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 in- $\operatorname{verz} \forall x \in M \ \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x = e.$ relacijo \sim .
- abelova grupa grupa s komutativno operacijo $\forall x, y \in M : x \cdot y = y \cdot x$.

Kolobarii

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 (distrubu-
- $\forall a, b \in R : ab \in R \text{ (zaprtost množenja)}$
- $\forall a, b, c \in R : (ab)c = a(bc) \text{ (asociativnost*)}$
- $\exists e \in R \ \forall a \in R : e \cdot a = a = e \cdot a \ (\text{enota*})$

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

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 deliteliev niča.

Razširitve kolobariev

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 deliteliev niča vendar niso vsi elementi obrnljivi. Dodamo ulomke definirane kot ekvivalenčne razrede dvojic z ekvivalenčno (refleksivno, simetrično, tranzitivno)

$$K \times K - \{0\} /_{\sim}$$

$$\frac{a}{b} \sim \frac{ka}{kb} \quad \forall k \in K - \{0\}$$

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

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 velia

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

Če tak n ne obstaja je karakteristika enaka 0.

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

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

Homomorfizem

Naj bosta K, L kolobarja. $f: K \to L$ je homo**morfizem**, 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 **uni**talen. 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 je surjektiven \iff Im f = L

Jedro / ničelna množica

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

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

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 elemen-

Maksimalen ideal

Pravi ideal je **maksimalen**, če vsebuje vse ostale prave ideale.

R obseg, $I \triangleleft R[x]$ ja maksimalen $\iff I = (p(x)),$ p(x) nerazcepen

Glavni ideali

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

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

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

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 opreaciii:

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

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

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

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

Naj bo $f: K \to L$ homomorfizem kolobarjev. Potem je $\operatorname{Ker} f \triangleleft K$ in imamo naravni izomorfizem:

$$\bar{f}: K/\mathrm{Ker}f \to \mathrm{Im}f$$

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

Kolobarji polinomov

Računanje s kompleksnimi števili

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

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

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

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 večkratnostio).

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

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

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 $\gcd(a_0,\ldots,a_n)=0$

Gaussova lema

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

Hornerjev algoritem

$$a_n x^n + \dots + a_0 = 0$$

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

Eisensteinov kriterii

Naj bo $a(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ 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{O} .

Rodovne funkcije

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

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

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

$$\frac{a_0 + \dots + a_{k-1} x^{k-1}}{1 - x^k} = a_0 + \dots + a_{k-1} x^{k-1} + a_0^k + \dots + a_{k-1} x^{2k-1} + \dots$$

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

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

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

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

Mobiusova formula

$$\mu(n) = \begin{cases} 1 & n = 1, & konec \ zanke \\ 0 & \exists p \in P : p^2 | n \\ (-1)^k & n \ \text{je produkt} \ k \ \text{različnih praštevil.} & \text{Trojica} \ (d, x, y), \ \text{ki jo vrne razširjen evklidov algoritem} \ x \ \text{vhodnim podutkomk} \ (a, b) \ \text{radoščevily} \end{cases}$$

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

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

Eulerjeva funkcija

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q} \qquad \sum_{n=0}^{b} q^n = \frac{1-q^{b+1}}{1-q} \qquad \qquad \varphi(n) = |\{k \in [n] : D(n,k) = 1\}|$$

$$= \text{ §t. proti n tujih števil, ki so } \leq n$$

$$\sum_{n=a}^{\infty} q^n = \frac{q^a}{1-q} \qquad \sum_{n=a}^{b} q^n = \frac{q^a-q^{b+1}}{1-q} \qquad \qquad \varphi(p) = p-1 \qquad p \in \mathbb{P}$$

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

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

Največii skupni deliteli

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

Razširjen evklidov algoritem

$$\begin{array}{lll} \mathit{vhod}: & (a,b) \\ & (r_0,\ x_0,\ y_0) \ = \ (a\ ,\ 1\ ,\ 0) \\ & (r_1,\ x_1,\ y_1) \ = \ (b\ ,\ 0\ ,\ 1) \\ & i = 1 \\ & \mathit{dokler}\ r_i \ \neq \ 0\colon \\ & i = i+1 \\ & k_i = r_{i-2}//r_{i-1} \\ & (r_i,x_i,y_i) \ = \ (r_{i-2},x_{i-2},y_{i-2}) - k_i(r_{i-1},x_{i-1},y_{i-1}) \\ & \mathit{konec}\ \mathit{zanke} \\ & \mathit{vrni}: \ (r_{i-1},x_{i-1},y_{i-1}) \end{array}$$

ritem z vhodnim podatkomk (a, b), zadošča:

$$ax + by = d$$
 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 **ner**azcepno, če

$$x = y \cdot z \implies y$$
 obrnljivo $\forall z$ obrnljivo

Števili x in y sta **asociativni**, če velja y = ax, kjer ie a obrnliiv.

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

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