

1. sklop dodatnih vaj iz Izbranih poglavij iz matematike

- (1) Z uporabo Evklidovega algoritma izračunaj največji skupni delitelj polinomov $p(x) = x^4 + 3x^3 + 4x^2 + 2$ in $q(x) = x^3 + 4x^2 + 2$ v $\mathbb{Z}_5[x]$.

Rešitev: $\gcd(p, q) = x + 2$.

- (2) Poišči polinoma $s, t \in \mathbb{R}[x]$, da bo veljalo

$$(x^3 - 1)s(x) + (x^2 + 1)t(x) = 1.$$

Rešitev: $s(x) = \frac{1}{2}(x - 1)$ in $t(x) = \frac{1}{2}(1 + x - x^2)$.

- (3) Pokaži, da so dani polinomi nerazcepni:

(a) $p(x) = x^7 + 6x^5 - 3x^4 + 60x^2 - 9x + 15 \in \mathbb{Q}[x]$,

(b) $p(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$,

(c) $p(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_3[x]$.

- (4) Naj bo $\mathbb{F}$ končen obseg karakteristike 2. Pokaži, da je enačba $x^2 = a$ rešljiva v obsegu $\mathbb{F}$ za vsak $a \in \mathbb{F}$.

- (5) Poišči največja skupna delitelja naslednjih Gaussovih celih števil:

(a) $a = 11 + 3i$ in $b = 1 + 8i$,

(b) $a = 32 + 9i$ in $b = 4 + 11i$.

Rešitev:

(a) $\gcd(a, b) = -1 + 2i$,

(b) $\gcd(a, b) = 1$.

- (6) Pokaži, da je kolobar Gaussovih celih števil glavnoidealski.

- (7) Na kolobarju $K = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ definirajmo normo s predpisom

$$N(a + b\sqrt{5}i) = a^2 + 5b^2.$$

- (a) Pokaži, da velja enakost $N(ab) = N(a)N(b)$ za poljubna $a, b \in K$ in nato poišči vse obrnljive elemente K .

- (b) Ali v kolobarju K velja izrek o enolični faktorizaciji?

Rešitev:

- (a) Obrnljiva sta elementa 1 in -1 .

- (b) Ne. Protiprimer je $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.

(8) Poišči vse homomorfizme kolobarjev:

- (a) $\mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$,
- (b) $\mathbb{Z}_4 \rightarrow \mathbb{Z}_8$.

Rešitev:

- (a) Homomorfizmi so $\phi(x) = 0$, $\phi(x) = x$, $\phi(x) = 5x$ in $\phi(x) = 6x$.
- (b) Edini homomorfizem $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_8$ je ničelni homomorfizem.

(9) Pokaži, da je $\phi(A) = 0$ edini homomorfizem kolobarjev $\phi : M_2(\mathbb{R}) \rightarrow \mathbb{R}$.

(10) Poišči vse ideale in maksimalne ideale v naslednjih kolobarjih:

- (a) $\mathbb{Z}_{18}$,
- (b) $\mathbb{Z}_{25}$.

Rešitev:

- (a) Ideali v $\mathbb{Z}_{18}$ so $\{0\}$, (2) , (3) , (6) , (9) in $\mathbb{Z}_{18}$. Maksimalna sta (2) in (3) .
- (b) Ideali v $\mathbb{Z}_{25}$ so $\{0\}$, (5) in $\mathbb{Z}_{25}$. Maksimalen je ideal (5) .

(11) Poišči vse ideale in maksimalne ideale v naslednjih kolobarjih:

- (a) $\mathbb{R}[x]/(x^2(x+1)^2)$,
- (b) $M_2(\mathbb{Z}_6)$.

Rešitev:

- (a) Ideali v $\mathbb{R}[x]/(x^2(x+1)^2)$ so $\{0\}$, (x) , $(x+1)$, (x^2) , $((x+1)^2)$, $(x(x+1))$, $(x^2(x+1))$, $(x(x+1)^2)$ in $\mathbb{R}[x]/(x^2(x+1)^2)$. Maksimalna sta (x) in $(x+1)$.
- (b) Ideali v $M_2(\mathbb{Z}_6)$ so $\{0\}$, $M_2((2))$, $M_2((3))$ in $M_2(\mathbb{Z}_6)$. Maksimalna sta $M_2((2))$ in $M_2((3))$.

(12) Pokaži, da ideal $(2, x)$ v kolobarju $\mathbb{Z}[x]$ ni glavni.

(13) Naj bo K komutativen kolobar z enoto, katerega edina ideala sta $\{0\}$ in K . Pokaži, da je potem K obseg.

(14) Naj bo Galoisov obseg $GF(3^2)$ definiran s polinomom $p(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$.

- (a) Kateri grupi je izomorfna grupa $(GF(3^2), +)$?
- (b) Kateri grupi je izomorfna grupa obrnljivih elementov obsega $GF(3^2)$?

Rešitev:

- (a) Grupa $(GF(3^2), +)$ je izomorfna grupi $\mathbb{Z}_3 \times \mathbb{Z}_3$. Ekspliciten izomorfizem $\phi : (GF(3^2), +) \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3$ je:

$$\phi(ax + b) = (a, b).$$

(b) Grupa obrnljivih elementov obsega $GF(3^2)$ je izomorfna ciklični grupi $\mathbb{Z}_8$. Eden izmed generatorjev je polinom x , njegove potence pa so

$$x, 2x + 1, 2x + 2, 2, 2x, x + 2, x + 1, 1.$$

(15) Naj bo obseg $GF(2^8)$ definiran s polinomom $p(x) = x^8 + x^6 + x^5 + x + 1 \in \mathbb{Z}_8[x]$.

(a) Izračunaj produkt polinomov $s(x) = x^6 + x^3$ in $t(x) = x^7 + x^5 + x^2 + 1$ v $GF(2^8)$.

(b) Izračunaj inverz polinoma $q(x) = x^3 + x^2 + 1$ v $GF(2^8)$.

Rešitev:

(a) $s(x) \cdot t(x) = x^3$.

(b) $q(x)^{-1} = x^6 + x^4 + x^2$.