IZBRANA POGLAVJA IZ MATEMATIKE

I KOLOBARJI IN OBSEGI

števila
polinomi
vektorji
matrike
funkcije

Kaj imajo skupnega?
Razlike?

seštevanje / odštevanje	neproblematično
množenje / deljenje	množenje v glavnem gre (vendar skalarni produkt vektorjev ni vektor, pri matrikah je potrebno paziti na dimenzijo ....)
odvajanje / integriranje	... morda polinomi, funkcije

Večini primerov je skupno, da lahko seštevamo / odštevamo in množimo. Pri tem veljajo običajna računska pravila

- - pri seštevanju ni pomemben vrstni red $(a+b=b+a)$ in združevanje $((a+b)+c=a+(b+c))$
  - imamo tudi ničelni element $a+0=a$ in nasprotne elemente $a+(-a)=0$
  - odštevamo tako, da prištejemo nasprotni element $a-b:=a+(-b)$
- pri množenju združujemo običajno $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, vrstni red pa je včasih pomemben (npr. pri matrikah)
- običajna zveza med seštevanjem in množenjem

$$(a+b)\cdot c=a\cdot c+b\cdot c \quad \text{in} \quad a\cdot(b+c)=a\cdot b+a\cdot c$$

Spoznali bomo, da nas iskanje stičnih točk pripelje do boljšega razumevanja vseh omenjenih struktur. Npr. polinomi bodo primerljivi s celimi števili, racionalne funkcije pa z ulomki. Tudi matrike bomo razumeli kot svojevrstna števila na ~~katerih~~ lahko definiramo polinome in druge, bolj zapletene funkcije (sin$x$, e^x, ...)

Kolobar K je množica, v kateri lahko seštevamo in množimo. Včasih pišemo $(K, +, \cdot)$.

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

Pri množenju nimamo dodatnih zahtev, razen ugla̋enosti s seštevanjem – distributivnost

Če ima množenje kakšno dodatno lastnost, potem po njej običajno poimenujemo podtip kolobarja

množenje je asociativno $\rightsquigarrow$ asociativni kolobar
je komutativno $\rightsquigarrow$ komutativni kolobar
ima enoto $\rightsquigarrow$ kolobar z enoto
vsak $0 \neq a \in K$ ima nasprotnega a^{-1} $\rightsquigarrow$ kolobar z deljenjem

Večinoma bomo obravnavali kolobarje, ki so asociativni in imajo enoto, zato tega ne bomo posebej poudarjali in jim bomo rekli kar kolobarji.
V splošnem pa ne bomo privzeli ne komutativnosti ne deljenja, zato bomo te lastnosti vedno izrecno navedli.
Kolobarju, ki ima vse štiri lastnosti bomo rekli obseg

Primeri

- cela števila $\mathbb{Z}$ — komutativni kolobar
- soda števila $2\mathbb{Z}$ — komutativni kolobar brez enote
- racionalna števila $\mathbb{Q}$; tudi $\mathbb{R}, \mathbb{C}$ — obsegi
- polinomi (s koeficienti v $\mathbb{Z}, \mathbb{Q}, ..$) $K[x]$ — kom. kolobar
- matrike $n \times n$ $M_n(K)$ — kolobar
- vektorji v $\mathbb{R}^3$ $(\mathbb{R}^3, +, \times)$ — neasociativni kolobar
- zvezne funkcije $f: \mathbb{R} \to \mathbb{R}$ — komutativni kolobar
  (kateri elementi so obrnljivi?)

Če kolobar nima enote, mu jo lahko preprosto dodamo:

K kolobar brez enote

Če dodamo 1, smo "prisiljeni" dodati tudi $-1, 2, -2, 3, \ldots$

na $\mathbb{Z} \times K$ vpeljemo $(n, a) + (m, b) := (n+m, a+b)$

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

ničla je $(0,0)$, nasprotni element $-(n, a) = (-n, -a)$

enota je $(1, 0)$

Če je K komutativen oz. asociativen, je to tudi $\mathbb{Z} \times K$.

Kaj dobimo, če je K že imel enoto?

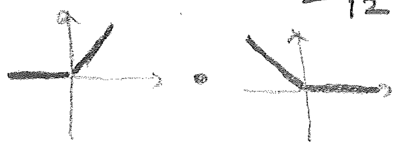
Kaj pa, če imamo kolobar, v katerem nekateri elementi niso obrnljivi in bi želeli dodati še njihove inverze (tako kot $\mathbb{Z}$ dodamo še ulomke in dobimo $\mathbb{Q}$).

Npr., če za $a, b \in K$, $b \neq 0$ vpeljemo simbole $\frac{a}{b}$ s katerimi računamo $\frac{a}{b} + \frac{a'}{b'} := \frac{ab' + a'b}{bb'}$ in $\frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}$

Pojavi se težava: kaj, če je $bb' = 0$, čeprav $b \neq 0$ in $b' \neq 0$?

Tega pri številih nismo vajeni, vendar

- matrike: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

- ostanki po modulu $\mathbb{Z}_{12}$ $\quad 2\cdot 6 = 0,\ 3\cdot 8 = 0, \ldots$
- funkcije  = ničelna funkcija

$0 \neq a \in K$ je delitelj niča, če obstaja $b \neq 0$, da je $a\cdot b = 0$

Delitelj niča ne more imeti inverza:
Če bi za $a \in K$ obstajala neničelna $b, c \in K$, da velja

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

bi dobili protislovje

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

Naj bo K komutativni kolobar brez deliteljev niča (celi kolobar)
tipični primeri: $\mathbb{Z}$, $\mathbb{R}[x]$, analitične funkcije ..
Tvorimo kolobar ulomkov $\bar{K}$:

elementi: $\frac{a}{b}$, vendar $\frac{a}{b} \equiv \frac{a'}{b'}$, če je $ab' = a'b$

ekvivalentni ulomki predstavljajo isti element $\bar{K}$

Operacije $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$, $\frac{a}{b}\cdot\frac{a'}{b'} = \frac{aa'}{bb'}$

Preverimo, da je $\bar{K}$ res obseg ...

Zakaj moramo enačiti sorazmerne ulomke?

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

dosej mora veljati $\frac{ka}{kb} \equiv \frac{a}{b}$.

<u>Primer</u> $\mathbb{Z} \rightsquigarrow \mathbb{Q}$

polinomi $\rightsquigarrow$ racionalne funkcije

Opazimo močno analogijo, ki jo še podkrepi podobna vloga Evklidovega algoritma pri določanju skupnih deliteljev

<u>OPOMBA</u> Z nekaj truda lahko vpeljemo ulomke tudi pri nekomutativnih kolobarjih in kolobarjih z delitelji niča.
Dobimo <u>kolobar ulomkov</u> (ne obseg)

Delitelj niča ne more biti obrnljiv, obrnljiv element pa ni delitelj niča. Ali je lahko element kolobarja še kaj, razen obrnljiv ali delitelj niča?

Seveda,

- $\mathbb{Z}$ nima deliteljev niča, obrnljiva sta le 1 in -1
- v $C(\mathbb{R},\mathbb{R})$ funkcija, ki ima ničlo ni obrnljiva, funkcija, ki ima končno ničel pa ni delitelj niča (zakaj?)
- kaj so delitelji niča v $M_n(\mathbb{R})$? Vse neobrnljive matrike
- $\mathbb{Z}_n$: npr. v $\mathbb{Z}_{12}$ — (0), 2, 3, 4, 6, 8, 9, 10 delitelji niča; 1, 5, 7, 11 obrnljivi ($1\cdot 1 = 5 \cdot 5 = 7\cdot 7 = 11 \cdot 11 = 1$)

V končnih kolobarjih ni drugih možnosti, zato dobimo znameniti

__Wedderburnov izrek__ (1905), Joseph Wedderburn 1882-1948

Končen kolobar brez deliteljev niča je obseg.

__Dokaz__

K končen, brez deliteljev niča

vsi elementi $K-\{0\}$ so obrnljivi

za poljuben $a \in K-\{0\}$ si ogledamo funkcijo

$l_a : K-\{0\} \to K$, $l_a(x) := a \cdot x$

- zaloga vrednosti l_a je $\subseteq K-\{0\}$, ker ni deliteljev niča
- $l_a(x) = l_a(y) \Leftrightarrow ax = ay \Rightarrow a(x-y) = 0 \Rightarrow x = y$, torej je l_a injektivna
- $\Rightarrow l_a : K-\{0\} \to K-\{0\}$ je bijektivna

Posebej, obstaja (natanko določen) a', da je $a \cdot a' = 1$

Analogno sklepamo za $d_a : K-\{0\} \to K$, $d_a(x) := x \cdot a$ in dobimo a'', da je $a'' \cdot a = 1$.

Iz $a'' = a'' \cdot \underbrace{(a \cdot a')}_{1} = \underbrace{(a'' \cdot a)}_{1} \cdot a' = a'$ sledi $a' = a'' = a^{-1}$

$\rightsquigarrow$ K je kolobar z deljenjem

Če je K komutativen, je obseg

Dokaz komutativnosti zahteva nekaj dodatne teorije grup, zato ga opustimo. Ideja je, da je center $Z(K)$ (elementi K, ki komutirajo z vsemi elementi K) obseg, cel K pa je vektorski prostor nad $Z(K)$. Iz primerjave multiplikativnih grup $(K-\{0\},\cdot)$ in $(Z(K)-\{0\},\cdot)$ se da izpeljati, da je K 1-razsežen nad $Z(K)$, tj $K=Z(K)$. Ta del opustimo.

☑

Očitna posledica: $\mathbb{Z}_n$ je obseg $\Leftrightarrow$ n je praštevilo

Karakteristika kolobarja K je najmanjši $n\in\mathbb{N}$, da za vsak $a\in K$ velja $na = \underbrace{a+\dots+a}_{n} = 0$. Oznaka: $\mathrm{char}(K)=n$. Če tak n ne obstaja, potem pišemo $\mathrm{char}(K)=0$.

Trditev

(a) Če $1\in K$, potem je $\mathrm{char}(K)$ = red enote = $\min n$, da je $\underbrace{1+\dots+1}_{n}=0$

(b) Če K nima deliteljev niča, potem je $\mathrm{char}\,K$ praštevilo ali 0

Dokaz

(a) $n1=0 \Rightarrow na=\underbrace{a+\dots+a}_{n} = (\underbrace{1+\dots+1}_{n})\cdot a = 0\cdot a = 0$

$\Rightarrow \mathrm{char}\,K\le n$; ker je red 1 enak n, sledi $\mathrm{char}\,K=n$

(b) Denimo $\mathrm{char}\,K = kl$ za $k,l>1$. Potem je

$0=kl1=(\underbrace{1+\dots+1}_{kl}) = (\underbrace{1+\dots+1}_{k})\cdot(\underbrace{1+\dots+1}_{l})$. Ker v K ni deliteljev niča, je $k1=0$ ali $l1=0$, zato je po (a) $\mathrm{char}\,K<kl$. Protislovje.

☑

Primer
- $\mathrm{char}\,\mathbb{Z}=0$; enako za $\mathbb{Q},\mathbb{R},\mathbb{C}$
- $\mathrm{char}\,\mathbb{Z}_n = n$
- $\mathrm{char}\,\mathbb{Z}_2\oplus\mathbb{Z}_2 = 2$
- $\mathrm{char}\,M_n(K) = \mathrm{char}\,K$

  $\mathrm{char}\,K[x] = \mathrm{char}\,K$ (oboje po točki (a) trditve)

Homomorfizmi

K, L kolobarja

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

$$f(a+b) = f(a) + f(b) \quad \text{in}$$
$$f(a \cdot b) = f(a) \cdot f(b) \quad \text{za poljubna } a, b \in K$$

Bijektivni homomorfizem je **izomorfizem**.

Primeri

- $\mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}_n$ premislek v bistvu ponovi korake dokaza, da je $\mathbb{Z}_n$ kolobar
- konjugiranje $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ je izomorfizem kolobarjev
- $a \in \mathbb{R}$, $f_a: \mathbb{Z}[x] \to \mathbb{R}$ $f_a(p) := p(a)$

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

Splošneje $f_a: C(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$, $f_a(g) := g(a)$ je tudi homomorfizem kolobarjev

- $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ je homomorfizem $\mathbb{R} \to M_2(\mathbb{R})$

$a \mapsto \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ <u>ni</u> homomorfizem kolobarjev (ohranja seštevanje, ne pa množenja)

- odvajanje $\mathbb{R}[x] \to \mathbb{R}[x]$ <u>ni</u> homomorfizem
- $\mathbb{C} \to M_2(\mathbb{R})$ $a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ je homomorfizem
- $a \mapsto a^p$ <u>je</u> homomorfizem $\mathbb{Z}_p \to \mathbb{Z}_p$ (p praštevilo)

Nekaj lastnosti homomorfizmov $f: K \to L$

- $f(0) = 0$, sledi iz $f(0) = f(0+0) = f(0) + f(0)$
- $f(-a) = -f(a)$, sledi iz $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$
- v splošnem ne zahtevamo $f(1) = 1$; če to vseeno velja pravimo, da je homomorfizem **unitalen**

$a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ ni unitalen (vsi ostali navedeni primeri so)

- f unitalen, a obrnljiv $\Rightarrow f(a)$ obrnljiv

Kot pri vseh funkcijah se tudi pri homomorfizmih vprašamo, kdaj so surjektivni oz. injektivni.

$f: K \to L$ homomorfizem

- zaloga vrednosti f je $f(K) = \{f(a) \mid a \in K\}$
  to je podkolobar v L (preverimo!), ki mu pravimo slika f, oznaka $\operatorname{Im} f$

  f je surjektivna $\iff \operatorname{Im} f = L$

- $f(a) = f(b) \rightsquigarrow f(a-b) = 0$ oz. $a - b \in f^{-1}(0)$

  $f^{-1}(0)$ je podkolobar v K, pravimo mu jedro f, $\operatorname{Ker} f$

  f je injektivna $\iff f^{-1}(0) = \{0\}$

  Vendar $\operatorname{Ker} f$ ni le podkolobar (tj. zaprt za $+, -, \cdot$)

  $$a \in K, x \in \operatorname{Ker} f \Rightarrow \begin{aligned} f(a \cdot x) &= f(a) \cdot f(x) = f(a) \cdot 0 = 0 \\ f(x \cdot a) &= f(x) \cdot f(a) = 0 \cdot f(a) = 0 \end{aligned}$$
  $$\Rightarrow a \cdot x, x \cdot a \in \operatorname{Ker} f$$

  $\rightsquigarrow$ $\operatorname{Ker} f$ je podkolobar, ki je zaprt za množenje s poljubnim elementom K

Podkolobar $I \leq K$ je ideal v K, če za vsak $a \in K, x \in I$ velja $a \cdot x \in I$ in $x \cdot a \in I$ (krajše: $K \cdot I \subseteq I$ in $I \cdot K \subseteq I$)
Oznaka: $I \triangleleft K$.
Videli bomo, da je pojem ideala ključen za študij kolobarjev (podobno podgrupam edinkam v teoriji grup)

Primeri:

- $\{0\} \triangleleft K$, $K \triangleleft K$ to sta "neprava" ideala
- $m\mathbb{Z} \triangleleft \mathbb{Z}$
- $\{a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_i \in \mathbb{R}\} \triangleleft \mathbb{R}[x]$; to so polinomi, za katere je $p(0) = 0$. Splošneje, za $a \in K$ je

  $$\{p \in K[x] \mid p(a) = 0\} \triangleleft K[x]$$

- podobno, za $A \subseteq \mathbb{R}$
$$\{ f \in C(\mathbb{R},\mathbb{R}) \mid f(A)=0 \} \triangleleft C(\mathbb{R},\mathbb{R})$$

- liha števila niso ideal v $\mathbb{Z}$

- $\left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \mid x,y \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$ je podkolobar
$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \pm \begin{pmatrix} x' & 0 \\ y' & 0 \end{pmatrix} = \begin{pmatrix} x \pm x' & 0 \\ y \pm y' & 0 \end{pmatrix} ; \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \cdot \begin{pmatrix} x' & 0 \\ y' & 0 \end{pmatrix} = \begin{pmatrix} xx' & 0 \\ yx' & 0 \end{pmatrix}$$
Poleg tega je
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} ax+by & 0 \\ cx+dy & 0 \end{pmatrix}, \text{ vendar}$$
$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} xa & xb \\ ya & yb \end{pmatrix}$$
Idealska lastnost je izpolnjena le za množenje z elementi kolobarja z leve, ne pa z desne.

Pri nekomutativnih kolobarjih ločimo leve ideale (velja $K \cdot I \subseteq I$), desne ideale ($I \cdot K \subseteq I$) in dvostranske ideale.

Matrike, kjer so izbrani stolpci ničelni so levi ideali v $M_n(K)$. Podobno so matrike, kjer so izbrane vrstice ničelne desni ideali v $M_n(K)$.
Kaj so dvostranski ideali v $M_n(K)$?

- Jedro homomorfizma je vedno dvostranski ideal.

- 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 ta ni zaprt za seštevanje. Potrebno je vzeti vse možne vsote izrazov $a \cdot x \cdot b$ ...

Ideal, ki je generiran z enim elementom imenujemo <u>glavni ideal</u>. Pišemo $(x) :=$ ideal generiran z $x \in K$.

<u>Primer</u>

- v $\mathbb{Z}$ so vsi ideali glavni
  $I \triangleleft \mathbb{Z}$; če $I = \{0\}$, potem $I = (0)$
  v nasprotnem primeru obstaja najmanjše pozitivno število $a \in I$.
  <u>a deli vse elemente I</u>
  Res, če je tudi $b = k \cdot a + r$, $0 < r < a$ element I, potem je tudi $r = b - k \cdot a \in I$, protislovje.
  $\Rightarrow I = (a)$
- D.N. tudi v $\mathbb{R}[X]$ so vsi ideali glavni
  (namig, Evklidov algoritem)

Kolobar, v katerem so vsi ideali glavni je <u>„glavnoidealski"</u>

Ključna lastnost dvostranskih idealov je, da lahko tvorimo kvocientne kolobarje (analogija s podgrupo edinko).

$I \triangleleft K$ dvostranski ideal
Na K vpeljemo relacijo $\sim$: $a \sim b$, če je $a - b \in I$
<u>$\sim$ je ekvivalenčna relacija</u>
$a \sim a$, ker je $a - a = 0 \in I$
$a \sim b \Rightarrow b \sim a$, ker iz $a - b \in I$ sledi $b - a \in I$
$a \sim b, b \sim c \Rightarrow a \sim c$, ker iz $a - b, b - c \in I$ sledi $a - c \in I$

Množico ekvivalenčnih razredov označimo s $K/_I$

Ekvivalenčni razred elementa $a \in K$ označimo $[a]$, ali $a + I$
(ker $b \in [a]$ pomeni $b \sim a$, oz. $b - a \in I$, torej $b = a + x$ za nek $x \in I$)
Zato je $[a] = \{a + x \mid x \in I\} \equiv a + I$.

Elemente $K/_I$ naravno seštevamo in množimo:

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

Operaciji sta neodvisni od izbire predstavnikov:

$$\left.\begin{array}{l} a'+I=a+I \\ b'+I=b+I \end{array}\right\} \rightsquigarrow \begin{array}{l} a-a'\in I \\ b-b'\in I \end{array} \rightsquigarrow (a+b)-(a'+b')\in I \rightsquigarrow (a+b)+I=(a'+b')+I$$

$$\Downarrow$$

$$\begin{array}{l} a'=a+x \\ b'=b+y \end{array} \text{ za } x,y\in I \rightsquigarrow a'b'=ab+\underbrace{a\cdot y+x\cdot b+x\cdot y}_{\in I},$$

ker je I dvostranski ideal

$$\rightsquigarrow a'b'+I=a\cdot b+I$$

Ko vemo, da sta $+,\cdot$ dobro definirani, lahko brez težav preverimo, da je $(K/_I,+,\cdot)$ res kolobar.

Primer

- $n\mathbb{Z}=(n)\lhd\mathbb{Z}$; $\mathbb{Z}/_{(n)}\cong\mathbb{Z}_n$
- $K/_{\{0\}}\cong K$, $K/_K\cong\{0\}$
- $\mathbb{R}[x]/_{(x)}\cong\mathbb{R}$
- $\mathbb{R}[x]/_{(x^2)}\cong\mathbb{R}\oplus\mathbb{R}x=\{a+bx\in\mathbb{R}[x]\}$ z običajnim seštevanjem

  in množenjem $(a+bx)\cdot(a'+b'x)=aa'+(ab'+a'b)x$
- $\mathbb{R}[x]/_{(x^2+1)}=\ ?$

  $p(x)=(x^2+1)\cdot q(x)+\underbrace{(a+bx)}_{\text{ostanek}}$, zato $p(x)+I=(a+bx)+I$

  za $x+I$ velja $(x+I)^2=x^2+I=-1+I$, ker je $x^2+1\in I$

  $\mathbb{R}[x]/_{(x^2+1)}\cong\mathbb{C}$

Namesto (lahkega) dokaza, raje izpeljemo izrek, ki sistematično rešuje podobne primere.

IZREK (o izomorfizmu)

$f: K \to L$ poljuben homomorfizem kolobarjev

Potem je $\operatorname{Ker} f \triangleleft K$ in imamo naravni izomorfizem

$$\bar{f} : K/_{\operatorname{Ker} f} \longrightarrow \operatorname{Im} f \ , \ \bar{f}(x + \operatorname{Ker} f) := f(x)$$

Dokaz

$\operatorname{Ker} f \triangleleft K$ že vemo.

- Korektnost definicije $\bar{f}$: za $u \in \operatorname{Ker} f$ je $f(x+u) = f(x)$, zato je definicija $\bar{f}(x + \operatorname{Ker} f)$ neodvisna od predstavnika razreda
- $\bar{f}$ je aditivna: $\bar{f}((x+\operatorname{Ker} f)+(y+\operatorname{Ker} f)) = \bar{f}((x+y)+\operatorname{Ker} f) = f(x+y) =$
  $= f(x) + f(y) = \bar{f}(x+\operatorname{Ker} f) + \bar{f}(y + \operatorname{Ker} f)$
  in podobno za množenje
- $\operatorname{Ker} \bar{f} = \{x + \operatorname{Ker} f \mid \underbrace{\bar{f}(x+\operatorname{Ker} f)}_{= f(x)} = 0\} = \{0 + \operatorname{Ker} f\} \leadsto \bar{f}$ injektivna

  $\operatorname{Im} \bar{f} = \operatorname{Im} f$, $\bar{f}$ je surjektivna

$\blacksquare$

Primer

Definiramo $f : \mathbb{R}[x] \to \mathbb{C}$, $p(x) \longmapsto p(i)$ videli smo že, da je to homomorfizem

- f je surjektivna, ker je $a + bi = f(a+bx)$
- $\operatorname{Ker} f = ?$ $p(i) = 0 \Rightarrow (x-i) \mid p(x)$

  $p(x)$ ima realne koeficiente, zato tudi $p(-i) = 0$, torej $(x+i) \mid p(x)$

  $\leadsto (x^2+1) \mid p(x) \leadsto \operatorname{Ker} f = (x^2+1)$

Po izreku o izomorfizmu je

$$\bar{f} : \mathbb{R}[x]/_{(x^2+1)} \xrightarrow{\cong} \mathbb{C}$$

S to konstrukcijo bomo dobili praktično vse primere obsegov.
Kako vemo, kdaj je K/I obseg?
(Odslej se omejimo na komutativne kolobarje).

<u>Trditev</u>
(Komutativni) kolobar K je obseg $\Leftrightarrow$ K nima pravih idealov.

<u>Dokaz</u>

$(\Rightarrow)$ $I \triangleleft K \rightsquigarrow \underline{I=(0) \text{ ali } I=K}$

Denimo $I \neq (0)$: potem obstaja $0 \neq x \in I$. Ker je x obrnljiv (smo v obsegu), potem za vsak $a \in K$ velja $a = (a \cdot x^{-1}) \cdot x \in I$, torej je $I = K$.

$(\Leftarrow)$ Naj bo $0 \neq a \in K$. Potem je $(a) = K \cdot a = a \cdot K$ ideal v K. Ker v K ni pravih idealov, je $(a) = K$, torej obstaja a', da je $a'a = aa' = 1$ $\rightsquigarrow$ a je obrnljiv.

$\boxed{//}$

Kaj so ideali v K/I? Označimo
$$\varrho : K \longrightarrow K/I$$
$$x \longmapsto x + I$$

<u>Če je $J \triangleleft K$, potem je $\varrho(J) \triangleleft K/I$</u>

$$a \in K,\ x \in J \rightsquigarrow \underbrace{(a+I)}_{\in K/I}\underbrace{(x+I)}_{\in \varrho(J)} = ax + I \in \varrho(J) \quad \text{(idealska lastnost)}$$

<u>Če je $J \triangleleft K/I$, potem je $\varrho^{-1}(J) \triangleleft K$ in $I \triangleleft \varrho^{-1}(J)$</u>

$$a \in K,\ x \in \varrho^{-1}(J) \rightsquigarrow \varrho(a \cdot x) = ax + I = \underbrace{(a+I)}_{\in K/I} \cdot \underbrace{(x+I)}_{\in J} \in J$$
$$\rightsquigarrow a \cdot x \in \varrho^{-1}(I)$$

<u>Trditev</u>
Funkcija $\{\text{ideali v } K, \text{ ki vsebujejo } I\} \longrightarrow \{\text{ideali v } K/I\}$
$$J \longmapsto \varrho(J)$$
je bijekcija.

$\boxed{/}$

Izrek

$I \triangleleft K$

K/I je obseg $\iff$ I je maksimalni ideal v K
(tj. pravi ideal v K, ki ni vsebovan v nobenem večjem pravem idealu)

Dokaz

K/I obseg $\iff$ K/I nima pravih idealov
$\iff$ K nima pravih idealov, ki vsebujejo I

$\boxed{/}$

Primeri

- v $\mathbb{Z}$ so vsi ideali glavni; oblike $(n) = n\mathbb{Z}$ za nek $n \in \mathbb{Z}$

  (n) je maksimalen $\iff$ n je praštevilo

  $(\Rightarrow)$ če je $n = k \cdot l$ za $1 < k, l < n$, potem je
  $(n) \underset{\neq}{\triangleleft} (k) \underset{\neq}{\triangleleft} \mathbb{Z}$, torej (n) ni maksimalen

  $(\Leftarrow)$ n praštevilo; če je $(n) \subseteq (k) \subseteq \mathbb{Z}$, potem
  $k | n \Rightarrow k = n$ ali 1; $\left.\begin{array}{l} k = n \Rightarrow (k) = (n) \\ k = 1 \Rightarrow (k) = \mathbb{Z} \end{array}\right\} \rightsquigarrow (n)$ je maks.

  Alternativno bi se lahko sklicali na izrek
  (n) je maksimalen $\iff$ $\mathbb{Z}/(n) = \mathbb{Z}_n$ je obseg $\iff$ n je praštevilo

- v $\mathbb{C}[X]$ so vsi maksimalni ideali oblike $(x - z)$ za $z \in \mathbb{C}$

  $(x-z)$ je maksimalen $\quad f_z : \mathbb{C}[x] \to \mathbb{C}$, $p(x) \mapsto p(z)$ $\quad \left.\begin{array}{l}\text{surjektivna} \\ (x-z) = \operatorname{Ker} f_z\end{array}\right\}$
  $\rightsquigarrow (x-z)$ je max

  $I \triangleleft \mathbb{C}[x]$ ~~maksimalen~~ $\Rightarrow I = (p(x))$; če $p(x)$ ni linearen
  je $p(x) = (x-z) q(x)$, kjer $q(x)$ ni konstanta
  $\Rightarrow (p) \underset{\neq}{\triangleleft} (q) \underset{\neq}{\triangleleft} \mathbb{C}[x]$

Podobno velja tudi za polinome več spremenljivk.
max ideali v $\mathbb{C}[x_1, \dots, x_n]$ so oblike $(x_1 - z_1, \dots, x_n - z_n)$
za $z_1, \dots, z_n \in \mathbb{C}$ <u>Nullstellensatz</u> (izrek o mestu ničel)

Izrek

R obseg; $I \trianglelefteq R[X]$ je maksimalen $\Leftrightarrow$ $I=(p(x))$ za nek nerazcepen polinom $p(x)$

($p(x) \in R[X]$ je razcepen, če je $p(x)=q(x)\cdot r(x)$ za nekonstantna polinoma $q(x), r(x) \in R[X]$

$x^2-3x-4=(x-4)(x+1)$

x^2+x+1 je nerazcepen v $\mathbb{R}[X]$ in razcepen v $\mathbb{C}[X]$)

Dokaz

($\Rightarrow$) $p(x)=q(x)\cdot r(x)$ $\rightsquigarrow$ $(p) \underset{\neq}{\trianglelefteq} (q) \underset{\neq}{\trianglelefteq} R[X]$

($\Leftarrow$) $I \trianglelefteq R[X]$, vsi ideali so glavni $\rightsquigarrow$ $I=(p)$

Če ni maksimalen, potem $(p) \underset{\neq}{\trianglelefteq} J \underset{\neq}{\trianglelefteq} R[X]$ in $J=(q)$

$\rightsquigarrow$ $p(x)=q(x)\cdot r(x)$

$\left.\begin{array}{l} \text{ker } (p) \neq (q) \text{, je } st(q) < st(p) \\ \text{ker pa je } (q) \neq R[X] \text{, je } st(q) > 0 \end{array}\right\}$ p je razcepen

$\boxed{/\!/}$

Primer

Ključno je, da imamo koeficiente v obsegu:

v $\mathbb{Z}[X]$, (x) ni maksimalen (ker $\mathbb{Z}[X]/_{(x)} \cong \mathbb{Z}$ ni obseg)

(px) za praštevilo p je maksimalen (ker $\mathbb{Z}[X]/_{(px)} \cong \mathbb{Z}_p$)