# Algebra 3

Luka Horjak (lh0919@student.uni-lj.si)

26. junij 2023

# Kazalo

# Uvod

V tem dokumentu so zbrani moji zapiski s predavanj predmeta Algebra 3 v letu 2022/23. Predavatelj v tem letu je bil prof. dr. Primož Moravec.

Zapiski niso popolni. Manjka večina zgledov, ki pomagajo pri razumevanju definicij in izrekov. Poleg tega nisem dokazoval čisto vsakega izreka, pogosto sem kakšnega označil kot očitnega ali pa le nakazal pomembnejše korake v dokazu.

Zelo verjetno se mi je pri pregledu zapiskov izmuznila kakšna napaka – popravki so vselej dobrodošli.

# 1 Galoisova teorija

*»Jezik se mi zapleta. Ne vem, ali bi moral več spit ali manj spit.«*
– prof. dr. Primož Moravec

## 1.1 Normalne in separabilne razširitve

17. februar 2023

**Definicija 1.1.1.** Enačba je *rešljiva z radikali*, če lahko rešitev izrazimo z operacijami $+$, $-$, $\cdot$, $\div$, $\sqrt[n]{\ }$ iz podanih parametrov.

**Definicija 1.1.2.** Polje $E$ je *radikalska razširitev* polja $F$, če obstaja tak $a \in F$, da je $E = F(\sqrt[n]{a})$ za nek $n \in \mathbb{N}$.

**Opomba 1.1.2.1.** Polinomska enačba $p(X) = 0$ za $p(X) \in F[X]$ je rešljiva z radikali natanko tedaj, ko obstaja veriga

$$F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = F(p)$$

radikalskih razširitev.

**Definicija 1.1.3.** Razširitev $E$ polja $F$ je *normalna*, če za vsak nerazcepen polinom $p(X) \in F[X]$ velja, da $E$ vsebuje bodisi vse bodisi nobene ničle polinoma $p$.

**Izrek 1.1.4.** Naj bo $E/F$ končna razširitev. Tedaj je $E/F$ normalna natanko tedaj, ko je $E$ razpadno polje nekega polinoma $p(X) \in F[X]$.

*Dokaz.* Predpostavimo, da je $E/F$ normalna. Naj bo $E = F(a_1, \dots, a_r)$ in naj bo $p_i$ minimalni polinom za $a_i$. Naj bo

$$p(X) = \prod_{i=1}^{r} p_i(X).$$

Ker je $p_i$ nerazcepen, so vse ničle polinoma $p_i$ vsebovane v $E$ za vsak $i$. Posledično so tudi vse ničle polinoma $p$ vsebovane v $E$. Sledi, da je $F(p) \subseteq E$. Ker je očitno $E \subseteq F(p)$, je $E = F(p)$.

Predpostavimo sedaj, da je $E = F(p)$ za polinom $p$. Naj bo $q$ poljuben nerazcepen polinom z ničlo $a \in E$. Naj bo $b$ poljubna ničla polinoma $q$. Opazimo, da je $q$ minimalen polinom za $a$ in $b$, zato je $F(a) \sim F(b)$ z izomorfizmom $\sigma \colon a \mapsto b$. Sledi, da obstaja izomorfizem $\tau \colon (F(a))(p) \to (F(b))(p)$, ki se na $F(a)$ ujema s $\sigma$:

$$\begin{tikzcd}
& F(a) \arrow[r, hook] \arrow[dd, "\sigma"] & (F(a))(p) = F(a)(b_1, \dots, b_r) \arrow[dd, "\tau"] \\
F \arrow[ur, hook] \arrow[dr, hook] & & \\
& F(b) \arrow[r, hook] & (F(b))(p) = F(b)(b_1, \dots, b_r)
\end{tikzcd}$$

Ker je $a \in F(p)$, je $a$ racionalna funkcija ničel polinoma $p$, zato je tudi $b = \sigma(a)$ racionalna funkcija ničel polinoma $p$, zato je $b \in F(p)$. $\square$

**Definicija 1.1.5.** Polinom $p(X) \in F[X]$ je *separabilen*, če ima same enostavne ničle.

**Definicija 1.1.6.** Končna razširitev $E/F$ je *separabilna*, če je za vse $a \in E$ minimalni polinom elementa $a$ separabilen.

**Izrek 1.1.7** (O primitivnem elementu)**.** Naj bo $\operatorname{char} F = 0$. Če je $E/F$ končna razširitev, je enostavna.

24. februar 2023

*Dokaz.* Dovolj je pokazati, da za poljubna $a, b \in E$ velja $F(a, b) = F(a + \lambda b)$ za nek $\lambda \in F$. Naj bosta $p$ in $q$ minimalna polinoma elementov $a$ in $b$ zaporedoma. Naj bodo njune ničle zaporedoma $a_1, a_2, \ldots, a_m$ in $b_1, b_2, \ldots b_n$, kjer je $a = a_1$ in $b = b_1$. Ker je $\operatorname{char} F = 0$, so ničle posameznega polinoma paroma različne.

Naj bo
$$\lambda \in F \setminus \left\{ \frac{a - a_i}{b_j - b} \;\middle|\; j > 1 \right\}.$$
Sedaj definiramo $\tilde{p}(X) = p(a + \lambda b - \lambda X) \in F(a + \lambda b)[X]$. Opazimo, da je $b$ edina skupna ničla polinomov $\tilde{p}$ in $q$. Sledi, da je $\gcd(\tilde{p}, q) = X - b$. Po Bezoutovi lemi obstajata taka polinoma $r, s \in F(a + \lambda b)[X]$, da velja
$$r\tilde{p} + sq = X - b,$$
zato je tudi $X - b \in F(a + \lambda b)[X]$. Sledi, da je $b \in F(a + \lambda b)$ in posledično $a \in F(a + \lambda b)$. □

**Izrek 1.1.8** (O primitivnem elementu)**.** Če je $E/F$ končna separabilna razširitev, je enostavna.

*Dokaz.* Če je $F$ neskončno polje, lahko naredimo enak razmislek kot pri dokazu izreka 1.1.7.

Naj bo $F$ sedaj končno polje. Sledi, da je tudi $E = F(a_1, \ldots, a_k)$ končno. Sledi, da je $(E \setminus \{0\}, \cdot)$ ciklična grupa – naj bo $a$ njen generator. Očitno je tedaj $E = F(a)$. □

## 1.2 Galoisova grupa

**Definicija 1.2.1.** Avtomorfizem $\sigma$ polja $E$ je $F$*-avtomorfizem*, če je $\sigma|_F = \mathrm{id}$. Množici $F$-avtomorfizmov pravimo *Galoisova grupa* razširitve $E/F$ in jo označimo z $\mathrm{Gal}(E/F)$.

**Opomba 1.2.1.1.** Galoisova grupa $\mathrm{Gal}(E/F)$ je podgrupa grupe $\mathrm{Aut}\, E$.

**Lema 1.2.2.** Naj bo $E/F$ razširitev polja. Naj bo $a \in E$ ničla polinoma $p \in F[X]$. Potem je za poljuben $\sigma \in \mathrm{Gal}(E/F)$ tudi $\sigma(a)$ ničla polinoma $p$.

*Dokaz.* The proof is obvious and need not be mentioned. □

**Zgled 1.2.2.1.** Velja $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Velja namreč $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \overline{z}\}$.

**Zgled 1.2.2.2.** Grupa $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ je trivialna.

**Trditev 1.2.3.** Če je $E/F$ končna normalna separabilna razširitev, je

$$|\mathrm{Gal}(E/F)| = [E : F].$$

*Dokaz.* Obstaja tak $a \in E$, da je $E = F(a)$. Naj bo $p$ minimalen polinom za $a$. Vse ničle polinoma $p$ so enostavne in vsebovane v $E$, velja pa $\deg p = [E : F]$. Da določimo $\sigma \in \mathrm{Gal}(E/F)$, je dovolj določiti $\sigma(a)$, za kar imamo natanko $\deg p$ možnosti – za poljubno ničlo $b$ polinoma $p$ preslikava $a \mapsto b$ inducira izomorfizem $E = F(a) \to F(b) \cong E$. □

**Definicija 1.2.4.** Naj bo $p \in F[X]$. *Galoisova grupa* polinoma $p$ je grupa

$$\mathrm{Gal}(p) = \mathrm{Gal}(F(p)/F).$$

**Opomba 1.2.4.1.** Preslikava $\sigma \in \mathrm{Gal}(p)$ je permutacija ničel $a_1, \ldots, a_k$ polinoma $p$, zato jo lahko vložimo v $S_k$.

## 1.3 Galoisova korespondenca

**Definicija 1.3.1.** Naj bo $G$ podgrupa v $\mathrm{Gal}(E/F)$. *Fiksno polje* glede na grupo $G$ je množica

$$E^G = \{a \in E \mid \forall \sigma \in G \colon \sigma(a) = a\}\,.$$

**Opomba 1.3.1.1.** Če so $F \subseteq L \subseteq E$ polja, je $\mathrm{Gal}(E/L)$ podgrupa v $\mathrm{Gal}(E/F)$.

**Lema 1.3.2.** Naj bodo $F \subseteq L \subseteq E$ polja. 3. marec 2023

i) Če je $E/F$ končna razširitev, je taka tudi $E/L$.

ii) Če je $E/F$ normalna razširitev, je taka tudi $E/L$.

iii) Če je $E/F$ separabilna razširitev, je taka tudi $E/L$.

*Dokaz.*

i) Ker je $E$ končnorazsežen vektorski prostor nad $F$, je končnorazsežen tudi nad poljem $L$.

ii) Naj bo $a \in E$ ničla nerazcepnega polinoma $p(x) \in L[x]$ in naj bo $q$ minimalni polinom $a$ nad $F$. Opazimo, da velja $\gcd(p, q) = p$, saj je nekonstanten. Tako dobimo $p \mid q$. Ker so zaradi normalnosti razširitve $E/F$ vse ničle polinoma $q$ vsebovane v $E$, enako velja za ničle $p$.

iii) Podobno kot pri drugi točki iz separabilnosti polinoma $q$ sledi separabilnost minimalnega polinoma $p$ za $a \in E$. □

**Definicija 1.3.3.** Normalnim separabilnim razširitvam pravimo *Galoisove razširitve.*

**Lema 1.3.4.** Naj bo $E/F$ končna Galoisova razširitev. Tedaj je $E^{\mathrm{Gal}(E/F)} = F$.

*Dokaz.* Naj bo $a \in E \setminus F$ in $p$ minimalni polinom za $a$. Dovolj je dokazati, da obstaja izomorfizem $\sigma \in \mathrm{Gal}(E/F)$, za katerega je $\sigma(a) \neq a$. Ker je $a \notin F$, je $\deg p > 1$. Zaradi separabilnosti ima $p$ tako še ničlo $b \neq a$. Ker imata $a$ in $b$ skupni minimalni polinom, obstaja izomorfizem $T \colon F(a) \to F(b)$, za katerega je $F(a) = b$.

Ker je polje $F(p)$ razpadno polje nad $F(a)$ in $F(b)$, se izomorfizem $T$ razširi[1] do avtomorfizma $\widehat{T}$ polja $F(p)$. Ker pa je tudi $E/F(p)$ normalna, se $\widehat{T}$ razširi do izomorfizma $\sigma$ polja $E$.

$$\begin{tikzcd}
 & F(a) \arrow[r, hook] \arrow[dd, "T"', "\cong"] & F(a)(p) = F(p) \arrow[r, hook] \arrow[dd, "\widehat{T}"', "\cong"] & E \arrow[dd, "\sigma"', "\cong"] \\
F \arrow[ur, hook] \arrow[dr, hook] & & & \\
 & F(b) \arrow[r, hook] & F(b)(p) = F(p) \arrow[r, hook] & E
\end{tikzcd}$$

Pri tem velja $\sigma(a) = b \neq a$, zato je $a \notin E^{\mathrm{Gal}(E/F)}$. □

[1] Algebra 2.

**Izrek 1.3.5** (Fundamentalni Galoisove teorije)**.** Naj bo $E/F$ končna Galoisova razširitev.

i) Korespondenca $L \mapsto \mathrm{Gal}(E/L)$, $G \mapsto E^G$ med vmesnimi polji in podgrupami je bijektivna, ti preslikavi pa sta si inverzni.

ii) Za $F \subseteq L \subseteq M \subseteq E$ velja

$$[\mathrm{Gal}(E/L) : \mathrm{Gal}(E/M)] = [M : L].$$

iii) Za $F \subseteq L \subseteq E$ je $L/F$ normalna razširitev natanko tedaj, ko je $\mathrm{Gal}(E/L) \triangleleft \mathrm{Gal}(E/F)$. V tem primeru je

$$\mathrm{Gal}(E/F) \big/ \mathrm{Gal}(E/L) \cong \mathrm{Gal}(L/F).$$

*Dokaz.*

i) Naj bo $L$ vmesna razširitev polja $F$. Sledi, da je tudi $E/L$ Galoisova razširitev. Sledi, da je $E^{\mathrm{Gal}(E/L)} = L$.

Naj bo sedaj $G \leq \mathrm{Gal}(E/F)$. Naj bo $\sigma \in G$ in $a \in E^G$. Po definiciji je $\sigma(a) = a$, zato je $\sigma \in \mathrm{Gal}(E/E^G)$ in posledično $G \leq \mathrm{Gal}(E/E^G)$. Pokažimo, da je $\left|\mathrm{Gal}(E/E^G)\right| \leq |G|$.

Ker so je $E/F$ končna separabilna razširitev, obstaja tak $a \in E$, da je $E = F(a)$. Sedaj definiramo

$$p(x) = \prod_{T \in G} (x - T(a)).$$

Ni težko opaziti, da za vsak $\sigma \in G$ velja

$$\sigma(p) = \prod_{T \in G} (X - \sigma(T(a))) = p,$$

zato je $p \in E^G[x]$. Sledi, da minimalni polinom $q$ za $a$ nad $E^G$ deli $p$. Tako dobimo

$$\left|\mathrm{Gal}(E/E^G)\right| = [E : E^G] = \deg q \leq \deg p = |G|.$$

ii) Ker velja $[E : L] = [E : M] \cdot [M : L]$, sledi

$$[M : L] = \frac{[E : L]}{[E : M]} = \frac{|\mathrm{Gal}(E/L)|}{|\mathrm{Gal}(E/M)|}.$$

iii) Naj bo $a$ ničla minimalnega polinoma $p \in F[x]$. Po dokazu prejšnje leme vidimo, da za vsako ničlo $b$ polinoma $p$ obstaja izomorfizem $\sigma \in \mathrm{Gal}(E/F)$, za katerega je $\sigma(a) = b$. Poleg tega je za vsak $\sigma \in \mathrm{Gal}(E/F)$ element $\sigma(a)$ ničla polinoma $p$, zato $\sigma(a)$ preteče natanko vse ničle polinoma $p$.

Pokažimo, da je $L/F$ normalna razširitev natanko tedaj, ko je $\sigma(L) = L$ za vsak $\sigma \in \mathrm{Gal}(E/F)$. Če je $L$ normalna, lahko zapišemo $L = F(p) = F(a_1, \ldots, a_n)$. Ker je za vsak $\sigma \in \mathrm{Gal}(E/F)$ element $\sigma(a_i)$ ničla minimalnega polinoma elementa $a_i$, je $\sigma(a_i) \in L$ zaradi normalnosti. Tako je res $\sigma(L) \subseteq L$ in zato $\sigma(L) = L$ zaradi enakosti dimenzij. Če je $\sigma(L) = L$, pa za vsaki ničli $a$ in $b$ nerazcepnega polinoma

$p \in F[x]$ obstaja izomorfizem $\sigma$, za katerega je $\sigma(a) = b$. Če $L$ vsebuje ničlo $a$, vsebuje torej tudi vse ostale ničle.

Pokažimo sedaj, da velja $\mathrm{Gal}(E/\sigma(L)) = \sigma \cdot \mathrm{Gal}(E/L) \cdot \sigma^{-1}$. Res, velja

$$\begin{aligned} \tau \in \mathrm{Gal}(E/\sigma(L)) &\iff \forall a \in L \colon \tau(\sigma(a)) = \sigma(a) \\ &\iff \forall a \in L \colon \sigma^{-1}(\tau(\sigma(a))) = a \\ &\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(E/L). \end{aligned}$$

Sedaj lahko dokažemo trditev. Velja namreč

$$\begin{aligned} E/F \text{ je normalna razširitev} &\iff \forall \sigma \in \mathrm{Gal}(E/F) \colon \sigma(L) = L \\ &\iff \forall \sigma \in \mathrm{Gal}(E/F) \colon \mathrm{Gal}(E/L) = \sigma \,\mathrm{Gal}(E/L)\sigma^{-1} \\ &\iff \mathrm{Gal}(E/L) \triangleleft \mathrm{Gal}(E/F). \end{aligned}$$

Denimo, da je $L$ res normalna razširitev. Naj bo $\Phi \colon \mathrm{Gal}(E/F) \to \mathrm{Gal}(L/F)$ homomorfizem s predpisom $\sigma \mapsto \sigma|_L$. Ker je $E/L$ separabilna, lahko zapišemo $E = L(a)$. Poljuben izomorfizem $\tau \in \mathrm{Gal}(L/F)$ lahko razširimo do izomorfizma $\sigma \in \mathrm{Gal}(E/F)$ tako, da definiramo $\sigma(a) = a$. V tem primeru je seveda $\Phi(\sigma) = \tau$, zato je $\Phi$ surjektiven. Očitno je $\ker \Phi = \mathrm{Gal}(E/L)$, zato po izreku o izomorfizmu sledi

$$\mathrm{Gal}(E/F) \big/ \mathrm{Gal}(E/L) \cong \mathrm{Gal}(L/F). \qquad \square$$

**Opomba 1.3.5.1.** Naj bo $E/F$ končna razširitev in $H \leq \mathrm{Gal}(E/F)$ podgrupa, $L = E^H$ pa vmesna razširitev. Najmanjšo normalno razširitev $\widetilde{L}/F$, za katero je $L \subseteq \widetilde{L}$, dobimo kot $\widetilde{L} = E^{\widetilde{H}}$, kjer je

10. marec 2023

$$\widetilde{H} = \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma H \sigma^{-1}.$$

**Definicija 1.3.6.** Polju $\widetilde{L}$ pravimo *normalno zaprtje* polja $L$.

## 1.4 Rešljivost grup

**Definicija 1.4.1.** Grupa $G$ je *rešljiva*, če obstaja končno zaporedje podgrup

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = G,$$

za za katerega za vsak $i < k$ velja $G_i \triangleleft G_{i+1}$ in je ${G_{i+1}}/{G_i}$ abelova.

**Trditev 1.4.2.** Naj bo $G$ rešljiva grupa.

i) Če je $H \leq G$, je tudi $H$ rešljiva.

ii) Če je $N \triangleleft G$, je tudi ${G}/{N}$ rešljiva.

*Dokaz.* Po definiciji obstaja zaporedje

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = G,$$

ki ustreza pogojem rešljivosti. Ni težko videti, da za zaporedje $H_i = H \cap G_i$ velja $H_i \triangleleft H_{i+1}$. Velja še

$$G_{i+1} \cap H \Big/ G_i \cap H = G_{i+1} \Big/ G_{i+1} \cap H \cap G_i \,.$$

Opazimo, da je po drugem izreku o izomorfizmu

$$G_{i+1} \Big/ G_{i+1} \cap H \cap G_i \cong (G_{i+1} \cap H)G_i \Big/ G_i \leq G_{i+1} \Big/ G_i \,,$$

zato so kvocienti abelovi. Sledi, da je $H$ rešljiva.

Naj bo sedaj $N \triangleleft G$. Tedaj je

$$1 = G_0N \Big/ N \leq G_1N \Big/ N \leq \cdots \leq G_kN \Big/ N = G \Big/ N \,.$$

Opazimo, da velja ${G_iN}/{N} \triangleleft {G_{i+1}N}/{N}$. Za $a \in G_i$, $b \in G_{i+1}$ in $n, m \in N$ namreč velja

$$(bmN)(anN)(bmN)^{-1} = \underbrace{bmb^{-1}}_{N}\underbrace{bab^{-1}}_{G_i}\underbrace{b(nm^{-1})b^{-1}}_{N} N \in G_iN \Big/ N \,.$$

Opazimo še

$$G_{i+1}N \Big/ G_iN = G_{i+1}G_iN \Big/ G_iN \cong G_{i+1} \Big/ G_{i+1} \cap G_iN \cong {G_{i+1}/G_i} \Big/ {G_{i+1} \cap G_iN / G_i} \,,$$

kar je abelova grupa. □

**Opomba 1.4.2.1.** Grupa $S_5$ ni rešljiva, saj $A_5$ ni rešljiva (je enostavna in ni abelova).

**Izrek 1.4.3** (Feit-Thompson)**.** Vsaka končna grupa lihe moči je rešljiva.

### 1.5 Reševanje polinomskih enačb z radikali

V nadaljevanju predpostavimo $\operatorname{char} F = 0$.

**Definicija 1.5.1.** Naj bo $p(X) \in F[X]$. Enačba $p(X) = 0$ je *rešljiva z radikali*, če obstaja tako zaporedje polj

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E,$$

da so razširitve $E_{i+1}/E_i$ radikalske in velja $F(p) \subseteq E$.

**Lema 1.5.2.** Naj bo $F$ polje, ki vsebuje $n$-te korene enote in $a \in F$. Tedaj je grupa $\operatorname{Gal}(X^n - a)$ ciklična.

*Dokaz.* Naj bo $\omega \in F$ primitiven $n$-ti koren enote. Tedaj so vse rešitve enačbe $X^n - a = 0$ ravno $b\omega^k$. Razpadno polje polinoma $X^n - a$ je tako kar $F(b)$.

Naj bo $\sigma \in \operatorname{Gal}(X^n - a)$ in $\sigma(b) = b\omega^\ell$. Opazimo, da je preslikava $\operatorname{Gal}(X^n - a) \to \mathbb{Z}_n$, $\sigma \mapsto \ell$, injektiven homomorfizem. □

**Izrek 1.5.3.** Recimo, da je enačba $p(X) = 0$ za $p(X) \in F[X]$ rešljiva z radikali. Potem je $\operatorname{Gal}_F(p)$ rešljiva grupa.

*Dokaz.* Naj bo

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m = E$$

zaporedje iz definicije rešljivosti z radikali. Naj bo še $a_i^{r_i} \in E_i$ za vsak $i$ in

$$n = \prod_{i=1}^{m-1} r_i.$$

Naj bo $\omega$ primitiven $n$-ti koren enote. Naj bo $\Omega$ Galoisova razširitev polja $F$, ki vsebuje $E$ in $\omega$. Naj bo $\widetilde{E}$ normalno zaprtje $E(\omega)$ v $\Omega$. Opazimo, da je

$$\widetilde{E} = F(\omega, a_1, \dots, a_{m-1}, \sigma_1(a_1), \dots).$$

Tako lahko najdemo zaporedje

$$F \subseteq F(\omega) \subseteq F(\omega, a_1) \subseteq \cdots \subseteq \widetilde{E}.$$

Z Galoisovo korespondenco dobimo zaporedje

$$\operatorname{Gal}\left(\widetilde{E}/\widetilde{E}\right) \subseteq \cdots \subseteq \operatorname{Gal}\left(\widetilde{E}/F(\omega, a_1)\right) \subseteq \operatorname{Gal}\left(\widetilde{E}/F(\omega)\right) \subseteq \operatorname{Gal}\left(\widetilde{E}/F\right).$$

Po zgornji lemi so kvocienti zaporednih grup ciklični. Sledi, da je $\operatorname{Gal}\left(\widetilde{E}/F\right)$ rešljiva grupa. Sledi, da je

$$\operatorname{Gal}(E/F) \cong \operatorname{Gal}\left(\widetilde{E}/F\right) \Big/ \operatorname{Gal}\left(\widetilde{E}/E\right)$$

rešljiva grupa. □

**Opomba 1.5.3.1.** Velja tudi obratno – če je $\operatorname{Gal}_F(p)$ rešljiva grupa, je enačba $p(X) = 0$ rešljiva z radikali.

# 2 Moduli

*"Moj tinitus samo slabši postaja.«*
– prof. dr. Primož Moravec

## 2.1 Definicija

**Definicija 2.1.1.** Naj bo $M$ neprazna množica in $R$ kolobar. Množica $M$ z operacijama $+\colon M \times M \to M$ in $\cdot\colon R \times M \to M$ je *$R$-modul*, če velja naslednje:

i) $(M, +)$ je abelova grupa.

ii) Za vse $r \in R$ in $m_1, m_2 \in M$ velja $r(m_1 + m_2) = rm_1 + rm_2$.

iii) Za vse $r_1, r_2 \in R$ in $m \in M$ velja $(r_1 + r_2)m = r_1m + r_2m$.

iv) Za vse $r_1, r_2 \in R$ in $m \in M$ velja $r_1(r_2m) = (r_1r_2)m$.

v) Za vse $m \in M$ je $1 \cdot m = m$.

**Definicija 2.1.2.** Naj bo $M$ $R$-modul. Neprazna množica $N \subseteq M$ je *podmodul* v $M$, če je $R$-modul z induciranimi preslikavami.

**Definicija 2.1.3.** Naj bo $M$ $R$-modul in $X \subseteq M$. Najmanjši podmodul v $M$, ki vsebuje $X$, označimo z $\langle X \rangle$.

17. marec 2023

**Trditev 2.1.4.** Velja

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i x_i \;\middle|\; n \in \mathbb{N} \land r_i \in R \land x_i \in X \right\}.$$

*Dokaz.* The proof is obvious and need not be mentioned. □

**Definicija 2.1.5.** Podmodul $N$ modula $M$ je *končnogeneriran*, če obstaja končna množica $X \subseteq M$, za katero je $\langle X \rangle = N$.

**Definicija 2.1.6.** Podmodul $N$ modula $M$ je *cikličen*, če za nek $x \in M$ velja $N = \langle \{x\} \rangle = \langle x \rangle$.

## 2.2 Homomorfizmi modulov

**Definicija 2.2.1.** Naj bosta $M$ in $M'$ $R$-modula. Preslikava $\varphi\colon M \to M'$ je *homomorfizem modulov*, če za vse $m_1, m_2 \in M$ in $r \in R$ velja

$$\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) \quad \text{in} \quad \varphi(rm_1) = r\varphi(m_1).$$

**Definicija 2.2.2.** Naj bo $\varphi\colon M \to M'$ homomorfizem modulov. Označimo

$$\ker\varphi = \{x \in M \mid \varphi(x) = 0\}$$

in

$$\operatorname{im}\varphi = \{\varphi(x) \mid x \in M\}.$$

**Definicija 2.2.3.** Naj bo $\varphi\colon M \to M'$ homomorfizem modulov. Pravimo, da je $\varphi$

i) *endomorfizem*, če je $M = M'$,

ii) *monomorfizem*, če je injektiven,

iii) *epimorfizem*, če je surjektiven,

iv) *izomorfizem*, če je bijektiven.

Če obstaja izomorfizem $\varphi\colon M \to M'$, pravimo, da sta modula $M$ in $M'$ izomorfna, oziroma $M \cong M'$.

**Definicija 2.2.4.** Naj bo $M$ $R$-modul in $N$ njegov podmodul. *Kvocientni modul* je definiran kot

$$M/N = \{m + N \mid m \in M\}$$

z naravno definiranim seštevanjem in množenjem.

**Opomba 2.2.4.1.** Kvocientni modul je spet $R$-modul.

**Definicija 2.2.5.** Preslikavi $\pi\colon M \to M/N$, podani s predpisom $\pi(m) = m+N$, pravimo *kanonični epimorfizem*.

**Opomba 2.2.5.1.** Kanonični epimorfizem je seveda epimorfizem.

## 2.3 Izreki o izomorfizmih

**Trditev 2.3.1.** Naj bo $\varphi\colon M \to N$ homomorfizem $R$-modulov in $L \leq M$. Če je $L \leq \ker \varphi$, $\varphi$ inducira homomorfizem $\tilde{\varphi}\colon M/L \to N$ s predpisom $\tilde{\varphi}(m + L) = \varphi(m)$. Pri tem velja $\operatorname{im} \tilde{\varphi} = \operatorname{im} \varphi$ in $\ker \tilde{\varphi} = \ker \varphi / L$.

*Dokaz.* Če je $m_1 + L = m_2 + L$, je očitno $\varphi(m_1) = \varphi(m_2)$, zato je preslikava dobro definirana. Ni težko videti, da je preslikava homomorfizem z zgoraj naštetima jedrom in sliko. $\square$

**Izrek 2.3.2** (O izomorfizmu)**.** Naj bo $\varphi\colon M \to N$ homomorfizem $R$-modulov. Tedaj je $M/\ker \varphi \cong \operatorname{im} \varphi$, $\varphi$ pa ima epi-mono razcep

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"'] & N \\ M/\ker\varphi \arrow[r, "\cong", "\varphi"'] & \operatorname{im}\varphi \arrow[u, hook, "i"'] \end{tikzcd}$$

*Dokaz.* V prejšnji trditvi vzamemo $L = \ker \varphi$. $\square$

**Izrek 2.3.3** (Noether)**.** Naj bodo $M$, $N$ in $L$ $R$-moduli.

i) Če je $M \leq N \leq L$, velja $N/M \leq L/M$ in
$$\left(L/M\right) \Big/ \left(N/M\right) \cong L/N\,.$$

ii) Če je $M, N \leq L$, velja
$$M \Big/ M \cap N \cong M + N \Big/ N$$

iii) Če je $M \leq L$, so podmoduli v $L$, ki vsebujejo $M$, v bijektivni korespondenci s podmoduli v $L/M$.

*Dokaz.* Preslikavi $\varphi\colon \left(L/M\right) \Big/ \left(N/M\right) \to L/N$ in $\psi\colon M/M \cap N \to M + N/N$ s predpisoma
$$\varphi\left((x + M) + N/M\right) = x + N$$
in
$$\psi(x + (M \cap N)) = x + N$$
sta izomorfizma. $\square$

## 2.4 Direktna vsota modulov

**Definicija 2.4.1.** Naj bodo $M_1, \ldots, M_s$ $R$-moduli. Množici

$$\prod_{i=1}^{s} M_i$$

s seštevanjem in množenjem po komponentah pravimo *direktna vsota* modulov in jo označimo z

$$\bigoplus_{i=1}^{s} M_i.$$

**Definicija 2.4.2.** $R$-modul $M$ je *notranja direktna vsota* podmodulov $N_1, \ldots, N_2$, če je abelova grupa $(M, +)$ notranja direktna vsota grup $(N_i, +)$.

**Trditev 2.4.3.** Naj bo $M$ $R$-modul in $N_1, \ldots, N_s$ njegovi podmoduli. Modul $M$ je direktna vsota $N_1, \ldots, N_s$ natanko tedaj, ko se da vsak $m \in M$ na enoličen način zapisati kot

$$m = \sum_{i=1}^{s} n_i,$$

pri čemer je $n_i \in N_i$ za vsak $i$.

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 2.4.4.** Če je $M$ notranja direktna vsota podmodulov $N_1, \ldots, N_s$, je izomorfen njihovi direktni vsoti. Zunanja direktna vsota modulov $N_1, \ldots, N_s$ je izomorfna notranji direktni vsoti podmodulov

$$\prod_{i=1}^{k-1} \{0\} \times N_k \times \prod_{i=k+1}^{s} \{0\} \leq \prod_{i=1}^{s} N_i.$$

*Dokaz.* The proof is obvious and need not be mentioned. □

**Opomba 2.4.4.1.** Lahko definiramo tudi direktno vsoto neskončno mnogo modulov, a pri tem zahtevamo, da je kvečjemu končno komponent neničelnih.

## 2.5 Prosti moduli

**Definicija 2.5.1.** Naj bo $M$ $R$-modul. Množici $X \subseteq M$ pravimo *baza* za $M$, če velja

i) $\langle X \rangle = M$ in

ii) za vse $n \in \mathbb{N}$, $\lambda_i \in R$ in $x_i \in X$ iz enakosti

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

sledi $\lambda_i = 0$ za vse $i$.

**Definicija 2.5.2.** $R$-modul $M$ je *prost*, če ima bazo.

**Izrek 2.5.3.** Za $R$-modul $M$ so ekvivalentne naslednje trditve:

i) $M$ je prost.

ii) $M$ je izomorfen direktni vsoti kopij $R$-modula $R$.

iii) Velja

$$M = \bigoplus_{\lambda \in \Lambda} M_\lambda$$

za $M_\lambda \subseteq M$ in $M_\lambda \cong R$.

*Dokaz.* Drugi točki sta očitno ekvivalentni. Naj bo $M$ prost $R$-modul. Tedaj velja

$$M = \bigoplus_{x \in X} \langle x \rangle ,$$

kjer je $X$ baza $M$, očitno pa je $R \cong \langle x \rangle$, saj je $r \mapsto r \cdot x$ izomorfizem.

Denimo sedaj, da obstaja izomorfizem

$$f \colon \bigoplus_{\lambda \in \Lambda} R \to M.$$

Tedaj je

$$X = \{f(e_\lambda) \mid \lambda \in \Lambda\}$$

očitno baza za $M$. □

**Posledica 2.5.3.1.** Vsak $R$-modul je kvocient prostega $R$-modula.

*Dokaz.* Naj bo $M$ $R$-modul. Tedaj je preslikava

$$f \colon \bigoplus_{m \in M} R \to M$$

s predpisom $f(e_m) = m$ epimorfizem $R$-modulov. □

**Opomba 2.5.3.2.** Če je vsak $R$-modul prost, je $R$ obseg.

**Opomba 2.5.3.3.** Podmodul prostega $R$-modula ni nujno prost.

**Trditev 2.5.4.** Naj bo $D$ obseg in $M$ $D$-modul. Tedaj veljajo naslednje trditve:

i) $M$ je prost.

ii) Iz vsakega ogrodja $M$ lahko izberemo bazo.

iii) Vsako linearno neodvisno množico lahko razširimo do baze.

iv) Poljubni bazi imata enako kardinalnost $\dim_D M$.

v) Za vsak $N \leq M$ velja $\dim_D M = \dim_D N + \dim_D {}^{M}\!/_{N}$.

vi) Za vsak homomorfizem $\varphi \colon M \to N$ je $\dim_D M = \dim_D \ker \varphi + \dim_D \operatorname{im} \varphi$.

*Dokaz.* Enak kot za vektorske prostore. $\square$

**Trditev 2.5.5** (Univerzalna lastnost prostih modulov)**.** $R$-modul $M$ je prost natanko tedaj, ko obstaja neprazna množica $X$ in preslikava $\iota \colon X \to M$, za katera za vsak $R$-modul $N$ in preslikavo $f \colon X \to N$ obstaja natanko en homomorfizem $g \colon M \to N$, za katerega je $f = g \circ \iota$.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\iota"'] & N \\ M \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

*Dokaz.* Naj bo $X$ baza za $M$ in $\iota \colon X \hookrightarrow M$ vložitev. Naj bo $N$ poljuben $R$-modul in $f \colon X \to N$ prelikava. Zdaj za vse $x_i \in X$ in $r_i \in R$ definiramo

$$g\left(\sum_{i=1}^{n} r_i x_i\right) = \sum_{i=1}^{n} r_i f(x_i).$$

Očitno je to homomorfizem. Ni težko videti, da je edini, ki zadošča $f = g \circ \iota$.

Sedaj predpostavimo, da za $M$ velja univerzalna lastnost. Naj bo

$$N = \bigoplus_{x \in X} R$$

in $f \colon X \to N$ preslikava, ki deluje po predpisu $f(x) = e_x$. Sledi, da obstaja enolična preslikava $g \colon M \to N$, za katero je $f = g \circ \iota$. Ker je $N$ prost, po univerzalni lastnosti obstaja enolična preslikava $h \colon N \to M$, za katero je $\iota = h \circ f$. Sedaj opazimo, da je

$$(g \circ h) \circ f = g \circ \iota = f = \mathrm{id} \circ f$$

in

$$(h \circ g) \circ \iota = h \circ f = \iota = \mathrm{id} \circ \iota.$$

Iz enoličnosti tako sledi $g \circ h = \mathrm{id}$ in $h \circ g = \mathrm{id}$, zato je $M \cong N$. $\square$

**Definicija 2.5.6.** Kolobar $R$ ima *lastnost enoličnega ranga*, če ima za vsak prost $R$-modul vsaka njegova baza enako moč. Moč baze označimo z $\operatorname{rang} M$.

**Definicija 2.5.7.** Naj bo $M$ $R$-modul in $I \triangleleft R$. Tedaj definiramo

$$I \cdot M = \left\{ \sum_{i=1}^{n} u_i m_i \;\middle|\; n \in \mathbb{N} \wedge u_i \in I \wedge m_i \in M \right\}.$$

**Opomba 2.5.7.1.** Velja $IM \leq M$.

**Lema 2.5.8.** Če je $M$ prost $R$-modul z bazo $X$, je $M/_{IM}$ prost $R/_{I}$-modul z bazo $X + IM$.

*Dokaz.* Očitno je $\langle X + IM \rangle = M/_{IM}$. Denimo, da je

$$\sum_{i=1}^{n} (r_i + I)(x_i + IM) = 0.$$

Ekvivalentno, velja

$$\sum_{i=1}^{n} r_i x_i \in IM,$$

zato je

$$\sum_{i=1}^{n} r_i x_i = \sum_{i=1}^{m} u_i \tilde{x}_i,$$

pri čemer so $u_i \in I$. Ker je $X$ baza $M$, sledi $r_i \in I$ za vse $i$. $\square$

**Trditev 2.5.9.** Naj bo $X$ baza $R$-modula $M$. Če je $I$ pravi ideal v $R$, je $|X + IM| = |X|$.

*Dokaz.* Denimo, da je $x + IM = y + IM$ za $x, y \in X$. Tedaj je

$$1 \cdot x - 1 \cdot y = \sum_{i=1}^{n} u_i x_i,$$

zato je $x = y$. $\square$

**Izrek 2.5.10.** Veljata naslednji trditvi:

i) Če ima kakšen netrivialen kvocient kolobarja $R$ lastnost enoličnega ranga, jo ima tudi $R$.

ii) Vsi komutativni kolobarji imajo lastnost enoličnega ranga.

*Dokaz.*

i) Naj bo $I \triangleleft R$ pravi ideal v $R$, za katerega ima $R/_{I}$ lastnost enoličnega ranga. Tedaj za prost $M$-modul z bazama $X$ in $Y$ velja

$$|X| = |X + IM| = |Y + IM| = |Y|\,.$$

ii) Naj bo $R$ komutativen kolobar. Predpostavimo, da $R$ ni polje, saj ta imajo lastnost enoličnega ranga. Naj bo $I \triangleleft R$ pravi ideal. Po Zornovi lemi obstaja maksimalni ideal $J \triangleleft R$, ki vsebuje $I$. Tedaj je $R/_{J}$ polje, saj nima pravih netrivialnih idealov. Po prvi točki ima $R$ lastnost enoličnega ranga. $\square$

## 2.6 Projektivni moduli

24. marec 2023

**Definicija 2.6.1.** Naj bo $R$ kolobar. $R$-modul $P$ je *projektiven*, če za vsak homomorfizem $R$-modulov $f\colon P \to N$ in epimorfizem $g\colon M \to N$ obstaja homomorfizem $h\colon P \to M$, za katerega je $g \circ h = f$.

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, dashed, "h"'] \\ M \arrow[r, two heads, "g"'] & M' \end{tikzcd}$$

**Trditev 2.6.2.** Vsak prost $R$-modul $F$ je projektiven.

*Dokaz.* Naj bo $f\colon F \to M'$ homomorfizem in $g\colon M \to M'$ epimorfizem. Za vsak $x \in X$ velja $f \circ \iota(x) \in M'$, zato obstaja tak $m_x \in M$, da je $f \circ \iota(x) = g(m_x)$. Sedaj definiramo preslikavo $\tau\colon X \to M$ s predpisom $\tau(x) = m_x$. Po univerzalni lastnosti prostih modulov obstaja homomorfizem $h\colon F \to M$, za katerega je $h \circ \iota = \tau$. Ker velja

$$(g \circ h) \circ \iota = g \circ \tau = f \circ \iota,$$

po univerzalni lastnosti sledi $g \circ h = f$. □

**Izrek 2.6.3.** Za $R$-modul $P$ so ekvivalentne naslednje trditve:

i) $P$ je projektiven.

ii) Za vsak epimorfizem $\varphi\colon M' \to P$ je $M' \cong P \oplus \ker \varphi$.

iii) Obstaja $R$-modul $M$, za katerega je $P \oplus M$ prost $R$-modul.

*Dokaz.* Denimo, da je $P$ projektiven in $\varphi\colon M' \to P$ poljuben epimorfizem. Zaradi projektivnosti $P$ obstaja tak homomorfizem $\psi\colon P \to M'$, da je $\varphi \circ \psi = \mathrm{id}$. Tako sledi, da je $\psi$ injektiven in zato $\operatorname{im} \psi \cong P$. Ni težko preveriti, da je $\operatorname{im} \psi \cap \ker \varphi = \{0\}$. Ker za vsak $m \in M'$ velja $m - \psi \circ \varphi(m) \in \ker \varphi$ in lahko zapišemo

$$m = (m - \psi \circ \varphi(m)) + \psi \circ \varphi(m),$$

je $M' = \operatorname{im} \psi \oplus \ker \varphi$.

Sedaj predpostavimo, da velja druga točka. Ker je $P$ kvocient nekega prostega $R$-modula $F$, velja

$$F \cong P \oplus \ker \pi.$$

Denimo sedaj, da je $P \oplus N$ prost $R$-modul in dokažimo, da je $P$ projektiven. Naj bo $f\colon P \to M'$ homomorfizem, $g\colon M \to M'$ pa epimorfizem. Definirajmo homomorfizem $\tilde{f}\colon P \oplus N \to M'$ kot $\tilde{f} = f \circ \pi$, kjer je $\pi\colon P \oplus N \to P$ projekcija. Ker je $P \oplus N$ projektiven, obstaja tak homomorfizem $\tilde{h}\colon P \oplus N \to M$, da je $g \circ \tilde{h} = \tilde{f}$. Sedaj lahko za $h\colon P \to M$ izberemo kar $h(p) = \tilde{h}(p, 0)$, saj velja

$$g \circ h(p) = g \circ \tilde{h}(p, 0) = \tilde{f}(p, 0) = f(p).$$ □

**Opomba 2.6.3.1.** Vsak projektiven modul nad lokalnim[2] kolobarjem je prost.

[2] Za vsak $x \in R$ je $x$ ali $1 - x$ obrnljiv.

## 2.7 Tenzorski produkt modulov

31. marec 2023

**Definicija 2.7.1.** Naj bo $R$ komutativen kolobar z enoto, $M$ in $N$ pa $R$-modula. Naj bo $P$ prost $R$-modul, generiran z množico $M \times N$. Naj bo $Y$ podmodul v $P$, generiran z naslednjimi množicami:

$$\begin{gathered}\{(m+m',n)-(m,n)-(m',n) \mid m,m' \in M \wedge n \in N\}, \\ \{(m,n+n')-(m,n)-(m,n') \mid m \in M \wedge n,n' \in N\}, \\ \{(rm,n)-r(m,n) \mid r \in R \wedge m \in M \wedge n \in N\}, \\ \{(m,rn)-r(m,n) \mid r \in R \wedge m \in M \wedge n \in N\}.\end{gathered}$$

Modulu

$$M \otimes_R N = {}^{P}\big/{}_{Y}$$

pravimo *tenzorski produkt* modulov $M$ in $N$.

**Opomba 2.7.1.1.** Sliko para $(m,n) \in P$ v $M \otimes_R N$ označimo z $m \otimes n$. Takim tenzorjem pravimo *enostavni tenozorji.*

**Opomba 2.7.1.2.** Preslikava $\tau\colon M \times N \to M \otimes_R N$ s predpisom $\tau(m,n) = m \otimes n$ je bilinearna.

**Izrek 2.7.2** (Univerzalna lastnost tenzorskih produktov)**.** Naj bodo $M$, $N$ in $T$ $R$-moduli.

i) Vsaka $R$-bilinearna preslikava $\varphi\colon M \times N \to T$ inducira enolično določen homomorfizem $R$-modulov $\tilde{\varphi}\colon M \otimes_R N \to T$, za katero je $\tilde{\varphi} \circ \tau = \varphi$.

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[d, "\tau"'] & T \\ M \otimes_R N \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

ii) Naj bo $\psi\colon M \times N \to T$ bilinearna preslikava. Če za vsako bilinearno preslikavo $\varphi\colon M \times N \to L$ obstaja natanko en homomorfizem $R$-modulov $\tilde{\varphi}\colon T \to L$, za katerega je $\tilde{\varphi} \circ \psi = \varphi$, je $T \cong M \otimes_R N$.

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[d, "\psi"'] & L \\ T \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

*Dokaz.*

i) Ker je $P$ prost $R$-modul nad $M \times N$, po univerzalni lastnosti obstaja enoličen homomorfizem $\hat{\varphi}\colon P \to T$, za katerega na $M \times N$ velja $\hat{\varphi}(m,n) = \varphi(m,n)$. Ni težko videti, da je $Y \subseteq \ker \hat{\varphi}$, zato $\hat{\varphi}$ inducira homomorfizem $\tilde{\varphi}\colon M \otimes_R N \to T$.

ii) Obstaja enoličen homomorfizem $\tilde{\psi}\colon M \otimes_R N \to T$, za katerega je $\tilde{\psi} \circ \tau = \psi$. Po predpostavki izreka obstaja enoličen homomorfizem $\tilde{\tau}\colon T \to M \otimes_R N$, za katerega je $\tilde{\tau} \circ \psi = \tau$. Opazimo, da velja

$$\tilde{\psi} \circ \tilde{\tau} \circ \psi = \tilde{\psi} \circ \tau = \mathrm{id} \circ \psi$$

in
$$\tilde{\tau} \circ \tilde{\psi} \circ \tau = \tilde{\tau} \circ \psi = \mathrm{id} \circ \tau.$$
Po enoličnosti sledi, da je $\tilde{\psi} = \tilde{\tau}^{-1}$. □

**Opomba 2.7.2.1.** Če je $M = \langle X \rangle$ in $N = \langle Y \rangle$, je

$$M \otimes_R N = \langle \{x \otimes y \mid x \in X \wedge y \in Y\} \rangle .$$

**Opomba 2.7.2.2.** Naj bosta $f\colon M_1 \to M_2$ in $g\colon N_1 \to N_2$ homomorfizma $R$-modulov. Tedaj $f$ in $g$ inducirata homomorfizem $f \otimes g\colon M_1 \otimes_R N_1 \to M_2 \otimes_R N_2$ s predpisom

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

**Trditev 2.7.3.** Naj bo $M$ $R$-modul. Potem je

$$M \otimes_R R \cong M \cong R \otimes_R M.$$

*Dokaz.* Preslikava $\varphi\colon R \times M \to M$ s predpisom $\varphi(r, m) = rm$ je bilinearna, zato inducira homomorfizem $\tilde{\varphi}\colon M \otimes_R R \to M$. Ni težko videti, da je $\tilde{\varphi}^{-1}(m) = m \otimes 1$. □

**Trditev 2.7.4.** Naj bo $M$ prost $R$-modul z bazo $\{m_i \mid i \in I\}$, $N$ pa prost $R$-modul z bazo $\{n_j \mid j \in J\}$. Potem je $M \otimes_R N$ prost $R$-modul z bazo

$$\{m_i \otimes n_j \mid i \in I \wedge j \in J\} .$$

*Dokaz.* Množica očitno generira $M \otimes_R N$, zato je dovolj preveriti linearno neodvisnost. Predpostavimo torej, da je
$$\sum r_{i,j}(m_i \otimes n_j) = 0.$$
Za vsak $k \in J$ definiramo homomorfizem $f_k\colon N \to R$, ki na bazi deluje po predpisu $f_k(n_j) = \delta_{k,j}$. Če zgornjo enačbo preslikamo z $(\mathrm{id} \otimes f_k)$, dobimo

$$0 = \sum r_{i,j}(m_i \otimes \delta_{k,j}),$$

oziroma
$$0 = \sum r_{i,k} m_i.$$
Sledi, da so vsi koeficienti enaki 0. □

**Trditev 2.7.5.** Naj bodo $A$, $B$ in $C$ $R$-moduli. Tedaj velja

i) $A \otimes_R B \cong B \otimes_R A$,

ii) $A \otimes_R (B \oplus C) \cong A \otimes_R B \oplus A \otimes C$,

iii) $(A \otimes_R B) \otimes_R C \cong A \otimes_R (B \otimes_R C)$.

*Dokaz.*

i) Preslikava $(a, b) \mapsto b \otimes a$ je bilinearna, zato inducira homomorfizem $\varphi\colon A \otimes_R B \to B \otimes_R A$, ki slika po predpisu $\varphi(a \otimes b) = b \otimes a$. Simetrično dobimo še njegov inverz.

ii) Naj bo $\varphi\colon A \times (B \oplus C) \to A \otimes_R B \oplus A \otimes C$ preslikava, ki deluje po predpisu
$$\varphi(a, (b, c)) = (a \otimes b, a \otimes c).$$
Očitno je bilinearna, zato inducira homomorfizem $\tilde{\varphi}\colon A \otimes_R (B \oplus C) \to A \otimes_R B \oplus A \otimes C$.

Definirajmo preslikavi $\psi_1\colon A \times B \to A \otimes_R (B \oplus C)$ in $\psi_2\colon A \times B \to A \otimes_R (B \oplus C)$ s predpisoma
$$\psi_1(a, b) = a \otimes (b, 0) \quad \text{in} \quad \psi_2(a, c) = a \otimes (0, c).$$
Očitno sta bilinearni, zato inducirata homomorfizma na tenzorskem produktu, to pa sta ravno komponenti inverza homomorfizma $\tilde{\varphi}$.

iii) Naj bo $\varphi_a\colon B \times C \to (A \otimes_R B) \otimes_R C$ preslikava s predpisom $\varphi_a(b, c) = (a \otimes b) \otimes c$. Očitno je bilinearna, zato inducira homomorfizem $\tilde{\varphi}_a$ $R$-modulov $B \otimes_R C$ in $(A \otimes_R B) \otimes_R C$ s predpisom
$$\tilde{\varphi}_a(b \otimes c) = (a \otimes b) \otimes c.$$
Preslikava $\varphi\colon A \times (B \otimes_R C) \to (A \otimes_R B) \otimes_R C$ s predpisom $\varphi(a, \omega) = \tilde{\varphi}_a(\omega)$ je bilinearna, zato inducira homomorfizem $\tilde{\varphi}$ ustreznih tenzorskih produktov. Simetrično lahko skonstruiramo tudi inverz $\tilde{\varphi}$. □

7. april 2023

**Trditev 2.7.6.** Naj bo $R$ komutativen kolobar, $M$ in $N$ pa prosta $R$-modula z bazama $\{m_i \mid i \in I\}$ in $\{n_j \mid j \in J\}$. Tedaj je $M \otimes_R N$ prost $R$-modul z bazo
$$\{m_i \otimes n_j \mid i \in I, j \in J\}.$$

*Dokaz.* Množica očitno generira $M \otimes_R N$, zato je dovolj preveriti linearno neodvisnost. Predpostavimo torej, da je
$$\sum r_{i,j}(m_i \otimes n_j) = 0.$$
Za vsak $k \in J$ definiramo homomorfizem $f_k\colon N \to R$, ki na bazi deluje po predpisu $f_k(n_j) = \delta_{k,j}$. Če zgornjo enačbo preslikamo z $(\mathrm{id} \otimes f_k)$, dobimo
$$0 = \sum r_{i,j}(m_i \otimes \delta_{k,j}),$$
oziroma
$$0 = \sum r_{i,k} m_i.$$
Sledi, da so vsi koeficienti enaki 0. □

**Opomba 2.7.6.1.** Za nekomutativne kolobarje definiramo $M \otimes_R N$ na naslednji način:

Naj bo $M$ desni, $N$ pa levi $R$-modul. Naj bo $F$ prosta abelova grupa nad množico $\{(m, n) \mid m \in M, n \in N\}$. Tedaj je
$$M \otimes_R N = {F}/{T},$$
kjer je $T$ podgrupa v $F$, generirana z
$$(m_1 + m_2, n) - (m_1, n) - (m_2, n), \quad (m, n_1 + n_2) - (m, n_1) - (m, n_2) \quad \text{in} \quad (mr, n) - (m, rn).$$

## 2.8 Skrčitve in razširitve skalarjev

**Trditev 2.8.1.** Naj bo $f\colon R \to S$ homomorfizem kolobarjev.

i) Naj bo $M$ $S$-modul. Tedaj je $M$ tudi $R$-modul z operacijo
$$r \cdot m = f(r) \cdot m.$$

ii) Naj bo $R$ komutativen kolobar, $M$ pa $R$-modul. Tedaj je $S \otimes_R M$ $S$-modul.

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 2.8.2.** Naj bo $f\colon R \to S$ homomorfizem kolobarjev, kjer je $R$ komutativen. Naj bo $M$ $R$-modul, $N$ pa $S$-modul. Tedaj sta
$$\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_S(S \otimes_R M, N)$$
izomorfni abelovi grupi.

*Dokaz.* Naj bo $\Phi\colon \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, N)$ preslikava, ki deluje po predpisu
$$\varphi \mapsto ((s \otimes m) \mapsto s\varphi(m)),$$
preslikava $\Psi\colon \mathrm{Hom}_S(S \otimes_R M, N) \to \mathrm{Hom}_R(M, N)$ pa po predpisu
$$\psi \mapsto (m \mapsto \psi(1 \otimes m)).$$
Ni težko preveriti, da sta to inverzni preslikavi. □

**Izrek 2.8.3.** Naj bo $R$ komutativen kolobar, $M$, $N$ in $P$ pa $R$-moduli. Tedaj je
$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

*Dokaz.* Preslikava
$$\varphi \mapsto (m \mapsto (n \mapsto \varphi(m \otimes n)))$$
je izomorfizem, saj je
$$\varphi \mapsto (m \otimes n \mapsto \varphi(m)(n))$$
njen inverz. □

## 2.9 Eksaktna zaporedja modulov

**Definicija 2.9.1.** *Zaporedje modulov* je zaporedje modulov $(M_n)_n$ in preslikav $(f_n)_n$, kjer je $f_n \colon M_n \to M_{n+1}$.

**Definicija 2.9.2.** Zaporedje modulov je *eksaktno* v $M_n$, če je $\operatorname{im} f_{n-1} = \ker f_n$. Zaporedje je eksaktno, če je eksaktno v vsakem modulu.

**Definicija 2.9.3.** Zaporedje modulov je *verižni kompleks*, če za vsako naravno število $n$ velja $\operatorname{im} f_n \subseteq \ker f_{n+1}$.

**Definicija 2.9.4.** Eksaktnim zaporedjem $R$-modulov oblike

$$0 \longrightarrow M \xrightarrow{\ f\ } N \xrightarrow{\ g\ } P \longrightarrow 0$$

pravimo *kratka eksaktna zaporedja.*

**Trditev 2.9.5.** Za kratko eksaktno zaporedje

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

so ekvivalentne naslednje trditve:

i) Obstaja homomorfizem $p \colon B \to A$, za katerega je $p \circ f = \mathrm{id}_A$.

ii) Obstaja homomorfizem $i \colon C \to B$, za katerega je $g \circ i = \mathrm{id}_C$.

iii) Obstajata homomorfizma $p \colon B \to A$ in $i \colon C \to B$, za katera je $p \circ f = \mathrm{id}_A$, $g \circ i = \mathrm{id}_C$ in $f \circ p + i \circ g = \mathrm{id}_B$.

*Dokaz.* Predpostavimo, da obstaja homomorfizem $p \colon B \to A$, za katerega je $p \circ f = \mathrm{id}_A$. Ker je $\operatorname{im} f \cap \ker p = \{0\}$ in za vsak $x \in B$ velja

$$x = (x - p \circ f(x)) + p \circ f(x),$$

je $B = \operatorname{im} f \oplus \ker p$. Sledi, da je $g|_{\ker p} \colon \ker p \to C$ izomorfizem. Preslikavo $i$ tako dobimo kot inverz tega izomorfizma.

Predpostavimo, da obstaja homomorfizem $i \colon C \to B$, za katerega je $g \circ i = \mathrm{id}_C$. Podobno kot zgoraj opazimo, da velja $B = \ker g \oplus \operatorname{im} s$. Sedaj lahko definiramo $p \colon B \to A$ tako, da za vsak $b \in B$ zapišemo $b = b_1 + b_2$, kjer je $b_1 \in \ker g = \operatorname{im} f$ in $b_2 \in \operatorname{im} s$. Sedaj preprosto vzamemo $p(b) = f^{-1}(b_1)$.

Prvi dve točki sta tako ekvivalentni. Pokazati moramo še, da implicirata tretjo točko, oziroma $i \circ g + f \circ p = \mathrm{id}_B$. Za $b \in B$ zapišimo $b = b_1 + b_2$, kjer je $b_1 \in \ker g$ in $b_2 \in \operatorname{im} i$. Tedaj je

$$f \circ p(b) + i \circ g(b) = f(f^{-1}(b_1)) + i \circ g(i(i^{-1}(b_2)) = b_1 + b_2 = b.$$

□

**Opomba 2.9.5.1.** Če veljajo ti pogoji, sledi $B \cong A \oplus C$. Pravimo, da je zaporedje *razcepno eksaktno.* Velja tudi obratno – če za $f \colon A \to B$ vzamemo inkluzijo, za $g \colon B \to C$ pa projekcijo, tvorijo moduli $A$, $B$ in $C$ razcepno eksaktno zaporedje.

**Trditev 2.9.6.** Če je v kratkem eksaktnem zaporedju $R$-modulov

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

$C$ prost, je zaporedje razcepno.

*Dokaz.* Naj bo $\{c_\lambda \mid \lambda \in \Lambda\}$ baza za $C$. Po aksiomu izbire lahko za vsak $c_\lambda$ izberemo $b_\lambda \in g^{-1}(c_\lambda)$ in definiramo
$$i(c_\lambda) = b_\lambda.$$
□

**Trditev 2.9.7.** Če je v kratkem eksaktnem zaporedju $R$-modulov

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

$C$ projektiven, je zaporedje razcepno.

*Dokaz.* Ker je $g$ epimorfizem, je

$$B \cong C \oplus \ker g = C \oplus \operatorname{im} f \cong C \oplus A.$$
□

**Izrek 2.9.8** (Kratka lema o petih)**.** Denimo, da sta v diagramu $R$-modulov

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$

vrstici eksaktni in diagram komutira. Tedaj veljajo naslednje trditve:

i) Če sta $\alpha$ in $\gamma$ monomorfizma, je tudi $\gamma$ monomorfizem.

ii) Če sta $\alpha$ in $\gamma$ epimorfizma, je tudi $\gamma$ epimorfizem.

iii) Če sta $\alpha$ in $\gamma$ izomorfizma, je tudi $\gamma$ izomorfizem.

*Dokaz.*

i) Naj bo $b \in B$ ničla $\beta$. Tedaj je

$$0 = g' \circ \beta(b) = \gamma \circ g(b).$$

Ker je $\gamma$ monomorfizem, sledi $g(b) = 0$. Sledi, da je $b \in \ker g = \operatorname{im} f$, zato lahko pišemo $b = f(a)$. Opazimo še, da je

$$0 = \beta \circ f(a) = f' \circ \alpha(a).$$

Ker sta tako $f'$ kot $\alpha$ monomorfizma, je tak tudi njun kompozitum, zato je $a = 0$ in posledično $b = 0$.

ii) Naj bo $b \in B'$. Ker sta $g$ in $\gamma$ epimorfizma, obstaja tak $b_2 \in B$, da je $\gamma \circ g(b_2) = g'(b)$. Opazimo, da je $g'(b - \beta(b_2)) = 0$, zato je $b - \beta(b_2) \in \ker g' = \operatorname{im} f$. Ker je $\alpha$ epimorfizem, obstaja tak $a \in A$, da je $b - \beta(b_2) = \alpha \circ f'(a)$. Naj bo $b_1 = f(a)$. Dobimo
$$\beta(b_1 + b_2) = \beta(f(a)) + \beta(b_2) = \alpha(f'(a)) + \beta(b_2) = b.$$

iii) Sledi iz prvih dveh točk. □

# 3 Teorija kategorij

*»Ups, niste videli…«*
– prof. dr. Primož Moravec

## 3.1 Definicija, izomorfizmi, začetni in končni objekti

14. april 2023

**Definicija 3.1.1.** *Kategorija* $\underline{\mathcal{C}}$ je struktura, ki ima

- razred objektov $\mathrm{Ob}\,\underline{\mathcal{C}}$,
- za vsaka $A, B \in \mathrm{Ob}\,\underline{\mathcal{C}}$ množico morfizmov $\underline{\mathcal{C}}(A, B)$,
- operacijo komponiranja $\circ \colon \underline{\mathcal{C}}(A, B) \times \underline{\mathcal{C}}(B, C) \to \underline{\mathcal{C}}(A, C)$, pri čemer je komponiranje asociativno in unitalno.[3]

**Definicija 3.1.2.** Naj bo $\underline{\mathcal{C}}$ kategorija in $f \in \underline{\mathcal{C}}(A, B)$ morfizem. $f$ je *izomorfizem*, če ima inverz $g \in \underline{\mathcal{C}}(B, A)$, za katerega je

$$f \circ g = 1_B \quad \text{in} \quad g \circ f = 1_A.$$

Objekta $A$ in $B$ kategorije $\underline{\mathcal{C}}$ sta *izomorfna*, če v $\underline{\mathcal{C}}(A, B)$ obstaja izomorfizem. Pišemo $A \cong B$.

**Opomba 3.1.2.1.** Inverz je enolično določen.

**Definicija 3.1.3.** Morfizem $f \in \underline{\mathcal{C}}(A, B)$ je

i) *prerez*, če ima levi inverz,

ii) *retrakt*, če ima desni inverz,

iii) *monomorfizem*, če za vsaka $g, h \in \underline{\mathcal{C}}(C, A)$ iz

$$f \circ g = f \circ h$$

sledi $g = h$,

iv) *epimorfizem*, če za vsaka $g, h \in \underline{\mathcal{C}}(B, C)$ iz

$$g \circ f = h \circ f$$

sledi $g = h$.

**Definicija 3.1.4.** Objekt $Z \in \mathrm{Ob}\,\underline{\mathcal{C}}$ je *začeten objekt*, če za vsak objekt $C \in \mathrm{Ob}\,\underline{\mathcal{C}}$ obstaja natanko en morfizem v $\underline{\mathcal{C}}(Z, C)$.

Objekt $K \in \mathrm{Ob}\,\underline{\mathcal{C}}$ je končen objekt, če za vsak objekt $C \in \mathrm{Ob}\,\underline{\mathcal{C}}$ obstaja natanko en morfizem v $\underline{\mathcal{C}}(C, K)$.

**Trditev 3.1.5.** Poljubna začetna objekta v $\underline{\mathcal{C}}$ sta izomorfna.

*Dokaz.* Naj bosta $Z_1$ in $Z_2$ začetna objekta. Sledi, da je $1_{Z_1}$ edini morfizem v $\underline{\mathcal{C}}(Z_1, Z_1)$. Obstajata še morfizma $f \in \underline{\mathcal{C}}(Z_1, Z_2)$ in $g \in \underline{\mathcal{C}}(Z_2, Z_1)$. Ker je $g \circ f \in \underline{\mathcal{C}}(Z_1, Z_1)$, je $g \circ f = 1_{Z_1}$. Simetrično dobimo $f \circ g = 1_{Z_2}$. $\square$

[3] Za vsak $A \in \underline{\mathcal{C}}$ obstaja $1_A \in \underline{\mathcal{C}}(A, A)$, za katerega je $f \circ 1_A = f$ in $1_A \circ g$.

**Opomba 3.1.5.1.** Enako velja za končne objekte.

**Definicija 3.1.6.** Naj bo $\underline{\mathcal{C}}$ kategorija. *Dualna kategorija* $\mathcal{C}^{\mathsf{op}}$ kategorije $\underline{\mathcal{C}}$ je kategorija, v kateri je

i) $\operatorname{Ob}\underline{\mathcal{C}}^{\mathsf{op}} = \operatorname{Ob}\underline{\mathcal{C}}$,

ii) $\underline{\mathcal{C}}^{\mathsf{op}}(A, B) = \underline{\mathcal{C}}(B, A)$ in

iii) za komponiranje $*$ velja $g * f = f \circ g$.[4]

**Opomba 3.1.6.1.** Morfizem $f$ je monomorfizem v $\underline{\mathcal{C}}$ natanko tedaj, ko je $f$ epimorfizem v $\underline{\mathcal{C}}^{\mathsf{op}}$.

**Opomba 3.1.6.2.** Objekt $Z$ je začetni objekt v $\underline{\mathcal{C}}$ natanko tedaj, ko je končen objekt v $\underline{\mathcal{C}}^{\mathsf{op}}$.

[4] Tu $\circ$ označuje komponiranje v $\underline{\mathcal{C}}$.

## 3.2 Funktorji in naravne transformacije

21. april 2023

**Definicija 3.2.1.** Naj bosta $\underline{\mathcal{C}}$ in $\underline{\mathcal{D}}$ kategoriji. *Funktor* $F$ iz $\underline{\mathcal{C}}$ v $\underline{\mathcal{D}}$ je predpis, sestavljen iz

i) predpisa $\operatorname{Ob}\underline{\mathcal{C}} \to \operatorname{Ob}\underline{\mathcal{D}}$, $A \mapsto F(A)$,

ii) za vsaka objekta $A$ in $B$ iz $\underline{\mathcal{C}}$ imamo predpis $\underline{\mathcal{C}}(A, B) \to \underline{\mathcal{D}}(F(A), F(B))$, $f \mapsto F(f)$.

Pri tem zahtevamo $F(1_A) = 1_{F(A)}$ za vsak $A \in \operatorname{Ob}\underline{\mathcal{C}}$ in $F(f \circ g) = F(f) \circ F(g)$ za vse smiselne $f$ in $g$.

**Definicija 3.2.2.** Naj bosta $\underline{\mathcal{C}}$ in $\underline{\mathcal{D}}$ kategoriji. *Kontravariantni funktor* (*kofunktor*) $F \colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ je predpis, sestavljen iz

i) predpisa $\operatorname{Ob}\underline{\mathcal{C}} \to \operatorname{Ob}\underline{\mathcal{D}}$, $A \mapsto F(A)$,

ii) za vsaka objekta $A$ in $B$ iz $\underline{\mathcal{C}}$ imamo predpis $\underline{\mathcal{C}}(A, B) \to \underline{\mathcal{D}}(F(B), F(A))$, $f \mapsto F(f)$.

Pri tem zahtevamo $F(1_A) = 1_{F(A)}$ za vsak $A \in \operatorname{Ob}\underline{\mathcal{C}}$ in $F(f \circ g) = F(g) \circ F(f)$ za vse smiselne $f$ in $g$.

**Opomba 3.2.2.1.** Kofunktor $F \colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ je funktor $F \colon \underline{\mathcal{C}}^{\mathsf{op}} \to \underline{\mathcal{D}}$.

**Opomba 3.2.2.2.** Funktorji ohranjajo izomorfizme, prereze in retrakte, ne pa nujno monomorfizmov, epimorfizmov, začetnih in končnih objektov.

**Definicija 3.2.3.** Naj bosta $F, G \colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ funktorja. *Naravna transformacija* $\mu \colon F \to G$ je nabor morfizmov $\mu_C \colon F(C) \to G(C)$ za $C \in \underline{\mathcal{C}}$, za katere diagram

$$\begin{tikzcd}
F(C) \arrow[r, "F(f)"] \arrow[d, "\mu_C"'] & F(D) \arrow[d, "\mu_D"] \\
G(C) \arrow[r, "G(f)"'] & G(D)
\end{tikzcd}$$

komutira za vse $f \in \underline{\mathcal{C}}(C, D)$.

## 3.3 Univerzalne konstrukcije

**Definicija 3.3.1.** Naj bosta $A$ in $B$ objekta kategorije $\underline{\mathcal{C}}$. *Produkt* $A$ in $B$ je tak objekt $C$ z morfizmoma $p\colon C \to A$ in $q\colon C \to B$, da za vsak $X \in \operatorname{Ob}\underline{\mathcal{C}}$ in morfizma $f\colon X \to A$ ter $g\colon X \to B$ obstaja natanko en morfizem $h\colon X \to C$, da velja $p \circ h = f$ in $q \circ h = g$.

$$\begin{tikzcd} A & C \arrow[l, "p"'] \arrow[r, "q"] & B \\ & X \arrow[ul, "f"] \arrow[u, dashed, "h"] \arrow[ur, "g"'] & \end{tikzcd}$$

**Trditev 3.3.2.** Naj bosta $A$ in $B$ objekta kategorije $\underline{\mathcal{C}}$ s produktoma

$$A \xleftarrow{p} C \xrightarrow{q} B$$

in

$$A \xleftarrow{p'} C' \xrightarrow{q'} B.$$

Tedaj je $C \cong C'$.

*Dokaz.* Obstaja morfizem $h\colon C' \to C$, za katerega je $p \circ h = p'$ in $q \circ h = q'$. Podobno obstaja morfizem $h'\colon C \to C'$, za katerega je $p' \circ h' = p$ in $q' \circ h' = q$. Sledi, da je

$$p \circ (h \circ h') = p \circ \mathrm{id}_C \quad \text{in} \quad q \circ (h \circ h') = q \circ \mathrm{id}_C$$

Po enoličnosti dobimo $h \circ h' = \mathrm{id}_C$ in simetrično $h' \circ h = \mathrm{id}_{C'}$. □

**Opomba 3.3.2.1.** Produkte v kategoriji $\underline{\mathcal{C}}$ lahko definiramo tudi tako, da za fiksna $A, B \in \operatorname{Ob}\underline{\mathcal{C}}$ definiramo kategorijo $\underline{\mathcal{D}}$, ki ima za objekte diagrame

$$A \xleftarrow{p} C \xrightarrow{q} B$$

in morfizme definirane na naraven način. Produkt $A$ in $B$ je končen objekt v kategoriji $\underline{\mathcal{D}}$.

**Definicija 3.3.3.** Naj bosta $A$ in $B$ objekta kategorije $\underline{\mathcal{C}}$. *Koprodukt* $A$ in $B$ je produkt $A$ in $B$ v $\underline{\mathcal{C}}^{\mathsf{op}}$.

**Opomba 3.3.3.1.** Ekvivalentno, koprodukt $A$ in $B$ je tak objekt $C$ z morfizmoma $p\colon A \to C$ in $q\colon B \to C$, da za vsak $X \in \operatorname{Ob}\underline{\mathcal{C}}$ in morfizma $f\colon A \to X$ ter $g\colon B \to X$ obstaja natanko en morfizem $h\colon C \to X$, da velja $h \circ p = f$ in $h \circ q = g$.

$$\begin{tikzcd} A \arrow[r, "p"] \arrow[dr, "f"'] & C \arrow[d, dashed, "h"] & B \arrow[l, "q"'] \arrow[dl, "g"] \\ & X & \end{tikzcd}$$

**Definicija 3.3.4.** Kategorija $\underline{\mathcal{C}}$ je *konkretna*, če imajo njeni objekti strukturo množice, morfizmi pa so preslikave.

**Definicija 3.3.5.** Naj bo $\underline{\mathcal{C}}$ konkretna kategorija in $X$ množica. *Prost objekt* v $\underline{\mathcal{C}}$ nad množico $X$ je objekt $F_X$ skupaj s strukturno preslikavo $\iota\colon X \to F_X$, za katera velja, da za vsak objekt $C \in \operatorname{Ob}\underline{\mathcal{C}}$ in preslikavo $j\colon X \to C$ obstaja natanko en morfizem $f\colon F_x \to C$, da je $f \circ \iota = j$.

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[d, "\iota"'] & C \\ F_X \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

**Trditev 3.3.6.** Prost objekt je enolično določen do izomorfizma natančno.

*Dokaz.* Naj bosta $F$ in $F'$ s preslikavama $\iota\colon X \to F$ in $\iota\colon X \to F'$ prosta objekta. Sledi, da obstaja preslikava $f\colon F \to F'$, za katero je $f \circ \iota = \iota'$, in preslikava $f'\colon F' \to F$, za katero je $f' \circ \iota' = \iota$. Sledi, da je

$$(f' \circ f) \circ \iota = \mathrm{id} \circ \iota,$$

zato je zaradi enoličnosti $f' \circ f = \mathrm{id}$. Simetrično dobimo $f \circ f' = \mathrm{id}$. □

**Opomba 3.3.6.1.** Proste objekte v kategoriji $\underline{\mathcal{C}}$ lahko definiramo tudi tako, da definiramo kategorijo $\underline{\mathcal{D}}$, ki ima za objekte diagrame

$$X \xrightarrow{\iota} A$$

in morfizme definirane na naraven način. Prost objekt je začetni objekt v kategoriji $\underline{\mathcal{D}}$.

## 3.4 Izomorfizem in ekvivalenca kategorij

5. maj 2023

**Definicija 3.4.1.** Funktor $F\colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ je *izomorfizem kategorij*, če obstaja tak funktor $G\colon \underline{\mathcal{D}} \to \underline{\mathcal{C}}$, da je
$$F \circ G = 1_{\underline{\mathcal{D}}} \quad \text{in} \quad G \circ F = 1_{\underline{\mathcal{C}}}.$$
Pišemo $\underline{\mathcal{C}} \cong \underline{\mathcal{D}}$.

**Definicija 3.4.2.** Naj bosta $F, G\colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ funktorja in $\mu\colon F \to G$ naravna transformacija. Funktorja $F$ in $G$ sta *naravno izomorfna*, če so vsi morfizmi $\mu_C\colon F(C) \to G(C)$ izomorfizmi.

**Definicija 3.4.3.** Kategorija $\underline{\mathcal{C}}$ je *majhna*, če sta $\operatorname{Ob}\underline{\mathcal{C}}$ in razred vseh morfizmov množici.

**Opomba 3.4.3.1.** Naj bo $\underline{\mathcal{C}}$ majhna kategorija in $\underline{\mathcal{D}}$ poljubna kategorija. Naj bo $\underline{\mathcal{D}}^{\underline{\mathcal{C}}}$ kategorija, katere objekti so funktorji $F\colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$, morfizmi med $F$ in $G$ pa naravne transformacije. Tedaj sta $F$ in $G$ naravno izomorfna natanko tedaj, ko sta izomorfna kot objekta $\underline{\mathcal{D}}^{\underline{\mathcal{C}}}$.

**Definicija 3.4.4.** Kategoriji $\underline{\mathcal{C}}$ in $\underline{\mathcal{D}}$ sta *ekvivalentni*, če obstajata taka funktorja $F\colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ in $G\colon \underline{\mathcal{D}} \to \underline{\mathcal{C}}$, da je $F \circ G$ naravno izomorfen $1_{\underline{\mathcal{D}}}$, $G \circ F$ pa naravno izomorfen $1_{\underline{\mathcal{C}}}$.

**Definicija 3.4.5.** Naj bo $F\colon \underline{\mathcal{C}} \to \underline{\mathcal{D}}$ funktor.

i) $F$ je *zvest*, če je injektiven na morfizmih – za vsaka $X, Y \in \operatorname{Ob}\underline{\mathcal{C}}$ je $F_{X,Y}\colon \underline{\mathcal{C}}(X,Y) \to \underline{\mathcal{D}}(F(X), F(Y))$ injektivna.

ii) $F$ je *poln*, če je surjektiven na morfizmih.

iii) $F$ je *gost*, če za vsak $Y \in \operatorname{Ob}\underline{\mathcal{D}}$ obstaja tak $X \in \operatorname{Ob}\underline{\mathcal{C}}$, da je $F(X) \cong Y$.

**Opomba 3.4.5.1.** Pravimo, da je funktor $F$ *ekvivalenca*, če je zvest, gost in poln.

**Definicija 3.4.6.** Naj bo $\underline{\mathcal{C}}$ majhna kategorija. Definirajmo funktor $\mathcal{Y}\colon \underline{\mathcal{C}} \to \underline{\mathrm{Set}}^{\underline{\mathcal{C}}^{\mathsf{op}}}$ na naslednji način:

i) Vsak Objekt $A$ preslikamo v funktor $F_A\colon \underline{\mathcal{C}}^{\mathsf{op}} \to \underline{\mathrm{Set}}$, ki deluje po predpisu $F_A(X) = \underline{\mathcal{C}}(X, A)$ na objektih in $F_A(f) = (\varphi \mapsto \varphi \circ f)$ na morfizmih.

ii) Vsak morfizem $f\colon A \to B$ preslikamo v naravno transformacijo $\mathcal{Y}(f)\colon F_A \to F_B$, z naborom morfizmov $\mathcal{Y}(f)_X\colon \underline{\mathcal{C}}(X, A) \to \underline{\mathcal{C}}(X, B)$ s predpisom $\mathcal{Y}(f)_X(\varphi) = f \circ \varphi$.

**Izrek 3.4.7** (Lema Yonede)**.** Naj bo $\underline{\mathcal{C}}$ majhna kategorija. Tedaj je funktor $\mathcal{Y}\colon \underline{\mathcal{C}} \to \underline{\mathrm{Set}}^{\underline{\mathcal{C}}^{\mathsf{op}}}$ zvest in poln.

*Dokaz.* Naj bosta $A$ in $B$ objekta kategorije $\underline{\mathcal{C}}$. Denimo, da za $f, g\colon A \to B$ velja $\mathcal{Y}(f) = \mathcal{Y}(g)$. Sledi, da je
$$f = f \circ 1_A = \mathcal{Y}(f)_A(1_A) = \mathcal{Y}(g)_A(1_A) = g \circ 1_A = g.$$
Sledi, da je $F$ zvest.

Pokažimo še polnost. Naj bo $\eta\colon F_A \to F_B$ naravna transformacija. Naj bo $e = \eta_A(1_A) \in \underline{\mathcal{C}}(A, B)$. Pokažimo, da je $\eta = \mathcal{Y}(e)$. Za poljuben morfizem $f\colon C \to A$ vemo, da komutira naslednji diagram:

$$\begin{tikzcd}
\underline{\mathcal{C}}(A, A) \arrow[r, "F_A(f)"] \arrow[d, "\eta_A"'] & \underline{\mathcal{C}}(C, A) \arrow[d, "\eta_C"] \\
\underline{\mathcal{C}}(A, B) \arrow[r, "F_B(f)"'] & \underline{\mathcal{C}}(C, B)
\end{tikzcd}$$

Opazimo, da je

$$F_B(f) \circ \eta_A(1_A) = F_B(f)(e) = e \circ f = \mathcal{Y}(e)_C(f),$$

po drugi strani pa je zaradi komutativnega diagrama

$$F_B(f) \circ \eta_A(1_A) = \eta_C \circ F_A(f)(1_A) = \eta_C(f).$$ □

**Opomba 3.4.7.1.** Ekvivalentno, vsako majhno kategorijo $\underline{\mathcal{C}}$ lahko vložimo v kategorijo kovariantnih funktorjev $\underline{\mathcal{C}} \to \underline{\text{Set}}$.

**Posledica 3.4.7.2** (Cayleyev izrek)**.** Vsaka grupa $G$ je izomorfna podgrupi grupe $\text{Sym}_G$.

*Dokaz.* Grupi $G$ priredimo kategorijo $\underline{G}$, katere element je $G$, morfizmi pa njeni elementi. Po lemi Yonede je preslikava $x \mapsto \mathcal{Y}(x)$ injektivna. Za preslikavo $\rho\colon G \to G^G$, ki deluje po predpisu $\rho(x) = \mathcal{Y}(x)_G$, zato velja $\rho(x) \neq \rho(y)$ za vse $x \neq y$. Injektivna je torej tudi preslikava $\rho$. Ni težko preveriti, da je $\rho\colon G \to \text{Sym}_G$ homomorfizem grup. □

# 4 Teorija upodobitev

*»Pa kemiki to uporabljajo ko opazujejo strukture kristalov. Samo da oni tega ne znajo.«*
– prof. dr. Primož Moravec

## 4.1 Upodobitve

**Definicija 4.1.1.** Naj bo $R$ komutativen kolobar z enoto. $R$-modul $A$ je *$R$-algebra*, če je kolobar in za vse $r \in R$ ter $a_1, a_2 \in A$ velja

$$r(a_1a_2) = (ra_1)a_2 = a_1(ra_2).$$

**Definicija 4.1.2.** Naj bo $A$ $R$-algebra. *Upodobitev* algebre $A$ je homomorfizem $R$-algeber $\rho\colon A \to \mathrm{End}_R(V)$, kjer je $V$ $R$-modul.

**Opomba 4.1.2.1.** Če je $V$ prost, lahko pišemo $\rho\colon A \to M_n(R)$. Številu $n$ pravimo *stopnja upodobitve.*

**Opomba 4.1.2.2.** Na vsako upodobitev $\rho$ $R$-algebre $A$ lahko gledamo kot $R$-modul $V$, ki je $A$-modul. Definiramo lahko namreč $a \cdot v = \rho(a)v$. Velja tudi obratno – $a \mapsto (v \mapsto av)$ je upodobitev $R$-algebre $A$.

**Definicija 4.1.3.** Naj bo $G$ grupa. *Grupna algebra $RG$* je prosti $R$-modul nad množico $G$ z množenjem

$$\left(\sum_{g\in G} \lambda_g g\right) \cdot \left(\sum_{h\in G} \mu_h h\right) = \sum_{g\in G} \left(\sum_{hk=g} \lambda_h \mu_k\right) g.$$

**Definicija 4.1.4.** Naj bo $G$ grupa. *upodobitev grupe $G$* nad $R$ je homomorfizem $R$-algeber $\rho\colon RG \to \mathrm{End}_R(V)$, kjer je $V$ $R$-modul.

**Trditev 4.1.5.** Zožitev $\rho|_G$ je homomorfizem grup $G$ in $\mathrm{GL}_R(V)$.

*Dokaz.* The proof is obvious and need not be mentioned. □

**Opomba 4.1.5.1.** Vsak homomorfizem grup $G$ in $\mathrm{GL}_R(V)$ lahko razširimo do homomorfizma $R$-algeber $RG$ in $\mathrm{End}_R(V)$. Tako lahko ekvivalentno definiramo upodobitev grupe $G$ nad $R$ kot homomorfizem grup $\rho\colon G \to \mathrm{GL}_R(V)$.

**Definicija 4.1.6.** Naj bo $\rho\colon G \to \mathrm{GL}_R(V)$ upodobitev. Podmodul $W$ $R$-modula $V$ je *$G$-invarianten*, če za vsaka $g \in G$ in $w \in W$ velja $\rho(g)w \in W$.

**Opomba 4.1.6.1.** Ekvivalentno je $W$ podmodul $RG$-modula $V$.

**Definicija 4.1.7.** Naj bo $W \le V$ $G$-invarianten podmodul. Upodobitvi $\rho_W\colon G \to \mathrm{GL}_R(W)$ s predpisom $g \mapsto (w \mapsto \rho(g)w)$ pravimo *podupodobitev* upodobitve $\rho$.

**Definicija 4.1.8.** Upodobitvi $\rho_1\colon G \to \mathrm{GL}_R(V_1)$ in $\rho_2\colon G \to \mathrm{GL}_R(V_2)$ sta *ekvivalentni*, če sta $V_1$ in $V_2$ izomorfna kot $RG$-modula.

**Opomba 4.1.8.1.** Ekvivalentno obstaja izomorfizem $T\colon V_1 \to V_2$ $R$-modulov, za katerega je $T \circ \rho_1(g) = \rho_2(g) \circ T$ za vse $g \in G$.

**Definicija 4.1.9.** *Direktna vsota* upodobitev $\rho_1 \colon G \to \mathrm{GL}_R(V_1)$ in $\rho_2 \colon G \to \mathrm{GL}_R(V_2)$ je upodobitev $\rho_1 \oplus \rho_2 \colon G \to \mathrm{GL}_R(V_1 \oplus V_2)$ s predpisom

$$g \mapsto ((v_1, v_2) \mapsto (\rho_1(g)v_1, \rho_2(g)v_2)) .$$

**Definicija 4.1.10.** *Tenzorski produkt* upodobitev $\rho_1 \colon G \to \mathrm{GL}_R(V_1)$ in $\rho_2 \colon G \to \mathrm{GL}_R(V_2)$ je upodobitev $\rho_1 \otimes \rho_2 \colon G \to \mathrm{GL}_R(V_1 \otimes_R V_2)$ s predpisom

$$g \mapsto (v_1 \otimes v_2 \mapsto \rho_1(g)v_1 \otimes \rho_2(g)v_2) .$$

## 4.2 Polenostavni moduli

**Definicija 4.2.1.** Naj bo $V$ $A$-modul.

i) Modul $V$ je *enostaven* (nerazcepen), če sta edina njegova $A$-podmodula $\{0\}$ in $V$.

ii) Modul $V$ je *polenostaven* (povsem razcepen), če je direktna vsota enostavnih $A$-podmodulov.

**Izrek 4.2.2** (Maschke)**.** Naj bo $G$ končna grupa in $F$ polje, za katerega $\operatorname{char} F \nmid |G|$. Naj bo $\rho\colon G \to \mathrm{GL}_F(V)$ upodobitev grupe $G$ nad $F$ za končnorazsežen vektorski prostor $V$ in $W$ $G$-invarianten podprostor v $V$. Potem obstaja $G$-invarianten podprostor $U$ v $V$, za katerega je $V = W \oplus U$.

*Dokaz.* Naj bo $\pi\colon V \to W$ projektor. Definirajmo preslikavo $\pi'\colon V \to V$ s predpisom

$$\pi' = \frac{1}{|G|} \sum_{g \in G} \rho(g)\pi\rho(g)^{-1}.$$

Tudi $\pi'$ je projektor na $W$. Za $w \in W$ namreč velja

$$\pi' w = \frac{1}{|G|} \sum_{g \in G} \rho(g)\pi\rho^{-1}(g)w = \frac{1}{|G|} \sum_{g \in G} \rho(g)\rho^{-1}(g)w = w,$$

saj je $\rho^{-1}(g)w \in W$, poleg tega pa je seveda $\operatorname{im}\pi' = W$. Sledi, da je $V = W \oplus \ker \pi'$. Dovolj je tako pokazati, da je $\ker \pi'$ $G$-invarianten. Zadošča torej, da je $\pi'\colon V \to W$ homomorfizem $G$-modulov. Velja pa

$$\begin{aligned}
\pi'(g \cdot v) &= \frac{1}{|G|} \sum_{g \in G} \rho(g)\pi\rho^{-1}(g)\rho(h)v \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(h)\rho(h^{-1}g)\pi\rho(g^{-1}h)v \\
&= \frac{1}{|G|}\rho(h) \sum_{g \in G} \rho(g)\pi\rho^{-1}(g)v \\
&= h \cdot (\pi' v).
\end{aligned}$$

□

**Posledica 4.2.2.1.** Naj bo $F$ polje in $G$ končna grupa, za katero $\operatorname{char} F \nmid |G|$. Potem je vsak končnorazsežen $FG$-modul polenostaven.

**Lema 4.2.3.** Naj bo $U = S_1 + \cdots + S_n$ $A$-modul, pri čemer so $S_i$ enostavni $A$-moduli. Naj bo $V$ podmodul v $U$. Potem obstaja podmnožica $I \subseteq \{i \in \mathbb{N} \mid i \leq n\}$, za katero je

$$U = V \oplus \bigoplus_{i \in I} S_i.$$

*Dokaz.* Naj bo $I$ maksimalna množica, za katero je

$$W = V \oplus \bigoplus_{i \in I} S_i$$

direktna vsota. Če obstaja $j$, za katerega je $S_j \not\subseteq W$, zaradi enostavnosti sledi $S_j \cap W = \{0\}$, kar je v prostislovju z maksimalnostjo množice $I$. Sledi, da je $W = U$. □

**Definicija 4.2.4.** Naj bo $U$ $A$-modul. *Kompozicijska vrsta* modula $U$ je zaporedje

$$\{0\} = U_0 \leq U_1 \leq \cdots \leq U_n = U,$$

pri čemer je za vsak $i$ modul $U_i$ maksimalen podmodul v $U_{i+1}$. Modulom, za katere obstaja končna kompozicijska vrsta, pravimo *moduli s končno kompozicijsko dolžino.*

**Trditev 4.2.5.** Naj bo $U$ $A$-modul. Naslednje trditve so ekvivalentne:

i) $U$ je direktna vsota končno mnogo enostavnih podmodulov.

ii) $U$ je direktna vsota končno mnogo enostavnih $A$-modulov.

iii) $U$ ima končno kompozicijsko dolžino in vsak podmodul v $U$ je direktni sumand $U$-ja.

Če drži katera od zgornjih trditev, velja tudi za vse podmodule in kvociente $U$-ja.

*Dokaz.* Prvi trditvi sta ekvivalentni po lemi 4.2.3. Ti trditvi po isti lemi implicirata tretjo.

Predpostavimo, da ima $U$ končno kompozicijsko dolžino in da je vsak podmodul v $U$ njegov direktni sumand. Opazimo, da to velja tudi za vse podmodule $V \leq U$, saj lahko za $W \leq V$ zapišemo $V = W \oplus (X \cap V)$. Nadaljujemo z indukcijo po dolžini kompozicijske vrste.

Če je dolžina vrste enaka 1, je $U$ enostaven, zato velja prva trditev. Če je dolžina vrste daljša, lahko zapišemo $U = V \oplus W$ in uporabimo indukcijsko predpostavko na $V$ ter $W$.

Dokažimo še dedovanje na podmodule in kvociente. Na podmodule se deduje tretja trditev. Za vsak kvocient ${}^{U}\!/_{V}$ lahko po tretji trditvi zapišemo $U = V \oplus W$. Ker je $W$ podmodul v $U$, zadošča prvi trditvi. Sledi, da ji zadošča tudi ${}^{U}\!/_{V} \cong W$. $\square$

## 4.3 Artin-Wedderburnov izrek

**Izrek 4.3.1** (Schurova lema)**.** Naj bo $A$ končnorazsežna algebra nad poljem $F$. Naj bosta $S_1$ in $S_2$ enostavna $A$-modula.

i) Če je $S_1 \not\cong S_2$, je $\mathrm{Hom}_A(S_1, S_2) = \{0\}$.

ii) $\mathrm{End}_A(S_1)$ je obseg.

iii) Če je $F$ algebraično zaprto, je $\mathrm{End}_A(S_1) \cong F$.

*Dokaz.*

i) Naj bo $\varphi\colon S_1 \to S_2$ neničeln homomorfizem $A$-modulov. Ker je $\operatorname{im}\varphi$ neničeln podmodul v $S_2$, je $\operatorname{im}\varphi = S_2$. Ker je $\ker\varphi \neq S_1$, je $\ker\varphi = \{0\}$. Sledi, da je $\varphi$ izomorfizem.

ii) Vsi neničelni homomorfizmi so po istem argumentu kot v prvi točki izomorfizmi.

iii) Naj bo $\lambda \in F$ lastna vrednost endomorfizma $\varphi$. Sledi, da $\varphi = \lambda I$ ni injektiven, zato je $\varphi = \lambda I$. □

**Definicija 4.3.2.** Za kolobar $A$ definiramo *nasprotni kolobar* $A^{\mathsf{op}}$ kot kolobar, katerega elementi so elementi $A$, seštevanje sovpada s seštevanjem v $A$, množenje pa je definirano z $a \cdot b = ba$.

**Lema 4.3.3.** Naj bo $A$ kolobar z enoto. Če na $A$ gledamo kot na $A$-modul, velja $\mathrm{End}_A(A) \cong A^{\mathsf{op}}$.

*Dokaz.* Preslikavi $\varphi \mapsto \varphi(1)$ in $x \mapsto (a \mapsto ax)$ sta inverzna homomorfizma. □

**Definicija 4.3.4.** Naj bo $A$ kolobar z enoto. $A$ je *polenostaven*, če so vsi $A$-moduli polenostavni.

**Lema 4.3.5.** Če je

$$U = \bigoplus_{i=1}^{r} U_i$$

$A$-modul, je $\mathrm{End}_A(U)$ izomorfen algebri $r \times r$ matrik $[\varphi_{i,j}]$, kjer je $\varphi_{i,j} \in \mathrm{Hom}_A(U_i, U_j)$.

*Dokaz.* Ni težko videti, da so endomorfizmi $\varphi \in \mathrm{End}_A(U)$ v bijektivni korespondenci z zgornjimi matrikami. Kratek izračun pokaže, da velja

$$\varphi \circ \psi(v_j) = \sum_{i=1}^{r} (\varphi \circ \psi)_{i,j}(v_j).$$

□

**Izrek 4.3.6** (Artin-Wedderburn)**.** Naj bo $A$ končnorazsežna algebra nad poljem $F$, za katero velja, da je vsak končnogeneriran $A$-modul polenostaven. Potem je $A$ direktna vsota matričnih algeber nad obsegi. Natančneje, če je

$$A = \bigoplus_{i=1}^{k} S_i^{n_i},$$

kjer so $S_i$ paroma neizomorfni enostavni $A$-moduli, je $A$ kot $F$-algebra izomorfna

$$\bigoplus_{i=1}^{k} M_{n_i}(D_i),$$

kjer je $D_i = \mathrm{End}_A(S_i)^{\mathsf{op}}$. Če je $F$ algebraično zaprto, je $D_i = F$.

*Dokaz.* Po Schurovi lemi je $\mathrm{Hom}_A\left(S_j^{n_j}, S_i^{n_i}\right) = \{0\}$ za vse $i \neq j$. Po lemi sledi, da je $\mathrm{End}_A(U)$ izomorfen algebri $n \times n$ matrik, ki pa so bločno diagonalne. Posebej, velja

$$\mathrm{End}_A(A) \cong \bigoplus_{i=1}^{k} \mathrm{End}_A\left(S_i^{n_i}\right).$$

Po zgornji lemi pa je $\mathrm{End}_A\left(S_i^{n_i}\right)$ izomorfna algebri $n_i \times n_i$ matrik z elementi iz $\mathrm{End}_A(S_i) = D_i^{\mathsf{op}}$. Velja torej

$$A^{\mathsf{op}} \cong \mathrm{End}_A(A) \cong \bigoplus_{i=1}^{k} M_{n_i}\left(D_i^{\mathsf{op}}\right).$$

Ker je $M_{n_i}\left(D_i^{\mathsf{op}}\right)^{\mathsf{op}} \cong M_{n_i}(D_i)$, je izrek dokazan. Enakost $D_i = F$ v primeru algebraične zaprtosti sledi iz Schurove leme. □

**Opomba 4.3.6.1.** Vsaka direktna vsota matričnih algeber je polenostavna.

**Opomba 4.3.6.2.** Algebra $M_n(D)$ je enostavna.

**Opomba 4.3.6.3.** Matrične algebre, ki nastopajo v razcepi, so enolično določene do izomorfizma natančno.

**Posledica 4.3.6.4.** Naj bo $A$ končnorazsežna $F$-algebra. Če je $A$ kot $A$-modul enak

$$A = \bigoplus_{i=1}^{r} S_i^{n_i},$$

kjer so $S_i$ paroma neizomorfni enostavni $A$-moduli, je $\{S_i \mid 1 \leq i \leq r\}$ množica vseh predstavnikov izomorfnih razredov enostavnih $A$-modulov. Če je $F$ algebraično zaprto, je $n_i = \dim_F S_i$ in

$$\dim_F A = \sum_{i=1}^{r} n_i^2.$$

*Dokaz.* Najprej opazimo, da je vsak enostaven $A$-modul izomorfen ${}^{A}/_{I}$. Res, naj bo $u \in U$ neničeln element modula. Ker je $Au$ netrivialen podmodul v $U$, je $Au = U$. Po izreku o izomorfizmu sledi ${}^{A}/_{\ker\varphi} \cong U$ za homomorfizem $\varphi \colon a \mapsto au$. Če $\ker\varphi$ ni maksimalen ideal, modul $U$ ni enostaven.

Za vsak enostaven $A$-modul $S$ tako sledi, da je kvocient modula

$$\bigoplus_{i=1}^{r} S_i^{n_i}.$$

Ker je kompozitum inkluzije $S_i \hookrightarrow A$ in kvocientne projekcije izomorfizem enostavnih modulov, sledi, da za nek $i$ velja $S \cong S_i$.

Naj bo sedaj $F$ algebraično zaprto. Po Schurovi lemi tako velja

$$A \cong \bigoplus_{i=1}^{r} M_{n_i}(F),$$

od koder sledi

$$\dim_F A = \sum_{i=1}^{r} n_i^2.$$

Preostane še dokaz enakosti $n_i = \dim_F S_i$. Pokažimo, da je $S_i^{n_i} \cong M_{n_i}(F)$.

Iz dokaza Artin-Wedderburnovega izreka vidimo, da za vsaka $s \in S_i^{n_i}$ in $t \in M_{n_j}(F)$ ob pogoju $i \neq j$ velja $st = 0$. Opazimo, da je $M_{n_i}(F) \cong {}^{A}/_{V}$, kjer je $V$ podmodul direktne vsote matričnih algeber, ki ga $M_{n_i}(F)$ anihilira. Kompozitum inkluzije $S_i^{n_i}$ v $A$ in kvocientne projekcije je tako surjektiven, zato je $\dim_F S_i^{n_i} \geq \dim_F M_{n_i}(F)$. Ker je

$$\dim_F A = \sum_{i=1}^{r} \dim_F S_i^{n_i},$$

sledi, da velja enakost. $\square$

**Posledica 4.3.6.5.** Naj bo $G$ končna grupa in $F$ polje, za katerega $\operatorname{char} F \nmid |G|$.

i) Kot kolobar je $FG$ izomorfen direktni vsoti matričnih algeber nad obsegi.

ii) Če je $F$ algebraično zaprto in je $S_1, \ldots, S_r$ kompleten nabor predstavnikov izomorfnih razredov enostavnih $FG$-modulov, za $d_i = \dim_F S_i$ velja, da je $d_i$ večkratnost, s katero $S_i$ nastopa v razcepu $FG$-modula $FG$ in je

$$|G| = \sum_{i=1}^{r} d_i^2.$$

## 4.4 Karakterji

**Definicija 4.4.1.** Naj bo $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ končnorazsežna upodobitev končne grupe $G$. Preslikavi $\chi\colon G \to \mathbb{C}$ s predpisom

$$\chi(g) = \operatorname{tr} \rho(g)$$

pravimo *karakter* upodobitve $\rho$.

**Trditev 4.4.2.** Naj bo $\chi$ karakter upodobitve $\rho$.

i) Velja $\chi(1) = \deg \rho$.

ii) Za vsak $g \in G$ je $\chi(x^{-1}) = \overline{\chi(g)}$.

iii) Za vse $g, h \in G$ je $\chi(hgh^{-1}) = \chi(g)$.

*Dokaz.* Dokažimo drugo točko. Ker je $\rho(g)^n = 1$, so lastne vrednosti $\rho(g)$ koreni enote. Ker velja $\lambda^{-1} = \overline{\lambda}$, sledi

$$\rho(g^{-1}) = \sum_{i=1}^{n} \lambda_i^{-1} = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{\rho(g)}.$$ □

**Definicija 4.4.3.** Naj bo $V$ končnorazsežen $\mathbb{C}G$-modul. S $\chi_V$ označimo karakter upodobitve $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$.

**Opomba 4.4.3.1.** Ta karakter je dobro definiran. Če sta $V$ in $W$ izomorfna $\mathbb{C}G$-modula, velja namreč

$$\rho_V(g) = T^{-1} \circ \rho_W(g) \circ T,$$

zato sta sledi enaki.

**Trditev 4.4.4.** Naj bosta $V$ in $W$ končnorazsežna $\mathbb{C}G$-modula. Tedaj je

i) $\chi_{V \oplus W} = \chi_V + \chi_W$,

ii) $\chi_{V \otimes W} = \chi_V \times \chi_W$ in

iii) $\chi_{V^*} = \overline{\chi_V}$.

*Dokaz.* Preprosto izračunamo sled pripadajočih matrik. Upodobitev $\rho^*\colon G \to \mathrm{GL}_{\mathbb{C}}(V^*)$ deluje s predpisom $\rho(g) = (\varphi \mapsto \varphi \circ \rho(g^{-1}))$. □

**Lema 4.4.5.** Naj bosta $V$ in $W$ končnorazsežna $\mathbb{C}G$-modula. Tedaj sta $G$-modula $\mathrm{Hom}_{\mathbb{C}}(V, W)$ in $V^* \otimes_{\mathbb{C}} W$ izomorfna.

*Dokaz.* Naj bo $\alpha\colon V^* \otimes_{\mathbb{C}} W \to \mathrm{Hom}_{\mathbb{C}}(V, W)$ preslikava, podana s predpisom $\varphi \otimes w \mapsto (v \mapsto \varphi(v)w)$. Očitno je $\mathbb{C}$-linearna, ker pa velja

$$\alpha(g(\varphi \otimes w)) = \alpha(g\varphi \otimes gw) = (v \mapsto (g\varphi)(v)gw) = (v \mapsto \varphi(g^{-1}v)gw) = g \cdot \alpha(\varphi \otimes w).$$

Zaradi enakosti dimenzij je dovolj, da dokažemo surjektivnost. Naj bo $f\colon V \to W$ poljuben homomorfizem. Za bazo $\{v_i \mid i \leq n\}$ naj bo $f(v_i) = w_i$. Naj bo $\{\varphi_i \mid i \leq n\}$ dualna baza in

$$\widetilde{f} = \sum_{i=1}^{n} \varphi_i \otimes f(v_i).$$

Tedaj je
$$\alpha\left(\widetilde{f}\right)v_j = f(v_j),$$
zato je $\alpha\left(\widetilde{f}\right) = f$. □

**Lema 4.4.6.** Naj bosta $V$ in $W$ končnorazsežna $\mathbb{C}G$-modula. Tedaj je $\mathrm{Hom}_{\mathbb{C}}(V,W)^G = \mathrm{Hom}_{\mathbb{C}G}(V,W)$.

*Dokaz.* Naj bo $\varphi \in \mathrm{Hom}_{\mathbb{C}}(V,W)$. Sledi, da je
$$\begin{aligned}\varphi \in \mathrm{Hom}_{\mathbb{C}}(V,W)^G &\iff \forall g \in G\colon g\cdot\varphi = \varphi\\ &\iff \forall g \in G\colon \forall v \in V: g\varphi(g^{-1}v) = \varphi(v)\\ &\iff \forall g \in G\colon \forall v \in V: \varphi(gv) = g\varphi(v)\\ &\iff \varphi \in \mathrm{Hom}_{\mathbb{C}G}(V,W).\end{aligned}$$
□

**Lema 4.4.7.** Naj bo $V$ $\mathbb{C}G$-modul. Tedaj je preslikava $\pi\colon V \to V$ s predpisom
$$\pi = \frac{1}{|G|}\sum_{g\in G} g$$
homomorfizem $G$-modulov in projektor na $V^G$ in velja
$$\mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G}\right) = \dim V^G.$$

*Dokaz.* Očitno je $\pi$ linearna. Ker je
$$\begin{aligned}\pi(hv) &= \left(\frac{1}{|G|}\sum_{g\in G} g\right)hv\\ &= \left(\frac{1}{|G|}\sum_{g\in G} gh\right)v\\ &= \pi(v)\\ &= \left(\frac{1}{|G|}\sum_{g\in G} hg\right)v\\ &= h\pi(v),\end{aligned}$$
je tudi homomorfizem $G$-modulov. Seveda je $\pi(v) \in V^g$. Ker je očitno $\pi|_{V^G} = \mathrm{id}$, je to res projektor. Ker je sled projektorja enaka dimenziji slike, velja tudi zgornja enakost. □

**Definicija 4.4.8.** Naj bosta $\varphi, \psi\colon G \to \mathbb{C}$ funkciji, konstantni na konjugiranostnih razredih. Definiramo *skalarni produkt*
$$\langle\varphi,\psi\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}\psi(g).$$

**Trditev 4.4.9.** Za vse $\varphi, \psi, \varphi_1$ in $\varphi_2$ velja:

i) $\langle \varphi, \varphi \rangle \geq 0$,

ii) $\langle \varphi, \varphi \rangle = 0 \iff \varphi = 0$,

iii) $\langle \varphi, \psi \rangle = \overline{\langle \psi, \varphi \rangle}$,

iv) $\langle \varphi_1 + \varphi_2, \psi \rangle = \langle \varphi_1, \psi \rangle + \langle \varphi_2, \psi \rangle$ in

v) $\langle \varphi_1 \varphi_2, \psi \rangle = \langle \varphi_1, \overline{\varphi_2} \psi \rangle$.

*Dokaz.* The proof is obvious and need not be mentioned. □

**Trditev 4.4.10.** Če sta $\chi$ in $\psi$ karakterja, velja $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle$.

*Dokaz.* Velja

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \psi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) \psi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g) \psi(g^{-1}) = \langle \psi, \chi \rangle .$$ □

**Trditev 4.4.11.** Veljata naslednji trditvi:

i) Če je $\chi$ karakter nerazcepne upodobitve $G$, je $\langle \chi, \chi \rangle = 1$.

ii) Če sta $\chi$ in $\psi$ karakterja neizomorfnih upodobitev $G$, je $\langle \chi, \psi \rangle = 0$.

*Dokaz.* Naj bosta $V$ in $W$ pripadajoča $\mathbb{C}G$-modula. Na elemente $g$ glejmo kot na delovanje na prostoru $\mathrm{Hom}_{\mathbb{C}}(V, W)$. Po Schurovi lemi je

$$\mathrm{tr}\left( \frac{1}{|G|} \sum_{g \in G} g \right) = \dim \mathrm{Hom}_{\mathbb{C}}(V, W)^G = \dim \mathrm{Hom}_{\mathbb{C}G}(V, W) = \begin{cases} 0, & V \not\cong W, \\ 1, & V \cong W. \end{cases}$$

Ker je

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \left( \overline{\chi} \psi \right)(g)$$

in je $\overline{\chi}\psi$ karakter $\mathrm{Hom}_{\mathbb{C}}(V, W)$, je

$$\langle \chi, \psi \rangle = \mathrm{tr}\left( \frac{1}{|G|} \sum_{g \in G} g \right).$$ □

**Posledica 4.4.11.1.** Naj bo

$$V = \bigoplus_{i=1}^{r} S_i^{n_i}$$

končnorazsežen $\mathbb{C}G$-modul, pri čemer so $S_i$ paroma neizomorfni enostavni $\mathbb{C}G$-moduli. Tedaj je

$$n_i = \langle \chi_V, \chi_i \rangle ,$$

kjer je $\chi_i$ karakter upodobitve $S_i$.

*Dokaz.* Velja

$$\chi_V = \sum_{i=1}^{r} n_i \chi_i .$$ □

**Posledica 4.4.11.2.** Naj bosta $V$ in $W$ končnorazsežna $\mathbb{C}G$-modula. Tedaj je $V \cong W$ natanko tedaj, ko je $\chi_V = \chi_W$.

*Dokaz.* Uporabimo prejšnjo posledico. □

**Posledica 4.4.11.3.** Če je $V$ končnorazsežen $\mathbb{C}G$-modul, za njegov karakter $\chi$ velja $\langle \chi, \chi \rangle = 1$ natanko tedaj, ko je enostaven.

*Dokaz.* Razpišemo lahko

$$\langle \chi, \chi \rangle = \sum_{i=1}^{r} n_i^2.$$

□

# Stvarno kazalo