[KOLOBARJI IN POLJA]

$(R, +, \cdot)$. Če je $(R, +)$ abelova grupa in:

$\forall a, b \in R: \ a \cdot b \in R$

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

$\forall a, b, c \in R: \ a(b+c) = ab + ac$

$(a+b)c = ac + ab$

R je komutativen kolobar, če $\forall a, b \in R: \ ab = ba$

R je kolobar z enoto, če $\exists 1 \in R \ni: 1 \neq 0 \wedge \forall a \in R: 1a = a1 = a$

<u>Def:</u> Direktna vsota kolobarjev:

let R, S kolobarja. $R \oplus S$ je dir. vs. kol. in velja

$(R \oplus S, +, \cdot)$ kolobar.

elementi $R \oplus S$ so urejeni pari (r, s); $r \in R, s \in S$

$R \oplus S = R \times S$

definiciji operacij:

plus iz $R \oplus S$ plus iz R plus iz S

$(r, s) + (r', s') = (r + r', s + s')$

$(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$

<u>Trditev:</u> Če sta R in S kolobarja, je tudi $R \oplus S$ kolobar.

Nadalje: če sta R in S komutativna, je tudi $R \oplus S$.

če sta z enoto, je tudi $R \oplus S$.

<u>Def:</u> let R kolobar. $S \subseteq R$ je za iz R podedovani operaciji podkolobar, če je $(S, +, \cdot)$ kolobar in je S zaprta za odštevanje in množenje.

<u>Izrek:</u> let $(R, +, \cdot)$ kolob. in $S \subseteq R$. S je podkolobar $\Leftrightarrow$ velja vse to:

(cont.)

(1.) $0 \in S$

(2.) $a, b \in S \Rightarrow a - b \in S$

(3.) $a, b \in S \Rightarrow a \cdot b \in S$

<u>Def.</u>: let $(R, +, \cdot)$ kolobar. Center kolobarja:

$$Z(R) = \{a \in R : \forall x \in R : ax = xa\}$$

<u>Izrek</u>: Center kolobarja je vedno podkolobar.

[DELITELJI NIČA IN CELI KOLOBARJI]

$(\mathbb{Z}_n, +_n, \cdot_n)$ je za vsak n kolobar. (kolobar ostankov)

$\mathbb{Z}_6$: $2 \cdot 3 = 0$

<u>Definicija</u>: Če v kolobarju R velja $a \cdot b = 0$ in sta $a \neq 0$ in $b \neq 0$, sta a in b delitelja niča.

<u>Definicija</u>: PRAVILO KRAJŠANJA (v kolobarju):
(ne velja vedno, glej dve strani)

$$\forall a, b, c \in R, a \neq 0 : ab = ac \Rightarrow b = c$$

NTS Q zakaj ne $\Leftarrow$?

ANS: operacija je dobro definirana, zato $\Leftarrow$ vedno velja.

<u>Definicija</u>: R je CEL KOLOBAR, če je komutativen z enoto $1 \neq 0$ in nima deliteljev niča.

Primer: $(\mathbb{Z}, +, \cdot)$ je cel kolobar

$(\mathbb{Z}_6, +_6, \cdot_6)$ ni cel kolobar

<u>Izrek</u>: let R komutativen kolobar z enoto $1 \neq 0$. Velja R cel $\Longleftrightarrow$ v R velja pravilo krajšanja.

<u>Dokaz</u>:

(cont.)

($\Longrightarrow$) predpostavimo R CEL kom. kol. z en. $1 \neq 0$.

predpostavimo $ab = ac$ za $a \neq 0$ in polj. b, c.

$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b-c) = 0$

ker je a cel in $a \neq 0$, mora biti

$b - c = 0$, sicer bi bila a in $b-c$

delitelja niča, kar bi bilo v

protislovju s predpostavko.

$b - c = 0 \Longleftrightarrow b = c$.

torej $ab = ac \Rightarrow b = c$

($\Longleftarrow$) predpostavimo, da v kom. kol. z en R

velja pravilo krajšanja.

predpostavimo $ab = 0$, $a \neq 0$.

dokazati je treba $b = 0$, sicer bi imeli

delitelje niča:

$$ab = 0 = a \cdot 0$$

$$\cancel{a}b = \cancel{a}\,0 \quad \text{po pravilu krajšanja}$$

$$b = 0$$

Def: komutativen kolobar $(R, +, \cdot)$ z enoto $1 \neq 0$

je polje, če je vsak neničeln element obrnljiv

v $(R, \cdot)$ $\sim$ $(R \setminus \{0\}, \cdot)$ je abelova grupa.

Def: kolobar $(R, +, \cdot)$ z enoto $1 \neq 0$ je obseg, če

je vsak neničeln element obrnljiv v $(R, \cdot)$ $\sim$

$(R \setminus \{0\}, \cdot)$ je abelova grupa. (tu ne zahtevamo komutativnosti)

Trditev: Vsako polje je cel kolobar (nima deliteljev niča)

Dokaz: $(R,+,\cdot)$ polje $\Rightarrow$ nima deliteljev niča.
$a\cdot b = 0$

Naj velja $a\cdot b=0$, kjer je $a\neq 0$.

$a\neq 0 \Rightarrow$ polje $\Rightarrow \exists a^{-1} \Rightarrow$

$$a\cdot b = 0 \quad /a^{-1}$$
$$a^{-1}ab = 0$$
$$1b = 0$$
$$b = 0$$

Vsled te trditve dobimo alternativno definicijo polja:

Polje je cel kolobar, v katerem so vsi neničelni elementi obrnljivi ↳ zahteva komutativnost.

kolobar:

- $ab=ba$ → komutativen kolobar
- $a1=1a=a$, $1\neq 0$ → kolobar z enoto

komutativen kolobar & kolobar z enoto

↓ ni deliteljev niča

cel kolobar

↓ $\forall a\neq 0\ \exists a^{-1} \ni: aa^{-1}=a^{-1}a=1$

polje

NISO PA VSI CELI KOLOBARJI POLJA.

protiprimer: $(\mathbb{Z},+,\cdot)$ je cel kolobar, toda nimamo vseh inverzov za množenje. Toda velja za končni

Izrek: Če je $(R,+,\cdot)$ končen cel kolobar $\Rightarrow R$ polje.

Dokaz: let $(R,+,\cdot)$, $|R|<\infty$, R cel kolobar.

(cont.)

Dokažimo, da $\forall a \in R.\ a \neq 0\ \exists a^{-1} \ni: aa^{-1} = 1$

Naj bo a poljuben $\in R$, $a \neq 0$.

oglejmo si $\{a^k ; \forall k > 0\}$ množica vseh potenc a.

Ker $|R| < \infty \Rightarrow \exists i,j$, bss $i > j \ni: a^i = a^j$.

zdb. Ker je R končen, se nek element „ponovi".

$$a^j \cdot a^{i-j} = a^i = a^j = a^j \cdot 1$$

Ker je kolobar cel $\Rightarrow a^j \neq 0$ in ker velja pravilo krajšanja $\Rightarrow a^{i-j} = 1$, pri čemer vemo, da je $i-j > 0$. Dva podprimera:

case $i-j = 1$:
$a = 1 \Rightarrow a$ je inverz od a ✓

case $i-j > 1$:
$$a = a \cdot a^{i-j-1} = 1,$$ torej je a^{i-j-1} inverz od a. ✓

✓

Izrek: Za $n \in \mathbb{N}$, $n \geq 2$, NTSE:

(1) $\mathbb{Z}_n$ je cel kolobar $(\mathbb{Z}_n, +_n, \cdot_n)$

(2) $\mathbb{Z}_n$ je polje

(3) n je praštevilo

Dokaz: (1) $\Leftrightarrow$ (2) po prejšnjem izreku.

↳ $1 \Rightarrow 2$ vemo, $2 \Rightarrow 1$ prejšnji izrek

$1 \Leftrightarrow 3$ domača naloga: najdemo delitelje niča v nepraš. itd.

Primer končnega polja, ki ni praštevilske moči:

$$\mathbb{Z}_3(i) = \{a+bi : a,b \in \mathbb{Z}_3\} = \quad \boxed{i^2 = -1}$$
$$= \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$$

$(\mathbb{Z}_3(i), +, \cdot)$ → zmnožimo v $\mathbb{C}$ in koeficienta mod 3.

seštejemo v kompleksnem in koeficiente izračunamo po modulu 3.

$$(1+2i) + (2+2i) = i$$

<u>Def.</u>: Če je R polje in $S \subseteq R$, je S podpolje, če je S polje za od R podedovani operaciji.

Da je S podpolje v R zadošča preveriti:

$1 \in S$, kjer je 1 enota v R

$a,b \in S \Rightarrow a-b \in S$ (grupa za $+$)

$a,b \in S,\ b \neq 0 \Rightarrow ab^{-1} \in S$

Karakteristika kolobarja:

$(R,+,\cdot)$ kolobar, $a \in R$, $n \in \mathbb{N}$.

Zapis $n \cdot a$ pomeni $\underbrace{a+a+a+\dots+a}_{n\text{-krat}}$

↳ to ni element R

<u>Def.</u> Karakteristika kolobarja je najmanjši $n \in \mathbb{N}$ $\ni$: $\forall a \in R : n \cdot a = 0$. Če tak n ne obstaja, pravimo, da je R kolobar s karakteristiko 0.

Oznaka: $\operatorname{char} R$

primer: $\operatorname{char} \mathbb{Z} = 0$

$\operatorname{char} \mathbb{Z}_n = n$

Izrek: Naj bo $(R,+,\cdot)$ kolobar z enoto. Če je $\operatorname{red}(1)$ v grupi $(R,+)$ enak $n \Rightarrow \operatorname{char} R = n$

Dokaz:

$$\underbrace{1+1+\dots+1}_{n} = 0 \qquad \underbrace{1+\dots+1}_{m<n} \neq 0 \quad \text{po def. reda.}$$

$$a^n = e$$
$$a+\dots+a=0$$

od tod sledi, da je $\operatorname{char} R \geq \operatorname{red} 1$

Vzemimo $a \in R$ poljuben.

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

$$\operatorname{char} R \leq \operatorname{red} 1$$

$$\Rightarrow \operatorname{char} R = \operatorname{red} 1$$

IZREK: Če je R cel kolobar je bodisi $\operatorname{char} R = 0$ bodisi $\operatorname{char} R = p$, kjer je p praštevilo.

case $\operatorname{char} R = 0$: ✓

case $\operatorname{char} R = n > 0$:

PDDRAA $n = pq$, $p,q > 1$, $p,q \in \mathbb{N}$

po prejšnjem izreku $\operatorname{char} R = n = \operatorname{red} 1$

$$\Rightarrow 0 = n\cdot 1 = (pq)\cdot 1 = \underbrace{1+\dots+1}_{pq\text{-krat}} =$$

distributivnost:

$$= (\underbrace{1+\dots+1}_{p\text{-krat}})\cdot(\underbrace{1+\dots+1}_{q\text{-krat}}) = (p\cdot 1)(q\cdot 1) = 0$$

smo v celem kolob.

$$\Rightarrow p\cdot 1 = 0 \quad \text{ali} \quad q\cdot 1 = 0$$

↯, saj bi bil red 1 p ali q, kar je $< pq$

11:15

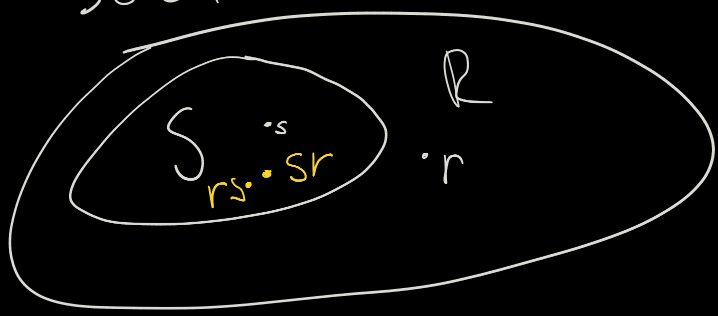
[IDEALI]

~ podobno kot podgrupa edinke

<u>Def.</u> Če je R kolobar, je njegov podkolobar S <u>ideal</u>, če velja $\forall r \in R, s \in S: rs, sr \in S$.

zdb: to je podkolobar, zaprt za zunanje množenje.

Skica:



Primer: $n \cdot \mathbb{Z}$ (večkratniki n) za fiksen n so ideal v $\mathbb{Z}$.

$\mathbb{Z}$ je podkolobar v $\mathbb{Q}$, toda ni ideal.

Kako preverimo, da je $I \subseteq R$ ideal?

$I \subseteq R$ je ideal $\iff$

$$0 \in I$$
$$\wedge \quad i, j \in I \Rightarrow i - j \in I$$
$$\wedge \quad i \in I, r \in R \Rightarrow ir \in I, ri \in I$$

let R kolobar in I, J ideala v .

let $I + J = \{ i + j : i \in I, j \in J \}$

let $I \cdot J = \{ i_1 j_1 + \dots + i_n j_n : i_1, \dots, i_n \in I, j_1, \dots, j_n \in J, n \in \mathbb{N} \}$

<u>Trditev:</u> Če je R kolobar, I, J ideala v R, sta $I + J$ in $I \cdot J$ spet ideala v R.

---

let R kolobar, I ideal v R.

$$R/I = \{ a + I, a \in R \}$$

v R/I vpeljemo operaciji takole:

aditivni odseki
$a + I = \{ a + i ; \forall i \in I \}$

$$(a+I) + (b+I) = a + b + I \qquad (*)$$
$$(a+I) \cdot (b+I) = ab + I$$

<u>IZREK:</u> Če je I ideal v R, je R/I za operaciji $(*)$ kolobar.

<u>Primer:</u> $R = M_{2\times 2}(\mathbb{Z})$ ... R so 2×2 matrike s celost. koef.

to je kolobar.

$I = M_{2\times 2}(\underline{2\mathbb{Z}})$ sodi koeficienti.

<u>I je ideal v R</u>

1.) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I$ ✓ enota za $+$ v R.

2.) za $A = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$ in $B = \begin{bmatrix} 2a' & 2b' \\ 2c' & 2d' \end{bmatrix}$

$$A - B = \begin{bmatrix} 2(a-a') & 2(b-b') \\ 2(c-c') & 2(d-d') \end{bmatrix} \in I \checkmark$$

3.) $A = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$ $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$

$$AB = \begin{bmatrix} 2(ax+bz) & 2(ay+bw) \\ 2(cx+dz) & 2(cy+dw) \end{bmatrix} \in I \checkmark$$

BA podobno $\in I$

sedaj si oglejmo R/I :

$$\underset{\substack{\downarrow \\ \text{neč } \in R}}{A} + I = \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} + \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix} ; \ a,b,c,d \in \mathbb{Z} \right\}$$

R/I ima 16 ekvivalenčnih razredov:

$$\begin{bmatrix} \text{sod/lih} & \text{sod/lih} \\ \text{sod/lih} & \text{sod/lih} \end{bmatrix}$$

$2 \cdot 2 \cdot 2 \cdot 2$