# Komutativna algebra - 9. domača naloga

Benjamin Benčina, 27192018

12. maj 2020

**Nal. 1:** Naj bo $m = k^2 n \in \mathbb{Z}$, kjer $k, n \in \mathbb{Z}$ in $n$ brez kvadratnih faktorjev. Pokažimo, da je celostno zaprtje $\mathbb{Z}[\sqrt{m}]$ v svojem obsegu ulomkov enako $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$, če je $n \equiv 1$ in $\mathbb{Z}[\sqrt{n}]$ sicer. Dodatno lahko predpostavimo $k \in \mathbb{N}$.

Polje ulomkov v našem primeru je $\mathbb{Q}(\sqrt{m})$, seveda pa velja $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(k\sqrt{n}) = \mathbb{Q}(\sqrt{n})$. Zanimajo nas celostni elementi oblike $a + b\sqrt{m} = a + bk\sqrt{n}$, kjer $a, b \in \mathbb{Q}$. Tak element seveda zadošča polinomu $(x - a - bk\sqrt{n})(x - a + bk\sqrt{n}) = x^2 - 2ax + a^2 - nk^2b^2$. Hočemo, da $-2a, a^2 - nk^2b^2 \in \mathbb{Z}$. Če to velja, potem seveda tudi $4(a^2 - nk^2b^2) = (2a)^2 - n(2kb)^2 \in \mathbb{Z}$ in deljivo s 4. Ker je $n$ brez kvadratnih faktorjev, sledi $2kb \in \mathbb{Z}$. Prestavimo se v kolobar $\mathbb{Z}_4$. Zgornji izraz je tam enak 0, edina kvadrata pa sta 0 in 1. Ločimo primere:

- $n \equiv 2$: V tem primeru iz $(2a)^2 \equiv 2(2kb)^2$ sledi $(2a)^2 \equiv 0$ in $(2kb)^2 \equiv 0$, saj sta 0 in 1 edina kvadrata. Če $a \notin \mathbb{Z}$, vemo pa $2a \in \mathbb{Z}$, potem $(2a)^2 \equiv 1$, kar je protislovje, torej $a \in \mathbb{Z}$. Z enakim premislekom dobimo $kb \in \mathbb{Z}$. Od tod torej $\overline{\mathbb{Z}[\sqrt{m}]} = \mathbb{Z}[\sqrt{n}]$.
- $n \equiv 3$: Isti premislek kot $n \equiv 2$.
- $n \equiv 0$: Z drugimi besedami, $4 = 2^2 | n$. V tem primeru je $n = 0$, sicer pridemo v protislovje s predpostavko, da $n$ nima kvadratnih faktorjev. Potem je tudi $m = 0$ in izjava je trivialno resnična.
- $n \equiv 1$: Tukaj je edina možnost, ko lahko $(2a)^2 \equiv 1$ in $(2kb)^2 \equiv 1$. To se na primer lahko zgodi v primeru $a = \frac{1}{2}, b = \frac{1}{2}$ za primerne $k$. Problem je seveda, da pokrajšamo število 2 znotraj oklepaja. Ker je 2 praštevilo, to tudi edini način, da lahko število 2 pokrajšamo, torej $\overline{\mathbb{Z}[\sqrt{m}]} = \mathbb{Z}[\frac{1}{2} + \frac{\sqrt{n}}{2}] = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$.

Hkrati smo tudi videli, da sta dobljena kolobarja res algebraično zaprta in da je bistveno, da je $n$ brez kvadratnih faktorjev (oz. kvadratne faktorje smo primorani pridružiti številu $k^2$).

**Nal. 2:** Naj bo $R \subseteq S$ celostna razširitev, $K$ algebraično zaprto polje in $f\colon R \to K$ homomorfizem. Pokažimo, da obstaja razširitev $F\colon S \to K$, torej $F|_R = f$.

Najprej opazimo, da je $\ker f$ praideal v kolobarju $R$, saj je $K$ polje. Označimo $P = \ker f$. Po izreku 9.11 s predavanj (lying over) obstaja praideal $Q \lhd S$, ki leži nad $P$, saj je $R \subseteq S$ celostna razširitev. Če pogledamo kompozitum $R \to S \to S/Q$, kjer je prva preslikava inkluzija, druga pa kvocientni homomorfizem, vidimo, da je jedro tega homomorfizma točno $P$ (po definiciji ideala $Q$). Prvi izrek o izomorfizmih nam da injektiven homomorfizem $\varphi\colon R/P \to S/Q$, kjer je $S/Q$ celosten nad $R/P$. Če si sedaj ogledamo polji ulomkov, je $\mathrm{Quot}(S/Q)$ algebraična razširitev $\mathrm{Quot}(R/P)$ (spomnimo se, da je pojem celostne razširitve le posplošitev pojma algebraične razširitve na kolobarje, v poljih pa sta pojma enaka).

Oglejmo si diagram

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "q_R"] & K \\
R/P \arrow[ur, "f'"] \arrow[r, "i_R"] & \mathrm{Quot}(R/P) \arrow[u, "f''"]
\end{tikzcd}$$

Začnemo s homomorfizmom $f$. Po prvem izreku o izomorfizmih obstaja homomorfizem $f'$. Potem obstaja tudi njegova razširitev v polju ulomkov $f''$. Radi bi, da analogen diagram velja za kolobar $S$. Po premisleku zgoraj seveda obstajata homomorfizma $q_S$ in $i_S$. Razvijmo zgornji diagram in si oglejmo

$$
\begin{tikzcd}
R \arrow[r, "i"] \arrow[d, "q_R"] & S \arrow[d, "q_S"] \\
R/P \arrow[r, "\varphi"] \arrow[d, "i_R"] & S/Q \arrow[d, "i_S"] \\
\mathrm{Quot}(R/P) \arrow[r, "\overline{\varphi}"] \arrow[d, "f''"] & \mathrm{Quot}(S/Q) \arrow[dl, "g"] \\
K &
\end{tikzcd}
$$

Iz teorije razširitev polj se spomnimo, da če imamo $F \subseteq E$ algebraično razširitev, lahko vsak homomorfizem polj $F \to K$ razširimo do homomorfizma polj $E \to K$ ($K$ je še vedno algebraično zaprto polje). Tako dobimo homomorfizem $g\colon \mathrm{Quot}(S/Q) \to K$, ki razširja homomorfizem $f''$. Iskana razširitev je potem očitno $F = g \circ i_S \circ q_S$.

Poskusimo poiskati še kakšen homomorfizem, ki ga ne moremo razširiti, če katera od predpostavk in izpolnjena.

Naj bo $R \subseteq S$ necelostna razširitev, kjer $R = \mathbb{C}[x]$ in $S = \mathbb{C}[x,y]/(xy-1)$, in naj bo $K = \mathbb{C}$ algebraično zaprto polje. Trdimo, da ničelnega homomorfizma $R \to K$ ne moremo razširiti na celoten $S$. Res, enačba $xy - 1 = 0$, ki ji v $S$ nad $R$ zadošča polinom $y$, se spremeni v protislovno enačbo $0 \cdot \overline{y} - 1 = 0$ (saj $x$ slikamo v 0).

Naj bo $Z \subseteq \mathbb{Q}$ celostna razširitev in naj bo $K = \mathbb{Z}_2$ polje, ki pa ni algebraično zaprto. Potem se kvocientnega homomorfizma $f\colon k \mapsto k \bmod 2$ ne da razširiti na vsa racionalna števila. Res, naj bo $F$ možna razširitev homomorfizma. Potem po eni strani $F(\frac{1}{2} + \frac{1}{2}) = F(1) = 1$, po drugi pa $F(\frac{1}{2} + \frac{1}{2}) = 2F(\frac{1}{2}) = 0$.