

Algebrske struktre

- **grupoid** (M, \cdot) urejen par z neprazno množico M in zaprto opreacijo \cdot .
- **polgrupa** grupoid z asociativno operacijo $\forall x, y, z \in M : (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- **monoid** polgrupa z enoto $\exists e \in M \ \forall x \in M : e \cdot x = x \cdot e = x$.
- **grupa** polgrupa v kateri ima vsak element inverz $\forall x \in M \ \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x = e$.
- **abelova grupa** grupa s komutativno operacijo $\forall x, y \in M : x \cdot y = y \cdot x$.

Kolobarji

Kolobar je množica R skupaj z dvema operacijama (oznaka: $+$, \cdot) tako, da velja:

- $(R, +)$ je abelova grupa
- $\forall a, b, c \in R : a(b + c) = ab + ac$ (distributivnost)
- $\forall a, b, c \in R : (a + b)c = ac + bc$ (distributivnost)
- $\forall a, b \in R : ab \in R$ (zaprtost množenja)
- $\forall a, b, c \in R : (ab)c = a(bc)$ (asociativnost*)
- $\exists e \in R \ \forall a \in R : e \cdot a = a = e \cdot a$ (enota*)

Kolobar je **komutativen**, če $\forall a, b \in R : ab = ba$. Kolobar je **kolobar z deljenjem**, če $\forall a \in R - \{0\} \ \exists a^{-1} \in R : aa^{-1} = 1$ element 1 je *enota kolobarja*.

Kolobar, ki ima vse naštete lastnosti je **obseg**.

Delitelji ničā in celi kolobarji

Naj bo R komutativen koloboar. Tedaj je $a \in R, a \neq 0$ **delitelj ničā**, če

$$\exists b \in R, b \neq 0 : ab = 0$$

Cel kolobar je komutativen kolobar z enoto ($1 \neq 0$), ki nima deliteljev ničā.

Razširitve kolobarjev

Naj bo K kolobar **brez enote**:

$$\begin{aligned} \mathbb{Z} \times K &= \{n \in \mathbb{Z}, a \in K \\ (n, a) + (m, b) &= (n + m, a + b) \\ (n, a) \cdot (m, b) &= (nm, nb + am + ab) \end{aligned}$$

Naj bo K komutativen kolobar *brez deliteljev ničā* vendar niso vsi elementi obrnljivi. Dodamo ulomke definirane kot ekvivalenčne razrede dvojic z ekvivalenčno (*refleksivno, simetrično, tranzitivno*) relacijo \sim .

$$\begin{aligned} K \times K - \{0\} / \sim \\ \frac{a}{b} \sim \frac{ka}{kb} \quad \forall k \in K - \{0\} \\ \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \\ \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'} \end{aligned}$$

Če bi bila b in b' delitelja ničā, bi imeli težave.

Tako dobimo **obseg ulomkov za K**.

Wedderburnov izrek

Končen kolobar brez deliteljev ničā je **obseg**.

Posledica: \mathbb{Z}_n je obseg $\iff n \in \mathbb{P}$

Karakteristika kolobarja

Karakteristika kolobarja R je najmanjši $n \in \mathbb{N}$, tako da velja

$$\forall a \in R : na = \underbrace{a + a + \dots + a}_{n\text{-krat}} = 0$$

Če tak n ne obstaja je karakteristika enaka 0.

Če je $1 \in R$, je $\text{char}(R) = \text{red enote oziroma najmanjši } n \in \mathbb{N}, \text{ da je } 1 \cdot n = 0$.

Če je R cel kolobar, je $\text{char}R \in \{0\} \cup \mathbb{P}$.

Homomorfizem

Naj bosta K, L kolobarja. $f : K \rightarrow L$ je **homomorfizem**, če $\forall a, b \in K$ velja:

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b) \end{aligned}$$

Iz aditivnosti sledi: $f(0) = 0$ in $f(-a) = -f(a)$.

Izomorfizem je bijektivni homomorfizem.

Avtomorfizem je homomorfizem $f : K \rightarrow K$.

Če je $f(1) = 1$, pravimo, da je homomorfizem **unitalen**. Če je unitelen in če je a obrnljiv, potem je $f(a^{-1}) = f(a)^{-1}$.

Slika / zaloga vrednosti

Zaloga vrednosti f je $f(K) = \{f(a) \mid a \in K\} = \text{Im}K \leq L$.

$$f \text{ je surjektivnen } \iff \text{Im}f = L$$

Jedro / ničelna množica

Prasluka 0 je $f^{-1}(0) = \{a \in K \mid f(a) = 0\} = \text{Ker}f \leq K$.

$$\begin{aligned} \forall a \in K, \forall x \in \text{Ker}f : f(ax) &= f(a)f(x) = 0 \\ \implies \text{Ker}f &\triangleleft K \end{aligned}$$

Ideali

Podkolobar $I \leq K$ je ideal, če velja $I \cdot K \subseteq I$ in $K \cdot I \subseteq I$. Oznaka: $I \triangleleft K$.

V nekumutativnih kolobarjih ločimo **leve** in **desne** ideale.

K in $\{0\}$ sta **neprava ideala**.

(komutativen) kolobar K je obseg \iff nima pravih idealov.

Še več, pravi ideali ne vsebujejo obrnljivih elementov.

Maksimalen ideal

Pravi ideal je **maksimalen**, če ni vsebovan v nobenem pravem idealu.

Glavni ideali

Naj bo K kolobar in $x, y \in K$.

$$(x) = Kx = \{kx \mid k \in K\}$$

$$(x, y) = (x) + (y) = \{kx + ly \mid k, l \in K\}$$

Kolobar je **glavno idealski**, če se vsi njegovi ideali glavni.

Če je F obseg, je $F[x]$ glavno idealski, maksimalni ideali pa pripadajo natanko nerazcepnim polinomom.

Kvocientni ideal

Za dvostranski ideal $I \triangleleft K$ definiramo ekvivalenčno relacijo \sim :

$$\forall a, b \in K : a \sim b \iff a - b \in I$$

K razdelimo na ekvivalenčne razrede K/\sim , ki pa jih lahko označimo tudi z K/I . Ekvivalenčni razred, ki pripada $x \in K$ označimo $[x]$ ali pa $(x + I)$.

Dodamo opreaciji:

$$\begin{aligned} (x + I) + (y + I) &= (x + y + I) \\ (x + I) \cdot (y + I) &= (x \cdot y + I) \end{aligned}$$

$(K/I, +, \cdot)$ je kolobar in podeduje lastnosti K .

K/I (K komutativen kolobar) je **obseg** $\iff I$ maksimalen ideal.

Funkcija

$$f : \{\text{ideali v } K, \text{ ki vsebujejo } I\} \leftrightarrow \{\text{ideali v } K/I\}$$

je bijekcija.

Ideali v $K/(x)$ so oblike $(d + (x))$, kjer $d|x$. Če je d nerazcepen, je ideal maksimalen.

Praideal

Ideal P v kolobarju K je *praideal*, če je $P \neq K$ in če $\forall a, b \in K : ab \in P \implies a \in P \vee b \in P$.

Izrek o izomorfizmu

Naj bo $f : K \rightarrow L$ homomorfizem kolobarjev (velja tudi za grupe). Potem je $\text{Ker}f \triangleleft K$ in imamo naravni izomorfizem:

$$\begin{aligned} \bar{f} : K/\text{Ker}f &\rightarrow \text{Im}f \\ \bar{f}(x + \text{Ker}f) &= f(x) \\ K/\text{Ker}f &\cong \text{Im}f \end{aligned}$$

Kolobarji polinomov

Računanje s kompleksnimi števili

$$z = x + iy = re^{i\varphi} = r(\cos \varphi + i \sin \varphi)$$

$$r = |z| = \sqrt{x^2 + y^2} \quad \varphi = \arg z = \arctan \frac{y}{x}$$

$$(a + bi)^{-1} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

De Moivreova formula

$$z^n = r^n (\cos \varphi n + i \sin \varphi n)$$

Osnovni izrek algebre

Vsak nekonstanten polinom $a_nx^n + \dots + a_0$ ima natanko n kompleksnih ničel (štetih z večkratnostjo).

Trigonometrične identitete

$$\sin(x \pm y) = \sin(x) \cos(y) \pm \cos(x) \sin(y)$$
$$\cos(x \pm y) = \cos(x) \cos(y) \mp \sin(x) \sin(y)$$

$$\tan(x \pm y) = \frac{\tan(x) \pm \tan(y)}{1 \mp \tan(x) \tan(y)}$$

$$\cot(x \pm y) = \frac{\cot(x) \cot(y) \mp 1}{\tan(x) \pm \tan(y)}$$

$$\sin^2(x) + \cos^2(x) = 1$$

$$1 + \cot^2(x) = \frac{1}{\sin^2(x)}$$

$$1 + \tan^2(x) = \frac{1}{\cos^2(x)}$$

$$\sin \frac{x}{2} = \pm \sqrt{\frac{1 - \cos x}{2}}$$

$$\cos \frac{x}{2} = \pm \sqrt{\frac{1 + \cos x}{2}}$$

Mali Fermantov izrek

$$\forall a \in \mathbb{Z}, p \in \mathbb{P} : \; a^p \equiv_p a$$

Polinomi

Polinom je **razcepen**, če ga lahko zapišemo kot produkt dveh nekonstantnih polinomov. Nekonstanten polinom, ki ni razcepen je **nerazcepen**.

Polinom $a_nx^n + \dots + a_0$ je **primitiven**, če velja $\gcd(a_0, \dots, a_n) = 1$

Gaussova lema

$$p(x) \in \mathbb{Z}[x] \text{ razcepen nad } \mathbb{Z} \\ \iff p(x) \text{ razcepen nad } \mathbb{Q}$$

Hornerjev algoritem

$$a_nx^n + ... + a_0 = 0$$

- možne cele ničle: \pm delitelji a_0
- možne racionalne ničle: $\pm \frac{\text{delitelji } a_0}{\text{delitelji } a_n} = k$

	a_n	a_{n-1}	\dots	a_0
k	ka_n	\dots		
	a_n	$ka_n - a_{n-1}$	\dots	ostanek

Eisensteinov kriterij

Naj bo $a(x) = a_nx^n + \dots + a_0 \in \mathbb{Z}[x]$ polinom. Če $\exists p \in \mathbb{P} : p|a_0, \dots, a_{n-1} \wedge p \nmid a_n \wedge p^2 \nmid a_0$, potem je $a(x)$ nerazcepen nad \mathbb{Q} .

Rodovne funkcije

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q} \qquad \sum_{n=0}^b q^n = \frac{1-q^{b+1}}{1-q}$$
$$\sum_{n=a}^{\infty} q^n = \frac{q^a}{1-q} \qquad \sum_{n=a}^b q^n = \frac{q^a - q^{b+1}}{1-q}$$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$$

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

$$\frac{1}{(1-x)^n} = \sum_{k=0}^n \binom{n+k-1}{k} x^k$$

$$B_{\lambda}(x) = \sum_n \binom{\lambda}{n} x^n = (1+x)^{\lambda}; \qquad \binom{\lambda}{n} = \frac{\lambda^n}{n!}$$

Mobiusova formula

$$\mu(n) = \begin{cases} 1 & n = 1, \\ 0 & \exists p \in P : p^2 | n \\ (-1)^k & n \text{ je produkt } k \text{ razli\u010dnih praštevil.} \end{cases}$$

Število nerazcepnih polinomov v $\mathbb{Z}_p[x]$ stopnje n je enako

$$N_p(n) = \frac{p-1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$$

Eulerjeva funkcija

$$\varphi(n) = |\{k \in [n] : D(n,k) = 1\}|$$
$$= \text{št. proti } n \text{ tujih števil, ki so } \leq n$$

$$\varphi(p) = p-1 \qquad p \in \mathbb{P}$$

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

$$\sum_{d|n} \varphi(d) = n$$

Najve\u010dji skupni delitelj

Za polinoma $a, b \in F[x]$ obstaja enoli\u010dno dolo\u010den najve\u010dji skupni delitelj $d = \gcd(a, b)$.

Raz\u0161irjen evklidov algoritem

```
vhod: (a, b)
(r0, x0, y0) = (a, 1, 0)
(r1, x1, y1) = (b, 0, 1)
i = 1

dokler ri ≠ 0:
i = i+1
ki = ri-2//ri-1
(ri, xi, yi) = (ri-2, xi-2, yi-2) - ki(ri-1, xi-1, yi-1)
konec zanke
vrni: (ri-1, xi-1, yi-1)
```

Trojica (d, x, y) , ki jo vrne raz\u0161irjen evklidov algoritem z vhodnim podatkomk (a, b) , zado\u0161\u010da:

$$ax + by = d \text{ in } d = \gcd(a, b)$$

Gaussova cela \u0161tevila

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Gaussovo celo \u0161tevilo $x \neq 0$, ki ni obrnljivo, je **nerazceпно**, \u010e

$$x = y \cdot z \implies y \text{ obrnljivo} \vee z \text{ obrnljivo}$$

\u0160tevili x in y sta **asociativni**, \u010e velja $y = ax$, kjer je a obrnljiv.

Liho pra\u0161tevilo $p \in \mathbb{P}$ je nad $\mathbb{Z}[i]$ nerazceпно $\iff p = 4k + 3$

Norma Gaussovega celega je $N(a + bi) = a^2 + b^2$.

Vsak par Gaussovih celih \u0161tevil $z, w \in \mathbb{Z}[i]$ lahko zapi\u0161emo kot

$$z = kw + r$$

Kjer je $N(z) > N(w)$ in $N(r) < N(w)$