ОДАБРАНА ПОГЛАВЉА АЛГЕБРЕ И МАТЕМАТИЧКЕ ЛОГИКЕ

ПРЕДАВАЊА

ЗОРАН ПЕТРОВИЋ

АКАДЕМСКА 2024/25 ГОДИНА

1 Прстени

У овом одељку, материјал ће нам углавном бити познат из претходних алгебарских курсева, али биће и понешто ново, или другачије описано.

За почетак имамо дефиницију прстена са јединицом, која нам је позната.

Дефиниција 1. Прстен са јединицом је уређена четворка $(R, +, \cdot, 1_R)$ за коју важи следеће.

1. $(R, +)$ је Абелова група.
2. $(R, \cdot, 1_R)$ је моноид.
3. За све $a, b, c, d \in R$: $(a + b) \cdot (c + d) = a \cdot c + a \cdot d + b \cdot c + b \cdot d$.

Ако са 0_R означимо неутрал у Абеловој групи $(R, +)$, онда, стављајући $a = b = c = d = 0_R$ у горњем услову, добијамо једнакост:

$$(0_R + 0_R) \cdot (0_R + 0_R) = 0_R \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R.$$

Како је $0_R + 0_R = 0_R$, онда имамо једнакост

$$0_R \cdot 0_R = 0_R \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R, \tag{1}$$

из чега следи

$$0_R \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R = 0_R. \tag{2}$$

Уколико узмемо произвољно $a \in R$, а ставимо да је $b = c = d = 0_R$, имамо да је

$$(a + 0_R) \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R,$$

те је
$$a \cdot 0_R = a \cdot 0_R + a \cdot 0_R + 0_R \cdot 0_R + 0_R \cdot 0_R.$$
Додавањем на обе стране $0_R \cdot 0_R$, и коришћењем једнакости (2) добијамо
$$0_R \cdot 0_R = a \cdot 0_R,$$
за свако $a \in R$. Но, како је $(R, \cdot, 1_R)$ моноид, имамо да је
$$0_R = 1_R \cdot 0_R = 0_R \cdot 0_R = a \cdot 0_R,$$
за свако $a \in R$. Наравно, читаоци могу да потраже и краћи доказ ове познате им чињенице. Уколико је $1_R = 0_R$, добија се да је $R = \{0_R\}$. Такав прстен се назива нула прстен и ми га нећемо сматрати за прстен са јединицом. Стога увек претпостављамо да је $1_R \neq 0_R$.

За вежбу изведите и једнакости $a \cdot (-b) = -(a \cdot b)$ и $(-a) \cdot b = -(a \cdot b)$. Даље ћемо писати само 1, односно 0 ако се зна о ком прстену је реч. Прстен је комутативан уколико је таква операција множења. Уместо $a \cdot b$ писаћемо само ab. Генерално, за сваки прстен $(R, +, \cdot, 1_R)$ можемо посматрати и његов ОПОЗИТНИ прстен $(R^{\mathrm{op}}, +^{\mathrm{op}}, \cdot^{\mathrm{op}}, 1_{R^{\mathrm{op}}})$, где је $R^{\mathrm{op}} = R$, $+^{\mathrm{op}} = +$, $1_{R^{\mathrm{op}}} = 1_R$, док је, за све $a, b \in R$: $a \cdot^{\mathrm{op}} b = b \cdot a$. Уколико је R комутативан прстен, онда је то исти прстен.

Наведимо неке примере прстена.

Пример 2. Ако је A Абелова група, са $\mathrm{End}(A)$ означавамо скуп свих ендоморфизама ове групе, тј. скуп свих хомоморфизама $f\colon A \to A$. Тада је $(\mathrm{End}(A), +, \circ, \mathrm{id}_A)$ прстен са јединицом, при чему је множење операција композиције ендоморфизама, а збир ендоморфизама f и g дефинисан је са: за $a \in A$ је $(f+g)(a) := f(a) + g(a)$. Ако су $f, g, h, k \in \mathrm{End}(A)$ и $a \in A$, имамо да је
$$\begin{aligned} &((f+g) \circ (h+k))(a) = (f+g)((h+k)(a)) = (f+g)(h(a)+k(a)) \\ &= f(h(a)+k(a)) + g(h(a)+k(a)) = f(h(a)) + f(k(a)) + g(h(a)) + g(k(a)) \\ &= (f \circ h)(a) + (f \circ k)(a) + (g \circ h)(a) + (g \circ k)(a) = (f \circ h + f \circ k + g \circ h + g \circ k)(a), \end{aligned}$$
те је заиста $(f+g) \circ (h+k) = f \circ h + f \circ k + g \circ h + g \circ k$. Остала својства су јасна. ♣

Пример 3. Нека је R прстен са јединицом, а G група. ГРУПНИ ПРСТЕН $(RG, +, \cdot, 1_{RG})$ дефинишемо на следећи начин.
$$RG := \{r\colon G \to R : r(g) \neq 0 \text{ само за коначно много } g \in G\}.$$
Ако су $r, s \in RG$ и $g \in G$, онда је:
$$(r+s)(g) := r(g) + s(g), \quad (r \cdot s)(g) := \sum_{hk=g} r(h)s(k).$$

Погодније је, у овом случају, уместо $r(g)$ писати r_g. Тада имамо:

$$(r+s)_g := r_g + s_g, \quad (r \cdot s)_g := \sum_{hk=g} r_h s_k.$$

Јединица прстена RG је функција 1_{RG} задата са:

$$1_{RG}(g) = \begin{cases} 1_R, & g = e \\ 0_R, & g \neq e, \end{cases}$$

где је e неутрал групе G. Уобичајено је писати елемент r из RG у облику формалне суме $r = \sum_{g \in G} r_g g$, где $r_g \in R$, при чему је $r_g \neq 0$, само за коначно много $g \in G$ (уколико је G коначна група, овај услов је наравно непотребан). У овом запису сабирање и множење изгледа овако:

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g,$$

$$\begin{aligned}\Big(\sum_{g \in G} r_g g\Big) \cdot \Big(\sum_{g \in G} s_g g\Big) &= \Big(\sum_{h \in G} r_h h\Big) \cdot \Big(\sum_{k \in G} s_k k\Big) \\ &= \sum_{h,k \in G} r_h s_k hk = \sum_{g \in G} \Big(\sum_{\substack{h,k \in G \\ hk = g}} r_h s_k\Big) g.\end{aligned}$$

♣

Пример 4. Уколико је R прстен са јединицом, можемо посматрати и скуп $M_n(R)$, свих квадратних матрица над R реда $n \geqslant 1$ са уобичајеним операцијама сабирања и множења (није никакав проблем што прстен R није нужно комутативан). ♣

Подсетимо се да је ПРАВИ делитељ нуле у прстену R елемент $a \neq 0$ за који постоји $b \neq 0$ такав да је $a \cdot b = 0$. Комутативан прстен са јединицом је ДОМЕН, ако у њему нема правих делитеља нуле. Елемент $a \in R$ је инвертибилан, ако постоји $b \in R$ такав да је $a \cdot b = 1$. Скуп инвертибилних елемената прстена R означавамо са $U(R)$; ово је наравно група. Прстен са јединицом је ПРСТЕН СА ДЕЉЕЊЕМ (или ТЕЛО), ако је у њему сваки елемент различит од нуле инвертибилан. Комутативан прстен са дељењем је поље.

Дефиниција 5. Нека су $(R, +^R, \cdot^R, 1_R)$ и $(S, +^S, \cdot^S, 1_S)$ прстени са јединицом такви да је $S \subseteq R$, $1_R = 1_S$ и за све $s_1, s_2 \in S$ важи:

$$s_1 +^S s_2 = s_1 +^R s_2, \quad s_1 \cdot^S s_2 = s_1 \cdot^R s_2.$$

Тада за прстен S кажемо да је један потпрстен са јединицом прстена R.

Ни појам хомоморфизма нам није стран.

Дефиниција 6. Нека су $(R, +^R, \cdot^R, 1_R)$ и $(S, +^S, \cdot^S, 1_S)$ прстени са јединицом и $\phi\colon R \to S$. Тада је ϕ хомоморфизам прстена са јединицом уколико важи следеће.

1. $(\forall a, b \in R)\phi(a +^R b) = \phi(a) +^S \phi(b)$
2. $(\forall a, b \in R)\phi(a \cdot^R b) = \phi(a) \cdot^S \phi(b)$
3. $\phi(1_R) = 1_S$.

Уколико је ϕ бијекција, кажемо да је ϕ изоморфизам.

Наравно, често ћемо због једноставности сабирање и у R и у S означавати само са $+$; слично и за множење. Језгро хомоморфизма ϕ, у ознаци $\mathrm{Ker}\,\phi$ је скуп свих елемената из R који се са ϕ сликају у 0 у S. Приметимо да тада за сваки $x \in \mathrm{Ker}\,\phi$ и сваки $r \in R$ имамо да важи:

$$\phi(r \cdot x) = \phi(r) \cdot \phi(x) = \phi(r) \cdot 0 = 0, \quad \phi(x \cdot r) = \phi(x) \cdot \phi(r) = 0 \cdot \phi(r) = 0.$$

Такође, за све $x, y \in \mathrm{Ker}\,\phi$: $\phi(x + y) = \phi(x) + \phi(y) = 0 + 0 = 0$, па $x + y \in \mathrm{Ker}\,\phi$.

Дефиниција 7. Нека је $(R, +, \cdot, 1)$ прстен са јединицом и $(I, +) \leqslant (R, +)$, Тада је

- I леви идеал у прстену R уколико за све $r \in R$ и све $x \in I$: $r \cdot x \in I$;
- I десни идеал у прстену R уколико за све $r \in R$ и све $x \in I$: $x \cdot r \in I$;
- I двострани идеал у прстену R уколико је и и леви и десни идеал у R.

Дакле, $\mathrm{Ker}\,\phi$ је један двострани идеал за сваки хомоморфизам ϕ.

Када имамо двострани идеал I можемо формирати количнички прстен по том идеалу. Приметимо најпре да, ако су $r, s \in R$ и $x, y \in I$, онда имамо

$$(a + x) \cdot (b + y) - a \cdot b = a \cdot b + a \cdot y + x \cdot b + x \cdot y - a \cdot b = a \cdot y + x \cdot b + x \cdot y \in I,$$

јер је I двострани идеал.

Дефиниција 8. Нека је $(R, +, \cdot, 1)$ прстен са јединицом и I један двострани идеал у R. Ако је $R/I = \{a + I : a \in R\}$ леви косет простор Абелове групе $(R, +)$ по подгрупи I, онда можемо дефинисати и множење у R/I са:

$$(a + I) \cdot (b + I) = a \cdot b + I.$$

Горња анализа нам показује да је ово множење добро дефинисано. Тако добијамо прстен са јединицом $(R/I, +, \cdot, 1 + I)$.

Уколико је I само леви или само десни идеал, онда на овај начин не можемо добити прстен. Добијамо само одговарајући модул, али о томе ћемо причати касније.

Став 9. Нека је R прстен са јединицом. Скуп $I \subset R$ је двострани идеал акко постоји прстен са јединицом S и хомоморфизам $\phi\colon R \to S$, такав да је $I = \operatorname{Ker} \phi$. У овом случају, $\phi[R]$ је потпрстен са јединицом прстена S, који је изоморфан количничком прстену $R/\operatorname{Ker} \phi$.

Доказ. Уколико је I двострани идеал, за тражени прстен S можемо узети $S = R/I$, а за хомоморфизам ϕ, функцију $\phi\colon R \to R/I$ дефинисану са $\phi(a) := a+I$. Из саме дефиниције следи да је ϕ хомоморфизам. Осим тога, $\phi(a) = 0 + I$ акко $a + I = I$ акко $a \in I$, па је $I = \operatorname{Ker} \phi$.

Знамо да је језгро хомоморфизма двострани идеал и остало је само да докажемо тврђење садржано у последњој реченици. Имамо да је $1_S = \phi(1_R) \in \phi[R]$. Такође, за све $r_1, r_2 \in R$: $\phi(r_1) \cdot \phi(r_2) = \phi(r_1 \cdot r_2) \in \phi[R]$ и $\phi(r_1) + \phi(r_2) = \phi(r_1 + r_2) \in \phi[R]$, те је $\phi[R]$ заиста потпрстен од S.

Дефинишемо $\psi\colon R/\operatorname{Ker} \phi \to \phi[R]$ са: $\psi(a + \operatorname{Ker} \phi) := \phi(a)$. Најпре, ако је $a + \operatorname{Ker} \phi = b + \operatorname{Ker} \phi$ имамо да је $a - b \in \operatorname{Ker} \phi$, па је $\phi(a - b) = 0$, те је $\phi(a) = \phi(b)$ и функција ψ је добро дефинисана.

Ако су $a, b \in R$, онда имамо:

$$
\begin{aligned}
\psi((a + \operatorname{Ker} \phi) + (b + \operatorname{Ker} \phi)) &= \psi(a + b + \operatorname{Ker} \phi) = \phi(a + b) \\
&= \phi(a) + \phi(b) = \psi(a + \operatorname{Ker} \phi) + \psi(b + \operatorname{Ker} \phi), \\
\psi((a + \operatorname{Ker} \phi) \cdot (b + \operatorname{Ker} \phi)) &= \psi(a \cdot b + \operatorname{Ker} \phi) = \phi(a \cdot b) \\
&= \phi(a) \cdot \phi(b) = \psi(a + \operatorname{Ker} \phi) \cdot \psi(b + \operatorname{Ker} \phi),
\end{aligned}
$$

као и $\psi(1_R + \operatorname{Ker} \phi) = \phi(1_R) = 1_S$, те је ψ хомоморфизам.

Из саме дефиниције ψ видимо да је она „на”. Остаје само да се провери да је и „1–1”. Претпоставимо стога да је, за неке $a, b \in R$, $\psi(a + \operatorname{Ker} \phi) = \psi(b + \operatorname{Ker} \phi)$. То значи да је $\phi(a) = \phi(b)$, те $a - b \in \operatorname{Ker} \phi$ из чега следи да је $a + \operatorname{Ker} \phi = b + \operatorname{Ker} \phi$, што је и тражено. □

Следећи став се лако доказује.

Став 10. Пресек ма које фамилије идеала (левих, десних, или двостраних) је такође идеал.

Дефиниција 11. За идеал M (леви, десни, двострани) прстена R кажемо да је МАКСИМАЛАН, ако је $M \neq R$ и ако не постоји идеал I такав да је $M \subset I \subset R$.

Став 12. Сваки прстен садржи максималан идеал.

Доказ. Доказ се изводи помоћу Цорнове леме. Рецимо да радимо са двостраним идеалима. Подсетимо се да Цорнова лема каже да, ако имамо неки парцијално уређени скуп $(P, \leqslant)$ (у даљем ПОСЕТ) и ако у њему сваки ланац (подскуп у коме су свака два елемента упоредива) има горње ограничење (мајоранту), онда у скупу постоји максимални елемент.

Дакле, нека је R прстен и $\mathcal{I}$ скуп свих правих идеала (различитих од целог прстена) у овом прстену. Јасно је да је $\mathcal{I}$ посет у односу на релацију $\subseteq$. Нека је $\mathcal{L}$ ланац у $\mathcal{I}$. Покажимо да је

$$L = \bigcup_{I \in \mathcal{L}} I$$

идеал у R.

Најпре, ако су $x, y \in L$ имамо да $x \in I'$ и $y \in I''$ за неке $I', I'' \in \mathcal{L}$. Но, како је $\mathcal{L}$ ланац, важи да је $I' \subseteq I''$ или $I'' \subseteq I'$. У првом случају $x, y \in I''$, па и $x + y \in I''$, јер је I'' идеал, а у другом $x, y \in I'$, па и $x + y \in I'$, пошто је I' идеал. Добијамо да $x + y \in L$.

Уколико је $x \in L$, а $r \in R$, онда $x \in I$ за неко $I \in \mathcal{L}$, па и $r \cdot x$ и $x \cdot r$ припадају I, јер је I двострани идеал, те су оба елемента у L што нам завршава доказ да је L идеал.

Како је јасно да је $I \subseteq L$ за свако $I \in \mathcal{L}$, то је L горње ограничење за $\mathcal{L}$, те по Цорновој леми $\mathcal{I}$ има максимални елелемент, а то је баш максимални идеал. $\square$

Ако је R комутативан прстен, онда за идеал I (овде се наравно леви, десни и двострани идеали поклапају) кажемо да је ПРОСТ уколико за све $a, b \in R$ важи: ако $ab \in I$ онда $a \in I$, или $b \in I$.

Следећа теорема би требало да буде позната из претходних алгебарских курсева.

Теорема 13. Нека је R комутативни прстен.
а) Идеал I је максималан акко R/I је поље.
б) Идеал I је прост акко R/I је домен.
в) Сваки максималан идеал је прост.

Наведимо неке примере идеала.

Пример 14. У прстену са дељењем нема правих идеала.

Пример 15. Нека је R прстен са јединицом, $n \geqslant 2$ и $S = M_n(R)$. Означимо типичан елемент из S са $A = (a_{ij})$.
а) Ако је $1 \leqslant k \leqslant n$, онда је скуп свих $A \in S$ таквих да је $a_{ij} = 0$ за све $i \neq k$ један десни идеал у S.
б) Ако је $1 \leqslant k \leqslant n$, онда је скуп свих $A \in S$ таквих да је $a_{ij} = 0$ за све $j \neq k$ један леви идеал у S. $\clubsuit$

За крај овог одељка, укажимо на једну занимљиву везу између групног прстена над $\mathbb{Z}$ и инвертибилних елемената у прстену.

Теорема 16. За сваку групу G и прстен са јединицом R постоји природна бијекција $\Phi_{G,R}$ између $\mathrm{Hom}(\mathbb{Z}G, R)$, скупа свих хомоморфизама прстена $\mathbb{Z}G$ у прстен R и $\mathrm{Hom}(G, U(R))$, скупа свих хомоморфизама група G у групу $U(R)$.

Доказ. Нека је $f\colon \mathbb{Z}G \to R$ хомоморфизам прстена. Дефинишемо хомоморфизам група $\Phi_{G,R}(f)\colon G \to U(R)$ са: $\Phi_{G,R}(f)(g) := f(g)$. Наиме, сваки елемент групе G посматран као елемент групног прстена $\mathbb{Z}G$ је инвертибилан у том прстену – инверз му је g^{-1}, његов инверз у групи G [1]. $\Phi_{G,R}(f)$ јесте хомоморфизам група: $\Phi_{G,R}(f)(g_1g_2) = f(g_1g_2) = f(g_1)f(g_2)$(јер је f хомоморфизам прстена) $= \Phi_{G,R}(f)(g_1)\Phi_{G,R}(f)(g_2)$.

Да бисмо доказали да је $\Phi_{G,R}$ бијекција, најпогодније је наћи инверз $\Psi_{G,R}$. У ту сврху, нека је $h\colon G \to U(R)$ хомоморфизам група. Дефинишемо хомоморфизам прстена $\Psi_{G,R}(h)\colon \mathbb{Z}G \to R$ са:

$$\Psi_{G,R}(h)\Big(\sum_{g\in G} r_g g\Big) := \sum_{g\in G} r_g h(g).$$

Подсетимо се да су овде $r_g \in \mathbb{Z}$. Проверимо да је ово заиста хомоморфизам прстена.

$$\begin{aligned}\Psi_{G,R}(h)\Big(\sum_{g\in G} r_g g + \sum_{g\in G} s_g g\Big) &= \Psi_{G,R}(h)\Big(\sum_{g\in G}(r_g + s_g)g\Big) = \sum_{g\in G}(r_g + s_g)h(g)\\ &= \sum_{g\in G} r_g h(g) + \sum_{g\in G} s_g h(g) = \Psi_{G,R}(h)\Big(\sum_{g\in G} r_g g\Big) + \Psi_{G,R}(h)\Big(\sum_{g\in G} s_g g\Big).\end{aligned}$$

$$\begin{aligned}\Psi_{G,R}(h)\Big(\Big(\sum_{g\in G} r_g g\Big)\cdot\Big(\sum_{g\in G} s_g g\Big)\Big) &= \Psi_{G,R}(h)\Big(\sum_{g\in G}\Big(\sum_{\substack{t,u\in G\\ tu=g}} r_t s_u\Big)g\Big)\\ = \sum_{g\in G}\Big(\sum_{\substack{t,u\in G\\ tu=g}} r_t s_u\Big)h(g) &= \sum_{g\in G}\Big(\sum_{\substack{t,u\in G\\ tu=g}} r_t s_u h(g)\Big) = \sum_{g\in G}\Big(\sum_{\substack{t,u\in G\\ tu=g}} r_t s_u h(tu)\Big)\\ = \sum_{g\in G}\Big(\sum_{\substack{t,u\in G\\ tu=g}} r_t s_u h(t)h(u)\Big) &= \sum_{t,u\in G} r_t s_u h(t)h(u) = \Big(\sum_{t\in G} r_t h(t)\Big)\Big(\sum_{u\in G} s_u h(u)\Big)\\ = \Big(\sum_{g\in G} r_g h(g)\Big)\Big(\sum_{g\in G} s_g h(g)\Big) &= \Psi_{G,R}(h)\Big(\sum_{g\in G} r_g g\Big)\cdot\Psi_{G,R}(h)\Big(\sum_{g\in G} s_g g\Big).\end{aligned}$$

Наравно, $\Psi_{G,R}(h)(1e) = 1h(e) = 1_R$.

Проверимо још и да су $\Phi_{G,R}$ и $\Psi_{G,R}$ инверзи један другом. Нека је $h \in \mathrm{Hom}(G, U(R))$ хомоморфизам група.

$$\Phi_{G,R}(\underbrace{\Psi_{G,R}(h)}_{f})(g) = f(g) = \Psi_{G,R}(h)(g) = h(g).$$

Дакле, $\Phi_{G,R}(\Psi_{G,R}(h)) = h$, па је $\Phi_{G,R} \circ \Psi_{G,R} = \mathrm{id}_{\mathrm{Hom}(G,U(R))}$.

[1] $g \in G$ видимо као формалну „суму” $1g$ у $\mathbb{Z}G$ (као функцију из G у $\mathbb{Z}$ која g слика у 1, а остале елементе у 0 – видети дефиницију групног прстена) и његов инверз је „сума” $1g^{-1}$

На сличан начин, ако је $f \in \mathrm{Hom}(\mathbb{Z}G, R)$ имамо:

$$\begin{aligned}\Psi_{G,R}(\underbrace{\Phi_{G,R}(f)}_{h})\Big(\sum_{g\in G} r_g g\Big) &= \sum_{g\in G} r_g h(g)\\ &= \sum_{g\in G} r_g \Phi_{G,R}(f)(g) = \sum_{g\in G} r_g f(g) = f\Big(\sum_{g\in G} r_g g\Big),\end{aligned}$$

те је $\Psi_{G_R} \circ \Phi_{G,R} = \mathrm{id}_{\mathrm{Hom}(\mathbb{Z}G,R)}$.

О каквој се „природности” ради у формулацији ове теореме? Ево о чему је реч. Ако имамо и групу G' и прстен R', онда имамо и бијекцију $\Phi_{G',R'}$. Но, групе G и G', као и прстене R и R' можемо „повезати” хомоморфизмима $\varphi\colon G' \to G$ и $\theta\colon R \to R'$. Хомоморфизам група φ индукује хомоморфизам прстена $\mathbb{Z}\varphi\colon \mathbb{Z}G' \to \mathbb{Z}G$:

$$\mathbb{Z}\varphi\Big(\sum_{g'\in G'} r_{g'} g'\Big) := \sum_{g'\in G'} r_{g'} \varphi(g'),$$

а хомоморфизам θ сужењем индукује хомоморфизам $U(\theta)\colon U(R) \to U(R')$: $U(\theta)(r) := \theta(r)$.

Приметимо да, ако је G'' још једна група и $\psi\colon G'' \to G'$ хомоморфизам група, важи једнакост $\mathbb{Z}(\varphi \circ \psi) = \mathbb{Z}\varphi \circ \mathbb{Z}\psi$, као и $\mathbb{Z}_{\mathrm{id}_G} = \mathrm{id}_{\mathbb{Z}G}$. Дакле, придруживање $G \mapsto \mathbb{Z}G$ задаје један ФУНКТОР из категорије група у категорију прстена са јединицом. На сличан начин, ако је $\rho\colon R' \to R''$ хомоморфизам прстена, важи једнакост $U(\rho\circ\theta) = U(\rho)\circ U(\theta)$, као и $U(\mathrm{id}_R) = \mathrm{id}_{U(R)}$. Дакле, придруживање $\theta \mapsto U(\theta)$ задаје један функтор из категорије прстена са јединицом у категорију група.

Помоћу хомоморфизама φ и θ и ова два функтора, можемо задати пресликавања скупова $\mathrm{Hom}(\mathbb{Z}\varphi, \theta)\colon \mathrm{Hom}(\mathbb{Z}G, R) \to \mathrm{Hom}(\mathbb{Z}G', R')$ и $\mathrm{Hom}(\varphi, U(\theta))\colon \mathrm{Hom}(G, U(R)) \to \mathrm{Hom}(G', U(R'))$ са:

$$\mathrm{Hom}(\mathbb{Z}\varphi, \theta)(f) := \theta \circ f \circ \mathbb{Z}\varphi, \quad \mathrm{Hom}(\varphi, U(\theta))(h) := U(\theta) \circ h \circ \varphi.$$

Природност о којој је реч се односи на то да одговарајући дијаграм (нацртати га) комутира, тј. да је

$$\mathrm{Hom}(\varphi, U(\theta)) \circ \Phi_{G,R} = \Phi_{G',R'} \circ \mathrm{Hom}(\mathbb{Z}\varphi, \theta).$$

Уверимо се да је то тачно. У ту сврху, нека је $f \in \mathrm{Hom}(\mathbb{Z}G, R)$ и $g' \in G'$. Тада је

$$\begin{aligned}(\mathrm{Hom}(\varphi, U(\theta)) \circ \Phi_{G,R})(f)(g') &= \mathrm{Hom}(\varphi, U(\theta))(\Phi_{G,R}(f))(g')\\ &= (U(\theta) \circ \Phi_{G,R}(f) \circ \varphi)(g') = U(\theta)(\Phi_{G,R}(f)(\varphi(g')))\\ &= U(\theta)(f(\varphi(g'))) = \theta(f(\varphi(g'))) = (\theta \circ f \circ \varphi)(g'),\end{aligned}$$

те је $(\mathrm{Hom}(\varphi, U(\theta)) \circ \Phi_{G,R})(f) = \theta \circ f \circ \varphi$.

С друге стране, имамо да је

$$\begin{aligned}(\Phi_{G',R'} \circ \mathrm{Hom}(\mathbb{Z}\varphi, \theta))(f)(g') &= \Phi_{G',R'}(\mathrm{Hom}(\mathbb{Z}\varphi, \theta)(f))(g') \\ &= \Phi_{G',R'}(\theta \circ f \circ \varphi)(g') = (\theta \circ f \circ \varphi)(g'),\end{aligned}$$

те је $(\Phi_{G',R'} \circ \mathrm{Hom}(\mathbb{Z}\varphi, \theta))(f) = \theta \circ f \circ \varphi$. Дакле, тражена једнакост заиста важи и тиме је цео доказ завршен. $\square$

Чињеница да постоји природна (у наведеном смислу) бијекција између скупова $\mathrm{Hom}(\mathbb{Z}G, R)$ и $\mathrm{Hom}(G, U(R))$ се кратко изражава речима да је функтор $G \mapsto \mathbb{Z}G$ лево адјунгован функтору $R \mapsto U(R)$, но ту терминологију ћемо објаснити у наредним лекцијама. Само напоменимо овде да терминологија долази од појма адјунгованог оператора: ако је A оператор на одговарајућем векторском простору и v, w вектори из тог простора, онда имамо једнакост: $\langle Av, w\rangle = \langle v, A^*w\rangle$ скаларних производа.

2 Модули

Почнимо дефиницијом модула над прстеном са јединицом.

Дефиниција 17. Нека је R прстен са јединицом. Леви R-модул је уређени пар (A, ρ),где је A Абелова група, а $\rho\colon R \to \mathrm{End}(A)$. Десни R-модул је леви R^{op}-модул.

Наравно, ако је прстен R комутативан, не разликујемо леве и десне R-модуле и можемо их кратко звати R-модулима.

Како је, за сваки $r \in R$, слика $\rho(r)$ један ендоморфизам Абелове групе A, то за све $a, b \in A$ важи:

$$\rho(r)(a + b) = \rho(a) + \rho(b) \tag{3}$$

Такође, како је ρ хомоморфизам прстена са јединицом R у прстен са јединицом $\mathrm{End}(A)$, то је за све $r, s \in R$ испуњено: $\rho(r + s) = \rho(r) + \rho(s)$. Имајући у виду како је задата операција сабирања у прстену $\mathrm{End}(A)$ имамо да за све $a \in A$ важи:

$$\rho(r + s)(a) = \rho(r)(a) + \rho(s)(a). \tag{4}$$

Када посматрамо операцију множења, имамо да је за све $r, s \in R$ испуњено $\rho(r \cdot s) = \rho(r) \circ \rho(s)$, те за све $a \in A$ важи:

$$\rho(r \cdot s)(a) = \rho(r)(\rho(s)(a)). \tag{5}$$

Осим тога је $\rho(1_R) = \mathrm{id}_A$, тј. за све $a \in A$:

$$\rho(1_R)(a) = a. \tag{6}$$

Ако уместо $\rho(r)(a)$ пишемо $r \bullet a$, онда једнакости (3)–(6) можемо написати на следећи начин.

M1. За све $r \in R$, $a, b \in A$: $r \bullet (a+b) = r \bullet a + r \bullet b$.

M2. За све $r, s \in R$, $a \in A$: $(r+s) \bullet a = r \bullet a + s \bullet a$.

M3. За све $r, s \in R$, $a \in A$: $(r \cdot s) \bullet a = r \bullet (s \bullet a)$.

M4. За све $a \in A$: $1_R \bullet a = a$.

У случају десног R-модула (у даљем ћемо кратко говорити о левом и десном R-модулу подразумевајући да имамо „множење” елементима из R), имамо да је $\rho(r \cdot^{\mathrm{op}} s)(a) = (\rho(r) \circ \rho(s))(a)$, односно $\rho(s \cdot r)(a) = \rho(r)(\rho(s)(a))$. Стога је овде природно уместо $\rho(r)(a)$ писати $a \bullet r$, те имамо одговарајућу једнакост: $(a \bullet (s \cdot r)) = (a \bullet s) \bullet r$. Видимо и зашто причамо о ЛЕВОМ и ДЕСНОМ модулу. Ако се A састоји само из једног елемента, дакле ако је $A = \{0_A\}$, онда се A може видети као модул над било којим прстеном и кажемо да је то ТРИВИЈАЛНИ МОДУЛ.

Наведимо неколико (нетривијалних) примера.

Пример 18. Најпре, свака Абелова група A је један $\mathbb{Z}$-модул: за $m \in \mathbb{Z}$ и $a \in A$ је $m \bullet a := ma$. ♣

Пример 19. Ако је K поље, онда K-модул није ништа друго до векторски простор над пољем K. ♣

Пример 20. Ако је R прстен са јединицом онда је сваки леви (десни) идеал I један леви (десни) R-модул: $r \bullet a := r \cdot a$ ($a \bullet r = a \cdot r$). Посебно је и R и леви и десни R-модул. ♣

Пример 21. Ако R прстен са јединицом, а G група, онда R постаје леви RG-модул са: $(\sum_g r_g g) \bullet s := \sum_g r_g s$. На аналогни начин је R један десни R-модул. ♣

Пример 22. Нека је R прстен. Тада је $M_n(R)$ леви R-модул: $r \bullet (a_{ij}) := (r \cdot a_{ij})$. Такође је R^n један леви $M_n(R)-$ модул: $(a_{ij}) \bullet (r_j) := (\sum_{j=1}^n a_{ij} \cdot r_j)$.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \bullet \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} := \begin{pmatrix} a_{11} \cdot r_1 + a_{12} \cdot r_2 + \cdots + a_{1n} \cdot r_n \\ a_{21} \cdot r_1 + a_{22} \cdot r_2 + \cdots + a_{2n} \cdot r_n \\ \vdots \\ a_{n1} \cdot r_1 + a_{n2} \cdot r_2 + \cdots + a_{nn} \cdot r_n \end{pmatrix}.$$

♣

Да бисмо имали категорију, потребни су нам и одговарајући морфизми.

Дефиниција 23. Нека су A и B леви R-модули. Тада је функција $\phi\colon A \to B$ један ХОМОМОРФИЗАМ ЛЕВИХ R-МОДУЛА уколико важи следеће:

1. За све $a_1, a_2 \in A$: $\phi(a_1 + a_2) = \phi(a_1) + \phi(a_2)$;

2. за све $r \in R$ и $a \in A$: $\phi(r \bullet a) = r \bullet \phi(a)$.

Ако су A и B леви R-модули, означимо са $\mathrm{Hom}_R(A, B)$ скуп свих хомоморфизама левих модула. Ово је Абелова група у односу на операцију $+$ задату са: $(\phi+\psi)(a) := \phi(a)+\psi(a)$. Проверимо горња својства.

$$\begin{aligned}(\phi+\psi)(a_1+a_2) &= \phi(a_1+a_2)+\psi(a_1+a_2) = \phi(a_1)+\phi(a_2)+\psi(a_1)+\psi(a_2)\\ &= (\phi(a_1)+\psi(a_1))+(\phi(a_2)+\psi(a_2)) = (\phi+\psi)(a_1)+(\phi+\psi)(a_2).\end{aligned}$$

$$\begin{aligned}(\phi+\psi)(r \bullet a) &= \phi(r \bullet a)+\psi(r \bullet a) = r \bullet \phi(a) + r \bullet \psi(a)\\ &= r \bullet (\phi(a)+\psi(a)) = r \bullet ((\phi+\psi)(a)).\end{aligned}$$

Ако са $\mathrm{Hom}(A, B)$ означимо скуп свих хомоморфизама Абелових група (а овај скуп јесте сам по себи Абелова група у односу на горезадату операцију сабирања), пошто је сваки хомоморфизам левих модула уједно и хомоморфизам одговарајућих Абелових група, можемо да констатујемо да је $\mathrm{Hom}_R(A, B) \subseteq \mathrm{Hom}(A, B)$. Но, важи и више, $\mathrm{Hom}_R(A, B) \leqslant \mathrm{Hom}(A, B)$. Да бисмо доказали да је подгрупа, приметимо најпре да је $\mathrm{Hom}_R(A, B) \neq \emptyset$, јер нула хомоморфизам 0 ($0(a) = 0_B$ за све $a \in A$) јесте хомоморфизам R-модула. Ако $\phi, \psi \in \mathrm{Hom}_R(A, B)$, онда је

$$\begin{aligned}(\phi-\psi)(r \bullet a) &= \phi(r \bullet a) - \psi(r \bullet a)\\ &= r \bullet \phi(a) - r \bullet \psi(a) = r \bullet (\phi(a)-\psi(a)) = r \bullet (\phi-\psi)(a).\end{aligned}$$

Стога и $\phi - \psi \in \mathrm{Hom}_R(A, B)$, па је $\mathrm{Hom}_R(A, B)$ заиста подгрупа групе $\mathrm{Hom}(A, B)$. Приметимо да је $\mathrm{Hom}_{\mathbb{Z}}(A, B) = \mathrm{Hom}(A, B)$.

За два модула A и B кажемо да су изоморфни ако постоји хомоморфизам $\phi \colon A \to B$ који је бијекција.

Категорију левих R-модула и хомоморфизама левих R-модула ћемо означити са ${}_R\mathfrak{M}$, а категорију десних R-модула и хомоморфизама десних R-модула са $\mathfrak{M}_R$. Ако је A један леви R-модул, то ћемо кратко писати овако: $A \in_R \mathfrak{M}$, а ако је $\phi \colon A \to B$, хомоморфизам левих R-модула, кратко ћемо рећи да је ϕ у ${}_R\mathfrak{M}$.

Дефиниција 24. Уколико је R прстен са јединицом, $A \in_R \mathfrak{M}$, $A' \subseteq A$, тада је A' ПОДМОДУЛ од A уколико је A' подгрупа од A и за сваки $a' \in A'$, $r \in R$ је $r \bullet a' \in A'$.

Ако је A' подмодул од A то ћемо означавати са $A' \leqslant A$. Пошто је A' и подгрупа Абелове групе A, можемо дефинисати количничку подгрупу A/A' но на њој можемо задати и структуру левог R-модула са: $r \bullet (a + A') := r \bullet a + A'$. Читаоцима остављамо да провере да је ова операција добро дефинисана и да заиста добијамо један леви R-модул. Он се назива КОЛИЧНИЧКИ МОДУЛ. Важи следећа теорема.

Теорема 25. Нека је $\phi\colon A \to B$ у ${}_R\mathfrak{M}$. Тада важи следеће.

1. $\operatorname{Ker}\phi := \{a \in A : \phi(a) = 0_B\} \leqslant A$;

2. $\operatorname{Im}\phi = \phi[A] \leqslant B$;

3. $A/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$.

Доказ. 1. Знамо да је $\operatorname{Ker}\phi$ подгрупа од A. Ако је $a \in \operatorname{Ker}\phi$ и $r \in R$, онда је $\phi(r \bullet a) = r \bullet \phi(a) = r \bullet 0_B = 0_B$, па је $\operatorname{Ker}\phi$ заиста подмодул од A.

2. Знамо да је $\operatorname{Im}\phi$ подгрупа од B. Уколико је $\phi(a) \in \operatorname{Im}\phi$ и $r \in R$ имамо да је $r \bullet \phi(a) = \phi(r \bullet a) \in \operatorname{Im}\phi$.

3. Дефинишемо $\psi\colon A/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ са: $\psi(a + \operatorname{Ker}\phi) := \phi(a)$. Из теорије група знамо да је ово добро дефинисана функција и да је изоморфизам група. Остаје само да проверимо да је модулски хомоморфизам:

$$\psi(r \bullet (a + \operatorname{Ker}\phi)) = \psi(r \bullet a + \operatorname{Ker}\phi) = \phi(r \bullet a) = r \bullet \phi(a) = r \bullet \psi(a + \operatorname{Ker}\phi).$$

Дакле, ψ је изоморфизам и доказ је завршен. □

Наравно, за $\operatorname{Ker}\phi$ кажемо да је језгро хомоморфизма ϕ, а за $\operatorname{Im}\phi$ да је слика тог хомоморфизма. Корисно је уочити да је $\operatorname{Ker}\phi = \phi^{-1}[\{0\}]$. Приметимо да можемо формирати и количнички модул $B/\operatorname{Im}\phi$ и њега означавамо са $\operatorname{Coker}\phi$ и то је којезгро хомоморфизма ϕ. Из теорије група знамо да је дати хомоморфизам „1–1” ако и само ако му је језгро тривијалан модул, док је таутолошка чињеница да је хомоморфизам „на” ако и само ако му је којезгро тривијалан модул.

Уколико је $A_1, A_2 \leqslant A$, онда можемо формирати суму модула A_1 и A_2: $A_1 + A_2 := \{a_1 + a_2 : a_1 \in A_1, a_2 \in A_2\}$ и то је такође подмодул од A. Наравно, и пресек подмодула је подмодул. Следећа теорема се лако изводи из претходно доказане теореме.

Теорема 26. 1. За $A_1, A_2 \leqslant A$ важи: $(A_1 + A_2)/A_1 \cong A_2/A_1 \cap A_2$.
2. Ако је $A'' \leqslant A' \leqslant A$, онда: $(A/A'')\big/(A'/A'') \cong A/A'$.

Доказ. 1. Дефинишемо $\phi\colon A_2 \to (A_1+A_2)/A_1$ са: $\phi(x) = x + A_1$. Уколико је $a_1 + a_2 \in A_1 + A_2$ произвољан елемент, онда је $(a_1+a_2)+A_1 = a_2 + A_1 = \phi(a_2)$, па је ϕ „на”. За $x \in A_2$ имамо да је $x \in \operatorname{Ker}\phi$ акко је $x + A_1 = A_1$ што је еквивалентно са $x \in A_1$. Дакле, $\operatorname{Ker}\phi = A_1 \cap A_2$ и резултат следи из теореме 25.

2. Дефинишемо $\phi\colon A \to (A/A'')\big/(A'/A'')$ са: $\phi(a) := (a + A'') + A'/A''$. Наравно, овде би ипак требало проверити да ли је $A'/A'' \leqslant A/A''$. Но, то лако следи из $A' \leqslant A$ (уверите се у ово). Јасно је да је ϕ „на”.

Приметимо да

$$\begin{aligned} a \in \operatorname{Ker}\phi \text{ акко } & (a + A'') + A'/A'' = A'/A'' \\ \text{акко } & a + A'' \in A'/A'' \\ \text{акко } & a + A'' = a_1 + A'' \text{ за неко } a_1 \in A' \\ \text{акко } & a - a_1 \in A'' \text{ за неко } a_1 \in A' \\ \text{акко } & a - a_1 = a_2 \text{ за неко } a_1 \in A' \text{ и неко } a_2 \in A'' \\ \text{акко } & a = a_1 + a_2 \text{ за неко } a_1 \in A' \text{ и неко } a_2 \in A''. \end{aligned}$$

Но, како је $A'' \subseteq A'$, добијамо да је последњи услов еквивалентан са $a \in A'$ (уверите се у ово), па је $\operatorname{Ker}\phi = A'$. □

Наравно, доказ под 2. смо могли извести и на стандардан начин, како смо радили у ранијим курсевима, али није лоше нешто и другачије урадити. ☺

Сада ћемо се на кратко посветити неким појмовима из теорије категорија. Могли бисмо и без тога, али ипак је корисније то урадити на овај начин. Као што знамо (рецимо из једног од курсева топологије), свака категорија $\mathcal{C}$ састоји се од КЛАСЕ објеката $O(\mathcal{C})$ и класе стрелица (или морфизама) $A(\mathcal{C})$.

⌈ Овде истичемо да користимо појам класе и то не само ради лепшег изражавања. Као што математику можемо засновати на аксиомама ZFC (Цермело–Френкел уз аксиому избора), тако постоји и аксиоматизација NBG (фон Нојман–Бернајс–Гедел) у којој се појављују, осим скупова и класе. Класа може бити подскуп друге класе, а ако је класа ЕЛЕМЕНТ неке друге класе, онда је она СКУП. Дакле, скупови су елементи неких класа. Ми знамо да не постоји скуп свих скупова, али постојаће УНИВЕРЗАЛНА класа која се састоји од свих скупова. Како ми желимо да разматрамо и категорију скупова, у којима су објекти сви скупови, а стрелице сва пресликавања међу њима, потребан нам је шири појам од скупа. Уколико у некој категорији објекти чине скуп за ту категорију кажемо да је МАЛА КАТЕГОРИЈА. ⌋

За свака два објекта A, B имамо СКУП стрелица из A у B, који се означава са $\mathcal{C}(A,B)$. Претпостављамо да је $\mathcal{C}(A,B) \cap \mathcal{C}(A',B') = \emptyset$ уколико је $(A,B) \neq (A',B')$. За сваки објекат A постоји и стрелица $1_A \in \mathcal{C}(A,A)$. Имамо и операцију композиција стрелица

$$\mathcal{C}(A,B) \times \mathcal{C}(B,C) \to \mathcal{C}(A,C), \quad (f,g) \mapsto g \circ f,$$

за коју важи:

$$(h \circ g) \circ f = h \circ (g \circ f), \text{ за } (f,g,h) \in \mathcal{C}(A,B) \times \mathcal{C}(B,C) \times \mathcal{C}(C,D)$$

и

$$1_B \circ f = f = f \circ 1_A, \text{ за } f \in \mathcal{C}(A,B).$$

Објекти свакако јесу скупови, али стрелице нису нужно функције. На пример, сваки посет P се природно може видети као (мала) категорија $\mathcal{P}$. Имамо да је $O(\mathcal{P}) = P$, док је за свака два $A, B \in P$:

$$\mathcal{C}(A,B) = \begin{cases} \{(A,B)\}, & \text{ако је } A \leqslant_P B, \\ \emptyset, & \text{иначе .} \end{cases}$$

Поента је да буде тачно један елемент у $\mathcal{C}(A,B)$ акко је $A \leqslant_P B$, не мора то бити баш овај који смо навели. Без обзира на чињеницу да стрелице не морају бити функције, ако је $f \in \mathcal{C}(A,B)$ пишемо то кратко: $f\colon A \to B$. Просто је то погодно тако писати.

Категорију која има тачно један елемент називамо моноид (а ако је то мала категорија, онда се заиста поклапа са појмом моноида који знамо), категорију у којој је свака стрелица изоморфизам (стрелица $f \in \mathcal{C}(A,B)$ је изоморфизам, уколико постоји стрелица $g \in \mathcal{C}(B,A)$ таква да је $g \circ f = 1_A$ и $f \circ g = 1_B$), називамо групоид, а категорију која је и моноид и групоид називамо група (ако је мала категорија у питању, то је заиста група у добро нам познатом смислу).

Ово што нам је сада важно је да уведемо појам производа и копроизвода у категорији.

Дефиниција 27. Нека је $\mathcal{C}$ нека категорија и A_i, за $i \in I$ фамилија објеката у $\mathcal{C}$.

1. Производ ових објеката, ако постоји, чине објекат P и стрелице $p_i\colon P \to A_i$ тако да је испуњено следеће. За сваки објекат X из $\mathcal{C}$ и стрелице $f_i\colon X \to A_i$ постоји тачно једна стрелица $f\colon X \to P$ тако да је $p_i \circ f = f_i$ за све $i \in I$.

2. Копроизвод ових објеката, ако постоји, чине објекат S и стрелице $q_i\colon A_i \to S$ тако да је испуњено следеће. За сваки објекат X из $\mathcal{C}$ и стрелице $f_i\colon A_i \to X$ постоји тачно једна стрелица $f\colon S \to X$ тако да је $f \circ q_i = f_i$ за све $i \in I$.

Писаћемо $(P; (p_i)_{i\in I})$ за производ и $(S; (q_i)_{i\in I})$ за копроизвод. Ни производ ни копроизвод неких објеката не мора постојати у датој категорији, али ако неки од њих постоји, он је јединствено одређен до на изоморфизам. Наиме, претпоставимо да и P', заједно са $p_i'\colon P' \to A_i$ задовољава услове из дефиниције производа. Тада постоји тачно једна стрелица $f\colon P' \to P$ таква да је $p_i \circ f = p_i'$ за све $i \in I$, као и тачно једна стрелица $g\colon P \to P'$ таква да је $p_i' \circ g = p_i$ за све $i \in I$. Тада добијамо да је $p_i' \circ (g \circ f) = p_i'$ за све $i \in I$. Но, тај услов испуњава и $\mathrm{id}_{P'}$. Због јединствености добијамо да мора бити $g \circ f = \mathrm{id}_{P'}$. На сличан начин добијамо да је и $f \circ g = \mathrm{id}_P$, па су f и g изоморфизми.

Пример 28. Нека је $\mathcal{C} = Set$, тј. категорија свих скупова и функција између њих. Није тешко проверити да производ објеката A_i, $i \in I$, у овој категорији, чини Декартов производ скупова $P = \prod_{i\in I} A_i$ заједно са пројекцијама $p_i \colon P \to A_i$ $(p_i(a_s)_{s\in I} = a_i)$.

Копроизвод чини дисјунктна унија ових скупова, тј. $S = \bigcup_{i\in I}(A_i \times \{i\})$, уз функције $q_i \colon A_i \to S$ задате са: $q_i(a) = (a, i)$ за $a \in A_i$. Уверите се да је ово заиста копроизвод у категорији скупова.

Вратимо се сада на категорију ${}_R\mathfrak{M}$.

Теорема 29. За сваки комутативан прстен R и фамилију левих R-модула A_i у категорији ${}_R\mathfrak{M}$ постоји и производ и копроизвод.

Доказ. Производ није тешко конструисати. Заправо, то је директан производ модула A_i: $P = \prod_{i\in I} A_i$, са операцијама задатим по координатама: $(a_i)_{i\in I} + (b_i)_{i\in I} := (a_i + b_i)_{i\in I}$, $r \bullet (a_i)_{i\in I} := (r \bullet a_i)_{i\in I}$, док су $p_i \colon P \to A_i$ пројекције. Уверимо се да је ово производ. У ту сврху, нека је X један леви R-модул и $f_i \colon X \to A_i$ хомоморфизми модула. Дефинишемо $f \colon X \to \prod_{i\in I} A_i$ са: $f(x) := (f_i(x))_{i\in I}$, за $x \in X$. Ово јесте хомоморфизам левих R-модула: $f(x+y) = (f_i(x+y))_{i\in I} = (f_i(x)+f_i(y))_{i\in I}$ (јер су f_i хомоморфизми) $= (f_i(x))_{i\in I} + (f_i(y))_{i\in I} = f(x) + f(y)$. Такође, $f(r \bullet x) = (f_i(r \bullet x))_{i\in I} = (r \bullet f_i(x))_{i\in I} = r \bullet (f_i(x))_{i\in I} = r \bullet f(x)$. Имамо и да је $(p_j \circ f)(x) = p_j(f(x)) = p_j(f_i(x))_{i\in I} = f_j(x)$ за све $j \in I$. Из овог последњег добијамо и да је f јединствено одређено.

Доказ егзистенције копроизвода је нешто сложенији. Нека је

$$S := \{(a_i) \in \prod_{i\in I} A_i : a_i \neq 0, \text{ само за коначно много } i \in I\}.$$

Јасно је да је ово леви R-модул (који је заправо подмодул од P). Дефинишемо $q_i \colon A_i \to S$ са:

$$(q_i(a))_j = \begin{cases} a, & \text{ако је } j = i \\ 0, & \text{иначе,} \end{cases}$$

за $a \in A_i$. Дакле, на i-ту координату смо поставили елементе из A_i а све остале координате су једнаке 0. Ако је X један леви R-модул и $f_i \colon A_i \to X$, онда можемо дефинисати $f \colon S \to X$ са: $f((a_i)_{i\in I}) := \sum_{i\in I} f_i(a_i)$. Ова сума је заправо коначна, јер је, за сваки $(a_i)_{i\in I} \in S$ само коначно много координата различито од нуле. Јасно је да је за свако $i \in I$: $(f \circ q_i)(a)) = f(q_i(a)) = \sum_{j\in I} f_j(q_i(a))_j = f_i(a)$ (пошто су остале координате једнаке нули). Појаснимо зашто имамо јединственост тог f. Нека је $F \colon S \to X$ ма који хомоморфизам за који важи $F \circ q_i = f_i$ за све $i \in I$. Уколико је $s \in S$, онда је $s_i \neq 0$ само за коначно много индекса i. Нека су то индекси $i_1, \ldots, i_n$. Посматрајмо елементе $a[1], \ldots, a[n] \in S$ задате са:

$$a[k]_i = \begin{cases} s_{i_k}, & \text{за } i = i_k, \\ 0, & \text{иначе }, \end{cases}$$

за $k \in \{1, \dots, n\}$. Видимо две ствари. Најпре, $a[k] = q_{i_k}(s_{i_k})$ за $k \in \{1, \dots, n\}$. А такође је $s = a[1] + \cdots + a[n]$. Стога имамо да је

$$\begin{aligned} F(s) &= F(a[1]) + \cdots + F(a[n]) = F(q_{i_1}(s_{i_1})) + \cdots + F(q_{i_n}(s_{i_n})) \\ &= (F \circ q_{i_1})(s_{i_1}) + \cdots + (F \circ q_{i_n})(s_{i_n}) = f_{i_1}(s_{i_1}) + \cdots + f_{i_n}(s_{i_n}) = f(s). \qquad \square \end{aligned}$$

За копроизвод S модула A_i користимо ознаку $\bigoplus_{i \in I} A_i$ и називамо га и ДИРЕКТНОМ СУМОМ модула A_i. У случају два модула користимо ознаку $A \oplus B$. Аналогно за n модула користимо запис $A_1 \oplus A_2 \oplus \cdots \oplus A_n$. Приметимо да у случају коначног скупа индекса за објекат који се појављује у дефиницији копроизвода добијамо исти као и у случају производа, но морфизми који чине структуру су, наравно, другачији.

Посматрајмо низ левих R-модула и хомоморфизама:

$$A' \xrightarrow{\alpha} A \xrightarrow{\beta} A''.$$

За овај низ кажемо да је тачан у A уколико је $\operatorname{Im} \alpha = \operatorname{Ker} \beta$. Приметимо да, ако је $\alpha = 0$, тј. хомоморфизам који све елементе из A' слика у 0_A, онда је горњи низ тачан у A акко је β „1–1". Слично, ако је $\beta = 0$, онда је низ тачан у A акко је α „на". Стога је низ

$$0 \to A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 0,$$

где смо са 0 означавили тривијалан R-модул, тачан у свим нетривијалним модулима уколико је α „1–1", $\operatorname{Im} \alpha = \operatorname{Ker} \beta$ и β је „на". Овакав низ зовемо и КРАТАК ТАЧАН НИЗ.

Следећа опсервација је понекад корисна. Претпоставимо да је низ

$$A' \xrightarrow{\alpha} A \xrightarrow{\beta} A''$$

тачан у A и нека је $\theta\colon A \to B$ изоморизам. Тада је низ

$$A \xrightarrow{\theta \circ \alpha} B \xrightarrow{\beta \circ \theta^{-1}} A''$$

тачан у B. Наиме,

$$\operatorname{Ker}(\beta \circ \theta^{-1}) = (\beta \circ \theta^{-1})^{-1}[\{0\}] = \theta[\beta^{-1}[\{0\}]] = \theta[\operatorname{Ker} \beta] = \theta[\operatorname{Im} \alpha] = \operatorname{Im}(\theta \circ \alpha).$$

Приметимо да сваки хомоморфизам $\phi\colon A \to B$ „производи" тачан низ

$$0 \to \operatorname{Ker} \phi \xrightarrow{\iota} A \xrightarrow{\phi} B \xrightarrow{\pi} \operatorname{Coker} \phi \to 0,$$

где је ι УКЉУЧЕЊЕ (инклузија) $\operatorname{Ker} \phi$ у A: $\iota(a) = a$, а π је задато са $\pi(b) = b + \operatorname{Im} \phi$. Приметимо још да два тачна низа

$$A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 0 \quad \text{и} \quad 0 \to A'' \xrightarrow{\gamma} A''' \xrightarrow{\delta} A'''',$$

можемо спојити у дужи тачан низ:

$$A' \xrightarrow{\alpha} A \xrightarrow{\gamma\circ\beta} A''' \xrightarrow{\delta} A''''.$$

Наиме, како је γ „1–1” то је $\mathrm{Ker}(\gamma\circ\beta) = \mathrm{Ker}\,\beta$ ($\gamma(\beta(a)) = 0$ акко $\beta(a) = 0$), а како је β „на”, то је $\mathrm{Im}(\gamma \circ \beta) = (\gamma \circ \beta)[A] = \gamma[\beta[A]] = \gamma[A''] = \mathrm{Im}\,\gamma$.

Из два тривијално тачна низа

$$0 \to A \xrightarrow{id_A} A \to 0 \quad \text{и} \quad 0 \to B \xrightarrow{id_B} B \to 0 \tag{7}$$

можемо формирати кратак тачан низ

$$0 \to A \xrightarrow{i} A \oplus B \xrightarrow{p} B \to 0, \tag{8}$$

где је $i(a) = (a, 0)$, а $p(a, b) = b$. Заправо, ако приметимо да је, на пример, $A \oplus 0 = A$, и додамо 0 модуле на крајеве ових низова:

$$0 \to A \xrightarrow{id_A} A \to 0 \to 0 \quad \text{и} \quad 0 \to 0 \to B \xrightarrow{id_B} B \to 0,$$

видимо да наведни кратак тачан низ добијамо налажењем директне суме ова два низа, тј. на свакој позицији узимамо директну суму наведених модула, а хомоморфизми су оно што морају бити. Стога се може природно рећи да два низа у (7) настају ЦЕПАЊЕМ тачног низа у (8).

Ово је била кратка мотивација за следећу теорему.

Теорема 30. Нека је $0 \to A' \xrightarrow{\mu} A \xrightarrow{\epsilon} A'' \to 0$ кратак тачан низ. Следећи услови су еквивалентни.

1. Постоји $\eta\colon A \to A'$ тако да је $\eta \circ \mu = \mathrm{id}_{A'}$.
2. Постоји $\eta\colon A \to A'$ тако да је (A, η, ϵ) производ модула A' и A''.
3. Постоји $\nu\colon A'' \to A$ тако да је $\varepsilon \circ \nu = \mathrm{id}_{A''}$.
4. Постоји $\nu\colon A'' \to A$ тако да је (A, μ, ν) копроизвод модула A' и A''.
5. Постоје $\eta\colon A \to A'$ и $\nu\colon A'' \to A$ тако да је $\mu \circ \eta + \nu \circ \epsilon = \mathrm{id}_A$.

Доказ. 1. $\Longrightarrow$ 2. Докажимо најпре да је ограничење (рестрикција) $\epsilon|_{\mathrm{Ker}\,\eta}\colon \mathrm{Ker}\,\eta \to A''$ изоморфизам. У ту сврху, нека је $a'' \in A''$. Како је ϵ „на”, то постоји $a \in A$ такав да је $\epsilon(a) = a''$. Наравно, то a не мора бити у језгру од η, али мало га „коригујмо”, тј. уочимо елемент $a_0 = a - \mu(\eta(a))$. Како је $\epsilon \circ \mu = 0$, то је и $\epsilon(a_0) = a''$, Осим тога $\eta(a_0) = \eta(a) - \eta(\mu(\eta(a))) = \eta(a) - \eta(a) = 0$, па $a_0 \in \mathrm{Ker}\,\eta$, те је наведено ограничење заиста „на”. Уколико се $a \in \mathrm{Ker}\,\eta$ при ϵ слика у 0, тј. ако $a \in \mathrm{Ker}\,\epsilon \cap \mathrm{Ker}\,\eta = \mathrm{Im}\,\mu \cap \mathrm{Ker}\,\eta$ имамо да је $a = \mu(a')$ за неко $a' \in A'$, а такође је и $0 = \eta(a) = \eta(\mu(a')) = a'$, па је $a = \mu(0) = 0$ и добили смо тражени изоморфизам.

Нека су $\phi\colon X \to A'$ и $\psi\colon X \to A''$ хомоморфизми R-модула. Треба показати да постоји тачно један хомоморфизам $f\colon X \to A$ такав да је $\eta \circ f = \phi$ и $\epsilon \circ f = \psi$. Тражени хомоморфизам f задајемо са:

$$f(x) = \mu(\phi(x)) + (\epsilon|_{\operatorname{Ker}\eta})^{-1}(\psi(x)).$$

Како $(\epsilon|_{\operatorname{Ker}\eta})^{-1}(\psi(x)) \in \operatorname{Ker}\eta$ имамо да је $\eta(f(x)) = \eta(\mu(\phi(x))) + 0 = \phi(x)$. Такође је $\epsilon(f(x)) = \epsilon(\mu(\phi(x))) + \psi(x) = \psi(x)$. Да бисмо показали јединственост, претпоставимо да је $F\colon X \to A$ хомоморфизам за који важи $\eta\circ F = \phi$ и $\epsilon\circ F = \psi$. Тада за сваки $x \in X$ добијамо да $F(x)-f(x) \in \operatorname{Ker}\epsilon \cap \operatorname{Ker}\eta$, а горе смо показали да је тај пресек тривијалан. То завршава доказ јединствености.

2. $\Longrightarrow$ 1. Дакле, имамо производ $A' \xleftarrow{\eta} A \xrightarrow{\epsilon} A''$, а такође и производ $A' \xleftarrow{p_1} A' \times A'' \xrightarrow{p_2} A''$. Стога постоји изоморфизам $\theta\colon A \to A' \times A''$ за који важи $p_1 \circ \theta = \eta$ и $p_2 \circ \theta = \epsilon$. Дакле, $\theta(a) = (\eta(a), \epsilon(a))$ и, за $a' \in A'$: $\theta(\mu(a')) = (\eta(\mu(a')), \epsilon(\mu(a')) = ((\eta \circ \mu)(a'), 0)$. Но, θ је изоморфизам и његово сужење $\underline{\theta}\colon \operatorname{Ker}\epsilon \to \operatorname{Ker}p_2$ је такође изоморфизам. Наиме, ако је $a \in \operatorname{Ker}\epsilon$, онда је $p_2(\theta(a)) = \epsilon(a) = 0$, па наведено сужење заиста постоји. Наравно, и сужење је „1–1”. Коначно, ако је $(a', a'') \in \operatorname{Ker}p_2$ постоји неко $a \in A$ (θ је „на”) такво да је $\theta(a) = (a', a'')$. Но, $0 = p_2(a', a'') = p_2(\theta(a)) = \epsilon(a)$, те $a \in \operatorname{Ker}\epsilon$, те је сужење и „на”. Јасно је да је $\operatorname{Ker}p_2 = A' \times \{0\}$, те $\underline{\theta}$ остварује изоморфизам између $\operatorname{Ker}\epsilon = \operatorname{Im}\mu$ и $A' \times \{0\}$, те онда композиција $\theta \circ \mu$ остварује изоморфизам између A' и $A' \times \{0\}$ облика $a' \mapsto ((\eta \circ \mu)(a'), 0)$ и коначно добијамо да је $\omega = \eta \circ \mu\colon A' \to A'$ изоморфизам. Ако за η' означимо композицију $\omega^{-1} \circ \eta\colon A \to A'$ добијамо да је $\eta' \circ \mu = (\omega^{-1} \circ \eta) \circ \mu = \omega^{-1} \circ (\eta \circ \mu) = \omega^{-1} \circ \omega = \mathrm{id}_A$ те смо добили тражени хомоморфизам.

Читаоцима остављамо да за вежбу по аналогији докажу да важи еквиваленција 3. $\Longleftrightarrow$ 4.

5. $\Longrightarrow$ 1. Дакле, постоје $\eta\colon A \to A'$ и $\nu\colon A'' \to A$ тако да је $\mu \circ \eta + \nu \circ \epsilon = \mathrm{id}_A$. Компоновањем са μ са десне стране (преткомпоновањем) добијамо $\mu \circ \eta \circ \mu + \nu \circ \epsilon \circ \mu = \mu$. Како је $\epsilon \circ \mu = 0$, добијамо $\mu \circ \eta \circ \mu = \mu$. Но, μ је „1–1” па следи да је $\eta \circ \mu = \mathrm{id}_{A'}$ (уверите се у ово).

5. $\Longrightarrow$ 3. Једнакост из 5. компонујемо сада са ϵ са леве стране (посткомпонујемо) и добијамо $\epsilon\circ\mu\circ\eta+\epsilon\circ\nu\circ\epsilon = \epsilon$. Како је $\epsilon\circ\mu = 0$, имамо $\epsilon\circ\nu\circ\epsilon = \epsilon$, па из чињенице да је ϵ „на” добијамо $\epsilon \circ \nu = \mathrm{id}_{A''}$ (уверите се зашто је ово заиста тако).

3. $\Longrightarrow$ 5. Посматрајмо хомоморфизам $\xi = \mathrm{id}_A - \nu \circ \epsilon\colon A \to A$. Посткомпоновањем са ϵ добијамо $\epsilon\circ\xi = \epsilon - \epsilon\circ\nu\circ\epsilon = \varepsilon - \varepsilon = 0$. Ово нам говори да је $\operatorname{Im}\xi \subseteq \operatorname{Ker}\epsilon = \operatorname{Im}\mu$. Како је μ „1–1”, постоји функција $\mu^{-1}\colon \operatorname{Im}\mu \to A'$, па можемо дефинисати функцију $\eta = \mu^{-1} \circ \xi$. Како је $(\mu \circ \mu^{-1})(a) = a$ за све $a \in \operatorname{Im}\mu$, имамо да је $\mu \circ \eta = \mu \circ \mu^{-1} \circ \xi = \xi = \mathrm{id}_A - \nu \circ \epsilon$, па добијамо $\mu \circ \eta + \nu \circ \epsilon = \mathrm{id}_A$.

Остављамо читаоцима за вежбу да докажу да 1. $\Longrightarrow$ 5. $\square$

Последица 31. Нека је $\pi\colon A \to A$ ПРОЈЕКТОР, тј. нека задовољава услов $\pi^2 = \pi$. Тада је $A \cong \operatorname{Im}\pi \oplus \operatorname{Ker}\pi$.

Доказ. Посматрамо кратак тачан низ

$$0 \to \operatorname{Ker}\pi \xrightarrow{\mu} A \xrightarrow{\epsilon} \operatorname{Im}\pi \to 0.$$

Наравно, μ је укључивање, а ϵ је сужење од π добијено смањивањем кодомена. Можемо дефинисати укључење $\nu\colon \operatorname{Im}\pi \to A$, тј. $\nu(a) = a$. Ако је $b \in \operatorname{Im}\pi$, је $b = \pi(a)$ за неко $a \in A$ и $\epsilon(\nu(b)) = \pi(\pi(a)) = \pi^2(a) = \pi(a) = b$, па је $\epsilon \circ \nu = \mathrm{id}_{\operatorname{Id}\pi}$. Стога је, по претходној теореми $A \cong \operatorname{Ker}\pi \oplus \operatorname{Im}\pi$. $\square$

Но, посветимо се још мало овом примеру. Наиме, и $\operatorname{Ker}\pi$ и $\operatorname{Im}\pi$ су подмодули од A и можемо формирати суму тих подмодула. Покажимо да важи следећи став.

Став 32. Нека је $\pi\colon A \to A$ пројектор као у претходној последици. Тада важи следеће.

(1) $\operatorname{Ker}\pi + \operatorname{Im}\pi = A$;

(2) $\operatorname{Ker}\pi \cap \operatorname{Im}\pi = \{0\}$;

(3) Сваки елемент $a \in A$ се на јединствен начин може изразити у облику $a = x + y$, где $x \in \operatorname{Ker}\pi$ и $y \in \operatorname{Im}\pi$.

Доказ. Нека је $a \in A$. Тада $a - \pi(a) \in \operatorname{Ker}\pi$. Наиме, $\pi(x) = \pi(a) - \pi^2(a) = \pi(a) - \pi(a) = 0$. Дакле, имамо да је $a = (a - \pi(a)) + \pi(a)$, при чему $a - \pi(a) \in \operatorname{Ker}\pi$, а $\pi(a) \in \operatorname{Im}\pi$ и показали смо да важи (1).

Уколико $a \in \operatorname{Ker}\pi \cap \operatorname{Im}\pi$ имамо да је $a = \pi(x)$ за неки $x \in A$, јер је $a \in \operatorname{Im}\pi$, као и да је $\pi(a) = 0$, јер је a у језгру. Но, тада имамо $0 = \pi(a) = \pi(\pi(x)) = \pi^2(x) = \pi(x) = a$ и доказали смо (2).

Коначно, ако је $a = x + y = x' + y'$, где $x, x' \in \operatorname{Ker}\pi$, а $y, y' \in \operatorname{Im}\pi$, онда $x - x' = y' - y \in \operatorname{Ker}\pi \cap \operatorname{Im}\pi = \{0\}$ и доказали смо и (3). $\square$

Користићемо ad hoc ознаку $\dot{+}$ за овакву суму и зваћемо је УНУТРАШЊА ДИРЕКТНА СУМА. Дакле, $A = \operatorname{Ker}\pi \dot{+} \operatorname{Im}\pi$. Општије, ако је A_i фамилија подмодула од A, онда $\dot{+}_{i\in I} A_i$ означава суму подмодула за коју важи да се сваки елемент те суме на јединствен начин може приказати у облику суме елемената из тих модула. Важи следећа теорема.

Теорема 33. Нека је A_i, $i \in I$ фамилија подмодула од A, $q_i\colon A_i \to A$ њихова укључења у A. Тада су следећи услови еквивалентни.

(1) $(A; (q_i)_{i\in I})$ је копроизвод (директна сума) подмодула A_i;

(2) $A = +_{i\in I} A_i$ и за свако $i \in I$: $A_i \cap (+_{j\neq i} A_j) = \{0\}$;

(3) $A = \dot{+}_{i\in I} A_i$.

Доказ. (1) $\Longrightarrow$ (2). Претпоставимо да је $A' = +_{i\in I} A_i \neq A$. Како је A копроизвод подмодула A_i, то постоји тачно једно $: A \to A/A'$ такво да је $f \circ q_i = 0$ за све $i \in I$. Но, то није тачно. И нула морфизам који слика све елементе из A у нулу и стандардни морфизам $p\colon a \mapsto a + A'$ испуњавају ова два услова, а $p \neq 0$, јер A/A' није тривијалан модул.

Претпоставимо да је за неко $i \in I$: $A_i \cap (+_{j\neq i} A_j) \neq \{0\}$ и нека је $b \neq 0$ нетривијалан елемент из тог пресека. Стога је $b = a_{j_1} + \cdots + a_{j_n}$ за неке $j_1, \ldots, j_n$ различите од i. Дефинишимо $f_k\colon A_k \to A$ са:

$$f_k = \begin{cases} q_i, & \text{ако је } k = i, \\ 0, & \text{иначе.} \end{cases}$$

По дефиницији копроизвода следи да постоји јединствен $f\colon A \to A$ такав да је $f \circ q_k = f_k$ за све $k \in I$. То значи да је $f(b) = f(q_i(b)) = f_i(b) = b$ и $f(a_{j_s}) = f(q_{j_s}(a_{j_s})) = f_{j_s}(a_{j_s}) = 0$ за све $s = \overline{1,n}$, па је $f(a_{j_1} + \cdots + a_{j_n}) = 0$. Добили смо да је $b = 0$ и та контрадикција завршава доказ ове импликације.

(2) $\Longrightarrow$ (3). Знамо да је $A = +_{i\in I} A_i$. Претпоставимо да приказ елемената из A у облику суме елемената из тих подмодула није јединствен. То значи да имамо једнакост $a_{i_1} + \cdots + a_{i_n} = b_{i_1} + \cdots + b_{i_n}$ за неке $i_1, \ldots, i_n$, при чему $a_{i_k}, b_{i_k} \in A_{i_k}$, а међу њима може бити и оних који су једнаки нули, али за бар једно s је $a_{i_s} \neq b_{i_s}$. Тада имамо једнакост:

$$A_{i_s} \ni a_{i_s} - b_{i_s} = \sum_{k\neq s} (b_{i_k} - a_{i_k}) \in +_{j\neq i} A_i.$$

Дакле, имамо елемент различит од нуле који се налази у тривијалном пресеку. Та контрадикција завршава доказ ове импликације.

(3) $\Longrightarrow$ (1). Нека је Y произвољан модул и $f_i\colon A_i \to Y$ произвољни хомоморфизми. Треба показати да постоји тачно један $f\colon A \to Y$ тако да је $f \circ q_i = f_i$ за све $i \in I$. Тражено f дефинишемо на следећи начин. Нека је $a \in A$. Како је $A = \dot{+}_{i\in I} A_i$, то је $a = a_{i_1} + \cdots + a_{i_n}$ за неке $i_1, \ldots, i_n$ и $a_{i_k} \in A_{i_k}$. Тада стављамо да је $f(a) = f_{i_1}(a_{i_1}) + \cdots + f_{i_n}(a_n)$. Ово јесте хомоморфизам модула. Најпре, ако је $r \in R$, онда је $r \bullet a = r \bullet a_{i_1} + \cdots + r \bullet a_{i_n}$, при чему $r \bullet a_{i_k} \in A_{i_k}$, јер су ово подмодули од A. Стога је

$$\begin{aligned} f(r \bullet a) = f_{i_1}(r \bullet a_{i_1}) + \cdots + f_{i_n}(r \bullet a_{i_n}) &= r \bullet f(a_{i_1}) + \cdots + r \bullet f(a_{i_n}) \\ &= r \bullet (f(a_{i_1}) + \cdots + f(a_{i_n})) = r \bullet f(a). \end{aligned}$$

Доказ да је $f(a+b) = f(a) + f(b)$ остављамо читаоцима за вежбу. Дакле, f јесте хомоморфизам модула и јасно је да је $f \circ q_i = f_i$ за све $i \in I$ пошто смо га управо тако и дефинисали. За доказ јединствености, претпоставимо да је $g\colon A \to Y$ неки хомоморфизам за који важи: $g \circ q_i =$

f_i. Уколико је $a \in A$, онда је, као и горе, $a = a_{i_1} + \cdots + a_{i_n}$, за неке a_{i_k} па је

$$\begin{aligned}g(a) = g(a_{i_1} + \cdots + a_{i_n}) = g(a_{i_1}) + \cdots + g(a_{i_n}) \text{ јер је } a \text{ хомоморфизам} \\ = g(q_{i_1}(a_{i_1})) + \cdots + g(q_{i_n}(a_{i_n})) = (g \circ q_{i_1})(a_{i_1}) + \cdots + (g \circ q_{i_n})(a_{i_n}) \\ = f_{i_1}(a_{i_1}) + \cdots + f_{i_n}(a_{i_n}) = f(a).\end{aligned}$$

Овим је завршен и доказ последње импликације. □

У даљем раду ћемо и унутрашњу директну суму подмодула A_i означавати са $\bigoplus_{i \in I} A_i$, а свакако ће нам из контекста бити јасно уколико се ради о њој.

Дефиниција 34. Нека је A леви R-модул и $S \subseteq A$. Подмодул генерисан скупом S је најмањи подмодул који садржи S као свој подскуп. Ако је S коначан, онда за такав модул кажемо да је коначно генерисан, а ако је једночлан, онда кажемо да је цикличан.

Став 35. Нека су A и S као у претходној дефиницији. Тада је подмодул B генерисан скупом S:

$$B = \left\{ \sum_{a \in S'} r_a \bullet a : S' \text{ је коначан подскуп од } S, r_a \in R \right\}.$$

Доказ. Ово је једноставно, остављамо читаоцима за лаку вежбу. □

Приметимо да се за тривијалан модул може узети да му је скуп генератора празан, али и једночлан – састоји се само од 0.

Важи следећа веома корисна карактеризација цикличних модула.

Став 36. Леви R-модул A је цикличан ако и само постоји леви идеал I у R тако да је $A \cong R/I$.

Доказ. Наравно, из примера 20 знамо да је сваки леви идеал подмодул прстена у коме се налази. Но, R/I јесте цикличан, генерисан је елементом $1 + I$: за све $r \in R$ је $r + I = r \bullet (1 + I)$.

Нека је A цикличан леви R-модул и нека је он генерисан елементом a_0. То значи да је $A = \{r \bullet a_0 : r \in R\}$. Посматрајмо функцију $\phi\colon R \to A$ задату са $\phi(r) := r \bullet a_0$. Имамо да је

$$\phi(r + r') = (r + r') \bullet a_0 = r \bullet a_0 + r' \bullet a_0 = \phi(r) + \phi(r').$$

Такође, $\phi(s \cdot r) = (s \cdot r) \bullet a_0 = s \bullet (r \bullet a_0) = s \bullet \phi(r)$. Стога је ϕ хомоморфизам левих R-модула. Јасно је да је ϕ „на”. Тада је $\operatorname{Ker} \phi$ идеал у прстену R, а на основу теореме 25 добијамо изоморфизам $R/\operatorname{Ker} \phi \cong A$. □

3 Функтор Hom

Најпре уводимо појам бимодула.

Дефиниција 37. Нека су R и S прстени са јединицом. Ако је A један леви R-модул и десни S-модул, онда кажемо да је A један (R, S)-бимодуле ако за све $r \in R$, $s \in S$, $a \in A$ важи: $(r * a) \star s = r * (a \star s)$.

Категорију свих (R, S)-бимодула означићемо са ${}_R\mathfrak{M}_S$. Приметимо да је сваки леви R-модул заправо један $(R, \mathbb{Z})$-бимодул. Слично се и десни модули могу видети као бимодули. Сваки (R, S)-бимодул можемо идентификовати са $(S^{\text{op}}, R^{\text{op}})$-бимодулом. Могао би се чак и (R, S)-бимодул идентификовати са левим $(R \times S^{\text{op}})$-модулом, али ипак то нећемо радити. Приметимо само да се, у случају комутативног прстена R сваки леви R модул може видети не само и као десни R-модул, него и као (R, R)-бимодул. Ради једноставности ознака, користићемо ознаку $\cdot$ и за лево и за десно дејство, док ћемо ознаку за множење у прстену изостављати кад год можемо.

Нека је $A \in_R \mathfrak{M}_S$, $B \in_R \mathfrak{M}_T$. Тада на Абеловој групи $\mathrm{Hom}_R(A, B)$ можемо задати структуру (S, T)-модула на следећи начин. Ако је $s \in S$, $t \in T$, $\phi \in \mathrm{Hom}_R(A, B)$, онда $s \cdot \phi$ и $\phi \cdot t$ дефинишемо са:

$$(s \cdot \phi)(a) := \phi(a \cdot s), \qquad (\phi \cdot t)(a) := \phi(a) \cdot t.$$

Треба проверити да $s \cdot \phi, \phi \cdot t \in \mathrm{Hom}_R(A, B)$.

$$\begin{aligned}(s \cdot \phi)(a_1 + a_2) = \phi((a_1 + a_2) \cdot s) &= \phi(a_1 \cdot s + a_2 \cdot s) \\ &= \phi(a_1 \cdot s) + \phi(a_2 \cdot s) = (s \cdot \phi)(a_1) + (s \cdot \phi)(a_2);\end{aligned}$$

$$(s \cdot \phi)(r \cdot a) = \phi((r \cdot a) \cdot s) = \phi(r \cdot (a \cdot s)) = r \cdot \phi(a \cdot s) = r \cdot (s \cdot \phi)(a);$$

$$\begin{aligned}(\phi \cdot t)(a_1 + a_2) = \phi(a_1 + a_2) \cdot t &= (\phi(a_1) + \phi(a_2)) \cdot t \\ &= \phi(a_1) \cdot t + \phi(a_2) \cdot t = (\phi \cdot t)(a_1) + (\phi \cdot t)(a_2);\end{aligned}$$

$$(\phi \cdot t)(r \cdot a) = \phi((r \cdot a) \cdot t) = \phi(r \cdot (a \cdot t)) = r \cdot \phi(a \cdot t) = r \cdot (\phi \cdot t)(a).$$

Проверавамо да ли је $\mathrm{Hom}_R(A, B)$ леви S-модул.

M1. $$\begin{aligned}(s \cdot (\phi_1 + \phi_2))(a) = (\phi_1 + \phi_2)(a \cdot s) &= \phi_1(a \cdot s) + \phi_2(a \cdot s) \\ &= (s \cdot \phi_1)(a) + (s \cdot \phi_2)(a) = (s \cdot \phi_1 + s \cdot \phi_2)(a);\end{aligned}$$

M2. $$\begin{aligned}((s_1 + s_2) \cdot \phi)(a) &= \phi(a \cdot (s_1 + s_2)) = \phi(a \cdot s_1 + a \cdot s_2) \\ &= \phi(a \cdot s_1) + \phi(a \cdot s_2) = (s_1 \cdot \phi)(a) + (s_2 \cdot \phi)(a) = (s_1 \cdot \phi + s_2 \cdot \phi)(a);\end{aligned}$$

M3. $((s_1 s_2) \cdot \phi)(a_1) = \phi(a \cdot (s_1 s_2)) = \phi((a \cdot s_1) \cdot s_2) = (s_2 \cdot \phi)(a \cdot s_1) = (s_1 \cdot (s_2 \cdot \phi))(a);$

M4. $(1_S \cdot \phi)(a) = \phi(a \cdot 1_S) = \phi(a)$.

Проверу да је $\mathrm{Hom}_R(A, B)$ десни T-модул остављамо за вежбу.

Такође треба проверити слагање ових дејстава:

$$((s \cdot \phi) \cdot t)(a) = (s \cdot \phi)(a) \cdot t = \phi(a \cdot s) \cdot t;$$

$$(s \cdot (\phi \cdot t))(a) = (\phi \cdot t)(a \cdot s) = \phi(a \cdot s) \cdot t.$$

Заиста је $(s \cdot \phi) \cdot t = s \cdot (\phi \cdot t)$.

Нека су дати модули $A, A_1, A_2, A_3 \in_R \mathfrak{M}_S$; $B, B_1, B_2, B_3 \in_R \mathfrak{M}_T$ и хомоморфизми $\phi \in \mathrm{Hom}_R(A_1, A_2)$, $\psi \in \mathrm{Hom}_R(A_2, A_3)$; $\kappa \in \mathrm{Hom}_R(B_1, B_2)$, $\lambda \in \mathrm{Hom}_R(B_2, B_3)$. Дефинишемо

$$\phi^* \colon \mathrm{Hom}_R(A_2, B) \to \mathrm{Hom}_R(A_1, B)$$

са $\phi^*(\alpha) := \alpha \circ \phi$ за $\alpha \in \mathrm{Hom}_R(A_1, A_2)$. Аналогно се дефинишу ψ^* и $(\psi \circ \phi)^*$.

Нека $\beta \in \mathrm{Hom}_R(A_3, B)$. Тада је

$$(\psi \circ \phi)^*(\beta) = \beta \circ (\psi \circ \phi) = (\beta \circ \psi) \circ \phi = \phi^*(\beta \circ \psi) = \phi^*(\psi^*(\beta)) = (\phi^* \circ \psi^*)(\beta),$$

па је

$$(\psi \circ \phi)^* = \phi^* \circ \psi^*.$$

Уколико је $A_1 = A_2 = B = A$ и $\phi = \mathrm{id}_A$, имамо да је $\mathrm{id}_A^*(\alpha) = \alpha \circ \mathrm{id}_A = \alpha$, па је

$$\mathrm{id}_A^* = \mathrm{id}_{\mathrm{Hom}_R(A,A)}.$$

Дефинишемо

$$\kappa_* \colon \mathrm{Hom}_R(A, B_1) \to \mathrm{Hom}_R(A, B_2)$$

са: $\kappa_*(\theta) := \kappa \circ \theta$, за $\theta \in \mathrm{Hom}_R(A, B_1)$. Аналогно се дефинишу λ_* и $(\lambda\kappa)_*$. Нека $\theta \in \mathrm{Hom}(A, B_1)$. Тада је

$$(\lambda \circ \kappa) * (\theta) = (\lambda \circ \kappa) \circ \theta = \lambda \circ (\kappa \circ \theta) = \lambda \circ (\kappa_*(\theta)) = \lambda_*(\kappa_*(\theta)) = (\lambda_* \kappa_*)(\theta),$$

па је

$$(\lambda \circ \kappa)_* = \lambda_* \circ \kappa_*.$$

Уколико је $A = A_1 = B_1 = B_2$ и $\kappa = \mathrm{id}_A$, имамо да је $(\mathrm{id}_A)_*(\theta) = \mathrm{id}_A \circ \theta = \theta$, па је

$$(\mathrm{id}_A)_* = \mathrm{id}_{\mathrm{Hom}(A,A)}.$$

Нека је $\mathcal{C}$ ма која категорија. Можемо дефинисати ОПОЗИТНУ категорију $\mathcal{C}^{\mathrm{op}}$ са: $O(\mathcal{C}^{\mathrm{op}}) = O(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) := \mathrm{Hom}_{\mathcal{C}}(B, A)$, $f \circ^{\mathrm{op}} g := g \circ f$. Кратко речено, опозитна категорија се добија од почетне категорије „обртањем” свих стрелица. Ако су $\mathcal{C}$ и $\mathcal{D}$ ма које категорије, онда је функтор F из категорије $\mathcal{C}$ у категорију $\mathcal{D}$, у ознаци $F\colon \mathcal{C} \to \mathcal{D}$, придруживање $O(\mathcal{C} \ni A \mapsto F(A) \in \mathcal{D}$ при чему важи да је $F(g \circ f) = F(g) \circ F(f)$ кад год постоји $g \circ f$, као и $F(1_A) = 1_{F(A)}$ за све $A \in \mathcal{C}$. За функтор $F\colon \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ кажемо и да је један КОНТРАВАРИЈАНТАН функтор из $\mathcal{C}$ у $\mathcal{D}$ (за обичан функтор се каже и да је КОВАРИЈАНТАН).

Сада можемо формулисати следећу теорему.

Теорема 38. Нека $A \in_R \mathfrak{M}_S$, $B \in_R \mathfrak{M}_T$. Тада је придруживање

$$X \mapsto \mathrm{Hom}_R(A, X), \quad (X \xrightarrow{\phi} Y) \mapsto (\mathrm{Hom}_R(A, X) \xrightarrow{\phi_*} \mathrm{Hom}_R(A, Y)$$

један коваријантни функтор из категорије ${}_R\mathfrak{M}_T$ у категорију ${}_S\mathfrak{M}_T$, а придруживање

$$X \mapsto \mathrm{Hom}_R(X, B), \quad (X \xrightarrow{\phi} Y) \mapsto (\mathrm{Hom}_R(Y, B) \xrightarrow{\phi^*} \mathrm{Hom}_R(X, B)$$

један контраваријантни функтор из категорије ${}_R\mathfrak{M}_S$ у категорију ${}_S\mathfrak{M}_T$.

Доказ. Заправо смо скоро све доказали у претходној дискусији. Остало је само да се покаже да су ϕ_* и ϕ^* хомоморфизми одговарајућих модула. Докажимо то за ϕ_*.

Дакле, треба показати да је $\phi_*(s \cdot \alpha) = s \cdot \phi_*(\alpha)$, за $s \in S$ и $\phi_*(\alpha \cdot t) = \phi_*(\alpha) \cdot t$, за $t \in T$. Нека је $a \in A$.

$$\begin{aligned} &\phi_*(s \cdot \alpha)(a) = (\phi \circ (s \cdot \alpha))(a) = \phi((s \cdot \alpha)(a)) = \phi(\alpha(a \cdot s)) \\ &= (\phi \circ \alpha)(a \cdot s) = \phi_*(\alpha)(a \cdot s) = (s \cdot \phi_*(\alpha))(a), \text{ па је } \phi_*(s \cdot \alpha) = s \cdot \phi_*(\alpha). \end{aligned}$$

$$\begin{aligned} &\phi_*(\alpha \cdot t)(a) = (\phi \circ (\alpha \cdot t))(a) = \phi((\alpha \cdot t)(a)) = \phi(\alpha(a) \cdot t) \\ &\quad = \phi(\alpha(a)) \cdot t = (\phi_*(\alpha))(a) \cdot t = (\phi_*(\alpha) \cdot t)(a), \text{ па је } \phi_*(\alpha \cdot t) = \phi_*(\alpha) \cdot t. \end{aligned}$$

Доказ за ϕ^* остављамо читаоцима за вежбу. □

Све ово што смо радили могло је да се примени и када имамо ситуацију у којој су A и B десни R-модули, тј. у случају да разматрамо $\mathrm{Hom}_R(A, B)$, где $A \in_S \mathfrak{M}_R$, а $B \in_T \mathfrak{M}_R$, но то се може свести на претходно тако што идентификујемо ${}_S\mathfrak{M}_R$ са ${}_{R^{\mathrm{op}}}\mathfrak{M}_{S^{\mathrm{op}}}$ и ${}_T\mathfrak{M}_R$ са ${}_{R^{\mathrm{op}}}\mathfrak{M}_{T^{\mathrm{op}}}$. Остављамо читаоцима формулације и провере тих тврђења (директно, без ове идентификације). То је добра, мада можда мало досадна вежба. Добро је да то бар једном „прође кроз руку”.

Теорема 39. Посматрајмо прстен R као један (R, R) модул (коришћењем множења у самом прстену). Уколико је $B \in_R \mathfrak{M}_S$, онда је $\mathrm{Hom}_R(R, B) \in_R \mathfrak{M}_S$ и постоји природан изоморфизам $\mathrm{Hom}_R(R, B) \cong B$.

Доказ. Дефинишемо функцију $F_B\colon \mathrm{Hom}_R(R, B) \to B$ са $F_B(\phi) := \phi(1)$.

F_B је хомоморфизам модула.

$$F_B(\phi + \psi) = (\phi + \psi)(1) = \phi(1) + \psi(1) = F_B(\phi) + F_B(\psi);$$

$$F_B(r\cdot\phi)=(r\cdot\phi(1))=\phi(1\cdot r)=\phi(r)=r\cdot\phi(1)=r\cdot F_B(\phi);$$
$$F_B(\phi\cdot s)=(\phi\cdot s)(1)=\phi(1)\cdot s=F_B(\phi)\cdot s.$$

F_B је „на”. Нека је $b\in B$ произвољан. Дефинишемо $\phi\in \mathrm{Hom}_R(R,B)$ са: $\phi(r):=r\cdot b$. Овако дефинисано ϕ јесте хомоморфизам левих модула. Наиме, $\phi(r_1+r_2)=(r_1+r_2)\cdot b=r_1\cdot b+r_2\cdot b=\phi(r_1)+\phi(r_2)$; такође је $\phi(rr_1)=(rr_1)\cdot b=r\cdot(r_1\cdot b)=r\cdot\phi(r_1)$. Како је $F_B(\phi)=\phi(1)=1\cdot b=b$, то је F_B „на”.

F_B је „1–1”. Нека је $F_B(\phi)=F_B(\psi)$. Тада је $\phi(1)=\psi(1)$. Ако је $r\in R$ произвољан, имамо да је $\phi(r)=r\cdot\phi(1)=r\cdot\psi(1)=\psi(r)$, па је заиста $\phi=\psi$.

Природност. Нека је $\alpha\colon B\to B'$ хомоморфизам модула. Треба показати да важи једнакост: $\alpha\circ F_B=F_{B'}\circ\alpha_*$. У ту сврху, нека је $\phi\in\mathrm{Hom}_R(R,B)$.

$$(\alpha\circ F_B)(\phi)=\alpha(F_B(\phi))=\alpha(\phi(1))=(\alpha\circ\phi)(1)=\alpha_*(\phi)(1)=F_{B'}(\alpha_*(\phi))=(F_{B'}\circ\alpha_*)(\phi).\ \square$$

Теорема 40. Нека $A, A_i{\in}_R\mathfrak{M}_S$, $B, B_i{\in}_R\mathfrak{M}_T$, за $i\in I$. Тада постоје природни изоморфизми (S,T)-бимодула:

$$\mathrm{Hom}_R(A,\prod_{i\in I}B_i)\cong\prod_{i\in I}\mathrm{Hom}_R(A,B_i),\ \mathrm{Hom}_R(\oplus_{i\in I}A_i,B)\cong\prod_{i\in I}\mathrm{Hom}_R(A_i,B).$$

Доказ. Ово лако следи из својстава производа и копроизвода: хомоморфизам у производ је потпуно одређен компонентама и слично за копроизвод. $\square$

Дефиниција 41. Претпоставимо да је $F\colon\mathcal{C}\to\mathcal{D}$ коваријантан функтор из неке категорије модула у неку категорију модула. Тада кажемо да је он ЛЕВО ТАЧАН ако кратак тачан низ у $\mathcal{C}$

$$0\to A'\xrightarrow{\mu}A\xrightarrow{\epsilon}A''\to 0 \tag{9}$$

преводи у тачан низ у $\mathcal{D}$

$$0\to F(A')\xrightarrow{F(\mu)}F(A)\xrightarrow{F(\epsilon)}F(A'').$$

У случају да је F контраваријантан функтор, кажемо да је лево тачан ако кратак тачан низ (20) преводи у тачан низ

$$0\to F(A'')\xrightarrow{F(\epsilon)}F(A)\xrightarrow{F(\mu)}F(A').$$

Теорема 42. Оба функтора разматрана у теореми 38 су лево тачни.

Доказ. Потребно је само доказати да су следећи низови тачни:

$$0\to\mathrm{Hom}_R(B,A')\xrightarrow{\mu_*}\mathrm{Hom}_R(B,A)\xrightarrow{\epsilon_*}\mathrm{Hom}_R(B,A'') \tag{10}$$

$$0\to\mathrm{Hom}_R(A'',B)\xrightarrow{\epsilon^*}\mathrm{Hom}_R(A,B)\xrightarrow{\mu^*}\mathrm{Hom}_R(A',B) \tag{11}$$

Но, ми смо имплицитно практично све ово доказали доказујући теорему 30! Али, урадимо то ипак сада и експлицитно.

Уколико је $\mu_*(\phi) = 0$, то значи да је $\mu \circ \phi = 0$, те је, за све $b \in B$: $\mu(\phi(b)) = 0$, те из чињенице да је μ „1–1" следи да је $\phi(b) = 0$. Стога је $\phi = 0$ и μ_* је „1–1". Уколико је $\epsilon_*(\psi) = 0$, то значи да је $\epsilon \circ \psi = 0$, те је $\operatorname{Im}\psi \subseteq \operatorname{Ker}\epsilon = \operatorname{Im}\mu$. Стога за сваки $b \in B$ постоји (и то тачно један, јер је μ „1–1") $a' \in A'$ такав да је $\mu(a') = \psi(b)$. Стога имамо дефинисану функцију $\theta\colon B \to A'$ са: $\theta(b) = a' \overset{\text{def}}{\Longleftrightarrow} \mu(a') = \psi(b)$. Проверите за вежбу да је $\theta \in \operatorname{Hom}_R(B, A')$. Тада имамо да је $\mu_*(\theta) = \mu \circ \theta = \psi$.

Уколико је $\epsilon^*(\gamma) = 0$, за $\gamma \in \operatorname{Hom}_R(A'', B)$, то је $\gamma \circ \epsilon = 0$. Ако је $a'' \in A''$, како је ϵ „на", то постоји $a \in A$ тако да је $a'' = \epsilon(a)$, па је $\gamma(a) = \gamma(\epsilon(a'')) = (\gamma \circ \epsilon)(a') = 0$, па је заправо $\gamma = 0$. Уколико је $\mu^*(\psi) = 0$, за $\psi \in \operatorname{Hom}_R(A, B)$, то је $\psi \circ \mu = 0$. То значи да је ограничење ψ на $\operatorname{Im}\mu = \operatorname{Ker}\epsilon$ једнако нули. Стога можемо дефинисати хомоморфизам $\overline{\psi}\colon A/\operatorname{Ker}\epsilon \to B$ са: $\overline{\psi}(a + \operatorname{Ker}\epsilon) := \psi(a)$. Наиме, ако је $a + \operatorname{Ker}\epsilon = a_1 + \operatorname{Ker}\epsilon$, онда је $a - a_1 \in \operatorname{Ker}\epsilon$, па је $\psi(a - a_1) = 0$, те је $\psi(a) = \psi(a_1)$. Проверите да је $\overline{\psi}$ хомоморфизам модула. Како је ϵ „на", то постоји изоморфизам $\overline{\epsilon} : A/\operatorname{Ker}\epsilon \cong A''$ који $a + \operatorname{Ker}\epsilon$ слика у $\epsilon(a)$. Нека је $\theta = \overline{\psi} \circ \overline{\epsilon}^{-1} \in \operatorname{Hom}_R(A'', B)$. Нека је $a \in A$. Тада је

$$\theta(\epsilon(a)) = \overline{\psi}(\overline{\epsilon}^{-1}(\epsilon(a)) = \overline{\psi}(a + \operatorname{Ker}\epsilon) = \psi(a).$$

Дакле, $\epsilon^*(\theta) = \theta \circ \epsilon = \psi$. □

4 Функтор $\bigotimes$

Било би корисно да су читаоци упознати са тензорским производом Абелових група, но то није неопходно у ономе што следи пошто ћемо све извести *ab ovo*.

Дефиниција 43. Нека $A \in_R\mathfrak{M}_S$, $B \in_S\mathfrak{M}_T$. Дефинишемо $A \otimes_S B$, тензорски производ од A и B над S на следећи начин. Нека је $\mathcal{F}(A \times B)$ слободна Абелова група са скупом генератора $A \times B$. Посматрамо подгрупу $\mathcal{R}(A \times B)$ ове групе генерисану елементима:

- $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$, $a_1, a_2 \in A$, $b \in B$;
- $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$, $a \in A$, $b_1, b_2 \in B$;
- $(as, b) - (a, sb)$, $a \in A$, $b \in B$, $s \in S$.

$$A \otimes_S B := \mathcal{F}(A \times B)/\mathcal{R}(A \times B).$$

Став 44. На Абеловој групи $A \otimes_S B$ задајемо структуру (R, T)-бимодула са:

$$r \cdot (a \otimes b) := (ra) \otimes b, \text{ за } a, \in A, b \in B, r \in R$$

$$(a \otimes b) \cdot t := a \otimes (bt), \text{ за } a \in A, b \in B, t \in T.$$

Са $a \otimes b$ означавамо класу елемента $(a, b) \in \mathcal{F}$.

Доказ. Како је скуп генератора за $\mathcal{F}(A\times B)$ скуп $A\times B$, то је сваки елемент из $\mathcal{F}(A\times B)/\mathcal{R}(A\times B)$ класа елемента $(a_1,b_1)+\cdots+(a_k,b_k)-(a_{k+1},b_{k+1})-\cdots-(a_n,b_n)$ за неке $a_i\in A$, $b_j\in B$, тј. добија се сабирањем и одузимањем класа елемената (a_i,b_i), тј. сабирањем и одузимањем $a_i\otimes b_i$. Дакле, елементи облика $a\otimes b$, за $a\in A$ и $b\in B$ су генератори ове групе. Но, не постоји јединственост приказа елемената из групе $\mathcal{F}(A\times B)/\mathcal{R}(A\times B)$ у овом облику, тј. може се десити да имамо једнакост

$$\begin{aligned} a_1\otimes b_1+\cdots+a_k\otimes b_k-a_{k+1}\otimes b_{k+1}-\cdots-a_n\otimes b_n\\ =a'_1\otimes b'_1+\cdots+a'_l\otimes b'_l-a'_{l+1}\otimes b'_{l+1}-\cdots-a'_m\otimes b'_m, \end{aligned}\tag{12}$$

при чему се ни број сабирака са леве и десне стране не мора поклапати, нити знаци самих сабирака, нити поједини сабирци. Ако бисмо користили суму са леве стране, онда бисмо множењем са r слева добили елемент

$$(ra_1)\otimes b_1+\cdots+(ra_k)\otimes b_n-(ra_{k+1})\otimes b_{k+1}-\cdots-(ra_n)\otimes b_n,\tag{13}$$

а ако бисмо користили суму са десне стране, добили бисмо елемент

$$(ra'_1)\otimes b'_1+\cdots+(ra'_l)\otimes b'_l-(ra'_{l+1})\otimes b'_{r+1}-\cdots-(ra'_m)\otimes b'_m\tag{14}$$

и морамо се уверити да се ради о истом елементу. Но, шта значи то да имамо једнакост (12)? То заправо значи да

$$\begin{aligned} (a_1,b_1)+\cdots+(a_k,b_k)-(a_{k+1},b_{k+1})-\cdots-(a_n,b_n)\\ -(a'_1,b'_1)-\cdots-(a'_l,b'_l)+(a'_{l+1},b'_{l+1})+\cdots+(a'_m,b'_m)\in\mathcal{R}. \end{aligned}\tag{15}$$

Једнакост елемената (13) и (14) еквивалентна је са

$$\begin{aligned} (ra_1,b_1)+\cdots+(ra_k,b_k)-(ra_{k+1},b_{k+1})-\cdots-(ra_n,b_n)\\ -(ra'_1,b'_1)-\cdots-(ra'_l,b'_l)+(ra'_{l+1},b'_{l+1})+\cdots+(ra'_m,b'_m)\in\mathcal{R}. \end{aligned}\tag{16}$$

Овде треба обратити пажњу на чињеницу да је $\mathcal{R}(A\times B)\subseteq\mathcal{F}(A\times B)$ и да су у $\mathcal{F}(A\times B)$ елементи (a,b) слободни генератори, па међу њима нема никаквих веза!

Покажимо да ако $\sum_i\pm_i(x_1,y_i)\in\mathcal{R}(A\times B)$, онда и $\sum_i\pm_i(rx_i,y_i)$ припада $\mathcal{R}(A\times B)$, за све $x_i\in A$, $y_i\in B$, $r\in R$, $\pm_i\in\{+,-\}$. Из тога следи да (15) $\Rightarrow$ (16). Довољно је показати да су генератори у $\mathcal{R}(A\times B)$. А то није тешко.

- Из $(a_1+a_2,b)-(a_1,b)-(a_2,b)\in\mathcal{R}(A\times B)$ имамо да је $(r(a_1+a_2),b)-(ra_1,b)-(ra_2,b)=(ra_1+ra_2)-(ra_1,b)-(ra_2,b)\in\mathcal{R}(A\times B)$ (користили смо да је $r(a_1+a_2)=ra_1+ra_2$ у A).
- Из $(a,b_1+b_2)-(a,b_1)-(a,b_2)\in\mathcal{R}(A\times B)$ непосредно следи да $(ra,b_1+b_2)-(ra,b_1)-(ra,b_2)\in\mathcal{R}(A\times B)$.

- Из $(as,b)-(a,sb) \in \mathcal{R}(A\times B)$ имамо да је $(r(as),b)-(ra,sb) = ((ra)s,b)-(ra,sb) \in \mathcal{R}(A\times B)$ (користили смо да је $r(as)=(ra)s$ у A).

Овим смо показали да је множење елементима из R слева добро дефинисано. На аналогни начин се доказује да је и множење елементима из T здесна добро дефинисано. Остављамо читаоцима да то ураде, као и да доврше доказ да се овако заиста добија (R,T)-бимодул. □

Уколико је $S=\mathbb{Z}$, уместо $A\otimes_{\mathbb{Z}} B$ кратко ћемо писати само $A\otimes B$. На основу дефиниције, у модулу $A\otimes_S B$ важе следеће релације:

$$(a_1+a_2)\otimes b = a_1\otimes b + a_2\otimes b \qquad a\otimes(b_1+b_2) = a\otimes b_1 + a\otimes b_2, \tag{17}$$

за све $a,a_1,a_2\in A$ и $b,b_1,b_2\in B$, као и

$$as\otimes b = a\otimes sb, \tag{18}$$

за све $a\in A$, $b\in B$ и $s\in S$.

Доказ следећег става остављамо читаоцима уз напомену да је можда очигледан, али да ипак покушају да све то лепо протумаче.

Став 45. *(i)* $A_1\otimes_S A_2 \cong A_2\otimes_{S^{\mathrm{op}}} A_1$.

(ii) Ако $A\in {}_R\mathfrak{M}_S$, $B\in {}_S\mathfrak{M}_T$, $C\in {}_T\mathfrak{M}_U$, онда је

$$(A\otimes_S B)\otimes_T C \cong A\otimes_S (B\otimes_T C).$$

Став 46. Ако $A\in {}_R\mathfrak{M}_S$ и ако се R посматра као (R,R)-бимодул, онда је $R\otimes_R A\cong A$. Аналогно важи и $A\otimes_S S\cong A$.

Доказ. Доказујемо само први изоморфизам, други се доказује аналогно. Дефинишемо $\phi\colon A\to R\otimes_R A$ са: $\phi(a)=1\otimes a$.

ϕ је хомоморфизам бимодула.

$$\phi(a_1+a_2) = 1\otimes(a_1+a_2) = 1\otimes a_1 + 1\otimes a_2 = \phi(a_1)+\phi(a_2);$$

$$\phi(ra) = 1\otimes(ra) = 1r\otimes a = r1\otimes a = r\cdot(1\otimes a) = r\cdot\phi(a).$$

$$\phi(as) = 1\otimes(as) = (1\otimes a)\cdot s = \phi(a)\cdot s$$

ϕ је „на”. Тензорски производ је генерисан елементима $r\otimes a$, за $r\in R$ и $a\in A$. Но, $r\otimes a = 1\otimes ra = \phi(ra)$. Како су сви генератори у $\operatorname{Im}\phi$, то је ϕ „на”.

ϕ је „1–1”. Претпоставимо да је $\phi(a)=0$. То значи да $(1,a)\in\mathcal{R}$ (видети дефиницију тензорског производа). Можемо да дефинишемо функцију $f\colon R\times A\to A$ са: $f(r,a)=ra$. Ако је $\mathcal{F}(R\times A)$ слободна Абелова група са скупом генератора $R\times A$, онда постоји јединствен хомоморфизам

Абелових група $\overline{f}\colon \mathcal{F}(R\times A)\to A$ за који је $\overline{f}(r,a)=f(r,a)=ra$ за све $r\in R$, $a\in A$. Приметимо да је

$$\begin{aligned}\overline{f}\big((r_1+r_2,a)-(r_1,a)-(r_2,a)\big)&=\overline{f}(r_1+r_2,a)-\overline{f}(r_1,a)-\overline{f}(r_2,a)\\&=(r_1+r_2)a-r_1a-r_2a=0.\end{aligned}$$

Слично,

$$\begin{aligned}\overline{f}\big((r,a_1+a_2)-(r,a_1)-(r,a_2)\big)&=\overline{f}(r,a_1+a_2)-\overline{f}(r,a_1)-\overline{f}(r,a_2)\\&=r(a_1+a_2)-ra_1-ra_2=0.\end{aligned}$$

Наравно, имамо и да је $\overline{f}\big((rs,a)-(r,sa)\big)=\overline{f}(rs,a)-\overline{f}(r,sa)=(rs)a-r(sa)=0$. Дакле, $\overline{f}$ слика сваки генератор од $\mathcal{R}(R\times A)$ у нулу, па стога слика целу ту подгрупу у 0. Самим тим је и $a=1\cdot a=\overline{f}(1,a)=0$.

Тиме смо завршили доказ да је ϕ изоморфизам модула. □

Користили смо да се сваки елемент у тензорском производу $A\otimes_R B$ може приказати у облику $a_1\otimes b_1+\cdots+a_k\otimes b_k-a_{k+1}\otimes b_{k+1}-\cdots a_n\otimes b_n$ за неке k и n и неке $a_i\in A$, $b_j\in B$. Заправо се сваки елемент може приказати у облику збира елемената облика $a\otimes b$, без коришћења знака за одузимање.

Најпре: $0_A\otimes b=0_{A\otimes_R B}$, за све $b\in B$; такође је: $a\otimes 0_B=0_{A\otimes_R B}$ за све $a\in A$. Наиме,

$$0_A\otimes b=(0_A+0_A)\otimes b=0_A\otimes b+0_A\otimes b \text{ (на основу (17)}$$

и скраћивањем у Абеловој групи $A\otimes_R B$ добијамо да је $0_A\otimes b=0_{A\otimes_R B}$. Одавде лако следи да је $-(a\otimes b)=(-a)\otimes b$:

$$a\otimes b+(-a)\otimes b=(a+(-a))\otimes b=0_A\otimes b=0_{A\otimes_R B}.$$

Наравно, на исти начин можемо радити са другим фактором у тензорском производу. Сада видимо зашто се сваки елемент у тензорском производу може приказати у облику збира елемената облика $a\otimes b$.

Нека је $\alpha\colon A\to A'$ у ${}_R\mathfrak{M}_S$ и $\beta\colon B\to B'$ у ${}_S\mathfrak{M}_T$. Желимо да дефинишемо $\alpha\otimes\beta\colon A\otimes_R B\to A'\otimes_R B'$ тако да буде $(\alpha\otimes\beta)(a\otimes b)=\alpha(a)\otimes\beta(b)$ за све $a\in A$ И $b\in B$. То ћемо урадити на следећи начин. Дефинишемо функцију $f\colon A\times B\to A'\otimes_R B'$ са $f(a,b):=\alpha(a)\otimes\beta(b)$. Ако је $\mathcal{F}(A\times B)$ слободна Абелова група са скупом генератора $A\times B$, онда постоји јединствен хомоморфизам Абелових група $\overline{f}\colon \mathcal{F}(A\times B)\to A'\otimes_R B'$, такав да је $\overline{f}(a,b)=\alpha(a)\otimes\beta(b)$. Да бисмо имали хомоморфизам из тензорског производа морамо проверити да се сви елементи из $\mathcal{R}(A\times B)$ сликају у нулу.

$$\begin{aligned}&\overline{f}\big((a_1+a_2,b)-(a_1,b)-(a_2,b)\big)=\overline{f}(a_1+a_2,b)-\overline{f}(a_1,b)-\overline{f}(a_2,b)\\&\qquad=\alpha(a_1+a_2)\otimes\beta(b)-\alpha(a_1)\otimes\beta(b)=\alpha(a_2)\otimes\beta(b)\\&=\big(\alpha(a_1)+\alpha(a_2)\big)\otimes\beta(b)-\alpha(a_1)\otimes\beta(b)=\alpha(a_2)\otimes\beta(b)=0 \text{ (на основу (17))}.\end{aligned}$$

Аналогно се добија да је $\overline{f}\big((a, b_1 + b_2) - (a, b_1) - (a, b_2)\big) = 0$.

$$\begin{aligned}\overline{f}\big((as, b) - (a, sb)\big) &= \overline{f}(as, b) - \overline{f}(a, sb) = \alpha(as) \otimes \beta(b) - \alpha(a) \otimes \beta(sb) \\ &= \alpha(a)s \otimes \beta - \alpha(a) \otimes s\beta(b) \ (\alpha \text{ и } \beta \text{ су хомоморфизми бимодула}) \\ &= 0 \ (\text{на освову релације (18)}).\end{aligned}$$

Дакле, заиста $\overline{f}$ слика сваки елемент из $\mathcal{R}(A \times B)$ у нулу, па индукује хомоморфизам Абелових група (који ћемо означити онако како смо желели) $\alpha \otimes \beta \colon A \otimes_R B \to A' \otimes_R B'$. Како је $a \otimes b$ заправо класа елемента (a, b), видимо да је заиста $(\alpha \otimes \beta)(a \otimes b) = \alpha(a) \otimes \beta(b)$. Само још треба проверити да је ово хомоморфизам бимодула.

$$\begin{aligned}(\alpha \otimes \beta)(r \cdot (a \otimes b)) &= (\alpha \otimes \beta)(ra \otimes b) = \alpha(ra) \otimes \beta(b) \\ &= r\alpha(a) \otimes \beta(b) = r \cdot (\alpha(a) \otimes \beta(b)) \ (\alpha \text{ је хомоморфизам бимодула}) \\ &= r \cdot (\alpha \otimes \beta)(a \otimes b).\end{aligned}$$

Слично се показује да је $(\alpha \otimes \beta)((a \otimes b) \cdot t) = (\alpha \otimes \beta)(a \otimes b) \cdot t$.

Уколико $\alpha' \colon A' \to A''$ и $\beta' \colon B' \to B''$, онда је

$$\begin{aligned}((\alpha' \otimes \beta') \circ (\alpha \otimes \beta))(a \otimes b) &= (\alpha' \otimes \beta')\big((\alpha \otimes \beta)(a \otimes b)\big) \\ &= (\alpha' \otimes \beta')(\alpha(a) \otimes \beta(b)) = \alpha'(\alpha(a) \otimes \beta'(\beta(b)) = (\alpha' \circ \alpha)(a) \otimes (\beta' \circ \beta)(b),\end{aligned}$$

па је $(\alpha' \otimes \beta') \circ (\alpha \otimes \beta) = (\alpha' \circ \alpha) \otimes (\beta' \circ \beta)$.

Ово нам омогућава да тензорски производ, као и Hom, посматрамо као функтор на два начина.

1. $A \otimes_S - \colon Y \mapsto A \otimes Y$, $(\beta \colon Y \to Y') \mapsto (\mathrm{id}_A \otimes \beta \colon A \otimes_S Y \to A \otimes_S Y')$.
2. $- \otimes B \colon A \mapsto X \otimes B$, $(\alpha \colon X \to X') \mapsto (\alpha \otimes \mathrm{id}_B \colon X \otimes_S B \to X' \otimes_S B)$.

Лако се можемо уверити да ово јесу (коваријантни) функтори.

Теорема 47. Овако задати функтори су десно тачни, тј.

а) за сваки кратак тачан низ у ${}_R\mathfrak{M}_S$

$$0 \to A' \xrightarrow{\mu} A \xrightarrow{\epsilon} A'' \to 0$$

и $B \in {}_S\mathfrak{M}_T$ низ

$$A' \otimes_S B \xrightarrow{\mu \otimes \mathrm{id}_B} A \otimes_S B \xrightarrow{\epsilon \otimes \mathrm{id}_B} A'' \otimes_S B \to 0$$

је тачан у ${}_R\mathfrak{M}_T$ и

б) за сваки кратак тачан низ у ${}_S\mathfrak{M}_T$

$$0 \to B' \xrightarrow{\phi} B \xrightarrow{\psi} B'' \to 0$$

и $A \in {}_R\mathfrak{M}_S$ низ

$$A \otimes_S B' \xrightarrow{\mathrm{id}_A \otimes \phi} A \otimes_S B \xrightarrow{\mathrm{id}_A \otimes \psi} A \otimes_S B'' \to 0$$

је тачан у ${}_R\mathfrak{M}_T$.

Доказ. Доказаћемо део под а). Део под б) доказује се на аналоган начин. Како је $\epsilon \circ \mu = 0$, то је и $(\epsilon \otimes \mathrm{id}_B) \circ (\mu \otimes \mathrm{id}_B) = (\epsilon \circ \mu) \otimes (\mathrm{id}_B \circ \mathrm{id}_B) = 0 \otimes \mathrm{id}_B = 0$. Пошто је ϵ „на", то за сваки $a'' \in A''$ постоји $a \in A$ тако да је $\epsilon(a) = a''$, па, стога, за сваки адитивни генератор $a'' \otimes b$ за $A'' \otimes B$ постоји $a \in A$ и $b \in B$ тако да је $(\epsilon \otimes \mathrm{id}_B)(a \otimes b) = \epsilon(a) \otimes \mathrm{id}_B(b) = a'' \otimes b$, те је $\epsilon \otimes \mathrm{id}_B$ такође „на". Остаје да се докаже да је $\mathrm{Ker}(\epsilon \otimes \mathrm{id}_B) \subseteq \mathrm{Im}(\mu \otimes \mathrm{id}_B)$.

Нека је $P = A \otimes_S B / \mathrm{Im}(\mu \otimes \mathrm{id}_B)$. Ако је $z \in A \otimes_S B$, са $[z]$ означавамо његову класу у P. Дефинишемо функцију $f \colon A'' \times B \to P$ са:

$$f(a'', b) := [a \otimes b] \overset{\mathrm{def}}{\iff} \epsilon(a) = a''.$$

Покажимо да је функција добро дефинисана. Наиме, претпоставимо да је $\epsilon(a) = \epsilon(a_1) = a''$. То значи да је $a - a_1 \in \mathrm{Ker}\, \epsilon = \mathrm{Im}\, \mu$, те постоји $a' \in A'$ тако да је $a - a_1 = \mu(a')$. Но, то значи да је

$$a \otimes b - a_1 \otimes b = (a - a_1) \otimes b = \mu(a') \otimes b = (\mu \otimes \mathrm{id}_B)(a' \otimes b),$$

па $a \otimes b - a_1 \otimes b \in \mathrm{Im}(\mu \otimes \mathrm{id}_B)$ те је $[a \otimes b] = [a_1 \otimes b]$.

Стога f дефинише на тачно један начин хомоморфизам Абелових група $\overline{f} \colon \mathcal{F}(A'' \times B) \to P$, тако да је $\overline{f}(a'', b) = f(a'', b)$, где је, наравно, $\mathcal{F}(A'' \times B)$, слободна Абелова група са скупом генератора $A'' \times B$. Означимо, као и раније, са $\mathcal{R}(A'' \times B)$ подгрупу ове групе из дефиниције 43. Тада је $A'' \otimes B = \mathcal{F}(A'' \times B) / \mathcal{R}(A'' \times B)$.

Нека $\sum_i a_i \otimes b_i \in \mathrm{Ker}(\epsilon \otimes \mathrm{id}_B)$. То значи да је $\sum_i \epsilon(a_i) \otimes b_i = 0_{A'' \otimes B}$, односно, то значи да $\sum_i (\epsilon(a_i), b_i) \in \mathcal{R}(A'' \times B)$. Покажимо да $\overline{f}$ слика све елементе из $\mathcal{R}(A'' \times B)$ у 0_P. Наравно, проверавамо на генераторима. Нека су $a''_1, a''_2 \in A''$, $b \in B$. Уколико је $\epsilon(a_1) = a''_1$ и $\epsilon(a_2) = a''_2$, онда је $\epsilon(a_1 + a_2) = \epsilon(a_1) + \epsilon(a_2) = a''_1 + a''_2$, па имамо да је $f(a''_1, b) = [a_1 \otimes b]$, $f(a''_2, b) = [a_2 \otimes b]$ и $f(a''_1 + a''_2, b) = [(a_1 + a_2) \otimes b]$. Стога

$$\begin{aligned}
&\overline{f}\big((a''_1 + a''_2, b) - (a''_1, b) - (a''_2, b)\big) = f(a''_1 + a''_2, b) - f(a''_1, b) - f(a''_2, b) \\
&= [(a_1 + a_2) \otimes b] - [a_1 \otimes b] - [a_2 \otimes b] = [a_1 \otimes b + a_2 \otimes b] - [a_1 \otimes b] - [a_2 \otimes b] \\
&\qquad = [a_1 \otimes b] + [a_2 \otimes b] - [a_1 \otimes b] - [a_2 \otimes b] = 0_P.
\end{aligned}$$

$$\begin{aligned}
\overline{f}\big((a'', b_1 + b_2) - (a'', b_1) - (a'', b_2)\big) &= f(a'', b_1 + b_2) - f(a'', b_1) - f(a'', b_2) \\
&= [a \otimes (b_1 + b_2)] - [a \otimes b_1] - [a \otimes b_2] = 0_P.
\end{aligned}$$

Уколико је $\epsilon(a) = a''$ и $s \in S$, онда је $\epsilon(as) = \epsilon(a)s = a''s$, па имамо да је $f(a'', b) = [a \otimes b]$ и $f(a''s, b) = [as \otimes b]$.

$$\overline{f}\big((as,b)-(a,sb)\big) = f(as,b)-f(a,sb) = [as\otimes b]-[a\otimes sb] = [a\otimes sb]-[a\otimes sb] = 0_P.$$

Дакле, $\overline{f}$ слика сваки елемент из $\mathcal{R}(A''\times B)$ у 0_P, што значи да добијамо да је и $\overline{f}\big(\sum_i(\epsilon(a_i), b_i)\big) = 0_P$. Но,

$$\overline{f}\big(\sum_i(\epsilon(a_i),b_i)\big) = \sum_i f(\epsilon(a_i),b_i) = \sum_i [a_i\otimes b_i] = \left[\sum_i (a_i\otimes b_i)\right],$$

што значи да $\sum_i(a_i\otimes b_i) \in \mathrm{Im}(\mu\otimes \mathrm{id}_B)$. □

Теорема 48. Нека $A, A_i \in_R\mathfrak{M}_S$, за $i \in I$; $B, B_i \in_S\mathfrak{M}_T$, за $i \in I$. Тада

$$\big(\bigoplus_{i\in I} A_i\big)\otimes_S B \cong \bigoplus_{i\in I}\big(A_i\otimes_S B\big) \text{ и } A\otimes_S\big(\bigoplus_{i\in I} B_i\big) \cong \bigoplus_{i\in I}(A\otimes_S B_i).$$

Доказ. Докажимо само први изоморфизам, други се доказује аналогно. Показаћемо да $\big(\big(\bigoplus_{i\in I} A_i\big)\otimes_S B; (q_k)_{k\in I}\big)$ испуњава услове дефиниције копроизвода (R,T)-бимодула $A_i\otimes_S B$, за погодно изабране хомоморфизме $q_k\colon A_i\otimes_S B \to \big(\bigoplus_{i\in I} A_i\big)\otimes_S B$, за $k \in I$. Најпре дефинишимо те хомоморфизме. Пођимо од функција $g_k\colon A_k\times B \to \big(\bigoplus_{i\in I} A_i\big)\otimes_S B)$ дефинисаних са $g_k(a_k, b) := (\overline{a_k})_{i\in I}\otimes b$, где је

$$(\overline{a_k})_i := \begin{cases} a_k, & i = k \\ 0_{A_i}, & i \neq k. \end{cases}$$

Напоменимо да овде користимо реализацију копроизвода модула A_i у облику подскупа производа $\prod_{i\in I} A_i$ у којима је само коначно много компонената различито од нуле, а операције су по координатама. Тада имамо јединствене хомоморфизме $\overline{g}_k\colon \mathcal{F}(A_k\times B) \to \big(\bigoplus_{i\in I} A_i\big)\otimes_S B$, такве да је $\overline{g}_k(a_k, b) = g_k(a_k, b)$ за све $(a_k, b) \in A_k\times B$. Као и раније, лако се провери да $\overline{g}_k$ слика све елементе из $\mathcal{R}(A_k\times B)$ у нулу, те добијамо индуковане хомоморфизме $q_k\colon A_k\otimes_S B \to \big(\bigoplus_{i\in I} A_i\big)\otimes_S B$.

Нека је $C \in_R\mathfrak{M}_T$, $\phi_i\colon A_i\otimes_S B \to C$ у $_R\mathfrak{M}_T$. Треба показати да постоји јединствен хомоморфизам $\phi\colon \big(\bigoplus_{i\in I} A_i\big)\otimes_S B \to C$ такав да је $\phi\circ q_i = \phi_i$ за све $i \in I$.

Најпре дефинишемо функцију $f\colon \big(\bigoplus_{i\in I} A_i\big)\times B \to C$ са: $f((a_i)_{i\in I}, b) := \sum_{i\in I}\phi_i(a_i\otimes b)$. Ова сума је коначна, јер је $a_i \neq 0$ само за коначно много $i \in I$. Понављамо добро нам познати поступак. Са $\mathcal{F}$ означимо слободну Абелову групу са групом генератора $\big(\bigoplus_{i\in I} A_i\big)\times B$, а са $\mathcal{R}$ подгрупу генерисану елементима из дефиниције 43. Задата функција f се на јединствен начин продужава до хомоморфизма $\overline{f}\colon \mathcal{F} \to C$ Абелових група. Генератори из $\mathcal{R}$ сликају се у 0_C.

$$\begin{aligned}
&\overline{f}\big(((a_i)_{i\in I}+(\bar{a}_i)_{i\in I},b)-((a_i)_{i\in I},b)-((\bar{a}_i)_{i\in I},b)\big)\\
&\qquad\qquad = f\big((a_i)_{i\in I}+(\bar{a}_i)_{i\in I},b\big)-f\big((a_i)_{i\in I},b\big)-f\big((\bar{a}_i)_{i\in I},b\big)\\
&\qquad\qquad = f\big((a_i+\bar{a}_i)_{i\in I},b\big)-f\big((a_i)_{i\in I},b\big)-f\big((\bar{a}_i)_{i\in I},b\big)\\
&\qquad\qquad = \sum_{i\in I}\phi_i((a_i+\bar{a}_i)\otimes b)-\sum_{i\in I}\phi_i(a_i\otimes b)-\sum_{i\in I}\phi_i(\bar{a}_i\otimes b)\\
&\qquad\qquad = \sum_{i\in I}\big(\phi_i(a_i\otimes b+\bar{a}_i\otimes b)-\phi_i(a_i\otimes b)-\phi_i(a_i\otimes b)\big)=\\
&\qquad\qquad\qquad \sum_{i\in I}\big(\phi(a_i\otimes b)+\phi_i(\bar{a}_i\otimes b)-\phi_i(a_i\otimes b)-\phi_i(\bar{a}_i\otimes b)\big)=0_C.
\end{aligned}$$

Проверу за друга два типа генератора остављамо читаоцима. Стога $\overline{f}$ индукује хомоморфизам Абелових група $\phi\colon \mathcal{F}/\mathcal{R}\to C$. Како је $\mathcal{F}/\mathcal{R}$ заправо $\big(\bigoplus_{i\in I}A_i\big)\otimes_S B$, то смо добили $\phi\colon \big(\bigoplus_{i\in I}A_i\big)\otimes_S B\to C$, за који је $\phi((a_i)_{i\in I}\otimes b)=\sum_{i\in I}\phi_i(a_i\otimes b)$. Приметимо да је

$$(\phi\circ q_k)(a_k\otimes b)=\phi(q_k(a_k\otimes b))=\phi((\overline{a_k})_{i\in I}\otimes b)=\sum_{i\in I}\phi_i((\overline{a_k})_i\otimes b)=\phi_k(a_k\otimes b),$$

па је $\phi\circ q_k=\phi_k$ за све $k\in I$. Јасно је да је ϕ овако јединствено задато. Наиме, ако је ϕ' други хомоморфизам који задовољава услов $\phi'\circ q_k=\phi_k$ за све $k\in I$, онда, за адитивни генератор $(a_i)_{i\in I}\otimes b$ најпре приметимо да је $a_i\neq 0$ само за коначно много индекса i. Нека су то $i_1,\ldots,i_s$. Но, тада је $(a_i)_{i\in I}$ збир од s елемената код којих је компонента различита од 0 тачно на једној позицији; прецизно: $(a_i)_{i\in I}=\sum_{l=1}^{s}\overline{a_{i_s}}$. Добијамо да је

$$\begin{aligned}
\phi'((a_i)_{i\in I}\otimes b)&=\sum_{l=1}^{s}\phi'(\overline{a_{i_l}}\otimes b)=\sum_{l=1}^{s}\phi'(q_{i_l}(a_{i_l})\otimes b)\\
&\qquad\qquad=\sum_{l=1}^{s}(\phi'\circ q_{i_;})(a_{i_l}\otimes b)=\sum_{l=1}^{s}\phi_{i_l}(a_{i_l}\otimes b)=\phi((a_i)_{i\in I}\otimes b),
\end{aligned}$$

па се добија да је $\phi'=\phi$ на адитивним генераторима, те је стога $\phi'=\phi$.

Остаје да се провери да је ϕ хомоморфизам (R,T)-бимодула.

$$\begin{aligned}
&\phi\Big(r\cdot\big((a_i)_{i\in I}\otimes b\big)\Big)=\phi\big((ra_i)_{i\in I}\otimes b\big)=\sum_{i\in I}\phi_i(ra_i\otimes b)\\
&=\sum_{i\in I}\phi_i(r\cdot(a_i\otimes b))=\sum_{i\in I}r\phi(a_i\otimes b)=r\cdot\sum_{i\in I}\phi_i(a_i\otimes b)=r\cdot\phi\big((a_i)_{i\in I}\otimes b\big).
\end{aligned}$$

Проверите за вежбу слагање са множењем здесна елементима из T. $\square$

Пример 49. Посматрајмо категорију Set свих скупова и функција међу њима. Тада имамо природну бијекцију између $Set(X \times Y, Z)$ и $Set(X, Set(Y, Z))$. Наиме, свакој функцији $f\colon X \times Y \to Z$ можемо придружити функцију $f^\sharp\colon X \to Set(Y, Z)$ са $f^\sharp(x)(y) := z$. Није тешко уверити се да је ово бијекција. Природност се састоји у следећем. Ако су X', Y', Z' неки други скупови и $\alpha\colon X' \to X$, $\beta\colon Y' \to Y$, $\gamma\colon Z \to Z'$, бијекције за тројке (X, Y, Z) и (X', Y', Z') лепо се слажу са овим функцијама у следећем смислу. Ако је $f \in Set(X \times Y, Z)$, онда јој можемо придружити функцију $\gamma \circ f \circ (\alpha \times \beta) \in Set(X' \times Y', Z')$, где смо са $\alpha \times \beta$ означили која $X \times Y$ слика у $X' \times Y'$ тако што (x, y) слика у $(\alpha(x), \beta(y))$. Слично, функцији g из $Set(X, Set(Y, Z))$ можемо придружити функцију из $Set(X', Set(Y', Z'))$ дефинисану са: $x' \mapsto \gamma \circ g(\alpha(x')) \circ \beta$. Означимо са

$$\Phi_{(X,Y,Z)}\colon Set(X \times Y, Z) \to Set(X, Set(Y, Z))$$

горенаведену бијекцију. Тада је, за све $f \in Set(X \times Y, Z)$ и $x' \in X'$:

$$\Phi_{(X',Y',Z')}\big(\gamma \circ f \circ (\alpha \times \beta)\big)(x') = \gamma \circ \Phi_{(X,Y,Z)}(f)\big(\alpha(x')\big) \circ \beta. \qquad (19)$$

Ово изгледа знатно компликованије него што у суштини јесте. Поента је да је горња бијекција дефинисана независно од било каквих избора у скуповима о којима је реч и зато се слаже са разним композицијама.

Проверимо једнакост (19). По дефиницији имамо да је, за $y' \in Y'$:

$$\Phi_{(X',Y',Z')}\big(\gamma \circ f \circ (\alpha \times \beta)\big)(x')(y') = (\gamma \circ f \circ (\alpha \times \beta))(x', y') = \gamma(f(\alpha(x'), \beta(y'))).$$

С друге стране, за $y' \in Y$:

$$(\gamma \circ \Phi_{(X,Y,Z)}(f)\big(\alpha(x')\big) \circ \beta)(y') = \gamma(\Phi_{X,Y,Z}(f)(\alpha(x')(\beta(y')) = \gamma(f(\alpha(x'), \beta(y'))).$$

Дакле, једнакост заиста важи.

Разлог зашто смо узимали, на пример, да α слика X' у X, а γ Z у Z' лежи у томе што такво α, за свако Z, индукује пресликавање из $Set(X, Z)$ у $Set(X', Z)$, док γ за свако X индукује пресликавање из $Set(X, Z)$ у $Set(X, Z')$. Кратко, $Set(-, -)$ је контраваријантно (обрће стрелице) по првој, а коваријантно по другој компоненти.

Из ових разлога, ако фиксирамо Y и посматрамо два функтора $X \mapsto X \times Y$ и $Z \mapsto Set(Y, Z))$ (уз јасно дефинисана и придруживања функција), онда наведена природна бијекција говори да је први функтор лево адјунгован другом функтору, односно, да је други функтор десно адјунгован првом функтору. ♣

Својство да неки функтор има њему десно (или лево) адјунгован функтор му даје извесне особине, али се ми тиме нећемо детаљно бавити због ограничености времена. Само наводимо важну везу између функтора $- \otimes_S B$ и $\mathrm{Hom}_T(B, -)$: први је лево адјунгован другом, односно важи следећа теорема.

Теорема 50. Нека $B \in {}_S\mathfrak{M}_T$. Тада постоји природан изоморфизам Абелових група

$$\mathrm{Hom}_{(R,T)}(A \otimes_S B, C) \cong \mathrm{Hom}_{(R,S)}(A, \mathrm{Hom}_T(B, C)),$$

где $A \in {}_R\mathfrak{M}_S$ и $C \in {}_R\mathfrak{M}_T$.

Доказ. Нека је $\theta \in \mathrm{Hom}_{(R,T)}(A \otimes_S B, C)$. Дефишемо

$$\Phi_{(A,B,C)}(\theta) \in \mathrm{Hom}_{(R,S)}(A, \mathrm{Hom}_T(B, C))$$

са: $\big(\Phi_{(A,B,C)}(\theta)(a)\big)(b) := \theta(a \otimes b)$. Треба показати неколико ствари.

Најпре,

$\mathbf{\Phi_{(A,B,C)}}(\theta)$ је хомоморфизам $(\mathbf{R}, \mathbf{S})$-бимодула. Нека $a \in A$, $b \in B$.

$$\begin{aligned}
\big(\Phi_{(A,B,C)}(\theta)(ra)\big)(b) &= \theta((ra) \otimes b) \\
&= \theta(r(a \otimes b)) \text{ по дефиницији структуре } R\text{-модула на } A \otimes_S B \\
&= r\theta(a \otimes b), \text{ јер је } \theta \text{ хомоморфизам } (S, T)\text{-модула} \\
&= r\big(\Phi_{(A,B,C)}(\theta)(a)\big)(b) = \big(r \cdot \Phi_{(A,B,C)}(\theta)(a)\big)(b),
\end{aligned}$$

па је $\Phi_{(A,B,C)}(\theta)(r \cdot a) = r \cdot \Phi_{(A,B,C)}(\theta)(a)$. Овде треба напоменути да се структура (R, S)-бимодула на $\mathrm{Hom}_T(B, C)$ задаје са:

$$(r \cdot \phi)(b) := r(\phi(b)), \quad (\phi \cdot s)(b) := \phi(sb).$$

Проверите да је овако заиста задата структура (R, S)-бимодула на $\mathrm{Hom}_T(B, C)$ и упоредите са тиме како задајемо бимодулску структуру у случају хомоморфизама левих модула (почетак одељка о функтору Hom).

$$\begin{aligned}
\big(\Phi_{(A,B,C)}(\theta)(as)\big)(b) &= \theta(as \otimes b) = \theta(a \otimes sb) = \big(\Phi_{(A,B,C)}(\theta)(a)\big)(sb) \\
&= \big(\Phi_{(A,B,C)}(\theta)(a) \cdot s\big)(b) \text{ (по структури бимодула на } \mathrm{Hom}_T(B, C)),
\end{aligned}$$

па је $\Phi_{(A,B,C)}(\theta)(as) = \Phi_{(A,B,C)}(\theta)(a) \cdot s$.

$$\begin{aligned}
\big(\Phi_{(A,B,C)}(\theta)(a_1 + a_2)\big)(b) &= \theta((a_1 + a_2) \otimes b) = \theta(a_1 \otimes b + a_2 \otimes b) \\
&= \theta(a_1 \otimes b) + \theta(a_2 \otimes b) = \big(\Phi_{(A,B,C)}(\theta)(a_1)\big)(b) + \big(\Phi_{(A,B,C)}(\theta)(a_2)\big)(b) \\
&= \big(\Phi_{(A,B,C)}(\theta)(a_1) + \Phi_{(A,B,C)}(\theta)(a_2)\big)(b),
\end{aligned}$$

па је $\Phi_{(A,B,C)}(\theta)(a_1 + a_2) = \Phi_{(A,B,C)}(\theta)(a_1) + \Phi_{(A,B,C)}(\theta)(a_2)$.

$\mathbf{\Phi_{(A,B,C)}}(\theta)(\mathbf{a})$ је хомоморфизам десних T-модула.

$$\begin{aligned}
\big(\Phi_{(A,B,C)}(\theta)(a)\big)(b_1 + b_2) &= \theta(a \otimes (b_1 + b_2)) = \theta(a \otimes b_1 + a \otimes b_2) \\
&= \theta(a \otimes b_1) + \theta(a \otimes b_2) = \big(\Phi_{(A,B,C)}(\theta)(a)\big)(b_1) + \big(\Phi_{(A,B,C)}(\theta)(a)\big)(b_2).
\end{aligned}$$

$$\big(\Phi_{(A,B,C)}(\theta)(a)\big)(a)(bt) = \theta(a \otimes bt) = \theta((a \otimes b)t)$$
$$= \theta(a \otimes b)t = \big(\Phi_{(A,B,C)}(\theta)(a)\big)(b)t.$$

$\mathbf{\Phi_{(A,B,C)}}$ је хомоморфизам Абелових група.

$$\big(\Phi_{(A,B,C)}(\theta_1 + \theta_2)(a)\big)(b) = (\theta_1 + \theta_2)(a \otimes b)$$
$$= \theta_1(a \otimes b) + \theta_2(a \otimes b) = \big(\Phi_{(A,B,C)}(\theta_1)(a)\big)(b) + \big(\Phi_{(A,B,C)}(\theta_2)(a)\big)(b),$$

па је $\Phi_{(A,B,C)}(\theta_1 + \theta_2) = \Phi_{(A,B,C)}(\theta_1) + \Phi_{(A,B,C)}(\theta_2)$.

$\mathbf{\Phi_{(A,B,C)}}$ је „1–1”. Нека је $\Phi_{(A,B,C)}(\theta) = 0_{\mathrm{Hom}_{(R,S)}(A,\mathrm{Hom}_T(B,C))}$. То значи да је за свако $a \in A$: $\Phi_{(A,B,C)}(\theta)(a) = 0_{\mathrm{Hom}_T(B,C)}$. Те је за свако $a \in A$ и свако $b \in B$: $\big(\Phi_{(A,B,C)}(\theta)(a)\big)(b) = 0_C$, тј. за $\theta(a \times b) = 0$ за све $a \in A$, $b \in B$. Како су ово адитивни генератори од $A \otimes_S B$, то закључујемо да је $\theta = 0_{\mathrm{Hom}_{(R,T)}(A \otimes_S B, C)}$.

$\mathbf{\Phi_{(A,B,C)}}$ је „на”. Нека $\xi \in \mathrm{Hom}_{(R,S)}(A, \mathrm{Hom}_T(B,C))$. Дефинишимо $f\colon A \times B \to C$ са: $f(a,b) := \xi(a)(b)$. Ако је $\overline{f}\colon \mathcal{F}(A \times B) \to C$ јединствен хомоморфизам Абелових група који проширује f, проверимо да слика све елементе из $\mathcal{R}(A \times B)$ у нулу.

$$\overline{f}\big((a_1 + a_2, b) - (a_1, b) - (a_2, b)\big) = f(a_1 + a_2, b) - f(a_1, b) - f(a_2, b)$$
$$= \xi(a_1 + a_2)(b) - \xi(a_1)(b) - \xi(a_2)(b) = (\xi(a_1) + \xi(a_2))(b) - \xi(a_1)(b) - \xi(a_2)(b)$$
$$= \xi(a_1)(b) + \xi(a_2)(b) - \xi(a_1)(b) - \xi(a_2)(b) = 0_C.$$

Лако се добија и да је $\overline{f}\big((a, b_1 + b_2) - (a, b_1) - (a, b_2)\big) = 0_C$.

$$\overline{f}\big((as, b) - (a, sb)\big) = f(as, b) - f(a, sb) = \xi(as)(b) - \xi(a)(sb)$$
$$= (\xi(a) \cdot s)(b) - \xi(a)(sb), \text{ јер је } \xi \text{ хомоморфизам десних } S\text{-модула}$$
$$= \xi(a)(sb) - \xi(a)(sb)$$
$$\text{(по дефиницији структуре десног } S\text{-модула на } \mathrm{Hom}_T(B,C)) = 0_C.$$

Дакле, $\overline{f}$ индукује хомоморфизам Абелових група $\theta\colon A \otimes B \to C$ и може се проверити да је то хомоморфизам (R,T)-модула. Како је, по самој дефиницији $\theta(a \otimes b) = f(a,b) = \xi(a)(b)$, то је $\Phi_{(A,B,C)}(\theta) = \xi$.

Прецизно разјашњење природности и проверу остављамо читаоцима за вежбу, јер је потпуно аналогно примеру за скупове. □

Задатак за вежбу.

Доказати да тачност низа R-модула

$$A' \xrightarrow{\mu} A \xrightarrow{\epsilon} A'' \to 0 \tag{20}$$

следи из тачности низа

$$0 \to \mathrm{Hom}_R(B, A') \xrightarrow{\mu_*} \mathrm{Hom}_R(B, A) \xrightarrow{\epsilon_*} \mathrm{Hom}_R(B, A'') \tag{21}$$

за сваки R-модул B, а следи такође и из тачности

$$0 \to \mathrm{Hom}_R(A'', B) \xrightarrow{\epsilon^*} \mathrm{Hom}_R(A, B) \xrightarrow{\mu^*} \mathrm{Hom}_R(A', B) \tag{22}$$

за сваки R-модул B. ♠

Размислите како бисте могли да искористите овај задатак и претходну теорему да докажете теореме 47 и 48.

5 Пројективни модули

Дефинишимо најпре слободне модуле.

Дефиниција 51. Нека је X неки скуп. Слободни леви R-модул на скупу X састоји се од левог R-модула F и функције $j\colon X \to F$ тако да важи следеће. За сваки леви R-модул A и функцију $f\colon S \to A$ постоји тачно један хомоморфизам левих R-модула $\overline{f}\colon F \to A$ такав да је $\overline{f} \circ j = f$.

Став 52. Функција j је „1–1" и њена слика $j[X]$ генерише F.

Доказ. Претпоставимо да постоје $x_1 \neq x_2$ у X за које је $j(x_1) = j(x_2)$. За модул A узмимо R као стандардни леви R-модул, а функцију $f\colon X \to R$ дефинишимо са: $f(x_1) = 1$, $f(x) = 0$ за $x \neq x_1$. Уколико би постојала функција $\overline{f}\colon F \to R$ таква да је $\overline{f} \circ j = f$, онда бисмо имали да је $1 = f(x_1) = \overline{f}(j(x_1)) = \overline{f}(j(x_2)) = f(x_2) = 0$.

Уколико $j[X]$ НЕ генерише F, посматрајмо подмодул од F генерисан овим скупом; означимо га са F'. Тада је $F/F' \neq 0$, и постојала би два различита хомоморфизма $\phi, \psi\colon F \to F/F'$ за које је $\phi \circ j = \psi \circ j = 0$. Наиме, за ϕ можемо узети 0, а за ψ канонску пројекцију F на F/F'. Ово противречи дефиницији, па закључујемо да $j[X]$ генерише F. □

Често ћемо и само модул F називати слободним модулом због једноставности изражавања (подразумевајући да постоји и функција j), а и сам скуп X скупом генератора за F (скуп X можемо заменити скупом $j[X]$ и тако постићи да је тај скуп баш подскуп од F). Слободан леви R-модул је јединствен до на изоморфизам.

Став 53. Нека, за скуп X, парови (F, j) и (F', j') испуњавају услове из дефиниције 51. Тада постоји изоморфизам $\phi\colon F \to F'$ такав да је $\phi \circ j = j'$.

Доказ. Како је (F, j) слободан леви R-модул, то за функцију $j'\colon X \to F'$ постоји хомоморфизам $\overline{j'}\colon F \to F'$ тако да је $\overline{j'} \circ j = j'$. На аналоган начин добијамо и хомоморфизам $\overline{j}\colon F' \to F$ за који је $\overline{j} \circ j' = j$. Но, тада имамо да је $(\overline{j} \circ \overline{j'}) \circ j = j$, но такође је и $\mathrm{id}_F \circ j = j$. Због јединствености у дефиницији 51 закључујемо да је $\overline{j} \circ \overline{j'} = \mathrm{id}_F$. Слично се добија да је и $\overline{j'} \circ \overline{j} = \mathrm{id}_{F'}$, па су $\overline{j}$ и $\overline{j'}$ изоморфизми. За тражено ϕ, узимамо да је $\phi = \overline{j'}$. $\square$

Треба још показати да слободни леви модули постоје. Покажимо да модул $\overline{F} := \bigoplus_{x \in X} R$ испуњава својства из дефиниције 51 за погодан избор функције $j\colon X \to \overline{F}$

Став 54. Ако је $j\colon X \to \overline{F}$ задата са $j(x') := (\overline{(1_R)_{x'}})_{x\in G}$, онда је пар $(\overline{F}, j)$ слободан леви R-модул.

Доказ. Подсетимо се (видети доказ теореме 48) да је $(\overline{(1_R)_{x'}})_x = 0_R$, за $x \neq x'$, а $(\overline{(1_R)_{x'}})'_x = 1_R$. Краће: ово је елемент који на позицији x' има 1_R, а на свим осталим 0_R. Тада, ако је задат модул A и функција $f\colon X \to A$, јединствени хомоморфизам $\overline{f}\colon \overline{F} \to A$ за који је $\overline{f} \circ j = f$ дат је са: $\overline{f}\big((r_x)_{x\in G}\big) := \sum_{x\in X} r_x f(x)$. Уверите се у то. $\square$

Следећи став нам указује на сличност са појмом векторског простора и његове базе. Заправо су слободни модули они који имају базу, тј. генераторни скуп који је линеарно независан. Сваки векторски простор има базу, али наравно да је немају сви модули.

Став 55. Нека је X скуп генератора левог R-модула B. Тада је B слободан модул на скупу X ако и само ако је X линеарно независан над R, тј. ако и само ако из једнакости

$$r_1x_1 + r_2x_2 \cdots + r_nx_n = 0_B$$

следи да је $r_1 = r_2 = \cdots = r_n = 0_R$.

Доказ. Претпоставимо најпре да је B слободан модул са базом X. Посматрајмо једнакост

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0_B$$

Дефинишимо $f\colon X \to R$ са: $f(x_1) = 1_R$, $f(x) = 0_R$ за све $x \neq x_1$. Тада постоји јединствен хомоморфизам $\overline{f}\colon B \to R$ за који је $\overline{f}(x) = f(x)$. Ако тај хомоморфизам применимо на горњу једнакост, добијамо:

$$\begin{aligned} 0_R = \overline{f}(0_B) &= \overline{f}(r_1x_1 + r_2x_2 \cdots + r_nx_n) = r_1\overline{f}(x_1) + r_2\overline{f}(x_2) \cdots + r_n\overline{f}(x_n) \\ &= r_1f(x_1) + r_2f(x_2) + \cdots + r_nf(x_n) = r_1 \cdot 1_R + r_2 \cdot 0_R + \cdots + r_n \cdot 0_R = r_1. \end{aligned}$$

Тако добијамо да је $r_1 = 0_R$ и слично и за остале бирањем погодних функција f.

Претпоставимо сада да базу X чине линеарно независни елементи. Покажимо да је B слободан. У ту сврху, нека је C неки леви R-модул и $f\colon X \to C$ нека функција. Ако је $b \in B \setminus \{0_B\}$, онда постоје (различити) $x_1, \ldots, x_m \in X$ такви да је $b = r_1x_1 + \cdots + r_mx_m$ за неке $r_i \in R \setminus \{0\}$. Но, ако би постојали и неки други (различити) елементи из G: $x'_1, \ldots, x'_n$ тако да је $b = r'_1 x'_1 + \cdots r'_n x'_n$, за неке $r'_i \in R \setminus \{0\}$, онда бисмо имали једнакост

$$r_1 x_1 + \cdots + r_m x_m = r'_1 x'_1 + \cdots + r'_n x'_n.$$

Ако би за неки индекс i важило да $x_i \notin \{x'_1, \ldots, x'_n\}$, онда бисмо, после пребацивања свих сабирака на једну страну, имали линеарну комбинацију елемената из X која би била једнака нули, али један од коефицијената није нула. Стога сваки елемент из $\{x_1, \ldots, x_n\}$ припада скупу $\{x'_1, \ldots, x'_m\}$. Но, важи и обратно, аналогним резоновањем. Закључујемо да су ово једнаки скупови и горња једнакост се своди на

$$(r_1 - r'_1)x_1 + \cdots + (r_n - r'_n)x_n = 0_B.$$

Из линеарне независности елемената из X следи да је $r_i - r'_i = 0_R$ за све i, те закључујемо да је приказ сваког елемента из $B \setminus \{0_B\}$ у облику линеарне комбинације генераторних јединствен. Стога можемо, на тачно један начин, дефинисати $\overline{f}\colon B \to C$ са: $\overline{f}(r_1 b_1 + \cdots + r_n b_n) := r_1 f(b_1) + \cdots + r_n f(b_n)$ и, наравно, $\overline{f}(0_B) = 0_C$. На стандардан начин се провери да је ово хомоморфизам левих R-модула. $\square$

Теорема 56. Сваки леви R-модул је хомоморфна слика слободног левог R-модула.

Доказ. Нека је A леви R-модул и F слободан леви R-модул са скупом генератора A. Идентитет $\mathrm{id}_A\colon A \to A$ индукује хомоморфизам левих R-модула $\overline{\mathrm{id}_A}\colon F \to A$, који је очигледно „на”. $\square$

Једно важно својство слободних модула, садржано у следећем ставу ће нам бити мотивација за увођење главног појма у овом одељку.

Став 57. Нека је F слободан леви R-модул, $A \xrightarrow{\epsilon} A'' \to 0$ тачан низ левих R-модула и $\phi\colon F \to A''$ хомоморфизам левих R-модула. Тада постоји хомоморфизам левих R-модула $\psi\colon F \to A$ такав да је $\epsilon \circ \psi = \phi$.

Доказ. Наравно, тачност низа $A \xrightarrow{\epsilon} A'' \to 0$ је еквивалентна услову да је ϵ „на” (али, ето може и тако да се то формулише ☺).

$$\begin{tikzcd} & F \arrow[dl, dashed, "\psi"'] \arrow[d, "\phi"] & \\ A \arrow[r, "\epsilon"] & A'' \arrow[r] & 0 \end{tikzcd}$$

Нека је X база за F. За сваки $x \in X$ изаберимо $a_x \in A$ такав да је $\epsilon(a_x) = \phi(x)$; ово можемо да урадимо зато што је ϵ „на” (наравно, користимо и аксиому избора). Тако имамо задату функцију $f\colon X \to A$: $f(x) := a_x$. Како је F слободан са базом X, то постоји (тачно један) хомоморфизам $\psi = \overline{f}\colon F \to A$ за који је $\psi(x) = f(x) = a_x$ за све $x \in X$. Стога је $(\epsilon \circ \psi)(x) = \epsilon(\psi(x)) = \epsilon(a_x) = \phi(x)$. Дакле, $(\epsilon \circ \psi)|_X = \phi|_X\colon X \to A$ па, због јединствености хоморфизма задатог на бази, добијамо да је $\epsilon \circ \psi = \phi$ чиме је доказ завршен. $\square$

Дефиниција 58. За леви R-модул P кажемо да је ПРОЈЕКТИВАН ако за сваки тачан низ $A \xrightarrow{\epsilon} A'' \to 0$ тачан низ левих R-модула ихомоморфизам левих R-модула $\phi\colon P \to A''$ постоји хомоморфизам левих R-модула $\psi\colon P \to A$ такав да је $\epsilon \circ \psi = \phi$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"'] \arrow[d, "\phi"] & \\ A \arrow[r, "\epsilon"] & A'' \arrow[r] & 0 \end{tikzcd}$$

Дакле, видели смо да је сваки слободан модул пројективан. Заправо је пројективност модула, која је слабији услов од „слободе", довољна за многе конструкције у хомолошкој алгебри, но ми се тиме нећемо бавити, овде се бавимо само основним својствима и примерима.

Став 59. Директна сума $\bigoplus_i P_i$ је пројективан модул ако и ако су сви модули P_i пројективни.

Доказ. Нека је $P = \bigoplus_i P_i$ пројективан модул и нека су задати тачан низ $A \xrightarrow{\epsilon} A'' \to 0$ и хомоморфизам $\phi_j\colon P_j \to A''$, за $j \in I$. Уколико задамо $\phi_i\colon P_i \to A''$ за $i \neq j$ са $\phi_i = 0$, имамо индуковани хомоморфизам $\phi\colon P \to A''$ за који је $\phi|_{P_j} \circ q_j = \phi_j$, где су q_i хомоморфизми који су део структуре директне суме. Како је P пројективан, то постоји $\psi\colon P \to A$ тако да је $\epsilon \circ \psi = \phi$. Но, тада је $\epsilon \circ (\psi \circ q_j) = (\epsilon \circ \psi) \circ q_j = \phi \circ q_i = \phi_j$, па је $\psi \circ q_j$ тражени хомоморфизам.

Ако су сви P_i пројективни модули, посматрајмо $\phi\colon P \to A''$ (и исти тачан низ наравно). Тада за све $\phi_i = \phi \circ q_i\colon P_i \to A''$ постоје $\psi_i\colon P_i \to A$ такви да је $\epsilon \circ \psi_i = \phi_i$, пошто су P_i пројективни. Но, тада постоји $\psi\colon P \to A$ тако да је $\psi \circ q_i = \psi_i$ за све i. Тада је

$$(\epsilon \circ \psi) \circ q_i = \epsilon \circ (\psi \circ q_i) = \epsilon \circ \psi_i = \phi_i = \phi \circ q_i,$$

за све i. Из јединствености хомоморфизма у дефиницији копроизвода следи да је $\epsilon \circ \psi = \phi$. $\square$

Наведимо неке примере базиране на овом ставу и чињеници да су слободни модули пројективни.

Пример 60. Како је $\mathbb{Z}_6 \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_3$, као Абелове групе, овај изоморфизам је и изоморфизам $\mathbb{Z}_6$-модула (свака Абелова група је $\mathbb{Z}$-модул, а Абелова група A је $\mathbb{Z}_n$-модул акко је $nA = 0$). Но, $\mathbb{Z}_6$ је наравно слободан $\mathbb{Z}_6$-модул, па су онда и $\mathbb{Z}_2$ и $\mathbb{Z}_3$ пројективни $\mathbb{Z}_6$-модули, који, наравно, нису слободни (иначе би били директне суме од $\mathbb{Z}_6$, а то свакако нису из баналних разлога – имају премало елемената ☺). ♣

Пример 61. Нека је $S = M_n(R)$, прстен матрица реда n над прстеном са јединицом R. Подсетите се примера 15. Леви идеали из дела под б) у директној суми дају прстен S:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_{12} & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & 0 & \cdots & a_{1n} \\ 0 & 0 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix},$$

па су сви они пројективни S-модули који нису слободни.

Став 62. Леви R-модул P је пројективан акко је функтор $\mathrm{Hom}_R(P,-)\colon {}_R\mathfrak{M} \to \mathfrak{Ab}$, где је са $\mathfrak{Ab}$ означена категорија Абелових група и хомоморфизама, тачан.

Доказ. Знамо да је овај функтор лево тачан по теореми 42. Остаје само да се провери да се хомоморфизми који су „на” преводе у хомоморфизме који су „на” акко је P пројективан. Али, то је таутолошка чињеница – то је само преформулација дефиниције пројективног модула. Уверите се у то. □

Теорема 63. Следећи услови за леви R-модул P су еквивалентни.

(1) P је пројективан.

(2) Сваки кратак тачан низ $0 \to A' \to A \to P \to 0$ се цепа.

(3) P је директан сабирак слободног модула.

Доказ. (1)$\Longrightarrow$(2). Посматрајмо десни крај овог тачног низа и нека је $\epsilon\colon A \to P$. Довољно је у дефиницији пројективног модула узети да је $\phi = \mathrm{id}_P$. Тада постоји $\psi\colon P \to A$ такав да је $\epsilon \circ \psi = \mathrm{id}_P$.

(2)$\Longrightarrow$(3). Модул P је слика слободног модула F при хомоморфизму p и нека је $K = \mathrm{Ker}\, p$. На основу претпоставке (2), кратак тачан низ $0 \to K \to F \xrightarrow{p} P \to 0$ се цепа, па је $F \cong P \bigoplus Q$ за неки леви R-модул P.

(3)$\Longrightarrow$(1). Ово следи из чињенице да је слободан модул пројективан и става 59. □

У ставу 62 видели смо везу пројективних модула и функтора Hom. Погледајмо сада везу са тензорским производом. Најпре дефинишемо појам равног модула.

Дефиниција 64. Леви R-модул B је РАВАН уколико је функтор $- \otimes_R B$ тачан.

Наравно, уколико је A десни R-модул, онда је $A \otimes_R B$ само Абелова група, а ако је A један (S,R)-бимодул, онда је $A \otimes_R B$ леви S-модул. Дакле, постоји више могућности за овај функтор, но ако је R комутативан прстен онда је $A \otimes_R B$свакако R-модул.

Теорема 65. Пројективни модули су равни.

Доказ. Докажимо најпре да су слободни модули равни. Дакле, ако је $\mu\colon A' \to A$ „1–1", треба показати да је и $\mu \otimes \mathrm{id}_F\colon A' \otimes_R F \to A \otimes_R F$ „1–1" ако је F слободан леви R-модул. Знамо да је тада $F \cong \bigoplus_{i\in I} R$ за неки скуп индекса I. На основу теореме 48 и става 46, знамо да је $A' \otimes_R F \cong \bigoplus_{i\in I} A'$; аналогно за A. Претпоставимо да је F реализован као подмодул директног производа R-ова тако да је у $(r_i)_{i\in I}$ $r_i \neq 0$ само за коначно много индекса $i \in I$. Тада је изоморфизам $\phi'\colon A' \otimes_R \bigoplus_{i\in I} R \to \bigoplus_{i\in I} A'$, на адитивним генераторима, задат са $\phi'\big(a' \otimes (r_i)_{i\in I}\big) = (a'r_i)_{i\in I}$. Слично је $\phi\big(a \otimes (r_i)_{i\in I}\big) = (ar_i)_{i\in I}$, док је $(\mu \otimes \mathrm{id}_{\bigoplus_{i\in I} R})(a' \otimes (r_i)_{i\in I}) = \mu(a') \otimes (r_i)_{i\in I}$. Стога овај хомоморфизам индукује хомоморфизам $M\colon \bigoplus_{i\in I} A' \to \bigoplus_{i\in I} A$ (за који је $M \circ \phi' = \phi \circ (\mu \otimes \mathrm{id}_{\bigoplus_{i\in I} R})$), $M((a_i')_{i\in I}) = (\mu(a_i'))_{i\in I}$:

$$\begin{aligned}(M \circ \phi')(a' \otimes (r_i)_{i\in I}) &= M(\phi'(a' \otimes (r_i)_{i\in I}) = M((a'r_i)_{i\in I}) \\ &= (\mu(a'r_i))_{i\in I} = (\mu(a')r_i)_{i\in i} = \phi(\mu(a') \otimes (r_i)_{i\in I}) \\ = \phi\big((\mu \otimes \mathrm{id}_{\bigoplus_{i\in I} R})&(a' \otimes (r_i)_{i\in I}\big) = (\phi \circ (\mu \otimes \mathrm{id}_{\bigoplus_{i\in I} R}))(a' \otimes (r_i)_{i\in I}).\end{aligned}$$

Уколико је $M\big((a_i')_{i\in I}\big) = 0_{\bigoplus_{i\in I} A}$, то значи да је $\mu(a_i') = 0_A$ за све i, те, из инјективности μ, следи да је $a_i' = 0_{A'}$ за све i, тј. $(a_i')_{i\in I} = 0_{\bigoplus_{i\in} A}$ те закључујемо да је M „1–1", те онда мора бити и $\mu \otimes \mathrm{id}_{\bigoplus_{i\in I} R}$. Дакле, добили смо да је слободан модул раван.

Нека је P пројективни модул. Тада је $P \bigoplus Q = F$ за неки модул Q и слободан модул F. Означимо са $\iota\colon P \to F$ укључење P у F, а са $\pi\colon F \to P$ пројекцију F на P. Тада је $\pi \circ \iota = \mathrm{id}_P$. Нека је $(\mu \otimes \mathrm{id}_{\mathrm{P}})(x') = 0$ за неки $x' \in A' \otimes P$. Тада је и $(\mathrm{id}_A \otimes \iota)(\mu \otimes \mathrm{id}_{\mathrm{P}})(x') = 0$. Но,

$$(\mathrm{id}_A \otimes \iota) \circ (\mu \otimes \mathrm{id}_{\mathrm{P}}) = \mu \otimes \iota = (\mu \otimes \mathrm{id}_F) \circ (\mathrm{id}_{A'} \otimes \iota),$$

па је $(\mu \otimes \mathrm{id}_F)\big((\mathrm{id}_{A'} \otimes \iota)(x')\big) = 0$. Но, $\mu \otimes \mathrm{id}_F$ је „1–1", јер је F слободан, па добијамо да је $(\mathrm{id}_{A'} \otimes \iota)(x') = 0$. Тада је и $(\mathrm{id}_{A'} \otimes \pi)((\mathrm{id}_{A'} \otimes \iota)(x')) = 0$. Но $(\mathrm{id}_{\mathrm{A'}} \otimes \pi) \circ (\mathrm{id}_{A'} \otimes \iota) = \mathrm{id}_{A'} \otimes (\pi \circ \iota) = \mathrm{id}_{A'} \otimes \mathrm{id}_P = \mathrm{id}_{A' \otimes P}$, па је $x' = 0$ и добили смо тражено. □

Обрат не важи, тј. није сваки раван модул пројективан. Пре него што дамо пример, приметимо да важи следеће. Елемент $a_1 \otimes b_1 + \cdots + a_n \otimes b_n \in A \otimes_R B$ је једнак $0_{A\otimes_R B}$ ако и само ако је он једнак $0_{A' \otimes_R B'}$ за неке коначно генерисане подмодуле A' и B'. Наиме, овај елемент је једнак нули у тензорском производу акко елемент $(a_1, b_1) + \cdots + (a_n, b_n)$ припада подгрупи $\mathcal{R}(A \times B)$. Другим речима, то значи да је

$$\begin{aligned}&\sum_{i=1}^{n} (a_i, b_i) = \sum_{j\in J} ((a_j' + a_j'', b_j') - (a_j', b_j') - (a_j'', b_j')) \\ &+ \sum_{k\in K} ((a_k''', b_k'' + b_k''') - (a_k''', b_k'') - (a_k''', b_k''')) + \sum_{l\in L} ((a_l''''r, b'''') - (a'''', rb'''')),\end{aligned}$$

за неке коначне скупове J, K, L, и за неке a-ове из A, b-ове из B, r-ове из R. Уколико за A' узмемо подгрупу генерисану свим a-овима који се појављују у овој једнакости, а са B' подгрупу генерисану свим b-овима, онда наведени елемент јесте у $A' \otimes_R B'$ (јер $a_i \in A'$, $b_i \in B'$) и заправо је ту једнак нули. Стога важи следећи став.

Став 66. Ако су сви коначно генерисани подмодули модула B равни модули, онда је и B раван модул.

Пример 67. Свака коначно генерисана подгрупа групе $\mathbb{Q}$ је слободна (она је, по теореми о класификацији коначно генерисаних Абелових група коначна директна сума цикличних, али у $\mathbb{Q}$ нема елемената коначног реда, па је онда коначна директна сума бесконачних цикличних, које су све изоморфне са $\mathbb{Z}$) те је, према претходна два става $\mathbb{Q}$ раван $\mathbb{Z}$-модул. Но, то није пројективан $\mathbb{Z}$-модул. Наиме, пројективан $\mathbb{Z}$-модул је подмодул слободног $\mathbb{Z}$-модула, а свака подгрупа слободне Абелове групе је слободна Абелова група. Но, $\mathbb{Q}$ није слободна – нема линеарно независне генераторе. Наиме, ако су $x = \frac{m}{n}$ и $y = \frac{p}{q}$ елементи из $\mathbb{Q}$, онда је $pnx - mqy = pn\frac{m}{n} - mq\frac{p}{q} = pm - mp = 0$. ♣

Ако је A леви R-модул, онда је његов дуални модул $A^* := \mathrm{Hom}_R(A, R)$ и то је десни R-модул: $(\phi \cdot r)(a) = \phi(a)r$ (ово је специјални случај раније дефинисаних модула хомоморфизама).

Теорема 68. Леви R-модул P је пројективан ако и само ако постоје фамилије $(x_i)_{i\in I} \in \prod_{i\in I} P$, $(f_i)_{i\in I} \in \prod_{i\in I} P^*$ тако да је за сваки $x \in X$, $f_i(x) \neq 0$ само за коначно много $i \in I$ и $x = \sum_{i\in I} f_i(x)x_i$.

Доказ. Претпоставимо да је P пројективан. То значи да постоји модул Q и слободан модул F тако да је $F = P \bigoplus Q$. Нека је $(z_i)_{i\in I}$ база за F. Тада, за све $i \in I$ имамо: $z_i = x_i + y_i$, за јединствено одређене $x_i \in P$, $y_i \in Q$. Дефинишимо функције $g_i\colon \{z_i : i \in I\} \to R$ са: $g_i(z_j) = 0_R$ за $j \neq i$ и $g_i(z_i) = 1_R$. Тада постоје јединствено одређени хомоморфизми модула $g_i\colon F \to R$ и дефинишемо f_i са: $f_i := g_i|_{P_i}\colon P \to R$.

Уколико је $x \in P$, онда постоје јединствено одређени $r_i \in R$ тако да је $x = \sum_{i\in I} r_i z_i$, при чему је, наравно, $r_i \neq 0$ само за коначно много индекса $i \in I$. Имамо да је тада, пошто је $z_i = x_i + y_i$,

$$P \ni x - \sum_{i\in I} r_i x_i = \sum_{i\in I} r_i y_i \in Q.$$

Стога је $x - \sum_{i\in I} r_i x_i = 0_P$, тј. $x = \sum_{i\in I} r_i x_i$. Имамо да је

$$f_i(x) = g_i(x) = g_i\left(\sum_{j\in I} r_j z_j\right) = \sum_{j\in I} r_j g_i(z_j) = r_i.$$

Дакле, заиста је $f_i(x) \neq 0_R$ само за коначно много индекса i и важи једнакост $x = \sum_{i\in I} f_i(x)x_i$.

Обратно, претпоставимо да постоје фамилије $(x_i)_{i\in I}$ и $(f_i)_{i\in I}$ са наведеним својствима. Нека је $F = \bigoplus_{i\in I} R$. Дефинишемо $\phi\colon F \to P$ са: $\phi\big((r_i)_{i\in I}\big) := \sum_{i\in I} r_i x_i$, а $\psi\colon P \to F$ са: $\psi(x) = (f_i(x))_{i\in I}$. Ово су хомоморфизми (уверите се у то) за које важи:

$$\phi(\psi(x)) = \phi\big((f_i(x)_{i\in I}\big) = \sum_{i\in I} f_i(x)x_i = x.$$

Дакле, имамо кратак тачан низ $0 \to P \xrightarrow{\psi} F \to F/\operatorname{Im}\psi \to 0$, који се цепа те је $F \cong P \bigoplus F/\operatorname{Im}\psi$ и закључујемо да је P пројективан модул. $\square$

Пар $\big((x_i)_{i\in I}, (f_i)_{i\in I}\big)$ називамо R-пројективна база за P. Наравно, $\{x_i : i \in I\}$ јесте генераторни скуп, но није нужно линеарно независан (иначе би P био слободан модул). Следећи резултат директно следи.

Последица 69. *Леви R-модул P је коначно генерисан пројективан модул ако и само ако постоје фамилије из претходне теореме за које је скуп индекса I коначан.* $\square$

Ако је F коначно генерисан слободан R-модул, онда је његов дуал коначно генерисан слободан десни R-модул. Стога, ако је P коначно генерисан пројективан леви R-модул, онда је P^* коначно генерисан пројективан десни R-модул. Тада је $P^{**} = (P^*)^*$ коначно генерисан леви R-модул. Имамо дефинисан хомоморфизам левих R-модула $P \to P^{**}$ задат са: $x \mapsto \widehat{x}$, где је $\widehat{x} \in P^{**}$ дефинисан са: $\widehat{x}(\phi) := \phi(x)$ за $\phi \in P^*$. Уколико је $\widehat{x} = 0_{P^{**}}$, то значи да је, посебно, $\widehat{(x)}(f_i) = 0$ за све f_i из пројективне базе за P. Дакле, $f_i(x) = 0$ за све i, па мора бити $x = 0$, тј. хомоморфизам $x \mapsto \widehat{x}$ је „1–1”. Заправо важи следећа теорема.

Теорема 70. *Ако је $\big((x_i)_{i\in I}, (f_i)_{i\in I}\big)$ коначна R-пројективна база за P, онда је $\big((f_i)_{i\in I}, (\widehat{x_i})_{i\in I}\big)$ коначна R-пројективна база за P^*.*

Доказ. Само треба показати да је за свако $f \in P^*$ (обратите пажњу на чињеницу да је P^* десни R-модул):

$$f = \sum_{i\in I} f_i \cdot \widehat{x_i}(f) = \sum_{i\in I} f_i \cdot f(x_i). \tag{23}$$

Но, ако је $g = \sum_{i\in I} f_i \cdot f(x_i)$, онда је за свако $x \in P$:

$$g(x) = \big(\sum_{i\in I} f_i \cdot f(x_i)\big)(x) = \sum_{i\in I} \big(f_i \cdot f(x_i)\big)(x) = \sum_{i\in I} f_i(x) f(x_i) = f\big(\sum_{i\in I} f_i(x)x_i\big) = f(x),$$

па је заиста $f = g$. $\square$

Између осталог, имамо и да је $P \cong P^{**}$. Заправо је $x \mapsto \widehat{x}$ тај изоморфизам. Да бисмо доказали да је и „на”, претпоставимо да је $\Psi \in P^{**}$. Уочимо елемент $x = \sum_{i\in I} \Psi(f_i)x_i$. Тада је, за свако $f \in P^*$:

$$\widehat{x}(f) = f(x) = f\bigg(\sum_{i\in I} \Psi(f_i)x_i\bigg) = \sum_{i\in I} \Psi(f_i) f(x_i) = \sum_{i\in I} \Psi\big(f_i \cdot f(x_i)\big) = \Psi\bigg(\sum_{i\in I} f_i \cdot f(x_i)\bigg) = \Psi(f),$$

па је $\widehat{x} = \Psi$. $\square$

Нека су A и B леви R-модули. Дефинишемо функцију

$$F\colon A^* \times B \to \mathrm{Hom}_R(A, B)$$

са $F(f, b)(a) := f(a)b$. За свако $f \in A^*$ и $b \in B$, $F(f, b) \in \mathrm{Hom}_R(A, B)$:

$$F(f,b)(a_1 + a_2) = f(a_1 + a_1)b = (f(a_1) + f(a_2))b = f(a_1)b + f(a_2)b = F(f,b)(a_1) + F(f,b)(a_2),$$

$$F(f, b)(ra) = f(ra)b = (rf(a))b = r(f(a)b) = rF(f, b)(a).$$

Стога она индукује хомоморфизам Абелових група $\overline{F}\colon \mathcal{F}(A^* \times B) \to \mathrm{Hom}_R(A, B)$. Као и у ранијим случајевима, провери се да се сви генератори групе $\mathcal{R}(A^* \times B)$ сликају у нули и имамо хомоморфизам Абелових група

$$\theta_{A,B}\colon A^* \otimes_R B \to \mathrm{Hom}_R(A, B). \tag{24}$$

Такође имамо природност. Ако су $\alpha\colon A' \to A$, $\beta\colon B \to B'$ из ${}_R\mathfrak{M}$, онда је $\alpha^*\colon A^* \to A'^*$ задато са $\alpha^*(f) = f \circ \alpha$ и имамо индуковане хомоморфизме $\alpha^* \otimes \beta\colon A^* \otimes B \to A'^* \otimes B^*$ и $\mathrm{Hom}(\alpha, \beta)\colon \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B')$ тако да дијаграм

$$\begin{tikzcd}
A^* \otimes_R B \arrow[r, "\theta_{A,B}"] \arrow[d, "\alpha^* \otimes \beta"] & \mathrm{Hom}_R(A, B) \arrow[d, "\mathrm{Hom}(\alpha,\beta)"] \\
A'^* \otimes_R B' \arrow[r, "\theta_{A',B'}"] & \mathrm{Hom}_R(A', B')
\end{tikzcd}$$

комутира, тј. да важи једнакост

$$\theta_{A',B'} \circ (\alpha^* \otimes \beta) = \mathrm{Hom}(\alpha, \beta) \circ \theta_{A,B},$$

где је $\mathrm{Hom}(\alpha, \beta)(\psi) = \beta \circ \psi \circ \alpha$.

Проверимо на адитивним генераторима и елементу $a' \in A'$.

$$\Big((\theta_{A',B'} \circ (\alpha^* \otimes \beta))(f \otimes b)\Big)(a') = \Big(\theta_{A',B'}\big((\alpha^* \otimes \beta)(f, b)\big)\Big)(a')$$
$$= \theta_{A',B'}\big(\alpha^*(f), \beta(b)\big)(a) = \theta_{A',B'}(f \circ \alpha, \beta)(a') = f(\alpha(a'))b;$$

$$\Big(\big(\mathrm{Hom}(\alpha, \beta) \circ \theta_{A,B}\big)(f \otimes b)\Big)(a') = \Big(\mathrm{Hom}(\alpha, \beta)\big(\theta_{A,B}(f \otimes b)\big)\Big)(a')$$
$$= (\beta \circ \theta_{A,B}(f \otimes b) \circ \alpha)(a') = \beta\big(\theta_{A,B}(f \otimes b)(\alpha(a'))\big) = \beta(f(\alpha(a')b) = f(\alpha(a'))\beta(b).$$

Теорема 71. Хомоморфизам $\theta_{A,B}$ из (24) је изоморфизам за сваки B ако и само ако је A коначно генерисан пројективан модул.

Доказ. Претпоставимо најпре да је $\theta_{A,B}$ изоморфизам за све модуле B. Узмимо да је $B = A$. Тада постоји елемент $f_1 \otimes a_1 + \cdots + f_n \otimes a_n \in A^* \otimes A$ такав да је $\theta_{A,A}(f_1 \otimes x_1 + \cdots + f_n \otimes x_n)) = \mathrm{id}_A$. То значи да за свако $x \in A$ имамо да је

$$x = \mathrm{id}_A(x) = \big(\theta_{A,A}(f_1 \otimes x_1 + \cdots + f_n \otimes x_n)\big)(x) = f_1(x)x_1 + \cdots + f_n(x)x_n,$$

тако да је $\big((x_i)_{i=\overline{1,n}}, (f_i)_{i=\overline{1,n}}\big)$ коначна пројективна база за A.

Обратно, претпоставимо да је A коначно генерисан пројективан R-модул и $\big((x_i)_{i=\overline{1,n}}, (f_i)_{i=\overline{1,n}}\big)$ коначна пројективна база за A. Покажимо да је $\theta_{A,B}$ изоморфизам за сваки леви R-модул B.

$\theta_{A,B}$ је „на”. Нека је $\psi \in \mathrm{Hom}_R(A, B)$. Покажимо да је

$$\theta_{A,B}\Big(\sum_{i=1}^{n}(f_i \otimes \psi(x_i))\Big) = \psi.$$

$$\theta_{A,B}\Big(\sum_{i=1}^{n}(f_i \otimes \psi(x_i))\Big)(x) = \sum_{i=1}^{n} f_i(x)\psi(x_i) = \psi\Big(\sum_{i=1}^{n} f_i(x)x_i\Big) = \psi(x).$$

$\theta_{A,B}$ је „1–1”. На основу теореме 70 знамо да су $f_1, \ldots, f_n$ генератори за A^*. Стога се сваки елемент из $A^* \otimes B$ може написати у облику $f_1 \otimes b_1 + \cdots + f_n \otimes b_n$ (покажите!). Нека $f_1 \otimes b_1 + \cdots + f_n \otimes b_n \in \mathrm{Ker}\,\theta_{A,B}$.То значи да је $\theta_{A,B}(f_1 \otimes b_1 + \cdots + f_n \otimes b_n)(x) = 0_B$ за сваки $x \in A$. Посебно је $\theta_{A,B}(f_1 \otimes b_1 + \cdots + f_n \otimes b_n)(x_i) = 0_B$ за све $i = \overline{1,n}$. Но,

$$\theta_{A,B}(f_1 \otimes b_1 + \cdots + f_n \otimes b_n)(x_i) = f_1(x_i)b_1 + \cdots + f_n(x_i)b_n = b_i,$$

па закључујемо да је $b_1 = \cdots = b_n = 0_B$ и $\mathrm{Ker}\,\theta_{A,B} = 0_{A^* \otimes_R B}$. $\square$

Знамо да није сваки раван модул пројективан, но постоји важна класа равних модула који ЈЕСУ пројективни.

Дефиниција 72. За модул A кажемо да се може КОНАЧНО ПРЕДСТАВИТИ уколико постоји тачан низ $F_1 \to F_0 \to A \to 0$, где су F_0 и F_1 коначно генерисани слободни модули.

Теорема 73. Сваки раван модул, који се може коначно представити је пројективан.

Доказ. Ако је $F_1 \to F_0 \to A \to 0$ једно представљање равног модула A, онда добијамо комутативни дијаграм.

$$\begin{array}{ccccccc}
0 & \longrightarrow & A^* \otimes_R A & \longrightarrow & F_0^* \otimes_R A & \longrightarrow & F_1^* \otimes_R A \\
 & & \downarrow{\scriptstyle \theta_{A,A}} & & \downarrow{\scriptstyle \theta_{F_0,A}} & & \downarrow{\scriptstyle \theta_{F_1,A}} \\
0 & \longrightarrow & \mathrm{Hom}_R(A,A) & \longrightarrow & \mathrm{Hom}_R(F_0,A) & \longrightarrow & \mathrm{Hom}_R(F_1,A)
\end{array}$$

Функтор $\mathrm{Hom}_R(-, R)$ је лево тачан, па је низ $0 \to A^* \to F_0^* \to F_1^*$ тачан. Но, A је раван модул, па добијамо тачан низ у горњем делу дијаграма. Низ у доњем делу дијаграма је тачан зато што је функтор $\mathrm{Hom}_R(-, A)$ лево тачан. На основу теореме 71, $\theta_{F_0,A}$ и $\theta_{F_1,A}$ су изоморфизми. Одатле следи (докажите то директно) да је и $\theta_{A,A}$ изоморфизам. Но, видели смо из доказа теореме 71, да из тог изоморфизма следи да је A коначно генерисан пројективан модул. $\square$

Нека је $\theta\colon R \to S$ хомоморфизам прстена. Тада сваки леви S-модул A постаје и леви R-модул: $r \cdot a := \theta(r)a$. На тај начин добијамо и функтор $U^\theta\colon {}_S\mathfrak{M} \to_R \mathfrak{M}$. Наравно, аналогно се ово може урадити и за десне модула. Посебно је и сам прстен S један R-модул (овде гледамо само структуру Абелове групе $(S, +)$).

Став 74. Нека је S пројективан као леви R-модул. Тада је сваки пројективан S-модул такође и пројективан R-модул.

Доказ. Даћемо два доказа овог резултата. Најпре ћемо доказ извести преко пројективних база. Нека је P пројективан S-модул. Ако је $\big((s_i)_{i\in I}, (g_i)_{i\in I}\big)$ (где $g_i \in \mathrm{Hom}_R(S, R)$) пројективна R-база за S, док је $\big((x_j)_{j\in J}, (f_j)_{j\in J}\big)$ (где $f_j \in \mathrm{Hom}_S(P, S)$) пројективна S-база за P, посматрајмо уређени пар

$$\big((s_i x_j)_{(i,j)\in I\times J}, (g_i \circ f_j)_{(i,j)\in I\times J}\big). \tag{25}$$

Имамо да је $g_j \circ f_i \in \mathrm{Hom}_R(P, R)$:

$$(g_i \circ f_j)(r \cdot x) = g_i(f_j(\theta(r)x)) = g_i(\theta(r)f_j(x)) = g_i(r \cdot f_j(x)) = rg_i(f_j(x)) = r(g_i \circ f_j)(x),$$

за све $r \in R$ и $x \in P$. Такође

$$\begin{aligned}(g_i \circ f_j)(x_1 + x_2) &= g_i(f_j(x_1 + x_2)) = g_i(f_j(x_1) + f_j(x_2))\\ &= g_i(f_j(x_1)) + g_i(f_j(x_2)) = (g_i \circ f_j)(x_1) + (g_i \circ f_j)(x_2),\end{aligned}$$

за све $x_1, x_2 \in P$. Такође је јасно да је $(g_i \circ f_j)(x) \neq 0$ само за коначно много парова (i, j). Најзад, ако је $x \in P$:

$$x = \sum_j f_j(x)x_j = \sum_j \Big(\sum_i g_i(f_j(x))s_i\Big)x_j = \sum_j \sum_i (g_i \circ f_j)(x)s_i x_j,$$

те можемо да закључимо да је уређени пар (25) једна пројективна R-база за P, те је P пројективан R-модул. $\square$

За други доказ ће нам требати следећи резултат.

Став 75. Постоји природан изоморфизам

$$F\colon \mathrm{Hom}_R(U^\theta P, X) \to \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, X)),$$

где је P леви S-модул, X, леви R-модул, а S видимо као (R, S)-бимодул.

Доказ. У овом доказу нећемо све проверавати, оставићемо то читаоцима као корисну (мада не и забавну) вежбу, коју заиста препоручујемо. Посебно остављамо прецизну формулацију природности.

Ако је $\phi \in \mathrm{Hom}_R(U^\theta P, X)$ дефинишемо $F(\phi) \in \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, X))$ са: $\big(F(\phi)(p)\big)(s) := \phi(sp)$, за $s \in S$, $p \in P$. Уместо провере да је F изоморфизам, дефинисаћемо $G\colon \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, X)) \to \mathrm{Hom}_R(U^\theta P, X)$ и показати да је је $G \circ F = \mathrm{id}_{\mathrm{Hom}_R(U^\theta P, X)}$ и $F \circ G = \mathrm{id}_{\mathrm{Hom}_S(P, \mathrm{Hom}_R(S,X))}$.

$$G\colon \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, X)) \to \mathrm{Hom}_R(U^\theta P, X)$$

задајемо са: $\big(G(\psi)\big)(p) := \big(\psi(p)\big)(1_S)$, за $\psi \in \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, X))$, $p \in P$.

$$\big((G \circ F)(\phi)\big)(p) = \big(G(F(\phi))\big)(p) = \big(\big(F(\phi)\big)(p)\big)(1_S) = \phi(1_s p) = \phi(p).$$

Дакле, $(G \circ F)(\phi) = \phi$.

$$\begin{aligned}\big(\big((F \circ G)(\psi)\big)(p)\big)(s) = \big(\big(\big(F(G(\psi))\big)(p)\big)(s) = \big(G(\psi)\big)(sp) = \big(\psi(sp)\big)(1_S) \\ = \big(s \cdot \psi(p)\big)(1_S) = \psi(p)(1_S s) = \psi(p)(s).\end{aligned}$$

Овде смо користили чињеницу да је ψ хомоморфизам S-модула и начин задавања структуре S-модула на $\mathrm{Hom}_R(S, X)$. Дакле, $(F \circ G)(\psi) = \psi$. $\square$

Други доказ става 74. У доказу користимо став 62. Нека је P пројективан S-модул. Посматрајмо тачан низ R-модула

$$0 \to A' \to A \to A'' \to 0. \tag{26}$$

Како је S пројективан R-модул, то је, на основу става 62, низ

$$0 \to \mathrm{Hom}_R(S, A') \to \mathrm{Hom}_R(S, A) \to \mathrm{Hom}_R(S, A'') \to 0 \tag{27}$$

тачан. Како је P пројективан S-модул, то је на основу истог става низ

$$0 \to \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, A')) \to \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, A)) \to \mathrm{Hom}_S(P, \mathrm{Hom}_R(S, A'')) \to 0 \tag{28}$$

тачан. Посматрајмо сада низ

$$0 \to \mathrm{Hom}_R(U^\theta P, A') \to \mathrm{Hom}_R(U^\theta P, A) \to \mathrm{Hom}_R(U^\theta P, A') \to 0. \tag{29}$$

На основу става 75 низ (28) слика се у (29) тако што су сви вертикални хомоморфизми заправо изоморфизми и добијени дијаграм комутира (због природности). Уверите се да из тачности низа (28) следи тачност низа (29) (користите добијени дијаграм који спаја ова два низа и потом једноставну „јурњаву по дијаграму”).

Стога је, на основу става 62 $U^\theta P$ пројективан R-модул. $\square$

Следећа последица је корисна у (ко)хомолошкој теорији група.

Последица 76. Пројективни $\mathbb{Z}[G]$-модул је слободна Абелова група.

Доказ. Нека је P пројективан $\mathbb{Z}[G]$-модул. Нека је $R = \mathbb{Z}$ и $S = \mathbb{Z}[G]$. S је слободни $\mathbb{Z}$-модул, јер јој елементи из G чине базу (по дефиницији групног прстена). Дакле, S је пројективан $\mathbb{Z}$-модул, P је пројективан S-модул, па је на основу става 74 P пројективан $\mathbb{Z}$-модул. Но, сваки пројективан $\mathbb{Z}$-модул је заправо слободан, тј. P је слободна Абелова група. □

6 Инјективни модули

У овом одељку бавићемо се модулима, који су дуални пројективним.

Дефиниција 77. Леви R-модул I је ИНЈЕКТИВАН уколико за сваки тачан низ $0 \to A' \xrightarrow{\mu} A$ у ${}_R\mathfrak{M}$ и хомоморфизам $\phi\colon A' \to I$ постоји хомоморфизам $\psi\colon A \to I$ за који је $\psi \circ \mu = \phi$.

$$\begin{tikzcd}
 & I & \\
A \arrow[ur, dashed, "\psi"] & A' \arrow[l, "\mu"'] \arrow[u, "\phi"'] & 0 \arrow[l]
\end{tikzcd}$$

Као што видимо, дијаграм у дефиницији инјективних модула добија се од дијаграма из дефиниције пројективних модула обртањем свих стрелица (то је дуалност о којој причамо).

Следећа два става су дуална одговарајућим код пројективних модула и њихови докази се остављају за вежбу.

Став 78. Директан производ $\prod_i I_i$ је инјективан акко је сваки од модула I_i инјективан.

Став 79. R-модул I је инјективан акко је функтор $\mathrm{Hom}_R(-, I)\colon {}_R\mathfrak{M}^{\mathrm{op}} \to \mathfrak{Ab}$ тачан.

Слободни модули су нам били први пример пројективних модула. У случају инјективних модула, ствар је нешто сложенија. Најпре ћемо се позабавити инјективним $\mathbb{Z}$-модулима, тј. Абеловим групама.

Дефиниција 80. Абелова група D је ДЕЉИВА уколико за свако $x \in D$ и свако $n \geqslant 1$ постоји $y \in D$ тако да је $ny = x$.

Јасно је да група $\mathbb{Z}$ није дељива, а нису то ни групе $\mathbb{Z}_m$, но дељиве су групе $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, као и група $\mathbb{Q}/\mathbb{Z}$. Ова последња ће нам бити посебно значајна. Проверимо зашто је дељива. Ако је $x = \frac{p}{q} + \mathbb{Z}$ произвољан елемент, онда је, за $y = \frac{p}{qn} + \mathbb{Z}$ јасно испуњено да је $ny = x$. Заправо, лако се показује да важи следећи став.

Став 81. а) Ако је D дељива група и B подгрупа од D, онда је и D/B дељива група.

б) Ако су D_i, $i \in I$ дељиве групе, онда је и група $\bigoplus_{i \in I} D_i$ дељива група.

Доказ. a) Наиме, ако је $\bar{x} = d + B \in D/B$ и $n \geqslant 1$, онда постоји $y \in D$ тако да је $d = ny$, па је тада $n(y + D) = ny + D = d + B = \bar{x}$.

б) Уколико је $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} D_i$ и $n \geqslant 1$, онда за свако $i \in I$, пошто је D_i дељива група, постоји $y_i \in D_i$ тако да је $ny_i = x_i$. Тада имамо да је $n(y_i)_{i\in I} = (x_i)_{i\in I}$. □

Следећа теорема оправдава увођење овог појма овде.

Теорема 82. Абелова група D је инјективан $\mathbb{Z}$-модул акко је дељива.

Доказ. Претпоставимо најпре да је D инјективан $\mathbb{Z}$-модул. Ако је $n \geqslant 1$ онда множење са n у $\mathbb{Z}$ јесте „1–1". Нека је $x \in D$. Уочимо дијаграм:

$$\begin{tikzcd} & D & \\ \mathbb{Z} \arrow[ur, dashed, "\psi"] & \mathbb{Z} \arrow[l, "n\cdot"'] \arrow[u, "\phi"'] & 0 \arrow[l] \end{tikzcd}$$

где је $\phi(1) := x$. Тада је $x = \phi(1) = \psi(n) = n\psi(1)$ и тражени y је $\psi(1)$.

Претпоставимо сада да је D дељива група и посматрајмо дијаграм.

$$\begin{tikzcd} & D & \\ A \arrow[ur, dashed, "\psi"] & A' \arrow[l, "\mu"'] \arrow[u, "\phi"'] & 0 \arrow[l] \end{tikzcd}$$

Показаћемо да ψ постоји користећи Цорнову лему. Ради једноставности ознака претпоставићемо да је $A' \leqslant A$ и да је μ укључење. Дакле, хомоморфизам ϕ треба са A' проширити на целу групу A. Нека је $\mathcal{P} := \{(B, \phi_B) : A' \leqslant B \leqslant A, \phi_B \in \mathrm{Hom}(B, D), \phi_B|_{A'} = \phi\}$. Јасно је да $\mathcal{P} \neq \emptyset$, јер $(A', \phi) \in \mathcal{P}$. Поредак на $\mathcal{P}$ можемо дефинисати са:

$$(B', \phi_{B'}) \preccurlyeq (B'', \phi_{B''}) \overset{\text{def}}{\Longleftrightarrow} B' \subseteq B'', \phi_{B''}|_{B'} = \phi_{B'}.$$

Нека је $\mathcal{L}$ ланац у $\mathcal{P}$. Ако је $\overline{B} = \bigcup_{(B,\phi_B)\in\mathcal{L}} B$, можемо задати $\overline{\phi}\colon \overline{B} \to D$ са: $\overline{\phi}(x) := \phi_B(x)$, ако $x \in B$. Ово не зависи од избора B. Наиме, ако је и $x \in B'$ за неки други B', онда, пошто је $\mathcal{L}$ ланац, имамо да је или $B \subseteq B'$ и $\phi_B(x) = \phi_{B'}|_B(x) = \phi_{B'}(x)$ или је $B' \subseteq B$ и $\phi_{B'}(x) = \phi_B|_{B'}(x) = \phi_B(x)$. Јасно је да $(\overline{B}, \overline{\phi}) \in \mathcal{P}$ и да је $(B, \phi_B) \preccurlyeq (\overline{B}, \overline{\phi})$, па смо добили мајоранту ланца $\mathcal{L}$. Стога постоји максималан елемент $(B_0, \phi_0) \in \mathcal{P}$. Ако је $B_0 \subset A$ (дакле, прави подскуп од A), узмимо неки елемент $a \in A \setminus B_0$. Посматрајмо $\mathbb{Z}a \cap B_0$ ($\mathbb{Z}a = \{ma : m \in \mathbb{Z}\}$ је наравно подгрупа од A генерисана елементом a).

Претпоставимо да је $\mathbb{Z}a \cap B_0 = \{0\}$. Тада је $A \geqslant B_0 + \mathbb{Z}a = B_0 \dot{+} \mathbb{Z}a$ и постоји јединствен $\phi_1\colon B_0 \dot{+} \mathbb{Z}a \to D$ задат са $\phi_1|_{B_0} = \phi_0$, $\phi_1|_{\mathbb{Z}a} = 0$.

Стога је $(B_1, \phi_1) \in \mathcal{P}$ и $(B_0, \phi_0) \prec (B_1, \phi_1)$, што противречи претпоставци да је (B_0, ϕ_0) максималан елемент у $\mathcal{P}$.

Дакле, $\mathbb{Z}a \cap B_0 \neq \{0\}$. Нека је $J = \{m \in \mathbb{Z} : ma \in B_0\}$. Тада $J \neq \{0\}$ и лако се провери да је J идеал у $\mathbb{Z}$:

$$m_1, m_2 \in J \Rightarrow m_1a, m_2a \in B_0 \Rightarrow (m_1+m_2)a = m_1a+m_2a \in B_0 \Rightarrow m_1+m_2 \in J;$$

$$m \in J, k \in \mathbb{Z} \Rightarrow ma \in B_0 \Rightarrow kma \in B_0 \Rightarrow km \in J.$$

Како је у $\mathbb{Z}$ сваки идеал главни, имамо да је $J = \mathbb{Z}n$ за неко $n \geqslant 2$ ($n = 1$ би значило да $a \in B_0$, а то није тачно). Како $na \in B_0$, то је дефинисано $x = \phi_0(na)$. Нека је $y \in D$ елемент за који је $ny = x$. Дефинишемо $\phi_1 \colon B_0 + \mathbb{Z}a \to D$ са: $\phi_1(b_0 + ma) := \phi_0(b_0) + my$. Ово јесте добро дефинисано. Наиме, ако је $b_0' + m'a = b_0 + ma$, онда је $(m' - m)a = b_0 - b_0' \in B_0$, па $m' - m \in J$, те је $m' - m = kn$ за неко k. Проверимо да ли је $\phi_0(b_0') + m'y = \phi_0(b_0) + my$:

$$\begin{aligned}\phi_0(b_0) - \phi_0(b_0') = \phi_0(b_0 - b_0') = \phi_0\big((m' - m)a\big) &= \phi_0(kna) \\ &= k\phi_0(na) = kx = kny = (m' - m)y.\end{aligned}$$

Одавде следи да је $\phi_0(b_0) + my = \phi_0(b_0') + m'y$. Наравно, лако се провери да је ϕ_1 хомоморфизам Абелових група и поново смо добили проширење од ϕ_0 што противречи чињеници да је (B_0, ϕ_0) максималан елемент у $\mathcal{P}$. Стога је $B_0 = A$ и то завршава доказ. $\square$

Прилично лако смо добили да је сваки модул (хомоморфна) слика пројективног модула, јер су слободни модули пројективни, а лако се закључује да је сваки модул слика слободног. Да бисмо показали да се сваки модул може утопити у ињективан модул (што је одговарајуће дуално тврђење) најпре ћемо то урадити за Абелове групе.

Теорема 83. Свака Абелова група може се утопити у дељиву (дакле ињективну) Абелову групу.

Доказ. Нека је A Абелова група. Дефинишимо хомоморфизам

$$\phi \colon \underbrace{\bigoplus_{a \in A \setminus \{0\}} \mathbb{Z}}_{F} \to A$$

са $\phi\big((m_a)_{a \in A \setminus \{0\}}\big) := \sum_{a \in A \setminus \{0\}} m_a a$. Јасно је да је ϕ „на” и нека је $K = \operatorname{Ker} \phi$. Посматрајмо укључење $\iota \colon \bigoplus_{a \in A \setminus \{0\}} \mathbb{Z} \to \bigoplus_{a \in A \setminus \{0\}} \mathbb{Q}$. Оно индукује утапање

$$\bar{\iota} \colon \Big(\bigoplus_{a \in A \setminus \{0\}} \mathbb{Z} \Big) / K \to \Big(\bigoplus_{a \in A \setminus \{0\}} \mathbb{Q} \Big) / \, \iota[K].$$

Но, $A \cong F/K$, а група $\left(\bigoplus_{a \in A \setminus \{0\}} \mathbb{Q}\right) / \, \iota[K]$ јесте дељива по ставу 81, па смо тако добили утапање групе A у дељиву групу. $\square$

Теорема 84. Нека је $\theta\colon R \to S$ хомоморфизам прстена и I инјективан R-модул. Тада је $\mathrm{Hom}_R(S, I)$ инјективан S-модул.

Доказ. Користимо ставове 79 и 75. У ту сврху, нека је

$$0 \to A' \to A \to A'' \to 0$$

тачан низ S-модула. Треба показати да је низ

$$0 \to \mathrm{Hom}_S(A'', \mathrm{Hom}_R(S, I)) \to \mathrm{Hom}_S(A, \mathrm{Hom}_R(S, I)) \to \mathrm{Hom}_S(A', \mathrm{Hom}_R(S, I)) \to 0$$

тачан. Но, на основу става 75 добијамо дијаграм

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_S(A'', \mathrm{Hom}_R(S, I)) \arrow[r] \arrow[d, "\cong"'] & \mathrm{Hom}_S(A, \mathrm{Hom}_R(S, I)) \arrow[r] \arrow[d, "\cong"'] & \mathrm{Hom}_S(A', \mathrm{Hom}_R(S, I)) \arrow[r] \arrow[d, "\cong"'] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(U^\theta A'', I) \arrow[r] & \mathrm{Hom}_R(U^\theta A, I) \arrow[r] & \mathrm{Hom}_R(U^\theta A', I) \arrow[r] & 0
\end{tikzcd}$$

у коме је доњи низ тачан, јер је I инјективан R-модул. Лако се онда показује да је и горњи низ тачан. $\square$

Ако применимо претходну теорему на јединствено задат хомоморфизам прстена $\theta\colon \mathbb{Z} \to R$, добијамо следећу последицу.

Последица 85. Нека је D дељива Абелова група. Тада је $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ инјективан R-модул.

Доказ. Подсетимо се само да се структура левог R-модула овде добија помоћу чињенице да је R десни R-модул: $(r' \cdot \xi)(r) := \xi(rr')$. $\square$

Теорема 86. Сваки R-модул може се утопити у инјективан R-модул.

Доказ. Нека је $\phi\colon U^\theta A \to D$ утапање Абелове групе U^θ у дељиву (дакле, инјективну) Абелову групу D. По последици 85 добијамо да је леви R-модул $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ инјективан. Дефинишимо $\psi\colon A \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ са: $\big(\psi(a)\big)(r) := \phi(ra)$. Покажимо да је ово „1–1" хомоморфизам левих R-модула. Најпре, за сваки $a \in A$: $\psi(a) \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$:

$$\big(\psi(a)\big)(r_1 + r_2) = \phi((r_1 + r_2)a) = \phi(r_1 a + r_2 a) = \phi(r_1 a) + \phi(r_2)(a) = \big(\psi(a)\big)(r_1) + \big(\psi(a)\big)(r_2).$$

Покажимо да је $\psi(a_1 + a_2) = \psi(a_1) + \psi(a_2)$:

$$\big(\psi(a_1 + a_2)\big)(r) = \phi(r(a_1 + a_2)) = \phi(ra_1 + ra_2) = \phi(ra_1) + \phi(ra_2) = \big(\psi(a_1)\big)(r) + \big(\psi(a_2)\big)(r).$$

Као и да је $\psi(r'a) = r' \cdot \psi(a)$:

$$\big(\psi(r'a)\big)(r) = \phi(r(r'a)) = \phi((rr')a), \quad \big(r' \cdot \psi\big)(r) = \psi(rr') = \phi((rr')a).$$

Коначно, $\mathrm{Ker}\,\psi = \{0_A\}$. Ако је $\psi(a) = 0_{\mathrm{Hom}_{\mathbb{Z}}(R,D)}$, онда је $\big(\psi(a)\big)(r) = 0_D$ за свако $r \in R$. Посебно, имамо да је $0_D = \big(\psi(a)\big)(1_R) = \phi(1_R a) = \phi(a)$. Но, како је ϕ утапање, добијамо да је $a = 0_A$. $\square$

Уведимо сада појам кослободног модула.

Дефиниција 87. Нека је F слободан десни R-модул. Тада леви R-модул $\mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z})$ називамо КОСЛОБОДНИМ модулом.

Став 88. Кослободан модул је инјективан.

Доказ. Како је $\mathrm{Hom}_{\mathbb{Z}}\big(\bigoplus_{i\in I} R, \mathbb{Q}/\mathbb{Z}\big) \cong \prod_{i\in I} \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$, резултат следи на основу последице 85 и става 78. □

За модул A уведимо ознаку $A^{\vee} := \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$.

Став 89. За модул A дефинишемо $\iota\colon A \to A^{\vee\vee}$ са: $\big(\iota(a)\big)(\phi) := \phi(a)$, за $a \in A$ и $\phi \in A^{\vee}$. Овако дефинисано ι је хомоморфизам модула који је „1–1".

Доказ. Нека је A леви R-модул (можемо исто урадити и за десни). Најпре проверимо да ι заиста слика A у $A^{\vee\vee}$:

$$\big(\iota(a)\big)(\phi_1+\phi_2) = (\phi_1+\phi_2)(a) = \phi_1(a)+\phi_2(a) = \big(\iota(a)\big)(\phi_1) + \big(\iota(a)\big)(\phi_2).$$

Проверимо слагање ι са сабирањем:

$$\big(\iota(a_1+a_2)\big)(\phi) = \phi(a_1+a_2) = \phi(a_1)+\phi(a_2) = \big(\iota(a_1)\big)(\phi) + \big(\iota(a_2)\big)(\phi).$$

И, напокон, слагање са множењем елементима из R:

$$\big(\iota(ra)\big)(\phi) = \phi(ra) = (\phi\cdot r)(a) = \big(\iota(a)\big)(\phi\cdot r) = \big(r\cdot\iota(a)\big)(\phi),$$

па је $\iota(ra) = r\cdot\iota(a)$ (подсетите се модулске структуре на хомоморфизмима).

Коначно проверавамо да је ι заиста „1–1". Покажимо да је $\mathrm{Ker}\,\iota = \{0_A\}$. У ту сврху, покажимо да из $a \neq 0_A$ следи да постоји $\phi \in A^{\vee}$ такав да је $\big(\iota(a)\big)(\phi) = \phi(a) \neq 0_{\mathbb{Q}/\mathbb{Z}}$, те је $\iota(a) \neq 0_{A^{\vee\vee}}$.

1. a је бесконачног реда у Абеловој групи A. Њега можемо сликати у ма који ненула елемент из $\mathbb{Q}/\mathbb{Z}$, на пример у $\frac{1}{2}+\mathbb{Z}$. Дефинишемо $\xi(ma) := \frac{m}{2}+\mathbb{Z}$. Тако имамо дефинисан хомоморфизам $\xi\colon \mathbb{Z}a \to \mathbb{Q}/\mathbb{Z}$ (овде је, наравно, $\mathbb{Z}a$ подгрупа од A генерисана елементом a). Како је $\mathbb{Q}/\mathbb{Z}$ инјективна, то се ξ са подгрупе $\mathbb{Z}a$ може проширити до хомоморфизма $\phi\colon A \to \mathbb{Q}/\mathbb{Z}$ и имамо да је $\phi(a) = \xi(a) = \frac{1}{2}+\mathbb{Z} \neq 0_{\mathbb{Q}/\mathbb{Z}}$.

2. Нека је ред елемента a из A једнак $n \geqslant 2$. Сликајмо га у елемент реда n у $\mathbb{Q}/\mathbb{Z}$ и проширимо до подгрупе коју генерише. Дакле, дефинишемо $\xi\colon \mathbb{Z}a \to \mathbb{Q}/\mathbb{Z}$ са: $\xi(ma) := \frac{m}{n}+\mathbb{Z}$. Ово јесте добро дефинисано, јер из $m_1a = m_2a$ следи да је $(m_1-m_2)a = 0_A$, па $n \mid (m_1-m_2)$. Стога је $\frac{m_1}{n} - \frac{m_2}{n} = k$ за неки $k \in \mathbb{Z}$, па је $\frac{m_1}{n}+\mathbb{Z} = \frac{m_2}{n}+\mathbb{Z}$. Као и у претходном случају, због чињенице да је $\mathbb{Q}/\mathbb{Z}$ инјективна, проширујемо ξ до хомоморфизма $\phi\colon A\to\mathbb{Q}/\mathbb{Z}$ и имамо да је $\phi(a) = \frac{1}{n}+\mathbb{Z} \neq 0_{\mathbb{Q}/\mathbb{Z}}$. □

Сада можемо показати „јачи" резултат од резултата у теореми 86.

Став 90. Сваки модул се може утопити у кослободан модул.

Доказ. Нека је A леви R-модул. Тада постоји кратак тачан низ

$$0 \to K \to F \xrightarrow{\epsilon} A^{\vee} \to 0$$

за неки слободан десни R-модул F. Како је $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ лево тачан добијамо тачан низ

$$0 \to A^{\vee\vee} \xrightarrow{\epsilon^{\vee}} F^{\vee} \to K^{\vee}.$$

Композиција $\epsilon^{\vee} \circ \iota \colon A \to F^{\vee}$ даје тражено утапање. □

Следећа теорема је аналогон теореми 63.

Теорема 91. Следећи услови за леви R-модул I су еквивалентни.

(1) I је инјективан.

(2) Сваки кратак тачан низ $0 \to I \xrightarrow{\mu} A \to A'' \to 0$ се цепа.

(3) I је директан чинилац (фактор) кослободног модула.

Доказ. (1)$\Longrightarrow$(2) следи из дефиниције инјективног модула, ако за A' узмемо баш I, а за ϕ узмемо id_I.

(2)$\Longrightarrow$(3) се добија ако се за μ узме утапање I у кослободан модул.

(3)$\Longrightarrow$(1) следи из ставова 88 и 78. □.

Став 92. Ако је P пројективан, онда је $P^{\vee}$ инјективан.

Доказ. Ако је P пројективан, онда постоји Q и слободан F тако да је $P \bigoplus Q = F$. Тада је $F^{\vee} \cong P^{\vee} \times Q^{\vee}$ и резултат следи. □

Лема 93. Низ $0 \to B' \xrightarrow{\mu} B$ је тачан ако и само је низ $B^{\vee} \xrightarrow{\mu^{\vee}} B'^{\vee} \to 0$ тачан.

Доказ. Како је $\mathbb{Q}/\mathbb{Z}$ инјективан, то је функтор $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ тачан, па из чињенице да је μ „1–1” следи да је $\mu^{\vee}$ „на”, а и из чињенице да је $\mu^{\vee}$ „на” следи да је $\mu^{\vee\vee}$ „1–1”. Но, $\iota_B \circ \mu = \mu^{\vee\vee} \circ \iota_{B'} \colon B' \to B'^{\vee\vee}$, где су $\iota_B, \iota_{B'}$ одговарајућа утапања из става 89 (уверите се у ову једнакост). Стога добијамо да је $\iota_B \circ \mu$ „1–1”, па је и μ „1–1”. □

Теорема 94. Модул A је раван акко је $A^{\vee}$ инјективан.

Доказ. Леви R-модул A је раван акко је за сваки тачан низ

$$0 \to B' \xrightarrow{\mu} B$$

низ

$$0 \to B' \otimes_R A \xrightarrow{\mu \otimes \mathrm{id}_A} B \otimes_R A$$

тачан. Из леме следи да је овај низ тачан акко је низ

$$(B \otimes_R A)^\vee \xrightarrow{(\mu \otimes \mathrm{id}_A)^\vee} (B' \otimes_R A)^\vee \to 0$$

тачан. Но, знамо да имамо природни изоморфизам

$$(B \otimes_R A)^\vee = \mathrm{Hom}_Z(B \otimes_R A, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_\mathbb{Z}(B, \mathrm{Hom}_\mathbb{Z}(A, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}_\mathbb{Z}(B, A^\vee).$$

Стога смо добили да је почетни низ тачан акко је низ

$$\mathrm{Hom}_\mathbb{Z}(B, A^\vee) \xrightarrow{\mu^*} \mathrm{Hom}_\mathbb{Z}(B', A^\vee) \to 0 \tag{30}$$

тачан (уверите се да наведени природни изоморфизам заиста преводи $(\mu \otimes \mathrm{id}_A)^\vee$ у μ^*, где је μ^* стандардно задато са $\mu^*(\phi) = \phi \circ \mu$). Но, $A^\vee$ је инјективан акко је за сваки тачан низ $0 \to B' \xrightarrow{\mu} B$ управо низ (30) тачан. $\square$

Овај одељак завршавамо на сличан начин као и претходни.

Теорема 95. Нека је $\theta\colon R \to S$ хомоморфизам прстена. Нека је S раван као десни R-модул. Тада је сваки инјективан леви S-модул инјективан као леви R-модул.

Доказ. Покажимо најпре да постоји природни изоморфизам:

$$\mathrm{Hom}_S(S \otimes_R A, I) \cong \mathrm{Hom}_R(A, U^\theta I), \tag{31}$$

где је A леви R-модул, а I леви S-модул. Тражени изоморфизам $F\colon \mathrm{Hom}_S(S \otimes_R A, I) \to \mathrm{Hom}_R(A, U^\theta I)$ задајемо са: $\big(F(\phi)\big)(a) := \phi(1_S \otimes a)$. Проверимо најпре да $F(\phi) \in \mathrm{Hom}_R(A, U^\theta I)$.

$$\big(F(\phi)\big)(a_1 + a_2) = \phi(1_S \otimes (a_1 + a_2)) = \phi(1_S \otimes a_1 + 1_S \otimes a_2) = \phi(1_S \otimes a_1) + \phi(1_S \otimes a_2) = \big(F(\phi)\big)(a_1) + \big(F(\phi)\big)(a_2).$$

$$\big(F(\phi)\big)(ra) = \phi(1_S \otimes ra) = \phi(\theta(r) \otimes a) = \theta(r)\phi(1 \otimes a) = r \cdot \phi(1 \otimes a) = r \cdot \big(F(\phi)\big)(a).$$

F јесте хомоморфизам група:

$$\big(F(\phi_1 + \phi_2)\big)(a) = (\phi_1 + \phi_2)(1_S \otimes a) = \phi_1(1_S \otimes a) + \phi_2(1_S \otimes a) = \big(F(\phi_1)\big)(a) + \big(F(\phi_2)\big)(a) = \big(F(\phi_1) + F(\phi_2)\big)(a).$$

$\mathrm{Ker}\, F = \{0_{\mathrm{Hom}_S(S \otimes_R A, I)}\}$. Претпоставимо да је $F(\phi) = 0_{\mathrm{Hom}_R(A, U^\theta I)}$. То значи да је за свако $a \in A$: $\big(F(\phi)\big)(a) = 0_{U^\theta I}$, тј. $\phi(1_S \otimes a) = 0_I$ за све $a \in A$. Ако је $x \in S \otimes_R A$, онда је $x = s_1 \otimes a_1 + \cdots + s_n \otimes a_n$, па је

$$\begin{aligned} &\phi(x) = \phi(s_1 \otimes a_1 + \cdots + s_n \otimes a_n) = \phi(s_1 \otimes a_1) + \cdots + \phi(s_n \otimes a_n) \\ &= \phi(s_1 \cdot (1_S \otimes a_1)) + \cdots + \phi(s_n \cdot (1_S \otimes a_n)) = s_1 \underbrace{\phi(1_S \otimes a_1)}_{0_I} + \cdots + s_n \underbrace{\phi(1_S \otimes a_n)}_{0_I} = 0_I. \end{aligned}$$

Стога је $\phi = 0_{\mathrm{Hom}_S(S \otimes_R A, I)}$.

F је „на”. Нека је $\psi \in \mathrm{Hom}_R(A, U^\theta I)$. Дефинишемо функцију $f\colon S \times A \to I$ са: $f(s,a) := s\psi(a)$ (подсетимо се да је $U^\theta I$ као Абелова група исто што и I, а I јесте и S-модул, те свакако $s\psi(a)$ јесте добро дефинисан елемент из I). Ово f даје јединствен хомоморфизам Абелових група $\overline{f}\colon \mathcal{F}(A \times B) \to I$. Остављамо читаоцима да провере да добијамо индуковани хомоморфизам $\phi\colon S \otimes_R A \to I$. Приметимо да за њега важи: $\phi(1_S \otimes a) = f(1_S, a) = 1_S\psi(a) = \psi(a)$, па је $F(\phi) = \psi$.

Нека је I инјективан леви S-модул. Треба показати да је $U^\theta I$ инјективан леви R-модул. Посматрајмо тачан низ левих R-модула.

$$0 \to A' \xrightarrow{\mu} A \xrightarrow{\epsilon} A'' \to 0. \tag{32}$$

Треба показати да је низ

$$0 \to \mathrm{Hom}_R(A'', U^\theta I) \xrightarrow{\epsilon^*} \mathrm{Hom}_R(A, U^\theta I) \xrightarrow{\mu^*} \mathrm{Hom}_R(A', U^\theta I) \to 0 \tag{33}$$

тачан. Како је S раван R-модул, то је низ

$$0 \to S \otimes_R A' \xrightarrow{\mathrm{id}_S \otimes \mu} S \otimes_R A \xrightarrow{\mathrm{id}_S \otimes \epsilon} S \otimes_R A'' \to 0 \tag{34}$$

тачан. Како је I инјективан леви S-модул, то је низ

$$0 \to \mathrm{Hom}_S(S \otimes_R A'', I) \xrightarrow{(\mathrm{id}_S \otimes \epsilon)^*} \mathrm{Hom}_S(S \otimes RA, I) \xrightarrow{(\mathrm{id}_S \otimes \mu)^*} \mathrm{Hom}_S(S \otimes_R A', I) \to 0 \tag{35}$$

тачан. Остаје само да применимо природни изоморфизам (31) и да проверимо да се добијају заиста наведени хомоморфизми у (33). То остављамо читаоцима. □

Из ове теореме непосредно следи следећа последица.

Последица 96. Нека је G група. Тада је сваки инјективан $\mathbb{Z}[G]$-модул дељива Абелова група. □

7 Нетерини прстени и модули

Дефиниција 97. Леви R-модул A је НЕТЕРИН уколико је сваки подмодул од A коначно генерисан. Прстен R је ЛЕВО НЕТЕРИН уколико је генерисан.

Теорема 98. Нека $A \in {}_R\mathfrak{M}$. Тада су следећи услови за A еквивалентни.

(1) A је Нетерин.

(2) Сваки растући ланац подмодула од A је коначан.

(3) Свака непразна колекција подмодула од A има максимални елемент.

Доказ. (1)$\Longrightarrow$(2). Претпоставимо да постоји бесконачан растући ланац подмодула од A:

$$A_0 \subset A_1 \subset \cdots \subset A_n \subset A_{n+1} \subset \cdots$$

Лако се провери да је $\bar{A} = \bigcup_{i \geqslant 0} A_i$ подмодул од A (проверите то). Из (1) следи да је он коначно генерисан. Нека је $\{x_1, \ldots, x_m\}$ један коначан скуп генератора за $\bar{A}$. Сваки од елемената из овог скупа налази се у неком од подмодула из ланца, јер је $\bar{A}$ унија ових подмодула: $x_j \in A_{k_j}$. Ако је $k = \max\{k_1, \ldots, k_m\}$, онда су сви ови генератори у A_k, јер из $k_j \leqslant k$ следи $A_{k_j} \subseteq A_k$. Дакле, $\{x_1, \ldots, x_m\} \subset A_k$, па је и $\bar{A} \subseteq A_k$, те заправо мора бити $A_k = \bar{A}$. Но, A_k је ПРАВИ подскуп од A_{k+1}, који је пак садржан у A. Ово није могуће, те нам ова контрадикција показује да бесконачан растући ланац подмодула од A не постоји.

(2)$\Longrightarrow$(3). Нека је $\mathcal{A} = \{A_i : i \in I\}$ нека непразна колекција модула. Претпоставимо да она нема максимални елемент. Узмимо било који модул $A_{i_0} \in \mathcal{A}$. Како он није максималан, постоји подмодул $A_{i_1} \in \mathcal{A}$ такав да је $A_{i_0} \subset A_{i_1}$. Но, ни A_{i_1} није максималан, па постоји $A_{i_2} \in \mathcal{A}$ за који је $A_{i_1} \subset A_{i_2}$. И тако настављамо. Добијамо бесконачан растући низ подмодула

$$A_{i_0} \subset A_{i_1} \subset A_{i_2} \subset \cdots$$

но такав низ не може да постоји на основу претпоставке. Стога у $\mathcal{A}$ мора постојати максималан елемент.

(3)$\Longrightarrow$(1). Нека је B подмодул од A. Посматрајмо све подмодуле од B који су коначно генерисани: $\mathcal{A} = \{C \leqslant B : C \text{ је коначно генерисан}\}$. По претпоставци постоји максималан елемент C_0 у $\mathcal{A}$. Ако је $C_0 \subset B$, онда узмимо било који елемент $x \in B \setminus C_0$. Тада је $C_0 \subset C_0 + Rx \leqslant B$, па је $C_0 + Rx \in \mathcal{A}$ елемент у овој колекцији који је већи од максималног. Ова контрадикција нам показује да је $B = C_0$, те је B коначно генерисан. $\square$

Теорема 99. Нека је $0 \to A' \xrightarrow{\mu} A \xrightarrow{\epsilon} A'' \to 0$ кратак тачан низ у ${}_R\mathfrak{M}$. Тада је A Нетерин ако и само ако су A' и A'' Нетерини.

Доказ. Претпоставимо да је A Нетерин. Сваки подмодул од A' се са μ изоморфно слика у подмодул од A. Та слика је коначно генерисана као подмодул Нетериног, па је стога и оригинални подмодул од A' коначно генерисан. Уколико је $B'' \leqslant A$", имамо да је $B\epsilon^{-1}[B''] \leqslant A$, па је B коначно генерисан: $B = Rx_1 + \cdots + Rx_n$ за неке $x_1, \ldots, x_n \in B$. Тада је

$$B'' = \epsilon[\epsilon^{-1}[B'']] = \epsilon[B] = R\epsilon(x_1) + \cdots + R\epsilon(x_n),$$

па је $\{\epsilon(x_1), \ldots, \epsilon(x_n)\}$ генераторни скуп за B'', те је и B'' коначно генерисан.

Претпоставимо сада да су A' и A'' Нетерини и нека је $B \leqslant A$. Његова слика при ϵ, $\epsilon[B]$, је подмодул од A'', па је коначно генерисан. Нека су $x_1, \ldots, x_m$ елементи из A чије слике при ϵ генеришу $\epsilon[B]$. Имамо и да је $\mu^{-1}[B]$ подмодул од A', који је Нетерин, па је и $\mu^{-1}[B]$ коначно генерисан. Нека су $y_1, \ldots, y_n \in A'$ генератори за $\mu^{-1}[B]$. Покажимо да је $\{\mu(y_1), \ldots, \mu(y_n), x_1 \ldots, x_m\}$ скуп генератора за B. У ту сврху, претпоставимо да $x \in B$. Тада $\epsilon(x) \in \epsilon[B]$, па постоје $r_1, \ldots, r_m$ такви да је $\epsilon(x) = r_1\epsilon(x_1) + \cdots + r_m\epsilon(x_m)$. То значи да је $\epsilon(x - r_1x_1 - \cdots - r_mx_m) = 0_{A''}$, па из тачности низа добијамо да је $x - r_1x_1 - \cdots - r_nx_n = \mu(y)$ за неко $y \in A'$. Но, како $x - r_1x_1 - \cdots - r_mx_m \in B$, имамо да $y \in \mu^{-1}[B]$, па постоје $s_1, \ldots, s_n \in R$такви да је $y = s_1y_1 + \cdots + s_ny_n$. Коначо добијамо $x - r_1x_1 - \cdots - r_nx_n = s_1\mu(y_1) + \cdots + s_n\mu(y_n)$, те је

$$x = s_1\mu(y_1) + \cdots + s_n\mu(y_n) + r_1x_1 + \cdots + r_mx_m,$$

што нам показује да је горенаведени коначни скуп заиста скуп генератора за B. $\square$

Последица 100. Ако су A_1 и A_2 подмодули од A, онда је $A_1 + A_2$ Нетерин ако и само ако су A_1 и A_2 Нетерини.

Доказ. Ако са $\iota_i \colon A_1 \to A_1 + A_2$ означимо укључење, из кратког тачног низа

$$0 \to A_1 \xrightarrow{\iota_1} A_1 + A_2 \to (A_1 + A_2)/A_1 \to 0$$

и претходне теореме, добијамо да је $A_1 + A_2$ Нетерин ако и само ако су A_1 и $(A_1 + A_2)/A_1$ Нетерини. Из теореме 26 имамо изоморфизам $(A_1 + A_2)/A_1 \cong A_2/A_1 \cap A_2$. Ако са $j_1 \colon A_1 \cap A_2 \to A_2$ означимо укључење, онда из кратког тачног низа

$$0 \to A_1 \cap A_2 \xrightarrow{j_1} A_2 \to A_2/A_1 \cap A_2) \to 0$$

и претходне теореме, добијамо да је A_2 Нетерин ако и само ако су $A_1 \cap A_2$ и $A_2/A_1 \cap A_2$ Нетерини.

Дакле, ако је A_2 Нетерин, добијамо да је то и $A_2/(A_1 \cap A_2)$, па је тада и $(A_1 + A_2)/A_1$ Нетерин, као њему изоморфан модул. Ако додамо и претпоставку да је A_1 Нетерин, добијамо да је тада и $A_1 + A_2$ Нетерин, на основу првог закључка у овом доказу. Наравно, из претпоставке да је $A_1 + A_2$ Нетерин, на основу претходне теореме директно закључујемо да су и његови подмодули A_1 и A_2 Нетерини. $\square$

Последица 101. Коначна директна сума Нетериних модула је Нетерин модул.

Доказ. Нека су $A_1, \ldots A_n$ Нетерини модули, $q_i \colon A_i \to (A_1 \bigoplus \cdots \bigoplus A_n)$ одговарајућа структурна пресликавања. Тада је $A_i \cong q_i[A_i]$ и

$$A_1 \bigoplus \cdots \bigoplus A_n = q_1[A_1] + \cdots + q_n[A_n]$$

и резултат следи из претходне последице. $\square$

Последица 102. Нека је R лево Нетерин прстен. Тада је сваки коначно генерисан леви R-модул Нетерин и он се може коначно представити.

Доказ. На основу претходне последице следи да је сваки коначно генерисан слободан леви R-модул Нетерин, јер је он коначна директна сума од R. Но, сваки коначно генерисан леви R-модул A је хоморфна слика коначно генерисаног слободног левог R-модула, тј. постоји тачан низ

$$0 \to K \xrightarrow{\iota} F_0 \xrightarrow{\epsilon} A \to 0,$$

за неки коначно генерисан слободан леви R-модул F_0 (овде је ι укључење $K = \operatorname{Ker} \epsilon$ у F_0) па је на основу теореме 99 и он Нетерин.

Како је F_0 Нетерин, то је његов подмодул K коначно генерисан, па постоји коначно генерисан слободан модул F_1 и $\epsilon_1 \colon F_1 \to K$, који је „на". Тако добијамо тачан низ

$$F_1 \to F_0 \to A \to 0,$$

који показује да се A може коначно представити. □

Теорема 103. Сваки коначно генерисан раван модул над лево Нетериним прстеном је пројективан.

Доказ. Резултат следи на основу претходне последице и теореме 73.□

Теорема 104. Нека је R комутативан прстен. Ако је R Нетерин, онда је и $R[X]$ Нетерин.

Доказ. Уколико је $a(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ полином за који је $a_n \neq 0$, тада пишемо да је $LC(a(X)) = a_n$ (a_n је водећи коефицијент у $a(X)$). Нека је I идеал у прстену $R[X]$. Дефинишимо идеал I_n у прстену R са:

$$I_n \colon = \{a_n \in R : (\exists a(X) \in R[X])(\deg a(X) = n \text{ и } LC(a(X)) = a_n)\} \cup \{0\}.$$

Кратко: у I_n се налазе водећи коефицијенти свих полинома степена n који се налазе у идеалу I, а осим њих је ту и 0 (нула нам је неопходна да бисмо имали идеал, а морамо је овако додати, јер она не може бити водећи коефицијент ниједног ненула полинома).

Докажимо најпре да је I_n идеал у R. Нека је $a_n \in I_n$ и $b \in R$. Ако је $ba_n = 0$, онда свакако $ba_n \in I_n$. Ако је $ba_n \neq 0$ и ако је $a(X) \in I$ полином степена n у I чији је водећи коефицијент a_n, онда је $ba(X)$ полином степена n у I чији је водећи коефицијент ba_n, па закључујемо да $ba_n \in I_n$.

Уколико $a_n, b_n \in I_n$, нека су $a(X)$, $b(X)$ полиноми степена n из I, такви да је $LC(a(X)) = a_n$, а $LC(b(X)) = b_n$. Ако је $a_n + b_n = 0$, онда је јасно да $a_n + b_n$ припада I_n. У супротном, полином $a(X) + b(X)$ је полином степена n из I (јер је I идеал) чији је водећи коефицијент $a_n + b_n$, те $a_n + b_n \in I_n$.

Није тешко доказати да је $I_n \subseteq I_{n+1}$. Наиме, ако је $a_n \in I_n$, онда постоји полином $a(X)$ из I степена n такав да је $LC(a(X)) = a_n$. Тада је $Xa(X)$ полином степена $n+1$ у I чији је водећи коефицијент такође a_n, те $a_n \in I_{n+1}$.

Тако смо добили неопадајући низ идеала у R:

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

Како је прстен R Нетерин, то је овај низ идеала стационаран, тј. постоји $m \geqslant 0$ тако да је $I_n = I_m$ за све $n \geqslant m$ (не постоји бесконачан растући низ). Осим тога, сви идеали I_k су коначно генерисани и нека је, за $0 \leqslant k \leqslant m$:

$$I_k = \langle a_{k1}, \ldots, a_{ks_k} \rangle$$

Са $\langle r_1, \ldots, r_k \rangle$ означавамо идеал генерисан елементима $r_1, \ldots, r_k$. Нека су $f_{kj_k} \in I$ полиноми степена k такви да је $LC(f_{kj_k}) = a_{kj_k}$. Докажимо да полиноми f_{kj_k} за $0 \leqslant k \leqslant m$, $1 \leqslant j_k \leqslant s_k$ генеришу идеал I. Означимо са $\widetilde{I}$ идеал у $R[X]$ генерисан овим полиномима. Очигледно је $\widetilde{I} \subseteq I$. Докажимо другу инклузију.

Нека је $f \in I \setminus \{0\}$. Доказ изводимо индукцијом по степену полинома f.

Претпоставимо да је $\deg f = 0$. То значи да је заправо f константан полином и да се налази у I_0. Како су и полиноми $f_{01}, \ldots, f_{0s_0}$ константни полиноми који генеришу овај идеал, видимо да $f \in \widetilde{I}$.

Претпоставимо да је полином f степена t и да је тврђење доказано за све полиноме степена мањег од t, Имамо две могућности.

$\mathbf{t \leqslant m}$. Дакле, f је полином степена t, те $LC(f) \in I_t$. Како $a_{t1}, \ldots, a_{ts_t}$ генеришу идеал I_t, то постоје $b_{t1}, \ldots, b_{ts_t} \in R$ такви да је

$$LC(f) = b_{t1}a_{t1} + \cdots + b_{ts_t}a_{ts_t}.$$

Подсетимо се да је $a_{tj_t} = LC(f_{tj_t})$ и да је $\deg f_{tj_t} = t$. То значи да је

$$\deg(f - b_{t1}f_{t1} - \cdots - b_{ts_t}f_{ts_t}) < t,$$

а овај полином свакако припада идеалу I. По индуктивној хипотези закључујемо да он припада $\widetilde{I}$, па је и $f \in \widetilde{I}$.

$\mathbf{t > m}$. Дакле, f је полином степена t, те $LC(f) \in I_t = I_m$. Како $a_{m1}, \ldots, a_{ms_m}$ генеришу идеал I_m, то постоје $b_{m1}, \ldots, b_{ms_m} \in R$ такви да је

$$LC(f) = b_{m1}a_{m1} + \cdots + b_{ms_m}a_{ms_m}.$$

Подсетимо се да је $a_{mj_m} = LC(f_{mj_m})$ и да је $\deg f_{mj_t} = m$. То значи да је

$$\deg(f - X^{t-m}b_{m1}f_{m1} - \cdots - X^{t-m}b_{ms_m}f_{ms_m}) < t,$$

а овај полином свакако припада идеалу I. По индуктивној хипотези закључујемо да он припада $\widetilde{I}$, па је и $f \in \widetilde{I}$.

Ово и завршава доказ, јер смо показали да коначно много полинома генеришу идеал I. □

Индукцијом се добија следећа последица.

Последица 105. Ако је R комутативан Нетерин прстен, $n \geqslant 1$, онда је и прстен $R[X_1, \ldots, X_n]$ Нетерин. □

Прстен полинома са бесконачно много неодређених $R[X_1, X_2, \ldots]$ није Нетерин, јер садржи бесконачан растући низ идеала:

$$\langle X_1 \rangle \subset \langle X_1, X_2 \rangle \subset \cdots$$

За крај овог одељка наведимо још један пример прстена који није Нетерин.

Пример 106. Нека је R прстен свих непрекидних функција $f\colon [0,1] \to \mathbb{R}$, при чему су операције међу функцијама дефинисане тачка по тачка:

$$(f+g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Посматрајмо низ идеала $I_n = \{f \in R : (\forall x < \frac{1}{n}) f(x) = 0\}$ (уверите се да је I_n идеал у R). Јасно је да је $I_n \subset I_{n+1}$. Наиме, како је $\frac{1}{n+1} < \frac{1}{n}$, јасно је да из $f(x) = 0$ за $x < \frac{1}{n}$ следи да је $f(x) = 0$ за $x < \frac{1}{n+1}$, но функција $g : [0,1] \to \mathbb{R}$ дефинисана са

$$g(x) = \begin{cases} 0, & x \leqslant \frac{1}{n+1} \\ x - \frac{1}{n+1} & \text{иначе,} \end{cases}$$

припада I_{n+1}, али не припада I_n, те имамо бесконачан растући низ идеала. Дакле, прстен R није Нетерин. ♣

8 Модули над главноидеалским и Дедекиндовим доменима

У овом одељку, разматраћемо модуле над главноидеалским и Дедекиндовим доменима. Подсетимо се да је домен комутативан прстен са јединицом у коме нема правих делитеља нуле. Да бисмо истакли да радимо са доменима, типично ћемо их означавати са D (као што смо опште прстене означавали са R).

Најпре се бавимо главноидеалским доменима. Главни примери су $\mathbb{Z}$ и $K[X]$ за неко поље K.

Теорема 107. Подмодул слободног D-модула, где је D главноидеалски домен, и сам је слобододан. Посебно, сваки пројективан D-модул над главноидеалским доменом је слободан.

Доказ. Нека је $F = \bigoplus_{i\in I} D$ слободан D-модул. Према принципу доброг уређења, $I = \{i_\alpha : \alpha < \mu\}$ за неки ординал μ (за оне који нису упознати са појмовима ординала сугеришемо да погледају, на пример, књигу *Математичка логика – Елементи теорије скупова*, аутора З. Петровића и Ж. Мијајловића). Нека је A подмодул од F. Конструисаћемо базу B за A на следећи начин. Означимо са $\pi_\alpha\colon F \to D$ пројекцију на координату i_α. Уведимо и ознаку $F_\alpha = \bigoplus_{i_\beta, \beta\leqslant\alpha} D$.

Постављамо $B_0 = \emptyset$.

Претпоставимо да је B_α дефинисано за неки ординал $\alpha < \mu$. Дефинишемо $B_{s(\alpha)}$ са

$$B_{s(\alpha)} = \begin{cases} B_\alpha, & \pi_\alpha[F_\alpha \cap A] = \{0\} \\ B_\alpha \cup \{f_\alpha\}, & \pi_\alpha(f_\alpha) \text{ је генератор од } \pi_\alpha[F_\alpha \cap A] \neq \{0\}. \end{cases}$$

Уколико је $\lambda \leqslant \mu$ гранични ординал, дефинишемо $B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha$. Тврдимо да је $B = B_\mu$ база за A.

B је линеарно независан скуп. Нека је $d_1 f_{\alpha_1} + \cdots + d_n f_{\alpha_n} = 0$ за неке $\alpha_1 < \cdots < \alpha_n < \mu$ и $d_1, \ldots, d_n \in D$. Тада је

$$0 = \pi_{\alpha_n}\big(d_1 f_{\alpha_1} + \cdots + d_n f_{\alpha_n}\big) = d_n \pi_{\alpha_n}(f_{\alpha_n}) \in D,$$

а $\pi_{\alpha_n}(f_{\alpha_n}) \neq 0$. Како је D домен, добијамо да је $d_n = 0$. Понављањем поступка добијамо да су сви коефицијенти једнаки 0.

B је скуп генератора за A. Нека је $x \in A$. Како је $x \in F$, то је $x \in F_\alpha$ за неко $\alpha < \mu$. Дакле, $x \in F_\alpha \cap A$ и нека је α најмањи ординал за који то важи. Стога је $\pi_\alpha(x) \neq 0$ и постоји $d_\alpha \in D$ тако да је $\pi_\alpha(x) = d_\alpha \pi_\alpha(f_\alpha)$, јер је $\pi_\alpha(f_\alpha)$ генератор слике $\pi_\alpha[F_\alpha \cap A]$. Тада $x - d_\alpha f_\alpha \in A \cap F_\beta$ за неки $\beta < \alpha$ и нека је α_1 најмањи такав. Понављамо поступак. Он се свакако завршава у коначно много корака пошто не постоји бесконачан опадајући низ ординала. Стога је B заиста скуп генератора. □

Дефиниција 108. D-модул A је ДЕЉИВ уколико за свако $a \in A$ и свако $d \neq 0$ из D постоји $y \in A$ тако да је $dy = x$.

Следећа теорема се доказује на исти начин на који и теорема 82 те стога доказ не наводимо.

Теорема 109. D-модул је инјективан ако и само ако је дељив.

Дефиниција 110. Нека је $a \in A \setminus \{0\}$, где је A D-модул. АНУЛАТОРСКИ ИДЕАЛ или, краће, АНУЛАТОР елемента a дефинише се са: $\mathrm{ann}(a) := \{d \in D : da = 0\}$. Јасно је да је ово идеал у D. Уколико је $\mathrm{ann}(a) \neq \{0\}$, за елемент a кажемо да је ТОРЗИОНИ и РЕД елемента a се дефинише као генератора овог идеала (који је наравно одређен до на инвертибилни умножак). Уколико је $\mathrm{ann}(a) = \{0\}$ кажемо и да је a бесконачног реда.

Став 111. Нека је A један D-модул. Тада је $T(A) := \{a \in A : \operatorname{ann}(a) \neq \{0\}\}$ један подмодул од A и називамо га торзиони подмодул.

Доказ. Нека $a_1, a_2 \in T(A)$. То значи да постоје $d_1, d_2 \in D$ такви да је $d_1 a_1 = 0_A$, $d_2 a_2 = 0_A$. Тада је $d_1 d_2 \neq 0_D$ и

$$d_1 d_2 (a_1 - a_2) = d_2(d_1 a_1) - d_1(d_2 a_2) = 0_A = d_2 0_A + d_1 0_A = 0_A,$$

па $a_1 - a_2 \in T(A)$. Такође, ако је $d \in D$, онда је

$$d_1(da_1) = (d_1 d)a_1 = (dd_1)a = d(d_1 a_1) = d0_A = 0_A,$$

па $da_1 \in T(A)$. □

Уколико за модул A важи да је $T(A) = \{0_A\}$, кажемо да је A торзионо слободан.

Став 112. Нека је A један D-модул, $T(A)$ његов торзиони подмодул. Тада је D-модул $A/T(A)$ торзионо слободан.

Доказ. Нека је $a + T(A) \in T\big(A/T(A)\big)$. То значи да постоји $d \in D \setminus \{0\}$ тако да је $d(a + T(A)) = 0_{A/T(A)}$, те $da \in T(A)$. Но, то значи да постоји $d' \in D \setminus \{0\}$ тако да је $d'(da) = 0_A$. Тада је и $(d'd)a = 0_A$, при чему је $d'd \neq 0_D$, па је $a \in T(A)$. Закључујемо да је $T\big(A/T(A)\big) = 0_{A/T(A)}$, па је $A/T(A)$ торзионо слободан. □

Теорема 113. Нетривијалан, коначно генерисан торзионо слободан D-модул је слободан.

Доказ. Најпре, приметимо да је сваки главноидеалски домен тривијално Нетерин домен. Стога је сваки коначно генерисан D-модул Нетерин.

Нека је $A \neq \{0\}$ торзионо слободан и коначно генерисан. Како сваки елемент $x \in A$ генерише слободан подмодул од A (функција која слика d у dx је изоморфизам D-модула – уверите се у то), то постоје слободни подмодули од A.

Означимо са $\mathcal{F}$ колекцију свих слободних подмодула од A. Видели смо да је она непразна. Како је A Нетерин, постоји максималан елемент M у $\mathcal{F}$. Нека је $\{x_1, \ldots, x_n\}$ скуп генератора за A. Уколико је $Dx_i \cap M = \{0\}$, онда је $Dx_i \dotplus M$ слободан подмодул од A који је већи од максималног. Стога постоји $d' \in D \setminus \{0\}$ за који је $d'x_i \in M$. То заправо значи да је $\operatorname{ann}(x_i + M) \neq \{0\}$. Означимо са d_i генераторе ових анулатора. Посматрајмо елемент $d = d_1 \cdots d_n$. Овај елемент је у пресеку свих ових анулатора, па $dx_i \in M$ за све i.

То значи да је dA подмодул од M. Но, функција $\phi\colon A \to dA$ задата са $\phi(a) = da$ успоставља изоморфизам између A и dA (наравно да је „на" и лако се провери да је модулски хомоморфизам; језгро је тривијално зато што је A торзионо слободан). Но, dA је подмодул слободног модула M, па је и сам слободан, те следи да је и A слободан. □

Ми свакако можемо да покажемо да ако постоји бијекција између скупова X и X', онда постоји и изоморфизам слободне групе F на скупу X и слободне групе F' на скупу X', но ипак још не знамо да ли из изоморфизма коначно генерисаних слободних D-модула F и F' следи да они имају исти број елемената у својим базама. Свакако се при изоморфизму база слика у базу, те је заправо централно питање: да ли сваке две базе у коначно генерисаном слободном модулу имају исти број елемената?

Теорема 114. Нека је F слободан D-модул, где је D домен, који има генераторни скуп од n елемената. Тада он има базу са највише n елемената. Штавише, сваке две базе од F имају исти број елемената.

Доказ. Идеја је да се пребацимо на случај векторских простора над пољем где су нам ово добро позната тврђења. У ту сврху, означимо са $Q(D)$ поље разломака над D. Подсетимо се да је то поље које се од D добија инвертовањем свих ненула елемената (D је домен) и чија конструкција одговара конструкцији рационалних бројева полазећи од целих бројева. Тада имамо и хомоморфизам $D \to Q(D)$, $x \mapsto \frac{x}{1}$, који је „1–1". Тада је и индуковани морфизам D- модула $F \otimes_D D \to F \otimes_D Q(D)(= \overline{F})$ „1–1". Но, $F \cong F \otimes_D D$, где се $x \mapsto x \otimes 1$, па имамо „1–1" хомоморфизам $\phi\colon F \to \overline{F}$ задат са $\phi\colon x \mapsto x \otimes 1$. Но, $\overline{F}$ је векторски простор над $Q(D)$. Важи следеће.

1. Ако су $x_1, \ldots, x_n$ генератори од F (не нужно слободни генератори), онда су $\phi(x_1), \ldots, \phi(x_n)$ генератори за $\overline{F}$. Довољно је показати да се сваки елемент из $\overline{F}$ облика $x \otimes \frac{r}{s}$ може приказати као линеарна комбинација ових. Но, $x = \sum_{i=1}^n d_i x_i$, јер су x-ови генератори, па је $x \otimes 1 = (\sum_{i=1}^n d_i x_i) \otimes 1 = \sum_{i=1}^n d_i(x_i \otimes 1) = \sum_{i=1}^n d_i \phi(x_i)$, па добијамо и да је $x \otimes \frac{r}{s} = \frac{r}{s}(x \otimes 1) = \frac{r}{s} \sum_{i=1}^n d_i \phi(x_i) = \sum_{i=1}^n \frac{r}{s} d_i \phi(x_i)$.

2. Ако су $x_1, \ldots x_n$ линеарно независни у F, онда су $\phi(x_1), \ldots, \phi(x_n)$ линеарно независни у $\overline{F}$. Претпоставимо да је $\sum_{i=1}^n \frac{r_i}{s_i} \phi(x_i) = 0_{\overline{F}}$. Нека је $S = s_1 \ldots s_n$, а $R_i = \frac{r_i S}{s_i}$. Добијамо да је $\frac{1}{S} \sum_{i=1}^n R_i x_i \otimes 1 = 0_{\overline{F}}$. Стога је и $\phi\big(\sum_{i=1}^n R_i x_i\big) = \sum_{i=1}^n R_i x_i \otimes 1 = 0_{\overline{F}}$. Како је ϕ „1–1", добијамо да је $\sum_{i=1}^n R_i x_i = 0_F$, те, како су x_i линеарно независни, следи да је $R_1 = \cdots = R_n = 0_D$, те се добија и да је $\frac{r_1}{s_1} = \cdots = \frac{r_n}{s_n} = 0_{Q(D)}$.

Докажимо сада тражено. Како је F слободан, он свакако има неку базу. Уколико би он имао базу са више од n елемената, та база би се са ϕ превела у базу векторског простора $\overline{F}$ са више од n елемената. Но, на основу претпоставке и доказаног, у $\overline{F}$ постоји генераторни скуп од n елемената, а из Линеарне алгебре знамо да тада у $\overline{F}$ постоји база за највише n елемената, а и свака база има исти број елемената. Стога у $\overline{F}$ свакако нема базе са више од n елемената. Осим тога, ако би у F постојале две базе које немају исти број елемената, оне би се са ϕ пресликале у базе од $\overline{F}$ које немају исти број елемената, а то није могуће. $\square$

Дакле, број елемената у бази коначно генерисаног слободног модула над доменом је јединствено одређен и назива се ранг слободног модула.

Следећом последицом теореме 113 започињемо класификацију коначно генерисаних модула над главноидеалским доменом.

Последица 115. Коначно генерисан D-модул је директна сума свог торзионог подмодула и коначно генерисаног слободног D-модула.

Доказ. Нека је A коначно генерисан D-модул. Посматрајмо тачан низ

$$0 \to T(A) \to A \to A/T(A) \to 0.$$

По претходној теореми је $A/T(A)$ коначно генерисан слободан D-модул и стога се овај низ цепа на основу теореме 63. Тако смо добили да је $A \cong T(A) \bigoplus A/T(A)$. □

Ако је $\phi\colon A \to A'$ изоморфизам коначно генерисаних модула над D, онда је свакако $\phi[T(A)] = T(A')$, пошто изоморфизам чува ред елемента ($d\phi(a) = 0$ акко $\phi(da) = 0$ акко $da = 0$) и индукује изоморфизам $\overline{\phi}\colon A/T(A) \to A'/T(A')$, а коначно генерисани слободни модули су потпуно одређени својим рангом. Сада можемо да се фокусирамо на торзиони подмодул.

Како је сваки главноидеалски домен D нужно и домен са једнозначним растављањем (факторизацијом), то се сваки елемент из D може представити у облику производа простих елемената и тај приказ је јединствен то на пермутацију и умношке инвертибилним елементима. Сетимо се да су два елемента a и b придружена (асоцирана) уколико постоји инвертибилан елемент u за који је $a = ub$. Ово је релација еквиваленције и претпоставимо да смо изабрали по један прост елемент из сваке од тих класа еквиваленције. Означимо скуп таквих елемената, за дати домен D, са $P(D)$.

Ако је T ма који торзиони модул над D, онда, за $p \in P(D)$, можемо посматрати скуп $T_p := \{x \in D :$ ред елемента x је степен од $p\}$. Да бисмо скратили писање, ред елемента x означимо са $\omega(x)$. Дакле, за сваки $x \in T_p$ постоји $\alpha \geqslant 1$ тако да је $\omega(x) = p^{\alpha}$.

Теорема 116. Нека је T торзиони D-модул. Тада су, за све $p \in P(D)$, T_P подмодули од T и T је њихова (унутрашња директна сума):

$$T = \dot{\sum_{p \in P(D)}} T_p.$$

Доказ. Ако $x, y \in T_p$, онда је $p^{\alpha}x = 0$ и $p^{\beta}y = 0$ за неке $\alpha, \beta \geqslant 1$, па је $p^{\max\{\alpha,\beta\}}(x - y) = 0$. За $d \in D$, имамо да је $p^{\alpha}(dx) = d(p^{\alpha}x) = 0$. Стога је T_p подмодул од T.

Покажимо најпре да је T сума својих подмодула T_p. Нека је $x \in T$ и $\omega(x) = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, где је u инвербилан и $\alpha_i \geqslant 1$ за све i. Нека је $r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ и $r_i = \frac{r}{p_i^{\alpha_i}}$. Тада су r_i узајамно прости, те је идеал који они генеришу једнак целом прстену. Стога постоје s_i такви да је $r_1 s_1 + \cdots + r_k s_k = 1$. Тада је $x = r_1 s_1 x + \cdots + r_k s_k x$, а $\omega(r_i x) = p^{\alpha_i}$. Стога је $x = x_1 + \cdots + x_k$, где $x_i \in T_{p_i}$ за све i.

Ова сума је директна. Наиме, нека $x \in T_p \cap (\underset{q \neq p}{\dot{+}} T_q)$. То значи да је $x = x_1 + \cdots + x_l$, где је $p^\alpha x = 0 = q_i^{\alpha_i} x_i$ за све i. Ако је $r = q_1^{\alpha_1} \cdots q_l^{\alpha_l}$, онда је $r x_i = 0$ за све i, па је $rx = r(x_1 + \cdots x_l) = 0$. Како су p^α и r узајамно прости, они генеришу цео прстен. Дакле, постоје d_1, d_2 такви да је $1 = d_1 p^\alpha + d_2 r$. Тада имамо да је $x = 1x = d_1 p^\alpha x + d_2 r x = 0$. □

Заправо, у овим сумама се појављују само прости елементи који су фактори у редовима генератора.

Став 117. Нека X генерише T. Посматрајмо следећи скуп простих елемета. $P_X(D) := \{p \in P : (\exists x \in X) p \mid \omega(x)\}$. Тада је $T_p \neq \{0\}$ ако и само ако $p \in P_X(D)$. Посебно, ако је скуп X коначан, растав T из претходне теореме је на коначан сабирака.

Доказ. Јасно је да, ако је $p \in P_X(D)$, имамо елемент $x \in X$ који је реда $p^\alpha r$, где $p \nmid r$, за неко $\alpha \geqslant 1$. Тада је $\omega(rx) = p^\alpha$, те $rx \in T_p$, па $T_p \neq \{0\}$.

Нека сад $p \notin P_X(D)$. Ако је $x \in T_p$, то постоје $x_1, \ldots, x_n \in X$ такви да је $x = s_1 x + \cdots + s_n x_n$ за неке $s_i \in D$. Ако је $r_i = \omega(x_i)$, и $r = r_1 \cdots r_n$, онда је $rx = s_1 r x_1 + \cdots + s_n r x_n = 0$. Но, из $x \in T_p$ следи да је $\omega(x) = p^\alpha$ за неко $\alpha \geqslant 1$. Но, $p \nmid r$, па, као и раније, постоје $d_1, d_2 \in D$ такви да је $1 = d_1 p^\alpha + d_2 r$. Тада је $x = 1x = d_1 p^\alpha x + d_2 r x = 0$. Стога је $T_p = \{0\}$. □

Сваки изоморфизам $\phi \colon A \to A'$ коначно генерисаних D-модула успоставља изоморфизам између $T_p(A)$ и $T_p(A')$, који су наравно и сами коначно генерисани. Остаје да установимо каква је структура од $T_p(A)$. Модуле за које је ред сваког ненула елемента степен од p, где је p прост, називамо p-модулима.

Теорема 118. Нека је $T \neq \{0\}$ коначно генерисан p-модул. Тада је

$$T \cong C_{p^{\alpha_1}} \bigoplus C_{p^{\alpha_2}} \bigoplus \cdots \bigoplus C_{p^{\alpha_k}}, \quad \alpha_1 \geqslant \alpha_2 \geqslant \cdots \alpha_k \geqslant 1,$$

где је $C_{p^{\alpha_i}}$ циклични модул чији је генератор реда p^{α_i}. Штавише, $\alpha_1, \ldots, \alpha_k$ су јединствено одређени модулом T.

Доказ. Нека је k минималан број чланова базе. За сваку базу од k чланова формирамо k-торку бројева $(\alpha_1, \ldots, \alpha_k)$ за које је $\alpha_1 \geqslant \cdots \geqslant \alpha_k \geqslant 1$, а p^{α_i} су редови тих базних елемената. Сада се посматра минимум збира $\alpha_1 + \cdots + \alpha_k$ и нека је $(x_1, \ldots, x_k)$ одговарајући скуп генератора. Покажимо да је $T_P = Dx_1 \dot{+} \cdots \dot{+} Dx_k$, што ће нам дати тражену декомпозицију.

Претпоставимо да ова сума није директна, тј. да је

$$(Dx_1 + \cdots + Dx_i) \cap Dx_{i+1} \neq \{0\}$$

за неко $i \in \{1, \ldots, k-1\}$. Нека је $I \lhd D$ задат са:

$$I = \{r \in D : rx_{i+1} \in Dx_1 + \cdots + Dx_i\}.$$

По претпоставци он није тривијалан и имамо да је $I = dD$, за неко $d \in D$. Како $p^{\alpha_{i+1}}x_{i+1} = 0$ свакако припада суми, то $d \mid p^{\alpha_{i+1}}$. Стога је $d = p^\beta$ за неко $\beta < \alpha_{i+1}$ (јер је $p^{\alpha_{i+1}}x_{i+1} = 0$, а у пресеку има елемената различитих од нуле). Дакле,

$$p^\beta x_{i+1} = \sum_{j=1}^{i} d_j p^{\gamma_j} x_j, \tag{36}$$

при чему $p \nmid d_j$ за $j = \overline{1, i}$. Множењем са $p^{\alpha_{i+1}-\beta}$ добијамо

$$0 = p^{\alpha_{i+1}} x_{i+1} = \sum_{j=1}^{i} d_j p^{\gamma_j + \alpha_{i+1} - \beta} x_j.$$

Зато мора бити $\gamma_j + \alpha_{i+1} - \beta \geqslant \alpha_j$, за све j. Стога је $\gamma_j - \beta \geqslant \alpha_j - \alpha_{j+1} \geqslant 0$, па је $\gamma_j \geqslant \beta$. Нека је $x' = x_{i+1} - \sum_{j=1}^{i} d_j p^{\gamma_j - \beta} x_j$. Но, из (36) следи да је $p^\beta x' = 0$. Како је и $(x_1, \ldots, x_i, x', x_{i+2}, \ldots, x_k)$ једна k-торка генератора, а збир њихових редова је мањи од $\sum_{i=1}^{k} \alpha_i$, добили смо контрадикцију и закључујемо да је сума заиста директна и имамо тражени изоморфизам.

Докажимо да из $T = C_{p^{\alpha_1}} \bigoplus \cdots \bigoplus C_{p^{\alpha_k}} \cong C_{p^{\beta_1}} \bigoplus \cdots \bigoplus C_{p^{\beta_l}} = T'$ следи да је $k = l$ и $\alpha_i = \beta_i$ за све i. Најпре, $\alpha_1 = \min\{\alpha \geqslant 1 : p^\alpha T = 0\}$. Стога је $\alpha_1 = \beta_1$. Радимо индукцијом по α_1.

Ако је $\alpha_1 = 1$, онда је $T = \sum_{i=1}^{k} C_p$, а ово су све векторски простори над пољем D/pD, па је $k = \dim T$ и стога је $k = l$, јер је $T \cong T'$.

Нека је $\alpha_1 \geqslant \cdots \geqslant \alpha_m \geqslant 2 > \alpha_{m+1} = \cdots = \alpha_k = 1$, а $\beta_1 \geqslant \cdots \geqslant \beta_n \geqslant 2 > \beta_{n+1} = \cdots = \beta_l = 1$. Имамо изоморфизам $pT \cong pT'$, односно $C_{p^{\alpha_1 - 1}} \bigoplus \cdots \bigoplus C_{p^{\alpha_m - 1}} \cong C_{p^{\beta_1 - 1}} \bigoplus \cdots \bigoplus C_{p^{\beta_n - 1}}$. По индуктивној хипотези можемо да закључимо да је $m = n$ и $\alpha_i = \beta_i$ за $i = \overline{1, m}$. Но, имамо и да је $T/pT \cong T'/pT'$, тј. $\bigoplus_{i=1}^{k} C_p \cong \bigoplus_{i=1}^{l} C_p$, па добијамо да је и $k = l$. Стога су и остали одговарајући бројеви једнаки и имамо тражену јединственост. $\square$

Приметимо да је циклични модул C_{p^α} заправо изоморфан количничком прстену $D/p^\alpha D$. Наиме, ако је x генератор тог модула, онда је $\operatorname{ann}(x) = p^\alpha D$, а $\operatorname{ann}(x)$ је заправо језгро хомоморфизма $\phi \colon D \to T_p$ задатог са $\phi(d) = dx$. Стога можемо да сажмемо све до сада што смо радили о класификацији коначно генерисаних модула над главноидеалски доменом D у следећој теореми. Са D^n наравно означавамо директну суму $\bigoplus_{i=1}^{n} D$.

Теорема 119. Сваки коначно генерисани модул над главноидеалским доменом изоморфан је модулу

$$\Big(\bigoplus_{i=1}^{n}\Big(\bigoplus_{j=1}^{m} D/p_i^{\alpha_{ij}}D\Big)\Big)\bigoplus D^r, \quad \alpha_{i1}\geqslant\cdots\geqslant\alpha_{im}\geqslant 1, \text{ за све } i=\overline{1,n}, \quad r\geqslant 0.$$

Прости елементи p_i су одређени једнозначно до на придруженост и редослед фактора. □

У наставку овог одељка, бавићемо се коначно генерисаним модулима над Дедекиндовим доменима. Најпре дајемо дефиницију Дедекиндових домена.

Дефиниција 120. Дедекиндов домен је комутативан прстен са јединицом у коме нема правих делитеља нуле и у коме за свака два идеала $I\subseteq J$ постоји идеал K такав да је $I = J\cdot K$.

Став 121. Ако су $I, J \neq \{0\}$, онда је идеал K из претходне дефиниције је јединствено одређен.

Доказ. Нека је $J\cdot K = J\cdot K'$. Ако је $b\in J\setminus\{0|]$, имамо да је $bD\subseteq J$, па постоји L тако да је $\langle b\rangle = L\cdot J$. Имамо да је тада $L\cdot J\cdot K = L\cdot J\cdot K'$, те следи $\langle b\rangle\cdot K = \langle b\rangle\cdot K'$, тј. $bK = bK'$. Како је D домен, добијамо да је $K = K'$. □

Дефиниција 122. За два идеала I и J у Дедекиндовом домену D кажемо да су у истој класи идеала уколико постоје $x, y\in D\setminus\{0\}$, за које је $xI = yJ$.

Са $[I]$ означићемо класу идеала I.

Став 123. За $I, J\lhd D$ важи: $[I]=[J]$ акко су I и J изоморфни као D-модули.

Доказ. $\Longrightarrow$. Дакле, постоје $x, y\in D\setminus\{0\}$ такви да је $xI = yJ$. Можемо дефинисати $\phi\colon I\to J$ са:

$$\phi(a) = b \overset{\text{def}}{\Longleftrightarrow} xa = yb.$$

Како из $xa_1 = yb_1$ и $xa_2 = yb_2$ следи $x(a_1+a_2) = y(b_1+b_2)$ и $xda_1 = ydb_1$, то добијамо да је ϕ хомоморфизам D-модула. Но, јасно је да на аналогни начин можемо дефинисати $\psi\colon J\to I$ који ће бити његов инверс.

Нека је $\phi\colon I\to J$ изоморфизам D-модула. Изаберимо $a_0\in I$. Тада за све $a\in A$ имамо: $a_0\phi(a) = \phi(a_0a) = \phi(aa_0) = a\phi(a_0) = \phi(a_0)a$. Стога је $a_0J = a_0\phi[I] = \phi(a_0)I$, па је $[J]=[I]$. □

Теорема 124. а) Сваки идеал у Дедекиндовом домену је коначно генерисан пројективан модул над D.

б) Сваки коначно генерисан пројективан модул над Дедекиндовим доменом је изоморфан директној суми идеала домена D.

Доказ. а) Нека је $I \neq \{0\}$ идеал у D. Ако је $a_0 \in I \backslash \{0\}$, онда је $a_0 D \subseteq I$, па постоји идеал J такав да је $a_0 D = I \cdot J$. Стога постоје $b_i \in I$, $c_j \in J$ за које је $a_0 = b_1 c_1 + \cdots + a_n b_n$. Дефинишемо хомоморфизме D-модула $\phi\colon D^n \to I$ и $\psi\colon I \to D^n$ са:

$$\phi(x_1, \ldots, x_n) := b_1 x_1 + \cdots + b_n x_n, \quad \psi(b) := \left(\frac{bc_1}{a_0}, \ldots, \frac{bc_n}{a_0}\right).$$

Приметимо да $bc_i \in I \cdot J = a_0 D$, тако да је bc_i/a заиста елемент из D. Тада је

$$\phi(\psi(b)) = \phi\left(\frac{bc_1}{a_0}, \ldots, \frac{bc_n}{a_0}\right) = b_1 \frac{bc_1}{a_0} + \cdots b_n \frac{bc_n}{a_0} = b\frac{b_1 c_1 + \cdots + b_n c_n}{a_0} = b.$$

Дакле, ϕ је „на”, те је I коначно генерисан, а и кратак тачан низ $0 \to \operatorname{Ker} \phi \to D^n \xrightarrow{\phi} I \to 0$ се цепа, те је $I \oplus \operatorname{Ker} \phi \cong D^n$ и закључујемо да је I коначно генерисан пројективан D-модул.

б) Доказаћемо и више од овога, тј. доказаћемо да је сваки подмодул коначно генерисаног слободног D-модула изоморфан директној суми идеала. У ту сврху, нека је $P \leqslant D^n$ и посматрајмо ограничење пројекције на последњу координату $\pi' = \pi_n|_P$. Можемо претпоставити да ово није нула пресликавање, пошто би у том случају P био садржан у подмодулу D^{n-1} па бисмо посматрали ограничење пројекције на $n-1$-у координату. Имамо кратак тачан низ $0 \to \operatorname{Ker} \pi' \to P \xrightarrow{\pi'} \pi'[P] \to 0$. Но, $I' = \pi'[D]$ је идеал у D, па је по а) пројективан модул и имамо цепање: $P \cong \operatorname{Ker} \pi' \bigoplus I'$. Понављањем поступка (разматрањем $\operatorname{Ker} \pi'$) добијамо да је P изоморфан директној суми идеала. □

Приметимо да смо у оквиру претходне теореме доказали да је сваки Дедекиндов домен Нетерин домен.

Последица 125. Сваки коначно генерисани торзионо слободан модул над Дедекиндовим доменом је пројективан модул.

Доказ. Нека је T торзионо слободан и коначно генерисан модул над Дедекиндовим доменом. Ако се погледа доказ теореме 113, можемо да видимо да постоји $d \in D$ тако да је dT подмодул слободног модула. Наравно, пошто у T нема торзије, имамо да је $dT \cong T$. А из доказа претходне теореме следи да је dT пројективан модул. □

Сада можемо поступити као и разматрању класификације коначно генерисаних модула над главноидеалским доменом. Нека је A коначно генерисан модул над D, где је D Дедекиндов домен и нека је $T(A)$ торзиони подмодул од A. Имамо кратак тачан низ

$$0 \to T(A) \to A \to A/T(A) \to 0.$$

На основу претходне последице, имамо да ја $A/T(A)$ пројективан, па се овај низ цепа. Стога добијамо изоморфизам $A \cong T(A) \bigoplus A/T(A)$.

Но, по теореми 124 знамо да је $A/T(A) \cong I_1 \bigoplus \cdots \bigoplus I_n$, за неке идеала $I_j \triangleleft D$.

У даљем показујемо како се може даље поједноставити ова директна сума. Најпре морамо показати још неке резултате о Дедекиндовим доменима.

Теорема 126. Сваки ненула идеал у Дедекиндовом домену може се, на јединствен начин, приказати у облику производа максималних идеала.

Доказ. Нека је $I \neq \{0\}$ и M максималан идеал за који је $I \subseteq M$. Ако је $I = M$, онда смо завршили. Иначе, постоји $I_1 (\supset I)$ тако да је $I = M \cdot I_1$. Уколико је I_1 максималан, завршили смо. Иначе, постоји максималан M_1 за који је $I_1 \subset M_1$, па је $I_1 = M_1 \cdot I_2$ за неки идеал $I_2 (\supset I_1)$. Тада је $I = M_1 \cdot M_2 \cdot I_2$ и $I \subset I_1 \subset I_2$. Како је D Нетерин, бесконачан низ растућих идеала не постоји, те се овај процес мора завршити и I је производ максималних идеала.

Нека је $M_1 \cdots M_n = M'_1 \cdots M'_m$, где су M_i, M'_j максимални идеали. Доказ јединствености можемо извести индукцијом по n.

$n = 1$. Дакле $M_1 = M'_1 \cdots M'_m$. M_1 је и прост идеал, па је $M'_j \subseteq M_1$. Како је M'_j максималан то је $M_1 = M'_j$. Скраћивањем добијамо да је $D = M'_1 \cdots \widehat{M'_j} \cdots M'_m$, па мора заправо бити $m = 1$.

Нека је $n > 1$ и јединственост важи за све бројеве мање од n. Као у бази индукције, један од $M'_1, \ldots, M'_m$ једнак је M_1. Због једноставности ознака, претпоставимо да је $M_1 = M'_1$. Ако скратимо са M_1 добијамо да је $M_2 \cdots M_n = M'_2 \cdots M'_m$. Индуктивна хипотеза завршава доказ. □

Последица 127. У Дедекиндовом домену, сваки прост идеал различит од $\{0\}$ је максималан.

Доказ. Нека је $P \neq \{0\}$ прост идеал. Тада, по претходној теореми, постоје максимални идеали $M_1, \ldots, M_n$ Такви да је $P = M_1 \cdots M_n$. Како је P прост, следи да је за неко j: $M_j \subseteq P$, па мора бити $P = M_j$ и P је максималан. □

Дакле, као што у домену са једнозначним растављањем имамо представљање сваког елемента, различитог од нуле, у облику производа простих елемената, тако у Дедекиндовом домену имамо представљање сваког идеала различитог од нуле у облику производа простих идеала. Даље се нећемо бавити коначног генерисаним торзионим модулима. Рецимо само да постоји потпуно аналогна класификација оној за главноидеалске домене – разлика је само у томе што уместо степена простих елемената имамо степене простих идеала!

Лема 128. За сваки идеал I у Дедекиндовом домену, количник D/I је главноидеалски прстен (који може да има делитеље нуле наравно).

Доказ. Како је сваки идеал у D производ максималних идеала, тако је и у прстену D/I. Идеали у D/I одговарају идеалима у D који садрже I. Посебно, максимални идеали у D/I одговарају максималним идеалима у A који садрже I, а то су баш идеали који учествују у растављању I на производ максималних. Стога их има коначно много и нека су то идеали $M_1, \dots, M_k$. Покажимо да постоје елементи y_i такви да је $\langle y_i \rangle + I = M_i$. Преласком на количнички прстен, добијамо да је $\overline{M_i} = \langle \overline{y_i} \rangle$, где са $\overline{a}$ означавамо слику елемента, односно идеала у количничком прстену. Стога је сваки максимални идеал у A/I, а како је сваки идеал ту производ максималних, сваки идеал је главни.

Посматрајмо идеале $M_1, \dots, M_{i-1}, M_i^2, M_{i+1}, \dots, M_n$. Они су свакако копрости (идеали I, J прстена R су копрости уколико је $I + J = R$). Наиме, ако би M_i^2 био садржан у неком M_j, за $j \neq i$, добили бисмо да је $M_i \subseteq M_j$, па би они били једнаки; стога је $M_i^2 + M_j = D$. Нека је $x_i \in M_i \setminus M_i^2$ (зашто је $M_i \neq M_i^2$?). По Кинеској теореми о остацима, постоји елемент y_i такав да је

$$y_i \equiv \begin{cases} x_i, & \mod M_i^2 \\ 1, & \mod M_j, \text{ за } j \neq i. \end{cases}$$

Дакле, $\langle y_i \rangle + I$ јесте садржан у M_i, а није садржан ни у једном M_j за $j \neq i$. Стога је он степен од M_i. Но, он није у M_i^2, јер $x_i \notin M_i^2$, па мора бити $\langle y_i \rangle + I = M_i$. □

Докажимо сада једну техничку лему.

Лема 129. За два дата нетривијална (различита од $\{0\}$) идеала I и J у Дедекиндовом домену D, постоји идеал I', такав да је $[I'] = [I]$, а I' и J су копрости.

Доказ. Нека је $a_0 \in I \setminus \{0\}$. Тада је $\langle a_0 \rangle \subseteq I$, па постоји K такав да је $\langle a_0 \rangle = K \cdot I$. Како је, по претходној леми, прстен $D/(J \cdot K)$ главно идеалски, то је идеал $\overline{K}$ главни, те постоји x_0 такав да је $K = J \cdot K + \langle x_0 \rangle$. Ако ову једнакост помножимо са I добијамо $K \cdot I = J \cdot K \cdot I + \langle x_0 \rangle \cdot I$, односно $\langle a_0 \rangle = a_0 J + x_0 I$. Дељењем са a_0 добијамо да је $D = J + \frac{x_0}{a_0} I$. То значи да је $I' = \frac{x_0}{a_0} I$ идеал у D који је копрост са J и $[I'] = [I]$ ($a_0 I' = x_0 I$). □

Лема 130. Ако су I и J нетривијални идеали у Дедекиндовом домену D, онда је D-модул $I \bigoplus J$ изоморфан D-модулу $D \bigoplus (I \cdot J)$.

Доказ. Ако I и J нису копрости, на основу претходне леме постоји I', који је, као D-модул, изоморфан са I (присетимо се става 123), а који је, као идеал, копрост идеалу J. Тада је $I \bigoplus J \cong I' \bigoplus J$. Уочимо кратак тачан низ:

$$0 \to I' \cap J \xrightarrow{\mu} I' \bigoplus J \xrightarrow{\epsilon} D \to 0,$$

где је $\epsilon(x,y) = x+y$, а $\mu(z) = (z,-z)$. Имамо да је ϵ „на” пошто су I' и J копрости. Уколико је $\epsilon(x,y) = 0$, то значи да је $I' \ni x = -y \in J$, па, ако узмемо $z = x$, то је $z \in I' \cap J$ такав да је $\mu(z) = (z,-z) = (x,y)$. Стога је низ заиста тачан. Но, D је слободан D-модул, те се овај низ цепа и имамо изоморфизам $I' \bigoplus J \cong D \bigoplus (I' \cap J)$. Како су I' и J копрости, имамо да је $I' \cap J = I' \cdot J$ (подсетите се зашто је то тако, или сами изведите, није тешко). Но, ако је $[I] = [I']$, онда постоје a, b такви да је $aI = bI'$, из чега следи да је $aI \cdot J = bI' \cdot J$, па је $[I \cdot J] = [I' \cdot J]$ те имамо изоморфизам D-модула: $I \cdot J \cong I' \cdot J$, из чега следи тражено. $\square$

Следећа теорема нам допуњује класификацију коначно генерисаних торзионо слободних модула над Дедекиндовим доменом (присетите се теореме 124 и последице 125).

Теорема 131. Нека су $I_1, \ldots, I_r$ и $J_1, \ldots, J_s$ нетривијални идеали у Дедекиндовом домену D. Тада имамо изоморфизам D-модула

$$I_1 \bigoplus I_2 \bigoplus \cdots \bigoplus I_r \cong J_1 \bigoplus J_2 \bigoplus \cdots \bigoplus J_s$$

ако и само ако је $r = s$ и $[I_1 \cdot I_2 \cdots I_r] = [J_1 \cdot J_2 \cdots J_s]$.

Доказ. Нека је $\phi\colon I_1 \bigoplus \cdots \bigoplus I_r \to J_1 \bigoplus \cdots \bigoplus J_s$ изоморфизам ових модула. Он је потпуно одређен хомоморфизмима $p_i \circ \phi \circ q_j\colon I_j \to J_i$ где су хомоморфизми p_i и q_j из структуре производа односно копроизвода: $p_i(y_1, \ldots, y_s) = y_i$, $q_j(x) = (0, \ldots, 0, \underset{j}{x}, 0, \ldots, 0)$.

Покажимо да је сваки хомоморфизам D-модула $\psi\colon I \to J$, где је I нетривијалан идеал, облика $\phi(a) = qa$ за неки q из поља разломака $Q(D)$. Идеја је као из доказа става 123. Ако су $a_0, a \in I$, $a_0 \neq 0$ имамо једнакости $a_0\phi(a) = \phi(a_0 a) = \phi(a a_0) = a\phi(a_0) = \phi(a_0)a$, па је заправо за свако $a \in I$: $\phi(a) = \frac{\phi(a_0)}{a_0} a$ и тражени елемент је $q = \frac{\phi(a_0)}{a_0}$. Стога за сваки хомоморфизам D-модула $\phi\colon I_1 \bigoplus \cdots \bigoplus I_r \to J_1 \bigoplus \cdots \bigoplus J_s$ постоји матрица $Q = (q_{ij}) \in M_{s\times r}(Q(D))$ таква да је $\phi(a_1, \ldots, a_r) = (b_1, \ldots, b_s)$ акко је

$$\begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1r} \\ q_{21} & q_{22} & \cdots & q_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ q_{s1} & q_{s2} & \cdots & q_{sr} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}.$$

Уколико је ϕ изоморфизам, онда је матрица Q инвертибилна и мора бити $r = s$. Тврдимо да важи једнакост $J_1 \cdots J_s = (\det Q) I_1 \cdots I_r$. Докажимо најпре да је $(\det Q) I_1 \cdots I_s \subseteq J_1 \cdots J_s$. Претпоставимо да $a_i \in I_i$. Тада је $(\det Q) a_1 \cdots a_s$ заправо детерминанта матрице

$$\begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1s} \\ q_{21} & q_{22} & \cdots & q_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ q_{s1} & q_{s2} & \cdots & q_{ss} \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_s \end{pmatrix} = \begin{pmatrix} q_{11}a_1 & q_{12}a_2 & \cdots & q_{1s}a_s \\ q_{21}a_1 & q_{22}a_2 & \cdots & q_{2s}a_s \\ \vdots & \vdots & \ddots & \vdots \\ q_{s1}a_1 & q_{s2}a_2 & \cdots & q_{ss}a_s \end{pmatrix}.$$

Но, $q_{ij}a_j \in J_i$, јер су q_{ij} заправо они елементи из поља разломака који одговарају хомоморфизмима $p_i \circ \phi \circ q_j \colon I_j \to J_i$. Дакле, елементи прве врсте ове матрице су у J_1, елементи друге врсте у J_2, ..., елементи s-те врсте у J_s. Стога је детерминанта ове матрице у производу идеала $J_1 \cdots J_s$. Како је $a_1 \cdots a_s$ био произвољни адитивни генератор производа идеала $I_1 \cdots I_s$, то закључујемо да је заиста $(\det Q)I_1 \cdots I_s \subseteq J_1 \cdots J_s$. На исти начин се показује да је $(\det Q^{-1})J_1 \cdots J_s \subseteq I_1 \cdots I_s$. Множењем са $\det Q$ добијамо да је $J_1 \cdots J_s \subseteq (\det Q)I_1 \cdots I_s$. Стога важи једнакост $(\det Q)I_1 \cdots I_s = J_1 \cdots J_s$. Ако је $\det Q = \frac{a}{b}$, онда добијамо да је $aI_1 \cdots I_s = bJ_1 \cdots J_s$, па је заиста $[I_1 \cdots I_s] = [J_1 \cdots J_s]$.

Доказ другог смера еквиваленције следи директно из чињенице да имамо изоморфизам $I \bigoplus I_2 \bigoplus \cdots \bigoplus I_s \cong D^{s-1} \bigoplus (I_1 \cdot I_2 \cdots I_s)$, који се добија једноставном индукцијом уз примену леме 130. $\square$

Дедекиндови домени су од значаја у алгебарској теорији бројева, пошто су прстени целих у бројевним пољима управо Дедекиндови домени, но ми се тим аспектом овде нећемо бавити.

9 Моритина теорема

Враћамо се поново у област општих прстена са јединицом. Нека је A неки R-модул. На $E = \mathrm{End}_R(A)(= \mathrm{Hom}_R(A, A))$ имамо структуру прстена – ендоморфизме модула A можемо да компонујемо и за све $\alpha, \alpha_1, \beta, \beta_1 \in E$ важи: $(\alpha+\alpha_1)\circ(\beta+\beta_1) = \alpha\circ\beta+\alpha\circ\beta_1+\alpha_1\circ\beta+\alpha_1\circ\beta_1$. Стога је A и леви E-модул. Дакле, A је један леви (R, E)-модул. Но, ово је мало мање погодно за рад, у овом тренутку би било повољно када бисмо функције записивале са десне стране, дакле када би функција елемент „вукла”, уместо да га „гура”. Стога посматрамо опозитни прстен: $S = E^{\mathrm{op}}$. Тада је A десни S-модул: $a \cdot \alpha := \alpha(a)$. Имамо да је $a \cdot (\alpha \circ^{\mathrm{op}} \beta) = (\alpha \circ^{\mathrm{op}} \beta)(a) = (\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(a \cdot \alpha) = (a \cdot \alpha) \cdot \beta$, за све $a \in A, \alpha, \beta \in S$. Тако A постаје (R, S)-бимодул. Заиста имамо: $(ra) \cdot \alpha = \alpha(ra) = r\alpha(a) = r(a \cdot \alpha)$, за све $a \in A, r \in R, \alpha \in S$. Дуални модул $A^* = \mathrm{Hom}_R(A, R)$ је стога (S, R)-бимодул. Следи да је $A^* \otimes_R A$ један (S, S)-бимодул, а $A \otimes_S A^*$ један (R, R)-бимодул.

Подсетимо се хомоморфизма $\theta_{A,B} \colon A^* \otimes_R B \to \mathrm{Hom}_R(A, B)$ (видети (24)). Теорема 71 каже да је ово изоморфизам за свако B ако и само ако је A коначно генерисан пројективан модул. Ако узмемо, $B = A$, добијамо функцију $\theta = \theta_{A,A}$:

$$\theta \colon A^* \otimes_R A \to E,$$

такву да је : $\theta(\phi \otimes b)(a) := \phi(a)b$, за $\phi \in A^*, a, b \in A$. Пошто је, гледано као Абелове групе, $S = E$, имамо да $\theta \colon A^* \otimes_R A \to S$ и то је заправо хомоморфизам (S, S)-бимодула. Проверимо на адитивним генераторима.

$$\theta\big(\alpha \cdot (\phi \otimes b)\big)(a) = \theta\big((\alpha \cdot \phi) \otimes b\big)(a) = \theta\big((\phi \circ \alpha) \otimes b\big)(a) = (\phi \circ \alpha)(a)b = \phi(\alpha(a))(b).$$

$$\big(\alpha\cdot(\theta(\phi\otimes b))\big)(a)=\big(\theta(\phi\otimes b)\circ\alpha\big)(a)=\theta(\phi\otimes b)(\alpha(a))=\phi(\alpha(a))b.$$

Дакле, заиста је $\theta\big(\alpha\cdot(\phi\otimes b)\big)=\alpha\cdot(\theta(\phi\otimes b))$ за $\alpha\in S,\phi\in A^*,b\in A$.

$$\theta\big((\phi\otimes b)\cdot\alpha\big)(a)=\theta\big(\phi\otimes(b\cdot\alpha)\big)(a)=\theta(\phi\otimes\alpha(b))(a)=\phi(a)\alpha(b).$$

$$\big(\theta(\phi\otimes b)\cdot\alpha\big)(a)=\big(\theta(\phi\otimes b)\circ^{\mathrm{op}}\alpha\big)(a)=\big(\alpha\circ\theta(\phi\otimes b)\big)(a)=\alpha\big(\theta(\phi\otimes b)(a)\big)=\alpha(\phi(a)b)=\phi(a)\alpha(b).$$

Дакле, имамо да је $\theta(\phi\otimes b)\cdot\alpha)=\theta(\phi\otimes b)\cdot\alpha$ за $\phi\in A^*,b\in A,\alpha\in S$. Знамо да је ово изоморфизам за сваки коначно генерисан пројективан леви R-модул A (на основу теореме 71 ово је изоморфизам Абелових група, али сада знамо да је то то хомоморфизам (S,S)-бимодула, па је стога и изоморфизам (S,S)-бимодула).

Уведимо сада хомоморфизам Абелових група $\tau\colon A\otimes_S A^*\to R$. Стандардно дефинишемо функцију $f\colon A\times A^*\to R$ са: $f(a,\phi):=\phi(a)$. Продужимо је до хомоморфизма Абелових група $\overline{f}\colon\mathcal{F}(A\times A^*)\to R$. Проверимо да ли генераторе за $\mathcal{R}(A\times B)$ шаље у 0_R.

$$\begin{aligned}&\overline{f}\big((a_1+a_2,\phi)-(a_1,\phi)-(a_2,\phi)\big)=\overline{f}(a_1+a_2,\phi)-\overline{f}(a_1,\phi)-\overline{f}(a_2,\phi)\\&\quad=f(a_1+a_2,\phi)-f(a_1,\phi)-f(a_2,\phi)=\phi(a_1+a_2)-\phi(a_1)-\phi(a_2)=0_R.\end{aligned}$$

$$\begin{aligned}&\overline{f}\big((a,\phi_1+\phi_2)-(a,\phi_1)-(a,\phi_2)\big)=\overline{f}(a,\phi_1+\phi_2)-\overline{f}(a,\phi_1)-\overline{f}(a,\phi_2)\\&=f(a,\phi_1+\phi_2)-f(a,\phi_1)-f(a,\phi_2)=(\phi_1+\phi_2)(a)-\phi_1(a)-\phi_2(a)=0_R.\end{aligned}$$

$$\overline{f}\big((a\cdot\alpha,\phi)-(a,\alpha\cdot\phi)\big)=f(\alpha(a),\phi)-f(a,\phi\circ\alpha)=\phi(\alpha(a))-(\phi\circ\alpha)(a)=0_R.$$

Стога имамо индуковани хомоморфизам Абелових група

$$\tau\colon A\otimes_S A^*\big(=\mathcal{F}(A\times A^*)/\mathcal{R}(A\times A^*)\big)\to R,$$

за који је $\tau(a\otimes\phi)=\phi(a)$, за $a\in A,\phi\in A^*$. Но, заправо је τ и хомоморфизам (R,R)-бимодула. Проверимо то на адитивним генераторима.

$$\tau\big(r\cdot(a\otimes\phi)\big)=\tau(ra\otimes\phi)=\phi(ra)=r\phi(a)=r\tau(a\otimes\phi).$$

$$\tau\big((a\otimes\phi)\cdot r\big)=\tau\big(a\otimes(\phi\cdot r)\big)=(\phi\cdot r)(a)=r\phi(a)=r\tau(a\otimes\phi).$$

Дакле, слика $\tau\big[A\otimes_S A^*\big]$ је двострани идеал у R. Овај идеал се назива идеал трага од A, у ознаци $\operatorname{Tr}A$.

Дефиниција 132. Леви R-модул A је R-генератор уколико је горедефинисан τ изоморфизам.

Испоставља се да је за то довољно да τ буде „на”, тј. да је $\operatorname{Tr}A=R$.

Став 133. Ако је $\tau\colon A\otimes_S A^*\to R$ „на”, онда је и „1–1”.

Доказ. Како је τ „на”, то постоје $a_i \in A, \phi_i \in A^*$ такви да је

$$\tau\left(\sum_{i=1}^{n} a_i \otimes \phi_i\right) = 1_R,$$

односно да је $\sum_{i=1}^{n} \phi_i(a_i) = 1_R$. Претпоставимо да $\sum_{j=1}^{m} b_j \otimes \psi_j \in \operatorname{Ker}\tau$ те је $\sum_{j=1}^{m} \psi_j(b_j) = 0_R$. Тада је

$$\begin{aligned}
\sum_{j=1}^{m} b_j \otimes \psi_j &= \sum_{j=1}^{m} 1_R b_j \otimes \psi_j = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} \phi_i(a_i)\right) b_j \otimes \psi_j = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} \phi_i(a_i) b_j\right) \otimes \psi_j \\
&= \sum_{j=1}^{m}\left(\sum_{i=1}^{n} \theta(\phi_i \otimes b_j)(a_i)\right) \otimes \psi_j = \sum_{i=1}^{n}\sum_{j=1}^{m} \theta(\phi_i \otimes b_j)(a_i) \otimes \psi_j = \sum_{i=1}^{n}\sum_{j=1}^{m} \big(a_i \cdot \theta(\phi_i \otimes b_j)\big) \otimes \psi_j \\
&= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i \otimes \theta(\phi_i \otimes b_j) \cdot \psi_j = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i \otimes \big(\psi_j \circ \theta(\phi_i \otimes b_j)\big) \\
&= \sum_{i=1}^{n} a_i \otimes \left(\sum_{j=1}^{m} \psi_j \circ \theta(\phi_i \otimes b_j)\right) = \bigstar.
\end{aligned}$$

Нека је $a \in A$. Тада имамо да је

$$\sum_{j=1}^{m} \big(\psi_j \circ \theta(\phi_i \otimes b_j)\big)(a) = \sum_{j=1}^{m} \psi_j\big(\theta(\phi_i \otimes b_j)(a)\big) = \sum_{j=1}^{m} \psi_j(\phi_i(a) b_j) = \sum_{j=1}^{m} \phi_i(a)\psi_j(b_j) = \phi_i(a)\sum_{j=1}^{m} \psi_j(b_j) = \psi_i(a) 0_R = 0_R.$$

Дакле, $\sum_{j=1}^{m} \psi_j \circ \theta(\phi_i \otimes b_j) = 0_{A^*}$ за све i, те је

$$\sum_{j=1}^{m} b_j \otimes \psi_j = \bigstar = \sum_{i=1}^{n} a_i \otimes 0_{A^*} = 0_{A \otimes A^*}$$

Стога је $\operatorname{Ker}\tau = \{0_{A \otimes A^*}$, те је τ „1–1”. $\square$

Дефиниција 134. Кажемо да је леви R-модул R-ПРОГЕНЕРАТОР УКОЛИКО ЈЕ КОНАЧНО ГЕНЕРИСАН ПРОЈЕКТИВАН R-ГЕНЕРАТОР.

Дакле, A је R-прогенератор ако и само је су θ и τ изоморфизми. За формулацију главне теореме у овом одељку требаће нам још неких појмова из теорије категорија.

Већ смо имали прилике да се имплицитно бавимо појмом природне трансформације функтора.

Дефиниција 135. Нека су $\mathcal{C}$ и $\mathcal{D}$ категорије и $F, G\colon \mathcal{C} \to \mathcal{D}$ функтори. Под ПРИРОДНОМ ТРАНСФОРМАЦИЈОМ $\tau\colon F \xrightarrow{\bullet} G$ подразумевамо придруживање $\mathcal{C} \ni C \mapsto \tau_C \in \mathcal{D}(F(C), F(D))$ тако да је за сваки морфизам $f \in \mathcal{C}(C, C')$ дијаграм

$$\begin{array}{ccc} F(C) & \xrightarrow{\tau_C} & G(C) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(C') & \xrightarrow{\tau_{C'}} & G(C') \end{array}$$

комутативан. Уколико је τ_C изоморфизам за свако C онда је τ ПРИРОДНИ ИЗОМОРФИЗАМ.

На пример, ако је $D(A) := A^\vee$ онда у ставу 89 разматрамо природну трансформацију функтора $i\colon \mathrm{Id} \xrightarrow{\bullet} DD$, где смо са Id означили идентички функтор на категорији ${}_R\mathfrak{M}$, а са DD композицију функтора D са самим собом. Сам D је функтор $D\colon {}_R\mathfrak{M}^{\mathrm{op}} \to \mathfrak{M}_R$. Ако постоји природан изоморфизам функтора F и G, кратко ћемо писати $F \cong G$. Појам природне трансформације се појављује и у појму адјунгованих функтора.

Дефиниција 136. Нека су $\mathcal{C}$ и $\mathcal{D}$ категорије. ПРОИЗВОД ове две, у ознаци, $\mathcal{C} \times \mathcal{D}$ дефинише се на следећи начин. Објекти у овој категорији су уређени парови (C, D), где $C \in O(\mathcal{C})$, $D \in \mathcal{D}$. Стрелице се исто дефинишу на природан начин: $(\mathcal{C} \times \mathcal{D})\big(C \times D, C' \times D'\big) := \mathcal{C}(C, C') \times \mathcal{D}(D, D')$.

Бифунктор се дефинише као функтор из производа неке две категорије у неку категорију $H\colon \mathcal{C} \times \mathcal{D} \to \mathcal{E}$.

Дефиниција 137. Нека су дати функтори $F\colon \mathcal{C} \to \mathcal{D}$ и $G\colon \mathcal{D} \to \mathcal{C}$. Кажемо да је функтор F ЛЕВО АДЈУНГОВАН функтору G (или да је G ДЕСНО АДЈУНГОВАН функтору F) уколико постоји природни изоморфизам $\mathcal{D}(F-, -) \cong \mathcal{C}(-, G-)$ функтора из категорије $\mathcal{C}^{\mathrm{op}} \times \mathcal{D}$ у категорију скупова Set. Прецизније, за сваки $C \in \mathcal{C}$ и $D \in \mathcal{D}$ постоји бијекција између скупова:

$$\tau_{C,D}\colon \mathcal{D}(F(C), D) \to \mathcal{C}(C, G(D))$$

тако да дијаграми

$$\begin{array}{ccc} \mathcal{D}(F(C), D) & \xrightarrow{\tau_{C,D}} & \mathcal{C}(C, G(D)) \\ {\scriptstyle \mathcal{D}(F(f),g)}\downarrow & & \downarrow{\scriptstyle \mathcal{C}(f,G(g))} \\ \mathcal{D}(F(C'), D') & \xrightarrow{\tau_{C',D'}} & \mathcal{C}(C', G(D')) \end{array}$$

комутирају.

Овде је: $\mathcal{D}(F(f), g)(\phi) := g \circ \phi \circ F(f)$, $\mathcal{C}(f, G(g))(\psi) := G(g) \circ \psi \circ f$ где $f \in \mathcal{C}(C', C)$, $g \in \mathcal{D}(D, D')$, $\phi \in \mathcal{D}(F(C), D)$, а $\psi \in \mathcal{D}(C, G(D))$.

Дефиниција 138. Две категорије $\mathcal{C}$ и $\mathcal{D}$ су еквивалентне уколико постоје функтори $\mathcal{C} \xrightarrow{F} \mathcal{D} \xrightarrow{G} \mathcal{C}$ и природни изоморфизми $\mathrm{Id}_{\mathcal{C}} \xrightarrow{\bullet} GF$, $\mathrm{Id}_{\mathcal{D}} \xrightarrow{\bullet} FG$.

Дакле, не тражи се, баш, на пример, да је $G(F(X)) = X$, него да постоји природан изоморфизам $G(F(X)) \cong X$. На пример, читаоци могу да размисле зашто су еквивалентне следеће две категорије: категорија коначних скупова и функција међу њима и категорија коначних ординала $(0, 1, 2, \dots)$ и функција међу њима.

Сваки функтор $F\colon \mathcal{C} \to \mathcal{D}$ задаје, за свака два објекта C, C' из $\mathcal{C}$ функцију $\mathcal{C}(C, C') \to \mathcal{D}(F(C), F(C'))$. Ако су, пак, $\mathcal{C}$ и $\mathcal{D}$ неке категорије модула, онда се природно разматрају адитивни функтори, тј. они функтори код којих су горње функције хомоморфизми Абелових група.

Најзад можемо да формулишемо и докажемо Моритину теорему.

Теорема 139. Нека је A један R-прогенератор. Тада су категорије $\mathfrak{M}_R$ и $\mathfrak{M}_S$ еквивалентне при функторима $F\colon \mathfrak{M}_R \to \mathfrak{M}_S$, $G\colon \mathfrak{M}_S \to \mathfrak{M}_R$ задатим са

$$F(M) := M \otimes_R A, \text{ за } M \in \mathfrak{M}_R \text{ и } G(N) := N \otimes_S A^*, \text{ за } N \in \mathfrak{M}_S.$$

Доказ. Имамо да важи:

$$\begin{aligned}(GF)(M) = G(F(M)) = (M \otimes_R A) \otimes_S A^* &\cong M \otimes_R (A \otimes_S A^*) \\ &\overset{\mathrm{id}_M \otimes \tau}{=\!=\!=} M \otimes_R R \text{ (јер је } A \text{ један } R\text{-генератор)} \\ &\cong M.\end{aligned}$$

$$\begin{aligned}(FG)(N) = F(G(N)) = (N \otimes_S A^*) \otimes_R A &\cong N \otimes_S (A^* \otimes_R A) \\ &\overset{\mathrm{id}_N \otimes \theta}{=\!=\!=} N \otimes_S S \text{ (јер је } A \text{ коначно генерисан пројективан)} \\ &\cong N.\end{aligned}$$

Наравно, сви су изоморфизми природни. □

Пример 140. Ако за A узмемо R^n, како имамо изоморфизам прстена $\mathrm{End}_R(R^n) \cong M_n(R)$, имамо да је, за свако n, категорија десних R-модула еквивалентна категорији десних $M_n(R)^{\mathrm{op}}$-модула. Посебно, ако је R комутативан прстен, добијамо да је категорија левих R-модула изоморфна категорији левих $M_n(R)$-модула. ♣

Зашто је слободан модул R^n један R-генератор? Уверите се у то.

Последица 141. Ако је A један R-прогенераторс, онда је $R \cong End_S(A)$, а изоморфизам је дат са: $x \mapsto \xi_r$, где је $\xi_r(a) = ra$.

Доказ. Како је функтор F из Моритине теореме адитиван, то он индукује изоморфизам Абелових група

$$F_*\colon \mathrm{Hom}_R(M_1, M_2) \cong \mathrm{Hom}_S(F(M_1), F(M_2))$$

за све M_1, M_2 из $\mathfrak{M}_R$. Ако узмемо да је $M_1 = M_2 = R$, онда добијамо изоморфизме

$$R \cong \mathrm{Hom}_R(R, R) \cong \mathrm{Hom}_S(R \otimes_R A, R \otimes_R A) \cong \mathrm{Hom}_S(A, A) = \mathrm{End}_S(A).$$

Први изоморфизам слика r у хомоморфизам $\alpha_r\colon r' \mapsto r'r$. Следећи изоморфизам слика $\alpha\colon R \to R$ у $\alpha \otimes \mathrm{id}_A$. И наравно, $R \otimes_R A \cong A$ слика $r \otimes a$ у ra. Дакле, ако се при композицији ових изоморфизама $r \in R$ слика у $\xi_r\colon A \to A$, онда имамо $\xi_r\colon a \mapsto 1 \otimes a \mapsto \alpha_r(1) \otimes a \mapsto \alpha_r(1)a = ra$, као што је и тврђено. □

Дакле, имамо „затворен круг”, боље речено, симетрију између R и S: $S = \mathrm{End}_R(A)^{\mathrm{op}}$, а $R \cong \mathrm{End}_S(A)$. Код првог изоморфизма ради се о левом R-модулу, а код другог о десном S-модулу.

10 Полупрости прстени

Дефиниција 142. Нека је R прстен. Леви R-модул A је ПРОСТ ако је нетривијалан и нема праве подмодуле; он је ПОЛУПРОСТ ако је директна сума простих модула. Прстен R је ЛЕВО (ДЕСНО) ПОЛУПРОСТ ако је полупрост као леви (десни) R-модул.

Следећа теорема карактерише полупросте модуле.

Теорема 143. Следећи услови за модул A из ${}_R\mathfrak{M}$ су еквивалентни.

(1) A је полупрост.

(2) Сваки подмодул од A је директан сабирак од A.

(3) A је сума простих подмодула.

Доказ. (1)$\Longrightarrow$(2). Нека је $A = \dot{+}_{i\in I} A_i$ и B подмодул од A. Нека је

$$\mathcal{J} = \{J \subseteq I : \Big(\dot{+}_{j\in J} A_j\Big) \cap B = \{0\}\}.$$

$(\mathcal{J}, \subseteq)$ је посет и очигледно је унија горње ограничење за ланац у $\mathcal{J}$ (уверите се у ово). Стога постоји максималан елемент K у $\mathcal{J}$. Нека је $C = \dot{+}_{k\in K} A_k$. Тврдимо да је $C \dot{+} B = A$. Како је већ $C \cap B = \{0\}$, то само треба показати да је $A = C + B$. Посматрамо подмодуле $C \dot{+} A_i$ од A, за $i \notin K$. На основу максималности K, имамо да је $(C \dot{+} A_i) \cap B \neq \{0\}$, па је $\pi_i[(C \dot{+} A_i) \cap B]$ нетривијалан подмодул простог модула A_i, где је $\pi_i(x) = a_i$, где је $x = c + a_i, c \in C, a_i \in A_i$ јединствени приказ x у облику збира елемента из C и елемента из A_i. Но, како је A_i прост, дакле нема правих нетривијалних подмодула, то значи да је

$$\pi_i[(C \dot{+} A_i) \cap B] = A_i. \tag{37}$$

Нека је $x \in A$. То значи да је $x = c + d$, за неки $c \in C$, $d \in \dot{+}_{i\notin K} A_i$. Дакле, $d = a_{i_1} + \cdots + a_{i_s}$ за неке $a_{i_j} \in A_{i_j}$, где $i_j \notin K$. На основу (37) постоје $c_{i_j} \in C$ тако да је $c_{i_j} + a_{i_j} = b_{i_j} \in B$. Добијамо

$$x = c + a_{i_1} + \cdots + a_{i_s} = c + b_{i_1} - c_{i_1} + \cdots + b_{i_s} - c_{i_s} = \underbrace{c - c_{i_1} - \cdots - c_{i_s}}_{\in C} + \underbrace{b_{i_1} + \cdots + b_{i_s}}_{\in B}.$$

(2)$\Longrightarrow$(3). Докажимо најпре да се својство из (2) преноси и на подмодуле. Дакле, претпоставимо да је $A_1 \leqslant A_0 \leqslant A$. По (2), како је A_1 подмодул и од A, постоји B_1 тако да је $A_1 \dotplus B_1 = A$. Тада је $A_1 \dotplus (B_1 \cap A_0) = A_0$. Најпре: $A_1 \cap (B_1 \cap A_0) = (A_1 \cap B_1) \cap A_0 = \{0\} \cap A_0 = \{0\}$. Осим тога, ако је $x \in A_0$, онда постоје $a_1 \in A_1$, $b_1 \in B_1$ такви да је $x = a_1 + b_1$. Сао треба показати да $b_1 \in B_1 \cap A_0$. Но, и x и a_1 припадају A_0 ($a_1 \in A_1 \subseteq A_0$), па следи да $b_1 \in A_0$.

Треба показати да је A сума простих модула (не треба да докажемо да је директна сума, својство(3) је наизглед слабије од својства (1)). У ту сврху, нека је

$$\mathcal{B} = \{B \leqslant A : B \text{ је сума простих модула}\}.$$

Наравно, $(\mathcal{B}, \leqslant)$ је посет. Ако је $\mathcal{L}$ ланац у $\mathcal{B}$, посматрајмо $C = \bigcup\limits_{B \in \mathcal{L}} B$. Пошто је $\mathcal{L}$ ланац, C је свакако подмодул. Сваки елемент $x \in C$ је у неком $B \in \mathcal{L}$, а сваки такав B је сума простих модула, па је и x у суми простих модула. Зато је и C сума простих модула. Дакле, у $\mathcal{B}$ постоји максималан елемент A'.

Претпоставимо да је $A' \neq A$. Стога је $A = A' \dotplus A''$, где је $A'' \neq \{0\}$. Нека је $a \in A'' \setminus \{0\}$. Посматрајмо све подмодуле од A'' који не садрже a. И тај скуп подмодула чини посет у односу на $\leqslant$ и јасно је да је унија подмодула из неког ланца такође подмодул који не садржи a. Дакле, постоји максималан такав подмодул и означимо га са X. Тада постоји подмодул Y за који је $X \dotplus Y = A''$. Тврдимо да је Y прост. У супротном, он садржи прави подмодул, па заправо постоје нетривијални подмодули Y_1, Y_2 од Y, за које је $Y = Y_1 \dotplus Y_2$. Како је $X \subset X \dotplus Y_i$, за $i \in \{1, 2\}$, то $a \in X \dotplus Y_1$, те је $a = x_i + y_i$ за неке $x_i \in X$, $y_i \in Y_i$. Дакле $x_1 + y_1 = x_2 + y_2$, па је $X \ni x_1 - x_2 = y_2 - y_1 \in Y$, а како је $X \cap Y = \{0\}$, добијамо да је $Y_1 \ni y_1 = y_2 \in Y_2$, па је $y_1 = y_2 = 0$, односно $a = x_1 \in X$ што противречи избору X. Закључујемо да је Y прост. Но, тада је $A = A' \dotplus A'' = A' \dotplus Y \dotplus X$, па имамо да је $A' \dotplus Y$ сума простих модула (A' је сума простих, а Y је прост), који је стриктно већи од максималног A' што није могуће. Зато је $A' = A$ и заиста је A сума простих модула.

(3)$\Longrightarrow$(1). Дакле, по претпоставци је A сума простих модула A_i, $i \in I$. Посматрамо

$$\mathcal{J} = \{J \subseteq I : \text{сума модула } A_j \text{ за } j \in J \text{ је директна}\}.$$

Као и раније, није тешко показати да $\mathcal{J}$ има максималан елемент K и посматрајмо суму $A' = \dotplus_{k \in K} A_k$. Тврдимо да је $A' = A$. Покажимо то тако што ћемо показати да за све $i \notin K$: $A_i \subseteq A'$. Како је A_i прост модул, имамо да је $A_i \cap A' = \{0\}$, или је $A_i \cap A' = A_i$. Но, ако је $A_i \cap A = \{0\}$, онда је сума $A' + A_i$ директна и то је, заправо, директна сума простих модула која је стриктно већа од A'. То би значило да $K \cup \{i\} \in \mathcal{J}$, што није могуће јер је K максималан елемент у том скупу. Дакле, $A_i \cap A' = A_i$, па $A_i \subseteq A'$. $\square$

Последица 144. Нека је $0 \to A' \xrightarrow{\mu} A \xrightarrow{\epsilon} A'' \to 0$ кратак тачан низ левих модула. Ако је A полупрост, онда су и A' и A'' полупрости и овај низ се цепа.

Доказ. Модул A' изоморфан је подмодулу $\mu[A']$ модула A. Но, у доказу претходне теореме, видели смо да је подмодул полупростог модула и сам полупрост, па онда и $\mu[A']$ полупрост, а тиме и A' као њему изоморфан модул.

Поново на основу претходне теореме следи да постоји подмодул A_2 модула A такав да је $\mu[A'] \dot{+} A_2 = A$. Тада ограничење $\epsilon|_{A_2}$ на подмодул A_2 успоставља изоморфизам између A_2 и A'':

$$\operatorname{Ker} \epsilon|_{A_2} = \left(\epsilon|_{A_2}\right)^{-1}[\{0\}] = \epsilon^{-1}[\{0\}] \cap A_2 = \operatorname{Ker} \epsilon \cap A_2 = \mu[A'] \cap A_2 = \{0_{A_2}\}.$$

Како је A_2 подмодул полупростог, он је и сам полупрост, па је стога и A'' полупрост као њему изоморфан модул.

Коначно, цепање низа се остварује, на пример, помоћу хомоморфизма $j \circ \left(\epsilon|_{A_2}\right)^{-1} \colon A'' \to A$, где је са j означено укључење A_2 у A:

$$\epsilon \circ \left(j \circ \left(\epsilon|_{A_2}\right)^{-1}\right) = (\epsilon \circ j) \circ \left(\epsilon|_{A_2}\right)^{-1} = \epsilon|_{A_2} \circ \left(\epsilon|_{A_2}\right)^{-1} = \mathrm{id}_{A''}. \qquad \square$$

Погледајте колико је јак услов да је неки прстен полупрост.

Теорема 145. Нека је R прстен. Тада су следећи услови еквивалентни.

(1) R је лево полупрост.

(2) Сваки леви R-модул је полупрост.

(3) Сваки кратак тачан низ R-модула се цепа.

(4) Сваки леви R-модул је инјективан.

(5) Сваки леви R-модул је пројективан.

Доказ. (1)$\Longrightarrow$(2). Како је R лево полупрост R-модул, то је таква и свака директна сума $\bigoplus_{i \in I} R$ (зашто је директна сума полупростих модула и сам полупрост модул?), тј. сваки слободан R-модул је полупрост. Како је сваки модул слика слободног, то резултат следи на основу претходне последице.

(2)$\Longrightarrow$(3). Директно из претходне последице.

(3)$\Longrightarrow$(4), (3)$\Longrightarrow$(5). Директно, на основу основних особина пројективних и инјективних модула.

(4)$\Longrightarrow$(1), (5)$\Longrightarrow$(1). Нека је $I \triangleleft R$ леви идеал у R. Посматрајмо кратак тачан низ R-модула: $0 \to I \to R \to R/I \to 0$. И (4) и (5) дају да се овај низ цепа (I је инјективан, или је R/I пројективан), па је I директан сабирак у R. $\square$

Наравно, свако поље је полупрост прстен, али има наравно много занимљивијих примера. Следећа теорема је од централног значаја за теорију репрезентација коначних група.

Теорема 146. (Машкеова теорема) Нека је G група реда n и F поље карактеристике 0 или карактеристике p, тако да $p \nmid n$. Тада је групни прстен лево (и десно) полупрост.

Доказ. Докажимо само да је лево полупрост. Доказ да је десно полупрост се аналогно изводи. Најпре, приметимо да је, по својој дефиницији, $F[G]$ векторски простор димензије n над пољем F. Нека је I леви идеал у $F[G]$. То је и векторски потпростор од $F[G]$. Нека је $w_1, \ldots, w_k$ база за тај потпростор и допунимо је до базе целог простора $F[G]$: $w_1, \ldots, w_k, v_{k+1}, \ldots, v_n$. Дефинишемо $\pi\colon F[G] \to F[G]$ задавањем на бази: $\pi(w_i) = w_i$, $\pi(v_j) = 0$. Имамо да је $(\pi \circ \pi)(w_i) = \pi(\pi(w_i)) = \pi(w_i) = w_i$, $(\pi \circ \pi)(v_j) = \pi(\pi(v_j)) = \pi(0) = 0$. Стога је $\pi^2 = \pi$, те је π један пројектор. Јасно је да је слика од π једнака I.

Свакако је π један F-хомоморфизам, он не мора бити и $F[G]$-хомоморфизам. То ћемо поправити „усредњавањем”. Дефинишемо функцију $\widehat{\pi}\colon F[G] \to F[G]$ са:

$$\widehat{\pi}(x) := \frac{1}{n} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot x).$$

Приметимо да је, на основу претпоставке $n1_F \neq 0_F$ те инверз овог елемента постоји и краће смо то писали као $\frac{1}{n}$ због поједностављења ознака. Нека је $r \in F$. Како је π један F-хомоморфизам, имамо:

$$\begin{aligned} \pi(rx) &= \frac{1}{n} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot (rx)) = \frac{1}{n} \sum_{g \in G} g \cdot \pi(rg^{-1} \cdot x) \\ &= \frac{1}{n} \sum_{g \in G} g \cdot r\pi(g^{-1} \cdot x) = \frac{1}{n} r \sum_{g \in G} g \cdot \pi(g^{-1} \cdot x) = r\Big(\frac{1}{n} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot x)\Big) = r\widehat{\pi}(x). \end{aligned}$$

Нека је $g' \in G$ и $x \in F[G]$. Тада је:

$$\begin{aligned} \widehat{\pi}(g' \cdot x) &= \frac{1}{n} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot (g' \cdot x)) = \frac{1}{n} \sum_{g \in G} g \cdot \pi((\underbrace{g^{-1}g'}_{h^{-1}}) \cdot x) \\ &= \frac{1}{n} \sum_{h \in (g')^{-1}G} (g'h) \cdot \pi(h^{-1} \cdot x) = \frac{1}{n} \sum_{h \in G} g' \cdot (h \cdot \pi(h^{-1} \cdot x)) \\ &= g' \cdot \left(\frac{1}{n} \sum_{h \in G} h \cdot \pi(h^{-1} \cdot x)\right) = g' \cdot \widehat{\pi}(x). \end{aligned}$$

Дакле, $\widehat{\pi}$ је хомоморфизам $F[G]$-модула. Но, јасно је да је $\operatorname{Im}\widehat{\pi} \subseteq \operatorname{Im}\pi = I$. Осим тога, ако је $x \in I$ имамо да и $g^{-1} \cdot x \in I$, јер је I леви идеал, па је $\pi(g^{-1} \cdot x) = g^{-1} \cdot x$. Стога, за $x \in I$ имамо:

$$\widehat{\pi}(x) = \frac{1}{n}\sum_{g\in G} g \cdot (g^{-1} \cdot x) = \frac{1}{n}\sum_{g\in G}(gg^{-1}) \cdot x = \frac{1}{n}\sum_{g\in G} x = x.$$

Овим добијамо две ствари. Најпре да је $\operatorname{Im}\pi \subseteq \operatorname{Im}\widehat{\pi}$, те важи једнакост. А потом и да је $\widehat{\pi}^2 = \widehat{\pi}$. На основу последице 31 добијамо да је

$$F[G] = \operatorname{Ker}\widehat{\pi} \dotplus \operatorname{Im}\widehat{\pi} = \operatorname{Ker}\widehat{\pi} \dotplus I.$$

Добили смо да је сваки леви идеал у $F[G]$ директан сабирак од $F[G]$ што нам показује да је $F[G]$ лево полупрост. □

До краја овог одељка (и курса) бавићемо се класификацијом левих полупростих прстена. Заправо показаћемо да је сваки такав прстен производ прстена матрица. Најпре доказујемо следећу лему.

Лема 147. Нека су I и J минимални леви идеали у прстену R. Тада је или $I \cdot J = \{0\}$ или је $I \cong J$.

Доказ. Када говоримо о минималним идеалима подразумевамо да се ради о нетривијалним идеалима. Наравно, производ идеала дефинише се са: $I \cdot J = \{x_1y_1 + \cdots + x_ny_n : x_i \in I, y_i \in I, n \in \mathbb{N}\}$. Ово је свакако леви идеал, пошто је I леви идеал. Приметимо да је за свако $a \in J$ скуп Ia такође један леви идеал и он је садржан у J. Како је J минималан леви идеал, то мора бити или $Ia = \{0\}$ или $Ia = J$. Уколико је $Ia = \{0\}$ за све $a \in J$, имамо да је $I \cdot J = \{0\}$. У супротном је $Ia = J$ за неко $a \in J$.

Посматрамо функцију $f\colon I \to J$ задату са $f(x) = xa$. Јасно је да је ово један хомоморфизам левих R-модула:

$$f(x_1{+}x_2){=}(x_1{+}x_2)a{=}x_1a{+}x_2a{=}f(x_1){+}f(x_2), f(rx){=}(rx)a{=}r(xa) = rf(x).$$

По претпоставци је f „на”. $\operatorname{Ker} f$ је леви идеал, а I је минималан леви идеал, па мора бити $\operatorname{Ker} f = \{0\}$ те је f изоморфизам. □

Приметимо да је неки нетривијалан леви идеал у прстену минималан ако и само ако је он прост леви R-модул. То је таутолошка чињеница.

Став 148. Нека је R лево полупрост прстен, те је $R = \dot{+}_\alpha J_\alpha$, где су J_α минимални леви идеали. Ако је I ма који минимални леви идеал у R, онда је $I \cong J_\alpha$ за неко α.

Доказ. Имамо да је $I = R \cdot I = \sum_\alpha J_\alpha \cdot I$. Ако би сви идеали у овом збиру били једнаки нули, I би био нула идеал. Како то није тако, на основу леме закључујемо да је $I \cong J_\alpha$ за неко α. □

Нека је R лево полупрост прстен, те је $R = \dot{+}_{\alpha \in A} J_\alpha$, где су J_α минимални леви идеали. Изаберимо $B \subseteq A$ тако да за свако $\alpha \in A$ постоји тачно једно $\beta \in B$ тако да је $J_\alpha \cong J_\beta$ Нека је

$$R_\beta = \dot{\sum_{J_\alpha \cong J_\beta}} J_\alpha$$

Дакле, за свако $\beta \in B$ је R_β збир свих минималних међусобно изоморфних левих идеала од R. Имамо да је

$$R = \dot{\sum_{\beta \in B}} R_\beta \tag{38}$$

Теорема 149. Нека је R лево полупрост прстен и ознаке као горе. Тада важе следећи резултати.

(1) Сваки R_β је двострани идеал.

(2) $R_\beta \cdot R_\gamma = \{0\}$ за $\beta \neq \gamma$.

(3) Скуп B је коначан.

(4) Прстен R је изоморфан производу прстена $\prod_{\beta \in B} R_\beta$.

Доказ. (1) Знамо да је R_β, као збир левих идеала и сам леви идеал. Нека је $a \in R$ и J_α један од идеала који се појављује као сабирак у R_β. Тада је $Ja = \{0\} \subset R_\beta$ или је $Ja \neq \{0\}$, а тада је $J \cong Ja$, па се и Ja појављује као сабирак у R_β те је и тада $Ja \subseteq R_\beta$.

(2) следи директно из леме: производ сваког идеала који се појављује као сабирак у R_β и сваког идеала који се појављује као сабирак у R_γ је нула идеал, јер би у супротном били изоморфни, а то нису.

(3) На основу (38) имамо да је $1_R = e_{\beta_1} + \cdots + e_{\beta_k}$ за неке $\beta_1, \ldots, \beta_k \in B$ и $e_{\beta_i} \in R_{\beta_i}$. Ако би постојао $\beta \notin \{\beta_1, \ldots, \beta_k\}$, онда би, на основу (2) и горњег растава јединице прстена R, имали да је за сваки $x \in R_\beta$: $x = xe_{\beta_1} + \cdots + xe_{\beta_k} = 0_R + \cdots + 0_R = 0_R$. Дакле, $B = \{\beta_1, \ldots, \beta_k\}$.

(4) Како је $e_{\beta_i} e_{\beta_2} = 0$ за $i \neq j$, добијамо да је $1_R^2 = e_{\beta_1}^2 + \cdots + e_{\beta_k}^2$, па су сви e_{β_i} идемпотенти: $e_{\beta_i}^2 = e_{\beta_i}$. Ако је $x \in R$, онда је $x = xe_{\beta_1} + \cdots + e_{\beta_k}$, где $xe_{\beta_i} \in R_{\beta_i}$ јер је R_{β_i} двострани идеал. Но, ако $x \in R_{\beta_i}$ имамо да је $xe_{\beta_j} = 0$, за $j \neq i$, па је $x = xe_{\beta_i}$. На аналоган начин добијамо да је и $x = e_{\beta_i} x$ за све $x \in R_{\beta_i}$. Закључујемо да су заиста R_{β_i} прстени са јединицом и да је $1_{R_{\beta_i}} = e_{\beta_i}$. На основу свега до сада, добијамо да је са $f(x_1, \ldots, x_k) = x_1 + \cdots + x_k$ задат један изоморфизам прстена са јединицом $f \colon \prod_{\beta \in B} R_\beta \to R$. $\square$

Следећа последица само истиче главни резултат претходне теореме.

Последица 150. Сваки лево полупрост прстен је изоморфан коначном директном производу лево полупростих прстена у којима су сви леви минимални идеали изоморфни.

Доказ. Леви идеали у R_{β_i} су, на основу свега показаног, заправо леви идеали у R који су садржани у R_{β_i}. Наиме, ако је $r \in R$ и $y \in R_{\beta_i}$, онда је $ry = (r_1 + \cdots + r_k)y = r_1 y + \cdots + r y_k = r_i y$. Дакле, множење елемената из R_{β_i} елементима из R своди се на множење елемената из R_{β_i}. Стога је заиста R_{β_i} збир СВОЈИХ минималних левих идеала. □

Напоменимо само да R_β ЈЕСУ прстени са јединицом и они ЈЕСУ садржани у R, али они НИСУ потпрстени са јединицом прстена R, јер им се јединице не поклапају. Они су у R само двострани идеали.

Дефиниција 151. Лево полупрост прстен R је ЛЕВО ПРОСТ ПРСТЕН уколико су му сви минимални леви идеали изоморфни.

Дакле, на основу претходног је сваки лево полупрост прстен изоморфан коначном директном производу лево простих прстена.

Став 152. Нека је R један лево прост прстен и $I \neq \{0\}$ леви идеал у R. Тада је $I \cdot R = R$.

Доказ. Дакле, $R = \dot{+}_\alpha J_\alpha$. Нека је I леви идеал. Како је R лево полупрост R-модул, то је такав и I као његов подмодул. То значи да је I сума минималних идеала, па свакако I садржи неки минималан идеал I'. Како је $I' \cdot R \subseteq I \cdot R$, довољно је показати да је $I' \cdot R = R$.

Имамо да је $R = I' \dot{+} K$. Нека је $\pi \colon R \to I'$ пројекција. Како су у R сви минимални леви идеали изоморфни, имамо, за свако α, изоморфизме $\phi_\alpha \colon I' \to J_\alpha$. Посматрајмо композицију $\phi_\alpha \circ \pi \colon R \to J_\alpha$. Нека је $r_\alpha = \phi_\alpha(\pi(1_R))$. Тада је за $x \in R$: $\phi_\alpha(\pi(x)) = x\phi_\alpha(\pi(1_R)) = x r_\alpha$. Посебно, ако је $y \in I'$, имамо: $\phi_\alpha(y) = \phi_\alpha(\pi(y)) = y r_\alpha$. Како је ϕ_α „на", добијамо да је $J_\alpha = I r_\alpha$. Нека је $1_R = x_{\alpha_1} + \cdots + x_{\alpha_k}$ за неке $x_{\alpha_i} \in J_{\alpha_i}$. Следи да постоје $y_{\alpha_i} \in I'$ такви да је $x_{\alpha_i} = y_{\alpha_i} r_{\alpha_i}$, за $i = \overline{1,k}$. Но, то значи да $1_R = y_{\alpha_1} r_{\alpha_1} + \cdots + y_{\alpha_k} r_{\alpha_k} \in I' \cdot R$, па је заиста $I' \cdot R = R$. □

Следећи резултат директно следи из овог става.

Последица 153. Лево прост прстен нема правих двостраних идеала. □

Теорема 154. Лево прост модул над лево простим прстеном је прогенератор.

Доказ. Нека је R лево прост прстен и A лево прост модул над R. На основу (5) из теореме 145 A је пројективан. Уколико је $a \in A \setminus \{0\}$ онда је $Ra = \{ra : r \in R\}$ нетривијалан подмодул од A, који је прост па је $A = Ra$, те је A цикличан. Посматрајмо кратак тачан низ

$$0 \to K \to R \xrightarrow{\epsilon} A \to 0,$$

где је $\epsilon \colon R \to A$ задато са: $\epsilon(r) = ra$. Пошто је A пројективан, постоји $\phi \colon A \to R$ тако да је $\epsilon \circ \phi = \mathrm{id}_A$. Покажимо да је (a, ϕ) пројективна база за A. Нека је $x \in A$. Тада је $x = \epsilon(\phi(x)) = \phi(x)a$.

Стога је $\tau(a, \phi) = \phi(a) \neq 0$, па је τ „на" на основу става 133. Дакле, A је R-прогенератор. □

Приметимо да нам овај доказ показује да је лево прост модул над лево простим прстеном R изоморфан минималном левом идеалу од R. Наиме, $A \cong \phi[A]$.

Следећа теорема је само констатација тога што смо до сада урадили.

Теорема 155. (Ведербернова теорема) Нека је R лево прост прстен, A лево прост R-модул. Тада, ако је $S = \mathrm{End}_R(A)^{op}$, онда је $R \cong \mathrm{End}_S(A)$, где је изоморфизам задат придруживањем $r \mapsto (a \mapsto ra)$. $\square$

Став 156. (Шурова лема) Прстен $S = \mathrm{End}_R(A)^{\mathrm{op}}$ је тело (прстен са дељењем).

Доказ. Ако је $\alpha\colon A \to A$ ендоморфизам модула A, онда су $\mathrm{Im}\,\alpha$ и $\mathrm{Ker}\,\alpha$ подмодули од A који је прост. Ако α није нула ендоморфизам, онда је $\mathrm{Im}\,\alpha = A$, а $\mathrm{Ker}\,\alpha = \{0\}$, те је α изоморфизам. Дакле, сваки елемент у $S \setminus \{0\}$ је инвертибилан, па је S тело. $\square$

Теорема 157. Нека је R лево прост прстен. Тада је R изоморфан прстену $M_n(S)$ за неко тело S.

Доказ. Како је R лево прост, он је једнак директној суми својих минималних левих идеала, који су сви изоморфни, а та директна сума је коначна, јер се 1_R представља у облику коначне суме елемената из тих минималних простих идеала. Дакле, можемо претпоставити да је $R \cong \underbrace{A \oplus \cdots \oplus A}_{n}$, где је A неки лево прост R-модул (изоморфан тим минималним левим идеалима). Тада је $R \cong \mathrm{End}_R(R)^{\mathrm{op}}$. Изоморфизам је задат са: $\Psi(r)(r') = r'r$. Ово множење здесна одговара опозитној структури. Наиме,

$$\Psi(r_1r_2)(r') = r'(r_1r_2) = (r'r_1)r_2 = \Psi(r_2)(r'r_1) = \Psi(r_2)(\Psi(r_1)(r')) = (\Psi(r_2) \circ \Psi(r_1)(r') = (\Psi(r_1) \circ^{\mathrm{op}} \Psi(r_2))(r').$$

Дакле, имамо низ изоморфизама:

$$R \cong \mathrm{End}_R(R)^{\mathrm{op}} \cong \mathrm{End}_R(\underbrace{A \oplus \cdots \oplus A}_{n})^{\mathrm{op}} \cong M_n\big(\mathrm{End}_R(A)^{\mathrm{op}}\big) = M_n(S),$$

где је S тело по Шуровој леми. Већ раније смо констатовали да хомоморфизми директне суме у директну суму одговарају матрицама одговарајућих хомоморфизама и то смо овде и искористили. $\square$

Последица 158. Нека је R лево полупрост прстен. Тада постоји изоморфизам $R \cong M_{n_1}(S_1) \times \cdots \times M_{n_k}(S_k)$ за неке $n_i \geqslant 1$ и тела S_i.

Доказ. Резултат се добија непосредно из претходне теореме и последице 150. $\square$

Наредна последица следи из ове класификације помоћу матрица пошто се ту јасно види да се лево и десно може заменити.

Последица 159. Прстен је лево полупрост акко је десно полупрост. $\square$

– Крај лекција–