Izbrana poglavja iz matematike

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

Junij 2020

1 Abstraktna algebra: kolobarji in obsegi

Definicija 1.1 (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 1.2 (Obseg)**.** *Kolobarju, v katerem je množenje asociativno, komutativno in ima enoto ter ima operacijo deljenja, rečemo* ***obseg****.*

1.1 Kolobarji

Zgled 1.3. *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 1.4 (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 1.5 ($\mathbb{Z}_{12}$: ostanki po modulu 12)**.**

$$2 \cdot 6 = 0$$

$$3 \cdot 8 = 0$$

Definicija 1.6 (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 1.7. *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 1.8 (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 1.9. $\mathbb{Z}$ *nima deliteljev niča, obrnljiva pa sta le* 1 *in* -1*.*

Zgled 1.10. $\mathbb{Z}_{12}$

- *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 1.11 (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 1.12. *$\mathbb{Z}_n$ je obseg $\Leftrightarrow$ n je praštevilo.*

Definicija 1.13 (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 1.14. *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 1.15. *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 1.16. *$\mathbb{Z} \xrightarrow{mod\ n} \mathbb{Z}_n$ je homomorfizem (dokaz ponovi korake dokaza, da je $\mathbb{Z}_n$ kolobar).*

Zgled 1.17. *Konjugiranje $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ je izomorfizem kolobarjev.*

Zgled 1.18. *Za poljuben $a \in \mathbb{R}$ definiramo f_a: $\mathbb{Z}[x] \to \mathbb{R}$ 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 1.19. $a \mapsto \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ *je homomorfizem $\mathbb{R} \to M_2(\mathbb{R})$.*

Zgled 1.20. *Splošneje f_a: $\mathscr{C}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ s predpisom $f_a(g) := g(a)$ je tudi homomorfizem kolobarjev.*

Zgled 1.21. $a \mapsto \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$ *<u>ni</u> homomorfizem $\mathbb{R} \to M_2(\mathbb{R})$ (ohranja seštevanje, ne pa množenja).*

Zgled 1.22. *Preslikava $\mathbb{C} \to M_2(\mathbb{R})$ s predpisom $a + bi \mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ je homomorfizem.*

Zgled 1.23. *$a \mapsto a^p$ je homomorfizem $\mathbb{Z}_p \to \mathbb{Z}_p$ (p praštevilo).*

Trditev 1.24. *Za homomorfizem f: $K \to L$ 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 1.25 (Unitalen homomorfizem)**.** *Homomorfizem, za katerega velja $f(1) = 1$, je* ***unitalen****.*

Trditev 1.26. *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 1.27. *Naj bo f: $K \to L$ homomorfizem kolobarjev. Potem je Imf 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. □

Trditev 1.28. *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 $x \cdot y \in Kerf$. □

Definicija 1.29 (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 $I \lhd K$.*

Zgled 1.30. *$\{0\} \lhd K$ in $K \lhd K$ sta "neprava"ideala.*

Zgled 1.31. *$n\mathbb{Z} \lhd \mathbb{Z}$*

Zgled 1.32. *$\{a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n \mid a \in \mathbb{R}\} \lhd \mathbb{R}[x]$ so polinomi, za katere je $p(0) = 0$. Splošneje, za $a \in K$ je $\{p \in K[x] \mid p(a) = 0\} \lhd K[x]$.*

Zgled 1.33. $\{\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \mid x, y \in \mathbb{R}\} \subseteq M_2(\mathbb{R})$ *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 1.34. *Naj bo f: $K \to L$ 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 $a \cdot x \in Kerf$. □

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

Trditev 1.36. *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. □

Definicija 1.37 (Glavnoidealski kolobar)**.** *Kolobar, v katerem so vsi ideali glavni, je* ***glavnoidealski****.*

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

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

Trditev 1.38. $\sim$ *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 $a \sim b, b \sim c \implies a \sim c$. □

Definicija 1.39 (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 1.40. *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 1.41 (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. $Kerf \triangleleft K$ že vemo.

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

$\overline{f}$ je aditivna:

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

Za množenje opravimo analogni razmislek.

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

$\overline{f}$ je torej injektivna.

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

$\overline{f}$ je surjektivna. □

Trditev 1.42. *Komutativen kolobar K je obseg natanko tedaj, ko nima pravih idealov (tj. edina ideala sta (0) in K).*

Dokaz $\implies$. 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 $\impliedby$. 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 1.43. *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 1.44 (Maksimalni ideal)**.** ***Maksimalni ideal*** *v kolobarju K je pravi ideal, ki ni vsebovan v nobenem drugem pravem idealu.*

Izrek 1.45. *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. □

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.

Definicija 1.46 (Razširitev obsega)**.** *Če je K podobseg obsega F, pravimo, da je F **razširitev** obsega K in pišemo $K \leq F$.*

Trditev 1.47. *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 1.48. *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 1.49.

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 1.50 (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 $Ker f = \{0\}$, torej a ni ničla nobenega (trivialnega) 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 1.51 (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 1.52. *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 1.53. *če je a transcendenten nad $K \leq F$, potem je $K[a] \cong K[x]$ in $K(a) \cong K(x)$.*