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
- $\forall a, b, c \in R : a(b + c) = ab + ac$ (distrubutivnost)
- $\forall a, b, c \in R : (a + b)c = ac + bc$ (distrubutivnost)
- $\forall a, b \in R : ab \in R$ (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 niča in celi kolobarji

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

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

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

Razširitve kolobarjev

Naj bo K kolobar **brez enote**:

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

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

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

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

Tako dobimo **obseg ulomkov za** K.

Wedderburnov izrek

Končen kolobar brez deliteljev niča 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

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

Če tak n ne obstaja je karakteristika enaka 0.

Če je $1 \in R$, je $\text{char}(R) =$ red enote oziroma najmanjši $n \in \mathbb{N}$, 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. $f : K \to L$ je **homomorfizem**, če $\forall a, b \in K$ velja:

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

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

Izomorfizem je bijektivni homomorfizem.

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

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

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

Jedro / ničelna množica

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

$$\forall a \in K, \forall x \in \text{Ker}f :\ f(ax) = f(a)f(x) = 0 \implies \text{Ker}f \lhd K$$

Ideali

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

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 $I \lhd K$ 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:

$$(x + I) + (y + I) = (x + y + I)$$
$$(x + I) \cdot (y + I) = (x \cdot y + I)$$

$(K/I, +, \cdot)$ 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 $f : K \to L$ homomorfizem kolobarjev (velja tudi za grupe). Potem je $\text{Ker}f \lhd K$ in imamo naravni izomorfizem:

$$\bar{f} : K/\text{Ker}f \to \text{Im}f$$
$$\bar{f}(x + \text{Ker}f) = f(x)$$
$$K/\text{Ker}f \cong \text{Im}f$$

Kolobarji polinomov

Računanje s kompleksnimi števili

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

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

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

De Moivreova formula

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

Osnovni izrek algebre

Vsak nekonstanten polinom $a_n x^n + \cdots + a_0$ 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 $a_n x^n + \cdots + a_0$ je **primitiven**, če velja $\gcd(a_0, \ldots, a_n) = 1$

Gaussova lema

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

Hornerjev algoritem

$$a_n x^n + ... + a_0 = 0$$

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

Eisensteinov kriterij

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

Rodovne funkcije

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

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

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

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

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

Mobiusova formula

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

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

$$\begin{aligned} \varphi(n) &= |\{k \in [n] : D(n,k) = 1\}| \\ &= \text{št. proti } n \text{ tujih števil, ki so} \leq n \\ \varphi(p) &= p - 1 \qquad p \in \mathbb{P} \\ \varphi(p^k) &= p^k - p^{k-1} = p^k(1 - \frac{1}{p}) \end{aligned}$$

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

Največji skupni delitelj

Za polinoma $a, b \in F[x]$ obstaja enolično določen največji skupni delitelj $d = \gcd(a, b)$.

Razširjen evklidov algoritem

```
vhod: (a, b)
(r_0, x_0, y_0) = (a, 1, 0)
(r_1, x_1, y_1) = (b, 0, 1)
i = 1

dokler r_i ≠ 0:
i = i+1
k_i = r_{i-2}//r_{i-1}
(r_i, x_i, y_i) = (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})
konec zanke
vrni: (r_{i-1}, x_{i-1}, y_{i-1})
```

Trojica (d, x, y), ki jo vrne razširjen evklidov algoritem z vhodnim podatkomk (a, b), zadošča:

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

Gaussova cela števila

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

Gaussovo celo število $x \neq 0$, ki ni obrnljivo, je **nerazcepno**, če

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

Števili x in y sta **asociativni**, če velja $y = ax$, kjer je a obrnljiv.

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

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

Vsak par Gaussovih celih števil $z, w \in \mathbb{Z}[i]$ lahko zapišemo kot

$$z = kw + r$$

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

Obsegi

Obseg je *komutativen* kkolobar v katerem so vsi neničelni elementi *obrnljivi.*

Razširitve obsegov

Če je K podobseg obsega F, pravimo, da je F **razširitev** obsega K in pišemo $K \leq F$.

F je avtomatično tudi vektorski prostor nad K dimenzije $\dim_K(F) = [F : K]$.

Če je $[F : K]$ končna, je F **končna razširitev**, sicer pa je **neskončna razširitev**.

$$K \leq F \leq E \implies [E : K] = [E : F] \cdot [F : K]$$

- Najmanjši podkolobar kolobarja F, ki vsebuje $K \leq F$ in $a \in F$ je
$$K[a] = \{p(a) \mid p(x) \in K[x]\}$$
- Najmanjši podobseg obsega F, ki vsebuje $K \leq F$ in $a \in F$ je
$$K(a) = \left\{ \frac{p(a)}{q(a)} \;\middle|\; p(x), q(x) \in K[x] \right\}$$

Enostavne razširitve obsegov

Naj bo $K \leq F$ in $a \in F$. Oglejmo si homomorfizem

$$\begin{aligned} f_a : K[x] &\to F \\ p(x) &\mapsto p(a) \end{aligned}$$

$$\begin{aligned} \mathrm{Im} f_a &= K[a] \\ \mathrm{Ker} f_a &= \{p(x) \in K[x] \mid p(a) = 0\} \end{aligned}$$

- a je **transcendenten** nad K

$\iff$ a ni ničala nobenega neničelnega polinoma iz $K[x]$

$\iff$ $\mathrm{Ker} f_a = (0)$

$\iff$ f_a injektivna

- a je **algebraičen** nad K

$\iff$ $\exists p(x) \in K[x], p \neq 0 : \; p(a) = 0$

Če so vsi elementi F algebraični nad K, je F **algebraična razširitev**. V nasprotnem primeru pa je F **transcendentna razširitev**.

Če je $a \in F$ *transcendenten* nad K, je

$$K[a] \cong K[x] \qquad K(a) \cong K(x)$$

Če je $a \in F$ *algebraičen* nad K, velja:

- $\exists$ natanko določen **minimalni polinom** $g_a \in K[x]$, ki deli vse polinome z ničlo v a. g_a **moničen** (*vodilni koef. =1*)
- $\mathrm{Ker} f_a = (g_a)$
- $K(a) = K[a] \cong K[x]/(g_a)$
- $[K(a) : K] = \deg g_a$, **stopnja** a nad K (oznaka: $\deg_K a$)
- Ideal $(g_a) \lhd K[x]$ je maksimalen $\implies K[x]/(g_a)$ je obseg

Naj bo F končna razširitev K, potem za vsak $a \in F$ velja

$$\deg_K(a) \big| [F : K]$$

Vse transcendentne razširitve so neskončne, algebraične pa so lahko končne ali pa neskončne (če dodamo več elementov).

Naj bo $K \leq F$ in $A \subseteq F$ množica števil, ki so algebraična nad K. Potem je $K(A)$ algebraična nad K.

Naj bo $K \leq F \leq E$, F algebraična nad K, E algebraična nad F. Potem je E algebraična nad K.

Razpadni obseg polinoma

Razpadni obseg polinoma $p(x)$ nad obsegom K označimo z $K(p(x))$. To je najmanjši podobseg K v katerem je $p(x)$ povsem razcepen.

Za vsak n obstaja razširitev stopnje n obsega $\mathbb{Z}_p$. Vsaka taka razširitev je izomorfna $\mathbb{Z}_p(x^{p^n} - x)$.

Edini (do izomorfizma) obseg moči n^p je **Galoisov obseg** $\mathrm{GF}(p^n)$.

Naj bo K končen kolobar (ne nujno komutativen). Če K nima deliteljev niča, je $|K| = p^n$ in $K \cong \mathrm{GL}(n^p)$.

Topologija

Naj bo X poljubna množica. Topologija na X je podana z družino odprtih množic τ, ki je zaprta za **poljubne unije** in **končne preseke**.

Prazna unija je prazna množica, prazen presek pa cela množica.

Najmanjša možna topologija je $\tau = \{\emptyset, X\}$ **trivialna**.

Največja možna topologija je $\tau = P(X)$ **diskretna**.

Topologija glede na metriko

$d : X \times X \to [0, \infty)$ je metrika, če velja:

- $d(x, y) = 0 \iff x = y$
- $d(x, y) = d(y, x)$
- $d(x, y) + d(y, z) \geq d(x, z)$

Topologija iz metrike na X je:

$$\tau_d = \{U \subseteq X \mid U \text{ odprta glede na } d\}$$

A je **odprta množica**, če so vse točke notranje ($\forall a \in A\ \exists \varepsilon > 0 :\ K(a, \varepsilon) \subseteq A$).

A je **zaprta množica** $\iff$ $A^\complement$ odprta $\iff$ vsebuje vse svoje robne točke.

Naj bo $A \subseteq X$.

- **Notranjost** $\mathrm{Int}(A) = \mathring{A} =$ največja odprta množica vsebovana v A.
- **Zaprtje** $\mathrm{Cl}(A) = \bar{A} =$ najmanjša zaprta množica, ki še vsebuje v A
  $=$ presek vseh zaprtih množic, ki vsebujejo A
- **Rob** $\mathrm{Fr}(A) = \partial A = \dot{A} = \mathrm{Cl}(A) - \mathrm{Int}(A)$

Metrizabilnost

(X, τ) je metrizabilen, če obstaja metrika d na X, da $\tau = \tau_d$

Zveznost

Funkcija $f : (X, \tau_X) \to (Y, \tau_Y)$ je zvezna, če

$$\forall x \in X\ \forall \varepsilon > 0\ \forall \delta > 0\ \forall x' \in X :$$
$$d(x, x') < \delta \implies d(f(x), f(x')) < \varepsilon$$

Ekvivalentna topološka definicija:

$$\forall V \in \tau_Y : f^{-1}(V) \in \tau_X$$

Funkcija je zvezva, če je praslika vsake odprte množice odprta.

Naslednje trditve so ekvivalentne:

- $f : X \to Y$ je zvezna
- $\forall A^{\mathrm{odp}} \subseteq Y :\ f^{-1}(A)$ odprta v X
- $\forall B^{\mathrm{zap}} \subseteq Y :\ f^{-1}(B)$ zaprta v X
- $\forall A \subseteq X :\ f(\bar{A}) \subseteq \overline{f(A)}$

Homeomorfizmi

$f : (X, \tau_X) \to (Y, \tau_Y)$ je **homeomorfizem**, če je f bijekcija in sta f in f^{-1} zvezni.

Prostora (X, τ_X) in (Y, τ_Y) sta **homeomorfna**. Oznaka $X \approx Y$.

$f : X \to Y$ je **odprta**, če je slika vsake odprte množice odprta.

$f : X \to Y$ je **zaprta**, če je slika vsake zaprte množice zaprta.

Naslednje trditve so ekvivalentne:

- $f : X \to Y$ je homeomorfizem
- f je zvezna bijekcija in f^{-1} je zvezna
- f je zvezna in odprta bijekcija
- f je zvezna in zaprta bijekcija

Kompaktnost

Odprto pokritje množice X je vsaka družina (odprtih množic) $\mathcal{U} \subseteq \tau$, katere unija je cel X.

Prostor X je **kompakten**, če v vsakem odprtem pokritju X obstaja končno podpokritje.

- Vsaka končna množica je kompaktna.
- V metričnem prostoru je vsaka kompaktna množica omejena.

$$A^{\mathrm{zap}} \subseteq X^{\mathrm{kompakten}} \implies A \text{ kompakten}$$

Heine-Borel-Lebesgue:

$$A \subseteq \mathbb{R}^n \text{ je kompakten } \iff A \text{ zaprt in omejen}$$

V kompaktnem prostoru ima vsaka neskončna množica vsaj eno stekališče.

Bolzano-Weierstrass:
Vsako omejeno zaporedje v $\mathbb{R}^n$ ima konvergentno podzaporedje.

Zvezna slika kompakta je kompakt.
$f : X \to Y$ zvezna, $A^{\mathrm{kompkt}} \subseteq X \implies f(A)$ kompakt

X kompakten $\iff$ v vsaki družini zap. podmnožic X, ki ima prazen presek, obstaja končna podmnožica, ki ima prazen presek.

Povezanost

Separacija množice X je razdelitev $X = A \amalg B$ na deve disjunktni, neprazni, odprti podmnožici.

Prostor, ki ima separacijo je **nepovezan**, sicer pa je **povezan**.

Alternativna definicija:

- X je povezan, če ga ni mogoče razdeliti na dve disjunktni neprazni množici
- X je povezan, če sta njegovi edini podmnožici, ki sta zaprti in odprti hkrati, $\emptyset$ in X.

Povezane množice v $\mathbb{R}$ so natanko intervali.

Zvezna funkcije ohranjajo povezanost.
$f : X \to Y$ zvezna, X povezana $\implies f(X)$ povezana

X je **povezan s potmi**, če za polubna $a, b \in X$ obstaja **pot** $p : [0, 1] \to X$, zvezna, $p(0) = a$, $p(1) = b$.

X povezan s potmi $\implies X$ povezan

Če je L povezan in je $L \subseteq M \subseteq \bar{L}$, je tudi M povezan.