých funkcí na M. Akce je dána pointwise $f \cdot X(m) := f(m)X(m)$, $m \in M$.
7. Obecně pro hladkou varietu M je prostor všech hladkých sekcí $\Gamma(\bigotimes_n^m TM)$ (tj. všech hladkých tenzorových polí typu m, n) $C^\infty(M)$ modulem.

Definice 1.5 (Podmodul)**.** Mějme R-modul M nad okruhem R. Podmnožinu N modulu M nazveme *podmodul R-modulu M* (případně pouze podmodul M), je-li N podgrupou M, která je uzavřená na akci okruhu R, tedy splňuje:

(i) $rn \in N\ \forall r \in R, \forall n \in N$ (je-li M levý R-modul)

(ii) $nr \in N\ \forall r \in R, \forall n \in N$ (je-li M pravý R-modul).

Častým úkolem při práci s moduly je určit, zda je podmnožina nějakého modulu M zároveň jeho podmodulem. V takové situaci je velmi užitečné následující kritérium:

Lemma 1.6 (Podmodulové kritérium)**.** *Pro okruh R uvažujme levý R-modul M spolu s podmnožinu $N \subseteq M$. Pak N je podmodulem modulu M, právě když platí následující podmínky:*

(i) $0 \in N$

(ii) $m + rn \in N$ *(resp.* $m + nr \in N$ *pro pravý R-modul)* $\forall m, n \in N$, $\forall r \in R$.

Definice 1.7 (Konečně generovaný modul)**.** Levý (pravý) R-modul M nazveme konečně generovaný, jestliže existuje konečná podmnožina $\{a_1, \ldots, a_n\} \subseteq M$ taková, že $\forall\ m \in M$ $\exists r_1, \ldots, r_n \in R : m = r_1a_1 + \ldots + r_na_n$ (resp. $m = a_1r_1 + \ldots + a_nr_n$).

Definice 1.8 (Homomorfismy modulů)**.** Buď R okruh a M a N (levé) R-moduly. Zobrazení $f\colon M \to N$ se nazývá homomorfismus (levých) R-modulů, jestliže pro každé $m, n \in M$ a $r \in R$ platí

(i) $f(m+n) = f(m) + f(n)$;

(ii) $f(rm) = r\big(f(m)\big)$.

Definice 1.9 (Faktormodul)**.** Buď R okruh, M (levý) R-modul a N podmodul modulu M. Na faktorgrupě M/N definujeme strukturu R-modulu předpisem pro každé $m \in M$ a každé $r \in R$:

$$r(m + N) = rm + N.$$

Potom modul M/N nazýváme *faktormodul modulu M podle podmodulu N*.

Definice 1.10 (Irreducibilní modul)**.** Řekneme, že nenulový R-modul M je *ireducibilní*, jestliže 0 a N jsou jeho jediné podmoduly.

V následujících příkladech uvažujeme R jako okruh s jednotkou a M jako levý R-modul, pokud není uvedeno jinak.

Příklad 1.11. Dokažte, že $0m = 0$ a $(-1)m = -m\ \forall m \in M$

Řešení.

$$0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m \Rightarrow 0 \cdot m = 0$$

$$(-1) \cdot m + m = (-1) \cdot m + 1 \cdot m = (-1+1) \cdot m = 0 \cdot m = 0 \Rightarrow (-1) \cdot m = -m \qquad \diamond$$

Příklad 1.12. Prvek m R-modulu M se nazývá *torzní*, jestliže $rm = 0$ pro nějaký nenulový prvek $r \in R$. Označme množinu torzních prvků

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ pro nějaké nenulové } r \in R\}.$$

1. Dokažte, že pokud je R oborem integrity, pak $\mathrm{Tor}(M)$ je podmodul M (tzv. *torzní* podmodul M).
2. Uveďte příklad okruhu R a R-modulu M takových, že $\mathrm{Tor}(M)$ není podmodulem M. [Uvažte torzní prvky v R-modulu R.]
3. Ukažte, že pokud R má dělitele nuly, pak každý nenulový R-modul má nenulové torzní prvky.

Řešení. 1. Z definice torzních prvků

$$x, y \in \mathrm{Tor}(M) \Rightarrow \exists a, b \in R\backslash\{0\} : ax = 0 = by$$

a použitím kritéria pro podmoduly dostáváme:

$$\begin{aligned}(ab)(x + ry) &= (ab)x + (ab)ry \\ &= (ba)x + (ab)ry \\ &= b(ax) + a(br)y \\ &= 0 + a(rb)y \\ &= (ar)by \\ &= (ar)0 \\ &= 0.\end{aligned}$$

Tedy $x + ry \in \mathrm{Tor}(M), \forall r \in R$ a $\mathrm{Tor}(M)$ je podmodulem M.

2. Uvažme okruh $R = \mathrm{Mat}_2\,\mathbb{R}$, který je abelovskou grupou vzhledem ke sčítání a okruhem s děliteli nul vzhledem k násobení. Dále vezměme $M = R$ a uvažujme následující matice:

$$A = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, B = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

Pak A i B jsou prvky $\mathrm{Tor}(M)$, ale jejich součet $A + B$ již nikoliv (ověřte). Není tedy splněna uzavřenost M vzhledem ke sčítání, čímž jsme hotovi.

3. Vezměme libovolné $x \in M$ $x \neq 0$. Je-li x torzním prvkem, pak jsme hotovy. Předpokládejme tedy, že x není torzní a uvažujme $r, d \in R\backslash\{0\} : rd = 0$.
Pak $dx \in \mathrm{Tor}(M)$, protože
$$r(dx) = (rd)x = 0x = 0.$$
Tedy $\mathrm{Tor}(M) \neq \{0\}$, což jsme chtěli ukázat. ◇

Příklad 1.13. Jestliže N je podmodul M, *annihilátor* N v R je definován takto:

$$\mathrm{Ann}_R(N) = \{r \in R \mid rn = 0 \quad \forall n \in N\}.$$

Dokažte, že *annihilátor* N v R je oboustranný ideál R.

Řešení. Chceme ukázat, že $\forall\ r \in R$, $\forall\ a \in \mathrm{Ann}_R(N)$ je $ra, ar \in \mathrm{Ann}_R(N)$. Buď tedy $n \in N$ libovolné.

1. $ra \in \mathrm{Ann}_R(N)$: $(ra)n = r(an) = r0 \Rightarrow ra \in \mathrm{Ann}_R(N)$.
2. $ra \in \mathrm{Ann}_R(N)$: $(ar)n = a(rn) = 0$ (neboť $rn \in N$) $\Rightarrow ar \in \mathrm{Ann}_R(N)$. ◇

Příklad 1.14. Je-li I pravý ideál R, *annihilátor* I v M je definován následovně:

$$\mathrm{Ann}_M(I) = \{m \in M \mid im = 0 \quad \forall i \in I\}.$$

Dokažte, že *annihilátor* I v M je podmodul M.

Řešení. Chceme:

$$m + rn \in \mathrm{Ann}_M(I),\ \forall m, n \in \mathrm{Ann}_M(I),\ \forall r \in R.$$

Pro libovolné $i \in I$ počítejme:

$$i(m + rn) = im + i(rn) = 0 + (ir)n = (ir)n.$$

Dále I je ideál a platí $ir \in I$, proto $(ir)n = 0$. Dostáváme $m + rn \in \mathrm{Ann}_M(I)$. ◇

Příklad 1.15. Buď M abelovská grupa (tj. $\mathbb{Z}$-modul) tvaru $M = \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.

1. Nalezněte generátor annihilátoru M v $\mathbb{Z}$
2. Nechť $I = 2\mathbb{Z}$. Popište annihilátor I v M jako součin cyklických grup.

Řešení. 1. M je generováno prvky $(1,0,0), (0,1,0), (0,0,1)$. Hledáme nejmenší $k \in \mathbb{Z}$, splňující $k \equiv 0 \pmod{24}$, $k \equiv 0 \pmod{15}$, $k \equiv 0 \pmod{50}$, což je nejmenší společný násobek čísel $24, 15, 50$. Proto generátor annihilátoru M v $\mathbb{Z}$ je číslo 600.

2. Nyní hledáme $(x, y, z) \in M$ takové, že $2(x, y, z) = 0$. Tedy $(2x, 2y, 2z) = (0,0,0) \Leftrightarrow x \in 12 \cdot \mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}/2$, $y \in 0 \cdot \mathbb{Z}/15\mathbb{Z} \cong 0$, $z \in 25 \cdot \mathbb{Z}/50\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Dohromady $\mathrm{Ann}_M(I) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. ◇

Příklad 1.16. Buď z prvek centra okruhu R, tj. $zr = rz$, $\forall r \in R$. Dokažte, že

$$zM = \{zm \mid m \in M\}$$

je podmodul M. Dále ukažte, že je li R okruh matic nad tělesem $\mathbb{F}$: $R = \mathrm{Mat}_2\,\mathbb{F}$ a $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, pak $A \cdot R$ není levý R-podmodul (kde $M = R$ chápeme jako levý R-modul, stejně jako v předešlém). Najděte nějaký prvek R, se kterým A nekomutuje.

Řešení. Podle kritéria pro podmoduly chceme ukázat, že $zm + s(zn) \in zM$ pro libovolné $m, n \in M, s \in R$, což plyne ihned z definice prvků centra:

$$\begin{aligned} zm + s(zn) &= zm + (sz)n \\ &= zm + (zs)n \\ &= zm + z(sn) \\ &= z(m + sn). \end{aligned}$$

Nyní uvažujme matici $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, ta leží v $A \cdot \mathrm{Mat}_2 \mathbb{F}$, protože $\mathrm{Mat}_2 \mathbb{F}$ obsahuje jednotkovou matici. Pak pro matici $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Mat}_2 \mathbb{F}$ platí $BA \notin \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \mathrm{Mat}_2 \mathbb{F}$.
Prvek R, který nekomutuje s A, je například D. Platí totiž:

$$AD = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$DA = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

$$AD \neq DA$$ ◇

Příklad 1.17. Ukažte, že ireducibilní $\mathbb{Z}$-moduly jsou tvaru $\mathbb{Z}/p\mathbb{Z}$, kde p je prvočíslo.

Řešení. Buď M libovolný (nenulový) ireducibilní $\mathbb{Z}$-modul. Uvažme libovolný nenulový homomorfismus $\alpha\colon \mathbb{Z} \to M$. Tento homomorfismus musí být surjektivní ($\mathrm{Im}\,\alpha$ je podmodul M). Jeho jádro je jakožto ideál $\mathbb{Z}$ tvaru $n\mathbb{Z}$ pro vhodné $n \in \mathbb{N}$, a tedy $M \cong \mathbb{Z}/n\mathbb{Z}$. Pokud by existoval ideál $\mathfrak{a}$ takový, že $\mathrm{Ker}\,\alpha \subsetneq \mathfrak{a} \subsetneq \mathbb{Z}$, pak by $\alpha(\mathfrak{a})$ byl nenulový vlastní podmodul. Tedy $\mathrm{Ker}\,\alpha$ musí být maximální ideál, a proto je tvaru $p\mathbb{Z}$ pro vhodné prvočíslo p, tj. $M \cong \mathbb{Z}/p\mathbb{Z}$. ◇

Příklad 1.18. Mějme homomorfismus okruhů s jednotkou $f\colon R \to S$. Ukažte, že pomocí tohoto homomorfismu lze na S zadefinovat struktura R-modulu, tj. popište akci R na S a ověřte pro ni potřebné axiomy.

Řešení. Akce R na S lze $\forall r_1, r_2 \in R,\ \forall s_1, s_2 \in S$ definovat tímto způsobem

$$r \cdot s = f(r)s$$

a platí

1. $(r_1 + r_2) \cdot s = f(r_1 + r_2)s = \big(f(r_1) + f(r_2)\big)s = f(r_1)s + f(r_2)s = r_1 \cdot s + r_2 \cdot s$
2. $r \cdot (s_1 + s_2) = f(r)(s_1 + s_2) = f(r)s_1 + f(r)s_2 = r \cdot s_1 + r \cdot s_2$
3. $(r_1 r_2) \cdot (s) = \big(f(r_1 r_2)\big)s = f(r_1)\big(f(r_2)s\big) = r_1 \cdot (r_2 \cdot s)$. ◇

Příklad 1.19. Nechť M je pravý R-modul a nechť α je endomorfismus M. Ukažte, že pravidlo

$$m \cdot (f_0 + f_1 T + \cdots + f_k T^k) = mf_0 + \alpha(mf_1) + \cdots + \alpha^k(mf_k)$$

zadává na M strukturu $R[T]$-modulu. Dále ukažte, že je-li M pravý $R[T]$-modul, pak je M pravý R-modul a zobrazení α definované vztahem $\alpha m = mT$ je ednomorfismus R-modulu M.

Řešení. Potřebujeme ověřit axiomy modulu. Buďte $m, n \in M, f, g \in R[T]$ libovolné. Platí

1. $m \cdot 1 = m$;
2. $(m + n)f = mf + nf$;
3. $m(f + g) = mf + mg$.

Zbývá ukázat, že $m(fg) = (mf)g$. To nám zřejmě stačí ukázat pro $f = T^k, g = T^l$, kde $k, l \in \mathbb{N}$. Platí

$$m(T^k \cdot T^l) = m(T^{k+l}) = \alpha^{k+l}(m) = \alpha^l(\alpha^k(m)) = (\alpha^k(m))T^l = (mT^k)T^l.$$

Nyní ukážeme, že zobrazení α definované vztahem $\alpha m = mT$ je endomorfismus R-modulu M.

$$\alpha(m+n) = (m+n)T = mT + nT = \alpha m + \alpha n;$$
$$\alpha(mr) = (mr)T = m(rT) = m(Tr) = (mT)r = (\alpha m)r.$$

Tím jsme ukázali, že α je skutečně endomorfismus R-modulu M. ◇

Příklad 1.20. Předpokládejme, že M a N jsou pravé $R[T]$-moduly s akcí prvku T zadanou endomorfismem α, resp. β. Dokažte, že $\pi\colon M \to N$ je homomorfismus $R[T]$-modulů právě, když je to homomorfismus R-modulů splňující $\pi\alpha = \beta\pi$.

Řešení. Předpokládejme, že π je homomorfismus R-modulů a platí $\pi\alpha = \beta\pi$. Potom

$$\begin{aligned}\pi(m \cdot (f_0 + f_1T + \cdots + f_kT^k)) &= \pi(mf_0 + \alpha(mf_1) + \cdots + \alpha^k(mf_k)) \\ &= \pi(m)f_0 + \beta\pi(m)f_1 + \cdots + \beta^k\pi(m)f_k \\ &= \pi(m)f_0 + \pi(m)f_1T + \cdots + \pi(m)f_kT^k \\ &= \pi(m)(f_0 + f_1T + \cdots + f_kT^k).\end{aligned}$$

Nyní předpokládejme, že π je homomorfismus $R[T]$-modulů. Pak je π také homomorfismus R-modulů a pro každé $m \in M$ platí

$$(\pi\alpha)m = \pi(\alpha m) = \pi(mT) = (\pi m)T = \beta(\pi m) = (\beta\pi)m.$$ ◇

Příklad 1.21. Nechť

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

je reálná matice $n \times n$, která má na diagonále i nad diagonálou jedničky, všude jinde nuly. Tato matice zadává na $\mathbb{R}^n$ strukturu $\mathbb{R}[T]$-modulu M. Pro každé $i = 1, 2, \ldots, n$ definujme $M_i = \mathrm{Lin}(e_1, \ldots, e_i)$, kde

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

jsou vektory standardní báze $\mathbb{R}^n$, a $M_0 = 0$. Ukažte, že podmoduly M jsou právě $M_i, i = 0, 1, \ldots, n$.

Řešení. Snadno se ověří, že M_i jsou podmoduly M, neboť $AM_i = \{Am, m \in M_i\} \subseteq M_i$.

Nyní dokážeme, že podmoduly modulů M_i jsou tvaru M_k pro vhodné $k = 0, \dots, i$. Tvrzení dokážeme indukcí vzhledem k i.

1. Pro $i = 0$ je tvrzení triviálně splněno.
2. Předpokládejme, že tvrzení platí pro všechna $i < r, r \in \mathbb{N}$.

Chceme ukázat, že pak tvrzení platí také pro $i = r$. Buď $L \subset M_r$ libovolný podmodul. Pokud je $L \subseteq M_{r-1}$, pak podle indukčního předpokladu je L tvaru M_k pro vhodné $k = 0, 1, \dots, r-1$. Předpokládejme, že $L \nsubseteq M_{r-1}$. Pak existuje $v \in L$, jehož r-tá složka je nenulová. Ukážeme, že platí $L = M_r$. K tomu nám stačí ukázat, že vektory $v, Av, A^2v, \dots, A^{r-1}v$ jsou lineárně nezávislé. Nechť $a_0, a_1, \dots, a_{r-1}$ jsou libovolná reálná čísla splňující

$$a_0 v + a_1 Av + \cdots + a_{r-1} A^{r-1} v = Bv = 0,$$

kde

$$B = a_0 I + a_1 A + \cdots + a_{r-1} A^{r-1} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{r-1} \\ 0 & a_0 & a_1 & \cdots & a_{r-2} \\ 0 & 0 & a_0 & \cdots & a_{r-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 \end{pmatrix}.$$

Pak $a_0 = a_1 = \cdots = a_{r-1} = 0$, protože r-tá složka v je nenulová. ◇

Nechť R a S jsou libovolné okruhy. Následující příklad ukazuje, že zadat na nějakém R-modulu strukturu S-R-bimodulu je v jistém smyslu to samé, jako zadat homomorfismus okruhů $S \to \mathrm{End}(M)$.

Příklad 1.22. Buď M pravý R-modul. Ukažte, že existuje bijekce

$$\{\text{homomorfismy okruhů } f\colon S \to \mathrm{End}(M)\} \longleftrightarrow \{S\text{-}R\text{-bimoduly } M\}.$$

Řešení. Buď $f\colon S \to \mathrm{End}(M)$ homomorfismus okruhů. Ukážeme, že přiřazení $sm = f(s)(m)$ zadává na M strukturu S-R-bimodulu. Pro libovolná $m, m' \in M, s, s' \in S, r \in R$ platí

1. $(ss')m = f(ss')m = \big(f(s) \circ f(s')\big)(m) = f(s)\big(f(s')(m)\big) = f(s)(s'm) = s(s'm)$;
2. $(s + s')(m) = f(s + s')(m) = \big(f(s) + f(s')\big)(m) = f(s)(m) + f(s')(m) = sm + s'm$;
3. $s(m + m') = f(s)(m + m') = f(s)(m) + f(s)(m') = sm + sm'$;
4. $s(mr) = f(s)(mr) = \big(f(s)(m)\big)r = (sm)r$.

Buď nyní M S-R-bimodul. Definujme zobrazení $f\colon S \to \mathrm{End}(M)$ předpisem

$$f(s)(m) = sm.$$

Není těžké ověřit, že $f(s) \in \mathrm{End}(M)$ pro každé $s \in S$. Pro libovolná $m, m' \in M$ a $r \in R$ platí

1. $f(s)(m + m') = s(m + m') = sm + sm' = f(s)(m) + f(s)(m')$;
2. $f(s)(mr) = s(mr) = (sm)r = \big(f(s)(m)\big)r$.

Ukážeme, že f je homomorfismus okruhů. Pro libovolná $m \in M, s, s' \in S$ platí

1. $f(s + s')(m) = (s + s')m = sm + s'm = f(s)(m) + f(s')(m)$, tj. $f(s + s') = f(s) + f(s')$;

2. $f(ss')(m) = (ss')m = s(s'm) = f(s)\big(f(s')(m)\big) = \big(f(s) \circ f(s')\big)(m)$, tj. $f(ss') = f(s) \circ f(s')$;
3. $f(1)(m) = 1m = m$, tj. $f(1) = id_M$.

Nechť f a g jsou dva homomorfismy zadávající na M stejnou strukturu bimodulu, tj. $f(s)(m) = sm = g(s)(m)$ pro všechna $s \in S, m \in M$. Pak $f = g$. ◇

Příklad 1.23. Buď M pravý R-modul. Ukažte, že existuje na M existuje právě jedna struktura $\mathbb{Z}$-R-bimodulu.

Řešení. Podle předchozího příkladu $\mathbb{Z}$-R-bimoduly M jednoznačně odpovídají homomorfismům $f\colon \mathbb{Z} \to \mathrm{End}(M)$, a takový je jediný. ◇

Příklad 1.24. Buď R komutativní okruh a M netriviální konečný (levý) R-modul bez torze. Ukažte, že R je těleso, a tedy M je ve skutečnosti vektorový prostor nad R.

Řešení. Ukážeme, že R je obor integrity. Připusťme na chvíli, že existují nenulové prvky $r, s \in R$ takové, že $r \cdot s = 0$. Pak pro libovolné nenulové $m \in M$ platí

$$0 = 0 \cdot m = (r \cdot s) \cdot m = r \cdot (s \cdot m).$$

Pokud $s \cdot m = 0$, pak $m \in \mathrm{Tor}(M)$; v opačném případě $s \cdot m \in \mathrm{Tor}(M)$. To je v obou případech spor s tím, že M je bez torze.

Nyní ukážeme, že R je konečné. Přesněji, ukážeme, že $|R| \leq |A|$. Předpokládejme, že $|R| > |A|$. To znamená, že existují prvky $r, s \in R, r \neq s$ takové, že $r \cdot m = s \cdot m$ pro nějaké nenulové m. Odtud dostáváme, že

$$r \cdot m - s \cdot m = \underbrace{(r - s)}_{\neq 0} \cdot m = 0,$$

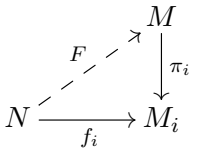
což opět není možné. Tím jsme ukázali, že R je konečný obor integrity, a tedy je to těleso. ◇

2. Součiny a přímé součty modulů, jádra a kojádra homomorfismů

Definice 2.1 (direktní součin)**.** Mějme indexovou množinu I a uvažujme R-moduly M_i, $i \in I$. Pak *direktní součin* modulů M_i je množinový kartézský součin $\prod_{i\in I} M_i$, pro který jsou akce okruhu R a sčítání definovány po složkách. Tento modul je dále vybaven *kanonickými projekcemi* na i-tou složku M_i, tj. homomorfismy $\pi_i\colon \prod_{i\in I} M_i \to M_i$, $\pi_i(m) = m_i$. Prvky součinu můžeme chápat jako posloupnosti (resp. I-tice) $m = (m_i)_{i\in I}$.
Direktní součin modulů M_i můžeme také definovat jako R-modul M splňující následující (*univerzální*) vlastnost:

(i) Jsou-li $f_i\colon N \to M_i$ homomorfismy modulů z libovolného R-modulu N, pak existuje jediný R-homomorfismus $F\colon N \to M$, splňující $\pi_i \circ F = f_i\colon N \to M_i$.

(ii) Tuto vlastnost lze vyjádřit diagramem, který komutuje pro libovolné N a f_i



Modul splňující tuto vlastnost značíme $\prod_{i\in I} M_i$ a je dán jednoznačně až na unikátní izomorfismus.

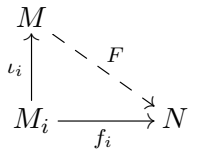
Definice 2.2 (direktní součet)**.** Pro libovolnou indexovou množinu I uvažujme R-moduly $M_i, i \in I$. Pak *direktní součet* modulů M_i je množina

$$\bigoplus_{i\in I} M_i = \{m \in \prod_{i\in I} M_i \mid \textit{pouze konečně mnoho } m_i \neq 0\}.$$

Prvky direktního součtu lze tedy chápat jako posloupnosti (I-tice), které mají konečně mnoho nenulových členů. Násobení a akce okruhu jsou dány po složkách. Tento modul je dále vybaven *kanonickými vloženími* M_i do M, tj. homomorfismy $\iota_i\colon M_i \to \bigoplus_{i\in I} M_i$, kde $\iota_i(m_i)$ je I-tice, která má na všech pozicích nuly, kromě i-té pozice, na které je prvek m_i.
Direktní součet modulů M_i můžeme také definovat jako R-modul M, splňující následující (*univerzální*) vlastnost:

(i) Jsou-li $f_i\colon M_i \to N$ homomorfismy modulů do libovolného R-modulu N, pak existuje jediný R-homomorfismus $F\colon M \to N$, splňující $F \circ \iota_i = f_i\colon M_i \to N$.

(ii) Což vyjádříme také pomocí diagramu, komutujícího pro všechna f_i:



Modul splňující tuto vlastnost zapisujeme ve tvaru $\bigoplus_{i\in I} M_i$ a je dán jednoznačně až na unikátní izomorfismus.

Poznámka.
Definice součtu a součinu jsou k sobě duální. Otočením směru šipek v prvním diagramu získáme diagram z definice druhé a naopak.

- *Vnitřní* a *vnější přímý součet* (definice vnitřního součtu viz. příklad 2.7 a především: Berrick A.J., Keating M.E. An introduction to rings and modules with K-theory in view 2000, str. 37.). Myšlenka zavedení vnitřního součtu spočívá v tom, že jsou-li $M_i \subseteq M$ podmoduly M, pak lze jejich prvky uvnitř M sčítat. Toho bychom chtěli využit k popisu M pomocí jeho vhodných podmodulů a poté psát $M = \bigoplus_{i\in I} M_i$. To by však nebylo korektní (totiž $m_1 + m_2 + ... + m_n \in M$, ale $(m_1, m_2, ..., m_n) \notin M$). K zavedení vnějšího přímého součtu nastává důvod v situaci, kdy neexistuje nějaký modul, který by obsahoval všechny M_i jako své podmoduly. Izomorfismus, který tento problém řeší je právě $m_1 + m_2 + ... + m_n \mapsto (m_1, m_2, ..., m_n)$.

Lemma 2.3. *Uvažujme R-moduly N, M_i, $i \in I$. Pak platí:*

(i) $\mathrm{Hom}_R\Big(N, \prod_{i\in I} M_i\Big) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$.

(ii) Platí rovnost $\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \cong \prod_{i\in I} \mathrm{Hom}_R\Big(M_i, N\Big)$.

Definice 2.4 (jádro/kernel)**.** Buď R okruh a $f\colon M \to N$ homomorfismus R-modulů. Jádrem f nazýváme množinu prvků z M, na kterých se f nuluje. Značíme

$$\ker(f) = \{m \in M \mid f(m) = 0_N\}.$$

Definice 2.5 (kojádro/cokernel)**.** Buď R okruh a $f\colon M \to N$ homomorfismus R-modulů. Kojádrem f nazýváme faktormodul $N/im(f)$. Značíme

$$\mathrm{coker}(f) = N/im(f).$$

Věta 2.6 (Vlastnosti direktního součtu)**.**

(i) Direktní součet je podmodul direktního součinu. Navíc, je-li v předešlé definici indexová množina I konečná, pak součin a součet je totéž.

(ii) Direktní součet je až na izomorfismus asociativní a komutativní.

Příklad 2.7. Buď $M = M_1 \oplus M_2$ vnitřní direktní součet R-modulů M_1, M_2. K nim uvažujme příslušnou množinu inkluzí a projekcí $\{\sigma_1, \sigma_2, \pi_1, \pi_2\}$. Pro daný endomorfismus $\mu \in \mathrm{End}(M)$ definujme pro $i, j \in \{1, 2\}$ následující R-homomorfismy modulů:

$$\pi_i \mu \sigma_j = \mu_{ij}\colon M_j \to M_i.$$

Ukažte, že pro $m \in M$, $m = m_1 + m_2$, $m_i \in M_i$, lze μ psát ve tvaru:

$$\mu(m) = (\mu_{11}(m_1) + \mu_{12}(m_2)) + (\mu_{21}(m_1) + \mu_{22}(m_2)).$$

Chápeme-li prvky M jako sloupce $\begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$, ukažte, že μ lze zapsat jako matici $\begin{pmatrix} \mu_{11} & \mu_{12} \\ \mu_{21} & \mu_{22} \end{pmatrix}$. Dále odvoďte, že okruh endomorfismů $\mathrm{End}(M)$ lze zapsat jako okruh matic 2×2:

$$\mathrm{End}(M) = \begin{pmatrix} \mathrm{End}(M_1) & \mathrm{Hom}(M_1, M_2) \\ \mathrm{Hom}(M_2, M_1) & \mathrm{End}(M_2) \end{pmatrix}.$$

Řešení. K ověření ekvivalentního vyjádření homomorfismu μ použijeme následující vlastnosti inkluzí σ_i a projekcí π_i:

1. $\sigma_i(m_i) = m_i$, $\forall m_i \in M_i$, $i = 1, 2$

2. $\pi_i(m_i) = m_i$, $\forall m_i \in M_i$, $i = 1, 2$
3. $m = \pi_1(m) + \pi_2(m)$, $\forall m \in M$.

Počítejme tedy:

$$\begin{aligned}
\mu(m) &= \big(\mu_{11}(m_1) + \mu_{12}(m_2)\big) + \big(\mu_{21}(m_1) + \mu_{22}(m_2)\big) \\
&= \pi_1\mu\sigma_1(m_1) + \pi_1\mu\sigma_2(m_2) + \pi_2\mu\sigma_1(m_1) + \pi_2\mu\sigma_2(m_2) \\
&= \pi_1(\mu\sigma_1(m_1) + \mu\sigma_2(m_2)) + \pi_2(\mu\sigma_1(m_1) + \mu\sigma_2(m_2)) \\
&= \pi_1(\mu(m_1) + \mu(m_2)) + \pi_2(\mu(m_1) + \mu(m_2)) \\
&= \pi_1(\mu(m_1 + m_2)) + \pi_2(\mu(m_1 + m_2)) \\
&= \pi_1(\mu(m)) + \pi_2(\mu(m)) \\
&= \mu(m)
\end{aligned}$$

Poslední úpravu jsme provedli díky tomu, že $\mu \in \mathrm{End}(M)$ (tedy $\mu(m) \in M$).

Chápeme-li prvky M jako sloupce tvaru $\begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$, $m_1 \in M_1$, $m_2 \in M_2$, pak

$$\mu(m) = (\mu_{11}(m_1) + \mu_{12}(m_2)) + (\mu_{21}(m_1) + \mu_{22}(m_2))$$

zapíšeme ve tvaru

$$\mu(m) = \begin{pmatrix} \mu_{11}(m_1) + \mu_{12}(m_2) \\ \mu_{21}(m_1) + \mu_{22}(m_2) \end{pmatrix}.$$

Z tohoto zápisu již lehce vidíme rovnost:

$$\mu(m) = \begin{pmatrix} \mu_{11} & \mu_{12} \\ \mu_{21} & \mu_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}. \qquad \diamond$$

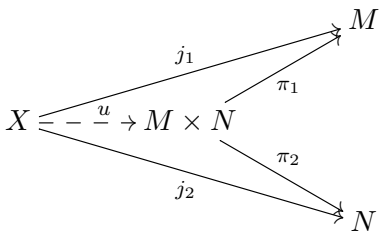
Příklad 2.8. Pro R-moduly M, N definujme jejich *biprodukt* jako modul X spolu s homomorfismy $i_1 \colon M \to X$, $i_2 \colon N \to X$, $j_1 \colon X \to M$, $j_2 \colon X \to N$ splňující rovnosti:

(i) $j_2 \circ i_1 = j_1 \circ i_2 = 0$
(ii) $j_1 \circ i_1 = id_M$
(iii) $j_2 \circ i_2 = id_N$
(iv) $i_1 \circ j_1 + i_2 \circ j_2 = id_X$

Ukažte, že $M \times N \cong X \cong M \oplus N$.

Řešení. Pomocí univerzální vlastnosti součinu. Uvažujme následující diagramy

$$M \underset{\pi_1}{\overset{i_1}{\rightleftarrows}} X \underset{\pi_2}{\overset{i_2}{\leftrightarrows}} N$$



Zobrazení u, které je dáno z univerzální vlastnosti součinu, dělá druhý diagram komutativní. Proto můžeme psát

$$\pi_1 \circ u = j_1,\ \pi_2 \circ u = j_2$$
$$u(x) = \big(\pi_1 \circ u(x), \pi_2 \circ u(x)\big) = \big(j_1(x), j_2(x)\big).$$

Prvně předpokládejme $u(x) = u(y)$ a ukažme injektivitu.

$$u(x) = u(y) \Rightarrow j_1(x) = j_1(y),\ j_2(x) = j_2(y) \Rightarrow$$
$$\Rightarrow i_1 \circ j_1(x) = i_1 \circ j_1(y),\ i_2 \circ j_2(x) = i_2 \circ j_2(y)$$

Sečteme-li poslední dvě rovností a aplikujeme poslední vztah z definice biproduktu získáváme

$$\big(i_1 \circ j_1 + i_2 \circ j_2\big)(x) = \big(i_1 \circ j_1 + i_2 \circ j_2\big)(y) \Rightarrow x = y.$$

Tedy u je injektivní. Dále $u(x) = \big(j_1(x), j_2(x)\big)$ a homomorfismy j_1, j_2 jsou surjektivní (v opačném případě by totiž nemohla platit druhá a třetí z rovností definujících biprodukt), je tedy i u surjektivní a dává izomorfismus mezi X a $M \times N$. Navíc tento součin je konečný, tedy platí $M \times N \cong M \oplus N$, což dává $X \cong M \oplus N$. ◇

Příklad 2.9. Ukažte, že pro okruh R a levé R-moduly M, $M_i, i \in I$ a N jsou množiny $\mathrm{Hom}_R\big(M, N\big)$, $\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$, $\prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ abelovské grupy. Dále ukažte, že je-li R komutativní, pak jde o levé R-moduly.

Řešení. Začněme s případem $\mathrm{Hom}_R\big(M, N\big)$. Prvky této množiny můžeme sčítat po složkách (*pointwise*):

$$(f + g)(m) = f(m) + g(m),$$

nulový prvek máme díky tomu, že mezi moduly existují nulové morfismy, inverze k f je $-f$ a asociativitu sčítání morfismů lze také vidět ihned:

$$\begin{aligned}\big(f + (g + h)\big)(m) &= f(m) + \big((g + h)\big)(m)\\ &= f(m) + \big(g(m) + h(m)\big)\\ &= \big(f(m) + g(m)\big) + h(m)\\ &= \big(f + g\big)(m) + h(m) = \big((f + g) + h\big)(m).\end{aligned}$$

Abychom ukázali, že pro R komutativní je $\mathrm{Hom}_R\big(M, N\big)$ levý R-modul, zaveďme levou akci prvků $r \in R$: $(r \cdot f)(m) := rf(m)$, kde $rf(m)$ dává smysl, neboť N je levý R-modul. Podmínky z definice modulu pro akci R jsou splněny:

1. $(r + s) \cdot f = (r + s)f = rf + sf = r \cdot f + s \cdot f$.
2. $r \cdot (f + g) = r(f + g) = rf + rg = r \cdot f + r \cdot g$.
3. $\big((rs) \cdot f\big)(m) = (rs)f(m) = r\big(sf(m)\big) = r \cdot \big(sf(m)\big) = r \cdot \big(s \cdot f\big)(m)$.

Komutativitu R potřebujeme pro kompatibilitu akce s multiplikativní strukturou R: pro $r, s \in R$, $m \in M$, $f \in \mathrm{Hom}_R\big(M, N\big)$ (tj. $sm \in M$ a $rf \in \mathrm{Hom}_R\big(M, N\big)$) lze psát:

$$\begin{aligned}\big((rs) \cdot f\big)(m) &= r \cdot \big(s \cdot f\big)(m)\\ &= r \cdot \big(sf(m)\big)\\ &= r \cdot \big(f(sm)\big)\\ &= rf(sm)\\ &= s\big(rf(m)\big)\\ &= s \cdot \big(r \cdot f(m)\big) = \big((sr) \cdot f\big)(m).\end{aligned}$$

Vidíme tedy, že libovolné $r, s \in R$ spolu musí komutovat.

Nyní pro libovolné $F, G \in \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$ a $m \in \bigoplus_{i\in I} M_i$ definujme

$$(F+G)(m) := F(m) + G(m).$$

Nulový prvek je nulový homomorfismus, inverzní prvek k F je $-F$. Pak díky tomu, že N je levý R-modul, lze psát:

1. $(-F+F)(m) = -F(m)+F(m) = 0_N, \forall m \in \bigoplus_{i\in I} M_i \Rightarrow -F+F = 0 \in \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$, tedy $-F$ je skutečně inverze k F.
2. $(F+G)(m) = F(m) + G(m) = G(m) + F(m) \Rightarrow (F+G) = (G+F)$.
3. $(F+(G+H))(m) = F(m) + (G+H)(m) = F(m) + G(m) + H(m) = (F(m)+G(m)) + H(m) \Rightarrow (F+(G+H)) = (F+G)+H$

Což platí pro libovolné $F, G, H \in \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$ a všechna $m \in \bigoplus_{i\in I} M_i$. Ověřili jsme tedy grupovou strukturu. Zavedeme-li levé násobení prvky z R:

$$(r \cdot F)m := rF(m),$$

pak lze identicky jako v předešlém ověřit, že $\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$ je také levý R-modul.

Pro $f, g \in \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ definujme

$$f + g := \big(f_i\big)_{i\in I} + \big(g_i\big)_{i\in I}.$$

Toto sčítání po složkách dává strukturu abelovské grupy díky vlastnostem cílového objektu morfismů f_i, $i \in I$ (tj. složek prvku $f \in \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$). Nulový objekt je zde I-tice nul a inverze k $f = \big(f_i\big)_{i\in I}$ je $-f = \big(-f_i\big)_{i\in I}$.
Skutečnost, že $\prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ je komutativní grupa, lze také vidět z toho, že každý prvek tohoto direktního součinu je abelovské grupa, což jsme ukázali na začátku tohoto cvičení. Levou akce R je po složkách:

$$r \cdot f := \big(r \cdot f_i\big)_{i\in I},$$

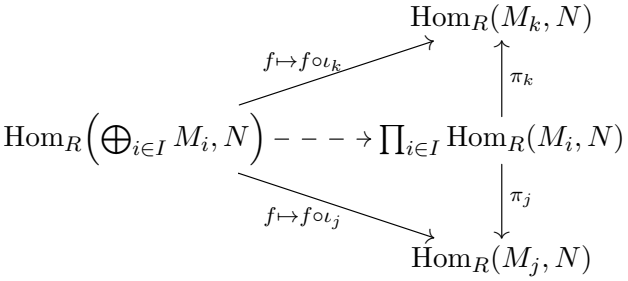
což je korektní, neboť na začátku tohoto cvičení jsme akci $r \cdot f_i$ zavedli a vzhledem k ní potřebné axiomy ověřili. ◇

Příklad 2.10. Dokažte, že $\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$ a $\prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ jsou izomorfní jako abelovské grupy, uvažujeme-li R jako okruh a M_i, N jako levé R-moduly. Dále ukažte, že je-li R komutativní, pak jde o izomorfismus levých R-modulů.

Řešení. Uvažujme $f \in \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$. Doména f je vybavena vnořeními $\iota_i \colon M_i \to \bigoplus_{i\in I} M_i$. Vyjádřeno diagramem:

$$M_i \xrightarrow{\iota_i} \bigoplus_{i\in I} M_i \xrightarrow{f} N$$

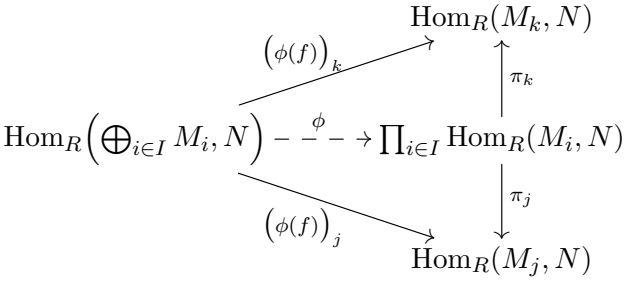
a pro všechna $i \in I$ je složení $f \circ \iota_i \colon M_i \to N$ prvek $\mathrm{Hom}_R(M_i, N)$. Proto $\big(f \circ \iota_i\big)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$.



Univerzální vlastnost direkntního součinu (viz. 2.1) nám říká, že máme-li objekt vybavený šipkami do všech prvků produktu, pak existuje (unikátní) zobrazení z tohoto objektu do produktu, které komutuje se všemi projekcemi, tj. máme morfismus

$$\phi \colon \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \to \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$$

definovaný takto: $\phi(f) = \big(\phi(f)\big)_{i\in I} = \big(f \circ \iota_i\big)_{i\in I}$.



Tvrzení je, že toto zobrazení je izomorfismus abelovských grup.
Prvně ověřme, že ϕ je skutečně homomorfismus.

1. $\big(\phi(0)\big)_i = 0 \circ \iota_i = 0$, $\forall i \in I$.
2. $\big(\phi(f+g)\big)_i = (f+g) \circ \iota_i = f \circ \iota_i + g \circ \iota_i = \big(\phi(f)\big)_i + \big(\phi(g)\big)_i$, $\forall i \in I$.

Dále ukažme, že ϕ je injektivní a surjektivní.

1. Buď $f \in \ker(\phi)$. Pak $\phi(f) = \big(\phi(f)\big)_{i\in I} = \big(f \circ \iota_i\big)_{i\in I} = 0 \Rightarrow f(m_i) = 0$, $\forall i \in I$, a všechna $m_i \in M_i$. Dohromady pro libovolné $m \in \bigoplus_{i\in I} M_i$ máme $f\big((m)_{i\in I}\big) = f\Big(\sum\limits_{i\in I} \iota_i(m)\Big) = \sum\limits_{i\in I} f\big(\iota_i(m)\big) = \sum\limits_{i\in I} 0 = 0$. Tedy $\ker \phi = 0$ a ϕ je injektivní.
2. Nyní vezměme libovolné $F \in \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$, které je dáno svými složkami $(F)_i = \pi_i(F) \colon M_i \to N$, $i \in I$. To ale znamená, že pro všechna $i \in I$ máme morfismus z M_i do N a podle univerzální vlastnosti koproduktu (viz. 2.2) existuje morfismus $f \in \bigoplus_{i\in I} M_i$ do N, který se všemi $(F)_i$ komutuje, tj. $f \circ \iota_i = (F)_i$, $\forall i \in I$. Pro něj platí $\phi(f) = F$.

Ukázali jsme, že ϕ je izomorfismus

$$\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N).$$

Našim posledním úkolem je ukázat, že uvažujeme-li všechny moduly tohoto cvičení jako levé moduly nad komutativním okruhem R, pak ϕ je izomorfismem levých R-modulů. Z předešlého příkladu víme, že má smysl se na takovýto izomorfismus ptát, protože již víme, jak struktura levých R-modulů na množinách $\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$, $\prod_{i\in I}\mathrm{Hom}_R(M_i,N)$ vypadá. Zbývá ukázat, že ϕ je kompatibilní se skalárním násobením. Uvažujme tedy libovolné $r\in R$, $f\in \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big)$ a počítejme:

$$\begin{aligned}\phi(r\cdot f) &= \big(\phi(rf)\big)_{i\in I}\\ &= \big((rf\circ\iota_i)\big)_{i\in I}\\ &= \big(r\cdot(f\circ\iota_i)\big)_{i\in I}\\ &= \big(r\cdot\phi(f)\big)_{i\in I}\\ &= r\cdot\big(\phi(f)\big)_{i\in I} = r\cdot\phi(f).\end{aligned}$$

Ukázali jsme, že ϕ je izomorfismus levých R-modulů. Proč je třeba předpokládat komutativitu R jsme viděli v předešlém příkladě. ◇

3. Volné moduly a projektivní moduly

3.1. Volné moduly

Definice 3.1 (Lineární nezávislost)**.** Mějme R-modul M a libovolnou množinu:

$$X = \{x_i \mid i \in I\} \subseteq M$$

Řekneme, že X je *lineárně nezávislá*, jestliže pro libovolnou konečnou podmnožinu $J \subseteq I$ platí:

$$\sum_{j \in J} r_j x_j = 0 \Rightarrow \forall j \in J : r_j = 0$$

Definice 3.2 (Báze)**.** Řekneme, že X je *báze* M, jestliže každé $x \in M$ umíme jediným způsobem vyjádřit jako součet:

$$x = \sum_{i \in I} r_i x_i$$

kde $r_i \in R$ pro každé $i \in I$, ale $r_i \neq 0$ pouze pro konečně mnoho i.

Definice 3.3 (Volný modul)**.** Modul M nad R nazveme volný, jestliže je součtem kopií R (jakožto modulu nad sebou samým), tj. jestliže existuje množina I splňující:

$$M \cong \bigoplus_{i \in I} R \quad \left(\text{zkráceně } \cong \bigoplus_{I} R \right)$$

Věta 3.4 (Vlastnosti volných modulů)**.** *Platí:*

(i) Množina X je báze R-modulu M právě tehdy, když $\langle X \rangle = M$ a X je lineárně nezávislá.

(ii) Volné moduly jsou právě ty, které mají bázi.

(iii) Každý R-modul je volný právě tehdy, když R je okruh s dělením.

(iv) Každý podmodul volného R-modulu je volný právě tehdy, když R je obor hlavních ideálů.

(v) Ideál J okruhu R je volný R-modul právě tehdy, když $J \cong R$.

(vi) Součet volných modulů je volný modul.

(vii) Součin volných modulů nemusí být volný modul.

Příklad 3.5. Přímo z definice nebo pomocí předchozí teorie argumentujte, zda jsou následující moduly volné.

1. $\mathbb{Z}$-modul $n\mathbb{Z}$
2. $\mathbb{Z}$-modul $\mathbb{Z} \times \mathbb{Z}$
3. $\mathbb{Z} \times \mathbb{Z}$-modul $\mathbb{Z} \times 0$
4. R-modul $R[x]$
5. $\mathbb{Z}$-modul $\mathbb{Z}_n$
6. $\mathbb{Z}_2$ modul $\mathbb{Z}_4$ s násobením $[k]_2 \cdot [\ell]_4 = [2k\ell]_4$
7. $\mathbb{Z}_2$-modul $\mathbb{Z}_8^*$ s násobením $[k]_2 \cdot [\ell]_8 = [\ell^k]_8$
8. $R[x, y]$-modul (x, y) (jako jeho ideál)

Řešení.

1. Ano, $n\mathbb{Z} \cong \mathbb{Z}$ skrze izomorfizmus $nk \mapsto k$.
2. Ano, konečné součiny splývají se součty, čili $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}$.
3. Ne. Pro libovolný prvek $x \in \mathbb{Z} \times 0$ platí $(1,1)x = (1,0)x$, čili $\mathbb{Z} \times 0$ nemůže mít nad $\mathbb{Z} \times \mathbb{Z}$ bázi.
4. Ano. Platí:
$$R[x] \cong \bigoplus_{n \in \mathbb{N}_0} Rx^n \cong \bigoplus_{\mathbb{N}_0} R$$
5. Ne. $\mathbb{Z}_n$ nemůže kvůli kardinalitě obsahovat sčítanec izomorfní se $\mathbb{Z}$.
6. Ne, $\mathbb{Z}_4$ sice obsahuje $\mathbb{Z}_2$-podmodul $2\mathbb{Z}_4$, ale není to jeho přímý sčítanec.
7. Ano, $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
8. Ne, neplatí $(x, y) \cong R[x, y]$, neboť tento ideál není hlavní.

◇

Příklad 3.6. Modul $\mathbb{Q}$ není volný $\mathbb{Z}$-modul.

Řešení. Předpokládejme, že máme bázi $X \subseteq \mathbb{Q}$ nad $\mathbb{Z}$. Jestliže $|X| > 1$, pak máme dvě různá $\frac{a}{b}, \frac{c}{d} \in X$ pro $a, b, c, d \in \mathbb{Z}$. Potom ale:

$$b \cdot \frac{a}{b} - d \cdot \frac{c}{d} = 0$$

což je spor s vlastností báze, neboť $b \neq 0 \neq d$. Proto by muselo platit $X = \{q\}$ tak, že pro každé $x \in \mathbb{Q}$ existuje $z \in \mathbb{Z}$ splňující $x = zq$, což je ale zřejmě nesmysl (jinak řečeno $\mathbb{Q}$ není cyklický $\mathbb{Z}$-modul). Proto $\mathbb{Q}$ nemá nad $\mathbb{Z}$ bázi a nemůže být volný. ◇

Příklad 3.7. Modul $\mathbb{R}$ není volný $\mathbb{Z}$-modul.

Řešení. Každá množina generující $\mathbb{R}$ nad $\mathbb{Z}$ by musela obsahovat alespoň dvě racionální čísla, protože $\mathbb{Q}$ není cyklický $\mathbb{Z}$-modul a $\mathbb{Z}$-lineární kombinací iracionálních čísel nedostaneme racionální číslo. Množina obsahující dvě různá racionální čísla nemůže být nezávislá nad $\mathbb{Z}$, jak vyplývá z předchozího příkladu. ◇

Příklad 3.8. Pro libovolné těleso $\mathbb{K}$ a libovolné $n \geq 2$ není $\mathbb{K}^n$ volný $\mathrm{Mat}_n(\mathbb{K})$-modul.

Řešení. Ukážeme, že každá jednoprvková množina v $\mathbb{K}^n$ je lineárně závislá nad $\mathrm{Mat}_n(\mathbb{K})$. Odtud posléze vyplyne, že tento modul nemůže mít bázi. Mějme libovolné nenulové $(x_1, \ldots, x_n) \in \mathbb{K}^n$. Protože $n \geq 2$, existují (ne všechna nulová) $r_1, \ldots, r_n \in \mathbb{K}$ splňující:

$$\sum_{i=1}^{n} r_i x_i = 0$$

Potom ale:

$$\begin{pmatrix} r_1 & \cdots & r_n \\ \vdots & \ddots & \vdots \\ r_1 & \cdots & r_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Přitom ale matice nalevo není celá nulová. ◇

Příklad 3.9. Ideál $J = (3, 2+\sqrt{-5})$ okruhu $\mathbb{Z}[\sqrt{-5}]$ není volný $\mathbb{Z}[\sqrt{-5}]$-modul.

Řešení. Musíme ukázat, že J není hlavní ideál. Nejprve uvažme zobrazení $h\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ s předpisem:

$$h(a+b\sqrt{-5}) = a^2 + 5b^2$$

Ukažme, že h je ve skutečnosti homomorfizmus monoidů (vzhledem k násobení). Platí:

$$\begin{aligned} h((a+b\sqrt{-5})(c+d\sqrt{-5})) &= (ac-5bd)^2 + 5(bc+ad)^2 \\ &= a^2c^2 - 10abcd + 25b^2d^2 + 5b^2c^2 + 10abcd + 5a^2d^2 \\ &= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 \\ &= (a^2+5b^2)(c^2+5d^2) = h(a+b\sqrt{-5})h(c+d\sqrt{-5}) \end{aligned}$$

Dále $h(x) = 1$ právě tehdy, když $x \in \{1, -1\}$. Nyní předpokládejme, že $J = (a)$. Nejprve uvažme možnost $J = \mathbb{Z}[\sqrt{-5}]$. Protože $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5)$, platí $J = \mathbb{Z}[\sqrt{-5}]$ právě tehdy, když $(3, x+2) = \mathbb{Z}[x]$. Pokud ale $1 = p(x)3 + q(x)(2+x)$ pro nějaké polynomy $p, q \in \mathbb{Z}[x]$, pak volbou $x = -2$ dostaneme $1 = p(-2)3$, což je spor. Proto J musí být vlastní ideál $\mathbb{Z}[\sqrt{-5}]$. Pro $a \neq \pm 1$. Dále musí existovat $x \in \mathbb{Z}[\sqrt{-5}]$ splňující $3 = ax$ a také $9 = h(3) = h(a)h(x)$. Protože $a \neq 1$, musí platit $h(x) = 1$ nebo $h(x) = 3$. Druhý případ není možný, neboť $a^2 + 5b^2 = 3$ nemá řešení v celých číslech. Proto $h(x) = 1$, tedy $x = \pm 1$ a $J = 3\mathbb{Z}[\sqrt{-5}]$. To je ovšem také spor, jelikož rovnice $2 + \sqrt{-5} = 3(a + b\sqrt{-5})$ nemá řešení v celých číslech. ◇

Příklad 3.10. Dokažte, že volný modul M nad oborem integrity R je bez torze.

Řešení. Nechť $x \in \mathrm{Tor}(M)$ a $r \in R$ jsou nenulové splňující $rx = 0$. Nechť $x_1, \ldots, x_n$ jsou prvky báze M a $r_1, \ldots, r_n \in R$ ne všechny nulové splňují $\sum_{i=1}^n r_i x_i = x$. Potom ale:

$$0 = rx = \sum_{i=1}^{n} r r_i x_i$$

Protože je R obor integrity, nemohou být všechny $rr_1, \ldots, rr_n$ nulové. Tím dostáváme nenulové vyjádření nuly, což je spor. Modul M musí být bez torze. ◇

Příklad 3.11. Dokažte, že konečně generovaný modul M bez torze nad oborem hlavních ideálů R je volný modul.

Řešení. Mějme množinu $\{x_1, \ldots, x_n\}$ generující modul M s minimální kardinalitou. Tvrzení dokážeme indukcí vzhledem k n. Nejprve zřejmě $\langle x_1 \rangle$ je volný R-modul, protože M je bez torze. Předpokládejme, že $\langle x_1, \ldots, x_i \rangle$ je volný a pro spor předpokládejme, že existuje $r \in R$ nenulové splňující:

$$r x_{i+1} + \sum_{k=1}^{i} r_k x_k = 0$$

Uvažme zobrazení $f(x) = rx$ pro $x \in \langle x_1, \ldots, x_{i+1} \rangle$. Každé takové x je tvaru $x = \sum_{k=1}^{i+1} s_k x_k$. Potom ale:

$$f(x) = r\sum_{k=1}^{i+1} s_k x_k = \sum_{k=1}^{i} r s_k x_k + s_{i+1} r x_{i+1} = \sum_{k=1}^{i} r s_k x_k + s_{i+1}\left(-\sum_{k=1}^{i} r_k x_k\right) \in \langle x_1, \ldots, x_n \rangle$$

Protože M je bez torze, je f monomorfizmus modulů. To znamená, že $\langle x_1, \ldots, x_i \rangle$ obsahuje podmodul, který není volný. To ale není možné, protože R je obor hlavních ideálů. ◇

Příklad 3.12. Dokažte, že každý konečně generovaný modul M nad oborem hlavních ideálů R lze rozložit $M \cong F \oplus T$, kde F je volný a T torzní modul.

Řešení. Mějme vzhledem ke kardinalitě nejmenší množinu X generující modul M. Položme $X_1 = X \cap \mathrm{Tor}(X)$ a $X_2 = X \setminus X_1$. Potom $\langle X_2 \rangle$ je konečně generovaný modul bez torze, tedy podle příkladu 3.11 volný. Modul $\langle X_1 \rangle$ je zřejmě torzní. Rovněž zřejmé je $M \cong \langle X_2 \rangle \oplus \langle X_1 \rangle$. ◇

Definice 3.13. R-modul M se nazývá *volný objekt nad množinou X v kategorii R-modulů*, jestliže existuje zobrazení $\iota : X \to M$ takové, že pro každý R-modul N a každé zobrazení $f : X \to N$ existuje právě jeden morfizmus $h : M \to N$ splňující $h \circ \iota = f$.

Věta 3.14. *Volné objekty v kategorii R-modulů jsou právě volné R-moduly.*

Příklad 3.15. Dokažte přímo z definice volného objektu, že zobrazení ι je vždy injektivní pro volné moduly nad netriviálním okruhem.

Řešení. Mějme netriviální okruh R a množinu X. Pokud X má méně než dva prvky, není co dokazovat. Nechť tedy existují $x, y \in X$, $x \neq y$, a nechť pro $\iota : X \to FX$ platí $\iota(x) = \iota(y)$. Zvolme zobrazení $h : X \to R$ dané:

$$h(m) = \begin{cases} 1 & \text{jestliže } m = x \\ 0 & \text{jinak} \end{cases}$$

Potom pro každé zobrazení (takže i každý morfizmus) $f : FX \to R$ musí platit:

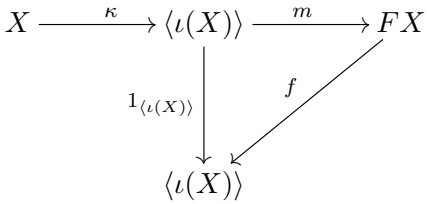
$$1 = h(x) = f(\iota(x)) = f(\iota(y)) = h(y) = 0$$

což není možné v netriviálním okruhu R. Proto ι musí být injektivní. ◇

Příklad 3.16. Dokažte přímo z předchozí definice, že pro každou množinu X platí:

$$\langle \iota(X) \rangle = FX$$

Řešení. Pro triviální okruh R je tato rovnice tvaru $\{0\} = \{0\}$ a není co dokazovat. Předpokládejme, že R je netriviální. Zřejmě $\langle \iota(X) \rangle \subseteq FX$, označme $m : \langle \iota(X) \rangle \to FX$ tuto inkluzi (jde o injektivní homomorfizmus modulů, ale to v tuto chvíli nepotřebujeme). Zobrazení $\iota : X \to FX$ se faktorizuje skrze m, tj. existuje $\kappa : X \to \langle \iota(X) \rangle$ splňující $\iota = m \circ \kappa$. Dostáváme unikátní homomorfizmus modulů $f : FX \to \langle \iota(X) \rangle$ z následujícího diagramu:



Potom platí $m \circ f = 1_{\langle \iota(X) \rangle}$, čili m je surjektivní a tedy identita. ◇

Příklad 3.17. Dokažte, že je-li F volný modul a $e : M \to F$ epimorfizmus, pak F je retrakt M, tj. existuje monomorfizmus $m : F \to M$ splňující $e \circ m = 1_F$.

Řešení. Mějme $\iota\colon X \to F$ vložení generátorů do volného modulu F. Protože je e surjektivní, pro každé $x \in X$ existuje $a_x \in M$ splňující $e(a_x) = x$ (v tomto momentě obecně potřebujeme axiom výběru). Položme $m(x) = a_x$. Z univerzální vlastnosti volného modulu plyne existence morfizmu $g\colon F \to M$ splňujícího $m = g \circ \iota$. Potom pro každé $y \in F$ plat $(e \circ m)(y) = e(a_y) = y$ neboli $e \circ m = 1_F$. ◇

Příklad 3.18. Dokažte znova příklad 3.12 pomocí příkladu 3.17.

Řešení. Je-li M konečně generovaný modul, potom $M/\operatorname{Tor}(M)$ je konečně generovaný modul bez torze, čili volný. Navíc máme přirozeně definovaný epimorfizmus - kanonickou projekci $p\colon M \to M/\operatorname{Tor}(M)$. Podle příkladu 3.17 je $M/\operatorname{Tor}(M)$ retrakt M a tedy jeho přímý sčítanec. Tím dostáváme součet

$$M \cong M/\operatorname{Tor}(M) \oplus \operatorname{Tor}(M).$$ ◇

Příklad 3.19. Z příkladu 3.12 plyne, že každý konečně generovaný modul nad oborem hlavních ideálů obsahuje maximální volný podmodul vzhledem k inkluzi. Rozhodněte, zda tuto vlastnost mají i nekonečně generované moduly.

Řešení. Ne, $\mathbb{Z}$-modul $\mathbb{Q}$ obsahuje nekonečný rostoucí systém volných podmodulů:

$$\mathbb{Z}\frac{1}{n} = \left\{ \frac{a}{n} \mid a \in \mathbb{Z} \right\}$$

jehož je $\mathbb{Q}$ sjednocením. Modul $\mathbb{Q}$ ovšem není volný, maximální volný podmodul tedy neobsahuje. ◇

Příklad 3.20. V příkladu 3.12 se tvrdí, že každý konečně generovaný modul nad oborem hlavních ideálů se dá rozložit na součet volného a torzního modulu. Rozhodněte, zda tuto vlastnost mají i nekonečně generované moduly.

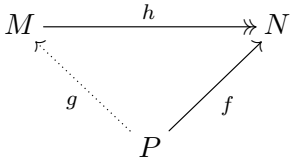
Řešení. Ne, uvažme $\mathbb{Z}$-modul $\mathbb{Q}$. Rozklad $\mathbb{Q} \cong \mathbb{Q} \oplus 0$ nepřichází v úvahu, protože $\mathbb{Q}$ není volný. Rozklad s netriviálním torzním podmodulem rovněž nepřichází v úvahu, neboť $\mathbb{Q}$ je bez torze. ◇

Příklad 3.21. V příkladu 3.12 se tvrdí, že každý konečně generovaný modul M nad oborem hlavních ideálů se dá rozložit $M \cong F \oplus T$, kde F je volný a T torzní modul. Můžeme přitom za F dosadit kterýkoli izomorfní podmodul M?

Řešení. Nemůžeme. Máme rozklad $\mathbb{Z} \cong \mathbb{Z} \oplus 0$. Přitom $\mathbb{Z} \cong n\mathbb{Z}$ pro libovolné $n \geq 1$, ale pro $n \geq 2$ není $n\mathbb{Z}$ přímý sčítanec $\mathbb{Z}$ (je mu pouze izomorfní). ◇

3.2. Projektivní moduly

Definice 3.22. Modul P se nazývá *projektivní*, jestliže pro libovolný epimorfizmus $h\colon M \to N$ a libovolný morfizmus $f\colon P \to N$ existuje morfizmus $g\colon P \to M$ splňující $h \circ g = f$. Neboli pokud:



Věta 3.23. *Vlastnosti projektivních modulů:*

(i) Každý volný modul je projektivní.

(ii) Součet projektivních modulů je projektivní.

(iii) Přímý sčítanec projektivního modulu je projektivní.

(iv) Projektivní moduly jsou právě přímé sčítance volných modulů.

(v) Projektivní moduly nad obory hlavních ideálů jsou volné.

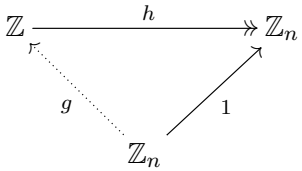
(vi) Pro každý idempotent e okruhu R je $\langle e\rangle$ $(= Re)$ projektivní R-modul.

Příklad 3.24. Dokažte, že $\mathbb{Z}$-moduly $\mathbb{Q}$ a $\mathbb{R}$ nejsou projektivní.

Řešení. Víme, že $\mathbb{Q}$ není volný $\mathbb{Z}$-modul. Pokud by modul $\mathbb{Q}$ byl projektivní, byl by přímým sčítancem nějakého volného $\mathbb{Z}$-modulu. Přímé sčítance volných komutativních grup jsou ovšem opět volné. Tatáž argumentace platí pro $\mathbb{R}$. ◇

Příklad 3.25. $\mathbb{Z}_n$ není projektivní $\mathbb{Z}$-modul pro žádné $n \geq 2$.

Řešení. Pokud by $\mathbb{Z}_n$ byl projektivní $\mathbb{Z}$-modul, potom by se identita $1\colon \mathbb{Z}_n \to \mathbb{Z}_n$ faktorizovala přes modul $\mathbb{Z}$ podle definice projektivního modulu:



Jenomže jediný morfizmus modulu $\mathbb{Z}_n$ do $\mathbb{Z}$ je nulový. Potom musí být nulové i jeho složení s h a předchozí trojúhelník nemůže nikdy komutovat. ◇

Příklad 3.26. Ideál $J = (3.2 + \sqrt{-5})$ okruhu $\mathbb{Z}[\sqrt{-5}]$ je projektivní $\mathbb{Z}[\sqrt{-5}]$-modul.

Řešení. Mějme morfizmus $p\colon \mathbb{Z}[\sqrt{-5}]^2 \to J$ daný předpisem:

$$p(r,s) = 3r + (2+\sqrt{-5})s$$

Zvolme zobrazení $e\colon J \to \mathbb{Z}[\sqrt{-5}]^2$ předpisem:

$$e(3a + (2+\sqrt{-5})b) = (2a + 3b - a\sqrt{-5}, a - b + (a+b)\sqrt{-5})$$

Toto zobrazení je $\mathbb{Z}[\sqrt{-5}]$-lineární. Nyní počítejme:

$$\begin{aligned}(p \circ e)(3a + (2+\sqrt{-5})b) &= p(2a+3b-a\sqrt{-5}, a-b+(a+b)\sqrt{-5}) \\ &= 3(2a+3b-a\sqrt{-5}) + (2+\sqrt{-5})(a-b+(a+b)\sqrt{-5}) \\ &= 3a + (2+\sqrt{-5})b\end{aligned}$$

neboli $p \circ e = 1_J$. To znamená, že J je retraktem R^2, čili jeho přímý sčítanec. Přímý sčítanec volného modulu je projektivní. ◇

Příklad 3.27. Nechť R je okruh a $e \in R$ idempotent. Dokažte:

1. Re je projektivní R-modul tím, že jej vyjádříte jako přímý sčítanec R
2. Re je volný R-modul právě tehdy, když $e \in \{0, 1\}$
3. jestliže R je obor integrity, tak Re je volný R-modul

Pomocí těchto výsledků rozložte následující okruhy R na netriviální součty projektivních R-modulů: $\mathbb{Z}_6$, $\mathrm{Mat}_2(\mathbb{R})$, $\mathbb{Z}[x]/(x^2+x)$.

Řešení. Nejprve si uvědomme, že pokud je e idempotent, potom také $1-e$ je idempotent:

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$$

1. Ukážeme, že $R \cong Re \oplus R(1-e)$. Nejprve každé $r \in R$ umíme vyjádřit jako $r = re + r(1-e)$. Nyní pokud $ae = b(1-e)$, potom $(a+b)e = b$ a $(a+b)e(1-e) = (a+b)(e-e) = 0$. Proto $Re \cap R(1-e) = \{0\}$ a jsme hotovi.
2. Zřejmě pokud $e \in \{0, 1\}$, pak Re je volný. Naopak pokud je Re volný, pak buď $Re = 0$ a $e = 0$, nebo $Re = R$ a e je jednotka. To by ale znamenalo $e = e1 = eee^{-1} = ee^{-1} = 1$.
3. V oboru integrity nemáme dělitelne nuly. Proto $e(1-e) = 0$ implikuje $e \in \{0, 1\}$ a Re je volný.

Okruh $\mathbb{Z}_6$ obsahuje netriviální idempotenty 3 a 4, v tomto případě platí $1-3 = 4$ a $1-4 = 3$. Proto:

$$\mathbb{Z}_6 \cong 3\mathbb{Z}_6 \oplus 4\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Okruh $\mathrm{Mat}_2(\mathbb{R})$ obsahuje celou řadu netriviálních idempotentů:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}, \dots$$

Dostáváme tředa následující rozklad:

$$\mathrm{Mat}_2(\mathbb{R}) \cong \mathrm{Mat}_2(\mathbb{R}) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus \mathrm{Mat}_2(\mathbb{R}) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Přitom:

$$\mathrm{Mat}_2(\mathbb{R}) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | a, b \in \mathbb{R} \right\}$$

$$\mathrm{Mat}_2(\mathbb{R}) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} | c, d \in \mathbb{R} \right\}$$

Idempotentní prvky okruhu $\mathbb{Z}[x]/(x^2+x)$ jsou faktory polynomu x^2+x:

$$\mathbb{Z}[x]/(x^2+x) \cong \{[0], [x]\} \oplus \{[0], [x+1]\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$ ◇

Příklad 3.28. Dokažte, že každý projektivní modul je bez torze.

Důkaz. Pokud by měl projektivní modul neprázdnou torzi, potom by také volný modul, jehož je přímým sčítancem, měl neprázdnou torzi, což není možné. □

Příklad 3.29. Najděte modul bez torze, který není projektivní.

Řešení. $\mathbb{Z}$-modul $\mathbb{Q}$ je zřejmě bez torze. Už jsme si ukázali, že tento modul není projektivní. ◇

Příklad 3.30. Dokažte, že pro každé těleso $\mathbb{K}$ je každý $\mathrm{Mat}_n(\mathbb{K})$-modul je projektivní.

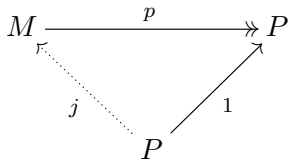
Řešení. Platí:

$$\mathbb{K} \cong \mathrm{Mat}_n(\mathbb{K}) \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Jelikož je matice napravo idempotentní, je tento modul projektivní (podle úvodní teorie nebo podle příkladu 3.27). ◇

Příklad 3.31. Dokažte, že modul P je projektivní právě tehdy, když pro každý epimofizmus $p\colon M \to P$ existuje $j\colon P \to M$ splňující $p \circ j = 1_P$.

Řešení.
$\Rightarrow$: Nechť P je projektivní a $p\colon M \to P$ je libovolný epimorfizmus. Podle definice projektivního modulu umíme následující trojúhelník doplnit na komutující:



čili $p \circ j = 1$.
$\Leftarrow$: Víme, že každý modul je homomorfním obrazem nějakého volného modulu. Mějme tedy takový epimorfizmus $p\colon F \to P$. Podle předpokladu existuje $j\colon P \to F$ splňující $p \circ j = 1_P$. Čili modul P je retraktem volného modulu a tedy jeho přímý sčítanec. Přímé sčítance volných modulů jsou projektivní. ◇

Příklad 3.32. Dokažte, že modul P je projektivní právě tehdy, když se libovolná krátká exaktní posloupnost následujícího tvaru štěpí:

$$0 \longrightarrow N \xrightarrow{m} M \xrightarrow{p} P \longrightarrow 0$$

Řešení.
$\Rightarrow$: Jestliže je modul P projektivní, pak se podle příkladu 3.31 štěpí a štěpí se i tato krátká exaktní posloupnost.
$\Leftarrow$: Libovolný epimorfizmus $p\colon M \to P$ zadává krátkou exaktní posloupnost:

$$0 \longrightarrow \ker p \xrightarrow{\iota} M \xrightarrow{p} P \longrightarrow 0$$

která se podle předpokladu štěpí. Štěpí se tedy i epimorfizmus p a P je opět podle příkladu 3.31 projektivní. ◇

Příklad 3.33. Dokžte implikaci $\Leftarrow$ v příkladu 3.31 přímo z definice projektivního modulu s využitím konstrukce tzv. pullbacku. Pullback morfizmů $f\colon A \to C$ a $g\colon B \to C$ je modul:

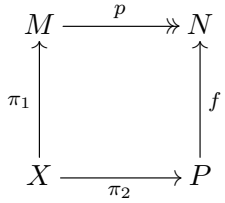
$$A \times_C B = \{(a, b) \in A \times B \mid f(a) = g(b)\}$$

Tento modul je podmodulem $A \times B$, má tedy přirozené definované morfizmy $p_1\colon A \times_C B \to A$ a $p_2\colon A \times_C B \to B$ s předpisy $p_1(a, b) = a$ a $p_2(a, b) = b$. (Pullback je jednoznačně určen svou univerzální vlastností, kterou se zde zabývat nebudeme.)

Řešení. Mějme libovolný epimorfizmus $p\colon M \to N$ a libovolný morfizmus $f\colon P \to N$. Uvažme pullback $X = M \times_N P$. Platí $p \circ p_1 = f \circ p_2$, ověřme:

$$(p \circ p_1)(a, b) = p(a) = f(b) = (f \circ p_2)(a, b)$$

Máme tedy komutativní čtverec:



Protože p je surjektivní, existuje ke každému $b \in P$ takové $a \in M$, že $p(a) = f(b)$. To znamená, že morfizmus p_2 je epimorfizmus a ten se podle předpokladu štěpí $p_2 \circ j = 1_P$. Dostáváme tedy morfizmus $g = p_1 \circ j$ splňující:

$$p \circ g = p \circ p_1 \circ j = f \circ p_2 \circ j = f$$

Modul P je tedy projektivní. $\diamond$

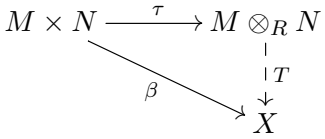
4. Tenzorový součin a jeho vlastnosti

Definice 4.1 (Tenzorový součin)**.** Buďte R okruh s jedničkou, M pravý a N levý R-modul. *Tenzorový součin* M s N nad okruhem R, značený $M \otimes_R N$, je abelovská grupa splňující následující univerzální vlastnost:

- Pro libovolný R-bilineární homomorfismus $\beta\colon M \times N \to X$, kde X je komutativní grupa, existuje jediné zobrazení $T\colon M \otimes_R N \to X$ splňující $T \circ \tau = \beta$. Homomorfismus grup $\tau\colon M \times N \to M \otimes_R N$ je dán $(m,n) \mapsto m \otimes n$, zachovává aditivitu v obou složkách (tj. je to bilineárního homomorfismus komutativních grup) a splňuje

$$\forall m_1, m_2 \in M,\ n_1, n_2 \in N:\ \tau(mr, n) = \tau(m, rn).$$

  Ekvivalentně pomocí komutativního diagramu



Konstrukce 4.2 (Konstrukce tenzorového součinu)**.** *Tenzorový součin je faktor grupa volné abelovské grupy F, generované prvky tvaru $m \otimes n$, $m \in M$, $n \in N$ (tj. $F = \langle m \otimes n,\ m \in M,\ n \in N \rangle$). Relace jsou generovány*

$$(m_1 + m_2) \otimes n \sim m_1 \otimes n + m_2 \otimes n$$
$$m \otimes (n_1 + n_2) \sim m \otimes n_1 + m \otimes n_2$$
$$mr \otimes n \sim m \otimes rn.$$

Provedeme-li následující označení:

$$l_1 = (m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n,$$
$$l_2 = m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2,$$
$$a_R = mr \otimes n - m \otimes rn,$$

lze psát

$$M \otimes_R N = F/\langle l_1,\ l_2,\ a_R \rangle.$$

Poznámka. R-balancovanost homomorfismu β není bilinearita jako u vektorových prostorů, o X se totiž nepředpokládá, že je R-modul. Proto není pravdivá rovnost $\beta(mr, n) = r\beta(m, n) = \beta(m, rn)$ (výraz $r\beta(m, n)$ by nedával smysl), ale platí pouze $\beta(mr, n) = \beta(m, rn)$. Tato vlastnost se také nazývá *R-bilinearita.*

Lemma 4.3 (Asociativita tenzorového součinu)**.** *Buďte M_i, $i \in \{1, 2, 3\}$ levé moduly nad komutativním okruhem R. Pak platí*

$$M_1 \otimes (M_2 \otimes M_3) \cong (M_1 \otimes M_2) \otimes M_3.$$

Věta 4.4. *Buď I indexová množina a pro všechna $i \in I$ uvažujme R-moduly M_i, dále uvažujme R-modul N. Pak platí*

$$N \otimes \left(\bigoplus_{i \in I} M_i \right) \cong \bigoplus_{i \in I} (N \otimes M_i),$$
$$\left(\bigoplus_{i \in I} M_i \right) \otimes N \cong \bigoplus_{i \in I} (M_i \otimes N).$$

Důsledek 4.5. *Buď R komutativní okruh, $M \cong R^s$, $N \cong R^t$ volné R-moduly s bázemi $m_1, ..., m_s$ a $n_1, ..., n_t$. Pak $M \otimes_R N$ je volný modul s bazí $m_i \otimes n_j$, $1 \leq i \leq s$, $1 \leq j \leq t$, tj. platí*

$$M \otimes_R N \cong R^{st}.$$

Příklad 4.6. Ukažte, že $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ a $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ jsou levé $\mathbb{R}$-moduly, které ale jako $\mathbb{R}$-moduly nejsou izomorfní.

Řešení. Levou akci $\mathbb{R}$ lze pro $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ i $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ zadefinovat stejně, necháme-li $r \in \mathbb{R}$ působit na první složku prvků tenzorových součinů

$$r \cdot z_1 \otimes_{\mathbb{R}} z_2 = rz_1 \otimes_{\mathbb{R}} z_2$$

$$r \cdot z_1 \otimes_{\mathbb{C}} z_2 = rz_1 \otimes_{\mathbb{C}} z_2.$$

Díky tomu skutečně získáváme strukturu $\mathbb{R}$-modulu na patřičné abelovské grupě, protože již $\mathbb{C}$ je $\mathbb{R}$-modulem. Pomocí elementárních úprav ověřme axiomy z definice modulu. Pro $\forall r_1, r_2 \in \mathbb{R}$ a $\forall z_1, z_2, z_3 \in \mathbb{C}$ platí

1. $(r_1 + r_2) \cdot z_1 \otimes z_2 = (r_1 + r_2)z_1 \otimes z_2 = r_1 z_1 \otimes z_2 + r_2 z_1 \otimes z_2 = r_1 \cdot z_1 \otimes z_2 + r_2 \cdot z_1 \otimes z_2$
2. $r \cdot (z_1 \otimes z_3 + z_2 \otimes z_3) = r \cdot (z_1 + z_2) \otimes z_3 = r(z_1 + z_2) \otimes z_3 = (rz_1 + rz_2) \otimes z_3 = rz_1 \otimes z_3 + rz_2 \otimes z_3) = r \cdot z_1 \otimes z_3 + r \cdot z_2 \otimes z_3)$
3. $(r_1 r_2) \cdot z_1 \otimes z_2 = (r_1 r_2)z_1 \otimes z_2 = r_1(r_2 z_1) \otimes z_2 = r_1 \cdot (r_2 z_1) \otimes z_2$

Abychom ukázali neexistenci izomorfismu mezi výše definovanými $\mathbb{R}$-moduly, použijeme dimenzionální analýzu. Z lineární algebry víme, že

$$\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R},$$

a proto podle věty 4.4

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^4.$$

Dále platí

$$\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C} \cong \mathbb{R}^2.$$

Vidíme tedy, že $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ a $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ jsou izomorfní vektorovým prostorům různých dimenzí. Z tohoto důvodu mezi nimi nemůže existovat izomorfismus. ◇

Příklad 4.7. Ukažte, že $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ a $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ jsou izomorfní jako $\mathbb{Q}$-moduly.

Řešení. Ověření, že obě dvě abelovské grupy jsou moduly nad $\mathbb{Q}$, se provede stejně jako v předešlém příkladě (akce je definována analogicky, tj. na levé složce). Pak $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ můžeme chápat jako jednodimenzionální vektorový prostor nad $\mathbb{Q}$, protože $\mathbb{Q}$ je těleso (moduly nad tělesy jsou právě vektorové prostory) a existuje *kanonický izomorfismus* který vypadá takto

$$q \mapsto q \otimes 1.$$

Z teorie vektorových prostorů víme, že každé dva konečně dimenzionální vektorové prostory nad stejným tělesem jsou jako vektorové prostory izomorfní (což v našem případě bude znamenat izomorfismus $\mathbb{Q}$-modulů). Stačí nám tedy ukázat, že $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ je vektorový prostor dimenze jedna.

Uvažujme prvek $1 \otimes 1$ a ukažme, že pomocí něj vygenerujeme libovolný prvek tvaru $p_1/p_2 \otimes q_1/q_2$. Protože akci $\mathbb{Q}$ jsme definovali na levé složce tenzorového součinu, jsme schopni vygenerovat prvek $p_1/p_2 \otimes 1$:

$$p_1/p_2 \otimes 1 = p_1/p_2 \cdot (1 \otimes 1).$$

Obdobně dostaneme q_1 na pravou složku, protože $q_1 \in \mathbb{Z}$, tj.

$$q_1 \cdot (p_1/p_2 \otimes 1) = q_1(p_1/p_2) \otimes 1 = (p_1/p_2)q_1 \otimes 1 = p_1/p_2 \otimes q_1.$$

Nakonec prvek $p_1/p_2 \otimes q_1/q_2$ získáme díky rovnostem

$$1/q \otimes 1 = 1/q \otimes (\sum_{i=1}^{q} 1/q) = \sum_{i=1}^{q} (1/q \otimes 1/q) = (\sum_{i=1}^{q} 1/q) \otimes 1/q = 1 \otimes 1/q.$$

Tenzor $1 \otimes 1$ je různý od nuly, tedy $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ je jím generován, proto je to jednodimenzionální $\mathbb{Q}$-vektorový prostor. Důsledkem je

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}. \qquad \diamond$$

Příklad 4.8.
Nechť $\varphi\colon R \to S$ je homomorfismus okruhů a uvažujme R-modul M. Popište na $S \otimes_R M$ strukturu S-modulu a dokažte pro každý S-modul N existenci izomorfismu

$$\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_S(S \otimes_R M, N).$$

Řešení.
V prvé řadě si vzpomeneme, že S je levý modul sám nad sebou. Dále pomocí homomorfismu φ lze na S definovat akci okruhu R:

$$s \cdot r := s\varphi(r),$$

(viz. příklad 1.18) tedy strukturu pravého R-modulu. Díky asociativitě S platí

$$(s_1 \cdot s_2) \cdot r = (s_1 s_2) \cdot r = (s_1 s_2)\varphi(r) = s_1(s_2\varphi(r)) = s_1 \cdot (s_2\varphi(r)) = s_1 \cdot (s_2 \cdot r)$$

(což je axiom provázanosti akcí y definice bimodulů). To z S dělá S-R-bimodul. Homomorfismus φ nám na $S \otimes_R M$ umožnil zavést strukturu S-modulu. Tento postup se nazývá *rozšíření skalárního násobení*. Můžeme tedy uvažovat abelovskou grupu $\mathrm{Hom}_S(S \otimes_R M, N)$ všech homomorfismů mezi $S \otimes_R M$ a N.

Ukážeme, jakým způsobem lze S-modul N chápat jako R-modul. Jinými slovy: pomocí φ provedeme tzv. *restrikci skalárního násobení* z prvků S na prvky R. Definujme pro $r \in R$ akci na N: $r \cdot n = \varphi(r)n$. Komutativní grupu $\mathrm{Hom}_R(M, N)$ tedy chápeme ve smyslu předešlého kroku.

Nyní k hledanému izomorfismu. Vezměme si libovolný prvek $f \in \mathrm{Hom}_R(M, N)$. Obraz f při homomorfismu $\Phi\colon \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, N)$ je dán následujícím složením

$$S \otimes_R M \xrightarrow{id_S \otimes f} S \otimes_R N \xrightarrow{P} N\ .$$

Morfismus S-modulů P je: $s \otimes n \mapsto sn$. Tedy

$$\Phi(f) = P \circ id_S \otimes f \in \mathrm{Hom}_S(S \otimes_R M, N).$$

Všimněte si prostředního člene. Je to rozšíření skalárního násobení R-modulu N na okruh S. Provedli jsme tedy nejprve restrikci a poté extenzi skalárů na N.

K sestrojení Φ^{-1} použijeme tzv. *kanonický izomorfismus*

$$I\colon M \cong R \otimes_R M,$$

$$m \mapsto 1 \otimes m.$$

Pak Φ^{-1} je pro libovolné $\psi \in \mathrm{Hom}_S(S \otimes_R M, N)$ dáno následujícím složením

$$M \xrightarrow{\ I\ } R \otimes_R M \xrightarrow{\varphi \otimes id_M} S \otimes_R M \xrightarrow{\ \psi\ } N\ .$$

Prvek $\psi \in \mathrm{Hom}_S(S \otimes_R M, N)$ je poslán na $\Phi^{-1}(\psi) = \psi \circ (\varphi \otimes id_M) \circ I\colon M \to N$.

To, že Φ je homomorfismem abelovských grup plyne z linearity tenzorového součinu v druhé složce. Zbývá ověřit $\Phi^{-1} \circ \Phi = id_{\mathrm{Hom}_R(M,N)}$ a $\Phi \circ \Phi^{-1} = id_{\mathrm{Hom}_S(S \otimes_R M, N)}$.

$$\Phi(\bullet) = \bullet \circ \varphi \otimes_R id_M \circ I,$$

$$\Phi^{-1}(\bullet) = P \circ id_S \otimes \bullet.$$

Pro $\psi \in \mathrm{Hom}_S(S \otimes_R M, N)$ platí

$$\Phi \circ \Phi^{-1}(\psi) = \Phi\big(\Phi^{-1}(\psi)\big) = (P \circ id_S \otimes \psi) \circ (\varphi \otimes_R id_M) \circ I,$$

které m posílá takto

$$m \mapsto 1_R \otimes m \mapsto \varphi(1_R) \otimes m \mapsto 1_S \otimes \psi(m) \mapsto 1_S \psi(m) = \psi(m) \Leftrightarrow m \mapsto \psi(m).$$

Ukázali jsme tedy, že $\big(\Phi \circ \Phi^{-1}(\psi)\big)(m) = \psi(m)$, pro libovolné $m \in M$. Proto

$$\Phi \circ \Phi^{-1} = Id_{\mathrm{Hom}_S(S \otimes_R M, N)}.$$

Analogicky se ukáže rovnost

$$\Phi^{-1} \circ \Phi = Id_{\mathrm{Hom}_R(M,N)}. \qquad \diamond$$

5. Ploché moduly

Definice 5.1. Nechť R je libovolný okruh a L, M jsou libovolné levé R-moduly. Pravý R-modul F nazveme *plochý* (nad R), jestliže pro libovolný injektivní homomorfismus R-modulů

$$\psi\colon L \longrightarrow M$$

je

$$id_F \otimes \psi\colon F \otimes_R L \longrightarrow F \otimes_R M$$

injektivní homomorfismus grup.

Věta 5.2. *Nechť D je pravý R-modul a L, M, N jsou levé R-moduly. Jestliže je posloupnost*

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

exaktní, pak je posloupnost

$$D \otimes_R L \xrightarrow{\psi} D \otimes_R M \xrightarrow{\varphi} D \otimes_R N \longrightarrow 0$$

exaktní.

Věta 5.3. *Každý projektivní R-modul je plochý.*

Nechť M je pravý R-modul. Na abelovské grupě $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ definujeme strukturu levého R-modulu následujícím způsobem:

$$\forall r \in R,\ \forall f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}),\ \forall x \in M: \quad (rf)(x) = f(rx).$$

Definice 5.4. Levý R-modul $M' := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ se nazývá *modul charakterů M.*

Věta 5.5 (Lambek)**.** *Pravý R-modul M je plochý právě tehdy, když jeho modul charakterů M' je injektivní.*

Tato věta nám společně s Baerovým kritériem dává kritérium pro ploché moduly:

Věta 5.6 (Kritérium pro ploché moduly)**.** *Pravý R-modul M je plochý právě tehdy, když pro každý konečně generovaný levý ideál $I \subseteq R$ je homomorfismus grup $M \otimes_R I \to MI$ daný předpisem $m \otimes i \mapsto mi$ izomorfismus.*

Příklad 5.7. Nechť A_1 a A_2 jsou R-moduly. Dokažte, že $A_1 \oplus A_2$ je plochý právě tehdy, když A_1 a A_2 jsou ploché.

Řešení. Nechť L, M jsou levé R-moduly a $\varphi\colon L \longrightarrow M$ je injektivní homomorfismus R-modulů. Z vlastností direktního součtu plyne: Indukovaná zobrazení

$$id_{A_1} \otimes \varphi\colon A_1 \otimes L \longrightarrow A_1 \otimes M,$$
$$id_{A_2} \otimes \varphi\colon A_2 \otimes L \longrightarrow A_2 \otimes M$$

jsou injektivní právě tehdy, když jejich direktní součet

$$(id_{A_1} \otimes \varphi) \oplus (id_{A_2} \otimes \varphi) \colon (A_1 \otimes L) \oplus (A_2 \otimes L) \longrightarrow (A_1 \otimes M) \oplus (A_2 \otimes M)$$

je injektivní. Aplikací věty 4.4 dostaneme diagram

$$\begin{array}{ccc} (A_1 \otimes L) \oplus (A_2 \otimes L) & \longrightarrow & (A_1 \otimes M) \oplus (A_2 \otimes M) \\ \cong \uparrow & & \uparrow \cong \\ (A_1 \oplus A_2) \otimes L & \xrightarrow[id_{A_1 \oplus A_2} \otimes \varphi]{} & (A_1 \oplus A_2) \otimes M \end{array}$$

Snadno se ověří, že tento diagram komutuje. To znamená, že indukované zobrazení

$$id_{A_1 \oplus A_2} \otimes \varphi \colon (A_1 \oplus A_2) \otimes L \longrightarrow (A_1 \oplus A_2) \otimes M$$

je injektivní právě, když $(id_{A_1} \otimes \varphi) \oplus (id_{A_2} \otimes \varphi)$ je injektivní. ◇

Příklad 5.8. Nechť R a S jsou okruhy s jedničkou. Předpokládejme, že M je pravý R-modul a N je (R, S)-bimodul. Ukažte, že pokud je M plochý nad R a N je plochý nad S, pak je také $M \otimes_R N$ plochý nad S.

Řešení. Nechť K, L jsou levé S-moduly a $\varphi \colon K \longrightarrow L$ je homomorfismus S-modulů. Chceme ukázat, že pak také indukované zobrazení

$$id_{M \otimes_R N} \otimes \varphi \colon (M \otimes_R N) \otimes_S K \longrightarrow (M \otimes_R N) \otimes_S L$$

je injektivní. Protože je N plochý nad S, máme, že indukované zobrazení

$$id_N \otimes \varphi \colon N \otimes_S K \longrightarrow N \otimes_S L$$

je injektivní homomorfismus R-modulů (zde využíváme toho, že na $N \otimes_S K$ a $N \otimes_S L$ máme strukturu levého R-modulu). Protože je M plochý nad R, dostáváme, že také

$$id_M \otimes (id_N \otimes \varphi) \colon M \otimes_R (N \otimes_S K) \longrightarrow M \otimes_R (N \otimes_S L)$$

je injektivní. Z věty 4.4 dostaneme následující diagram

$$\begin{array}{ccc} M \otimes_R (N \otimes_S K) & \longrightarrow & M \otimes_R (N \otimes_S L) \\ \cong \uparrow & & \uparrow \cong \\ (M \otimes_R N) \otimes_S K & \longrightarrow & (M \otimes_R N) \otimes_S L. \end{array}$$

Tento diagram je zřejmě komutativní, a proto je indukované zobrazení

$$id_{M \otimes_R N} \otimes \varphi \colon (M \otimes_R N) \otimes_S K \longrightarrow (M \otimes_R N) \otimes_S L$$

injektivní. ◇

Příklad 5.9. Dokažte, že R-modul A je plochý právě tehdy, když pro každý konečně generovaný ideál I okruhu R je zobrazení $A \otimes_R I \to A \otimes_R R$ indukované inkluzí $I \subseteq R$ injektivní.

Řešení. Pokud je A plochý, tak přímo z definice plyne, že $A \otimes_R I \to A \otimes_R R$ je injekce.

Naopak, předpokládejme, že pro každý konečně generovaný ideál I okruhu R je indukované zobrazení $id_A \otimes \iota \colon A \otimes_R I \to A \otimes_R R$ injektivní. Nechť $\varphi \colon A \otimes_R I \to A \cdot I$ je homomorfismus grup daný předpisem $m \otimes i \mapsto mi$. Snadno se ověří, že diagram

$$\begin{array}{ccc} A \otimes_R I & \xrightarrow{id_A \otimes \iota} & A \otimes_R R \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \cong} \\ A \cdot I & \xrightarrow[\subseteq]{} & A \end{array}$$

komutuje. Homomorfismus φ je zřejmě surjektivní. Budeme hotovi, pokud ukážeme, že je také injektivní. Ale to plyne z komutativity diagramu. To znamená, že φ je izomorfismus, a podle Věty 5.6 je pak A plochý. ◇

Příklad 5.10. Dokažte, že nad oborem integrity R je každý plochý R-modul A bez torze.

Řešení. Ukážeme, že $TA = \{0\}$. Buď $a \in TA$ libovolný prvek. To znamená, že existuje nenulové $r \in R$ takové, že $ar = 0$. Zobrazení $\psi_r \colon R \to R$ dané předpisem $\psi_r(s) = sr$ je zřejmě injektivní homomorfismus R-modulů (zde jsme využili toho, že R je obor integrity a $r \neq 0$). Protože je A plochý, tak příslušné indukované zobrazení $id_A \otimes \psi_r \colon A \otimes_R R \to A \otimes_R R$ je také injektivní. Prvek $a \otimes 1$ leží v jádře $id_A \otimes \psi_r$, neboť platí

$$id_A \otimes \psi_r(a \otimes 1) = a \otimes \psi_r(1) = a \otimes r = ar \otimes 1 = 0 \otimes 1 = 0.$$

Z injektivity $id_A \otimes \psi_r$ plyne, že $a \otimes 1 = 0$. Uvažme nyní zobrazení $\varphi \colon A \otimes_R R \to A$ dané předpisem $\varphi(a \otimes r) = ar$. (Jedná se o izomorfismus R-modulů.) Platí

$$a = \varphi(a \otimes 1) = \varphi(0 \otimes 1) = 0.$$

Tím jsme ukázali, že A je bez torze. ◇

Opačná implikace obecně neplatí, což ukazuje následující příklad.

Příklad 5.11. Nechť $\Bbbk$ je obor integrity. Ukažte, že $\Bbbk[x,y]$-modul $(x,y) \subseteq \Bbbk[x,y]$ je bez torze, ale není plochý.

Řešení. Označme $R = \Bbbk[x,y]$, $I = (x,y)$. Podle Věty 5.6 stačí ukázat, že homomorfismus grup $I \otimes_R I \to I^2$ není injektivní. Ukážeme, že $x \otimes y \neq y \otimes x$. Uvažme zobrazení $\varphi \colon I \times I \to R$ dané předpisem

$$\varphi(f,g) = f(x,0) \cdot g \qquad \forall f, g \in I.$$

Snadno se ověří, že toto zobrazení je R-bilineární. Existuje tedy homomorfismus $\psi \colon I \otimes_R I \to R$ takový, že $\psi(f \otimes g) = \varphi(f,g)$. Zřejmě $\varphi(x,y) \neq \varphi(y,x)$, a proto $x \otimes y \neq y \otimes x$. ◇

Příklad 5.12. Buď R okruh hlavních ideálů. Dokažte, že R-modul A je plochý právě tehdy, když je bez torze.

Řešení. Nechť A je plochý. Pak podle příkladu 5.10 je A bez torze.

Naopak, předpokládejme, že A je bez torze. Ukážeme, že pak A je plochý. Buď I libovolný nenulový ideál okruhu R. Podle předpokladu je I tvaru rR pro vhodné nenulové $r \in R$. Zobrazení $\psi_r \colon R \to I$ dané předpisem $\psi_r(s) = sr$ je izomorfismus R-modulů. Složení

$$R \xrightarrow{\psi_r} I \xrightarrow{\iota} R$$

zobrazení ψ_r s inkluzí $\iota \colon I \subseteq R$ odpovídá násobení prvkem r. Uvažme homomorfismus R-modulů $\varphi \colon A \to A$, jež je dán předpisem $\varphi(a) = ar$. Tento homomorfismus je injektivní, neboť A je bez torze. Není těžké ověřit, že diagram

$$\begin{array}{ccccc} A \otimes_R R & \xrightarrow{id_A \otimes \psi_r} & A \otimes_R I & \xrightarrow{id_A \otimes \iota} & A \otimes_R R \\ \cong \uparrow & & & & \uparrow \cong \\ A & & \xrightarrow{\qquad\qquad\varphi\qquad\qquad} & & A \end{array}$$

komutuje. Ukážeme, že $id_A \otimes \psi_r$ je izomorfismus R-modulů.

Zřejmě se jedná o surjektivní homomorfismus, neboť vzorem prvku $b \otimes s$ je prvek $b \otimes \psi_r^{-1}(s)$. Pokud by $id_A \otimes \psi_r$ nebylo injektivní, pak by nebylo injektivní ani složení $(id_A \otimes \iota) \circ (id_A \otimes \psi_r)$, což podle předchozího není možné.

Z toho, že je $id_A \otimes \psi_r$ izomorfismus, plyne, že $id_A \otimes \iota$ je injektivní. Podle příkladu 5.9 je tedy A plochý. ◇

6. Direktní kolimity, Lazardova věta, Regulární okruhy

Základním pojmem této části budou direktní kolimity, což jsou jisté moduly s univerzální vlastností, které použijeme ke klasifikaci všech plochých modulů (*Lazardova věta*).

Nejprve si uveďme několik motivačních příkladů:

1. Racionální čísla $\mathbb{Q}$ jako $\mathbb{Z}-$modul. Jistě je tato abelovská grupa generovaná zlomky typu $\frac{1}{p}$, kde p je libovolné prvočíslo, pokud tedy chceme zadat libovolný homomorfismus z $\mathbb{Q}$, stačí k tomu popsat obrazy všech zlomků $\frac{1}{p}$ (máme-li na paměti rovnost $p\cdot\frac{1}{p} = q\cdot\frac{1}{q}$ pro libovolná dvě prvočísla p, q, kterou musíme respektovat). Avšak můžeme se na $\mathbb{Q}$ rovněž dívat tak, že je generované všemi možnými zlomky tvaru $\frac{1}{m}$, kde $m \in \mathbb{N}$. Zadat homomorfismus z $\mathbb{Q}$ je potom to stejné jako zadat obrazy $\frac{1}{m}$ pro každé m. Ty však rovněž nemůžeme volit libovolně, neboť jsme svázani podmínkami $m \cdot \frac{1}{mn} = \frac{1}{n}$. Jinými slovy, máme inkluzi podgrup $\iota\colon \frac{1}{m}\cdot\mathbb{Z} \hookrightarrow \frac{1}{mn}\cdot\mathbb{Z}$ a libovolný homomorfismus z $\mathbb{Q}$ zúžen na tyto podgrupy zřejmě musí respektovat ι.
2. Konečná tělesa charakteristiky p. Buď p libovolné prvočíslo a buďte $\mathbb{F}_{p^n}, n \in \mathbb{N}$ všechna konečná tělesa charakteristiky p. Víme, že konečné těleso je určeno jednoznačně počtem svých prvků q (až na izomorfismus), q je vždy mocnina p a navíc víme, že každé konečné těleso o p^n prvcích je rozkladovým tělesem polynomu $x^{p^n} - x$. Dále víme, že $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, právě když $n|m$. Algebraickým uzávěrem $\mathbb{F}_p$ je sjednocení všech konečných těles charakteristiky p, tedy $\overline{\mathbb{F}}_p = \cup\mathbb{F}_{p^n}$ přes všechna $n \in \mathbb{N}$. Chceme-li popsat zobrazení z algebraického úzávěru $\overline{\mathbb{F}}_p$, opět nám stačí popsat zobrazení z $\mathbb{F}_{p^n}$ pro každé $n \in \mathbb{N}$, přitom však musíme opět respektovat uvedené inkluze mezi jednotlivými tělesy.

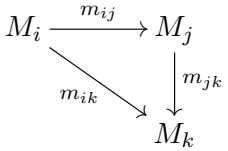
Definice 6.1 (Usměrněná množina)**.** Řekneme, že uspořádaná množina I je shora usměrněná, pokud každé dva prvky $i, j \in I$ mají horní závoru.

Usměrněné množině se někdy říká direktní množina či direktní uspořádaná množina.

Příklad 6.2. Důležitými příklady direktních usměrněných množin jsou tyto množiny:

1. $(\mathbb{N}, \leq)$,
2. $(\mathbb{N}, |)$, tedy přirozená čísla spolu s dělitelností (stačí vzít nejmenší společný násobek),

Definice 6.3 (Direktní systém modulů)**.** Buď dán okruh R a buď dána direktní uspořádaná množina $(I, \leq)$. Buď dále pro každé $i \in I$ zadán R-modul M_i a pro každé $i, j, \in I$, $i \leq j$ dán homomorfismus modulů $m_{ij} : M_i \to M_j$, přičemž $m_{ii} = \mathrm{id}_{M_i}$. Řekneme, že systém $\{M_i\}_{i\in I}$ tvoří direktní systém modulů, pokud pro každé $i, j, k \in I$, $i \leq j \leq k$ platí $m_{jk} \circ m_{ij} = m_{ik}$, tedy že následující diagram komutuje:



Příklad 6.4 (Kolimita direktního systému)**.** Buď tedy R libovolný okruh a mějme dán direktní systém $R-$modulů $\{M_i\}_{i\in I}$. Sestrojme nyní $R-$modul M (*kolimitu*), který bude (obrazně řečeno) obsahovat všechna data popsaná naším systémem:

Označme A disjunktní sjednocení M_i (vezměme například $A = \cup M_i \times \{i\}$) a uvažme na A následující relaci $\sim$: $(a, i) \sim (b, j)$, právě když existuje $k \in I, k \geq i, j$ takové, že $m_{ik}(a) =$

$m_{jk}(b)$. Snadno se ověří, že tato relace je vskutku relací ekvivalence (symetrie je bezprostřední, reflexivita plyne z požadavku $m_{ii} = id_{M_i}$ a k tranzitivě stačí využít usměrněnosti našeho direktního systému). Modul $A/\sim$ je potom naše hledaná kolimita.

Na $A/\sim$ zavedeme strukturu $R-$modulu pomocí reprzentantů. Stále máme na paměti, že prvek (x, i) žije v $i-$tém modulu M_i. Libovolný prvek $A/\sim$ je tvaru $[(a, i)]$ pro nějaké $a \in M_i$. Definujme násobení skaláry $r \cdot [(a, i)] = [(r \cdot a, i)]$ a součet $[(a, i)], [(b, j)] \in A/\sim$ jako $[(a, i)], [(b, j)] = [(m_{ik}(a) + m_{jk}(b), k)]$ pro dostatečně velké $k \geq i, j$. Opět se snadno ověří, že s takto definovanými operacemi je $A/\sim$ $R-$modul.

Snadno se nyní uvidí několik velmi důležitých vlastností:

(i) Každý prvek kolimity pochází z některého z modulů M_i,

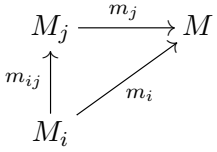
(ii) Každý prvek $(a, i) \in M_i$ zadává v kolimitě stejný prvek jako $(m_{ij}(a), j)$ pro libovolné $j \geq i$,

(iii) Platí-li v kolimitě $[(a, i)] = [(b, j)]$, pak existuje $k \in I$ tak, že $m_{ik}(a) = m_{jk}(b)$, tedy pokud dva prvky určují stejnou třídu v kolimitě, musely „být stejné“ už někde v našem systému, speciálně tedy:

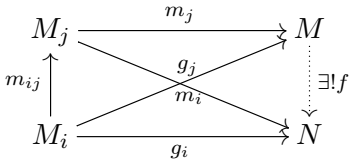
(iv) Platí-li v kolimitě $[(a, i)] = 0$, existuje pro $[(a, i)]$ nulový reprezentant a každý reprezentant (b, j) leží v jádře některého z homomorfismů m_{jk}, nemusí ovšem ležet v jádrech všech homomorfismů $m_{\alpha\beta}$).

Za malou chvíli ukážeme, že námi sestrojená kolimita M odpovídá *kategoriální* definici direktní kolimity, a tedy že splňuje podmínky z následující definice:

Definice 6.5 (Direktní kolimita)**.** Buď dán okruh R, direktní uspořádaná množina $(I, \leq)$ a $\{M_i\}_{i \in I}$ direktní systém modulů. Buď dále M R-modul a nechť jsou dány homomorfismy $m_i : M_i \to M$ tak, že pro $i, j, \in I$, $i \leq j$ platí $m_j \circ m_{ij} = m_i$, tedy že následující diagram komutuje:



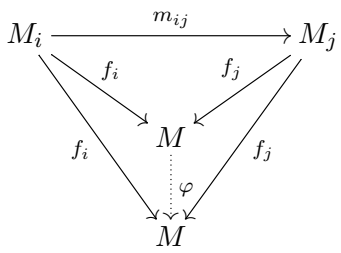
Řekneme, že M je *direktní kolimita* systému $\{M_i\}_{i \in I}$, pokud pro každý $R-$modul N s homomorfismy $g_i : M_i \to N$ tak, že pro $i, j, \in I$, $i \leq j$ platí $g_j \circ m_{ij} = g_i$ existuje jediný homomorfismus $f : M \to N$ tak, že $f \circ m_i = g_i$, tedy



Direktní kolimity zpravidla značíme $M = \operatorname{colim} M_i$. V modulech direktní kolimity existují a díky své univerzální vlastnosti jsou jistě určené jednoznačně až na izomorfismus.

Vskutku, máme-li M, N dvě direktní kolimity systému $\{M_i\}$, pak jistě existuje jediné $f : M \to N$ tak, že $f \circ f_i = g_i$ a existuje jediné $g : N \to M$ tak, že $g \circ g_i = f_i$ pro každé i.

Z definice M jako direktní kolimity máme následující diagram:



kde zobrazení φ je dáno jednoznačně. Avšak jistě identita $\mathrm{id} : M \to M$ splní podmínku z definice direktní kolimity. Pokud ukážeme, že rovněž $g \circ f$ tuto podmínku splní, dostaneme $gf = \mathrm{id}$ (a symetricky $fg = \mathrm{id}$ a tedy f je hledaný isomorfismus mezi M a N. Avšak $g \circ f : M \to M$ a platí $(g \circ f) \circ f_i = g \circ (f \circ f_i) = g \circ g_i = f_i$.

Všimněme si, že nestačí říct, že z unikátnosti zobrazení f v definici direktní kolimity automaticky plyne, že gf je identita na M, ale musíme ověřit, že zobrazení gf opravdu vyhovuje podmínkám kladeným na zobrazení z kolimity.

Ukažme nyní, že námi sestrojená kolimita M systému z příkladu 6.4 je opravdu direktní kolimitou ve smyslu definice 6.5. Jistě máme homomorfismy $f_i : M_i \to M$ dané následovně: $a_i \in M_i \mapsto [a_i]$. Jistě potom $f_j \circ m_{ij} = f_i$ pro každé $i \leq j \in I$, neboť obrazy prvků v m_{ij} zadávají stejné prvky v kolimitě.

Ověřme nyní univerzální vlastnost M. Mějme $R-$modul N a homomorfismy $g_i : M_i \to N$ tak, že $i, j, \in I$, $i \leq j$ platí $g_j \circ m_{ij} = g_i$ a hledejme homomorfismus $f : M \to N$ tak, že $f \circ f_i = g_i$.

Jedinou volbou může být $f([(a,i)]) = g_i(a)$. Ukažme, že je takto definované zobrazení f dobře definované (ověřit, že potom půjde o homomorfismus lze podobně jako při ověřování, že M je vskutku $R-$modul). Buď tedy $[(a,i)] = [(b,j)]$. Ukažme, že $g_i(a) = f([(a,i)]) = f([(b,j)]) = g_j(b)$. Avšak protože $\exists k \in I$ tak, že $m_{ik}(a_i) = m_{jk}(b_j)$ a protože platí $g_k \circ m_{ik} = g_i$, $g_k \circ m_{jk} = g_j$, dostáváme $g_i(a_i) = g_k \circ m_{ik}(a_i) = g_k \circ m_{jk}(b_j) = g_j(b_j)$ a tedy naše zobrazení je definováno korektně.

Odtud již dostáváme $M = \operatorname{colim} M_i$.

Cvičení 6.6. Spočtěte direktní kolimitu vzhledem k množině s největším prvek.

Řešení. Ukažme, že je to největší prvek této množiny. Vskutku, označme t největší prvek I a ukažme, že $\operatorname{colim} M_i \cong M_t$. Podle příkladu 6.4 stačí zkoumat, které prvky jednotlivých modulů se slepí pomocí relace $\sim$. Jistě však pro každé $i \in I$ existuje zobrazení m_{it} a tedy všechny prvky $a \in M_i$ budou ekvivalentní $m_{it}(a) \in M_t$. Protože však z M_t již nevede žádný homomorfismus (vyjma identity), budou v kolimitě třídy určené prvky M_t různé. Zobrazení m_t bude tedy isomorfismus $M_t \simeq \operatorname{colim} M_i$. ◇

Cvičení 6.7. Spočtěte direktní kolimitu vzhledem ke konečné množině.

Řešení. Konečná usměrněná množina jistě obsahuje největší prvek, použitím předchozího příkladu bude kolimitou opět modul odpovídající největšímu prvku dané usměrněné množiny. ◇

Příklad 6.8. Napište $\mathbb{Z}[\frac{1}{p}]$ jako direktní kolimitu modulů izomorfních se $\mathbb{Z}$.

Řešení. Buď $I = \mathbb{N}_0$ uspořádané jako řetězec a uvažme následující direktní systém modulů s homomorfismy danými inkluzemi:

$$\mathbb{Z} \xrightarrow{\subseteq} \mathbb{Z} \cdot \tfrac{1}{p} \xrightarrow{\subseteq} \mathbb{Z} \cdot \tfrac{1}{p^2} \longrightarrow \cdots \longrightarrow \mathbb{Z} \cdot \tfrac{1}{p^k} \xrightarrow{\subseteq} \mathbb{Z} \cdot \tfrac{1}{p^{k+1}} \longrightarrow \cdots$$

Jistě $\mathbb{Z} \cdot \frac{1}{p^k} \cong \mathbb{Z}$ jako $\mathbb{Z}$-moduly a tento izomorfismus je popsán $\frac{1}{p^k} \mapsto 1$, tedy násobením p^k. Pomocí těchto izomorfismů tedy můžeme přepsat naši posloupnost na

$$\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \xrightarrow{\cdot p} \cdots \xrightarrow{\cdot p} \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \xrightarrow{\cdot p} \cdots$$

kde jistě zobrazení m_{ij} je dáno násobením p^{j-i}.

Označme nyní $M = \operatorname{colim} \mathbb{Z}$ kolimitu tohoto systému a ukažme, že je rovna $\mathbb{Z}[\frac{1}{p}]$. Jistě máme pro $i \leq j$ zobrazení

$$\begin{array}{ccc} (\mathbb{Z} \cdot \frac{1}{p^i} \cong)\, \mathbb{Z} = M_i & \xrightarrow{\cdot p^{j-i}} & M_j = \mathbb{Z}\, (\cong \mathbb{Z} \cdot \frac{1}{p^j}) \\ & \searrow^{g_i = \cdot p^{-i}} & \downarrow{\scriptstyle g_j = \cdot p^{-j}} \\ & & \mathbb{Z}[\frac{1}{p}] \end{array}$$

Tyto zobrazení jistě komutují. Ukažme tedy, že $M \cong \mathbb{Z}[\frac{1}{p}]$. Z definice kolimity víme, že existuje jediné zobrazení $f : M \to \mathbb{Z}[\frac{1}{p}]$, které s právě sestrojenými zobrazeními komutuje. Ukažme, že je to bijekce.

Předpokládejme, že $f(a) = 0$ pro nějaké $a \in M$. Nechť $[a_i] = a$, kde $a_i \in M_i$ je libovolný reprezentant. Protože $f \circ f_i = g_i$, dostáváme $\frac{1}{p^i} \cdot a_i = 0$ a tedy $a_i = 0$ a nutně $a = 0$. f je tedy injektivní.

Naopak ukažme, že každý zlomek $\frac{1}{p^k}$ má vzor (pro $k \in \mathbb{N}$). Tyto jistě generují $\mathbb{Z}[\frac{1}{p}]$ jako $\mathbb{Z}-$modul. Vskutku, označme $a = f_k(1_k)$, kde 1_k generuje M_k. Pak jistě $g_k(1_k) = \frac{1}{p^k}$, což vzhledem k rovnosti $f \circ f_k = g_k$, dává, že $f_k(1_k)$ je vzor $\frac{1}{p^k}$ v zobrazení f a f je tudíž na. ◇

Příklad 6.9. Napište $\mathbb{Q}$ jako direktní kolimitu modulů izomorfních se $\mathbb{Z}$.

Řešení. Podobně jako v předchozím příkladu buď $I = (\mathbb{N}, |)$ a uvažme následující direktní systém modulů $\{M_m\}$, kde $M_m = \mathbb{Z}$ (protože $\mathbb{Z} \cong \mathbb{Z} \cdot \frac{1}{m}$) a homomorfismy definujme $\mu_{m,mn} : M_m = \mathbb{Z} \to \mathbb{Z} = M_{mn}$, $a \mapsto n \cdot a$. Opět máme homomorfismy

$$\begin{array}{ccc} \mathbb{Z} = M_m & \xrightarrow{\cdot n} & M_{mn} = \mathbb{Z} \\ & \searrow^{g_m = \cdot \frac{1}{m}} & \downarrow{\scriptstyle g_{mn} = \cdot \frac{1}{mn}} \\ & & \mathbb{Q} \end{array}$$

Označme nyní $M = \operatorname{colim} \mathbb{Z}$ kolimitu tohoto systému a ukažme, že je rovna $\mathbb{Q}$. Námi sestrojená zobrazení g_i jistě komutují se zobrazeními direktního systému. Z definice kolimity tedy víme, že existuje jediné zobrazení $f : M \to \mathbb{Q}$, které s právě sestrojenými zobrazeními komutuje. Ukažme, že je to bijekce.

Předpokládejme, že $f(a) = 0$ pro nějaké $a \in M$. Nechť $[(a, m)] = a$, kde $a \in M_m$ je libovolný reprezentant. Protože $f \circ f_m = g_m$ a g_m jsou všechno injekce, je nutně f injektivní.

Naopak ukažme, že každý zlomek $\frac{1}{m}$ má vzor. Tyto jistě generují $\mathbb{Q}$ jako $\mathbb{Z}-$modul. Vskutku, označme $a = f_m(1)$, kde 1_m generuje M_m. Pak jistě $g_m(1) = \frac{1}{m}$, což vzhledem k rovnosti $f \circ f_m = g_m$, dává, že $f_m(1)$ je vzor $\frac{1}{m}$ v zobrazení f a f je tudíž na. ◇

Nyní si ukážeme některé vlastnosti direktních kolimit.

Tvrzení 6.10 (Vlastnosti direktních kolimit)**.**

(i) Každý modul je direktní kolimitou svých konečně generovaných podmodulů,

(ii) Direktní kolimitu M lze rovněž sestrojit jako kvocient přímého součtu modulů M_i,

(iii) $\oplus_I M_i = \operatorname{colim}_{J\subset I} \oplus_{j\in J} M_j$,

(iv) Direktní kolimita komutuje s tenzorovým součinem, tedy $A \otimes \operatorname{colim} M_i = \operatorname{colim} A \otimes M_i$,

(v) Direktní kolimita plochých modulů je plochý modul.

(vi) Každý modul je direktní kolimitou konečně prezentovatelných modulů.

Důležitým tvrzením je následující klasifikace plochých modulů:

Věta 6.11 (Lazard, 1969)**.** *$R-$Modul M je plochý, právě když je direktní kolimitou projektivních modulů.*

Z příkladů (v) ihned dostáváme následující aplikaci Lazardovy věty:

Důsledek 6.12 (Ploché moduly)**.** *Následující moduly jsou ploché:*

(i) $\mathbb{Z}$-modul $\mathbb{Q}$,

(ii) $\mathbb{Z}$-modul $\mathbb{Z}[\frac{1}{p}]$ pro libovolné prvočíslo p.

Tvrzení 6.10 nám dává následující tvrzení pro abelovské grupy:

Cvičení 6.13 (Torze)**.** Buď A abelovská grupa. Dokažte následující tvrzení o $\mathbb{Z}[\frac{1}{p}] = \{\frac{a}{p^k} | a \in \mathbb{Z}, k \in \mathbb{N}\}$ a $\mathbb{Z}_{(p)} = \{\frac{a}{b} | a, b \in \mathbb{Z}, p \nmid b\}$:

1. $A \otimes \mathbb{Z}[\frac{1}{p}] = 0$, právě když A je $p-$torzní,
2. $A \otimes \mathbb{Z}_{(p)} = 0$, právě když A je $p'-$torzní.

Řešení. Rozepišme $A \otimes \mathbb{Z}[\frac{1}{p}] = A \otimes \operatorname{colim} \mathbb{Z} = \operatorname{colim} A \otimes \mathbb{Z} = \operatorname{colim} N_i$. Jaká jsou ovšem zobrazení mezi N_i a N_j? Jedná se o naše násobení p^{j-i}. Nyní již stačí použít kritérium pro nulovost prvků v direktní kolimitě: prvek $[a \otimes x]$ bude v kolimitě nulový, pokud jeho obraz v některém zobrazení bude nulový. Avšak to znamená, že $0 = p^k \cdot a \otimes x = (p^k \cdot a) \otimes x$ a tedy $p^k \cdot a = 0 \in A$ a a je $p-$torzní.

Všechny $p-$torzní prvky grupy A tedy při tenzorování s $\mathbb{Z}[\frac{1}{p}]$ zmizí a odtud plyne zbytek tvrzení 1.

V části 2 se využije stejného rozepsání, neboť $\mathbb{Z}_{(p)}$ lze napsat jako direktní kolimitu téměř stejným způsobem jako $\mathbb{Q}$ a postup je poté analogický předchozí části. ◇

Stejným způsobem se dá vyřešit následující cvičení:

Cvičení 6.14. Spočítejte $\mathbb{Z}[\frac{1}{p}] \otimes \mathbb{Z}_{(p)} = \mathbb{Q}$.

Definice 6.15. Řekneme, že okruh R je *von Neumann regulární*, pokud pro každé $x \in R$ existuje $a \in R$ tak, že $xax = x$.

Příklad 6.16. 1. Každý *Booleovský okruh* je regulární.

2. Každý okruh s dělením je regulární, tedy všechna tělesa jsou regulární.

3. $k^{n\times n}$ okruh matic $n \times n$ nad tělesem k je regulární okruh.

Řešení. 1. Vskutku, máme tam jednotku a každý prvek je idempotent.

2. Vskutku, existují inverze.

3. Vskutku, za prvek a stačí zvolit pseudoinverzi prvku $x \in k^{n\times n}$ (pro prostory se skalárním součinem lze volit např. Mooreovu−Penroseovu pseudoinverzi, pro obecné prostory se dá pseudoinverze sestrojit přímo analogickým způsobem ke konstrukci pomocí adjungovaného zobrazení). ◇

Cvičení 6.17. Nechť R je komutativní regulární okruh. Ukažte, že pro každé $x \in R$ existuje jediné $y \in R$ tak, že $xyx = x$ a $yxy = y$.

Řešení. Z definice regulárního okruhu víme, že existuje $a \in R$ tak, že $xax = x$. Položme $y = axa$. Potom zřejmě

$$xyx = x(axa)x = (xax)ax = xax = x,$$

$$yxy = (axa)x(axa) = a(xax)axa = axaxa = a(xax)a = axa = y$$

Předpokládejme nyní, že pro $z \in R$ platí $xzx = x$, $zxz = z$. Potom platí

$$z = zxz = z(xyx)z = zx(yxy)xz = y^2zx^3z = y^2x(zxz)x = y^2xzx = y^2x = yxy = y$$

A tedy y je dáno jednoznačně. ◇

Pro komutativní von Neumann regulární okruhy tedy máme kanonický způsob, jak volit *slabou inverzi* x.

Důležitá je zejména následující věta:

Věta 6.18. *Okruh R je regulární, právě když libovolný R-modul je plochý.*

Jednoduchým důsledkem této věty je následující tvrzení:

Důsledek 6.19. *Každý vektorový prostor nad tělesem je plochý.*

7. Krátké exaktní posloupnosti

Exaktní posloupnosti jsou velmi obecným aparátem. Jako takové je možné zavést tento objekt i pro jiné objekty než jsou moduly, např.: obecné nekomutativní grupy, lieovy algebry. V našem kontextu bude exaktní posloupnost chápána výhradně jako exatkní posloupnost modulů (pokud nebude řečeno jinak). Vzhledem k tomu, že několik případů bude zaměřeno na grupy, je dobré si hned ze začátku uvědomit, že libovolná komutativní grupa má zrejmou strukturu $\mathbb{Z}$-modulu.

Definice 7.1 (Exaktní posloupnost)**.** Exaktní posloupnost $\mathcal{E}$ je dána posloupností Modulu $\{\mathrm{M}_i \,|i \in \mathbb{Z}\}$ a posloupností homomorfismů modulů $\{f_i \,|i \in \mathbb{Z}\}$, tak že

$$\mathcal{E}: \ \ldots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots \ ,$$

kde pro každé dva po sobě jdoucí homomorfismy f_i, f_{i+1} platí

$$\operatorname{Im} f_i = \operatorname{Ker} f_{i+1} \, .$$

Poznámka.

- Zejména platí, že každé složení dvou po sobě jdoucích zobrazení je nulové zobrazení, tzn.:
$$f_{i+1} \circ f_i = 0$$
opak ovšem neplatí, výše uvedená podmínka znamená jen $\operatorname{Im} f_i \subseteq \operatorname{Ker} f_{i+1}$.
- V definici není explicitně řečeno, zda-li jsou dané moduly nenulové. Tedy zejména na první pohled velá exaktní posloupnost muže ve skutečnosti sestávat pouze z dvou nenulových modulů
$$0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0 \ .$$
Kde všechny předchozí i následující moduly i zobrazení jsou nulové. V tomto případě je netřeba explicitně vypisovat.

Mezi exaktními posloupnostmi hraje velmi významnou roli speciální typ, takzvaná *Krátká exaktní posloupnost.*

Definice 7.2 (Krátká exaktní posloupnost)**.** Je speciálním typem exaktní posloupnosti sestávající se z 3 modulů

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \ .$$

Tento, zdánlivě triviální objekt má velké množství využití jak, koneckonců uvidíme v příkladech.

Poznámka. Abychom získaly intuici pro nadefinovaný pojem uvedeme si čtyři typické situace, které nám pomohou daný pojem lépe pochopit.

- V jistém smyslu triviální případ krátké exaktní posloupnosti je následující posloupnost
$$M \longrightarrow M \oplus N \longrightarrow N$$
Tento typ nazýváme štěpící se posloupnost. Obecně charakterizujeme stěpící se posloupnost v níže uvedeném lematu.

- V kontextu rozšíření modulů se hodí následující interpretace

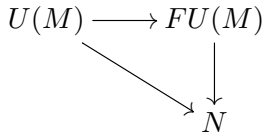
$$M \longrightarrow N \longrightarrow N/M \ ,$$

správná interpretace prostředního modulu je jako rozšíření modulu M na modul N.

- V kontextu zobrazení jsou důležité dvě duální krátké exaktní posloupnosti

$$\operatorname{Ker} f \longrightarrow M \longrightarrow \operatorname{Im} f$$
$$\operatorname{coim} f \longrightarrow M \longrightarrow \operatorname{coker} f$$

- Poslední podstatný příklad je takzvaná prezentace modulu M. Označme $U(M)$ nosnou množinu modulu M a $F(S)$ volný modul na množině generátorů S. Z univerzální vlastnosti



máme zobrazení

$$FU(M) \xrightarrow{p} M$$

nýní s využitím vety o isomorfismu, můžeme napsat $FU(M)/\operatorname{Ker}(p) \simeq M$ a tedy máme krátkou exaktní posloupnost

$$\operatorname{Ker}(p) \longrightarrow FU(M) \xrightarrow{p} M \ .$$

Modul $FU(M)$ chápeme jako modul generátorů a $\operatorname{Ker}(p)$ jakožto modul relací na generátorech. Je zajímavé zamyslet se nad iterací tohoto postupu. Pro $\operatorname{Ker}(p)$ jsme schopni udělat stejný trik. Tedy po libovolném počtu kroků dostaneme posloupnost

$$FU(\operatorname{Ker}(p_2)) \longrightarrow FU(\operatorname{Ker}(p_1)) \longrightarrow FU(\operatorname{Ker}(p)) \longrightarrow FU(M) \xrightarrow{p} M \ .$$

Tato posloupnost (takzvaná volná resolventa) je jedním z objektů zkoumaných homologicou teorii, zde se jím ale bohužel nemáme místo zabývat.

Lemma 7.3. *Posloupnost*

$$A \xrightarrow{f} B \xrightarrow{g} C \ ,$$

se štěpí v jednom z následujících případu, (tzn. pakliže je spněno jedno z ekvivalentních tvrzení)

(i) Existuje zobrazení $\sigma : C \to B$ takové, že $g \circ \sigma$ je identita.

(ii) Existuje zobrazení $\tau : B \to A$ takové, že $\tau \circ f$ je identita.

(iii) Modul B je isomorfní direknímu součtu modulů A, C.

Poznámka. Část tohoto lemma si dokážeme ve cvičeních.

Příklad 7.4. Dvě neekvivalentní posloupnosti, problém rozšíření. Ukážeme si, že dvě posloupnosti

$$A \xrightarrow{f} B_1 \xrightarrow{g} C \qquad A \xrightarrow{f} B_2 \xrightarrow{g} C \ .$$

Nemusejí být nutně isomorfní.

Řešení. Zkonstrujeme velmi jednoduchý ale zároveň obecný příklad. Uvažujme $\mathbb{Z}$-modul $\mathbb{Z}/n\mathbb{Z}$. Pro názornost vezměme $n = 2$. Nyní uvažujme posloupnost

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow A \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \ ,$$

otázka zní, jak lze zvolit A aby byla posloupnost exakntí. Zřejmě se naskýta možnost

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \ .$$

Zároveň máme i druhou možnosti (dokonce i poslední což nebudeme ukazovat) a to

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \ .$$

Tyto dvě volby prostředního modulu jsou jistě neisomorfní protože zejména jakožto abelovské grupy mají prvky různých řádů. ◇

Příklad 7.5 („Lepení posloupností“)**.** V tomto příkladu ilustrujeme, že krátké exaktní posloupnosti jsou v jistém smyslu základní stavební bloky všech exaktních posloupností. Přesněji to znamená, že z každé dlouhé exaktní posloupnosti jsme schopni vytvořit několik krátkých exaktních posloupností, a naopakt jsme schopni lepit krátké posloupnosti do dlouhých.

Řešení. Začneme s jednodušším směrem, uvažujme posloupnost

$$\ldots \longrightarrow A_{i-2} \xrightarrow{d_{i-2}} A_{i-1} \xrightarrow{d_{i-1}} A_i \xrightarrow{d_i} A_{i+1} \xrightarrow{d_{i+1}} A_{i+2} \longrightarrow \ldots$$

nyní, rozsekáme posloupnost následujícím způsobem, zafixujme si člen A_i a vezměme posloupnost

$$0 \longrightarrow \operatorname{Ker} d_{i-1} \xrightarrow{d_{i-1}} A_i \xrightarrow{d_i} \operatorname{Im} d_i \longrightarrow 0 \ ,$$

ta je zřejmě exaktní. Podobným způsobem dostaneme všechny posloupnosti

$$\vdots \qquad .$$

$$0 \longrightarrow \operatorname{Ker} d_{i-2} \xrightarrow{d_{i-2}} A_i \xrightarrow{d_{i-1}} \operatorname{Im} d_{i-1} \longrightarrow 0$$

$$0 \longrightarrow \operatorname{Ker} d_{i-1} \xrightarrow{d_{i-1}} A_i \xrightarrow{d_i} \operatorname{Im} d_i \longrightarrow 0$$

$$\vdots$$

Nyní se podíváme na opačný směr, mějme krátké exaktní posloupnosti

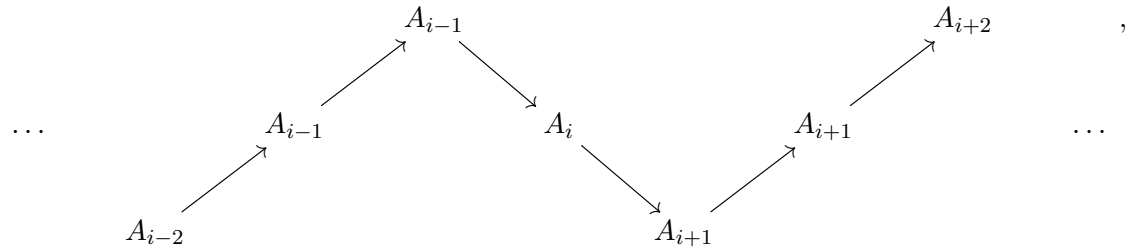
$$\vdots \qquad .$$

$$0 \longrightarrow A_{i-1} \longrightarrow A_i \longrightarrow A_{i+1} \longrightarrow 0$$

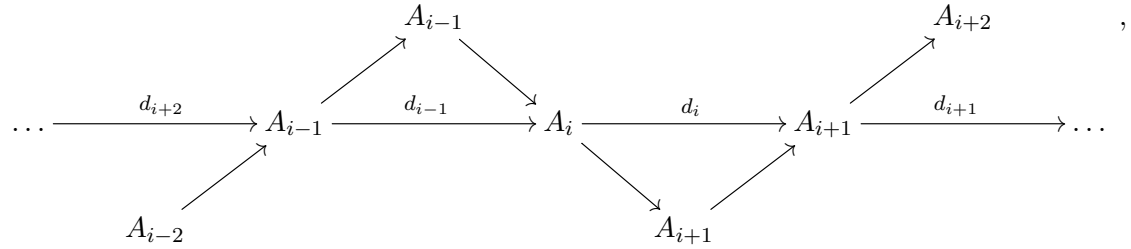
$$0 \longrightarrow A_{i+1} \longrightarrow A_{i+2} \longrightarrow A_{i+3} \longrightarrow 0$$

$$\vdots$$

nyní vytvoříme posloupnost (zatím neexaktní)



kde na diagonálách máme položeny naše původní posloupnosti.Nyní je potřeba zadefinovat zobrazení d_i tak, že



horizontální posloupnost je exaktní. ◇

Příklad 7.6. Je názorné ukázat si ještě jeden obdobný příklad kdy předchozí situace nenastane. Uvažujme podobný problém rozšíření

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow A \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \ .$$

Zde nenastane situace jako v předchozím příklade protože $2, 3$ jsou nesoudělné a $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Tedy pro tyto $\mathbb{Z}$ moduly existuje jedineé netriviální rozšíření. Tuto jedinečnost zatím nebudeme dokazovat a podíváme se na ní v dalším příkladě v obecnější rovině.

Poznámka. Na tomto místě je vhodné uvědomit si důležitou věc. Jak již bylo uvedeno, každá komutativní grupa může být chápána jako $\mathbb{Z}$ modul. Toto ovšem neplatí pro grupy nekomutativní! Má smysl tedy hledat netriviální rozšíření pro předchozí případ ve světě nekomutativních grup, takové opravdu existuje jak nyní ukážeme.

Uvažujme grupu symetrickou grupu na třech prvcích S_3. Počet prvků je shodný ale rozhodně není isomorfní $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$ například právě z důvodu nekomutativity. Nyní uvažujme alternující grupu A_3 ta je podgrupou S_3 a je isomorfní $\mathbb{Z}/3\mathbb{Z}$. Nyní známe vše podstatné abychom napsali rozšíření

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow S_3 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \ .$$

Ještě jednou podotkněme, že posloupnost je zde chápána jako posloupnost nekomutativních grup nikoliv modulů.

Příklad 7.7 (Grupy nesoudělných řádů)**.** V tomto příkladu uvedeme zobečnění předchozího případu. Nechť G, H jsou konečné komutativní grupy nesoudělného řádu, tedy $(|G| \nmid |H|)$. Potom každá exaktní posloupnost

$$0 \longrightarrow G \longrightarrow A \longrightarrow H \longrightarrow 0 \ ,$$

se štěpí, tedy $A \simeq G \oplus H$.

Řešení. Označme si řády grup $g := |G|\, h := |H|$. Vzheldem k nesoudělnosti víme, z bezoutovy nerovnosti, že existují celá čisla, tak že $ag + bh = 1$. ◇

Příklad 7.8 (Determinant)**.** V tomto příkladu si ukážeme jednu méně triviální exaktní posloupnost nekomutativních grup.

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R} \longrightarrow 1$$

Řešení. Stačí uhádnout co jsou dané zobrazení, potom je příklad přímočarý. Z grupy $\mathrm{GL}_n(\mathbb{R})$ mám známý grupový homomorfismus do grupy $\mathbb{R}$ a tedy i homomorfismus $\mathbb{Z}$-modulů. Tímto zobrazením je determinant. Nyní si připomeneme definici grupy

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}$$

Nyní si stačí uvědomit, že lze grupu $\mathrm{SL}_n(\mathbb{R})$ chápat jako jádro determinantu, tzn.

$$\mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{R})$$

Odtur již plnyne náš příklad jakožto speciální případ posloupnosti

$$\mathrm{Ker}\, f \longrightarrow A \xrightarrow{f} B \ .$$ ◇

Příklad 7.9 (Afinní grupa)**.** V podobném duchu k předchozímu příkladu si ukážeme takzvané afinní rozšíření obecné lineární grupy. Tento příklad je možná čtenáři znám jako polopřímí součin dvou grup. Je třeba mít na paměti, že v tomto příkladu se zabýváme nekomutativnímy grupamy (tedy né okruhy) ale pro čtenáře obeznámeného s základní teorii grup by neměl být problém příklad pochopit. Uvažujme následující posloupnost

$$0 \longrightarrow \mathbb{R}^n \longrightarrow \mathrm{Aff}_n(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{R}) \longrightarrow 1$$

Řešení. Pokusíme se vysvětlit konstrukci afinní grupy. Uvědomme si, že grupa $\mathrm{GL}_n(\mathbb{R})$ má standardní reprezentaci na prostoru $\mathbb{R}$. To z prostoru $\mathbb{R}$ dělá levý $\mathrm{GL}_n(\mathbb{R})$-modul. Necháme na čtenáři porovnal axiomy akce (skrze reprezentaci) s axiomy modulu. Navíc můžeme na $\mathrm{GL}_n(\mathbb{R})$ nahlížet jako na okruh a tedy zejména jako na modul nad sebou samým.

Nyní máme vše potřebné abychom stvořili afinní grupu. Množinově položme $\mathrm{Aff}_n(\mathbb{R}) = \mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n$. Nyní definujme operaci pomocí zmíněné reprezentace jako

$$(A, b)(C, d) = (AC, Ad + b)\,.$$

V tomto případě značíme grupu jako $\mathrm{Aff}_n(\mathbb{R}) = \mathrm{GL}_n(\mathbb{R}) \ltimes \mathbb{R}^n$. ◇

Příklad 7.10. V tomto příkladu si charakterizujeme některé známé vlastnosti zobrazeni pomocí exaktní posloupnosti.

1. Zobrazení f je surjektivní právě tehdy když je posloupnost

$$M \xrightarrow{f} N \longrightarrow 0\ ,$$

exaktní.

2. Zobrazení f je injektivní právě tehdy když je posloupnost

$$0 \longrightarrow M \xrightarrow{f} N\ ,$$

exaktní.

Řešení. Tento příklad je přímou aplikací definice, uvedeme proto řešení pouze první části a druhou necháme na čtenáři. Zobrazení vedoucí z N do nulového modulu nemůže být nic jiného než nulové zobrazení. Zejména tedy víme, že jeho jádro je celý modul N. Z exaktnosti plyne, že obraz zobrazení f je roven modulu N.

Opačným směrem, ze surjektivity víme, že obraz je celý modul N dále zřejmé. ◇

Příklad 7.11. Nyní charakterizujeme projektivní injektivní a ploché moduly v řečí exaktních posloupností. Mějme obecnou krátkou exaktní posloupnost

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0\ ,$$

víme, že aplikací $\mathrm{Hom}(\_, X)$, $\mathrm{Hom}(X, \_)$ či $\_ \otimes X$ nemusíme dostat exaktní posloupnosti. Nicméně, platí následujíci charakterizace

(i) Modul P je projektivní právě tehdy když aplikací $\mathrm{Hom}(P, \_)$ obdržíme opět exaktní posloupnost.

(ii) Modul I je injektivní právě tehdy když aplikací $\mathrm{Hom}(\_, I)$ obdržíme opět exaktní posloupnost.

(iii) Modul F je plochý právě tehdy když aplikací $\_ \otimes F$ obdržíme opět exaktní posloupnost.

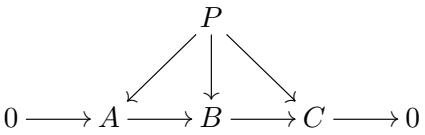
Řešení. Ukážeme pouze první a třetí charakterizaci druhou ponecháme jako lehké cvičení (duální k první). Mějme nejprve libovolnou exaktní posloupnost modulů

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0\ .$$

Aplikací $\mathrm{Hom}(P, \_)$ obdržíme novou posloupnost (né nutně exaktní).

$$0 \longrightarrow \mathrm{Hom}(P, A) \xrightarrow{f_*} \mathrm{Hom}(P, B) \xrightarrow{g_*} \mathrm{Hom}(P, C) \longrightarrow 0 \ .$$

Je dobré si přepsat posloupnosti jako



Je jasné, že zobrazení indukovaná zobrazení f_*, g_* působí jako prekompozice. Z tohoto plyne, že $g_* \circ f_*$. Je tedy potřeba ověřit jen opačný směr inkluzí příslušných jader k obrazům. ◇

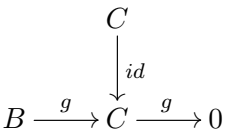
Příklad 7.12. Tento příklad ilustruje propojení projektivních a injektivních modulů. Je dán okruh R dokažme ekvivalencí následujících vět.

1. Každý modul nad daným okruhem R je projektivní.
2. Každý modul nad daným okruhem R je injektivní.

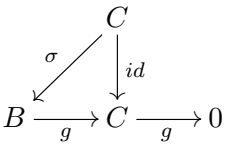
Řešení. Dokážeme nejdříve $(i) \Rightarrow (ii)$, mějme obecnou exaktní posloupnost (projektivních) modulů

$$A \xrightarrow{f} B \xrightarrow{g} C \ ,$$

aplikací definice projektivního modulu C a exaktnosti v posledním členu



dostáváme zvednutí identity



což nám dává štěpení exaktní posloupnosti

$$A \xrightarrow{f} A \oplus C \xrightarrow{g} C \ .$$

Z toho vidíme, že A je injektivní modul. Důkaz opačným směrem je duální akorát dostaneme štěpení v prvním členu. Tedy každá exaktní posloupnost se štěpí a tedy je poslední modul projektivní. ◇

Příklad 7.13. V tomto příkladě si ukážeme zajímavou posloupnost se vztahem k algebraicke geometrii. Nechť je dáno $\mathbb{C}$ a zároveň okruh polynomů nad tímto polem, tzn.:

$$\mathbb{C}[x] = \left\{ f : \mathbb{C} \to \mathbb{C} \,\middle|\, f(x) = \sum_{i=0}^{n} a_i x^i \right\} .$$

Nyní definujme funkci $\mathrm{ev}_0 : \mathbb{C}[x] \to \mathbb{C}$ jako $\mathrm{ev}_0(f) = f(0) = a_0$. Exaktní posloupnost je

$$0 \longrightarrow \mathbb{C}[x] \longrightarrow \mathbb{C}[x] \longrightarrow \mathbb{C} \longrightarrow 0 \ ,$$

druhé zobrazení je zmíněná evaluace a zobrazení mezi $\mathbb{C}[x] \to \mathbb{C}[x]$ je dáno $X : f(x) \mapsto xf(x)$.

Řešení. Nezbývá moc práce, je totiž téměř jasné, že evaluace libovolného polynomu $xf(x)$ je nula. Naopak, každý polynom který má $f(0) = 0$ nemůže mít absolutní člen, a proto lze najít vzor vydělením x. ◇

Příklad 7.14 (Homomorfismus krátkých exaktních posloupností)**.** Uvažujme následující dvě posloupnosti

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \ ,$$

$$0 \longrightarrow \mathbb{Z}/k\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \ ,$$

takové, že $m = kn$. Zobrazení jsou vždy násobení n a kanonick8 projekce. Nyní vytvoříme následující diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}/k\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \end{array}$$

Přesvědčte se o komutativitě diagramu

Řešení. Pro jednoduchost vezměme konkrétní diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

kommutativita druhého čtverce je zřejmá

$$\begin{array}{ccc} \mathbb{Z} & & \\ \downarrow & \searrow & \\ \mathbb{Z}/6\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \end{array}$$

jedná se jen o po sobě složenou projekci. První čtverec má v řádcích "stejná"zobrazení. Vzhledem k definici násobení v třídách ekvivalence se nám čtverec musí komutovat. ◇

Příklad 7.15 (Fibrovaný součin)**.** Tato užitečná konstrukce je zobecněním přímého součinu modulů. Nechť jsou dány dvě zobrazení modulů

$$f : A \to C \qquad g : B \to C \, ,$$

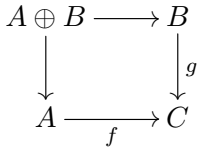
a uvažujme následující diagram

$$\begin{array}{ccc} & & B \\ & & \downarrow g \\ A & \xrightarrow[f]{} & C \end{array}$$

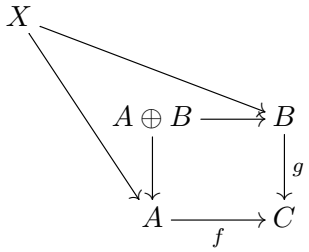
Zkonstruujte modul X tak, aby následující diagram komutoval

$$\begin{array}{ccc} X & \longrightarrow & B \\ \downarrow & & \downarrow g \\ A & \xrightarrow[f]{} & C \end{array}$$

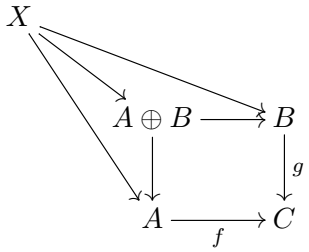
Řešení. Nejdříve si uvědome, že můžeme zkonstruovat modul $A \oplus B$ a jeho projekcemi "napojit"na náš diagram.



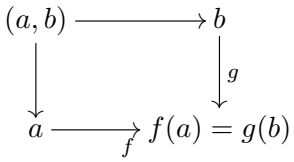
tento diagram ovšem nekomutuje! Uvažujme, že existuje modul X ze zadání tedy máme



z universality produktu (součtu) modulů se musí faktorovat zobrazení z X přes $A \oplus B$ tedy



tato skutečnost nám může napovědět hledat X jako podmodul součtu potom podmínka komutace nám říká, že pro libovolné $(a, b) \in A \oplus B$ musíme mít



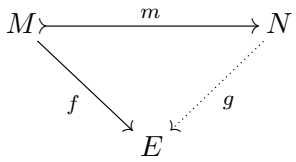
to je naše podmínka, tedy modul X je dán jako

$$X = \{(a, b) \in A \oplus B | f(a) = g(b)\}.$$ ◇

8. Injektivní moduly, injektivní obal modulů

8.1. Injektivní moduly

Definice 8.1 (Injektivní modul)**.** Modul E nad okruhem R je *injektivní*, jestliže pro libovolný monomorfizmus $m : M \to N$ a pro libovolný morfizmus $f : M \to E$ existuje morfizmus $g\colon N \to E$ takový, že $g \circ m = f$ neboli:



Věta 8.2. *Platí:*

(i) Součin injektivních modulů je injektivní.

(ii) Přímý sčítanec injektivního modulu je injektivní.

(iii) Injektivní $\mathbb{Z}$-moduly jsou právě divizibilní komutativní grupy.

(iv) Vektorové prostory jsou injektivní moduly.

Příklad 8.3. Ukažte, jak z předchozí teorie plyne (ne)injektivita následujících modulů:

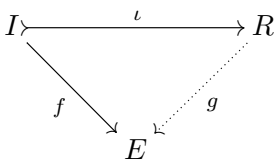
1. $\mathbb{Z}$-modul $\mathbb{Q}$
2. $\mathbb{Z}$-modul $\mathbb{R}$
3. $\mathbb{Q}$-modul $\mathbb{R}$
4. $\mathbb{Z}$-modul $\mathbb{Q}/\mathbb{Z}$
5. $\mathbb{Z}$-modul $\mathbb{Z}$
6. $\mathbb{Z}$-modul $\mathbb{Z}_n$

Řešení.

1. Ano. $\mathbb{Q}$ je divizibilní grupa.
2. Ano. $\mathbb{R}$ je divizibilní grupa.
3. Ano. $\mathbb{R}$ je vektorový prostor nad $\mathbb{Q}$.
4. Ano. $\mathbb{Q}/\mathbb{Z}$ je divizibilní grupa.
5. Ne. $\mathbb{Z}$ není divizibilní grupa.
6. Ne. $\mathbb{Z}_n$ není divizibilní grupa.

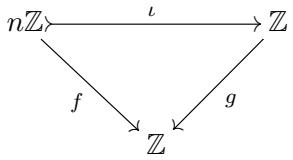
◇

Věta 8.4. (Baerovo kritérium) *Mějme R-modul E. Potom E je injektivní právě tehdy, když pro libovolný levý ideál I okruhu R a libovolný morfizmus $f\colon I \to E$ existuje morfizmus $g\colon R \to E$, jehož zúžení na I je f neboli:*



Příklad 8.5. Pomocí Baerova kritéria dokažte, že $\mathbb{Z}$ není injektivní $\mathbb{Z}$-modul.

Řešení. Pro $\mathbb{Z}$-modul $\mathbb{Z}$ mějme inkluzi libovolného ideálu $\iota : n\mathbb{Z} \to \mathbb{Z}$ pro libovolné $n > 1$. Mějme morfizmus $f : n\mathbb{Z} \to \mathbb{Z}$ určený předpisem $f(nk) = k$ a předpokládejme, že existuje morfizmus $g\colon \mathbb{Z} \to \mathbb{Z}$ takový, že následující trojúhelník komutuje:



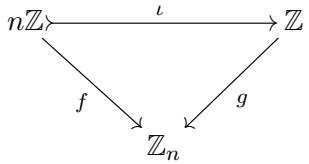
Potom platí:

$$ng(1) = g(n) = f(n) = 1$$

což není možné pro žádné $n > 1$. ◇

Příklad 8.6. Pomocí Baerova kritéria dokažte, že $\mathbb{Z}_n$ není injektivní $\mathbb{Z}$-modul pro žádné $n > 1$.

Řešení. Mějme inkluzi ideálu $\iota : n\mathbb{Z} \to \mathbb{Z}$ a morfizmus $f : n\mathbb{Z} \to \mathbb{Z}_n$ s předpisem $f(nk) = [k]_n$. Podle Baerova kritéria existuje morfizmus $g\colon \mathbb{Z} \to \mathbb{Z}_n$ takový, že následující trojúhelník komutuje:



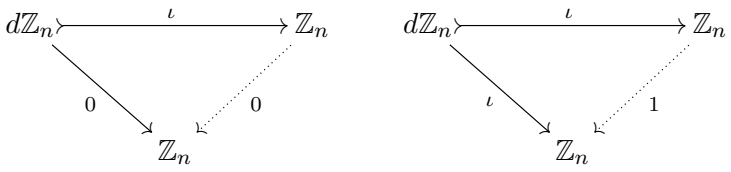
Potom ale:

$$0 = ng(1) = g(n) = f(n) = 1$$

což je spor. ◇

Příklad 8.7. Pomocí Baerova kritéria dokažte, že $\mathbb{Z}_n$ je injektivní $\mathbb{Z}_n$-modul pro každé $n \in \mathbb{N}$.

Řešení. Použijeme Baerovo kritérium. Libovolný ideál $\mathbb{Z}_n$ je tvaru $d\mathbb{Z}_n = \{kd \mid k \in \mathbb{Z}\}$ pro nějaký dělitel d čísla n. Každé $\mathbb{Z}_n$-lineární zobrazení libovolného z těchto ideálů do $\mathbb{Z}_n$ je buď nulové zobrazení nebo inkluze podmodulu. V obou případech jsme schopni doplnit na komutativní trojúhelník:



◇

Příklad 8.8. Dokažte, že pro každý obor integrity R je jeho těleso zlomků $\mathcal{Q}(R)$ injektivní R-modul.

Řešení. Mějme libovolný morfizmus $f\colon I \to \mathcal{Q}(R)$, kde I je ideál okruhu R. Pokud $I = 0$, je tvrzení triviální. Nechť $x \in I \setminus \{0\}$, definujeme zobrazení $g\colon R \to \mathcal{Q}(R)$ předpisem:

$$g(r) = r\frac{f(x)}{x}$$

Toto zobrazení je zřejmě R-lineární a pro každé $r \in I$ platí:

$$g(\iota(r)) = g(r) = r\frac{f(x)}{x} = \frac{f(rx)}{x} = \frac{f(xr)}{x} = x\frac{f(r)}{x} = f(r)$$

Modul $\mathcal{Q}(R)$ je tedy injektivní. ◇

Věta 8.9. *Modul E je injektivní právě tehdy, když* $\mathrm{Hom}(-, E)$ *zobrazuje monomorfizmy na epimorfizmy.*

Příklad 8.10. Dokažte, že E je injektivní modul právě tehdy, když $\mathrm{Hom}(-, E)$ je exaktní funktor.

Řešení.
⇒: Nechť E je injektivní modul a mějme krátkou exaktní posloupnost:

$$0 \longrightarrow M \overset{m}{\rightarrowtail} N \overset{e}{\twoheadrightarrow} K \longrightarrow 0$$

Chceme ukázat, že i následující posloupnost je exaktní:

$$0 \longleftarrow \mathrm{Hom}(M, E) \overset{\mathrm{Hom}(m,E)}{\longleftarrow} \mathrm{Hom}(N, E) \overset{\mathrm{Hom}(e,E)}{\longleftarrow} \mathrm{Hom}(K, E) \longleftarrow 0$$

Funktor $\mathrm{Hom}(-, E)$ zobrazuje vždy epimorfizmy na monomorfizmy. Pro libovolné $f, g\colon K \to E$ můžeme využít definice epimorfizmu a psát:

$$\mathrm{Hom}(e, E)(f) = \mathrm{Hom}(e, E)(g) \Rightarrow f \circ e = g \circ e \Rightarrow f = g$$

Zobrazení $\mathrm{Hom}(e, E)$ je injektivní, tedy monomorfizmus. Dále protože je E injektivní, zobrazuje monomorfizmy na epimorfizmy. Zbývá dokázat:

$$\ker \mathrm{Hom}(m, E) = \mathrm{Im}\, \mathrm{Hom}(e, E)$$

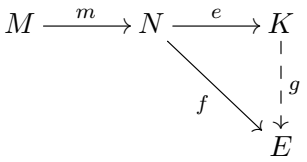
Inkluze $\supseteq$ plyne z $e \circ m = 0$ a:

$$[\mathrm{Hom}(m, E) \circ \mathrm{Hom}(e, E)]\,(f) = f \circ e \circ m = 0$$

Pro opačnou inkluzi nechť $f \in \ker \mathrm{Hom}(m, E)$, tj:

$$f \circ m = \mathrm{Hom}(m, E)(f) = 0$$

Potom z univerzální vlastnosti kojádra $e\colon N \to E$ plyne existence $g\colon K \to E$ takového, že následující diagram komutuje:



To znamená:

$$f = g \circ e = \mathrm{Hom}(e, E)(g)$$

čili $f \in \mathrm{Im}\,\mathrm{Hom}(e, E)$.

$\Leftarrow$: Nechť je $\mathrm{Hom}(-, E)$ exaktní. Libovolný monomorfizmus $m\colon M \to N$ nám zadává krátkou exaktní posloupnost:

$$0 \longrightarrow M \overset{m}{\rightarrowtail} N \overset{p}{\twoheadrightarrow} N/M \longrightarrow 0$$

Tu nám funktor $\mathrm{Hom}(-, E)$ podle předpokladu zobrazí na krátkou exaktní posloupnost, ve které bude $\mathrm{Hom}(m, E)$ epimorfizmus. Tento funktor tedy zobrazuje monomorfizmy na epimorfizmy, proto E musí být injektivní. ◇

Příklad 8.11. Dokažte, že součet injektivních modulů nad noetherovským okruhem je injektivní modul.

Řešení. Mějme systém M_i, $i \in I$, injektivních R-modulů a nechť R je noetherovský. Označme $M = \bigoplus_{i \in I} M_i$. Mějme libovolný ideál I okruhu R a libovolné R-lineární zobrazení $f\colon I \to M$. Protože R je noetherovský, je ideál I konečně generovaný a obraz f můžeme zúžit na $M_J = \bigoplus_{j \in J} M_j$ pro nějakou konečnou podmnožinu $J \subseteq I$. Tento konečný součet splývá se součinem a jakožto součin injektivních modulů je injektivní. Proto existuje $g : R \to M_J$ komutující $g \circ \iota = f$. Zobrazení g můžeme zpět rozšířit na zobrazení typu $R \to M$ a M je injektivní. ◇

Definice 8.12. Nechť R je obor integrity. Řekneme, že R-modul M je *divizibilní*, jestliže pro každé $r \in R \setminus \{0\}$ a $x \in M$ existuje $y \in M$ splňující $ry = x$, tj. jestliže $rM = M$ pro každé $r \in R \setminus \{0\}$.

Příklad 8.13. Dokažte, že každý injektivní modul M nad oborem integrity R je divizibilní.

Řešení. Mějme $r \in R$ libovolné. Zřejmě platí, že $rM \subseteq M$. Pro opačnou inkluzi mějme $x \in M$ libovolné. Uvažme rR jako ideál oboru R. Zvolme morfizmus $\ell_x\colon Rr \to M$ s předpisem $\ell_x(sr) = sx$. Díky injektivitě M se tento morfizmus rozšíří podél inkluze $Rr \hookrightarrow R$ na morfizmus $h\colon R \to M$. Přitom platí:

$$rh(1) = h(r) = \ell_x(r) = x$$

Našli jsme tedy hledané $y = h(1)$ a M je divizibilní. ◇

Příklad 8.14. Dokažte, že každý divizibilní modul M nad oborem hlavních ideálů R je injektivní.

Řešení. Využijeme Baerovo kritérium. Mějme libovolný ideál I okruhu R a morfizmus $f\colon I \to M$. Podle předpokladu $I = (r)$ pro nějaké $r \in R$. V tom případě je zobrazení f jednoznačně určeno obrazem $f(r) = x$. Protože je modul M divizibilní, existuje $y \in M$ splňujíci $ry = x$. Zadejme zobrazení $g\colon R \to M$ předpisem $g(a) = ay$. Potom pro každé $sr \in I$ platí:

$$(g \circ \iota)(sr) = sry = sx = sf(r) = f(sr)$$

Modul M je tedy injektivní. ◇

Příklad 8.15. Dokažte, že každý divizibilní modul M bez torze nad oborem integrity R je injektivní.

Řešení. Pro splnění Baerova kritéria nechť I je libovolný ideál R a $f : I \to M$ libovolný morfizmus. Pro libovolné $r \in I$ z divizibility plyne existence prvku $x \in M$ splňujícího $f(r) = rx$. Pokud je $s \in I$ další prvek, pak platí:

$$rf(s) = f(rs) = f(sr) = sf(r) = srx = rsx$$

Protože M je bez torze, plyne z toho $f(s) = sx$. V tom případě máme automaticky rozšíření g morfizmu f s předpisem $g(r) = rx$ pro $r \in R$. Modul M je tedy injektivní. ◇

8.2. Injektivní obal a podstatná rozšíření

Definice 8.16 (Podstatné rozšíření)**.** Podmodul N modulu M nazýváme *podstatný* (zapisujeme $N \subseteq_e M$), jestliže pro libovolný podmodul K modulu M, platí implikace:

$$K \cap N = 0 \Rightarrow K = 0$$

Modul M nazýváme *podstatné rozšíření* modulu N.

Příklad 8.17. Dokažte přímo z definice, zda je N podstatný podmodul M pro:

1. $M = \mathbb{Z}$ a $N = n\mathbb{Z}$ pro $n \geq 2$
2. $M = \mathbb{Q}$ a $N = \mathbb{Z}$
3. $M = \mathbb{R}$ a $N = \mathbb{Z}$
4. $M = \mathbb{R}$ a $N = \mathbb{Q}$
5. $M = \mathbb{C}$ a $N = \mathbb{R}$

Řešení.

1. Ano. Libovolný netriviální podmodul $\mathbb{Z}$ je tvaru $k\mathbb{Z}$ pro $k \in \mathbb{N}$ a vždy platí $d \in k\mathbb{Z} \cap n\mathbb{Z}$, kde d je největší společný násobek čísel n a k.
2. Ano. Libovolný netriviální podmodul $\mathbb{Q}$ musí obsahovat nenulové $\frac{a}{b}$. Potom ale musí obsahovat i $b\frac{a}{b} = a \in \mathbb{Z}$.
3. Ne. Pro libovolné transcendentní číslo $x \in \mathbb{R}$ platí $\langle x \rangle \cap \mathbb{Z} = 0$.
4. Ne. Podobně jako předchozí bod dokonce $\langle x \rangle \cap \mathbb{Q} = 0$.
5. Ne. Například $i\mathbb{R} \cap \mathbb{R} = 0$. ◇

Příklad 8.18. Pro modul M a jeho podmoduly N a K dokažte:

1. $K \subseteq_e N \wedge N \subseteq_e M \Rightarrow K \subseteq_e M$
2. $N \cap K \subseteq_e M \Leftrightarrow N \subseteq_e M \wedge K \subseteq_e M$

Řešení.

1. Nechť L je libovolný podmodul M. Argumentujme:

$$K \cap L = 0 \Rightarrow K \cap (N \cap L) = 0 \Rightarrow N \cap L = 0 \Rightarrow L = 0$$

2. Nechť znova je L libovolný podmodul M. Pro směr $\Leftarrow$:

$$(N \cap K) \cap L = N \cap (K \cap L) = 0 \Rightarrow K \cap L = 0 \Rightarrow L = 0$$

   Pro směr $\Rightarrow$:

$$N \cap L = 0 \Rightarrow N \cap K \cap L = 0 \Rightarrow L = 0$$
$$K \cap L = 0 \Rightarrow N \cap K \cap L = 0 \Rightarrow L = 0$$

◇

Definice 8.19. *Injektivní obal* R-modulu M je takový injektivní modul $E_R(M)$, že existuje monomorfizmus $M \to E_R(M)$ a pro každý injektivní modul, který obsahuje podmodul izomorfní M, obsahuje také podmodul izomorfní $E_R(M)$.

Věta 8.20. *Mějme modul M a jeho nadmodul E. Potom následující podmínky jsou ekvivalentní:*

(i) *E je injektivní obal modulu M.*

(ii) *E je injektivní modul a je podstatným rozšířením modulu M.*

(iii) *E je maximální podstatné rozšíření modulu M.*

Příklad 8.21. Dokažte, že pro libovolný modul M a jeho podmodul N platí:

$$N \subseteq_e M \Rightarrow E(N) = E(M)$$

Řešení. Podle věty 8.20 je $M \subseteq_e E(M)$. Podle příkladu 8.18 zase:

$$N \subseteq_e M \subseteq_e E(M) \Rightarrow N \subseteq_e E(M)$$

Opět využitím věty 8.20 je $E(N) = E(M)$. ◇

Příklad 8.22. Pro každý obor integrity R platí $E_R(R) \cong \mathcal{Q}(R)$, kde $\mathcal{Q}(R)$ je těleso zlomků oboru R.

Řešení. Víme, že $\mathcal{Q}(R)$ je injektivní R-modul. Stačí ukázat, že R je podstatný podmodul $\mathbb{Q}(R)$. To však jde okamžitě vidět, neboť libovolný podmodul N modulu $\mathbb{Q}(R)$ obsahující nenulový zlomek $\frac{r}{s}$, musí obsahovat také $s\frac{r}{s} = r \in R$. ◇

Příklad 8.23. Pro $k \in \mathbb{N}$ a prvočíslo p uvažme $\mathbb{Z}_{p^k}$ jakožto $\mathbb{Z}$-modul. Určete $E_{\mathbb{Z}}(\mathbb{Z}_{p^k})$.

Řešení. Ukážeme:

$$E_{\mathbb{Z}}(\mathbb{Z}_{p^k}) \cong \mathbb{Z}_{p^\infty} = \mathbb{Z}[1/p^n \mid n \in \mathbb{N}]/\mathbb{Z}$$

přičemž grupu $\mathbb{Z}_{p^k}$ ztotožníme s podgrupou $\{n/p^k \mid 0 \leq n < p^k\}$. Grupa $\mathbb{Z}_{p^\infty}$ je zřejmě divizibilní, čili injektivní $\mathbb{Z}$-modul. Stačí ukázat, že $\mathbb{Z}_{p^k}$ je její podstatný podmodul. To je ale také snadné, neboť $\mathbb{Z}_{p^k}$ obsahuje $1/p$ nehledě na k, stejně jako každá jiná netriviální podgrupa. ◇

Příklad 8.24. Nechť $\mathbb{K}$ je těleso a uvažme na $\mathbb{K}$ strukturu $\mathbb{K}[x]$-modulu zadaného $k \cdot u = ku$ pro $k \in \mathbb{K}$ a $x \cdot u = 0$, nebo také jinak $p(x) \cdot u = qu$, kde q je absolutní člen polynomu $p \in \mathbb{K}[x]$. Zkonstruujte injektvní obal $\mathbb{K}[x]$-modulu $\mathbb{K}$.

Řešení. Ukážeme:

$$E_{\mathbb{K}[x]}(\mathbb{K}) \cong \mathbb{K}[x^{-1}] = \{k/x^n \mid n \in \mathbb{N}, k \in \mathbb{K}\}$$

Na modulu $\mathbb{K}[x^{-1}]$ máme zavedenu strukturu $\mathbb{K}[x]$-modulu předpisy:

$$k \cdot (a_0 + a_1x^{-1} + \ldots + a_nx^{-n}) = ka_0 + ka_1x^{-1} + \ldots + ka_nx^{-n}$$
$$x \cdot (a_0 + a_1x^{-1} + \ldots + a_nx^{-n}) = a_1 + a_2x^{-1} + \ldots + a_nx^{-n+1}$$

kde $k \in \mathbb{K}$. Modul $\mathbb{K}[x^{-1}]$ obsahuje přirozeně podmodul $\mathbb{K}$ a ten je zřejmě jeho podstatný podmodul. Nyní ukážeme, že $\mathbb{K}[x^{-1}]$ je také injektivní. Pro využití Baerova kritéria nechť

$J \subseteq \mathbb{K}[x]$ je libovolný ideál a $f\colon J \to \mathbb{K}[x^{-1}]$ je morfizmus $\mathbb{K}[x]$-modulů. Pokud $J = 0$, pak není co dokazovat. Naopak nechť $q(x) \in J$ je nekonstantní polynom. Platí $q(x)q(x^{-1}) = a^2$, kde $a \neq 0$ je vedoucí koeficient polynomu q. Zadejme $g\colon \mathbb{K}[x] \to \mathbb{K}[x^{-1}]$ předpisem:

$$g(p(x)) = p(x)f(q(x))q(x^{-1})a^{-2}$$

Potom pro každé $p(x) \in J$ platí:

$$\begin{aligned} g(p(x)) &= p(x)f(q(x))q(x^{-1})a^{-2} = f(p(x)q(x))q(x^{-1})a^{-2} \\ &= f(p(x))q(x)q(x^{-1})a^{-2} = f(p(x))a^2a^{-2} = f(p(x)) \end{aligned}$$

a důkaz je hotov. ◇

9. Jednoduché a Polojednoduché moduly

Polojednoduché moduly jsou speciálním typem modulů. Tato skupina má velké využití v teorii reprezentací. Zásadní větou celé teorie polojdnoduchých modulů je Wedderburnova věta, která nám dává úplnou charakterizaci pomocí takzvaných jednoduchých modulů, které je třeba chápat jako základní stavební bloky teorie. Jednoduché moduly jsou značně omezené svoji strukturou, toto nám říká jednoduché ale přitom silné *Shurovo Lemma*.

Definice 9.1 (Jednoduchý modul)**.** Jednoduchý modul M nemá žádný netriviální podmodul.

Poznámka. Tato skutečnost jde též vystihnout tak, že v libovolné následující posloupnosti

$$0 \longrightarrow I \xrightarrow{f} M \ ,$$

je zobrazení f vždy identicky nulové, tedy neexistuji netriviální injekce do tohoto modulu.

Díky této definici můžeme říct co je jednoduchý okruh

Definice 9.2 (Jednoduchý okruh). Okruh R nazveme jednoduchý, pakliže je jednoduchý jakožto modul nad sebou samým.

Poznámka. Jinak řečeno okruh R nemá žádné netriviální ideály.

Definice 9.3 (Polojednoduchý modul)**.** Polojednoduchý modul M je součtem konečně mnoha jednoduchých modulů.

Věta 9.4. *Nechť M je polojednoduchý modul, pak následující podmínky jsou ekvivalentní*

(i) *M je Noetherovský*

(ii) *M je Artinovský*

(iii) *M je přímý součin konečně mnoha jednoduchých modulů*

(iv) *M je konečně generovaný*

Poznámka. Všimněme si zejména posledního bodu, kde máme obsaženu jistou konečněrozměrnost modulu.

Lemma 9.5 (Shur)**.** *Nechť je M jednoduchý modul, potom platí, že každý endomorfismus je nutně izomorfismem.*

Poznámka. My se nemusíme trápit charakteristikou tělesa, protože v našich příkladech bude použito výhradně těleso $\mathbb{C}$.

Definice 9.6 (Reprezentace)**.** Reprezentace grupy G je grupový homomorfismus

$$G \to \mathrm{End}(V)$$

Definice 9.7 (Grupová algebra)**.** Grupová algebra je krásným a konkrétním příkladem, kde se přirozeně objeví teorie polojednoduchých modulů. Nechť je dána konečná grupa G a okruh R. Uvažujme prostor $R[G] = \bigoplus_{g\in G} a_g g$ formálních kombinací prvků z G a koeficienty z okruhu.

Z konstrukce je jasné, že je prostor R modulem. Navíc máme strukturu okruhu, kde násobení je dáno následovně

$$\sum_{g\in G} a_g g \sum_{h\in G} a_h h = \sum_{g\in G}\sum_{h\in G} a_g a_h (gh) = \sum_{g\in G}\sum_{kg^{-1}\in G} a_g a_{kg^{-1}} k$$

Uvedeme si ještě jednu větu popisující strukturu grupové algebry

Věta 9.8 (Mashke)**.** *Nechť G je konečná grupa a $\mathbb{F}$ těleso takové, že jeho charakteristika nedělí řád grupy, potom platí, že $\mathbb{F}G$ je polojednoduchý.*

Příklad 9.9 (Jednoduchý modul)**.** V tomto příkladu si ukážeme, že jednoduchý modul má velmi jednoduchou strukturu. Platí totiž, že libovolný jednoduchý R-modul

$$M \simeq \langle m \rangle_R \simeq R/\mathrm{Ann}(m)\,,$$

tedy je generován nějakým svým prvkem, anebo je izomorfní faktoru okruhu dle anihilátoru daného prvku.

Řešení. Začneme prvním isomorfismem. Vezměme prvek libovolný prvek $m \in M$. Zkonstruujme podmodul generovaný tímto prvkem tedy

$$\langle m \rangle_R = Rm$$

Zřejmě je tento modul podmodulem M, ale z jednoduchosti dostáváme, že poté již musí být celým modulem. Druhou část izomorfismu dostaneme jako jednoduchý důsledek věty o izomorfismu. Uvažujme homomorfismus modulů

$$R \xrightarrow{f} \langle m \rangle_R \qquad\qquad r \mapsto rm\ ,$$

toto je jistě homomorfismus a to dokonce surjektivní. Z věty o izomorfismu víme, že $R/\operatorname{Ker}(f) \simeq \langle m \rangle_R$. Nyní se stačí přesvědčit o tom, že $\operatorname{Ker}(f) = \mathrm{Ann}(m)$. To je ale jasné z definice $\operatorname{Ker}(f) = \{r \in R | rm = 0\} = Ann(m)$. ◇

Příklad 9.10 (Maticová algebra)**.** Důležitým příkladem polojednoduchých modulů jsou moduly nad maticovým okruhem. Definujme obecný maticový okruh nad okruhem s dělením D.

$$\mathrm{Mat}_n(D) = \left\{ \left. \begin{pmatrix} d_1^1 & d_2^1 & \dots & d_n^1 \\ d_1^2 & d_2^2 & \dots & d_2^2 \\ \vdots & \vdots & \ddots & \vdots \\ d_1^n & d_2^n & \dots & d_n^n \end{pmatrix} \right| d_j^i \in D \right\}. \tag{9.11}$$

Je zřejmé, že takto zobecněné matice na obecný okruh s dělením jsou též okruhem.

1. Podíváme se, jak vypadají levé, pravé a oboustranné ideály našeho maticového okruhu.
2. Ověříme, že D^n jakožto $\mathrm{Mat}_n(D)$ modul je jednoduchý.
3. Ověříme, že $D^n \oplus D^n \oplus \ldots \oplus D^n$ jakožto $\mathrm{Mat}_n(D)$ modul je polojednoduchý.

Řešení. Začneme prvním bodem. Zásadním faktem je uvědomit si, jak funguje maticové násobení. Uvažujme matici A působící na B zleva. Tento součin zřejmě nemíchá sloupce matice B. Tedy zejména matice tvaru

$$B = \begin{pmatrix} 0 & \dots & 0 & a^1 & 0 & \dots & 0 \\ 0 & \dots & 0 & a^2 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a^n & 0 & \dots & 0 \end{pmatrix},$$

zůstane po násobení libovolnou maticí zleva ve stejném tvaru. Duálně bude vypadat situace s pravým násobením a maticí tvaru

$$B = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \\ a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Odsud můžeme usoudit, že ideály bodu přesně dané „řádkové“ a „sloupcové“ matice. Je snadné všimnout si, že tato volba ideálu je minimální (čtenář jistě najde vhodnou matici, kterou z libovolného sloupce dostane libovolný jiný). Jinými slovy neexistuje žádný ideál sloupečku. ◇

Příklad 9.12 (Okruh s dělením)**.** Okruh s dělením je přímým zobecněním tělesa, někteří autoři dokonce nazývají okruh s dělením nekomutativním tělesem. Chtěli bychom ukázat, že $\mathrm{End}(M)$ pro okruh s dělením D.

Řešení. Tento příklad je jednoduchým důsledkem Frobeniovy věty. Nechť M je jednoduchý modul ◇

Poznámka. Existuje úplná charakterizace konečných okruhů s dělením nad jakožto $\mathbb{R}$ algeber. Věta (*Frobeniova*) tvrdí že až na isomorfismus existují pouze $\mathbb{R}, \mathbb{C}$ a kvaterniony $\mathbb{H}$.

Příklad 9.13 (Grupová algebra dihedrální grupy)**.** Uvažujme dihedrální grupu na pěti prvcích D_5. Prezentace této grupy je dána následovně

$$\langle r, s | r^4 = 1,\ s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$$

Pro názornost uvedeme konkrétní maticovou reprezentaci

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

necháme na čtenáři, aby ověřil příslušné relace pro dané generátory.

Řešení. Nyní ukážeme konkrétní realizaci grupové algebry a najdeme její podmodul, tedy ukážeme, že je grupová algebra polojednoduchá. ◇

Příklad 9.14 (Modul nad PID)**.** Zúžením na speciální typ okruhů (PID) se teorie modulů velmi zjednodušuje. V tomto příkladu nastíníme charakterizaci obecného modulu nad PID. Čtenář obeznámený s teorii klasifikací abelovských konečných grup jistě uvidí analogii.

Příklad 9.15 (Jednoduché moduly nad $\mathbb{Z}$)**.** Ukážeme, že všechny jednoduché $\mathbb{Z}$-moduly jsou izomorfní s $\mathbb{Z}/n\mathbb{Z}$ pro n provočíslo.

Řešení. Začněme pozorováním, že samotné $\mathbb{Z}$ jako modul nad sebou samým není jednoduchý. To je zřejmé, protože zejména známe jak vypadají všechny jeho ideály. Nyní využijeme charakterizace z prvního cvičení, že každý jednoduchý modul nad $\mathbb{Z}$ je tvaru

$$M \simeq \mathbb{Z}/\mathrm{Ann}(m)\,,$$

anihilátor prvku m je ideálem a z vlastnosti PID musí být $n\mathbb{Z}$. Ale zároveň víme, že kdyby n nebylo prvočíslo, tak by výsledný modul šel napsat ve tvaru $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}$. ◇

Příklad 9.16 (Jednoduché moduly nad F[x])**.** Tento příklad je podobný předchozímu a budeme se zde snažit ukázat, že každý jednoduchý F[x]- modul je izomorfní F[x]/I kde I je prvoideál.

Řešení. Budeme postupovat obdobně jako v předchozím cvičení. Využitím prvního cvičení máme

$$M \simeq \mathrm{F}[x]/\mathrm{Ann}(m)\,,$$

Jediné, co je potřeba ověřit je, že Ann(m) je prvoideál. Víme, že F[x] je PID okruh tedy Ann(m) jakožto ideál musí mít jeden generátor p. Tvrdíme, že polynom p musí být ireducibilní. Musíme rozebrat dva případy

1. Když je $p = qr$ kde jsou oba faktory nesoudělné.
2. Když je $p = q^n$

Z PID plyne, že p má jednoznačný rozklad $p = \alpha q_1^{n_1} \dots q_k^{n_k}$. Řečeno jazykem ideálů, dostáváme

$$\langle p\rangle = \langle q_1^{n_1}\rangle \cap \dots \cap \langle q_k^{n_k}\rangle\,,$$

z čínské věty o zbytcích víme, že

$$\mathrm{F}[x]/\langle p\rangle \simeq \mathrm{F}[x]/\langle q_1^{n_1}\rangle \oplus \dots \oplus \mathrm{F}[x]/\langle q_k^{n_k}\rangle\,.$$

To je ve sporu s ireducibilitou. Tedy jediné, co se může stát, je možnost $\langle p\rangle = \langle q^n\rangle$ to by ale modul též nebyl jednoduchý. ◇

Poznámka. Je důležitým požadavkem, že F je těleso. Kdyby tak nebylo, pak okruh nebude PID. Uvažujte například $\mathbb{Z}[x]$ a jeho ideál $\langle 3, x\rangle$.

Příklad 9.17. Ukážeme si krásný geometrický příklad neasociativního okruhu, který čtenář jistě zná již od střední školy. Uvažujme vektorový prostor R^3 společně s vektorovým násobením. Z analytické geometrie víme, že dohromady se součtem jistě tvoří okruh, ovšem neasociativní! Dokážeme, že tento okruh je sám nad sebou jednoduchý.

Řešení. Předpokládejme, že existuje podmodul M s prvkem u a bez ztráty obecnosti vezměme normovaný vektor. Doplňme tento prvek na ortonormální bázi (u, v, w). Vektorový součin na této bázi vypadá

$$u \times v = w \quad v \times w = u \quad w \times u = v\,,$$

tedy zapůsobením na v vektory u, w dostaneme celou bázi a ta generuje celé $\mathbb{R}^3$. ◇

Příklad 9.18 (Weylova Algebra)**.** Ukážeme si velmi zajímavý příklad jednoduchého modulu. Nechť je dán $\mathbb{C}[x]$ okruh polynomů. Ten zřejmě můžeme chápat jako modul nad sebou samým. My ale rozšíříme bázový okruh. Definujme

$$\partial : \mathbb{C}[x] \to \mathbb{C}[x]$$

$$\partial(a_n x^n + \dots + a_1 x + a_0) = n a_n x^{m-1} + \dots + a_1$$

tedy jako klasickou derivaci. Vzhledem ke konečnosti polynomů můžeme tuto operaci chápat čistě algebraicky, tedy není třeba žádných analytických metod. Nyní definujme okruh $\mathcal{D}(\mathbb{C}[x])$, což bude okruh všech diferenciálních operátorů na $\mathbb{C}[x]$. Tedy prvky mají tvar

$$d = f_n(x)\partial^n + \dots + f_1(x)\partial + f_0(x)\,.$$

Z tvaru obecného prvku je jednoduché přesvědčit se o tom, že okruh $\mathcal{D}(\mathbb{C}[x])$ je generován symboly $\{x, \partial\}$ jako nekomutativní okruh. Navíc z vlastnosti operace derivace vidíme

$$(\partial x)f = f + (x\partial)f \qquad [\partial, x] := \partial x - x\partial = 1\,.$$

Můžeme tedy napsat $\mathcal{D}(\mathbb{C}[x])$ jako

$$\frac{\mathbb{C}\langle\partial, x\rangle}{\langle[\partial, x] - 1\rangle}\,,$$

tedy jako okruh nekomutativních polynomů s jednou relací. Nyní tvrdíme, že $\mathbb{C}[x]$ jakožto $\mathcal{D}(\mathbb{C}[x])$-modul je jednoduchý.

Řešení. Vzhledem k tomu, že $\mathcal{D}(\mathbb{C}[x])$ obsahuje $\mathbb{C}[x]$, stačí ukázat, že každý podmodul obsahuje prvek $1 \in \mathbb{C}[x]$ a tedy bude celým modulem. To je ovšem jednoduché: nechť M je podmodulem a $p \in M \subset \mathbb{C}[x]$. Element je tvaru

$$p = a_n x^n + \ldots + a_1 x + a_0\,,$$

aplikací

$$d = (a_n n!)^{-1}\partial^n\,,$$

dostaneme polynom 1, tedy podmodul je celým modulem. Okruh $\mathcal{D}(\mathbb{C}[x])$ je zároveň $\mathbb{R}$ algebrou a jak název cvičení naznačuje je znám jako Weylova algebra. ◇

10. Noetherovské a artinovské okruhy a moduly

Definice 10.1 (Noetherovský modul)**.** Řekneme, že (levý) $R-$modul M je *(levý) noetherovský*, jestliže pro každý neklesající řetězec $N_1 \subseteq N_2 \subseteq N_3 \dots$ (levých) podmodulů modulu M platí, že existuje $n \in \mathbb{N}$ tak, že $N_n = N_{n+1} = \dots$.

Tato definice se dá rovněž zformulovat tak, že každý neklesající řetězec podmodulů se nutně stabilizuje (často je tato podmínka nazývaná (ACC) - *ascending chain condition*). Okruh nazveme *(levý) noetherovský*, pokud je *(levý) noetherovský* jako (levý) modul sám nad sebou. Podmínka na podmoduly pak přechází na podmínku na (levé) ideály v daném okruhu. Rovněž lze definovat pojem noetherovský pro pravé podmoduly, v případě okruhů pro pravé ideály.

Definice 10.2 (Artinovský modul)**.** Řekneme, že R modul M je *(levý) artinovský*, jestliže pro každý řetězec (levých) podmodulů $N_1 \supseteq N_2 \supseteq N_3 \dots$ modulu M platí, že existuje $n \in \mathbb{N}$ tak, že $N_n = N_{n+1} = \dots$.

Opět můžeme definici formulovat tak, že se každý nerostoucí řetězec (levých) podmodulů stabilizuje (někdy (DCC) - *descending chain condition*). Podobně okruh nazveme *(levý) artinovský*, pokud je (levý) artinovský jako modul sám nad sebou, dostáváme pak podmínky pro (levé) ideály. Rovněž lze mluvit o pravých artinovských okruzích a modulech.

Příklad 10.3 (Zoologie noetherovských okruhů a modulů)**.** Rozhodněte o noetherovskosti následujících okruhů, popř. dejte podmínky na to, kdy budou dané okruhy noetherovské. Dále rozhodněte o noetherovskosti uvedených modulů.

1. $\mathbb{Z}$ okruh celých čísel,
2. Libovolné těleso k,
3. Okruh hlavních ideálů R,
4. $A[x_i]$ okruh polynomů nekonečně mnoha proměnných nad okruhem A,
5. $\mathbb{Z}[i]$ okruh Gaussovských celých čísel,
6. $\mathbb{B}$ okruh celých algebraických čísel, tedy algebraických čísel, jejichž minimální polynom je normovaný,
7. $\mathbb{Q}$ jako $\mathbb{Z}-$modul.

Řešení. K řešení těchto příkladů se dá přistoupit mnoha způsoby, pokusme se o (neúplný) výčet argumentů, které se dají v různých situacích použít:

1. $\mathbb{Z}$ vskutku je noetherovský, například neboť každý nenulový ideál $I \subset \mathbb{Z}$ je generovaný jedním prvkem $I = (n), n \in \mathbb{N}$ a víme, že $(a) \subset (b)$, právě když $b|a$. Z jednoznačnosti rozkladu na prvočísla v $\mathbb{Z}$ dostáváme, že nad každým nenulovým ideálem v $\mathbb{Z}$ může ležet pouze konečně mnoho ideálů a tedy $\mathbb{Z}$ je nutně noetherovský.
2. Ano, každé těleso obsahuje pouze dva ideály, a to nulový ideál a samo sebe.
3. Ano, uvažme sjednocení celého řetězce $\bigcup_{i\in\mathbb{N}} I_i = I$, což je jistě opět ideál. Pak platí, že $I = (a)$ pro nějaké $a \in R$ a tedy $a \in I_n$ pro nějaké $n \in \mathbb{N}$. Odtud ovšem $I_n = I_{n+1} = \cdots$
4. $A[x_i]$ okruh polynomů nekonečně mnoha proměnných nad okruhem A nikdy není noetherovský okruh. Posloupnost ideálů $(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \cdots, x_n) \subset$ je jistě nekonečný rostoucí řetězec ideálů, který se nikdy nestabilizuje.

5. $\mathbb{Z}[i]$ je noetherovský. Je to dokonce tzv. *Dedekindův okruh*, které jsou vždy noetherovské (celouzavřené, noetherovské a každý prvoideál je maximální - *Krullovy dimenze* 1). Obecně okruhy, které vzniknou jako celý uzávěr $\mathbb{Z}$ v číselném tělese (konečného rozšíření $\mathbb{Q}$, ekvivalentně přidáním jediného algebraického čísla ke $\mathbb{Q}$) jsou Dedekindovy, a tudíž noetherovské okruhy. Avšak $\mathbb{Z}[i]$ je navíc okruh s jednoznačným rozkladem a je na něm definována multiplikativní *norma* $\mathbb{Z}[i] \to \mathbb{N}_0$, $a+bi \mapsto a^2+b^2$, která nám umožňuje zavést *Euklidův algoritmus* a můžeme tedy použít stejný argument jako pro $\mathbb{Z}$.
6. Okruh celých algebraických čísel $\mathbb{B}$ není noetherovský, neboť obsahuje nekonečnou rostoucí posloupnost ideálů $(2) \subset (\sqrt{2}) \subset (\sqrt[4]{2}) \cdots$. Naproti tomu okruh všech algebraických čísel noetherovský je, jelikož jde o těleso.
7. Ne, $\mathbb{Q}$ není noetherovský modul jako abelovská grupa. Můžeme uvážit například nekonečnou posloupnost podgrup $\mathbb{Z} \subset \frac{1}{2}\cdot\mathbb{Z} \subset \frac{1}{4}\cdot\mathbb{Z} \cdots \subset \frac{1}{2^n}\cdot\mathbb{Z} \subset \cdots$, která se jistě nikdy nestabilizuje. ◇

Oproti noetherovským okruhům, artinovské okruhy mají obecně mnohem složitější strukturu. Ačkoliv se (DCC) zdá jako duální podmínka k (ACC), ve skutečnosti jde o mnohem silnější podmínku a platí, že každý artinovský okruh je noetherovský okruh. Caveat: neplatí pro moduly, artinovský modul nemusí být noetherovský.

Příklad 10.4 (Příklady artinovských okruhů a modulů)**.** Rozhodněte o artinovskosti následujících okruhů či modulů.

1. $\mathbb{Z}$ okruh celých čísel,
2. Obor integrity R,
3. $\mathbb{Q}/\mathbb{Z}$ jako $\mathbb{Z}-$modul,
4. $\mathbb{Z}[\frac{1}{p}]$ jako $\mathbb{Z}-$modul, tedy zlomky, kde ve jmenovali povolíme pouze mocniny předem zafixovaného prvočísla p,
5. $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ jako $\mathbb{Z}-$modul,
6. k těleso, V vektorový prostor nad k konečné dimenze.

Řešení. Opět naznačíme několik možných způsobů rozhodování, zda je okruh artinovský.

1. $\mathbb{Z}$ není artinovský, neboť máme nekonečný řetězec ideálů $(p) \supset (p^2) \supset \cdots \supset (p^n) \supset \cdots$, který se jistě nestabilizuje.
2. Předpokládejme, že R je artinovský. Buď $a \in R$ libovolný nenulový prvek. Potom jistě mám klesající posloupnost ideálů $(a) \supset (a^2) \supset \ldots$, která se podle předpokladu stabilizuje, tedy pro nějaké $n \in \mathbb{N}$ platí $(a^n) = (a^{n+1})$. Avšak vzhledem k vlastnostem hlavních ideálů to znamená, že $a^{n+1}|a^n$, tedy že existuje $b \in R$ tak, že $a^{n+1}\cdot b = a^n$. Vydělením a^n (R je obor integrity) dostáváme, že $ab = 1$ a tedy a je jednotka. Libovolný nenulový prvek oboru integrity R je jednotka a tudíž R je těleso. Zřejmě všechna tělesa jsou artinovská (vždyť mají jen dva ideály), dostáváme tedy, že obor integrity je artinovský, právě když je tělesem.
3. $\mathbb{Q}/\mathbb{Z}$ není artinovský modul jako abelovská grupa, neboť můžeme uvážit následující posloupnost podmodulů: v prvním podmodulu zakážeme zlomky, které obsahují ve svém jmenovateli mocniny 2, ve druhém zakážeme navíc i ty, které obsahují ve svém jmenovateli mocniny 3, v n-tém zakážeme navíc ty zlomky, které mají ve jmenovateli mocninu p_n, n-tého prvočísla. Tato klesající posloupnost se zřejmě nikdy nestabilizuje.

4. Tento okruh není artinovský, neboť pro libovolné prvočíslo $q \neq p$ obsahuje nekonečný klesající řetězec $\mathbb{Z}(\frac{1}{p}) \supset q \cdot \mathbb{Z}(\frac{1}{p}) \supset q^2 \cdot \mathbb{Z}(\frac{1}{p}) \supset \cdots$, který se nikdy nestabilizuje.
5. Snadno se uvidí, že jediné podmoduly (podgrupy) okruhu $R = \mathbb{Z}(\frac{1}{p})/\mathbb{Z}$ jsou generované $\frac{1}{p^k} + \mathbb{Z}$ pro $k \in \mathbb{Z}_{\geq 0}$. Vskutku, předpokládejme, že naše podgrupa obsahuje prvek s p^k jako největší mocninou ve jmenovateli v jeho zápise v bázi $1+\mathbb{Z}, \frac{1}{p}+\mathbb{Z}, \ldots$. Vhodným násobkem můžeme docílit toho, že koeficient u $\frac{1}{p^k}+\mathbb{Z}$ bude 1. Pak ovšem vynásobením p^{k-1} zjistíme, že naše podgrupa nutně obsahuje $\frac{1}{p} + \mathbb{Z}$, případným odečtením vhodného násobku $\frac{1}{p} + \mathbb{Z}$ a vynásobením našeho prvku p^{k-2} zjistíme, že naše podgrupa obsahuje $\frac{1}{p^2} + \mathbb{Z}$ a stejným způsobem tedy nutně obsahuje $\frac{1}{p^k} + \mathbb{Z}$. Jistě tedy libovolná podgrupa obsahuje buďto vše nebo je generovaná $\frac{1}{p^n} + \mathbb{Z}$ pro nějaké $n \in \mathbb{Z}_{\geq 0}$. Odtud má jistě každý vlastní podmodul modulu R pouze konečně mnoho vlastních podmodulů a tedy R je nutně artinovský.
6. Podmoduly jsou v tomto případě vektorové podprostory a protože platí, že dva do sebe vnořené podprostory stejné dimenze musí být stejné a vzhledem ke konečnosti V/k dostáváme, že V je artinovský modul nad k. ◇

Věta 10.5 (Ekvivalentní podmíky Noetherovskosti)**.** *Buď R okruh a buď dále M libovolný $R-$modul. Následující podmínky jsou ekvivalentní:*

(i) M je noetherovský, tedy splňuje (ACC),

(ii) každý podmodul $N \subset M$ je konečně generovaný,

(iii) každý neprázdný systém podmodulů M má maximální prvek (vůči inkluzi).

Tvrzení této věty jsou jednoduché, avšak velice mocné, je tedy vhodné zamyslet se nad jejím důkazem a ztotožnit se s myšlenkami, které se v přechodech mezi jednotlivými implikacemi používají, což je obsahem následujícího cvičení.

Cvičení 10.6. Dokažte předcházející větu:

Řešení. Dokážeme jednotlivé implikace.

$1 \to 2$ Sporem. Buď $N \subset M$ podmodul a induktivně konstruujte moduly $M_1 = \langle a_1 \rangle$, $a_1 \in N$, $M_2 = \langle a_1, a_2 \rangle$, $a_2 \in N - M_1$, obecně $M_n = \langle a_1, \ldots, a_{n-1}, a_n \rangle$, kde $a_n \in N - M_{n-1}$ a $\langle x, y \rangle$ je podmodul generovaný prvky x, y. Dále použijte noetherovskost pro moduly M_i.

$2 \to 1$ Uvažte nekonečnou rostoucí posloupnost podmodulů M_i modulu M. Co lze říci o sjednocení těchto podmodulů?

$1 \to 3$ Z předpokladu, že existuje neprázdný systém podmodulů bez maximálního prvku vybudujte nekonečnou rostoucí posloupnost podmodulů a odvoďte spor s noetherovskostí M. (Začněte s libovolným podmodulem z daného systému a zkoumejte jeho maximalitu.)

$3 \to 2$ Předpokládejte, že každý neprázdný systém podmodulů M má maximální prvek (vzhledem k inkluzi podmodulů) a pro daný podmodul N uvažte systém jeho konečně generovaných podmodulů.

$2 \to 3$ Nechť tedy M_j je neprázdný systém podmodulů. Buď M_1 libovolný modul tohoto systému, pokud je maximální, jsme hotovi, v opačném případě existuje modul $M_2 \supset M_1$. Pokud je M_2 maximální, jsme hotovi, jinak opět existuje modul $M_3 \supset M_2$. Takto

získáme posloupnost vnořených modulů $M_1 \subset M_2 \subset \cdots$ a uvažme sjednocení $\cup M_i = N$ (obecně není prvkem našeho systému). Avšak víme, že N je konečně generovaný modul, generovaný $a_1, \ldots, a_n \in M$. Pak ovšem existuje $k \in \mathbb{N}$ tak, že $a_1, \ldots, a_n \in M_k$ a tedy každý neprázdný rostoucí řetězec má horní závoru a z Zornova lemmatu dostáváme maximální prvek celého systému.

$3 \to 1$ Předpokládejte, že máte nekonečný rostoucí řetězec podmodulů $M_1 \subset M_2 \subset \cdots$. Pak jistě $M_1, M_2, \cdots$ je neprázdný systém podmodulů M a podle předpokladu tedy obsahuje maximální prvek, řekněme M_n. Avšak potom pro každé $i > n$ platí (z maximality) $M_i \subset M_n$, (z předpokladu o řetězci) $M_i \supset M_n$ a tedy $M_n = M_i$ a řetězec se stabilizoval. ◇

Podobně lze říci ekvivalentní podmínky pro artinovskost modulu:

Věta 10.7. *Buď R okruh a M buď $R-$modul. Pak následující jsou ekvivalentní:*

(i) M je artinovský, tedy splňuje (DCC),

(ii) každý neprázdný systém podmodulů modulu M obsahuje minimální prvek vůči inkluzi.

Toto tvrzení je opět jednoduché a znovu nám dává užitečný nástroj, jak s artinovskými moduly pracovat.

Cvičení 10.8. Dokažte předcházející větu.

Řešení. Ukažme každou implikaci zvlášť:

$2 \to 1$ Jistě každý klesající řetězec podmodulů $M_1 \supset M_2 \supset \ldots$ tvoří neprázdný systém podmodulů a tedy musí obsahovat minimální prvek M_k. Potom však pro všechny $i \in \mathbb{N}$, $i > k$ platí, že $M_i \supset M_k$ (minimalita M_k) a zároveň $M_k \supset M_i$ (z předpokladu o řetězci). Každý klesající řetězec podmodulů se tedy nutně stabilizuje.

$1 \to 2$ Opět použijeme Zornovo lemma: Uvažme tedy neprázdný systém podmodulů modulu M. Pak se jistě každý klesající řetězec nutně stabilizuje (vždyť M je artinovský), tedy každý klesající řetězec má dolní závoru. Odtud z Zornova lemmatu existuje minimální prvek celého systému. ◇

Důležitým poznatkem o noetherovských, popř. artinovských modulech je následující věta:

Věta 10.9 (O exaktní posloupnosti noetherovských, resp. artinovských modulů)**.** *Nechť R je okruh a M, M', M'' buďte $R-$moduly. Buď $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ krátká exaktní posloupnost modulů. Potom platí:*

(i) M je noetherovský, právě když M' i M'' jsou noetherovské,

(ii) M je artinovský, právě když M' i M'' jsou artinovské.

Tato věta nám umožňuje hledat nové noetherovské či artinovské moduly. Jednoduše odtud odvodíme následující vlastnosti:

Důsledek 10.10. *Nechť R je okruh a M buď libovolný $R-$modul. Pak platí:*

(i) Podmoduly noetherovských (artinovských) modulů jsou noetherovské (artinovské),

(ii) Kvocienty noetherovských (artinovských) modulů jsou noetherovské (artinovské),

(iii) Homomorfní obraz noetherovského (artinovského) modulu je noetherovský (artinovský),

(iv) *Přímý součet dvou noetherovských (artinovských) modulů je noetherovský (artinovský),*

(v) *Pro každé $n \in \mathbb{N}$, pokud M je noetherovský (artinovský), pak M^n je noetherovský (artinovský).*

Z věty o korespondenci dostáváme následující příklad.

Příklad 10.11. Buď R okruh a M libovolný R-modul. Pokud pro každý nenulový podmodul $N \subseteq M$ platí, že kvocient M/N je konečný, je R noetherovský.

Řešení. Z věty o korespondenci dostáváme, že podmoduly kvocientu M/N odpovídají přesně podmodulům M, které obsahují N. Protože je však tento kvocient konečný, N je obsaženo pouze v konečně mnoha podmodulech M a tedy M je nutně noetherovský. ◇

Věta 10.12 (Hilbertova věta o bázi)**.** *Pokud R je noetherovský, pak i okruh polynomů jedné proměnné $R[x]$ je noetherovský okruh.*

Důkaz této věty lze najít ve všech standardních učebnicích algebry či algebraické geometrie. My dokážeme upravené tvrzení. Jeho důkaz však bude pouze imitací klasického důkazu pro Hilbertovu větu o bázi.

Věta 10.13. *Pokud R je noetherovský, pak i okruh formálních mocninných řad jedné proměnné $R[[x]]$ je noetherovský okruh.*

Důkaz. V klasickém znění Hilbertovy věty o bázi se zabýváme členem největšího stupně, u mocninných řad žádný takovýto však neexistuje. Můžeme však uvážit nejmenší člen a jeho koeficient:

Řekneme, že řada $f = a_r x^r + a_{r+1}x^{r+1} + \ldots$, kde $r \in \mathbb{N}_0$, $a_i \in R$ pro $i \in \mathbb{Z}_{\geq 0}$, $i \geq r$, $a_r \neq 0$ má stupeň r, vedoucí člen $a_r x^r$ a vedoucí koeficient a_r.

Buď $I \subset R[[x]]$ vlastní ideál a ukažme, že je konečně generovaný. Konstruujme jeho bázi postupně. Vyberme $f_1 \in I$ nejmenšího stupně d_1. Označme jeho vedoucí koeficient a_1. V každém kroku potom k již vybraným řadám $f_1, \ldots, f_k$ stupňů $d_1, \ldots, d_k$ a vedoucích koeficientů $a_1, \ldots, a_k$ vyberme polynom $f_{k+1} \in I$ nejmenšího možného stupně d_{k+1} a s vedoucím koeficientem a_{k+1} splňující $(a_{k+1}) \nsubseteq (a_1, \ldots, a_k)$.

Jelikož $(a_1) \subset (a_1, a_2) \subset \ldots$, tento postup se zastaví, řekněme po n krocích. Ukažme, že potom $I = (f_1, \ldots, f_k)$. Jistě jsme takto vybrali bázi ideálu všech vedoucích koeficientů řad $f \in I$, která má navíc následující vlastnosti: $d_i \leq d_{i+1}$ pro každé $i \in 1, \ldots, n-1$ a navíc pro každou $f \in I$ stupně d s vedoucím koeficientem a existuje nejmenší k takové, že $a \in (a_1, \ldots, a_k)$ a $d \geq d_k$.

Vskutku, kdyby $d_2 < d_1$, měli bychom spor s volbou f_1. Pokud by bylo $d_i > d_{i+1}$ pro některé $i > 1$, dostali bychom spor s volbou d_i, neboť jistě $(a_{i+1}) \nsubseteq (a_1, \ldots, a_{i-1})$. Ze stejného důvodu pokud k je nejmenší takové, že $a \in (a_1, \ldots, a_k)$, pak jistě $d_k \leq d$, neboť jinak bychom v k-tém kroku vybrali řadu f, neboť a neleží v $a \in (a_1, \ldots, a_{k-1})$.

Pišme $a = \sum_{i=1}^{k} c_{i0} a_i$ a dodefinujme $g_0 = \sum_{i=1}^{k} c_{i0} x^{d-d_i} f_i$. Potom $g - g_0$ je stupně většího než d (vedoucí koeficienty se odečtou). Jistě $g_0 \in (f_1, \ldots, f_k) \subset (f_1, \ldots, f_n)$. Zopakováním stejném úvahy pro $g - g_0$ získáme řadu $g_1 \in (f_1, \ldots, f_n)$ stupně alespoň $d+1$.

Induktivně tedy získáme $g = \sum_{j=0}^{\infty} g_j = \sum_{j=0}^{\infty} \sum_{i=1}^{k} c_{ij} x^{d-d_i} f_i$. Protože však vnitřní suma je pouze konečná, můžeme zaměnit pořadí sumace a platí tedy, že $g = h_1 f_1 + \ldots h_n f_n$ pro nějaké $h_i \in R[[x]]$. □

Přímým důsledkem Hilbertovy věty o bázi je pak následující tvrzení:

Důsledek 10.14. *Je-li R noetherovský okruh, pak okruh polynomů konečně mnoha proměnných $R[x_1, \ldots, x_n]$ je noetherovský okruh.*

Důležitým důsledkem této věty (v kombinaci s předchozími tvrzeními o kvocientech) je následující cvičení. Buď R komutativní okruh. Připomeňme, že A je $R-$algebra (pro komutativní okruh R), pokud je to $R-$modul a máme na něm definováno bilineární zobrazení $\cdot : A \times A \to A$ tak, že $(A, \cdot, +)$ je okruh.

Cvičení 10.15 (Konečná generovanost)**.** Buď R noetherovský okruh a N, A buďte $R-$moduly.

1. (*moduly*) Pokud N je konečně generovaný jako $R-$modul, pak je N noetherovský modul.
2. (*algebry*) Pokud R je komutativní a A je konečně generovaný jako $R-$algebra, pak A je noetherovský okruh.

Řešení. Buď tedy R okruh a N, A buďte $R-$moduly.

1. (*moduly*) Konečná generovanost znamená, že existuje surjektivní zobrazení $R^n \to N$ pro nějaké $n \in \mathbb{N}$. Avšak konečný součin noetherovských modulů je noetherovský (z věty o exaktní posloupnosti noetherovských modulů). Protože kvocienty noetherovských jsou opět noetherovské, bude N nutně noetherovský.
2. (*algebry*) Jelikož konečně generovaný jako $R-$algebra znamená, že existuje surjektivní zobrazení $R[x_1, \ldots, x_n] \to A$ pro nějaké $n \in \mathbb{N}$. Avšak z Hilbertovy věty o bázi je okruh $R[x_1, \ldots, x_n]$ noetherovský a z uzavřenosti noetherovských modulů na kvocienty platí, že A je noetherovský okruh. ◇

Cvičení 10.16. Buď R obor integrity, který je noetherovský. Dokažte, že potom libovolný nenulový prvek, který není jednotka, lze napsat jako součin ireducibilních prvků.

Řešení. Buď $a \in R \setminus R^\times$ libovolný prvek, který není jednotka.

Ukažme napřed, že je dělitelný nějakým ireducibilním prvkem. Pokud je a ireducibilní, jsme hotovi. V opačném případě existují $b_1, c_1 \in R \setminus R^\times$, tak, že $a = b_1 \cdot c_1$. Pokud je alespoň jedno z b_1, c_1 ireducibilní, jsme hotovi. V opačném případě lze psát $c_1 = b_2 \cdot c_2$ pro nějaké $b_2, c_2 \in R \setminus R^\times$. Analogicky můžeme postupovat dále. Všimněme si, že $(a) \subset (c_1) \subset (c_2) \cdots$, protože R je noetherovský, musí se tento řetězec stabilizovat, což znamená, že $(c_n) = (c_{n+1})$ a c_n, c_{n+1} jsou asociované, což je spor. Tedy a je dělitelné ireducibilním prvkem.

Stejným způsobem ukažme, že a lze napsat jako součin ireducibilních prvků: pišme $a = p_1 \cdot b_1$, kde p_1 je ireducibilní. Pokud je b_1 ireducibilní, jsme hotovi. V opačném případě $b_1 = p_2 \cdot b_2$ a můžeme argument opakovat. Opět $(a) \subset (b_1) \subset (b_2) \subset \cdots$, z noetherovskosti dostáváme, že pro nějaké $n \in \mathbb{N}$ platí, že b_n je asociované s p_n je ireducibilní a tedy $a = p_1 \cdots p_n$ součin ireducibilních prvků. ◇

Cvičení 10.17. Buď R komutativní okruh ve kterém každý prvoideál je konečně generovaný. Ukažte, že R je noetherovský.

Řešení. Předpokládejme, že existují ideály v R, které nejsou konečně generované. Tvrzení dokážeme opět za předpokladu Zornova lemmatu. Uvažme systém všech ideálů, které nejsou konečně generované. Buď $\{I_i \mid i \in \mathbb{N}\}$ libovolný řetězec takových ideálů a uvažme sjednocení $I = \cup_{i \in \mathbb{N}} I_i$. Kdyby toto sjednocení bylo konečně generované, řekněme prvky $a_i, \ldots, a_n \in R$, existovalo by $k \in \mathbb{N}$ takové, že $a_1, \ldots, a_n \in I_k$ a tedy $I_k = I$, což je spor s tím, že I_i nejsou konečně generované. Tedy ani I není konečně generovaný ideál a tudíž v systému všech ideálů,

které nejsou konečně generované, má každý řetězec horní závoru. Dle Zornova lemmatu tedy dostáváme maximální prvek J tohoto systému.

Zbývá ukázat, že J je konečně generovaný. K tomu stačí ukázat množinu generátorů či ukázat, že J je prvoideál - pak bude konečně generovaný z předpokladu tvrzení. Buď $a, b \in R$ libovolně tak, že $ab \in J$ a předpokládejme, že a neleží v ideálu J.

Pak jistě $(J, a) \supset J$ ostře a tedy (J, a) je konečně generovaný. Uvažme dále podíl ideálů $J : (a) = \{x \in R : xa \in J\}$ (není těžké ověřit, že jde opět o ideál okruhu R). Protože zřejmě $J \subset J : (a)$, pokud dostaneme opět ostrou nerovnost, bude i $J : (a)$ konečně generovaný. Avšak jistě $b \in J : (a)$ (neboť $ab \in J$), pokud tedy $J = J : (a)$, dostáváme, že $b \in J$, J je prvoideál a jsme hotovi.

Předpokládejme tedy, že $J \subsetneq J : (a)$ a řekněme, že $x_1, \ldots, x_r$ generují $J : (a)$. Zvolme generátory $a, y_1, \ldots, y_s$ ideálu (J, a). Případným odečtením násobku a můžeme navíc předpokládat, že $y_1, \ldots, y_s$ leží v J (vždyť každý prvek (J, a) je tvaru $\alpha a + \beta j$, kde $\alpha, \beta \in R$ a $j \in J$).

Jelikož pro každé $x \in J$ platí $x \in (J, a)$, existují $c, c_1, \ldots c_s$ tak, že $x = ca + c_1 y_1 + \ldots + c_s y_s$, avšak potom $ca \in J$ a tedy $c \in J : (a)$ a lze psát $c = d_1 x_1 + \ldots d_r x_r$ pro nějaké $d_1, \ldots, d_r \in R$. Pak ovšem x lze psát jako $R-$lineární kombinaci prvků $ax_1, \ldots, ax_r, y_1, \ldots, y_s$ a J je konečně generovaný, což je spor. ◇

Na závěr uveďme několik doplňujících otázek, které by měly otestovat porozumění uvedeným termínům i ve spojitosti s předchozími kapitolami:

Cvičení 10.18. Zodpovězte následující otázky:

1. Jsou-li A, B $R-$moduly, A noetherovský, je modul $A \otimes_R B$ opět noetherovský?
2. Je-li každý vlastní podmodul A konečně generovaný, je A noetherovský modul?

Řešení. 1. Ne, např. pro každý A noetherovský a $A-$modul B, který není noetherovský, platí $A \otimes_A B \cong B$, což není noetherovský modul. Tedy stačí volit $A = \mathbb{Z}$ a $B = \mathbb{Q}$.

2. Nikoliv, viděli jsme příklad $\mathbb{Z}-$modulu $R = \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$, jehož každý vlastní podmodul je konečně generovaný, avšak sám modul konečně generovaný není. ◇