Izbrana poglavja iz matematike

Napisal Jure Pustoslemšek po zapiskih predavanj prof. dr. Petarja Pavešiča

Junij 2020

1 Abstraktna algebra: kolobarji in obsegi

Definicija 1.0.1 (Kolobar)**.** *Kolobar je množica, kateri smo priredili notranji operaciji seštevanja in množenja, ki zadostujeta spodnjim kriterijem. Eksplicitno ga lahko zapišemo kot* $(K, +, \cdot)$.

Pri seštevanju velja komutativnost in asociativnost obstaja ničla 0 in za vsak $a \in K$ *obstaja nasprotni element* $(-a) \in K$*, torej lahko vedno odštevamo.*

$$\forall a, b \in K : a + b = b + a$$

$$\forall a, b, c \in K : (a + b) + c = a + (b + c)$$

$$\forall a \in K \exists (-a) \in K : a + (-a) = a - a = 0$$

Pri množenju nimamo dodatnih zahtev, wazen uglašenosti s seštevanjem - distibutivnost.

$$\forall a, b, c \in K : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Rečeno drugače, kolobar je grupa za seštevanje in zaprta za množenje.

Če ima množenje kakšno dodatno lastnost, to lastnost običajno izpostavimo

Množenje je asociativno	$\rightarrow$	asociativni kolobar
Množenje je komutativno	$\rightarrow$	komutativni kolobar
Množenje ima enoto	$\rightarrow$	kolobar z enoto
Vsak $a \neq 0 \in K$ ima inverz a^{-1}	$\rightarrow$	kolobar z deljenjem

Literatura velikokrat v definiciji kolobarja zahteva tudi asociativnost in obstoj enote, zato bomo v nadaljevanju privzeli, da z izrazom "kolobar" mislimo na asociativen kolobar z enoto, komutativnost in deljenje pa bomo izrecno navedli.

Definicija 1.0.2 (Obseg)**.** *Kolobarju, v katerem je množenje asociativno, komutativno in ima enoto ter ima operacijo deljenja, rečemo* ***obseg****.*

1.1 Kolobarji

Zgled 1.1.1. *Če dani kolobar nima enote, mu jo lahko dodamo:*
K kolobar brez enote
Če dodamo 1, smo prisiljeni dodati tudi $-1, 2, -2, 3, -3, ...$
Rešitev: na $\mathbb{Z} \times K$ vpeljemo:

$$(n, a) + (m, b) := (n + m, a + b)$$

$$(n, a) \cdot (m, b) := (nm, nb + ma + ab)$$

Ničla je $(0, 0)$, nasprotni element je $-(m, a) = (-m, -a)$, enota je $(1, 0)$. Če je K komutativen oz. asociativen, je to tudi $\mathbb{Z} \times K$.

Kaj pa, če imamo kolobar, v katerem nekateri elementi nimajo inverza, ampak bi jih želeli dodati? Poskusimo to storiti na takšen način, kot smo v osnovni šoli definirali racionalna števila s celimi števili, in sicer z uvedbo ulomkov.

Naj bo K kolobar z enoto. Za $a, b \in K, b \neq 0$ vpeljemo simbole $\frac{a}{b}$, s katerimi računamo

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

Pojavi se težava: lahko se zgodi, da je $bd = 0$, čeprav $b \neq 0$ in $d \neq 0$. Tega pri številih nismo vajeni vendar:

Zgled 1.1.2 (Matrike)**.**

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Zgled 1.1.3 ($\mathbb{Z}_{12}$: ostanki po modulu 12)**.**

$$2 \cdot 6 = 0$$

$$3 \cdot 8 = 0$$

Definicija 1.1.4 (Delitelj niča)**.** *V kolobarju K je $0 \neq a \in K$ **delitelj niča**, če obstaja tak $b \neq 0$, da je $a \cdot b = 0$.*

Trditev 1.1.5. *Delitelj niča nima inverza.*

Dokaz. Če za $a \in K$ obstajata takšna neničelna $b, c \in K$, da velja

$$a \cdot b = 0 \text{ in } c \cdot a = 1$$

dobimo protislovje

$$b = 1 \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$$

□

Definicija 1.1.6 (Celi kolobar)**.** ***Celi kolobar*** *je komutativni kolobar, v katerem ni deliteljev niča. Ekvivalentno, v celem kolobarju iz* $a \cdot b = 0$ *sledi* $a = 0$ *ali* $b = 0$.

Naj bo K celi kolobar. Tvorimo **kolobar ulomkov** $\overline{K}$: elementi so ulomki $\frac{a}{b}$, vendar $\frac{a}{b} \equiv \frac{c}{d}$, če je $ad = bc$ (ulomke lahko krajšamo). Definiramo operaciji kot prej:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Preverimo lahko, da je $\overline{K}$ obseg.

Zakaj moramo enačiti sorazmerne ulomke?

Zaradi definicije operacij: $\frac{a}{b} - \frac{ka}{kb} = \frac{kab-kab}{kb^2} = 0$, torej mora veljati $\frac{ka}{kb} \equiv \frac{a}{b}$.

Opomba. *Z nekaj truda lahko vpeljemo ulomke tudi pri nekomutativnih kolobarjih in kolobarjih z deliterlji niča. Takrat dobimo kolobarje ulomkov, ki niso obsegi.*

Delitelj niča ne more biti obrnljiv, obrnljiv element pa ni delitelj niča. Ali je lahko element kolobarja niti obrnljiv niti delitelj niča?

Zgled 1.1.7. $\mathbb{Z}$ *nima deliteljev niča, obrnljiva pa sta le* 1 *in* -1.

Zgled 1.1.8. $\mathbb{Z}_{12}$

- *Delitelji niča:* $0, 2, 3, 4, 6, 8, 9, 10$
- *Obrnljivi:* $1, 5, 7, 11$

V končnih kolobarjih ni drugih možnosti, kar pove naslednji znameniti izrek.

Izrek 1.1.9 (Wedderburnov izrek)**.** *Končen kolobar brez deliteljev niča je obseg.*

Dokaz. Naj bo K končen kolobar brez deliteljev niča. Dokazati moramo, da so vsi elementi $K - \{0\}$ obrnljivi.

Za poljuben $a \in K - \{0\}$ definiramo funkcijo

$$l_a : K \to K$$

$$l_a(x) := a \cdot x$$

Recimo, da za neka $x, y \in K$ velja $l_a(x) = l_a(y)$. Potem je $ax = ay$, torej $a(x - y) = 0$. Ker K nima deliteljev niča, sledi $x = y$. Torej je l_a injektivna in ker slika iz K v K, tudi bijektivna.

Ker je $l_a(K) = K$, je $l_a(b) = a \cdot b = 1$ za nek $b \in K$. Ponovimo razmislek za $d_a(x) := x \cdot a$ in dobimo, da je $d_a(c) = a \cdot c = 1$ za nek $c \in K$. Iz $c = c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$ sledi $c = b = a^{-1}$. K je torej kolobar z deljenjem. Če je K komutativen, je obseg.

Dokaz komutativnosti zahteva nekaj dodatne teorije grup, zato ga ne bomo natančno navedli. Ideja je, da je center $Z(K)$ (tj. elementi K, ki komutirajo z vsemi elementi K) obseg, celoten K pa je vektorski prostor nad $Z(K)$. Iz primerjave multiplikativnih grup lahko izpeljemo, da je K 1-razsežen vektorski prostor nad $Z(K)$, torej $K = Z(K)$. □

Posledica 1.1.10. *$\mathbb{Z}_n$ je obseg $\Leftrightarrow$ n je praštevilo.*

Definicija 1.1.11 (Karakteristika kolobarja)**.** ***Karakteristika*** *kolobarja K je najmanjši $n \in \mathbb{N}$, za katerega velja, da je $n \cdot a = a + ... + a = 0$. Zapišemo jo kot $char(K) = n$ ali $charK = n$. Če tak n ne obstaja, potem pišemo $char(K) = 0$.*

Trditev 1.1.12. *Naj bo K kolobar.*

a) Če $1 \in K$, potem je $char(K) =$ red enote $=$ min n, da je $n \cdot 1 = 0$.

b) Če K nima deliteljev niča, potem je $char(K)$ praštevilo ali 0.

Dokaz (a). Naj bo n red enote, torej je $n \cdot 1 = 0$. Potem za vsak $a \in K$ velja:

$$n \cdot a = (n \cdot 1) \cdot a = 0 \cdot a = 0$$

Iz tega sledi, da je $charK \leq n$. Ker je red 1 enak n, je $charK \geq n$, torej $charK = n$. □

Dokaz (b). Denimo, da je $charK = k \cdot l$ za $k, l > 1$. Potem je $0 = k \cdot l \cdot 1 = k \cdot l$. Ker v K ni deliteljev niča, je $k \cdot 1 = 0$ ali $l \cdot 1 = 0$, zato je po (a) $charK < k \cdot l$. Protislovje. □

Definicija 1.1.13. *Naj bosta K, L kolobarja.*

*$f \colon K \to L$ je **homomorfizem kolobarjev**, če velja:*

$$f(a + b) = f(a) + f(b)$$

$$f(a \cdot b) = f(a) \cdot f(b)$$

za poljubna $a, b \in K$.

Bijektivnemu homomorfizmu rečemo **izomorfizem**.

Poglejmo nekaj primerov homomorfizmov:

Zgled 1.1.14. $\mathbb{Z} \xrightarrow{mod\ n} \mathbb{Z}_n$ *je homomorfizem (dokaz ponovi korake dokaza, da je $\mathbb{Z}_n$ kolobar).*

Zgled 1.1.15. *Konjugiranje* $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ *je izomorfizem kolobarjev.*

Zgled 1.1.16. *Za poljuben* $a \in \mathbb{R}$ *definiramo* $f_a\colon \mathbb{Z}[x] \to \mathbb{R}$ *s predpisom* $f_a(p) = p(a)$

$$f_a(p+q) = (p+q)(a) = p(a) + q(a) = f_a(p) + f_a(q)$$

$$f_a(p+q) = (p \cdot q)(a) = p(a) \cdot q(a) = f_a(p) \cdot f_a(q)$$

Zgled 1.1.17. $a \mapsto \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ *je homomorfizem* $\mathbb{R} \to M_2(\mathbb{R})$.

Zgled 1.1.18. *Splošneje* $f_a\colon \mathscr{C}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ *s predpisom* $f_a(g) := g(a)$ *je tudi homomorfizem kolobarjev.*

Zgled 1.1.19. $a \mapsto \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$ *ni homomorfizem* $\mathbb{R} \to M_2(\mathbb{R})$ *(ohranja seštevanje, ne pa množenja).*

Zgled 1.1.20. *Preslikava* $\mathbb{C} \to M_2(\mathbb{R})$ *s predpisom* $a + bi \mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ *je homomorfizem.*

Zgled 1.1.21. $a \mapsto a^p$ *je homomorfizem* $\mathbb{Z}_p \to \mathbb{Z}_p$ *(p praštevilo).*

Trditev 1.1.22. *Za homomorfizem* $f\colon K \to L$ *velja:*

a) $f(0) = 0$

b) $f(-a) = -f(a)$

Dokaz (a). $f(0) = f(0+0) = f(0) + f(0)$ □

Dokaz (b). $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$ □

Definicija 1.1.23 (Unitalen homomorfizem)**.** *Homomorfizem, za katerega velja* $f(1) = 1$*, je* ***unitalen****.*

Trditev 1.1.24. *Če je* f *unitalen homomorfizem in* a *obrnljiv, je* $f(a)$ *obrnljiv.*

Dokaz. Naj bo $f : K \to L$ unitalen homomorfizem kolobarjev in $a \in K$ obrnljiv. Potem je

$$1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

Potem je $f(a^{-1})$ desni inverz za $f(a)$. Po podobnem razmisleku vidimo, da je $f(a^{-1})$ tudi levi inverz za $f(a)$. Torej je $f(a^{-1}) = f(a)^{-1}$. □

Trditev 1.1.25. *Naj bo* $f\colon K \to L$ *homomorfizem kolobarjev. Potem je* $Im f$ *podkolobar v* L.

Dokaz. Vzamemo poljubna $x, y \in Imf$. Potem obstajata takšna $a, b \in K$, da je $f(a) = x$ in $f(b) = y$ in zato velja

$$x + y = f(a) + f(b) = f(a + b) \in Imf$$

$$x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \in Imf$$

Torej je Imf podkolobar v L. $\square$

Trditev 1.1.26. *Naj bo $f : K \to L$ homomorfizem kolobarjev. Potem je $Kerf$ podkolobar v K.*

Dokaz. Vzamemo poljubna $x, y \in Kerf$. Potem je $f(x+y) = f(x)+f(y) = 0+0 = 0$, torej je $x+y \in Kerf$. Podobno je $f(x\cdot y) = f(x)\cdot f(y) = 0\cdot 0 = 0$, torej je $x \cdot y \in Kerf$. $\square$

Definicija 1.1.27 (Ideal kolobarja)**.** *Podkolobar $I \leq K$ je* ***ideal*** *v K, če za vsak $a \in K, x \in I$ velja $a \cdot x \in I$ (levi ideal) in $x \cdot a \in I$ (desni ideal). Označimo ga z $I \triangleleft K$.*

Zgled 1.1.28. $\{0\} \triangleleft K$ *in* $K \triangleleft K$ *sta "neprava"ideala.*

Zgled 1.1.29. $n\mathbb{Z} \triangleleft \mathbb{Z}$

Zgled 1.1.30. $\{a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n \mid a \in \mathbb{R}\} \triangleleft \mathbb{R}[x]$ *so polinomi, za katere je $p(0) = 0$. Splošneje, za $a \in K$ je $\{p \in K[x] \mid p(a) = 0\} \triangleleft K[x]$.*

Zgled 1.1.31. $\{\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \mid x, y \in \mathbb{R}\} \subseteq M_2(\mathbb{R})$ *je podkolobar.*

$$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \pm \begin{bmatrix} z & 0 \\ w & 0 \end{bmatrix} = \begin{bmatrix} x \pm z & 0 \\ y \pm w & 0 \end{bmatrix}$$

$$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \cdot \begin{bmatrix} z & 0 \\ w & 0 \end{bmatrix} = \begin{bmatrix} xz & 0 \\ yw & 0 \end{bmatrix}$$

Poleg tega je

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} = \begin{bmatrix} ax + by & 0 \\ cx + dy & 0 \end{bmatrix}$$

$$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ax & bx \\ ay & by \end{bmatrix}$$

Podana množica je levi ideal.

Trditev 1.1.32. *Naj bo $f\colon K \to L$ homomorfizem kolobarjev. Potem je $Kerf$ (dvostranski) ideal v K.*

Dokaz. Vzemimo $x \in Kerf$ in $a \in K$. $f(x)\cdot f(a) = f(x)\cdot f(a) = 0\cdot f(a) = 0$, torej je $x \cdot a \in Kerf$. Analogno, $f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0 = 0$, torej je tudi $a \cdot x \in Kerf$. $\square$

Za $x \in K$ je $K \cdot x = \{a \cdot x \mid a \in K\}$ levi ideal v K, $x \cdot K$ pa desni. Dvostranski ideal, ki ga generira x, pa ni $K \cdot x \cdot K$, ker ni zaprt za seštevanje. Potrebno je vzeti vse možne vsote izrazov $a \cdot x \cdot b$.

Definicija 1.1.33 (Glavni ideal)**.** *Ideal, ki ga generira en sam element, imenujemo* ***glavni ideal*** *in ga zapišemo z* (x)*, kjer je* $x \in K$*.*

Trditev 1.1.34. *V* $\mathbb{Z}$ *so vsi ideali glavni.*

Dokaz. Naj bo $I \triangleleft \mathbb{Z}$. Če je $I = \{0\}$, potem je $I = (0)$. Recimo, da $I \neq (0)$. Potem obstaja vsaj eno pozitivno število v I. Vzemimo najmanjše pozitivno število $a \in I$. Pokazati moramo, da a deli vse elemente I.

Poljuben $b \in I$ je po izreku o deljenju enak $b = k \cdot a + r$ za natanko določena $k \in \mathbb{Z}$ in $0 \leq r < a$. Potem je $r = b - k \cdot a \in I$. Ker je a najmanjše pozitivno število v I, je $r = 0$, torej je $b = k \cdot a$. I je torej generiran z a. $\square$

Definicija 1.1.35 (Glavnoidealski kolobar)**.** *Kolobar, v katerem so vsi ideali glavni, je* ***glavnoidealski****.*

Trditev 1.1.36. *Naj bo* K *obseg. Vsi ideali v* $K[x]$ *so glavni.*

Dokaz. Vzemimo $I \triangleleft K$. Če je $I = 0$, je $I = (0)$. Privzemimo, da je $I \neq (0)$: Potem obstaja neničelni nekonstantni polinom najmanjše stopnje $p \in K[x]$, za katerega lahko privzamemo, da je moničen. Pokažimo, da p deli vse elemente I.

Vzemimo poljuben $q \in I$. Po izreku o deljenju je $q(x) = k(x)p(x) + r(x)$ za natanko določena $k \in K[x]$ in $r \in K[x]$, ki je strogo manjše stopnje kot p. Vidimo, da je $r(x) = q(x) - k(x)p(x) \in I$. Ker pa je p polinom najmanjše stopnje med vsemi v I, mora biti $r(x) = 0$. To pa pomeni, da je $q(x) = k(x)p(x)$. Ideal I je torej generiran z p. Sledi, da so vsi ideali v $K[x]$ glavni. $\square$

Naj bo $I \triangleleft K$ dvostranski ideal. Na K vpeljemo relacijo $\sim$:

$$a \sim b \iff a - b \in I$$

Trditev 1.1.37. $\sim$ *je ekvivalenčna relacija.*

Dokaz.

$a - a = 0 \in I$, torej je $a \sim a$.

Če $a - b \in I$, je tudi $b - a \in I$, torej $a \sim b \implies b \sim a$.

Če $a - b \in I$ in $b - c \in I$, je tudi $a - c \in I$. Torej je $a \sim b, b \sim c \implies a \sim c$. $\square$

Definicija 1.1.38 (Kvocientni kolobar)**.** *Množico ekvivalenčnih razredov relacije* $\sim$ *označimo z* K/I *in jo imenujemo* ***kvocientni kolobar****.*

Ekvivalenčni razred elementa $a \in K$ označimo $[a]$ ali $a + I$ (oznaka je smiselna, ker je $[a] = \{a + x \mid x \in I\}) \equiv a + I$.

Elemente K/I naravno seštevamo in množimo:

$$(a + I) + (b + I) := (a + b) + I$$

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

Da bosta operaciji dobro definirani, moramo preveriti, sta neodvisni od izbire predstavnikov ekvivalečnih razredov. Najprej preverimo operacijo seštevanja:

Če $a' + I = a + I$ in $b' + I = b + I$, je $a - a' \in I$ in $b - b' \in I$.

$$(a - a') + (b - b') = (a + b) - (a' + b') = (a + b) + I = (a' + b') + I$$

Preverimo še za množenje:

$$a' = a + x \text{ in } b' = b + y \text{ za } x, y \in I.$$

$$a' \cdot b' = a \cdot b + ay + xb + xy$$
$$(a' \cdot b') + I = (a \cdot b) + I$$

Zdaj vemo, da sta operaciji dobro definirani. Sedaj preverimo, da je K/I res kolobar.

Trditev 1.1.39. *Naj bo K kolobar in $I \triangleleft K$. Potem je K/I tudi kolobar.*

Dokaz. Vzemimo poljubne $a, b, c \in K/I$. Najprej preverimo, da je grupa za seštevanje:

asociativnost:
$$((a+b)+c)+I = (a+I)+(b+I)+(c+I) = (a+I)+((b+c)+I) = (a+(b+c))+I$$
komutativnost:
$$(a + b) + I = (a + I) + (b + I) = (b + I) + (a + I) = (b + a) + I$$
negativni element: $(a + b) + I = 0 + I \implies a + I = -b + I$

Preverimo še asociativnost in obstoj enote za množenje:

asociativnost:
$$((a \cdot b) \cdot c) + I = (a + I) \cdot (b + I) \cdot (c + I) = (a + I) \cdot ((b \cdot c) + I) = (a \cdot (b \cdot c)) + I$$
komutativnost: $(a \cdot b) + I = (a + I) \cdot (b + I) = (b + I) \cdot (a + I) = (b \cdot a) + I$

□

Izrek 1.1.40 (Izrek o izomorfizmu)**.** *Naj bo $f\colon K \to L$ homomorfizem kolobarjev. Potem je $Kerf \triangleleft K$ in imamo naravni izomorfizem:*

$$\overline{f}\colon K/Kerf \to Imf \text{ s predpisom } \overline{f}(x + Kerf) := f(x)$$

Dokaz. $Ker f \triangleleft K$ že vemo.

Za $u \in Ker f$ je $f(x+u) = f(x)$, zato je definicija $\overline{f}$ neodvisna od predstavnika razreda.

$\overline{f}$ je aditivna:

$$\overline{f}((x + Ker f) + (y + Ker f)) = \overline{f}((x+y) + Ker f)$$

$$= f(x+y) = f(x) + f(y) = \overline{f}(x + Ker f) + \overline{f}(y + Ker f)$$

Za množenje opravimo analogni razmislek.

$$Ker\overline{f} = \{x + Ker f \mid \overline{f}(x + Ker f) = 0\} = \{x \mid f(x) = 0\} = \{0 + Ker f\}$$

$\overline{f}$ je torej injektivna.

$$Im\overline{f} = Im f$$

$\overline{f}$ je surjektivna. □

Trditev 1.1.41. *Komutativen kolobar K je obseg natanko tedaj, ko nima pravih idealov (tj. edina ideala sta (0) in K).*

Dokaz $\Longrightarrow$. Recimo, da je K obseg in $I \triangleleft K$ neničelni ideal v K ($I \neq (0)$). Potem obstaja $0 \neq x \in I$. Ker je x obrnljiv v K, potem za vsak $a \in K$ velja $a = (a \cdot x^{-1}) \cdot x \in I$, torej je $I = K$. □

Dokaz $\Longleftarrow$. Recimo, da K nima pravih idealov. Naj bo $0 \neq a \in K$. Potem je $(a) = K \cdot a = a \cdot K \triangleleft K$. Ker v K ni pravih idealov, je $(a) = K$. Ker K vsebuje enoto in je celoten generiran z a, je $a \cdot b = b \cdot a = 1$ za nek $b \in K$. Sledi, da je a obrnljiv, in ker smo za a izbrali poljuben element K, so vsi elementi v K obrnljivi. Torej je K obseg. □

Poiščimo ideale v K/I. Za pomoč definirajmo funkcijo

$$\begin{aligned} q\colon K &\to K/I \\ x &\mapsto x + I \end{aligned}$$

Trditev 1.1.42. *Naj bo K komutativen kolobar in $I \triangleleft K$.*

a) Če je $J \triangleleft K$, potem je $q(J) \triangleleft K/I$.

b) Če je $J \triangleleft K/I$, potem je $q^{-1}(J) \triangleleft K$ in $I \triangleleft q^{-1}(J)$

Dokaz (a). Vzamemo $a \in K$ in $x \in J$. Potem je $a+I \in K/I$ in $x+I \in q(J)$.

$$(a+I)(x+I) = (a \cdot x) + I \in q(J)$$

□

Dokaz (b). Vzamemo $a \in K$ in $x \in q^{-1}(J)$. Potem je $a + I \in K/I$ in $x + I \in J$.

$$q(a \cdot x) = (a \cdot x) + I = (a + I)(x + I) \in J \implies ax \in q^{-1}(J)$$

□

Pokazali smo, da so ideali v K/I natanko ideali oblike J/I. J je torej natanko ideal v K, ki vsebuje I, hkrati pa je $I \triangleleft J$.

Definicija 1.1.43 (Maksimalni ideal)**.** ***Maksimalni ideal*** *v kolobarju K je pravi ideal, ki ni vsebovan v nobenem drugem pravem idealu.*

Izrek 1.1.44. *Naj bo K kolobar in $I \triangleleft K$. K/I je obseg natanko takrat, ko je I maksimalni ideal v K.*

Dokaz. Vemo, da je K/I obseg natanko takrat, ko nima pravih idealov. Ker nima pravih idealov, ni idealov v K, ki bi vsebovali I, torej je I maksimalen ideal. □

Izrek 1.1.45. *Naj bo R obseg. $I \triangleleft R[x]$ je maksimalen natanko tedaj, ko je $I = (p(x))$ za nek nerazcepen polinom $p(x)$.*

Dokaz $\implies$. Vzamemo $p(x) = q(x) \cdot r(x) \in R[x]$, kjer je q nekonstanten nerazcepen polinom in r neničeln polinom. Ker je *st* $p \geq$ *st* q, je $(p) \triangleleft (q) \triangleleft R[x]$. □

Dokaz $\impliedby$. Naj bo $I = (p)$ za nek polinom $p \in R[x]$. Če ni maksimalen, je $(p) \triangleleft J \triangleleft R[x]$. Vsi ideali v $R[x]$ so glavni, zato je $J = (q)$ za nek $q \in R[x]$. Za q lahko predpostavimo, da nerazcepen. Torej je $p(x) = q(x) \cdot r(x)$ in *st* $q <$ *st* p, torej r ni konstanten. Sledi, da je p razcepen polinom. □

1.2 Obsegi

Obseg je komutativen kolobar, v katerem so vsi neničelni elementi obrnljivi. Stvari, ki nas zanimajo pri kolobarjih, npr. ulomki, ideali, kvocienti itd., so pri obsegih precej nezanimive. Namesto tega se bomo ukvarjali z bolj zanimivimi pojmi.

1.2.1 Razširitve obsegov

Definicija 1.2.1 (Razširitev obsega)**.** *Če je K podobseg obsega F, pravimo, da je F **razširitev** obsega K in pišemo $K \leq F$.*

Trditev 1.2.2. *Če je F razširitev obsega K, je F vektorski prostor nad K.*

Dimenzijo K-vektorskega prostora F $dim_K F$ običajno označimo z $[F : K]$. Če je dimenzija končna, pravimo, da je F **končne razširitev**, sicer pa je **neskončna razširitev** K.

Izrek 1.2.3. *Za obsege $K \leq F \leq E$ velja $[E : K] = [E : F] \cdot [F : K]$.*

Dokaz. Za neskončne razširitve je očitno, zato se omejimo na končne razširitve.

Naj bo $x_1, ..., x_m$ baza za F nad K in naj bo $y_1, ..., y_n$ baza za E nad F. Pokazati moramo, da je $\{x_i y_j \mid i = 1, ..., m, j = 1, ..., n\}$ baza E nad K.

Vzemimo $e \in E$. $e = f_1 y_1 + ... + f_n y_n$ za $f_1, ..., f_n \in F$. Obenem je $f_i = k_{i1} x_1 + ... + k_{im} x_m$ za $k_{ij} \in K$. Torej je $e = \sum_{i=1}^{n} \sum_{j=1}^{m} k_{ij} x_j y_i$.

Pokažimo tudi linearno neodvisnost baze. Recimo, da je linearno odvisna. Potem je $0 = \sum_{i=1}^{n} \sum_{j=1}^{m} k_{ij} x_j y_i$. Ker so y_i linearno neodvisni, ke $\sum_{j=1}^{m} = 0$. Ker so tudi x_j linearno neodvisni, je $k_{ij} = 0$ za vse i in j. □

Poglejmo si, kako izgleda najmanjša razširitev obsega K, ki vsebuje nek $a \in F$.

Trditev 1.2.4.

a) Najmanjši podkolobar F, ki vsebuje K in $a \in F$, je $K[a] = \{p(a) \mid p \in K[x]\}$.

b) Najmanjši podobseg F, ki vsebuje K in $a \in F$, je $K(a) = \{\frac{p(a)}{q(a)} \mid p, q \in K[x], q(a) \neq 0\}$.

Dokaz (a)*.* Vsak kolobar, ki vsebuje K in a, mora vsebovati tudi vse potence a in njihove K-linearne kombinacije $k_0 + k_1 a + ... + k_n a^n$. Nadaljevanje dokaza izpuščeno. □

Dokaz (b)*.* Obseg mora poleg K-linearnih kombinacij potenc a vsebovati še vse kvociente, katere predstavimo z ulomki oblike $\frac{p(a)}{q(a)}$. Konstruiramo obseg ulomkov. □

Kolobar lahko razširimo z več elementi $a_1, a_2, ..$ naenkrat. Takšne razširitve označimo z $K[a_1, a_2, ...]$ za kolobarje in $K(a_1, a_2, ...)$ za obsege. Vrstni red dodanih elementov je lahko v zapisu poljuben.

Definicija 1.2.5 (Enostavna razširitev)**.** *Razširitev obsega K je* ***enostavna,*** *če smo obsegu K dodali eden element $a \in F$.*

Definiramo poseben homomorfizem kolobarjev:

$$\phi_a \colon K[x] \to F$$
$$\phi_a \colon p(x) \mapsto p(a)$$

Zanima nas, ali je ϕ_a injektiven.

Če je ϕ_a injektiven, je $Kerf = \{0\}$, a ni ničla nobenega (netrivialnega) polinoma s koeficienti v K. Tedaj pravimo, da je a **transcendenten** nad K.

Če pa ϕ_a ni injektiven, potem obstaja netrivialen polinom s koeficienti v K, v katerem je a ničla. Tedaj pravimo, da je a **algebraičen** nad K.

Definicija 1.2.6 (Algebraična razširitev)**.** *Naj bo F razširitev nad obsegom K. Če so vsi elementi F algebraični nad K, pravimo, da je F* ***algebraična razširitev*** *nad K.*

Definicija 1.2.7 (Transcendentna razširitev)**.** *Naj bo F razširitev nad obsegom K. Če je vsaj eden element F transcendenten nad K, je F* ***transcendentna razširitev*** *nad K.*

Opomba. *Za dano število je običajno zelo težko dokazati, da je transcendentna nad $\mathbb{Q}$. Na primer, transcendentnost e je bila dokazana leta 1873, transcendentnost π je bila dokazana leta 1882, še vedno pa ne vemo, ali je $\pi + e$ transcendentna nad $\mathbb{Q}$.*

Izrek 1.2.8. *če je a transcendenten nad $K \leq F$, potem je $K[a] \cong K[x]$ in $K(a) \cong K(x)$.*

Bolj zanimive so algebraične razširitve.

Če je $a \in F$ algebraičen nad K, potem je $Ker\phi_a$ pravi ideal v $K[x]$. V $K[x]$ so vso ideali glavni, zato je $Ker\phi_a = (g)$ za nek polinom $g \in K[x]$. Če dodatno zahtevamo, da je g moničen (vodilni koeficient je 1), potem je g enolično določen in mu pravimo **minimalni polinom** za element a nad K in ga označimo z $g_a(x)$.

Po izreku o izomorfizmu velja

$$K[a] \cong K[x]/(g_a)$$

Zgled 1.2.9. $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(x^2 - 2)$, *ker je* $g_{\sqrt{2}}(x) = x^2 - 2$.

Lema 1.2.10. *Ideal $(g_a) \triangleleft K[x]$ je maksimalen.*

Dokaz. Pokazati moramo, da je g_a nerazcepen. Če bi veljalo $g_a(x) = p(x) \cdot q(x)$ za polinoma strogo nižje stopnje v $K[x]$, bi iz $0 = g_a(a) = p(a) \cdot q(a)$ dobili $p \in Ker\phi_a$ ali $q \in Ker\phi_a$. To je v protislovju z zahtevo, da g_a deli p in q. $\square$

Posledica 1.2.11. *$K[x]/(g_a)$ je obseg, torej $K(a) \cong K[a]$.*

Zato je $K[x]/(g_a)$ vektorski prostor z bazo $1+(g_a), x+(g_a), ..., x^{n-1}+(g_a)$, kjer je n stopnja polinoma g_a. Izomorfize, $\overline{\phi_a}$ to bazo preslika v elemente $1, a, ..., a^{n-1} \in F$.

Ugotovitve povzemimo v naslednjem izreku.

Izrek 1.2.12. *Naj bo $a \in F$ algebraični element nad $K \leq F$*

a) Obstaja natanko določen monični polinom $g_a \in K[x]$, ki deli vse polinome, ki imajo a za ničlo.

b) $K(a) \cong K[a] \cong K[x]/(g_a)$

c) $[K(a) : K] = deg_K g_a$ je stopnja a nad K (pišemo $deg_K a$). Za bazo $K(a)$ lahko vzamemo $1, a, ..., a^{n-1}$, kjer je $n = deg_K a$.

Posledica 1.2.13. *Če je F končna razširitev K, potem za vsak $a \in F$ velja $deg_K a \mid [F : K]$*

Dokaz. Iz $K \leq K(a) \leq F$ sledi $[F : K] = [F : K(a)] \cdot [K(a) : K] = [F : K(a)] \cdot deg_K a$. $\square$

Videli smo, da so vse transcendentne razširitve neskončne, enostavne algebraične razširitve pa končne. Splošne algebraične razširitve so pa lahko tudi neskončne.

Izrek 1.2.14.

a) Vsaka končna razširitev je algebraična.

b) Naj bo $K \leq F$ razširitev obsega. Če je $A \subseteq F$ podmnožica števil, ki so algebraična nad K, potem je $K(A)$ algebraična raširitev K.

c) Če je F algebraična razširitev K in je E algebraična razširitev F, potem je E algebraična razširitev K.

Dokaz (a). Naj bo $[F : K]$ in $a \in F$. Potem je množica $\{1, a, ..., a^n\}$ linearno odvisna, torej obstaja netrivialna K-linearna kombinacija

$$k_0 1 + k_1 a + ... + k_n a^n = 0$$

Torej je a algebraičen nad K. $\square$

Dokaz (b). Vsak element $a \in K(A)$ se da zapisati kot

$$a = \frac{p(a_1, a_2, ..., a_n)}{q(a_1, a_2, ..., a_n)}$$

za primerno izbrane polinome $p, q \in K[x_1, x_2, ..., x_n]$ in $a_1, a_2, ..., a_n \in A$. To pomeni, da je $a \in K(a_1, ..., a_n)$, ki je končna razširitev K. Po (1) je a algebraična nad K. □

Dokaz (c). Naj bo $a \in E$. Po privzetku obstaja $p(x) = a_0 + a_1 x + ... + a_n x^n \in F[x]$, za katerega je $p(a) = 0$. To pomeni, da je a algebraičen nad $K(a_1, ..., a_n)$, ki je končna algebraična razširitev K. Sledi, da je tudi a algebraičen nad K. □

Definicija 1.2.15 (Algebraično zaprt obseg)**.** *Če dani obseg nima nobene prave algebraične razširitve oz. nad njim ni algebraičnih števil, je ta obseg **algebraično zaprt**.*

Definicija 1.2.16 (Algebraično zaprtje)**.** *Najmanjša razširitev obsega K, ki je algebraično zaprta, je **algebraično zaprtje** obsega K.*

1.2.2 Razpadni obsegi

Definicija 1.2.17 (Razpadni obseg polinoma)**.** *Naj bo K obseg in $p \in K[x]$. **Razpadni obseg polinoma** je najmanjša razširitev K, ki vsebuje vse ničle polinoma p.*

Privzemimo, da je $p \in K[x]$ nerazcepen. Potem je $K[x]/(p(x))$ razširitev, v kateri je $a := x + (p(x))$ ničla polinoma $p(x)$.

$p(x)$ lahko delimo z $(x-a)$ in dobimo kvocient s koeficienti v $K[x]/(p(x))$. Postopek ponavljamo, dokler (po največ *deg* p korakih) ne dobimo razširitve F, v kateri $p(x)$ razpade na linearne faktorje. Lahko se zgodi, da smo dodali preveč ničel, zato vzamemo najmanjši podobseg F, ki vsebuje K in vse ničle $p(x)$.

Končni rezultat je neodvisen od zaporedja razširitev, zato je razširitev enolično določena.

Pokazali bomo, da vsak končni obseg dobimo kot razpadni obseg točno določenega polinoma nad $\mathbb{Z}_p$.

1.2.3 Končni obsegi

Naj bo F končni obseg. Njegova karakteristika je $p = char\ F$ in F je končno razsežni vektorski prostor nad $\mathbb{Z}_p$. Sledi, da ima F natanko p^n elementov, kjer je $n = [F : \mathbb{Z}_p]$.

Izrek 1.2.18. *Za vsak n obstaja razširitev stopnje n obsega $\mathbb{Z}_p$. Vsaka takšna razširitev je izomorfna razpadnemu obsegu polinoma $x^{(p^n)} - x \in \mathbb{Z}_p[x]$.*

Dokaz. Opazimo, da ima $x^{(p^n)} - x$ same različne ničle. Če bi imel večkratno ničlo, potem bi imel skupnega delitelja s svojim odvodom:

$$(x^{(p^n)} - x)' = p^n x^{p^n - 1} - 1 \equiv -1 \ (modp)$$

$x^{p^n} - x$ ima n različnih ničel. Trdimo, da te ničle tvorijo obseg. Če $x = x^{p^n}$ in $y = y^{p^n}$, potem očitno enako velja tudi za $x \cdot y$ in x/y. Vendat tudi $x \pm y$ ustrezata temu pogoju, ker je $(x \pm y)^{p^n} \equiv x^{p^n} \pm y^{p^n} (mod\ p)$.

Sklepamo, da množica ničel obseg in sicer ravno razpadni obseg polinoma $x^{p^n} - x$.

Obratno, če ima F p^n elementov, potem elementi F zadoščajo enačbi $x \cdot (x^{p^n} - 1) = 0$, torej F vsebuje vse ničle $x^{p^n} - x$ in je po izreku o enoličnosti izomorfen $\mathbb{Z}_p(x^{p^n} - x)$. □

Definicija 1.2.19 (Galoisov obseg)**.** *Končni obsegi moči p^n so* ***Galoisov obseg*** *$GF(p^n)$.*