UNIVERZA NA PRIMORSKEM
Fakulteta za matematiko, naravoslovje in informacijske tehnologije

Zbirka rešenih nalog iz teorije kolobarjev in končnih polj

dr. Amar Bapić **Nina Klobas**

DRUGO UČNO GRADIVO

101 stran

Matematika, dodiplomski študijski program

PRVA IZDAJA

Koper, 2023

Delo naj se citira kot:
A. Bapić in N. Klobas. *Zbirka rešenih nalog iz teorije kolobarjev in končnih polj.* Univerza na Primorskem, Fakulteta za matematiko, naravoslovje in informacijske tehnologije, Koper, 2023.

Predgovor

Pred vami je zbirka rešenih nalog za predmet Algebra IV - algebrske strukture, namenjena je študentkam in študentom študijskega programa Matematika na UP FAMNIT. Upava, da vam bo zbirka koristila, vsekakor pa ni mišljena kot nadomestilo za vaje, kjer so stvari razložene bolje, bolj izčrpno in razumljivo.

Vsebina in naloge so v skaldu z učnim načrtom. Obravnavamo naslednje teme:

- Kolobarji. Ideali. Homomorfizem kolobarjev. Faktorski kolobarji. Celi kolobarji. Evklidski kolobarji. Glavni kolobarji. Gaussovi kolobarji. Gaussova števila. Kitajski izrek o ostanku.
- Polja. Podpolja. Razširitve. Končne razširitve.
- Stopnja razširitve. Stolpni izrek. Enostavne algebraične razširitve. Razcepna polja.

Večina predstavljenih nalog je rešenih. Rešitve so podane natančno in precizno, s ciljem, da bralec razume in osvoji določen postopek reševanja in pri tem dobi intuicijo, kako pristopiti k reševanju podobnih nalog. Zbirka vsebuje tudi nekaj dodatnih nalog, ki so prepuščene bralcu za samostojno reševanje. Na koncu je podan tudi seznam teoretičnih vprašanj temeljnih pojmov s področja teorije kolobarjev in polj.

Gradivo lahko vsebuje tudi napake. Vesela bova, če naju boste nanje opozorili.

Avtorja

Kazalo

KOLOBARJI

1.1. Uvod v kolobarje

Aditivne grupe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ in $\mathbb{C}$ so osnovni zgledi Abelovih grup. Na teh množicah lahko definiramo tudi množenje, vendar zanj množice niso grupe, pač pa le polgrupe. Ker sta seštevanje in množenje povezana preko zakona distributivnosti, tako $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ in $\mathbb{C}$ ustrezajo pogojem naslednje definicije, in so torej primeri kolobarjev.

Definicija 1.1

Naj bo $K \neq \emptyset$. Urejena trojica $(K, +, \cdot)$ je ***kolobar***, če veljajo naslednje lastnosti:

(K1) $(K, +)$ je komutativna grupa.

(K2) $(K, \cdot)$ je polgrupa.

(K3) Za vse $a, b, c \in K$ velja

$$(a+b)\cdot c = a\cdot c + b\cdot c \quad \text{in} \quad c\cdot(a+b) = c\cdot a + c\cdot a.$$

Nevtralni element za seštevanje označimo z 0 ali 0_K (če ni razvidno iz konteksta). Če kolobar K premore nevtralni element za množenje, ta element imenujemo **identiteta** in ga označimo z 1 ali 1_K. Kolobar K pa imenujemo **kolobar z identiteto**. Če je operacija množenja v K komutativna, je K **komutativen kolobar**. Aditivni inverz elementa $a \in K$ označimo z $-a$. na definiramo kot

$$na = \begin{cases} a + a + \ldots + a, & n > 0 \\ 0_K, & n = 0 \ (0_K \in K,\ 0 \in \mathbb{Z}) \\ (-a) + (-a) + \ldots + (-a), & n < 0 \end{cases}$$

Multiplikativni inverz elementa a v kolobarju K z identiteto $1 \neq 0$ je takšen element $a^{-1} \in K$ za katerega velja $aa^{-1} = a^{-1}a = 1$. V tem primeru pravimo, da je element a **obrnljiv**.

Če so v kolobarju K z identiteto $1 \neq 0$ vsi neničelni elementi obrnljivi, je K **obseg**. Komutativen obseg imenujemo **polje**.

Najenostavnejši primer kolobarja je kolobar z enim samim elementom. Označevali ga bomo z $\{0\}$ in imenovali **ničelni** ali **trivialni** kolobar. V tem kolobarju

elementa 0 in 1 sovpadata. Kolobar je **neničelen**, če vsebuje več kot en element. Ekvivalentno, v tem kolobarju je $1 = 0$. Namreč, iz $1 = 0$ sledi, da je $x = 1x = 0x = 0$ za vsak $x \in K$.

Izrek 1.1

Naj bo K kolobar in 0 aditivni nevtralni element. Za vsak $a, b \in K$ velja:

(i) $0a = a0 = 0$.

(ii) $a(-b) = (-a)b = -(ab)$.

(iii) $(-a)(-b) = ab$

Dokaz:

(i) Iz $0a = (0+0)a = 0a + 0a$ sledi $0a = 0$. Podobno izpeljemo $a0 = 0$.

(ii) Iz $0 = a0 = a(b + (-b)) = ab + a(-b)$ razberemo, da je $a(-b) = -(ab)$. Podobno dokažemo, da je $(-a)b = -(ab)$.

(iii) Iz (ii) sledi, da je $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

♠

Iz teorije grup vemo, da podrgupa določene grupe nujno vsebuje nevtralni elemnt grupe (0). Ko govorimo o podkolobarju kolobarja vemo, da podkolobar vsebuje 0, ampak ni nujno da vsebuje identiteto kolobarja (če ta obstaja). Lahko se zgodi, da podkolobar premore identiteto, ki je različna od identite kolobarja.

Zgled 1.1.1. $(\mathbb{Z}, +, \cdot)$ je komutativen kolobar z identiteto za običajno seštevanje in množenje celih števil. Kolobar $(2\mathbb{Z}, +, \cdot)$ je podkolobar kolobarja $(\mathbb{Z}, +, \cdot)$, vendar $(2\mathbb{Z}, +, \cdot)$ nima enote za množenje.

Izrek 1.2

Podmnožica $L \subset K$ kolobarja K je podkolobar v K natanko tedaj, ko velja:

1. $(a - b) \in L,\ \forall a, b \in L,$

2. $ab \in L,\ \forall a, b \in L.$

Dokaz: Vsak podkolobar seveda vsebuje razlike in produkte svojih elementov. Dokažimo obratno implikacijo. Ker je $ab \in L$ za vse $a, b \in L$, je množenje zaprta operacija na L. Naj bo $a - b \in L$ za vse $a, b \in L$. Za $a \in L$ imamo, da je $a - a = 0 \in L$ in dodatno $0 - a = -a \in L$. Če vzamemo $a, b \in L$, potem $-b \in L$ in velja $a - (-b) = a + b \in L$.

To pomeni, da je seštevanje zaprta operacija. Ker so asociativnost, komutativnost in zakona distributivnosti dedne lastnosti, je $(L,+,\cdot)$ kolobar.

♠

Zgled 1.1.2. Kolobar celih števil $\mathbb{Z}$ je podkolobar kolobarja racionalnih števil $\mathbb{Q}$.

Zgled 1.1.3. ***Center kolobarja*** K definiramo enako kot center grupe, torej kot množico

$$Z(K) = \{c \in K : cx = xc,\ \forall x \in K\}.$$

Zlahka se prepričamo, da je $Z(K)$ podkolobar kolobarja K.

Homomorfizem lahko opišemo kot preslikavo, ki ohranja operacije, značilne za obravnavano algebrsko strukturo.

Definicija 1.2

Naj bosta $(K,+_K,\cdot_K)$ in $(R,+_R,\cdot_R)$ kolobarja. Preslikavo $\phi : K \to R$ imenujemo ***homomorfizem***, če za vsak $a,b \in K$ velja:

1. $\phi(a +_K b) = \phi(a) +_R \phi(b)$.
2. $\phi(a \cdot_K b) = \phi(a) \cdot_R \phi(b)$.

Zalogi vrednosti homomorfizma ϕ pravimo ***slika homomorfizma*** in jo označimo z $\mathrm{im}\phi$ ali $\phi(K)$. Torej je

$$\mathrm{im}\phi = \{\phi(x) : x \in K\}.$$

Jedro homomorfizma ϕ je množica

$$\ker\phi = \{x \in K : \phi(x) = 0_R\}.$$

Bijektivnemu homomorfizmu pravimo **izomorfizem**, surjektivnemu homomorfizmu **epimorfizem**, injektivnemu homomorfizmu **monomorfizem**. Homomorfizmu iz K v K pravimo **endomorfizem**, bijektivnemu endomorfizmu pa **avtomorfizem**.

Izrek 1.3

Naj bo $\phi : K \to K'$ homomorfizem kolobarjev. Če je 0 aditivna identiteta v K, potem je $\phi(0) = 0'$ aditivna identiteta v K', in če je $a \in K$, potem je $\phi(-a) = -\phi(a)$. Če je S podkolobar kolobarja K, potem je $\phi[S] = \{\phi(s) : s \in S\}$ podkolobar kolobarja K'. Če K premore identiteto 1, potem je $\phi(1)$ identiteta v $\phi[K]$.

Komentar 1.1

$\phi(1)$ ni nujno identiteta za K'.

Zgled 1.1.4. (Projektivni homomorfizem) Naj bodo $K_1, K_2, \ldots, K_n$ kolobarji. Za poljuben $i \in \{1, \ldots, n\}$ definirajmo preslikavo $\pi_i : K_1 \times K_2 \times \ldots \times K_n \to K_i$ s $\pi_i(k_1, k_2, \ldots, k_n) = k_i$ ki imenujemo projektivni homomorfizem. Očitno veljata obe lastnosti homomorfizma.

Zgled 1.1.5. Kot komutativni grupi, sta $(\mathbb{Z}, +)$ in $(2\mathbb{Z}, +)$ izomorfni pod preslikavo $\phi : \mathbb{Z} \to 2\mathbb{Z}$ definirano z $\phi(x) = 2x$ za $x \in \mathbb{Z}$. Vendar, ϕ ni izomorfizem kolobarjev, saj je $\phi(xy) = 2xy \neq 4xy = 2x2y = \phi(x)\phi(y)$.

Naloge

1. Naj bo X neprazna množica in $K = 2^X$ potenčna množica množice X. Ali je $(K, \cup, \cap)$ kolobar?

2. Naj bo X neprazna množica. Pokaži, da je potenčna množica $K = 2^X$, skupaj z operacijama simetrične razlike $A + B = A \triangle B = (A \cap \overline{B}) \cup (B \cap \overline{A})$ in preseka $AB = A \cap B$ kolobar. Ali je K komutativen? Ali premore identiteto?

3. Naj bo $(G, +)$ abelska grupa. V G definirajmo množenje s predpisom $ab = 0$ za vse $a, b \in G$. Preveri, da je G kolobar.

4. V kolobarju $K = \mathbb{R}^{2\times 2}$ je dana podmnožica M vseh matrik oblike $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$.

   (a) Dokaži, da je M podkolobar kolobarja K.

   (b) Ali je kolobar M komutativen? Ali ima identiteto?

5. Če je možno najdi primer homomorfizma $\phi : K \to K'$, kjer sta K in K' kolobarja z identitetama $1 \neq 0$ in $1' \neq 0'$ in velja $\phi(1) \neq 0'$ in $\phi(1) \neq 1'$.

6. Poišči vse homomorfizme kolobarjev iz $\mathbb{Z}$ v $\mathbb{Z}$.

7. Poišči vse homomorfizme kolobarjev iz $\mathbb{Z} \times \mathbb{Z}$ v $\mathbb{Z}$.

8. Naj bo $(K, +, \cdot)$ algebrska struktura ki zadošča vsem aksiomom kolobarjev razen komutativnosti seštevanja. Dokaži: če K premore identiteto, potem je K kolobar.

9. Pokaži, da kolobar K ne premore neničelnega nilpotenta[1] natanko tedaj ko je 0 edina rešitev enačbe $x^2 = 0$ v K.

[1] Element a kolobarja K imenujemo **nilpotent**, če obstaja takšen $n \in \mathbb{Z}^+$, da je $a^n = 0$.

10. Pokaži, da je vsak Boolov kolobar[2] tudi von Neumannovo regularen kolobar[3]. Ali je komutativen?

11. Naj bo K kolobar brez nilopotentega elementa. Poaži, da tedaj za vsak idempotent e in vsak $x \in K$ velja $xe = ex$.

Rešitve

1. Ni, ker $(K, \cup)$ ni grupa. Natančneje, za poljubno množico $A \neq \emptyset$ ne obstaja takšna obrnljiva množica $\overline{A}$, da velja $A \cup \overline{A} = \emptyset$.

2. Naj bodo $A, B, C \in K$ poljubne množice. Prva stvar, ki jo je vedno potrebno preveriti je zaprtost operacij seštevanja in množenja. Očitno sta $A+B$ in $A \cdot B$ vedno v množici K.

   (a) i. `Asociativnost seštevanja.`

$$\begin{aligned}
A+(B+C) &= (A \cap \overline{B+C}) \cup (\overline{A} \cap (B+C)) \\
&= (A \cap \overline{(B \cap \overline{C}) \cup (\overline{B} \cap C)}) \cup (\overline{A} \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C))) \\
&= (A \cap (\overline{B} \cup C) \cap (B \cup \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \\
&= (A \cap \overline{B} \cap B) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap C \cap B) \cup \\
&\cup (A \cap C \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \\
&= (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)
\end{aligned}$$

   Podobno se pokaže da velja

$$(A+B)+C = (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C).$$

   Torej je operacija asociativna.

   ii. `Obstoj nevtralnega elementa.` Naj bo A poljubna množica v K. Ker velja

$$A + \emptyset = \emptyset + A = A,$$

   je $\emptyset \in K$ nevtralni element za seštevanje.

[2] Kolobar K z identiteo imenujemo **Boolov**, če za vse $a \in K$ velja $a^2 = a$. Torej, vsak element je idempotent.

[3] Kolobar z identiteto K v katerem za vsak element $x \in K$ obstaja element $y \in K$, takšen, da je $xyx = x$, imenujemo **von Neumannev regularen kolobar.**

iii. `Obstoj obrnljivega elementa.` Za poljubno množico $A \in K$ obstaja množica $\overline{A} = A$ takšna, da velja

$$A + \overline{A} = \overline{A} + A = \emptyset.$$

iv. `Komutativnost.` Zaradi komutativnosti operacij $\cup$ in $\cap$ velja

$$A + B = (A \cap \overline{B}) \cup (\overline{A} \cap B) = (B \cap \overline{A}) \cup (\overline{B} \cap A) = B + A.$$

Torej, $(K, +)$ je komutativna grupa.

(b) Očitno je

$$A \cdot (B \cdot C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cdot B) \cdot C$$

zaradi asociativnosti operacije $\cap$. Torej je $(K, \cdot)$ `polgrupa`.

(c) `Zakona distributivnosti.`

$$\begin{aligned}
A \cdot (B + C) &= A \cap (B + C) = A \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C)) \\
&= (A \cap (B \cap \overline{C})) \cup (A \cap (\overline{B} \cap C)) \\
&= (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap C) \\
A \cdot B + A \cdot C &= (A \cap B) + (A \cap C) = ((A \cap B) \cap \overline{(A \cap C)}) \cup (\overline{(A \cap B)} \cap (A \cap C)) \\
&= ((A \cap B) \cap (\overline{A} \cup \overline{C}) \cup ((\overline{A} \cup \overline{B}) \cap (A \cap C)) \\
&= (A \cap B \cap \overline{A}) \cup (A \cap B \cap \overline{C}) \cup (\overline{A} \cap A \cap C) \cup (\overline{B} \cap A \cap C) \\
&= (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap C)
\end{aligned}$$

Torej $A \cdot (B + C) = A \cdot B + B \cdot C$. Podobno se pokaže, da velja $(A + B) \cdot C = A \cdot C + B \cdot C$.

Od tod lahko zaključimo, da je $(K, +, \cdot)$ kolobar. Ker je $\cap$ komutativna operacija je očitno $A \cdot B = B \cdot A$. Kolobar K premore identiteto $1 = X$, ker za poljubno množico $\emptyset \neq A \in K$ velja $A \cdot X = X \cdot A = A$, je K komutativen kolobar z identiteto X.

3. Preveriti moramo, če je $(G, \cdot)$ polgrupa in če veljata distributivnosti. Naj bodo $a, b, c \in G$ poljubni elementi. Ker je $a \cdot b = 0 \in G$, je množenje zaprta operacija. Velja tudi naslednje:

$$\begin{aligned}
a \cdot (b \cdot c) &= a \cdot 0 = 0, \\
(a \cdot b) \cdot c &= 0 \cdot c = 0.
\end{aligned}$$

Torej je $(G, \cdot)$ polgrupa. Preverite lahko tudi distributivnost.

4. (a) Uporabili bomo Izrek 1. Nevtralni element za seštevanje matrik v kolobarju $K = \mathbb{R}^{2\times 2}$ je $O_K = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ in očitno je $O_K \in M$. Naj bosta $A, B \in M$ poljubna.

$$A - B = \begin{bmatrix} a & b \\ b & a \end{bmatrix} - \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} \underbrace{a-b}_{\in\mathbb{R}} & \underbrace{b-d}_{\in\mathbb{R}} \\ b-d & a-b \end{bmatrix} \in M$$

$$AB = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{bmatrix} \in M$$

Ker so zadovoljeni vsi pogoji Izreka 1 lahko zaključimo, da je M podkolobar kolobarja K s standardnima operacijama $+$ in $\cdot$ v $\mathbb{R}^{2\times 2}$.

(b) Zaradi komutativnosti operacij $+$ in $\cdot$ v $\mathbb{R}$ se lahko preveri, da velja $A \cdot B = B \cdot A$. Kolobar M premore identiteto $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Torej, je M komutativen kolobar z identiteto I_2.

5. Poglejmo preslikavo $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definirano s $\phi(n) = (n, 0)$. Ni težko pokazati, da je ϕ homomorfizem kolobarjev. Identiteta v $\mathbb{Z}$ je 1, v $\mathbb{Z} \times \mathbb{Z}$ je $1' = (1,1)$ in velja $1 \neq 1'$. Z druge strani, $\phi(1) = (1,0) \neq (1,1) = 1'$.

6. Homomorfizem kolobarjev ohrani idempotente. Ker v $\mathbb{Z}$ velja $1^2 = 1$ imamo $\phi(1)^2 = \phi(1)$. Od tod sledi, da je $\phi(1) = 1$ ali $\phi(1) = 0$. Z druge strani,

$$\phi(n) = \phi(n \cdot 1) = \phi(1 + 1 + \ldots + 1) = \phi(1) + \ldots + \phi(1) = n\phi(1)$$

in ker je $\phi(-n) = -\phi(n)$ velja, da je za vsak $n \in \mathbb{Z}$, $\phi(n) = 0$ ali $\phi(n) = n$. To sta edina homomorfizma. Pravimo jima trivialni in identični homomorfizem.

7. Ker $(0,1)$ in $(1,0)$ generirata aditivno grupo $\mathbb{Z} \times \mathbb{Z}$, njune slike določata iskani homomorfizem:

$$\begin{aligned} \varphi(m,n) &= \varphi(m(1,0) + n(0,1)) = \varphi(m(1,0)) + \varphi(n(0,1)) \\ &= \varphi(\underbrace{(1,0) + \ldots + (1,0)}_{m}) + \varphi(\underbrace{(0,1) + \ldots + (0,1)}_{n}) \\ &= \underbrace{\varphi(1,0) + \ldots + \varphi(1,0)}_{m} + \underbrace{\varphi(0,1) + \ldots + \varphi(0,1)}_{n} \\ &= m\varphi(1,0) + n\varphi(0,1). \end{aligned}$$

Ker sta elementa $(0,1)$ in $(1,0)$ idempotenta v $\mathbb{Z} \times \mathbb{Z}$, se morata preslikati v 0 ali

1. Torej:

$$\begin{aligned}\varphi_1(m,n) &= 0,\\ \varphi_2(m,n) &= m,\\ \varphi_3(m,n) &= n,\\ \varphi_4(m,n) &= m+n.\end{aligned}$$

Ni težko preveriti, da so φ_1, φ_2 in φ_3 res homomorfizmi kolobarjev. Ker

$$\varphi_4(m,n) = \varphi_4((1,1)(m,n)) = \varphi_4(1,1)\varphi_4(m,n) = (1+1)(m+n) = 2(m+n) = 2\varphi_4(m,n) \to \leftarrow$$

8. Naj bosta $a, b \in K$ poljubna. Ker R premore identiteto 1, velja:

$$0 = b\cdot 0 = b\cdot(1+(-1)) = b\cdot 1 + b\cdot(-1) \Rightarrow b(-1) = -b.$$

Z druge strani,

$$\begin{aligned}&0 = (-b)+(-a)+a+b = b(-1)+a(-1)+a+b = (b+a)(-1)+a+b\\ &\quad\Rightarrow a+b = -(b+a)(-1) \text{ in}\\ &0 = (b+a)\cdot 0 = (b+a)\cdot((-1)+1) = (b+a)(-1)+b+a\\ &\quad\Rightarrow b+a = -(b+a)(-1).\end{aligned}$$

Torej, $a+b = b+a$.

9. $\boxed{\Rightarrow}$ Če K nima neničelnih nilpotentnih elementov, je $x = 0$ očitno res edina rešitev enačbe $x^2 = 0$.

$\boxed{\Leftarrow}$ Naj bo $x = 0$ edina rešitev enačbe $x^2 = 0$ in naj bo $a \neq 0$ nilpotent. Z n označimo najmanjšo naravno število za katero je $a^n = 0$. Če je n sod, potem je

$$\underbrace{a^{\frac{n}{2}}}_{\text{ni nilpotent}} \neq 0 \Rightarrow a^n = \left(a^{\frac{n}{2}}\right)^2 = 0 \Rightarrow a^{\frac{n}{2}} \text{ neničelna rešitev enačbe } x^2 = 0 \quad \to \leftarrow$$

Če je n lih, potem je

$$a^{\frac{n+1}{2}} \neq 0 \Rightarrow \left(a^{\frac{n+1}{2}}\right)^2 = a^{n+1} = a^n a = 0a = 0 \Rightarrow a^{\frac{n+1}{2}} \text{ neničelna rešitev enačbe } x^2 = 0 \quad \to \leftarrow$$

Torej K ne premore neničelnega nilpotenta.

10. Naj bo K Boolov kolobar in $x \in K$ poljuben. Če vzamemo $y = x$ je

$$xyx = x^3 = x^2x = xx = x^2 = x.$$

Torej je K von Neumannev regularen. Naj bosta $a, b \in K$ poljubna.

$$\begin{aligned} a+b = (a+b) &= a^2 + ab + ba + b^2 = a + ab + ba + b \\ &\Rightarrow a + b = a + b + ab + ba \quad ((K,+) \text{ komutativna grupa}) \\ &\Rightarrow 0 = ab + ba \quad (\text{zakoni krajšanja}) \\ &\Rightarrow ab = -ba \end{aligned}$$

Za $b = a$ imamo $aa = -aa \Rightarrow a = -a$. Torej je vsak element v K sam sebi inverz. Natančneje, ker $ba \in K$ sledi $ba = -ba$. Torej $ab = -ba = ba$.

11. Poglejmo si elelmenta $(xe - exe)^2$ in $(ex - exe)^2$.

$$\begin{aligned} (xe - exe)^2 &= (xe - exe)(xe - exe) \\ &= xexe - xe^2xe - exexe + exe^2xe \\ &= xexe - xexe - exexe + exexe \\ &= 0 \\ &\Rightarrow xe - exe = 0 \quad (\text{ker ni nilpotent}) \end{aligned}$$

$$\begin{aligned} (ex - exe)^2 &= (ex - exe)(ex - exe) \\ &= exex - exexe - exe^2x + exe^2xe \\ &= exex - exexe - exex + exexe \\ &= 0 \\ &\Rightarrow ex - exe = 0 \quad (\text{ker ni nilpotent}) \end{aligned}$$

Torej,

$$xe - exe = ex - exe \Rightarrow xe = ex.$$

Dodatne naloge

1. Preveri, ali so naslednje množice kolobarji pri danih operacijah:

   (a) $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $+$ in $\cdot$ sta običajno seštevanje in množenje v $\mathbb{Q}$.

   (b) $R = \{(a,b) : a, b \in \mathbb{Z}\}$, $+$ in $\cdot$ sta definirana z

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b) \cdot (c,d) = (ac + bd, ad + bc).$$

(c) Množica vseh vektorjev v 3-dim Euklidskem prostoru s seštevanjem in množenjem vektorjev.

2. Naj bo K kolobar brez enote. Pokaži, da množica $\mathbb{Z} \times K$ postane kolobar (z enoto!), če jo opremimo z binarnima operacijama seštevanja in množenja takole:

$$(m,x)+(n,y) := (m+n, x+y),$$
$$(m,x)\cdot(n,y) := (mn, nx+my+xy)$$

(tu je mn produkt celih števil m in n, xy produkt elementov x in y v K ipd.)

3. Pokaži, da bi lahko kolobar ekvivalentno definirali brez zahteve o komutativnosti seštevanja (da torej enakost $x+y=y+x$ sledi iz ostalih aksiomov).

4. Dokaži: Množica $\mathrm{End}(G)$ vseh endomorfizmov abelove grupe G je kolobar za operaciji seštevanja in množenja, ki sta definirana z

$$(f+g)(a) = f(a)+g(a), \quad (f\cdot g)(a) = f(g(a)),$$

za $f,g \in \mathrm{End}(G)$.

5. Dokaži, da je kolobar vseh $n \times n$ matrik nad poljem F, von Neumannovo regualaren.

6. Če ima kolobar R enolični levi nevtralni element 1_l, potem je 1_l enota (1_l je tudi desni nevtralni element). Ali trditev velja, če izpustimo besedo "enolični"?

7. * Naj bo R končni kolobar velikosti $n > 1$, kjer je n produkt različnih praštevil. Dokaži da je R komutativen.

8. Dokaži, da za vsako praštevilo p obstaja nekomutativen kolobar velikosti p^2.

   Namig: Naj bo $R = \{(x,y) : x,y = 0,1,\ldots,p-1\}$. Seštevanje je definirano z $(x_1,x_2)+(y_1,y_2) = (x_1 +_p y_1, x_2 +_p y_2)$, množenje pa z $(x_1,x_2)\cdot(y_1,y_2) = (x_1 \cdot_p (y_1 +_p y_2), x_2 \cdot_p (y_1 +_p y_2))$. Pokaži, da je $(R,+,\cdot)$ nekomutativen kolobar velikosti p^2.

9. Naj bo $\mathbb{Z}_n$ kolobar celih števil po modulu n (množica ekvivalenčnih razredov celih števil po modulu n), elemente iz množice označujemo z $\overline{0},\overline{1},\ldots,\overline{n-1}$. Dokaži naslednjo trditev: če sta $m,n > 1$ tuji si števili, potem ima kolobar $\mathbb{Z}_{mn}$ vsaj še dva idempotentna elementa različna od $\overline{0}$ in $\overline{1}$.

10. ** Naj bo R kolobar v katerem je $x^3 = x$ za vse $x \in R$. Pokaži da je R komutativen.

    Namig: (Moj) dokaz je "precej grd". Namig je, da gre za poseben primer izreka N. Jacobsona ☺.

1.2. Delitelji niča. Celi kolobarji

Zgled 1.2.1. Naj $M_2(\mathbb{R})$ označuje množico vseh realnih matrik velikosti 2×2. Zlahka se prepričamo, da je $(M_2(\mathbb{R}), +, \cdot)$ kolobar z običajnim seštevanjem in množenjem matrik. Še več, $M_2(\mathbb{R})$ premore identiteto $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Za matriki

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ in } B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

velja $AB = B$ in $BA = 0_2$. Torej kolobar $M_2(\mathbb{R})$ ni komutativen.

Iz prejšnjega primera lahko vidimo še nekaj: produkt neničelnih elementov v kolobarju je lahko enak nič. Računanje je v kolobarjih torej vendarle nekoliko drugačno od računanja s števili.

Definicija 1.3

Če sta $a, b \in K$ taka neničelna elementa kolobarja K, da velja

$$ab = 0,$$

potem rečemo elementu a ***levi delitelj niča***, elementu b pa ***desni delitelj niča***. Posebej velja poudariti, da $0 \in K$ ni delitelj niča.

Pomembno je tudi izpostaviti, da delitelji niča nimajo inverznega elementa. Velja namreč naslednje.

Izrek 1.4

Levi delitelj niča je brez levega inverznega elementa, desni delitelj niča pa brez desnega inverznega elementa.

Dokaz: Naj bo produkt $ab = 0$ in naj ima faktor a levi inverzni element a', torej je $a'a = 1$. Če pomnožimo obe strani enačbe $0 = ab$ z a' z leve strani, dobimo po asociativnem zakonu $0 = a'(ab) = (a'a)b = 1b = b$. To je protislovje, saj je b delitelj niča in je neničelen.

♠

Zgled 1.2.2. Poglejmo si kolobar $\mathbb{Z}_{12}$. Lahko se prepričamo, da so $2, 3, 4, 6, 8, 9$ in 10 delitelji niča v $\mathbb{Z}_{12}$ ($2 \cdot_{12} 6 = 0$, $8 \cdot_{12} 3 = 0$, itn). Vidimo, da so delitelji niča v $\mathbb{Z}_{12}$ tisti elementi, ki niso tuji 12, tj. tisti elementi $a \in \mathbb{Z}_{12}$ za katere velja $nsd(a, 12) \neq 1$.

Izrek 1.5

Naj bo $m \in \mathbb{Z}_n$. Če je $m \neq 0$ in sta m in n tuja potem je m enota v $\mathbb{Z}_n$, če je $m \neq 0$ in m in n nista tuja, potem je m delitelj niča v $\mathbb{Z}_n$.

Dokaz: Predpostavimo, da je $m \neq 0$ in $nsd(m,n) = d \neq 1$. Iz $m\frac{n}{d} = \frac{m}{d}n$ velja, da je $\frac{m}{d}$ večkratnik n. To pomeni, da v $\mathbb{Z}_n$ velja $m\frac{n}{d} = 0 \in \mathbb{Z}_n$. Ker sta m in $\frac{n}{d}$ neničelna to pomeni, da je m delitelj niča.

Predpostavimo sedaj, da je $nsd(m,n) = 1$. Potem obstajata takšni celi števili $a, b \in \mathbb{Z}$, da velja $an + bm = 1$. Po Evklidovem algoritmu obstajata takšni celi števili q, r, da velja $0 \leq r < n$ in $b = nq + r$. Torej:

$$rm = (b - nq)m = bm - nqm = 1 - an - nqm = 1 - n(a + qm).$$

To pomeni, da je $rm = mr = 1$ v $\mathbb{Z}_n$, tj. m je enota.

♠

Posledica 1.1

Če je p praštevilo, potem je vsak neničelen element v $\mathbb{Z}_p$ enota. Z drugimi besedami, $\mathbb{Z}_p$ je polje in nima deliteljev niča.

Še en pokazatelj pomembnosti koncepta delitelja niča je prikazan v naslednjem izreku. Naj bo K kolobar in $a, b, c \in K$. V K veljata (multiplikativna) **zakona krajšanja**, če $ab = ac$ z $a \neq 0$ implicira $b = c$, in če $ba = ca$ z $a \neq 0$ implicira $b = c$. Seveda aditivna zakona krajšanja veljata v K, saj je $(K, +)$ grupa.

Izrek 1.6

Zakona krajšanja veljata v kolobarju K natanko tedaj, ko je K brez deliteljev niča.

Dokaz: Naj bo K kolobar v katerem zakona krajšanja držita. Predpostavimo, da velja $ab = 0$ za $a, b \in K$. Predpostavimo, da je $a \neq 0$. Ker veljata zakona krajšanja, iz $ab = a0$ sledi $b = 0$. Torej velja, da je $a = 0$ ali $b = 0$.

Sedaj predpostavimo, da K ne vsebuje deliteljev niča in naj bo $ab = ac$ z $a \neq 0$. Torej

$$ab - ac = a(b - c) = 0.$$

Ker je $a \neq 0$ in K nima deliteljev niča sledi, da je $b - c = 0$ oz $b = c$. Podobno se pokaže, da $ba = ca$, kjer je $a \neq 0$, implicira $b = c$.

♠

Definicija 1.4

Komutativen kolobar z identiteto $1 \neq 0$ in brez deliteljev niča, je ***cel kolobar***.

Izrek 1.7

Vsako polje je kolobar brez deliteljev niča.

Dokaz: Naj za elementa x in y kolobarja K velja $xy = 0$. Denimo, da je x obrnljiv. Enakost $xy = 0$ z leve pomnožimo z x^{-1} in dobimo $y = 0$. Podobno vidimo, da iz obrnljivosti y sledi $x = 0$.

♠

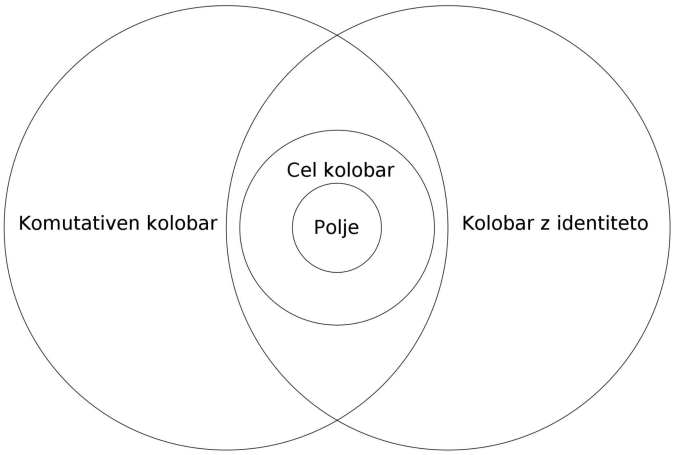
Zgled 1.2.3. Obrat prejšnje trditve ne drži. Namreč, kolobar $\mathbb{Z}$ nima deliteljev niča, vendar ni obseg.

Izrek 1.8

Vsak končen cel kolobar je polje.

Dokaz: Naj bo K končen cel kolobar in $0 \neq a \in K$ poljuben. Definirajmo preslikavo $f : K \to K$ z $f(x) = ax$. Pokažimo, da je f injektivna. Naj bo $f(x_1) = f(x_2)$, tj. $ax_1 = ax_2$. Ker je $a \neq 0$ in držita zakona krajšanja, velja $x_1 = x_2$. Ker je K končen, mora biti f surjektivna preslikava. Torej je f bijekcija. Z drugimi besedami, obstaja takšen enoličen $b \in K$, da je $f(b) = ab = 1$. Ker je K komutativen, velja $ba = 1$. To pomeni, da je a enota.

♠



Slika 1.1: Kolekcija kolobarjev.

Naloge

1. Ali je lahko delitelj niča v kolobarju z identiteto tudi obrnljiv?
2. Poišči delitelje niča v kolobarjih $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}^{2\times 2}$. Ali poznaš kakšen kolobar brez deliteljev niča?
3. Dokaži, da imamo v obsegu točno dva idempotentna elementa.
4. Dokaži naslednje; če je K končen kolobar z identiteto $1 \neq 0$ in brez deliteljev niča, potem je K obseg.
5. Naj bo $K \neq 0$ končen kolobar. Dokaži, da K premore desno identiteto natanko tedaj, ko premore (neničelni) element, ki ni desni delitelj niča.
6. Pokaži, da kolobarja $2\mathbb{Z}$ in $3\mathbb{Z}$ nista izomorfna. Ali sta $\mathbb{R}$ in $\mathbb{C}$ izomorfna?
7. Naj bo K kolobar, ki vsebuje p elementov, kjer je p praštevilo. Pokaži da je $K \cong (\mathbb{Z}_p, +, \cdot)$, če K vsebuje vsaj en neničeln produkt.
8. Naj bo K kolobar v katerem je $xy = \pm yx$ za vse $x, y \in K$. Dokaži, da je bodisi K komutativen kolobar, bodisi $xy = -yx$, za vse $x, y \in K$.
9. Naj bo K končen kolobar z vsaj enim elementom, ki ni delitelj niča. Dokaži:
   (a) K je kolobar z identiteto.
   (b) Če $b \in K$ ni obrnljiv, potem je b delitelj niča.

Rešitve

1. Naj bo K kolobar z enoto $1 \neq 0$. Predpostavimo, da takšen element obstaja. To pomeni, $ab = 0$ za $0 \neq a, b \in K$. Če je a obrnljiv, lahko najdemo $a^{-1} \in K$ in velja $aa^{-1} = a^{-1}a = 1$. Sledi,

$$a^{-1}a = 1 \Rightarrow (a^{-1}a)b = b \Rightarrow a^{-1}(ab) = b \Rightarrow 0 = b \rightarrow\leftarrow$$

2. V $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ velja samo za $\overline{2}$, da je $\overline{2}\cdot\overline{2} = 2\cdot 2 \mod 4 = 0$. Torej je $\overline{2}$ levi in desni delitelj niča. V $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ velja $\overline{2}\cdot\overline{3} = 2\cdot 3 \mod 6 = 0$ in $\overline{3}\cdot\overline{4} = 3\cdot 4 \mod 6 = 0$. V $\mathbb{Z}^{2\times 2}$ imamo neskončno mnogo deliteljev niča. Za $a, b \neq 0$ je

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

   Kolobarji $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ nimajo deliteljev niča.

Komentar: Obstajajo neskončni kolobarji z delitelji ničla. Na primer, naj bo $X \neq \emptyset$. Kolobar $B = (2^X, \triangle, \cap)$ je Boolov kolobar, torej, $A^2 = A$ za vse množice $A \in 2^X$. Če je $A \neq X, \emptyset$ potem sta A in $X \setminus A$ delitelja ničla v B. Naj bo $K = B \times B \times \ldots \times B \times \ldots$ kartezični produkt številno mnogo kopij B. Potem je K neskončen kolobar z delitelji ničla.

3. Očitna idempotenta sta 0 in 1. Predpostavimo, da je $a \neq 0,1$ idempotent, torej, $a^2 = a$. Ker smo v obsegu, obstaja a^{-1} in ko z njim pomnožimo obe strani prejšnje enakosti, dobimo $a = 1$. $\rightarrow\leftarrow$

4. Pokazati moramo, da je vsak element $a \neq 0$ kolobarja K obrnljiv. To pomeni, da obstaja takšen a^{-1}, da je $aa^{-1} = a^{-1}a = 1$. Ker je K končen, lahko brez izgube za splošnost pišemo

$$K = \{0, 1, a_1, \ldots, a_n\}.$$

Naj bo $a \neq 1$ poljuben element v K. Naj bo $S = aK$. Imamo torej

$$S = \{0, a, aa_1, \ldots, aa_n\}.$$

Trdimo, da so vsi elementi v S paroma različni. Ker nimamo deliteljev ničla, zakoni krajšanja veljajo. Torej, če bi bilo $aa_i = aa_j$, bi imeli $a_i = a_j$, vendar to ni možno. Od tod sledi, da je

$$S = \{0, a, aa_1, \ldots, aa_n\} = \{0, 1, a_1, \ldots, a_n\} = K.$$

Z drugimi besedami, obstaja takšen $a_i \in K$, da je $aa_i = 1$. Podobno, če vzamemo $S = Ka$, dobimo da obstaja takšen a_j, da je $a_j a = 1$. Če ima element levi in desni inverz, potem je obrnljiv. Torej, ker je bil a poljuben, je K obseg.

5. $\boxed{\Rightarrow}$ Naj bo $e \in K$ desna identiteta v K, torej, $ae = a$ za vse $a \in K$. Ker je $K \neq 0$ sledi $e \neq 0$. Če je $xe = 0$, sledi $x = 0$. Torej e ni desni delitelj ničla.

$\boxed{\Leftarrow}$ Predpostavimo, da K premore element $d \neq 0$, ki ni delitelj ničla. Torej,

$$ad \neq 0, \ \forall a \in K \setminus \{0\}.$$

Definirajmo preslikavo $f : K \to K$ s predpisom $f(x) = xd$.

Trdimo, da je f injekcia.

$$\begin{aligned} f(x) = f(y) &\Rightarrow xd = yd \\ &\Rightarrow xd - yd = 0 \\ &\Rightarrow (x-y)d = 0 \end{aligned}$$

$$\Rightarrow x - y = 0 \quad (d \text{ ni delitelj niča})$$
$$\Rightarrow x = y$$

Ker je K končen in f injekcia, je f surjekcia. Torej obstaja $x \in K$ takšen, da $f(x) = d$. Pokažimo, da je x desna identiteta v K.

$$\begin{aligned} f(x) = d &\Rightarrow xd = d \\ &\Rightarrow y(xd) = yd, \ \forall y \in K \\ &\Rightarrow (yx)d - yd = 0, \ \forall y \in K \\ &\Rightarrow (yx - y)d = 0, \ \forall y \in K \\ &\Rightarrow yx - y = 0, \ \forall y \in K \\ &\Rightarrow yx = y, \ \forall y \in K \end{aligned}$$

6. Če je $f : 2\mathbb{Z} \to 3\mathbb{Z}$ izomorfizem, iz teorije grup za $(2\mathbb{Z}, +)$ in $(3\mathbb{Z}, +)$ vemo, da je bodisi $f(2) = 3$, bodisi $f(2) = -3$. Torej sta možna homomorfizma $f(2n) = 3n$ ali $f(2n) = -3n$.

   - $f(2n) = 3n$. Za $n = 2$ imamo $f(4) = 6$, ampak $f(2)f(2) = 9$.
   - $f(2n) = -3n$. Za $n = 2$ imamo $f(4) = -6$, ampak $f(2)f(2) = 9$.

   Torej $(2\mathbb{Z}, +, \cdot) \ncong (3\mathbb{Z}, +, \cdot)$.

   Predpostavimo, da je $f : \mathbb{C} \to \mathbb{R}$ izomorfizem. Ker homomorfizem kolobarjev ohrani idempotente velja $f(1) = 1$. Homomorfizem kolobarjev ohrani tudi obrnljivost, torej $f(-1) = -1$. Naj bo $a = f(i)$. Imamo

   $$a^2 = f(i)f(i) = f(i^2) = f(-1) = -1,$$

   ampak vemo, da ne obstaja takšen $a \in \mathbb{R}$, da je $r^2 = -1$. Torej ne more obstajati izomofrizem med $\mathbb{C}$ in $\mathbb{R}$.

7. Naj bo K kolobar s p elementi, kjer je p praštevilo. Ker je vsaka grupa praštevilčnega reda ciklična, je ciklična tudi $(K, +)$. Če je a eden izmed generatorjev grupe, potem imamo

   $$K = \{a, 2a, 3a, \ldots, (p-1)a, pa = 0\}.$$

   Naj bo $a^2 = ka, \ 1 \leq k \leq p$. Če je $k = p$, potem so vsi produkti v K enaki 0, kar je v protislovju s predpostavko, da obstaja vsaj en neničelen produkt. Torej $k \neq p$. Z

drugimi besedami: $nsd(k,p)=1$. Iz teorije števil vemo:

$$(\exists l,m\in\mathbb{Z})\ lk+mp=1.$$

Trdimo, da je preslikava $f:\mathbb{Z}_p\to K$ s predpisom $f(\bar{i})=ila$ izomorfizem kolobarjev.

(i) Injektivnost. Naj bosta $\bar{i},\bar{j}\in\mathbb{Z}_p$ poljubna.

$$\begin{aligned} f(\bar{i})=f(\bar{j}) &\Rightarrow ila=jla\\ &\Rightarrow ila-jla=0\\ &\Rightarrow (i-j)la=0\\ &\overset{(\star)}{\Rightarrow} i-j=0\\ &\Rightarrow i=j\\ &\Rightarrow \bar{i}=\bar{j} \end{aligned}$$

$(\star)$: $a\neq 0$, ker je a generator. Če bi $l=0$, bi imeli $mp=1$, kar pa ni možno, ker je $p>1$.

(ii) Surjektivnost. Ker je K končen in f injekcia, je f surjekcia.

(iii) Homomorfizem. Naj bosta $\bar{i},\bar{j}\in\mathbb{Z}_p$ poljubna.

$$\begin{aligned} f(\bar{i}+\bar{j})=f(\overline{i+j})=(i+j)la=ila+jla=f(\bar{i})+f(\bar{j})\\ f(\bar{i})f(\bar{j})=(ila)(jla)=\underbrace{(a+a+\ldots+a)}_{il}\underbrace{(a+a+\ldots+a)}_{jl}=ijl^2a^2=ijl^2ka=ijllka\\ =ijl(1-mp)a=ijla-ijm\underbrace{(pa)}_{=0}=ijla=f(\overline{ij}) \end{aligned}$$

Iz $(i),(ii),(iii)$ sledi, da je f izomorfizem med K in $\mathbb{Z}_p$.

8. Naj bo $a\in K$ poljuben fiksen element. Definirajmo množici

$$\begin{aligned} C_a&=\{x\in K|xa=ax\}\\ D_a&=\{x\in K|xa=-ax\}. \end{aligned}$$

Imamo $K=C_a\cup D_a,\ C_a\cap D_a=\emptyset$ za vse $a\in K$. Če je $K\neq C_a$ in $K\neq D_a$, potem obstajata elementa $c\in C_a\setminus D_a$ in $d\in D_a\setminus C_a$. Ker je $(K,+)$ komutativna grupa, velja $c+d\in K$. Torej, za $a\in K$ velja $(c+d)a=a(c+d)$ ali $(c+d)=-a(c+d)$. Če je $(c+d)a=a(c+d)$, potem $ca+da=ac+ad\Rightarrow da=ad$, kar pomeni da je $d\in C_a$, kar je protislovlje. Podobno dobimo, da je $c\in D_a$, kar je protislovlje. Torej,

$K = C_a \veebar K = D_a$. Označimo z

$$U = \{a \in K : C_a = K\}$$
$$V = \{a \in K : D_a = K\}$$

Opazimo, da je $K = U \cup V$. Če je $K \neq U$ in $K \neq V$, lahko najdemo elementa $u \in U \setminus V$ in $v \in V \setminus U$.

$$u \in U \setminus V \Rightarrow C_u = K \ \wedge C_u \neq D_u \Rightarrow xu = ux \ \wedge xu \neq -ux$$
$$v \in V \setminus U \Rightarrow D_v = K \ \wedge D_v \neq C_v \Rightarrow xv = -vx \ \wedge xv \neq vx$$

Ker je $u+v \in K$, imamo $u+v \in U$ ali $u+v \in V$. Če je $u+v \in U$, potem $C_{u+v} = K$. To pomeni, da za vse $x \in K$, $x(u+v) = (u+v)x \Rightarrow xu+xv = ux+vx$. Ker je $ux = xu$, sledi $xv = vx$, $\forall x \in K$. Torej $C_v = K$, od tod bi sledilo da $v \in U$, kar je protislovje. Na podoben način pokažemo $D_u = K$, od koder sledi, da je $u \in V$, kar je protislovje. Torej, $K = U \veebar K = V$. Z drugimi besedami, K je komutativen ali pa velja $xy = -yx$, za vse $x, y \in K$.

9. (a) Naj bo $a \in K$ element, ki ni delitelj niča. Ker je K končen vemo, da obstajata takšni pozitivni celi števili m in n, da velja $a^m = a^n$. Predpostavimo, da je $m < n$. Imamo $a^{m-1}\left(a - a^{n-m+1}\right) = 0$ in ker a ni delitelj niča, velja $a^{n-m+1} = a$.

   Naj bo $b \in K$ poljuben. Imamo $ba = ba^{n-m+1}$, ali ekvivalentno $(b - ba^{n-m})a = 0$. Od tod sledi $b = ba^{n-m}$ (ker a ni delitelj niča). Podobno dobimo $b = a^{n-m}b$. Torej je a^{n-m} enota v kolobarju K.

   (b) Iz (a) sledi, da za vsak element a, ki ni delitelj niča obstaja inverz $a^{-1} = a^{n-m-1}$. Z uporabo protislovja dobimo: če $b \in K$ ne premore inverza, potem je b delitelj niča.

1.3. Karakteristika kolobarja. Izreka Fermata in Eulerja.

Definicija 1.5

Če za kolobar K obstaja takšno pozitivno celo število n, da velja $n \cdot a = 0$ za vse $a \in K$, potem najmanjšemu takšnemu številu n pravimo ***karakteristika kolobarja*** K in pišemo $char(K) = n$. Če takšno število ne obstaja, potem pravimo, da je K karakteristike 0.

Zgled 1.3.1. Karakteristika kolobarja $\mathbb{Z}_n$ je enaka n. Kolobarji $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ in $\mathbb{C}$ imajo karakteristiko 0.

Na prvi pogled se zdi, da določanje karakteristike ni enostavno razen, če je kolobar karakteristike 0. Ali res moramo preveriti, če vsak element a kolobarja K zadošča zgoraj napisani definiciji? Naslednji izrek pravi, da če kolobar premore identiteto 1, potem je dovolj preveriti definicijo za $a = 1$.

Izrek 1.9

Naj bo K kolobar z identiteto. Če je $n \cdot 1 \neq 0$ za vse $n \in \mathbb{Z}^+$, potem ima K karakteristiko 0. V nasprotnem je najmanjše število n, za katero je $n \cdot 1 = 0$, karakteristika kolobarja K.

Dokaz: Predpostavimo, da je $n \cdot 1 \neq 0$ za vse $n \in \mathbb{Z}^+$, potem zagotovo ne moremo imeti $n \cdot a = 0$ za nek $a \in K$ in nek $n \in \mathbb{N}$. To pomeni, da je K karakteristike nič. Z druge strani, če je $n \cdot 1 = 0$. Potem, za poljuben $a \in K$, velja

$$n \cdot a = a + a + \cdots + a = a(1 + 1 + \cdots + a) = a(n \cdot 1) = a0 = 0.$$

♠

Vemo, da sta, kot aditivni grupi, $\mathbb{Z}_n$ in $\mathbb{Z}/n\mathbb{Z}$ izomorfni, pri čemer odsek $a + n\mathbb{Z}$ ustreza elementu a za vsak $a \in \mathbb{Z}_n$. Poleg tega lahko seštevanje odsekov v $\mathbb{Z}/n\mathbb{Z}$ izvedemo tako, da izberemo poljubne predstavnike, jih dodamo v $\mathbb{Z}$ in poiščemo odsek v $n\mathbb{Z}$, ki vsebuje njihovo vsoto. Ni težko opaziti, da je mogoče $\mathbb{Z}/n\mathbb{Z}$ razširiti v kolobar tako, da množenje odsekov definiramo na podoben način, tj. z množenjem poljubnih izbranih predstavnikov odsekov. Čeprav bomo to kasneje pokazali v bolj splošni situaciji, bomo sedaj naredili poseben primer. Pokazati moramo le, da je takšno množenje predstavnikov dobro definirano, saj bodo asociativnost množenja in distribucijski zakoni sledili iz izbrane lastnosti predstavnikov v $\mathbb{Z}$. Izberimo sedaj predstavnika $a + rn$ in $b + sn$ (namesto a in b) iz odsekov $a + n\mathbb{Z}$ in $b + n\mathbb{Z}$. Potem je

$$(a + rn)(b + sn) = ab + (as + rb + rsn)n,$$

ki je tudi element $ab + n\mathbb{Z}$. S tem smo pokazali, da je množenje dobro definirano in naši odseki tvorijo kolobar izomorfen kolobarju $\mathbb{Z}_n$. Naslednji izrek bo v veliko pomoč pri reševanju sledečih nalog.

Izrek 1.10: Fermatov mali izrek

Za vsako celo število a in praštevilo p, ki je a tuje, velja:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz: Kolobar $\mathbb{Z}_p$ je polje, kar pomeni, da so vsi neničelni elementi v $\mathbb{Z}_n$ enote. Torej, $(\mathbb{Z}_p^*, \cdot)$ je grupa s $p-1$ elementi. Red poljubnega elementa $b \in \mathbb{Z}_p^*$ je delitelj $|Z_p^*| = p-1$. To pomeni, da je $b^{p-1} = 1 \in \mathbb{Z}_p$. Kolobarja $\mathbb{Z}_p$ in $\mathbb{Z}/p\mathbb{Z}$ sta izomorfna, pri čemer element $b \in \mathbb{Z}_p$ ustreza odseku $b + p\mathbb{Z}$. Za poljuben $a \in \mathbb{Z}$, ki ni delitelj večkratnika p, velja $a + p\mathbb{Z} = b + p\mathbb{Z}$ za nek $0 \leq b \leq p-1$. Torej,

$$(a + p\mathbb{Z})^{p-1} = (b + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}.$$

Z drugimi besedami,

$$a^{p-1} \equiv 1 (\text{mod } p).$$

♠

Posledica 1.2

Za poljubo celo število a in praštevilo p velja:

$$a^p \equiv a \pmod{p}.$$

Poznamo tudi Eulerjevo posplošitev Fermatovega izreka, ki sledi iz našega naslednjega izreka, ki ga dokažemo s štetjem.

Izrek 1.11

Množica G_n neničelnih elementov kolobarja $\mathbb{Z}_n$, ki niso delitelji niča, tvori multiplikativno grupo.

Dokaz: Najprej moramo dokazati, da je G_n zaprt pod množenjem modulo n. Naj bosta $a, b \in G_n$ poljubna. Če $ab \notin G_n$, potem obstaja takšen $c \neq 0$ v $\mathbb{Z}_n$, da velja $(ab)c = 0$. To pomeni, da je $a(bc) = 0$. Ker je $b \in G_n$ in $c \neq 0$ je $bc \neq 0$. Ampak od tod bi sledilo, da $a \notin G_n$, kar nas privede do protislovja. Pokažimo sedaj, da elementi v G_n tvorijo multiplikativno grupo. Ni se težko prepričati, da je množenje modulo n asociativno ter $1 \in G_n$. Pokazati moramo še, da so elementi v G_n enote. Naj bo $a \in G_n$ poljuben in naj so

$$1, a_1, \ldots, a_r$$

elementi v G_n. Elementi $a1, aa_1, \ldots, aa_r$ so paroma različni. Z drugimi besedami, če je $aa_i = aa_j$, potem je $a(a_i - a_j) = 0$. Ker je $a \in G_n$ in ni delitelj niča velja, da je $a_i - a_j = 0$

oz $a_i = a_j$. To pomeni, da je bodisi $a1 = 1$ bodisi $aa_i = 1$, za nek $a_i \in G_n$. Torej je a enota v G_n.

♠

Definicija 1.6: Eulerjeva funkcija

Eulerjeva funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ je multiplikativna aritimetična funkcija poljubnega pozitivnega celega števila n in vrne skupno število pozitivnih celih števi, ki so manjša od n in so n tuja. Z drugimi besedami:

$$\varphi(n) = |\{d \in \mathbb{N} : nsd(d,n) = 1,\ 1 \leq d < n\}|.$$

Zgled 1.3.2. $\varphi(12) = 4$, ker so $1,5,7$ in 11 tuji 12.

Sedaj lahko pokažemo Eulerjevo generalizacijo malega Fermatovega izreka.

Izrek 1.12: Euler

Za poljubno celo število a, ki je tuje n, velja

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dokaz: Če je a tuje n, potem odsek $a + n\mathbb{Z}$ od $n\mathbb{Z}$ vsebuje celo število $b < n$, ki je tuje n. Ker je množenje predstavnikov odsekov dobro definirano velja

$$a^{\varphi(n)} \equiv b^{\varphi(n)} (\text{mod } n).$$

Z druge strani, ker je b tuje n potem b ni delitelj niča v $\mathbb{Z}_n$. To pomeni, da je $b \in G_n$ in je reda $\varphi(n)$. Od tod sledi, da je

$$b^{\varphi(n)} \equiv 1 (\text{mod } n).$$

Trditev sledi iz osnovnih lastnosti kongruenc.

♠

S pomočjo Izreka 1.11 lahko najdemo vse rešitve linearne kongruence $ax \equiv b (\text{mod } m)$. Zaradi lažjega računanja ponavadi raje delamo z enačbo v $\mathbb{Z}_m$ in rezultate interpretiramo za kongruence.

Izrek 1.13

Naj bo $m \in \mathbb{N}$ in $a \in \mathbb{Z}_m$ tuje m. Za vsak $b \in \mathbb{Z}_m$ ima enačba $ax = b$ točno eno rešitev v $\mathbb{Z}_m$.

Dokaz: Po Izreku 1.11 je a enota v $\mathbb{Z}_m$ in $s = a^{-1}b$ je rešitev dane enačbe. Če pomnožimo obe strani dane enačbe z a^{-1} z leve, vidimo, da je to edina rešitev.

♠

Ko interpretiramo ta izrek za kongruence, dobimo naslednjo posledico.

Posledica 1.3

Če sta a in b tuja, potem ima za vsako celo število b kongruenca $ax \equiv b (\text{mod } m)$ za rešitev vsa cela števila, ki so v natanko enem razredu ostankov modulo m.

Izrek 1.14

Naj bo $m \in \mathbb{N}$ in $a, b \in \mathbb{Z}_m$ pri čemer je $d = nsd(a,m)$. Enačba $ax = b$ ima v $\mathbb{Z}_m$ rešitev natanko tedaj, ko d deli b. Še več, enačba ima v tem primeru točno d rešitev v $\mathbb{Z}_m$.

Dokaz: Najprej pokažimo, da v $\mathbb{Z}_m$ ni rešitve dane enačbe, razen če d deli b. Recimo, da je $s \in \mathbb{Z}_m$ rešitev. Potem je $as - b = qm$ v $\mathbb{Z}$, torej $b = as - qm$. Ker d deli oba a in m vidimo, da d deli desno stran enačbe $b = as - qm$ in zato deli b. Tako lahko rešitev s obstaja le, če d deli b. Recimo sedaj, da d deli b. Naj bo

$$a = a_1 d, \quad b = b_1 d, \quad m = m_1 d.$$

Nato lahko enačbo $as - b = qm$ v $\mathbb{Z}$ prepišemo kot $d(a_1 s - b_1) = dqm_1$. Vidimo, da je $as - b$ večkratnik m natanko tedaj, ko je $a_1 s - b_1$ večkratnik m_1. Takšne rešitve s enačbe $ax = b$ v $\mathbb{Z}_m$ so ravno elementi, ki po modulu m_1 rešijo enačbo $a_1 x = b_1$ v $\mathbb{Z}_{m_1}$. Sedaj naj $s \in \mathbb{Z}_{m_1}$ zadošča pogojem Izreka 1.13, torej je enolična rešitev enačbe $a_1 x = b_1$ v $\mathbb{Z}_{m_1}$. Števila v $\mathbb{Z}_m$, ki se reducirajo na s po modulu m_1, so ravno tista, ki jih lahko izračunamo v $\mathbb{Z}_m$ kot

$$s,\ s + m_1,\ s + 2m_1,\ s + 3m_1, \ldots,\ s + (d-1)m_1.$$

Torej dobimo, da obstaja točno d rešitev enačbe v $\mathbb{Z}_m$.

♠

Posledica 1.4

Naj bo $d = nsd(a,m)$. Kongruenca $ax \equiv b (\text{mod } m)$ ima rešitev natanko tedaj, ko d deli b. Še več, rešitve so cela števila, ki so v točno d različnih razredih ostankov po modulu m.

Komentar 1.2

Več o uporabi Fermatovega in Eulerjevega izreka, ter metodi reševanja linearnih enačb predstavimo v naslednjem podrazdelku.

Naloge

1. Poišči ostanek pri deljenu števila 37^{49} s številom 7.
2. Poišči vse rešitve danih kongruenc:
   (a) $2x \equiv 6 \pmod 4$
   (b) $155x \equiv 75 \pmod{65}$
   (c) $39x \equiv 52 \pmod{130}$
3. Poišči ostanek pri deljenu števila $2^{2^{17}}+1$ s številom 24.
4. Pokaži, da za poljuben $n \in \mathbb{N}$ velja $n^{33} \equiv n \pmod{15}$.
5. Poišči $\varphi(p^n)$, kjer je p praštevilo in $n \in \mathbb{N}$.
6. Poišči $\varphi(p_1 p_2 \dots p_r)$, pri čemer so $p_1, \dots, p_r$ paroma različna praštevila.
7. Poišči $\varphi(n)$ za poljubno celo število n. S pomočjo pridobljene formule in Eulerjevega izreka poišči zadnji dve števki od 19^{4322}.
8. Dokaži, da je karakteristika celega kolobarja D enaka 0 ali p, pri čemer je p praštevilo.
9. Naj bo K komutativen kolobar z identiteto in $char(K) = 3$. Izračunaj in poenostavi $(a+b)^9$, $a, b \in K$.
10. Pokaži: 1 in $p-1$ sta edina elementa v $\mathbb{Z}_p$, ki sta sama sebi multiplikativna inverza.
11. Naj bo D cel kolobar, ki premore $0 \neq a \in D$ in $n \in \mathbb{N}$, da je $na = 0$. Pokaži, da je karakteristika celega kolobarja D pozitivno celo število d, ki deli n.
12. Naj bo K kolobar in n takšno pozitivno celo število, da velja $x^n = x$, za vse $x \in R$. Pokaži: če je n liho, potem je $char(K)$ enak produktu različnih števil, in če je n sodo, potem je $char(K) = 2$.
13. Naj bo $(K, +, \cdot)$ kolobar v katerem je vsak element idempotent. Pokaži, da ima kolobar K karakteristiko 2 in da je komutativen.

Rešitve

1. Ker je $nsd(37,7) = 1$, po Fermatovem malem izreku velja $37^6 \equiv 1 \pmod 7$. Za izračun 37^{49} bomo uporabili standardne matematične operacije, natančneje potenciranje in množenje. (Podobno, kot če bi delali z običajnimi enačbami).

$$\begin{aligned} 37^6 &\equiv 1 \pmod 7 \quad \Big|^{8} \\ 37^{48} &\equiv 1 \pmod 7 \quad \Big| \cdot 37 \\ 37^{49} &\equiv 37 \pmod 7 \\ 37^{49} &\equiv 2 \pmod 7 \end{aligned}$$

2. Če sta $a,n \in \mathbb{N}$ in $b \in \mathbb{Z}$, ima kongruenca $ax \equiv b \pmod n$ rešitev natanko tedaj, ko $d|b$, pri čemer je $d = nsd(a,n)$.Če je ta pogoj izpolnjen, ima kongruenca natanko d nekongruentnih rešitev modulo n, ki so oblike

$$x_0 + \frac{n}{d}t,\ t = 0,1,\ldots,d-1,$$

kjer je x_0 enolična rešitev kongruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Če $d \nmid b$, potem kongruenca nima rešitev.

(a) Ker je $nsd(2,4) = 2$ in $2|6$, ima kongruenca natanko dve rešitvi. Poglejmo si kongruenco $x \equiv 3 \pmod 2$. Ugotovimo lahko, da je $x_0 = 3$, kar pomeni, da sta rešitvi oblike $x \equiv 3 \pmod 4$ in $x \equiv 5 \pmod 4 \equiv 1 \pmod 4$.

(b) $nsd(155,65)$ izračunamo z uporabo Euklidevega algoritma..

$$\begin{aligned} 155 &= 2 \cdot 65 + 25 \\ 65 &= 2 \cdot 25 + 15 \\ 25 &= 1 \cdot 15 + 10 \\ 15 &= 1 \cdot 10 + 5 \\ 10 &= 2 \cdot 5 \end{aligned}$$

Ker je $nsd(155,65) = 5$ in $5|75$, ima kongruenca natanko 5 rešitev. Poglejmo si kongruenco $31x \equiv 15 \pmod{13}$. V prejšnjem primeru je bilo zelo enostavno videti, kaj je x_0, saj smo imeli samo x na levi strani kongruence. Sedaj se bomo rešitve lotili nekoliko drugače. Z uporabo zgornjega Evklidskega

algoritma bomo ugotovili, kaj je x_0 (ta metoda vedno deluje in je zelo enostavna, le pri izračunih moramo biti previdni). Kar moramo narediti je, da se sprehodimo čez Evklidski algoritem v obratnem vrstnem redu in ugotovimo za katera cela števila $x, y \in \mathbb{Z}$ velja $5 = 155x + 65y$.

$$\begin{aligned} 5 &= 15 - 10 \\ &= 15 - (25 - 15) \\ &= 2 \cdot 15 - 25 \\ &= 2 \cdot (65 - 2 \cdot 25) - 25 \\ &= 2 \cdot 65 - 5 \cdot 25 \\ &= 65 - 5 \cdot (155 - 2 \cdot 65) \\ &= 12 \cdot 65 + (-5) \cdot 155 \end{aligned}$$

Torej imamo, $155 \cdot (-5) + 65 \cdot 12 = 5$. Če pomnožimo dano enakost s 15 dobimo $155 \cdot (-75) + 65 \cdot 180 = 75$, oz. $155 \cdot (-75) \equiv 75 \pmod{65}$. Kar pomeni, da je $x_0 \equiv -75 \pmod{65} \equiv -10 \pmod{65} \equiv 55 \pmod{65}$. Ena rešitev je $x \equiv 55 \pmod{65}$. Za $t = 1, \ldots, 4$ ugotovimo, da so preostale nekongruentne rešitve po modulu 65 dane z $x \equiv 3, 16, 29, 42 \pmod{65}$.

(c) Ker je $nsd(39, 130) = 13$ in $13|52$, ima dana kongrenca natanko 13 rešitev. Poglejmo si kongruenco $3x \equiv 4 \pmod{10}$. Uganemo lahko, da je $x_0 = 8$. Torej so rešitve dane kongruence dane z $x \equiv 8 + 10t \pmod{130}$, where $t = 0, 1, \ldots, 12$.

3. Ker je $nsd(2, 19) = 1$, po Fermatovem malem izreku sledi, da je $2^{18} \equiv 1 \pmod{19}$. Poglejmo si koliko je $2^{17} \pmod{18}$.

$$2^{17} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 \cdot 2 \equiv (-2) \cdot (-2) \cdot (-2) \cdot (-2) \cdot 2 \pmod{18} \equiv 32 \pmod{18} \equiv 14 \pmod{18}$$

Z drugimi besedami; obstaja takšen $q \in \mathbb{Z}$, da velja $2^{17} = 18q + 14$. Torej,

$$2^{2^{17}} = 2^{18q+14} = (2^{18})^q \cdot 2^{14} \equiv 1^q \cdot 2^{14} \pmod{19}.$$

Z druge strani:

$$2^{14} = (2^4)^3 \cdot 2^2 \equiv (-3)^3 \cdot 4 \pmod{19} \equiv -108 \pmod{19} \equiv -13 \pmod{19} \equiv 6 \pmod{19}.$$

To pomeni,

$$2^{2^{17}} \equiv 6 \pmod{19} \Rightarrow 2^{2^{17}} + 1 \equiv 7 \pmod{19}.$$

4. Ker je $15 = 3 \cdot 5$, zadostuje, da pokažemo $n^{33} \equiv n \pmod{3}$ in $n^{33} \equiv n \pmod{5}$.

Če $3|n$, potem $3|n(n^{32}-1) \Rightarrow 3|(n^{33}-n)$. Z drugimi besedami, $n^{33} \equiv n \pmod 3$. Če $3 \nmid n$ po Fermatovem malem izreku sledi

$$\left.\begin{aligned} n^2 \equiv 1 \pmod 3 \end{aligned}\right|^{16} \Rightarrow n^{32} \equiv 1 \pmod 3$$
$$\Rightarrow n^{33} \equiv n \pmod 3$$

Torej za vse $n \in \mathbb{N}$ velja, da je $n^{33} \equiv n \pmod 3$. Podobno se pokaže, da je $n^{33} \equiv n \pmod 5$, za vse $n \in \mathbb{N}$.

5. Naj bosta m in n dve tuji celi števili. Poglejmo si kolobarja $\mathbb{Z}_{mn}$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. V našem primeru vemo, da je $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Ker sta oba kolobarja končna, je število enot v $\mathbb{Z}_m \times \mathbb{Z}_n$ enako številu enot v $\mathbb{Z}_m$ pomnoženemu s številom enot v $\mathbb{Z}_n$. Število enot v $\mathbb{Z}_n$ je enako $\varphi(n)$. Tako je zaradi izomorfizma število enot v $\mathbb{Z}_{mn}$ $\varphi(mn)$ in je enako $\varphi(m)\varphi(n)$. Z uporabo dejstva, da so $p_1, \ldots, p_r$ vsa paroma tuja števila in $\varphi(p_i) = p_i - 1$ dobimo, da je

$$\varphi(p_1 p_2 \ldots p_r) = (p_1 - 1)(p_2 - 1)\ldots(p_r - 1).$$

6. Vsa pozitivna cela števila, manjša od p^n, ki niso deljiva s p, so p tuja. Tako iz $p^n - 1$ celih števil izbrišemo cela števila manjša od p^n deljiva s p: $p, 2p, \ldots, (p^{n-1}-1)p$. Torej,
$$\varphi(p^n) = p^n - 1 - (p^{n-1} - 1) = p^n p^{n-1} = p^{n-1}(p-1).$$

7. Naj bo $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ faktorizacija števila n. Za vsak $1 \leq i, j \leq r,\ i \neq j$, velja, da je $\gcd(p_i^{k_i}, p_j^{k_j}) = 1$. Po ugotovitvah iz prejšnjih dveh problemov dobimo:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\ldots\varphi(p_r^{k_r}) \\ &= p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\ldots p_r^{k_r-1}(p_r-1) \end{aligned}$$

Če vzamemo faktor p_i od $(p_i - 1)$, dobimo

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Z uporabo zgornje formule in destva, da je $nsd(19, 100) = 1$ sledi, da je $\varphi(100) = 40$. Sedaj uporabimo Eulerjev izrek in dobimo, da je $19^{40} \equiv 1 \pmod{100}$. Če sedaj obe strani kongruence potenciramo s 108, dobimo $19^{4320} \equiv 1 \pmod{100}$. Ker je $19^2 = 361 \equiv 61 \pmod{100}$, sledi, da je $19^{4322} \equiv 61 \pmod{100}$. Z drugimi besedami, zadnji dve števki 19^{4322} sta 6 in 1.

8. Naj bo D cel kolobar z enoto 1. Upoštevali bomo dva primera na podlagi

aditivnega reda enote 1:

(a) $ord(1)$ je neskončen. V tem primeru ne more obstajati takšno pozitivno celo število $n \in \mathbb{N}$, da je $n \cdot 1 = 0$. Tako je $char(D) = 0$.

(b) $ord(1) = n$. Recimo, da je $n = kl$ za nek $1 < k,l < n$. Ker D nima deliteljev niča in ker je

$$0 = n \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1),$$

moramo imeti bodisi $k \cdot 1 = 0$ bodisi $l \cdot 1 = 0$, kar je protislovje s tem, da je n najmanjše celo število, za katerega $n \cdot 1 = 0$. Tako mora biti n praštevilo. Poleg tega velja, če je $a \in D$ je $na = (n \cdot 1) \cdot a = 0a = 0$, oz.$char(D) = n$.

9. Ker je R **komutativen**, velja binomski izrek. To pomeni, da za poljubna števila $a,b \in R$ in $n \in \mathbb{N}$ velja

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Za $n = 9$ je torej

$$(a+b)^9 = a^9 + \sum_{k=1}^{8} \binom{9}{k} a^{9-k} b^k + b^9.$$

Ker je $char(R) = 3$ in $3 | \binom{9}{k}$ za $1 \leq k \leq 8$, je srednja vsota zgoraj enaka nič. Torej je $(a+b)^9 = a^9 + b^9$.

10. Če je $a \in \mathbb{Z}_p$ sam sebi inverz, potem velja $a \cdot a = a^2 = 1$. Torej je $a^2 - 1 = (a-1)(a+1)$. Ker $\mathbb{Z}_p$ nima deliteljev niča, je bodisi $a - 1 = 0 \pmod p$ bodisi $a + 1 = 0 \pmod p$. Torej $a = 1$ ali $a = -1 \pmod p$.

11. Naj bo $char(D) = d$, pri čemer je $d \leq n$. Velja:

$$0 = na = (n \cdot 1) \cdot \underbrace{a}_{\neq 0} \Rightarrow n \cdot 1 = 0, \ \forall n.$$

Če vzamemo poljuben $x \in D$, potem $nx = n \cdot 1 \cdot x = 0$. Predpostavimo, da $d \nmid n$. To pomeni, da obstajata takšna $k,l \in \mathbb{Z}$, da je $n = kd + l, \ l < d$. Če pomnožimo dano enakost z x dobimo

$$0 = nx = \underbrace{kdx}_{=0} + lx \Rightarrow lx = 0,$$

kar je v protislovju z $l < d$.

12. Naj bo $k \in \mathbb{N}$ in $x \in R$, potem $kx \in R$. Torej,

$$(kx)^n = kx$$

$$\Leftrightarrow k^n x^n = kx$$
$$\Leftrightarrow k^n x = kx$$
$$\Leftrightarrow (k^n - k)x = 0$$

Dokažimo najprej naslednjo trditev.
Trditev: Če je $char(R) = c > 0$ in $dx = 0$ za vse $x \in R$, potem $c|d$.

Dokaz. Predpostavimo, da $c \nmid d$. Po osnovnem izreku o deljenju, obstajata takšna $l, k \in \mathbb{Z}^+$, da je $d = kc + l$ in $l < c$. Če pomnožimo enakost z $x \in R$, dobimo

$$0 = dx = k(cx) + lx = 0 + lx = lx,$$

kar je protislovje, ker je $char(R) = c > l$. Torej mora veljati, da $c|d$. □

Iz trditve sledi, da je $char(R)|(k^n - k)$ za vsak $k \in \mathbb{N}$. Brez izgube za splošnost predpostavimo, da je $char(R) = p^2$, kjer je $p > 2$ praštevilo. Sedaj imamo

$$p^2|(k^n k),\ \forall k \in \mathbb{N} \Rightarrow p^2|(p^n p) \Rightarrow p^2|p(p^{n-1} - 1) \Rightarrow p|p^{n-1} - 1,$$

vendar to ni res, saj smo dobili, da je p enak zmnožku različnih praštevil. Če je $x \in R$ potem $-x \in R$. Naj bo $n = 2k$, potem je

$$-x = (-x)^n = (-x)^{2k} = [(-x)^2]^k = [x^2]^k = x^{2k} = x.$$

Od tod mora slediti, da je $x = -x$, oziroma $2x = 0$, kar pomeni, da je $char(R) = 2$.

13. Naj bo $x \in R$ poljuben. Ker je vsak element idempotenten, to pomeni, da je tudi $x + x$ idempotent, torej je

$$(x+x)^2 = x + x \Leftrightarrow x^2 + x^2 + x^2 + x^2 = x + x \Rightarrow x + x + x + x = x + x \Rightarrow 2x = 0.$$

Ker je bil x poljuben, sledi, da je $char(R) = 2$. Naj bodo $x, y \in R$ poljubni in različni. Imamo:

$$(x+y)^2 = x + y \Rightarrow x^2 + xy + yx + y^2 = x + y \Rightarrow x + xy + yx + y = x + y \Rightarrow xy + yx = 0$$

Ker je $xy \in R$, sledi, da je $2xy = 0$ Torej $xy + yx = 2xy \Rightarrow yx = xy$.

1.4. Polje ulomkov

Kot smo že omenili na predavanjih, je vsako polje tudi cel kolobar. Obratno pa ni nujno res: obstaja veliko celih kolobarjev, ki niso polja. Vprašanje, ki se seveda

pojavi, pa je naslednje: kako lahko cel kolobar na naraven način "dopolnimo" do polja? Kot zgled in motivacijo si najprej poglejmo konstrukcijo racionalnih števil $\mathbb{Q}$ iz (celega kolobarja) celih števil: racionalna števila je mogoče predstaviti kot formalne količnike dveh celih števil. Element $p/q \in \mathbb{Q}$, kjer je $q \neq 0$, je kvocient dveh celih števil p in q. Vendar pa lahko različni pari celih števil predstavljajo isto racionalno število. Na primer, $1/2 = 2/4 = 3/6$. Vemo, da je

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \qquad (b \neq 0, d \neq 0).$$

Bolj formalen način obravnavanja tega problema je definicija racionalnih števil v smislu ekvivalenčnih relacij. Elemente v $\mathbb{Q}$ si lahko predstavljamo kot urejene pare v $\mathbb{Z} \times \mathbb{Z}$. Vsak ulomek p/q lahko zapišemo kot urejeni par (p,q), kjer je $q \neq 0$. Pri tem smatramo urejena para (a,b) in (c,d), kjer je $b \neq 0, d \neq 0$, za ekvivalentna, če je $ad = bc$. Preko te konstrukcije (ki jo bomo v nadaljevanju bolj natančno predstavili za poljuben cel kolobar D) dobimo polje racionalnih števil $\mathbb{Q}$, ki vsebuje (cel) kolobar celih števil. Pravzaprav je mogoče pokazati, da je $\mathbb{Q}$ najmanjše polje, ki vsebuje cela števila: vsako polje, ki vsebuje celi števili m in n (kjer je $n \neq 0$), vsebuje tudi inverz $1/n$ ter produkt $m \cdot (1/n) = m/n$. Torej vsako polje, ki vsebuje kolobar celih števil, vsebuje tudi polje racionalnih števil. Posledično je polje racionalnih števil najmanjše polje, ki vsebuje kolobar celih števil.

Naj bo sedaj D cel kolobar. Glavna naloga tega poglavje je odgovoriti na naslednje vprašanje: kako zgraditi najmanjše polje F, ki vsebuje podkolobar D', ki je izomorfen kolobarju D? Pri tem si bomo izrazito pomagali z zgoraj opisano konstrukcijo racionalnih števil.

Naj bo D poljuben cel kolobar in naj bo

$$S = \{(a,b) : a,b \in D, b \neq 0\} \subseteq D \times D.$$

Na množici S definirajmo relacijo $\sim$ z naslednjim predpisom:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Pokažimo najprej, da je relacija $\sim$ ekvivalenčna relacija.

Lema 1.1

Relacija $\sim$, definirana na množici S, je ekvivalenčna relacija.

Dokaz: Spomnimo se, da je D cel kolobar, kar med drugim pomeni, da je

množenje v kolobarju D komutativno. Za poljubna elementa $a,b \in D$, $b \neq 0$, zato velja $ab = ba$, kar pa po definiciji relacije $\sim$ pomeni, da je $(a,b) \sim (a,b)$. Torej je relacija$\sim$ refleksivna na množici S. Predpostavimo sedaj, da je za urejena para $(a,b),(c,d) \in S$ velja $(a,b) \sim (c,d)$. To pomeni, da je $ad = bc$. Zaradi komutativnosti seveda velja tudi $cb = da$. Po definiciji relacije $\sim$ torej dobimo $(c,d) \sim (a,b)$, kar pa pomeni, da je relacija $\sim$ simetrična. Pokažimo še, da je relacija $\sim$ tranzitivna. Naj za $(a,b),(c,d),(e,f) \in S$ velja, da je $(a,b) \sim (c,d)$ in $(c,d) \sim (e,f)$. Torej je $ad = bc$ in $cf = de$. Če pomnožimo obe strani enakosti $ad = bc$ z f ter obe strani enakosti $cf = de$ z b (spomnimo se, da je $b \neq 0$ in $f \neq 0$) dobimo

$$afd = adf = bcf = bde = bed.$$

Ker je D cel kolobar, veljata zakona krajšanja, in zato velja, da je $af = be$ oz. $(a,b) \sim (e,f)$. Torej je relacija $\sim$ tudi tranzitivna na S.

♠

Ker je ralacija $\sim$ ekvivalenčna relacija na množici S, nam na množici S porodi tako-imenovane ekvivalenčne razrede. Naj bo $(a,b) \in S$. Ekvivalenčni razred $[(a,b)]$ elementa (a,b) (glede na relacijo $\sim$) je množica

$$[(a,b)] = \{(c,d) \in S \colon (a,b) \sim (c,d)\}.$$

Spomnimo se, da imamo naslednjo lepo zvezo med presekoma dveh ekvivalenčnih razredov: za $(a,b),(c,d) \in S$ velja:

$$[(a,b)] = [(c,d)] \Leftrightarrow (a,b) \sim (c,d)$$

$$[(a,b)] \cap [(c,d)] = \emptyset \Leftrightarrow (a,b) \not\sim (c,d)$$

Množico vseh ekvivalenčnih razredov na S bomo označili z F_D:

$$F_D = \{[(a,b)] \colon (a,b) \in S\}.$$

Naša naslednja naloga je definirati seštevanje in množenje na množici F_D. Za poljubna ekvivalenčna razreda $[(a,b)],[(c,d)] \in F_D$ definirajmo operaciji seštevanja in množenja takole

$$[(a,b)] + [(c,d)] = [(ad+bc,bd)] \text{ and } [(a,b)] \cdot [(c,d)] = [(ac,bd)]. \tag{1.4.1}$$

Pri tem so produkti ad, bc, bd, ac in vsota $ad + bc$ seveda izračunani v kolobarju D.

Naslednja lema nam pove, da sta ti dve operaciji neodvisni od izbire predstavni-

kov iz vsakega ekvivalenčnega razreda (oziroma z drugimi besedami, da sta ti dve operaciji dobro definirani).

Lema 1.2

Zgoraj definirani operaciji seštevanja in množenja na F_D sta dobro definirani: če so $[(a_1,b_1)],[(a_2,b_2)],[(c_1,d_1)],[(c_2,d_2)] \in F_D$ za katere velja $[(a_1,b_1)] = [(a_2,b_2)]$, $[(c_1,d_1)] = [(c_2,d_2)]$, potem je tudi

$$[(a_1,b_1)] + [(c_1,d_1)] = [(a_2,b_2)] + [(c_2,d_2)]$$

in

$$[(a_1,b_1)][(c_1,d_1)] = [(a_2,b_2)][(c_2,d_2)].$$

Dokaz: Dokazali bomo, da je operacija seštevanja dobro definirana. Dokaz, da je tudi množenje dobro definirano, ostane kot vaja. Ker je po definiciji $[(a_1,b_1)] + [(c_1,d_1)] = [(a_1d_1 + b_1c_1, b_1d_1)]$ in $[(a_2,b_2)] + [(c_2,d_2)] = [(a_2d_2 + b_2c_2, b_2d_2)]$, moramo pokazati, da velja

$$[(a_1d_1 + b_1c_1, b_1d_1)] = [(a_2d_2 + b_2c_2, b_2d_2)],$$

oziroma ekvivalentno, da je

$$(a_1d_1 + b_1c_1)(b_2d_2) = (b_1d_1)(a_2d_2 + b_2c_2).$$

Ker je $[(a_1,b_1)] = [(a_2,b_2)]$ in $[(c_1,d_1)] = [(c_2,d_2)]$, sledi, da je $a_1b_2 = b_1a_2$ in $c_1d_2 = d_1c_2$. Torej,

$$\begin{aligned}(a_1d_1 + b_1c_1)(b_2d_2) &= a_1d_1b_2d_2 + b_1c_1b_2d_2 \\ &= a_1b_2d_1d_2 + b_1b_2c_1d_2 \\ &= b_1a_2d_1d_2 + b_1b_2d_1c_2 \\ &= (b_1d_1)(a_2d_2 + b_2c_2).\end{aligned}$$

S tem je dokaz zaključen.

♠

Lema 1.3

Množica F_D vseh ekvivalenčnih razredov množice S glede na ekvivalenčno relacijo $\sim$ je za operaciji seštevanja in množenja, ki sta definirani v (1.4.1), polje.

Dokaz:

1. $(F_D, +)$ je komutativna grupa.

   - asociativnost. Drži zaradi asociativnosti operacije $+$ v D. Podrobnosti preverite sami za domačo nalogo.
   - aditivni nevtralni element (ničla). Ničla v F_D je element $[(0,1)]$, ker za vsak $[(a,b)] \in F_D$ velja

   $$[(0,1)] + [(a,b)] = [(0 \cdot b + 1 \cdot a, 1 \cdot b)] = [(a,b)]$$
   $$[(a,b)] + [(0,1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)]$$

   - aditivni inverz. Za vsak element $[(a,b)] \in F_D$ obstaja enolično določen element $[(-a,b)] \in F_D$, za katerega velja

   $$[(a,b)] + [(-a,b)] = [(a \cdot b + b \cdot (-a), b \cdot b)] = [(0, b^2)]$$
   $$[(-a,b)] + [(a,b)] = [(-a \cdot b + b \cdot a, b \cdot b)] = [(0, b^2)]$$

     Hitro lahko opazimo, da sveda velja $(0, b^2) \sim (0,1)$. Torej je $[(0,b^2)] = [(0,1)]$, in je zato element $[(-a,b)] \in F_D$ aditivni inverz elementa $[(a,b)]$.
   - komutativnost. Za poljubna $[(a,b)], [(c,d)] \in F_D$ velja, da je

   $$[(a,b)] + [(c,d)] = [(ad + bc, bd)] = [(cb + da, db)] = [(c,d)] + [(a,b)],$$

     pri čemer smo zopet izkoristili dejstvo, da je D komutativen.

   Torej je $(F_D, +)$ res komutativna grupa.

2. asociativnost množenja. Velja zaradi asociativnosti množenja v D. Podrobnosti preverite za domačo nalogo.

3. identiteta v F_D (nevtralni element za množenje). Element $[(1,1)] \in F_D$ je nevtralni element za množenje, saj za vsak $[(a,b)] \in F_D$ velja

   $$[(a,b)] \cdot [(1,1)] = [(1,1)] \cdot [(a,b)] = [(a,b)].$$

4. enote (multiplikativni inverzi). Vzemimo poljuben $[(a,b)] \in F_D \setminus \{[(0,1)]\}$. Hitro se lahko prepričamo, da je zaradi $[(a,b)] \neq [(0,1)]$ element a neničelen. Torej je tudi $[(b,a)]$ element množice F_D. Seveda velja

   $$[(a,b)] \cdot [(b,a)] = [(b,a)] \cdot [(a,b)] = [(ab, ab)].$$

Ker kolobar D nima deliteljev niča, velja $ab \neq 0$, in zato je $[(ab,ab)] \in F_D$. Ugotovimo še, da je $[(1,1)] = \{(c,c) : c \in D, c \neq 0\}$, in zato $[(ab,ab)] = [(1,1)]$. Torej je element $[(b,a)]$ res multiplikativni inverz elementa $[(a,b)]$.

5. komutativnost množenja. Drži zaradi komutativnosti množenja v D. Podrobnosti preverite sami za domačo nalogo.

6. distributivnostna zakona.. Naj bodo $[(a,b)],[(c,d)],[(e,f)] \in F_D$ poljubni.

$$\begin{aligned}
[(a,b)] \cdot ([(c,d)] + [(e,f)]) &= [(a,b)] \cdot [(cf+de,df)] = [(a(cf+de),bdf)] \\
[(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)] &= [(ac,bd)] + [(ae,bf)] \\
&= [(acbf+bdae,bdbf)] \\
&= [(ba(cf+de),b(bdf))]
\end{aligned}$$

Ker očitno velja, da je $a(cf+de)b(bdf) = bdfba(cf+de)$, velja tudi $[(ba(cf+de),b(bdf)] = [(a(cf+de),bdf)]$. Torej,

$$[(a,b)] \cdot ([(c,d)] + [(e,f)]) = [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)].$$

Ker smo že pokazali, da je množenje v F_D komutativno, nam drugega distributivnostnega zakona ni potrebno posebej dokazovati.

To pomeni, da je $(F_D,+,\cdot)$ polje.

♠

Definicija 1.7

Polje F_D se imenuje ***polje ulomkov*** celega kolobarja D.

Sedaj pa bomo dokazali, da polje F_D res vsebuje podkolobar D', ki je izomorfen kolobarju D. Začnimo z naslednjo lemo.

Lema 1.4

Množica

$$D' = \{[(a,1)] : a \in D\}$$

je komuativen podkolobar polja F_D, ki vsebuje nevtralni element za množenje polja F_D.

Dokaz: Hitro lahko opazimo, da množica D' vsebuje tako aditivni kot tudi multiplikativni nevtralni element: $[(0,1)],[(1,1)] \in D'$. Ker asociativnost seštevanja, komutativnost seštevanja, asociativnost množenja, komutativnost množenja ter distributivnost

veljajo za vse elemente polja F_D, veljajo seveda tudi za elemente množice D'. Ker za poljubna elementa $[(a,1)],[(b,1)] \in D'$ velja

$$[(a,1)]+[(b,1)] = [(a1+1b,1\cdot 1)] = [(a+b,1)] \in D',$$

$$[(a,1)][(b,1)] = [(ab,1\cdot 1)] = [(ab,1)] \in D',$$

je množica D' zaprta za operaciji seštevanja in množenja elementov iz polja F_D. Ker končno za vsak element $[(a,b)] \in D'$ velja tudi, da je $[(-a,1)] \in D'$, množica D' z vsakim svojim elementom vsebuje tudi njegov aditivni inverz. Torej je D' res komuativen podkolobar polja F_D, ki vsebuje nevtralni element za množenje polja F_D.

♠

Sedaj pa pokažimo, da sta kolobarja D in D' izomorfna.

Lema 1.5

Funkcija $i : D \to D'$ definirana z $i(a) = [(a,1)]$, predstavlja izomorfizem med kolobarjema D in D'.

Dokaz: Za poljubna $a,b \in D$ velja

$$i(a+b) = [(a+b,1)]$$

ter

$$i(a)+i(b) = [(a,1)]+[(b,1)] = [(a1+1b,1)] = [(a+b,1)].$$

Torej je $i(a)+i(b) = i(a+b)$. Podobno:

$$i(ab) = [(ab,1)]$$

ter

$$i(a)i(b) = [(a,1)][(b,1)] = [(ab,1\cdot 1)] = [(ab,1)].$$

Torej velja tudi $i(ab) = i(a)i(b)$, kar pomeni, da je i homomorfizem kolobarjev D in D'.

Preslikava i je očitno surjektivna, saj za poljuben element $[(a,1)] \in D'$ velja $a \in D$ in $i(a) = [(a,1)]$. Preverimo še, da je preslikava i injektivna. Če za elementa $a,b \in D$ velja, da je $i(a) = i(b)$, potem je

$$[(a,1)] = [(b,1)] \Rightarrow (a,1) \sim (b,1) \Rightarrow a1 = 1b \Rightarrow a = b.$$

Torej je i izomorfizem med kolobarjem D in kolobarjem D'.

♠

Opomba. Strogo formalno kolobar D NI VSEBOVAN v polju F_D. Namreč, elementi polja F_D so ekvivalenčni razredi množice S glede na relacijo $\sim$, in zato množic D in F_D ne moremo med seboj primerjati glede na inkluzijo. Bomo pa v smislu zgornje leme kolobar D identificirali s kolobarjem D', ter posledično rekli, da je D vsebovan v F_D.

Za poljuben element $[(a,b)]$ polja F_D očitno velja naslednja enakost:

$$([a,b)] = [(a,1)][(1,b)] = [(a,1)] \cdot [(b,1)]^{-1} = i(a) \cdot i(b)^{-1} = i(a)/i(b).$$

S tem smo pravzaprav dokazali naslednji izrek.

Izrek 1.15

Vsak cel kolobar D je mogoče razširiti do polja F_D tako, da lahko vsak element polja F_D izrazimo kot količnik dveh elementov iz D.

Polje F_D je tudi minimalno polje, ki vsebuje cel kolobar D. V naslednjem izreku to lastnost bolj natančno opišemo.

Izrek 1.16

Naj bo D cel kolobar in naj bo F_D njegovo polje ulomkov. Dalje, naj bo L katerokoli polje, ki vsebuje D. Potem obstaja podpolje L' polja L in izomorfizem $\psi : F_D \to L'$, za katerega velja, da je $\psi(a) = a$ za vsak $a \in D$.

Dokaz: Ker polje L vsebuje kolobar D, lahko poljubnima dvema elementoma $a,b \in D$, $b \neq 0$, priredimo element $ab^{-1} \in L$. Ta element bomo označevali tudi kot $a/_L b$. Definiramo podmnožico $L' \subseteq L$ na naslednji način:

$$L' = \{ab^{-1} = a/_L b \colon a,b \in D, b \neq 0\}.$$

Definirajmo sedaj preslikavo $\psi : F_D \to L'$ takole:

$$\Psi([(a,b)]) = a/_L b.$$

Pokažimo najprej, da je preslikava ψ dobro definirana. Izberimo si $[(a,b)], [(a_1,b_1)] \in F_D$, za katera velja $[(a,b)] = [(a_1,b_1)]$. Torej je $(a,b) \sim (a_1,b_1)$, oziroma $ab_1 = ba_1$. Če to enakost pomnožimo z b^{-1} in z b_1^{-1}, dobimo

$$\psi([(a,b)]) = a/_L b = ab^{-1} = a_1 b_1^{-1} = a_1/_L b_1 = \psi([(a_1,b_1)]).$$

Preslikava ψ je torej res dobro definirana.

Pokažimo sedaj, da je ψ homomorfizem. Izberimo si poljubna $[(a,b)],[(c,d)] \in F_D$. Potem je

$$\psi([(a,b)]+[(c,d)]) = \psi([(ad+bc,bd)]) = (ad+bc)/_L(bd) = (ad+bc)(bd)^{-1} =$$

$$(ad+bc)(b^{-1}d^{-1}) = ab^{-1}+cd^{-1} = a/_Lb+c/_Ld = \psi([(a,b)])+\psi([(c,d)]).$$

Podobno dobimo

$$\psi([(a,b)][(c,d)]) = \psi([(ac,bd)]) = (ac)/_L(bd) = (ac)(bd)^{-1} =$$

$$(ac)(b^{-1}d^{-1}) = ab^{-1}cd^{-1} = a/_Lb\ c/_Ld = \psi([(a,b)])\psi([(c,d)]).$$

Preslikava ψ je torej res homomorfizem.

Preslikava ψ je tudi očitno surjektivna: poljuben element $x \in L'$ je oblike $x = a/_Lb$ za neka $a,b \in D$, $b \neq 0$, in zato velja $\psi([(a,b)]) = a/_Lb = x$. Pokažimo, da je ψ tudi injektivna. Naj za $[(a,b)],[(c,d)] \in F_D$ velja, da je $\psi([(a,b)]) = \psi([(c,d)])$. Torej velja $a/_Lb = c/_Ld$, in zato $ab^{-1} = cd^{-1}$. Če pomnožimo to enakost z b in z d, dobimo, da velja $ad = bc$, oziroma $(a,b) \sim (c,d)$. To pa pomeni, da je $[(a,b)] = [(c,d)]$. Torej je preslikava ψ res injektivna. Sledi, da je ψ izomorfizem (in je tudi zato L' res podpolje v L).

Ostane nam še za dokazati, da je $\psi(a) = a$ za vsak $a \in D$. Tu se bomo najprej spomnili, da smo element $a \in D$ identificirali z elementom $[(a,1)] \in F_D$. Z upoštevanjem te identifikacije torej dobimo:

$$\psi(a) = \psi([(a,1)]) = a/_L1 = a1^{-1} = a1 = a.$$

S tem je dokaz zaključen.

♠

Končajmo poglavje z nekaj posledicami, katerih dokazi so vam prepuščeni za domačo nalogo.

Posledica 1.5

Katerikoli dve polji ulomkov celega kolobarja D sta izomorfni.

Posledica 1.6

Naj bo F polje karakteristike nič. Potem F vsebuje podpolje, ki je izomorfno $\mathbb{Q}$.

Posledica 1.7

Naj bo F polje karakteristike p. Potem F vsebuje podpolje, ki je izomorfno $\mathbb{Z}_p$.

1.5. Kolobar polinomov

Ali sta polinoma $f(x) = 0$ in $g(x) = x^2 - x$ enaka? Če ju obravnavamo kot "abstraktna zapisa", karkoli že to pomeni, nista enaka. Če pa ju obravnavamo na primer kot preslikavi $f, g : \mathbb{Z}_2 \to \mathbb{Z}_2$, velja $f(\overline{0}) = \overline{0} = g(\overline{0})$ in $f(\overline{1}) = \overline{0} = g(\overline{1})$, torej sta f in g enaki preslikavi. Priznajmo torej, da ne vemo, kaj so polinomi, ali bolje: polinome moramo natančno definirati, če jih želimo primerjati in sploh početi kaj z njimi.

Naj bo K kolobar. Vsakemu zaporedju $f : \mathbb{N}_0 \to K$, za katerega obstaja tak $n \in \mathbb{N}_0$, da je $f_k = 0$ za vse $k \geq n$, rečemo **polinom** (**ene spremenljivke**) **nad** K. Polinom f lahko predstavimo tudi kot

$$f = (f_0, f_1, \ldots, f_n, f_{n+1}, \ldots) = (f_0, f_1, \ldots, f_n, 0, 0, \ldots).$$

Elementom $f_i \in K$ rečemo **koeficienti** polinoma f nad K. Iz definicije polinoma je razvidno, da sta polinoma f, g nad K enaka, $f = g$, natanko tedaj, ko je $f_i = g_i$ za vse $i \in \mathbb{N}_0$. Množico polinomov ene spremenljivke nad K označujemo s $\mathrm{Pol}(K)$. Če je f_n zadnji koeficient, ki je različen od nič, torej $f_n \neq 0$ in $f_k = 0$ za $k > n$, je polinom f stopnje n. **Stopnjo** polinoma f bomo označevali z ∂f ali $\deg(f)$. Za polinom, v katerem so vsi koeficienti enaki nič, stopnja ni določena.

Definirajmo seštevanje in množenje polinomov.

1. Vsota zaporedij

   $$f = (f_0, f_1, f_2, \ldots) \text{ in } g = (g_0, g_1, \ldots)$$

   je zaporedje vsot istoležnih članov zaporedij f in g, torej je

   $$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots).$$

   Zaporedje $f + g$ ima očitno skoraj vse člene enake nič natanko tedaj, ko velja isto za zaporedji f in g. Torej je vsota polinomov polinom. Množica polinomov $\mathrm{Pol}(K)$ je Abelova grupa pod operacijo seštevanja. Zakona komutativnosti in asiciativnosti veljata, saj veljata za seštevanje elementov kolobarja K. Polinom nič je zaporedje, v katerem so vsi členi enaki nič. Razliko dveh polinomov pa definiramo kot

   $$f - g = (f_0 - g_0, f_1 - g_1, \ldots).$$

2. Produkt polinomov f in g je polinom

$$fg = (c_0, c_1, \ldots)$$

s koeficienti c_k, ki jih izračunamo po formuli

$$c_k = \sum_{i=0}^{k} f_i g_{k-i},\ k = 0, 1, \ldots$$

Veljata tudi zakona asociativnosti in distributivnosti. Dokaz zahteva le nekaj preprostega računanja, ki je prepuščeno bralcu.

Z upoštevanjem zgoraj naštetih lastnosti ugtovimo, da je množica $\mathrm{Pol}(K)$ kolobar. Množenje polinomov je očitno komutativno, če in samo če je K komutativen. Polinom $(a, 0, 0, \ldots)$, $a \in K$, je stopnje nič. Vsota in produkt polinomov stopnje nič sta polinoma stopnje nič

$$(a, 0, \ldots) + (b, 0, \ldots) = (a + b, 0, \ldots), \qquad (a, 0, \ldots) \cdot (b, 0, \ldots) = (ab, 0, \ldots).$$

Od tod sledi, da polinomi stopnje nič sestavljajo kolobar. Upodobitev, po kateri pripada elementu $a \in K$ polinom $(a, 0, \ldots)$, je izomorfizem kolobarja K na kolobar polinomov stopnje nič. Zaradi tega izomorfizma označimo polinom $(a, 0, \ldots)$ kar z a. Torej je identiteta 1 kolobarja K (če obstaja) tudi identiteta v kolobarju polinomov. Polinom f pomnožimo z elementom $a \in K$ tako, da pomnožimo vse njegove koeficiente z a.

Označimo z x polinom, pri katerem je $a_1 = 1$ in $a_k = 0$ za $k \neq 1$:

$$x = (0, 1, 0, \ldots).$$

Njegove zaporedne potence so

$$x^2 = (0, 0, 1, 0, \ldots), \qquad x^3 = (0, 0, 0, 1, 0, \ldots), \text{ itd.}$$

Polinom $f = (f_0, f_1, \ldots, f_n, 0, 0, \ldots)$ stopnje n razstavimo na vsoto

$$f = (f_0, 0, \ldots) + (0, 0, f_1, 0, \ldots) + \cdots + (0, 0, \ldots, 0, f_n, 0, \ldots).$$

Ker je

$$(0, f_1, 0, \ldots) = f_1 x,\ \ (0, 0, f_2, \ldots) = f_2 x^2,\ \ \ldots\ \ (0, \ldots, 0, f_n, 0, \ldots) = f_n x^n$$

lahko vsak polinom f zapišemo v naslednji obliki

$$f = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n.$$

Zato pravimo, da je f polinom spremenljivke x. Če želimo spremenjivko eksplicitno navesti, zapišemo polinom kot $f(x)$. Pri množenju in seštevanju polinomov zapisanih v tej obliki spremenjivko x upoštevamo kot element osnovnega kolobarja K. Če smo spremenljivko, torej polinom $(0,1,0,\ldots)$, označili z x, označimo kolobar polinomov s $K[x]$.

Pri izražanju polinomov v obliki $f(x)$ smo predpostavili, da je v kolobarju K element 1. Ker se da vsak kolobar vložiti v kolobar z identiteto, lahko pišemo polinome v obliki $f(x)$ tudi v primeru, ko v prvotnem kolobarju K ni elementa 1.

Če je K kolobar in sta x in y dve spremenljivki, potem lahko konstruiramo kolobar $(K[x])[y] := K[x,y]$. Elementi tega kolobarja so polinomi spremnljivke y, koeficienti pa so polinomi spremnljivke x. Torej

$$f(x,y) = f_0(x) + f_1(x)y + \ldots + f_n(x)y^n.$$

Če je $f_k(x) = a_{0k} + a_{1k}x + \ldots + a_{mk}x^m$, lahko zapišemo $f(x,y)$ v naslednji obliki

$$f(x,y) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{ij}x^i y^j,$$

pri čemer so koeficienti a_{ij} iz osnovnega kolobarja K. Vrstni red spremnljivk x in y lahko zamenjamo. Če uvedemo najprej y in nato x, dobimo kolobar $K[y,x]$. Njegovi elementi so polinomi spremnljivke x, katerih koeficienti so polinomi spremenljivke y. To implicira obstoj naravnega izomorfizma med $K[x,y]$ in $K[y,x]$. Podobno lahko definiramo kolobar več spremenljivk oz. **kolobar polinomov n spremenljivk** $K[x_1,x_2,\ldots,x_n]$.

Komentar 1.3

Če je D cel kolobar, potem je tudi $D[x]$ cel kolobar. Velja tudi, če je F polje, potem je $F[x]$ polje. Opazimo lahko, da $F[x]$ ni polje, ker x ni enota. To pomeni, da ne obstaja takšen polinom $f \in F[x]$, da je $xf(x) = 1$. Ker je $F[x]$ cel kolobar, lahko konstruiramo polje ulomkov $F(x)$. Velja namreč, da lahko vsak element v $F(x)$ predstravimo kot kvocient $f(x)/g(x)$ dveh polinomov v $F[x]$ z $g(x) \neq 0$. Podobno lahko definiramo polje ulomkov $F(x_1,\ldots,x_n)$ od $F[x_1,\ldots,x_n]$ in ga imenujemo ***polje racionalnih funkcij n spremenljivk nad*** F.

Sedaj lahko nadaljujemo in pokažemo, kako lahko homomorfizme uporabimo za "reševanje polinomskih enačb". Naj bosta E in F takšni polji, da je $F \leq E$. Naslednji

izrek potrjuje obstoj zelo pomembnega homomorfizma $F[x] \to E$.

Izrek 1.17: Evaluacijski homomorfizem za teorijo polj

Naj bo F podpolje polja E in naj bo $\alpha \in E$ poljuben ter x spremenljivka. Funkcija $\phi_\alpha : F[x] \to E$ definirana z

$$\phi_\alpha(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

za $a_0 + a_1x + \ldots + a_nx^n \in F[x]$ je homomorfizem med $F[x]$ in E. Poleg tega je $\phi_\alpha(x) = \alpha$ in $\phi_\alpha(a) = a$ za vse $a \in F$. Homomorfizem ϕ_α predstavlja ***evaluacijo*** v α.

Dokaz: Funkcija ψ_α je dobro definirana, to pomeni, da je neodvisna od reprezentacije polinoma $f(x) \in F[x]$ kot končne vsote $a_0 + a_1x + \ldots + a_nx^n$, saj lahko takšno končno zamenimo z dodajanjem in brisanjem členov oblike $0x^i$, kar ne vpliva na vrednost $\phi_\alpha(f(x))$. Če so $f(x) = \sum_{i=0}^{n} a_ix^i$, $g(x) = \sum_{i=0}^{m} b_ix^m$ in $h(x) = f(x) + g(x) = \sum_{i=0}^{r} c_ix^i$, je

$$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(h(x)) = \sum_{i=0}^{r} c_i\alpha^i.$$

Z druge strani dobimo

$$\phi_\alpha(f(x)) + \phi_\alpha(g(x)) = \sum_{i=0}^{n} a_i\alpha^i + \sum_{i=0}^{m} b_i\alpha^i.$$

Po definiciji seštevanja polinomov velja $c_i = a_i + b_i$ in posledično je

$$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x)).$$

Ker je

$$f(x)g(x) = d_0 + d_1x + \ldots + d_sx^s$$

dobmo

$$\phi_\alpha(f(x)g(x)) = d_0 + d_1\alpha + \ldots + d_s\alpha^s.$$

Z druge strani

$$\phi_\alpha(f(x))\phi_\alpha(g(x)) = (a_0 + a_1\alpha + \ldots + a_n\alpha^n)(b_0 + b_1\alpha + \ldots + b_m\alpha^m).$$

Po definiciji množenja polinomov velja $d_j = \sum_{i=0}^{j} a_ib_{j-i}$ in posledično je

$$\phi_\alpha(f(x)g(x)) = \phi_\alpha(f(x))\phi_\alpha(g(x)).$$

Po definiciji, ϕ_α slika konstantni polinom $a \in F[x]$, kjer je $a \in F$, v a. To pomeni, da ϕ_α slika F izomorfno z identično preslikavo. Ponovno, po definiciji ϕ_α sledi $\phi_\alpha(x) = \phi_\alpha(1x) = 1a = a$.

♠

Naj še enkrat izpostvimo, da ta izrek velja (z uporabo enakega dokaza), tudi v primeru, ko sta F in E zgolj komutativna kolobarja z identiteto in ne polji. Vendar bo za nas izrek pomemben predvsem v primeru, ko sta F in E polji.

Težko je preveč poudariti pomen tega preprostega izreka za nas, saj predstavlja temelj našega nadaljnega dela v teoriji polj. Ker je tako preprost, ga lahko upravičeno imenujemo kar opazka in ne izrek. Morda je bil njegov dokaz, zaradi zapisa polnomov, nekoliko težek, vendar naj poudarimo, da ni.

Zgled 1.5.1. Naj bosta $F = \mathbb{Q}$ in $E = \mathbb{R}$. Poglejmo si evaluacijski izomorfizem $\phi_2 : \mathbb{Q}[x] \to \mathbb{R}$. Velja

$$\phi_2(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_12 + \ldots + a_n2^n.$$

Opazimo, da je

$$\phi_2(x^2 + x - 6) = 2^2 + 2 - 6 = 0.$$

Torej, $x^2 + x - 6 \in \ker(\phi_2)$. Poleg tega vemo, da je $x^2 + x - 6 = (x-2)(x+3)$ ker je $\phi_2(x-2) = 2 - 2 = 0$.

Zgled 1.5.2. Naj bosta $F = \mathbb{Q}$ in $E = \mathbb{C}$. Poglejmo si evaluacijski homomorfizem $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$. Opazimo, da je

$$\phi_i(x^2 + 1) = i^2 + 1 = 0$$

in posledično $x^2 + 1 \in \ker(\phi_i)$.

Zgled 1.5.3. Naj bosta $F = \mathbb{Q}$ in $E = \mathbb{R}$. Polgejmo si evaluacijski homomorfizem $\phi_\pi : \mathbb{Q}[x] \to \mathbb{R}$. Ni težko pokazati, da je $a_0 + a_1\pi + \ldots + a_n\pi^n = 0$ natanko tedaj, ko je $a_i = 0$ za vsak $i = 0, \ldots, n$. Torej $\ker(\phi_\pi) = \{0\}$ in posledično je ϕ_π monomorfizem. To pomeni, da vsi formalni polinomi v π z racionalnimi koeficienti tvorijo kolobar, ki je izomorfen $\mathbb{Q}[x]$ z zapisom $\phi_\pi(x) = \pi$.

Sedaj zaključujemo s povezavo med našimi novimi idejami in klasičnim konceptom reševanja polinomskih enačb. Ko bomo želili rešiti polinomsko enačbo, bomo rekli kar, da želimo poiskati ničle polinoma.

Definicija 1.8

Naj bo F podpolje polja E in naj bo $\alpha \in E$. Z $f(x) = a_0 + a_1x + \ldots + a_nx^n$ označimo polinom v $F[x]$ in naj bo $\phi_\alpha : F[x] \to E$ evaluacijski homomorfizem. Če je $f(\alpha) := \phi_\alpha(f(x)) = 0$, potem α imenujemo ***ničla polinoma*** f.

Z uporabo zgornje definicije lahko klasični problem iskanja vseh realnih števil r za katere je $r^2 + r - 6 = 0$ zapišemo kot iskanje takšnih elementov $\alpha \in \mathbb{R}$, da velja

$$\phi_\alpha(x^2 + x - 6) = 0,$$

pri čemer je $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{R}$ evaluacijski homomorfizem. Očitno je

$$\{\alpha \in \mathbb{R} : \phi_\alpha(x^2 + x - 6) = 0\} = \{r \in \mathbb{R} : r^2 + r - 6 = 0\} = \{2, -3\}.$$

Naloge

1. Izračunaj produkt polinomov $f(x) = 2x^2 + 3x + 4$ in $g(x) = 3x^2 + 2x + 3$ v $\mathbb{Z}_6[x]$.
2. Koliko polinomov stopnje m premore $\mathbb{Z}_n[x]$?
3. Če je $F = E = \mathbb{Z}_7$, izračunaj vrednost evaluacijskih homomorfizmov:
   (a) $\phi_3((x^4 + 2x)(x^3 - 3x^2 + 3))$,
   (b) $\phi_4(3x^{106} + 5x^{99} + 2x^{53})$.
4. S pomočjo malega Fermatovega izreka, poišči vse ničle polinoma $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$ v $\mathbb{Z}_5$.
5. Poišči šest elementov v jedru evaluacijskega homomorfizma $\phi_5 : \mathbb{Q}[x] \to \mathbb{R}$.
6. Naj bo D cel kolobar. Pokaži, da je tudi $D[x]$ cel kolobar.
7. Naj bosta $f, g \in D[x]$, kjer je D cel kolobar. Pokaži, da je $\deg(fg) = \deg(f) + \deg(g)$. Ali trditev drži, če D premore delitelje niča?
8. Kaj so enote v celemu kolobarju $D[x]$?

Rešitve

1. Skozi celotno nalogo ne pozabite, da seštevamo in množimo po modulu 6. S tem v mislih enostavno izračunamo, da je $f(x) \cdot g(x) = x^3 + 5x$.

2. Naj bo $f(x) = a_0 + a_1x + \ldots + a_{m-1}x^{m-1} + a_mx^m$ poljuben polinom stopnje m v $\mathbb{Z}_n[x]$. Ker je vodilni koeficient a_m neničelen vemo, da je $a_m \in \{1,2,\ldots,n-1\}$ in da lahko za ostale koeficiente a_i izberemo poljuben elemnt v $\mathbb{Z}_n$. Torej imamo $n^m \cdot (n-1)$ polinomov stopnje m v $\mathbb{Z}_n[x]$.

3. (a) Opazimo, da je $f(x) = (x^4+2x)(x^3-3x^2+3) = x^7+4x^6+5x^4+x^3+6x$. Torej,

$$\phi_3(f(x)) = f(3) = 3^7 + 4\cdot 3^6 + 5\cdot 3^4 + 3^3 + 6\cdot 3.$$

S pomočjo malga Fermatovega izreka in njegove posledice sledi, da je $3^7 \mod 7 = 3$ in $3^6 \mod 7 = 1$. Poleg tega ni težko izračunati, da je $3^4 \mod 7 = 4$ in $3^3 \mod 7 = 6$. Torej,

$$\phi_3(f(x)) = 3+4+5\cdot 4+6+4 = 2.$$

(b) Po malem Fermatovem izreku sledi, da je $4^6 \equiv 1 \pmod 7$. Sedaj želimo "razširiti" 4^6 tako, da se čim bolj približimo 4^{106}. V našem primeru, $(4^6)^{17} = 4^{102} \equiv 1 \pmod 7$. Z druge strani, $4^4 \equiv 4 \pmod 7$. Če pomnožimo ti dve kongruenci dobimo, da je $4^{106} \equiv 4 \pmod 7$. Podobno se izračuna, da je $4^{99} \equiv 1 \pmod 7$ in $4^{53} \equiv 2 \pmod 7$. Torej je

$$\phi_4(3x^{106} + 5x^{99} + 2x^{53}) = 3\cdot 4 + 5\cdot 1 + 2\cdot 2 = 0.$$

4. Po malem Fermatovem izreku sldei, da je $a^4 \equiv 1 \pmod 5$ za $a \in \{1,2,3,4\}$. V izrazu $f(x)$, zapišimo eksponente d od x v obliki $d = 4q + l,\ l < d$. Dobimo, da je

$$f(x) = 2\cdot (x^4)^{54}\cdot x^3 + 3\cdot (x^4)^{18}\cdot x^2 + 2\cdot (x^4)^{14}\cdot x + 3\cdot (x^4)^{11}.$$

Sedaj enostavno izračunamo vredonsti $f(x)$ za $x \in \mathbb{Z}_5$.

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 2+3+2+3 = 0 \\ f(2) &= 1+2+4+3 = 0 \\ f(3) &= f(-2) = 4+2+1+3 = 0 \\ f(4) &= f(-1) = 3+3+3+3 = 2 \end{aligned}$$

Torej so ničle $f(x)$ natanko $0,1,2$ in 3.

5. Očitno je $f_1(x) = x-5 \in \ker(\phi_5)$. Vsi večkratniki f_1 so tudi v $\ker(\phi_5)$.

6. Ker je D komutativen kolobar z enoto $1 \neq 0$ vemo, da je $D[x]$ komutativen

kolobar z enoto $1 \neq 0$. Preveriti moramo še, če $D[x]$ premore delitelje niča.

Naj bosta $f, g \in D[x]$ poljubna neničelna polinoma. Brez izgube za splošnost, lahko napišemo

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i,\ a_i, b_j \in D,\ i = \overline{0,n}, j = \overline{0,m}.$$

Ker je D cel kolobar sledi, da je $a_n b_m \neq 0$ in posledično

$$a_n b_m x^{n+m} \neq 0 \Rightarrow f(x)g(x) \neq 0.$$

Z drugimi besedami, $D[x]$ nima deliteljev niča.

7. Naj bosta

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i,\ a_i, b_j \in D,\ i = \overline{0,n}, j = \overline{0,m}$$

poljubna neničelna polinoma v $D[x]$. "Največji" monom, ki se lahko pojavi v $f(x)g(x)$ je x^{n+m} s koeficientom $a_n b_m$. Ker je D cel kolobar vemo, da je $a_n b_m \neq 0$. Torej je

$$\deg(fg) = n + m = \deg(f) + \deg(g).$$

Poglejmo si kolobar $\mathbb{Z}_6[x]$. Če vzamemo $f(x) = 2x^2$ in $g(x) = 3x^3 + 2$, je $f(x)g(x) = 4x^2$. Torej je

$$\deg(fg) = 2 \neq 5 = \deg(f) + \deg(g).$$

8. Predpostavimo, da je $f(x) \in D[x]$ enota. Torej

$$(\exists g(x) \in D[x])\ f(x)g(x) = 1.$$

Od tod sledi, da je $\deg(fg) = \deg(1) = 0$. Brez izgube za splošnost predpostavimo, da je $\deg(f) = n,\ \deg(g) = m,\ n, m \geq 0$. Ker je $D[x]$ cel kolobar je $\deg(fg) = n + m = 0$, kar pomeni, da je $n = m = 0$. Z drugimi besedami, f in g sta konstantna polinoma, tj. enote v $D[x]$ so natanko tisti elementi, ki so enote v D.

Dodatne naloge

1. Poišči enote v $\mathbb{Z}[x]$ in $\mathbb{Z}_4[x]$.

2. Naj bo F polje karakteristike 0 in naj bo $D : F[x] \to F[x]$ polinom definiran z

naslednjim predpisom

$$D\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

(a) Pokaži, da je $D : F[x] \to F[x]$ automorfizem grup $(F[x], +)$. Ali je D homomorfizem kolobarjev?

(b) Poišči $\ker(D)$.

(c) Poišči $\mathrm{im}(D)$.

3. Naj bo F podpolje polja E.

(a) Definiraj evaluacijski homomorfizem $\phi_{\alpha_1,\ldots,\alpha_n} : F[x_1,\ldots,x_n] \to E,\ \alpha_i \in E$, na podoben način, kot smo to storili na vajah s standardnim evaluacijskim homomorfizmom.

(b) Če je $F = E = \mathbb{Q}$, izračunaj $\phi_{-3,2}(x_1^2 x_2^3 + 3x_1^4 x_2)$.

(c) Definiraj koncept ničle polinoma $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ na podoben način kot smo definirali ničlo polinoma $f(x)$.

4. Naj bo F polje in F^F množica vseh funkcij $F \to F$. Za poljubna elementa $\phi, \psi \in F^F$ definiramo seštevanje $\phi + \psi$ z

$$(\phi + \psi)(a) = \phi(a) + \psi(a)$$

in množenje $\phi \cdot \psi$ z

$$(\phi \cdot \psi)(a) = \phi(a) \cdot \psi(a)$$

pri čemer je $a \in F$.

(a) Dokaži, da je $(F^F, +, \cdot)$ kolobar.

Element $\phi \in F^F$ je polinom, če obstaja takšen $f(x) \in F[x]$, da je $\phi(a) = f(a)$ za vse $a \in F$.

(b) Dokaži, da je množica P_F vseh polinomov nad F podkolobar kolobarja F^F.

(c) Dokaži, da P_F ni nujno izomorfen $F[x]$. (Namig: Pokaži, da če je F končen potem $F[x]$ in F^F nista iste velikosti).

(d) Dokaži, da, če je $F = \mathbb{Z}_2^{\mathbb{Z}_2}$ potem je $P_F = F^F$.

5. Naj bodo vsi neničelni koeficienti polinoma $f \in K[x]$ delitelji niča v K. Ali je potem polinom f delitelj niča v $K[x]$?

1.6. Faktorizacija polinomov nad poljem

Spomnimo se, da se ukvarjamo z iskanjem ničel polinomov. Naj bosta E in F takšni polji, da je $F \leq E$. Predpostavimo, da je $f(x) \in F[x]$ razcepen v $F[x]$ tako, da je $f(x) = g(x)h(x)$ za poljubna $g(x), h(x) \in F[x]$ in naj bo $\alpha \in E$. Sedaj za evalvacijski homomorfizem ϕ_α velja, da je

$$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha).$$

Če je torej $\alpha \in E$, potem je $f(\alpha) = 0$ natanko tedaj, ko je bodisi $g(\alpha) = 0$ bodisi $h(\alpha) = 0$. Iskanje ničle za $f(x)$ se reducira na problem iskanja ničle faktorja $f(x)$. To je en izmed razlogov, zakaj je preučevanje faktorizacije polinomov koristno.

Izrek 1.18: Osnovni izrek o deljenju v $F[x]$

Naj bosta $f(x) = \sum_{i=0}^{n} a_i x^i$ in $g(x) = \sum_{i=0}^{m} b_i x^i$ elementa v $F[x]$, pri čemer sta $a_n, b_m \in F$ neničelna in $m > 0$. Potem obstajata takšna enolična polinoma $q(x)$ in $r(x)$ v $F[x]$, da je $f(x) = q(x)g(x) + r(x)$, pri čemer je bodisi $r(x) = 0$ bodisi $\deg(r) < m$.

Dokaz: Poglejmo si množico $S = \{f(x) - g(x)s(x) : s(x) \in F[x]\}$. Če je $0 \in S$, potem obstaja takšen polinom $s(x)$, da velja $f(x) - g(x)s(x) = 0$. Torej, $f(x) = g(x)s(x)$. Trditev očitno velja, če vzamemo, da je $q(x) = g(x)$ in $r(x) = 0$. Naj bo sedaj $r(x)$ element v S z najmanjšo stopnjo. To pomeni, da je

$$f(x) - q(x)g(x) = r(x) \to f(x) = q(x)g(x) + r(x),$$

za nek $q(x) \in F[x]$. Sedaj moramo dokazati, da je $\deg(r) < m$. Predpostavimo, da je

$$r(x) = c_t x^t + x_{t-1}x^{t-1} + \ldots + c_1 x + c_0,\ c_j \in F,\ c_t \neq 0.$$

Če je $t \geq m$, potem je

$$f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x) = r(x) - (c_t x^t + \text{ členi manjše stopnje}),$$

kar je polinom stopnje manjše kot $t = \deg(r)$. Opazimo, da je polinom $f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x) = f(x) - [q(x) - (c_t/b_m)x^{t-m}] \in S$, kar je protislovje s predpostavko, da je $r(x)$ najmanjše stopnje. Torej mora veljati, da je $\deg(r) < m$. Za enoličnost, predpostavimo, da je $f(x) = g(x)q_1(x) + r_1(x)$ in $f(x) = g(x)q_2(x) + r_2(x)$. Ko odštejemo dani enakosti, dobimo:

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Ker je bodisi $r_2(x) - r_1(x) = 0$ bodisi $\deg(r_2 - r_1) < \deg(g)$, je $q_1(x) - q_2(x) = 0$, tj. $q_1(x) = q_2(x)$. To pomeni, da je tudi $r_2(x) - r_1(x) = 0$, tj. $r_1(x) = r_2(x)$.

♠

Posledica 1.8: Faktorski izrek

Element $a \in F$ je ničla polinoma $f(x) \in F[x]$ natanko tedaj, ko je $x - a$ faktor od $f(x)$ v $F[x]$.

Dokaz: ($\Rightarrow$) Predpostavimo, da je $f(a) = 0$, za nek $a \in F$. Po Izreku 1.18 obstajata takšna polinoma $q(x), r(x) \in F[x]$, da je

$$f(x) = (x - a)q(x) + r(x),$$

pri čemer je bodisi $r(x) = 0$ bodisi $\deg(r) < 1$. To pomeni, da je $r(x) = c$ za nek $c \in F$ in posledično

$$f(x) = (x - a)q(x) + c.$$

Z uporabo evaluacijskega homomorfizma dobimo, da je

$$0 = f(a) = 0q(a) + c,$$

kar pomeni, da je $c = 0$. Torej je $f(x) = (x - a)q(x)$. Z drugimi besedami, $x - a$ je faktor od $f(x)$.

($\Leftarrow$) Naj bo $x - a$ faktor od $f(x)$ v $F[x]$, pri čemer je $a \in F$. Če uporabimo evaluacijski homomorfizem ϕ_a na $f(x)$ dobimo, da je $f(a) = 0q(a) = 0$. Torej je a ničla od $f(x)$.

♠

Posledica 1.9: Število ničel polinoma

Neničelni polinom $f(x) \in F[x]$ stopnje n premore največ n ničel v polju F.

Dokaz: Iz Posledice 1.8 sledi naslednje; če je $a_1 \in F$ ničla polinoma $f(x)$ potem je

$$f(x) = (x - a)q_1(x),$$

pri čemer je $\deg(q_1) = n - 1$. Če je $a_2 \in F$ ničla polinoma $q_1(x)$, je

$$f(x) = (x - a_1)(x - a_2)q_2(x).$$

Če ta postopek nadaljujemo dobimo, da je

$$f(x) = (x-a_1)\cdots(x-a_r)q_r(x),$$

pri čemer q_r nima ničel v F. Ker je stopnja $f(x)$ največ n, se lahko največ n faktorjev $(x-a_i)$ pojavi na desni strani zgornje enačbe. To pomeni, da je $r \leq n$. Naj bo $b \in F$ poljuben element, različen od a_i za $i = 1,\ldots,r$. Potem je $f(b) = (b-a_1)\cdots(b-a_r)q_r(b) \neq 0$, saj F nima deliteljev niča in noben izmed faktorjev $b-a_i$ in $q_r(b)$ ni enak 0 (po konstrukciji). To pomeni, da so edine možne ničle $f(x)$ v F elementi $a_1,\ldots,a_4$ ($r \leq n$).

♠

Končna posledica Izreka 1.18 se nanaša na strukturo multiplikativne grupe F^* neničelnih elementov polja F.

Posledica 1.10

Če je G končna podgrupa multiplikativne grupe $(F^*,\cdots)$ polja F, potem je G ciklična. Še več, multiplikativna grupa vseh neničelnih elementov končnega polja je ciklična.

Dokaz: Iz teorije grup vemo, da je vsaka končna komutativna grupa G izomorfna direktnemu produktu $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$, pri čemer so d_i potence praštevil. Predstavljamo si lahko, da je vsak $\mathbb{Z}_{d_i}$ ciklična grupa reda d_i v multiplikativni notaciji. Naj bo m najmanjši skupni večkratnik števil $d_1,\ldots,d_r$. Opazimo, da je $m \leq d_1 d_2 \ldots d_r$. Če je $a_i \in \mathbb{Z}_{d_i}$, potem je $a_i^{d_i} = 1$ in posledično je $a_i^m = 1$, saj $d_i | m$. Torej za vsak $\alpha \in G$ velja, da je $\alpha^m = 1$. To pomeni, da je vsak element v G ničla polinoma $x^m - 1$. G ima $d_1 \ldots d_r$ elementov. Z druge strani, po Posledici 1.9 sledi, da ima $x^m - 1$ največ m ničel v F. To pomeni, da je $m \geq d_1 \ldots d_r$ in posledično mora veljati, da je $m = d_1 \ldots d_r$. Torej so praštevila, ki se pojavijo v $d_1, d_2, \ldots, d_r$ paroma različna, grupa G pa je izomorfna ciklični grupi $\mathbb{Z}_m$.

♠

Naša naslednja definicija predstavi posebn vrsto polinomov v $F[x]$, ki bodo zelo pomembni za nas.

Definicija 1.9

Nekonstantni polinom $f(x) \in F[x]$ je ***nerazcepen*** nad F (pravimo mu tudi ***nerazcepen polinom*** v $F[x]$), če polinoma $f(x)$ ne moremo zapisati kot produkt $g(x)h(x)$ dveh polinomov $g(x), h(x) \in F[x]$, ki sta manjše stopnje kot $f(x)$. Če $f(x)$ ni nerazcepen nad F pravimo, da je $f(x)$ ***razcepen*** nad F.

Opazimo lahko, da je zelo pomembno zapisati "nerazcepen **nad** F" in ne samo "nerazcepen". Polinom $f(x)$ je lahko nerazcepen nad F, vendar je morda razcepen v večjem polju E, ki vsebuje F.

Zgled 1.6.1. Polinom x^2-2 je očitno nerazcepen nad $\mathbb{Q}$, saj ga ne moremo zapisati v obliki $(ax+b)(cx+d)$ za $a,b,c,d \in \mathbb{Q}$. Vendar, če polinom obravnavamo nad poljem $\mathbb{R}$, potem je $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$, kar pomeni, da je polinom razcepen nad $\mathbb{R}$.

Nerazcepni polinomi bodo imeli odslej zelo pomembno vlogo pri našem delu. Problem, kjer želimo ugotoviti ali je dani polinom $f(x) \in F[x]$ nerazcepen nad F, ni preprost. Sedaj bomo podali nekaj kriterijev za določanje nerazcepnost, ki so uporabni v nekaterih primerih. Ena od tehnik za določanje razcepnosti kvadratnih in kubičnih polinomov je dana z naslednjim izrekom.

Izrek 1.19

Naj bo $f(x) \in F[x]$ polinom stopnje 2 ali 3. Potem je $f(x)$ razcepen nad F natanko tedaj, ko premore ničlo v F.

Dokaz: Če je $f(x)$ razcepen nad F, torej $f(x)=g(x)h(x)$, kjer sta stopnji polinomov $g(x)$ in $h(x)$ manjši kot stopnja polinoma $f(x)$, potem, ker je $f(x)$ kvadratni ali kubični polinom, je bodisi $g(x)$ bodisi $h(x)$ stopnje 1. Predpostavimo sedaj, da je $g(x)$ stopnje 1, potem je g oblike $x-a$ (po možnosti pomnožen še s faktorjem iz F). Od tod sledi, da je $g(a)=0$, kar pomeni, da je $f(a)=0$. Torej ima $f(x)$ ničlo v F. Z druge strani, če je $f(a)=0$ za $a \in F$ potem je $x-a$ faktor polinoma $f(x)$ in je torej $f(x)$ razcepen v $F[x]$.

♠

Dokaza naslednjega izreka in posledice sta prepuščena bralcu.

Izrek 1.20

Če je $f(x) \in \mathbb{Z}[x]$, potem se $f(x)$ lahko zapiše kot produkt dveh polinomov stopenj $r,s < \deg(f)$ v $\mathbb{Q}[x]$ če in samo če lahko $f(x)$ napišemo kot produkt dveh polnomov v $\mathbb{Z}[x]$, stopenj r in s.

Posledica 1.11

Če ima polinom $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ v $\mathbb{Z}[x]$, z $a_0 \neq 0$, ničlo v $\mathbb{Q}$, potem ima tudi ničlo m v $\mathbb{Z}$, kjer m deli a_0.

Za konec obravnave kriterijev za določanje nerazcepnosti predstavimo še naslednji znameniti Eisteinov kriterij.

Izrek 1.21: Eisensteinov kriterij

Naj bo $p \in \mathbb{Z}$ praštevilo in naj bo $f(x) = a_n x^n + \ldots + a_1 + a_0$ takšen polinom v $\mathbb{Z}[x]$, da je $a_n \not\equiv 0 \pmod{p}$, $a_0 \not\equiv 0 \pmod{p^2}$ in $a_i \equiv 0 \pmod{p}$ za $i < n$. Potem je $f(x)$ nerazcepen nad $\mathbb{Q}$.

Dokaz: Po Izreku 1.20 je dovolj, če pokažemo, da $f(x)$ ne moremo razcepiti na polinome manjših stopenj v $Z[x]$. Predpostavimo sedaj nasprotno; naj bo

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

razcep polinoma $f(x)$ v $Z[x]$, pri čemer je $b_r \neq 0, c_s \neq 0$ in $r, s < n$. Ker $a_0 \not\equiv 0 \pmod{p^2}$ potem velja, da ne moreta biti oba b_0 in c_0 kongruentna 0 modulo p. Recimo, da je $b_0 \not\equiv 0 \pmod{p}$ in $c_0 \equiv 0 \pmod{p}$. Ker je $a_n \not\equiv 0 \pmod{p}$ sta $b_r, c_s \not\equiv 0 \pmod{p}$ (to sledi iz dejstva, da je $a_n = b_r c_s$). Naj bo sedaj m najmanjše število za katero je $c_m \not\equiv 0 \pmod{p}$. Potem je

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + \begin{cases} b_m c_0, & \text{če je } r \geq m, \\ b_r c_{m-r}, & \text{če je } r < m. \end{cases}$$

Ker vemo, da b_0 in c_m nista kongruentna 0 modulo p in ker za $c_{m-1}, \ldots, c_0$ velja, da so kongruentni 0 modulo p, potem je $a_m \not\equiv 0 \pmod{p}$, kar pomeni, da je $m = n$. Od tod sledi, da je $s = n$, kar je v protislovju s predpostavko, da je $s < n$ (netrivialen rezcep).

♠

Zgled 1.6.2. Z uporabo Eisensteinovega kriterija, v primeru ko je $p = 3$, dobimo, da je $25x^5 - 9x^4 - 3x^2 - 12$ nerazcepen nad $\mathbb{Q}$.

O enoličnosti razcepa polinomov bomo govorili, v razdelku, kjer se bomo učili o idealih.

Naloge

1. Naj bosta polinoma $f(x)$ in $g(x)$ v $\mathbb{Z}_{11}[x]$ dana z naslednjima predpisoma $f(x) = x^5 - 2x^4 + 3x - 5$ in $g(x) = 2x + 1$. Poišči polinoma $q(x)$ in $r(x)$ v $\mathbb{Z}_{11}[x]$, za katera je $f(x) = g(x)q(x) + r(x)$, pri čemer je $\deg(r) < \deg(g)$.

2. Polinom $f(x) = 2x^3 + 3x^2 - 7x - 5$ lahko zapišemo kot produkt linearnih polinomov v $\mathbb{Z}_{11}[x]$. Poišči ta razcep.

3. Ali je $x^3 + 2x + 3$ nerazcepen v $\mathbb{Z}_5[x]$? Če je to utemelji, če ni zapiši njegov razcep kot produkt nerazcepnih polinomov v $\mathbb{Z}_5[x]$.

4. Koliko nerazcepnih polinomov stopnje 2 je v $\mathbb{Z}_p[x]$?

5. Pokaži, da je $x^p + a$ razcepen v $\mathbb{Z}_p[x]$ za vsak $a \in \mathbb{Z}_p$, pri čemer je p praštevilo.

6. Pokaži, da je $f(x) = x^2 + 8x - 2$ nerazcepen nad $\mathbb{Q}$. Ali je $f(x)$ nerazcepen nad $\mathbb{R}$? Nad $\mathbb{C}$?

7. Pokaži, da je $x^3 + 3x^2 - 8$ nerazcepen nad $\mathbb{Q}$.

8. Dokaži naslednjo trditev. Če je polinom $p(x)$ nerazcepen nad poljem F, potem je tudi polinom $p(x+a)$, $a \in F$, nerazcepen nad F.

9. Naj bo F polje. Za polinom $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$ definiramo njegov odvod $f'(x)$ s
$$f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}.$$
   (a) Pokaži, da je funkcija $D : F[x] \to F[x]$ definirana s $D(f(x)) = f'(x)$ linearna preslikav med dvema vektorskima prostoroma.
   (b) Poišči $\ker(D)$.
   (c) Dokaži, da za D velja Leibnitzovo pravilo: $D(f(x)g(x)) = D(f(x))g(x) + f(x)D(g(x))$, za vse $f(x), g(x) \in F[x]$.

Rešitve

1. $q(x) = 6x^4 + 7x^3 + 2x^2 + 10x + 2,\ r(x) = 4$

$$
\begin{array}{rl}
 & 6x^4+7x^3+2x^2+10x+2 \\
\cline{2-2}
2x+1 \big) & x^5-2x^4+0x^3+0x^2+\ 3x-5 \\
 & \underline{x^5+6x^4} \quad \downarrow \\
 & 3x^4+0x^3 \\
 & \underline{3x^4+7x^3} \quad \downarrow \\
 & 4x^3+0x^2 \\
 & \underline{4x^3+2x^2} \quad \downarrow \\
 & 9x^2+\ 3x \\
 & \underline{9x^2+10x} \quad \downarrow \\
 & 4x+6 \\
 & \underline{4x+2} \\
 & 4
\end{array}
$$

2. $x=3$ je ničla polinoma $f(x)$. Torej je $x-3$ linearni člen v razcepu polinoma $f(x)$, kar pomeni, da $x-3$ deli $f(x)$. Izračunajmo sedaj količnik pri deljenju $f(x)$ z $x-3$.

$$\begin{array}{rl} & 2x^2+9x+9 \\ \hline x-3 \,\big) & 2x^3+3x^2-7x-5 \\ & \underline{2x^3+5x^2} \quad \downarrow \\ & 9x^2+4x \\ & \underline{9x^2+6x} \quad \downarrow \\ & 9x+6 \\ & \underline{9x+6} \\ & 0 \end{array}$$

Torej je $f(x)=(x-3)(2x^2+9x+9)$. Ker je $x=4$ ničla polinoma $2x^2+9x+9$, lahko ta poliom delimo z $x-4$.

$$\begin{array}{rl} & 2x+6 \\ \hline x-4 \,\big) & 2x^2+9x+9 \\ & \underline{2x^2+3x} \quad \downarrow \\ & 6x+9 \\ & \underline{6x+9} \\ & 0 \end{array}$$

Tore je $f(x)=(x-3)(x-4)(2x+6)$.

3. Ne, saj je $x=2$ ničla polinoma $f(x)$ in $\deg(f)=3$, sedaj z uporabo Izreka 1.19 sledi, da je $f(x)$ razcepen.

$$
\begin{array}{r}
x^2+2x+1 \\
\hline
x-2\,\big)\; x^3+0x^2+2x+3 \\
\underline{x^3+3x^2} \quad \downarrow \\
2x^2+2x \\
\underline{2x^2+\;\;x} \quad \downarrow \\
x+3 \\
\underline{x+3} \\
0
\end{array}
$$

Opazimo, da je $x^2+2x+1=(x+1)^2$ in posledično $f(x)=(x-2)(x+1)^2$.

4. Brez izgube za splošnost lahko kateri koli kvadratni polinom zapišemo v obliki $a(x^2+px+q)$, kjer so $a,p,q\in\mathbb{Z}_p$ in $a\neq 0$. Ker nas zanimajo ničle se bomo osredotočili na polinom x^2+px+q. Recimo, da je

$$x^2+px+d=(x-c)(x-d).$$

Če je $c\neq d$, potem obstaja $\binom{p}{2}$ izbir za c in d. Če je $c=d$, potem obstaja p izbir za c. Torej obstaja $p+\binom{p}{2}=\frac{p(p+1)}{2}$ razcepnih polinomov stopnje 2 v $\mathbb{Z}_p$. Vemo, da v v $\mathbb{Z}_p[x]$ obstaja natanko $p^2(p-1)$ kvadratnih polinomov (glej 2. nalogo iz 4. vaj). Zato je število nerazcepnih kvadratnih polinomov v $\mathbb{Z}_p[x]$ enako

$$p^2(p-1)-\frac{p(p+1)}{2}=\frac{p^2-p^2-p^2-p}{2}=\frac{p^3-p^2-p}{2}=\frac{p(p-1)^2}{2}.$$

5. Če je $p=2$, potem sta edina možna polinoma $x^2=x\cdot x$ in $x^2+1=x^2+1^2=(x+1)^2$, ki sta oba razcepna. Predpostavimo, da je $p\neq 2$. Potem je p lih. Za poljuben $a\in\mathbb{Z}_p$ velja $-a\in\mathbb{Z}_p$. Iz

$$(-a)^p+a=-a^p+a=-a+a=0,$$

sledi, da je $-a$ ničla polinoma x^p+a, tj., x^p+a je razcepen.

6. Za $p=2$ velja $p|8$, $p|2$, $p\nmid 1$ in $p^2\nmid 2$. Torej, po Eisensteinovem kriteriju sledi, da je $f(x)$ nerazcepen nad $\mathbb{Q}$. Ker je,

$$D=b^2-4ac=64+8=72>0$$

ima $f(x)$ ničle v $\mathbb{R}[x]$ in je torej razcepen nad $\mathbb{R}$. Ker je $\mathbb{R}\subset\mathbb{C}$, je $f(x)$ razcepen

tudi nad $\mathbb{C}$.

7. Če je x^3+3x^2-8 razcepen nad $\mathbb{Q}$, vemo, da je razcepen tudi nad $\mathbb{Z}[x]$ (po Izreku 1.20) in ima torej faktor $x-a$ v $\mathbb{Z}[x]$. To pomeni, da je a ničla polinoma in deli -8 (slednje sledi iz **Izreka o racionalnih ničel**: Če ima polinom $f(x)=a_x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ celoštevilne koeficiente, potem je vsaka racionalna ničla polinoma $f(x)$ oblike p/q kjer je p faktor od a_0 in q faktor od a_n. Če je vodilni koeficient enak 1, so možne ničle kar faktorji konstantnega koeficienta.). Torej so možne ničle $a=\pm1,\pm2,\pm4,\pm8$. Ko izračunamo vrednost polinoma za vseh 8 možnosti opazimo, da vrednost ni nikoli enaka nič, kar pomeni, da je polinom nerazcepen nad $\mathbb{Q}$.

8. Predpostavimo, da je $p(x+a)$ razcepen nad F, tj.

$$p(x+a)=q(x)s(x),$$

kjer sta $q(x)$ in $s(x)$ polinoma pozitivnih stopenj. Če v zgornji enačbi zamenjamo x z $x-a$ dobimo

$$p(x)=q(x-a)s(x-a),$$

kjer sta $q(x-a)$ in $s(x-a)$ še vedno polinoma pozitivne stopnje. Ampak to pomeni, da je $p(x)$ razcepen nad F, kar ni možno. Torej je $p(x+a)$ nerazcepen nad F.

9. (a) Naj bo $g(x)=b_0+b_1x+\ldots+b_mx^m$. Brez izgube za splošnost predpostavimo, da je $n\geq m$. Torej lahko zapišemo $g(x)=\sum_{i=0}^n b_ix^i$ pri čemer so $b_{m+1}=\ldots=b_n=0$.

$$\begin{aligned}D(f(x)+g(x))&=D(\sum_{i=0}^n(a_i+b_i)x^i)=\sum_{i=0}^n i(a_i+b_i)x^{i-1}\\&=\sum_{i=0}^n ia_ix^{i-1}+\sum_{i=0}^n ib_ix^{i-1}=D(f(x))+D(g(x))\end{aligned}$$

Na pooben način pokažemo, da je $D(\alpha f(x))=\alpha D(f(x))$ za vse $\alpha\in F$. Torej je D linearna preslikava.

(b) Predpostavimo, da je $char(F)=p$.

$$\begin{aligned}D(f(x))=0&\Leftrightarrow\sum_{i=1}^n ia_ix^{i-1}=0\\&\Leftrightarrow ia_i=0,\ \forall i=0,\ldots,n\\&\Leftrightarrow a_i=0,\ \forall i=0,\ldots,n\ \text{ kjer } p\nmid i\end{aligned}$$

Torej je $\ker(D) = \{a_0 + a_p x^p + a_{2p} x^{2p} + \ldots + a_{np} x^{np} : a_i \in F, n \in \mathbb{Z}_{\geq 0}\}$. Če je $char(F) = 0$, potem je očitno $\ker(D) = F$.

(c) Za začetek pokažimo, da trditev velja za $f(x) = x^n$. Brez izgube za splošnost predpostavimo, da je $n \geq m$.

$$D(x^n g(x)) = D(x^n \cdot \sum_{i=0}^{m} b_i x^i) = \sum_{i=0}^{m} (i+n) b_i x^{i+n-1} = \sum_{i=0}^{m} i b_i x^{i+n-1} + \sum_{i=0}^{m} n b_i x^{i+n-1}$$
$$= x^n \sum_{i=0}^{m} i b_i x^{i-1} + n x^{n-1} \sum_{i=0}^{m} b_i x^i = x^n D(g(x)) + D(x^n) g(x)$$

Preostali del naloge bomo dokazali z matematično indukcijo po $\deg(f(x)) = d$. Če je $d = 0$ je $f(x) \in F$ in zaradi linearnosti velja $D(f(x)g(x)) = f(x)D(g(x))$. To pomeni, da je

$$D(f(x)) \cdot g(x) + f(x) \cdot D(g(x)) = 0 + f(x)D(g(x)) = D(f(x)g(x)).$$

Predpostavimo sedaj, da trditev drži za $d = n - 1 > 0$. Poglejmo primer, ko je $d = n$. Označimo z $f_{n-1}(x) = \sum_{i=0}^{n-1} a_i x^i$.

$$\begin{aligned} D(f(x)g(x)) &= D((a_n x^n + f_{n-1}(x))g(x)) = D(a_n x^n g(x) + f_{n-1}(x)g(x)) \\ &= a_n D(x^n g(x)) + D(f_{n-1}(x)g(x)) \\ &= a_n \cdot (n x^{n-1} g(x) + x^n D(g(x))) + D(f_{n-1}(x))g(x) + f_{n-1}(x)D(g(x)) \\ &= (n a_n x^{n-1} + D(f_{n-1}(x)))g(x) + (x^n + f_{n-1}(x))D(g(x)) \\ &= D(f(x))g(x) + f(x)D(g(x)) \end{aligned}$$

Dodatne naloge

1. Preverite razcepnost naslednjih polinomov nad $\mathbb{Q}$.

   (a) $x^2 + 4x + 2$

   (b) $x^4 - 10x^2 + 1$

   (c) $x^3 + 3x^2 + 6x + 3$

   (d) $x^3 - x^2 - 4$

   (e) $4x^3 - 2x^2 + x + 1$

   (f) $x^{50} + 14x - 56$

2. Določite razcep polinomov $f(x) = x^4 - 1$ in $g(x) = 4x^5 + 4x^4 - 13x^3 - 11x^2 + 10x + 6$ nad $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$.

3. Poiščite kvocient in ostanek pri deljenju polinoma $f(x)$ z $g(x)$ v $\mathbb{Z}_n[x]$, če je:

   (a) $f(x) = 4x^5 + 3x^2 + 2x + 4,\ g(x) = 2x^2 + 5,\ n = 7$

(b) $f(x) = x^7 + 7x^5 + 3x^2 + 11x + 5,\ g(x) = x^4 + 3x^2 + 8x + 4,\ n = 13.$

4. Poiščite vsa takšna praštevila p, da je $x+2$ faktor od $x^4 + x^3 + x^2 - x + 1$ v $\mathbb{Z}_p[x]$.

5. Poiščite vse nerazcepne polinome stopnje 3 v $\mathbb{Z}_3[x]$.

1.7. Deljivost in razcepnost v celih kolobarjih. Gaussov kolobar.

Definicija 1.10

Naj bo K komutativen kolobar in $a, b \in K$ njegova poljubna elementa. Pravimo, da b deli a ($b|a$), če obstaja takšen element $c \in K$, da je $a = bc$.

Definicija 1.11

Naj bo K cel kolobar in $a, b, c \in K$ njegovi poljubni elementi.

1. Če je $a = ub$, kjer je u enota v K, potem pravimo, da sta si $a, b \in K$ podobna v K ($a \sim b$).

2. Naj bo a neničelen element, ki ni enota. Element a je nerazcepen v K, če iz $a = bc$ za neka $b, c \in K$ sledi, da je b ali c enota. Sicer je a razcepen.

3. Naj bo p neničelen element, ki ni enota. Element p je praelement v K, če iz $p|ab$ sledi $p|a$ ali $p|b$ za vsaka $a, b \in K$.

Definicija 1.12

Naj bo K cel kolobar. Element $d \in K$ je skupni delitelj elementov $a_1, \ldots, a_n \in K$, če $d|a_i$ za $i = 1, \ldots, n$.

Definicija 1.13

Naj bo K cel kolobar in $a, b \in K$ njegova poljubna elementa. Pravimo, da je $d \in K$ največji skupni delitelj elementov a in b ($d = \gcd(a, b)$), če je

- d skupni delitelj a in b ter,
- v primeru, ko obstaja nek $p \in K$, ki je skupni delitej a in b, potem velja $p|d$.

Definicija 1.14

Naj bo K cel kolobar in $f(x), g(x) \in K[x]$. Pravimo da je $d(x) \in K[x]$ največji skupni delitelj $f(x)$ in $g(x)$, če:

- je $d(x)$ skupni delitelj $f(x)$ in $g(x)$ ter,
- v primeru, ko obstaja nek $p(x) \in K[x]$, ki je skupni delitelj $f(x)$ in $g(x)$, potem velja $p(x)|d(x)$;
- $d(x)$ je polinom z vodilnim koeficientom 1 (moničen polinom).

Definicija 1.15

Naj bo K cel kolobar. Preslikavi $N : K \to \mathbb{N}_0$ pravimo multiplikativna norma na K, če velja:

1. $N(a) = 0 \Leftrightarrow a = 0$.
2. $N(ab) = N(a)N(b)$ za vsaka $a, b \in K$.

Izrek 1.22

Naj bo N mulitplikativna norma na K in K cel kolobar. Potem velja:

1. $N(x) = 1$ natanko tedaj, ko je x enota v K.
2. Če je $N(x)$ praštevilo, potem je x nerazcepen v K.

Izrek 1.23

V celem kolobarju je vsak praelement nerazcepen.

Dokaz: Naj bo $p \in K$ praelement. Potem $p \neq 0$ in p ni enota. Če je $p = ab$ za neka $a, b \in K$, potem $p|ab$. Ker je p praelement, velja $p|a$ ali $p|b$. Denimo, da $p|a$. Torej je $a = pc$ za nek $c \in K$ in je $p = pcb$. Ker veljata zakona krajšanja je $cb = 1$. To pomeni, da je b enota. Posledično je p nerazcepen v K.

♠

Definicija 1.16

Cel kolobar K je kolobar z enolično faktorizacijo ali Gaussov kolobar, če velja:

- poljuben neničelen element $a \in K$, ki ni enota, lahko zapišemo kot končen produkt $a = a_1 a_2 \dots a_n$ nerazcepnih elementov $a_1, \dots, a_n \in K$ in

- ta končen razcep je enoličen do asociiranosti in vrstnega reda natančno: če je $a = b_1 \dots b_m$ še en razcep elementa a (kjer so $b_i \in K$ nerazcepni elementi), potem je $m = n$ in obstaja takšna permutacija $\sigma \in S_n$, da za vse $1 \leq i \leq n$ velja $a_i \sim b_{\sigma(i)}$.

Naloge

1. Pokaži, da obstaja cel kolobar, ki vsebuje dva elementa, ki nimata $\gcd$.
2. Poišči $d(x) = \gcd(f(x), g(x))$ in ga zapiši kot $d(x) = s(x)f(x) + t(x)g(x)$, če sta $f(x) = 2x^3 + 2x^2$ in $g(x) = x^4 + 2x^3 + x$ v $\mathbb{Z}_3[x]$.
3. Pokaži, da je 5 razcepen v $\mathbb{Z}[i]$ vendar nerazcepen v $\mathbb{Z}[\sqrt{2}]$.
4. Naj bo $D \neq 0$ cel kolobar v katerem sta si vsaka dva neničelna elementa podobna. Dokaži, da je D polje.
5. Poišči $\gcd(3, 1 + i\sqrt{5})$ v $\mathbb{Z}[i\sqrt{5}]$.
6. Pokaži, da v $\mathbb{Z}[\sqrt{-5}]$ ne obstaja $\gcd\ 6$ in $2(1 + \sqrt{-5})$.
7. Pokaži, da $\mathbb{Z}[\sqrt{-5}]$ ni Gaussev kolobar.
8. Izračunaj $\gcd(3 + 13i, 4 + 3i)$ v $\mathbb{Z}[i]$.

Rešitve

1. Naj bo F polje. Z S označimo podmnožico polinomov iz $F[x]$, ki nimajo linearnega faktorja:

$$S = \{\sum_{i=0}^{n} a_i x^i \in F[x] : n \in \mathbb{N}, a_1 = 0\}.$$

Trdimo, da je S cel podkolobar kolobarja $F[x]$. Dovolj je, da pokažemo, da je S podkolobar. Naj bosta $f(x), g(x) \in S$ poljubna.

- $0 \in S$
- $f(x) - g(x) \in S(x)$, ker $a_1 - b_1 = 0 - 0 = 0$
- $f(x)g(x) \in S(x)$, ker $a_1 b_0 - a_0 b_1 = 0$

Torej, po kriteriju za podkolobarje, sledi da je $S \leq F[x]$, tj. S je cel podkolobar. Poglejmo si elementa $x^5, x^6 \in S$.

Monični delitelji od x^5 so $1, x^2$ in x^3. Monični delitelji od x^6 so $1, x^2, x^3$ in x^4. Delitelji obeh so torej $1, x^2$ in x^3. Vendar nimamo največjega skupnega delitelja, saj 2. pogoj definicije ni zadoščen ($x^2 \nmid 1,\ x^3 \nmid x^2,\ x^2 \nmid x^3$).

2.

$$\begin{array}{r} x+2 \\ 2x^2+x+0 \,\big)\, 2x^3+2x^2+0x+0 \\ \underline{2x^3+\ x^2+0x} \quad \downarrow \\ x^2+0x+0 \\ \underline{x^2+2x+0} \\ x+0 \end{array} \qquad \begin{array}{r} 2x+2 \\ 2x^3+2x^2+0x+0 \,\big)\, x^4+2x^3+0x^2+\ x+0 \\ \underline{x^4+\ x^3+0x^2+0x} \quad \downarrow \\ x^3+0x^2+\ x+0 \\ \underline{x^3+\ x^2+0x+0} \\ 2x^2+\ x+0 \end{array}$$

$$\begin{aligned} q_1(x) &= 2x^2+2,\ r_1(x) = 2x^2+x & g(x) &= q_1(x)f(x)+r_1(x) \\ q_2(x) &= x+2,\ r_2(x) = x & f(x) &= q_2(x)r_1(x)+r_2(x) \\ q_3(x) &= 2x+1,\ r_3(x) = 0 & r_1(x) &= q_3(x)r_2(x) \end{aligned}$$

Torej je

$$\begin{aligned} r_2(x) &= f(x)-q_2(x)r_1(x) = f(x)-q_2(x)(g(x)-q_1(x)f(x)) \\ &= (1+q_1(x)q_2(x))f(x)-q_2(x)g(x) \\ x &= (2x^2+2)f(x)+(2x+1)g(x) \end{aligned}$$

3. Enote v $\mathbb{Z}[i]$ so $\{1,-1,i,-i\}$. Ker je $5=(2+i)(2-i)$ in sta $N(2+i)=N(2-i)=5$ praštevili, se lahko 5 zapiše kot produkt nerazcepnih elementov (po definiciji nerazcepni elementi **niso enote**) v $\mathbb{Z}[i]$ in je posledično razcepen v $\mathbb{Z}[i]$. Enote v $\mathbb{Z}[\sqrt{2}]$ so

$$\{a+b\sqrt{2} : N(a+b\sqrt{2})=1\} = \{a+b\sqrt{2} : a^2-2ab^2 = \pm 1\}.$$

Če bi bil 5 razcepen v $\mathbb{Z}[\sqrt{2}]$, potem bi veljalo, da je

$$5=(a+b\sqrt{2})(c+d\sqrt{2}) \Rightarrow 25 = N(a+b\sqrt{2})N(c+d\sqrt{2}) = |(a^2-2b^2)(c^2-2d^2)|.$$

Ker je $a^2-2b^2, c^2-2d^2 \in \mathbb{Z}$ imamo naslednje možnosti:

(i) $a^2-2b^2=\pm 5$. Če študiramo to enačbo v $\mathbb{Z}_5$ dobimo $a^2-2b^2=0$. Iz tabele:

a,b	$a^2,b^2 \pmod 5$	$2b^2 \pmod 5$
0	0	0
1	1	2
2	4	3
3	4	3
4	1	2

vidimo, da je $a^2-2b^2 \pmod 5 = 0$ samo, če je $a=b=0$. To pomeni, da sta a in b deljiva s 5 v $\mathbb{Z}$. Torej:

$$25|a^2,b^2 \Rightarrow 25|(a^2-2b^2) \Rightarrow 25|\pm 5 \text{ `}.$$

(ii) $a^2-2b^2=\pm 1$. Potem je $a+b\sqrt{2}$ enota.

(iii) $a^2-2b^2=\pm 25$. Potem je $c^2-2d^2=\pm 1$, kar pomeni, da je $c+d\sqrt{2}$ enota.

Torej lahko 5 zapišemo kot produkt dveh elementov le v primeru, ko je vsaj eden enota, tj. 5 je nerazcepen v $\mathbb{Z}[\sqrt{2}]$.

4. Naj bo $a \neq 0$ element v D. Po predpostavki sta si a in a^2 podobna v D. Torej $a^2=au$ za neko enoto $u \in D$. To pomeni, da je $a(a-u)=0$. Ker je D cel kolbar in $a \neq 0$ je $a-u=0$. Z drugimi besedami, vsak neničelen element je enota v D, tj. D je polje.

5. Če je $d=\gcd(3,1+i\sqrt{5})$ v $\mathbb{Z}[i\sqrt{5}]$, potem $N(d)$ deli $N(3)=9$ in $N(d)$ deli $N(1+i\sqrt{5})=6$. Torej, $N(d) \in \{1,3\}$. Če si pogledamo enačbo $a^2+5b^2=3$ v $\mathbb{Z}_5$, dobimo da je $a^2=3$. Ampak, 3 ni kvadrat v $\mathbb{Z}_5$. Torej mora veljati: $N(d)=1$, tj. d je enota v $\mathbb{Z}[i\sqrt{5}]$. Enoti v $\mathbb{Z}[\sqrt{-5}]$ sta 1 in -1, kar pomeni, da je $1=\gcd(3,1+i\sqrt{5})$.

6. Opazimo, da je $N(6)=36$ in $N(2(1+\sqrt{-5}))=24$. Če je $x+y\sqrt{-5}=d=\gcd(6,2(1+\sqrt{-5}))$, potem $N(d)|36$ in $N(d)|24$. Torej je $N(d) \in \{1,2,3,4,6,12\}$. Z druge strani, 2 deli $2(1+\sqrt{-5})$ in $1+\sqrt{-5}$ deli 6 ($6=(1+\sqrt{-5})(1-\sqrt{-5})$). Torej je $N(2)=4$ in $N(1+\sqrt{-5})=6$ deli $N(d)$. Od tod sledi, da je $N(d)=12$. Če si pogledamo enačbo $a^2+5b^2=12$ v $\mathbb{Z}_5$ dobimo, da je $a^2=2$. Ampak, 2 ni kvadrat v $\mathbb{Z}_5$. Torej, ne obstajata takšna elementa $a,b \in \mathbb{Z}$, da je $a^2+5b^2=12$. Z drugimi besedami, $\gcd(6,2(1+\sqrt{-5}))$ ne obstaja.

7. Vsak element kolobarja $\mathbb{Z}[\sqrt{-5}]$ je oblike $a+b\sqrt{-5}$ za neki celi števili a,b. Na $\mathbb{Z}[\sqrt{-5}]$ je definirana norma N z

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

Poglejmo si primer, ko je $a = 2, b = 1$. Torej je

$$(2+\sqrt{-5})(2-\sqrt{-5}) = 9 = 3 \cdot 3. \tag{1.7.1}$$

Trdimo, da so števila $3, 2 \pm \sqrt{-5}$ nerazcepni elementi v $\mathbb{Z}[\sqrt{-5}]$. Dovolj je pokazati, da **je vsak element v $\mathbb{Z}[\sqrt{-5}]$, ki ima normo 9, nerazcepen**.

Naj bo α takšen element v $\mathbb{Z}[\sqrt{-5}]$, da je $N(\alpha) = 9$. Predpostavimo, da je $\alpha = \beta\gamma$ za neka $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$. Naš cilj je, da pokažemo, da je bodisi β bodisi γ enota. Imamo:

$$9 = N(\alpha) = N(\beta)N(\gamma).$$

Ker je norma nenegativno celo število je $N(\beta) \in \{1, 3, 9\}$. Če je $N(\beta) = 1$, potem je β enota. Če je $N(\beta) = 3$, potem lahko zapišemo $\beta = a + b\sqrt{-5}$ za neki celi števili a, b, in dobimo, da je

$$3 = N(\beta) = a^2 + 5b^2.$$

Hiter pregled pokaže, da ne obstajata taki celi števili a, b, ki bi izplonjevali dano enakost. Torej primer, ko je $N(\beta) = 3$ ni možen. Če je $N(\beta) = 9$, potem je $N(\gamma) = 1$, kar pomeni, da je γ enota. Torej je vsaj eden izmed β in γ enota. Opazimo, da imajo elementi $3, 2 \pm \sqrt{-5}$ normo 9, in so kot takšni nerazcepni.

Ker sta enoti v $\mathbb{Z}[\sqrt{-5}]$ enaki ± 1, očitno $3 \nsim 2 \pm \sqrt{-5}$. Z drugimi besedami, faktorizacija ni enolična, kar pomeni, da $\mathbb{Z}[\sqrt{-5}]$ ni Gaussev kolobar.

8. Za izračun $\gcd$ bomo uporabili Evklidov algoritem. Spomnimo se, ko smo uporabljali Evklidov algoritem za cela števila, je bil ostanek strogo manjši od prejšnjega $(r_i < r_{i-1})$, v primeru polinomov pa je bila stopnja vsakega ostanka strogo manjša od stopnje prejšnjega ostanka $(\deg(r_i(x)) < \deg(r_{i-1}(x)))$. Podobno imamo sedaj pogoj, ki nam pove "če smo na pravi poti". Velja namreč, da je norma vsakega ostanka manjša od norme prejšnjega ostanka $(N(r_i) < N(r_{i-1})$, kjer je $N : \mathbb{Z}[i] \to nN_0$ definiran z

$$N(a+ib) = a^2 + b^2.$$

Izračunajmo norme danih elementov:

$$N(3+13i) = 178, \;\; N(4+3i) = 25.$$

Ker je $178 > 25$ delimo $3+13i$ z $4+3i$.

$$\frac{3+13i}{4+3i} = \frac{3+13i}{4+3i}\cdot\frac{4-3i}{4-3i} = \frac{51+43i}{25} = \frac{51}{25}+\frac{43}{25}i$$

Sedaj vzamimo najbližji celi števili številoma $\frac{51}{25}$ in $\frac{43}{25}$, torej število 2 v obeh primerih. Tako je naš količnik $q_1 = 2+2i$ in ostanek

$$r_1 = (3+13i)-(4+3i)\cdot q_1 = 1-i.$$

Ker je $N(r_1) = 2 < 25 = N(4+3i)$, smo na pravi poti. Nato delimo $4+3i$ z $1-i$ in dobimo

$$\frac{4+3i}{1-i} = \frac{4+3i}{1-i}\cdot\frac{1+i}{1+i} = \frac{1+7i}{2} = \frac{1}{2}+\frac{7}{2}i.$$

Vzemimo $q_2 = 3i$ in dobimo $r_2 = 4+3i-(1-i)\cdot 3i = 1$. Sedaj bi lahko naredili naslednji korak, ampak ker je r_2 enota, bi za ostanek dobili nič. Tako je $\gcd(3+13i, 4+3i) = 1$.

Komentar 1.4

Naj bosta a in b elementa celega kolobarja D in naj bo d $\gcd(a,b)$. Potem je množica $\gcd$-jev od a in b množica podobnih elementov od d (Dokaz prepuščen bralcu za domačo nalogo). Na podlagi tega dejstva je $\gcd(3+13i, 4+3i)$ enak 1 oz. celo ± 1, saj sta -1 in 1 podobna v $\mathbb{Z}[i]$. Zato bomo pri pisanju rešitve zapisali, da je največji skupni delitelj 1 skupaj z vsemi njemu podobnimi elelemnti.

Dodatne naloge

1. Poišči $\gcd$ polinomov nad danim poljem:

   (a) $f_1(x) = x^3 - x^2 - x + 1,\ g_1(x) = x^4 - 3x^2 - 2x + 4$ nad $\mathbb{Q}$

   (b) $f_2(x) = x^4 + 3x^2 + 4x,\ g_2(x) = 2x^2 - 2x - 4$ nad $\mathbb{Q}$

   (c) $f_3(x) = x^5 + 3x^3 + x^2 + 2x + 2,\ g_3(x) = x^4 + 3x^3 + 3x^2 + x + 2$ nad $\mathbb{Z}_5$

   Za vsak par polinomov $f_i(x)$ in $g_i(x)$, zapiši $\gcd$ v obliki $s_i(x)f_i(x) + t_i(x)g_i(x)$, $i = 1,2,3$.

2. Poišči vse podobne elemente $a+ib \in \mathbb{Z}[i]$.

3. Kaj so nerazcepni elementi v $\mathbb{Z}$?

4. Katera cela števila v $\{2,3,5,7,11,13,17,19\}$ so nerazcepna v $\mathbb{Z}[\sqrt{5}]$?

5. Ali je 2 praelement $\mathbb{Z}[\sqrt{-5}]$?

6. Dokaži, da v celem kolobarju D z multiplikativno normo N velja $N(1) = 1$ in $N(u) = 1$ za vsako enoto $u \in D$.

7. Dokaži, da $N(a+b\sqrt{-5}) = a^2+5b^2$ definira normo na $\mathbb{Z}[\sqrt{-5}]$.

8. Pokaži, da $\mathbb{Z}[\sqrt{-6}]$ ni KEF (Namig: Poglej si element 10).

9. Pokaži, da so $\sqrt{-2}, 1-\sqrt{-2}, 1+\sqrt{-2}, 5$ in 7 nerazcepni v $\mathbb{Z}[\sqrt{-2}]$.

10. Pokaži, da je 5 praelement v kolobarju $\mathbb{Z}[\sqrt{2}]$, vendar 7 ni.

11. Dokaži, da obstaja neskončno mnogo enot v $\mathbb{Z}[\sqrt{2}]$. (Namig: Poglej si element $(1+\sqrt{2})^n,\ n \in \mathbb{N}$).

12. Poišči $\gcd(5, 1+3i)$ v $\mathbb{Z}[i]$.

13. Pokaži, da naslednje trditve držijo za kolobar $R = \mathbb{Z}[\sqrt{-6}]$:

    (a) R ne premore elementov z normo 2 ali 5;

    (b) elementi $2, 5, 2-\sqrt{-6}$ so nerazcepni, vendar niso praelementi;

    (c) $\gcd(5, 2+\sqrt{-6}) = 1$, pri čemer je 1 identiteta v R;

    (d) $\gcd(10, 4+2\sqrt{-6})$ ne obstaja.

14. Izračunaj $\gcd$ od $7-3i$ in $5+3i$ v $\mathbb{Z}[i]$.

IDEALI IN KVOCIENTNI KOLOBARJI

2.1. Homomorfizmi in kvocientni kolobarji. Ideali.

V sekciji 1.1 smo uvedli pojem in osnovne lastnosti homomorfizmov kolobarjev. Podobno kot v teoriji grup definiramo kvocientne grupe, lahko v teoriji kolobarjev govorimo o njihovih analognih, kolobarjih kvocientov. Preden jih definiramo, bomo navedli naslednje uporabne izreke.

Izrek 2.1

Naj bo $\phi : R \to R'$ homomorfizem kolobarjev z jedrom H. Potem aditivni odseki H tvorijo kolobar R/H čigar binarni operaciji sta definirani z izbiro predstavnikov, tj. vsota dveh odsekov je definirana z

$$(a+H)+(b+H) = (a+b)+H, \tag{2.1.1}$$

produkt dveh odsekov pa z

$$(a+H)(b+H) = (ab)+H. \tag{2.1.2}$$

Velja še, da je funkcija $\mu : R/H \to \phi[R]$ definirana kot $\mu(a+H) = \phi(a)$ izomorfizem.

V naslednjem izreku opisujemo točno tiste H, za katere je (2.1.2) dobro definiran.

Izrek 2.2

Naj bo H podkolobar kolobarja R. Produkt aditivnih odsekov

$$(a+H)(b+H) = (ab)+H$$

je dobro definiran v H natanko tedaj, ko za vse $a,b \in R$ in $h \in H$, velja: $ah \in H$ in $hb \in H$.

V teoriji grup so grupe edinke ravno tista podstruktura grup, ki je potrebna za tvorbo kvocientne grupe z dobro definirano operacijo na odsekih.

Iz Izreka 2.2, vidimo, da mora v teoriji kolobarjev analogna podstruktura biti tak podkolobar H kolobarja R, da je $aH \subseteq H$ in $Hb \subseteq H$ za vsaka $a,b \in R$, kjer je $aH = \{ah : h \in H\}$ in $Hb = \{hb : h \in H\}$. Od zdaj naprej bomo uporabljali N namesto

H, ko bomo govorili o kolobarju, ki je analogen grupam edinkam. V ta namen definiramo naslednjo pomembno strukturo.

Definicija 2.1

Aditivna podgrupa N kolobarja R, ki zadovoljuje lastnosti

$$aN \subseteq N \quad \wedge \quad Nb \subseteq N, \ \forall a, b \in R$$

se imenuje (dvostranski) ***ideal***.

Komentar 2.1

Če velja le $RN \subseteq N$ (oz. $NR \subseteq N$), potem je N ***levi*** (oz. ***desni***) ideal kolobarja R.

Izrek 2.3

$N \subseteq R$ je desni (levi) ideal v R natanko tedaj, ko velja:

(i) $0 \in N$

(ii) $a - b \in N, \ \forall a, b \in N$

(iii) $na \in N \ (an \in N), \ \forall n \in N, \ a \in R$

Komentar 2.2

Očitno je vsak ideal v kolobarju R (levi, desni ali dvostranski) podkolobar kolobarja R.

Sedaj lahko definiramo kvocientne kolobarje.

Posledica 2.1

Naj bo N ideal v kolobarju R. Aditivni odseki ideala N tvorijo kolobar R/N z binarnima operacijama (2.1.1) in (2.1.2), kjer je $N = H$.

Definicija 2.2

Kolobar R/N se imenuje ***faktorski kolobar*** (ali ***kvocientni kolobar***) kolobarja R po idealu N.

Za zaključek si poglejmo naslednji pomemben in uporaben rezultat.

Izrek 2.4

Naj bo $\phi : R \to R'$ homomorfizem kolobarjev z jedrom N. Potem je $\phi[R]$ kolobar in $\mu : R/N \to \phi[R]$ izomorfizem, definiran kot $\mu(x+N) = \phi(x)$. Če je $\gamma : R \to R/N$ homomorfizem kolobarjev, definiran kot $\gamma(x) = x+N$, potem za vsak $x \in R$ velja $\phi(x) = \mu(\gamma(x))$.

Naloge

1. Poišči vse ideale kolobarja $\mathbb{Z}$. Ali je $\mathbb{Z}$ ideal v $\mathbb{Q}$?

2. Naj bo K kolobar z enoto 1 in naj bo J poljuben (enostranski ali dvostranski) ideal v K. Dokaži:

   (a) Če je $1 \in J$, potem je $J = K$.

   (b) Če je K polje, potem sta 0 in K edina ideala v K.

3. Poišči vse ideale v $\mathbb{Z}_{18}$. Posploši rezultat na $\mathbb{Z}_n$.

4. Naj bosta R in R' kolobarja in I' ideal v R'. Naj bo $f^{-1}(I') = I$ praslika ideala I' pod f. Pokaži, da je I ideal v R.

5. Naj bosta R in R' komutativna kolobarja in $f : R \to R'$ epimorfizem kolobarjev. Naj bo I ideal v R in I' ideal v R'.

   (a) Dokaži, da je $f(\sqrt{I}) \subset \sqrt{f(I)}$.[1]

   (b) Dokaži, da je $\sqrt{f^{-1}(I')} = f^{-1}(\sqrt{I'})$.

   (c) Če je $\ker(f) \subset I$, potem je $f(\sqrt{I}) = \sqrt{f(I)}$.

6. Ali množica vseh nilpotentnih elementov v komutativnem kolobarju R tvori ideal v R? Kaj pa, če izpustimo besedo "komutativen".

7. Predpostavimo, da je $f : R \to R'$ epimorfizem. Dokaži, da če je R noetherski kolobar[2], potem je tudi R'.

8. Naj bo R kolobar in I njegov ideal. Dokaži, da je R/I komutativen kolobar natanko tedaj, ko je $(rs - sr) \in I$ za vsaka $r, s \in R$.

9. Naj bo R kolobar z enoto in I levi ideal v R. Dokaži; če R premore levo enoto a, potem je $I = R$.

[1] Za ideal I v R definiramo njegov **radikalni ideal** $\sqrt{I}$ kot $\sqrt{I} = \{a \in R : a^n \in I \text{ za nek } n \in \mathbb{N}\}$.

[2] Kolobarju R pravimo, da je **noetherski**, če za naraščajočo verigo idealov $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$ kolobarja R obstaja naravno število $N \in \mathbb{N}$ za katero velja $I_N = I_{N+1} = \ldots$

10. Naj bo $R = \left\{ \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} : u, v \in \mathbb{Q} \right\}$ kolobar. Pokaži, da je $I = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{Q} \right\}$ ideal v R. Dokaži, da je kvocientni kolobar R/I izomorfen $\mathbb{Q}$.

Rešitve

1. Naj bo I ideal v $\mathbb{Z}$. Potem je I podkolobar v $\mathbb{Z}$. Torej, $(I,+) \leq (\mathbb{Z},+) \Rightarrow I = m\mathbb{Z}$ za nek $m \in \mathbb{N}_0$.

   Trditev: I je ideal v $\mathbb{Z}$ natanko tedaj, ko je $I = m\mathbb{Z},\ m \in \mathbb{N}_0$.

   $\boxed{\Rightarrow}$ Že dokazano.

   $\boxed{\Leftarrow}$ Naj bo $I = m\mathbb{Z}$ za nek $m \in \mathbb{N}_0$. Potem je I podkolobar v $\mathbb{Z}$ za katerega očitno veljata točki (i) in (ii) Izreka 2.3. Pokazati moramo le točko (iii). Naj bosta $x \in \mathbb{Z}$ in $y \in m\mathbb{Z}$ poljubna.

$$\begin{aligned} &\Rightarrow y = m\tilde{y},\ \tilde{y} \in \mathbb{Z} \\ &\Rightarrow xy = xm\tilde{y} = m(x\tilde{y}) \in m\mathbb{Z} \\ &\quad\ yx = m\tilde{y}x = m(\tilde{y}x) \in m\mathbb{Z} \\ &\Rightarrow I \text{ je ideal v } \mathbb{Z} \end{aligned}$$

   Ker je $(\mathbb{Z},+) \leq (\mathbb{Q},+)$ točki (i) in (ii) Ireka 2.3 očitno držita. Preverimo še (iii). Če vzamemo $x = 2 \in \mathbb{Z}$ in $y = \frac{1}{3} \in \mathbb{Q}$ dobimo $yx = \frac{2}{3} \notin \mathbb{Z}$. Torej, $\mathbb{Z}$ ni ideal v $\mathbb{Q}$.

2. (a) Vzemimo poljuben element $k \in K$. Ker je $k = k \cdot 1$ in $1 \in J$ sledi, da je $k \in J$ (ker je J ideal v K). Torej, $K \subseteq J$. Očitno, $J \subseteq K$ kar pomeni, da je $J = K$.

   (b) Naj bo J poljuben ideal v K. Če je $J = \{0\}$, smo končali. Predpostavimo, da je $J \neq \{0\}$. To pomeni, da obstaja element $0 \neq x \in J$. Ker je F polje, obstaja $x^{-1} \in F$. Torej $x^{-1} \cdot x = 1 \in J$. Iz (a) sledi, da je $J = K$.

3. Vsak ideal v kolobarju je tudi podkolobar in je kot tak aditivna podgrupa v aditivni grupi kolobarja. Ciklična grupa $\mathbb{Z}_{18}$ vsebuje naslednje podgrupe:

$$\{0\} = 18\mathbb{Z}_{18},\ 9\mathbb{Z}_{18},\ 6\mathbb{Z}_{18},\ 3\mathbb{Z}_{18},\ 2\mathbb{Z}_{18},\ \mathbb{Z}_{18}.$$

   Za bralca: Potrdite, da so vse zgornje množice res ideali v $\mathbb{Z}_{18}$.

   Posplošitev: Za vsak $n \in \mathbb{N}$ velja, da so ideali v $\mathbb{Z}_n$ oblike $k\mathbb{Z}_n$, kjer je k delitelj od n.
   Dokaz. Naj bo I poljuben ideal v $\mathbb{Z}_n$. Vemo, da je $(I,+) \leq (\mathbb{Z}_n,+)$. Ker je (aditivna grupa) $\mathbb{Z}_n$ ciklična so tudi vse njene podgrupe ciklične. Natančneje,

vse podgrupe so oblike $k\mathbb{Z}_n$, kjer je k delitelj od n. Naj bosta $x \in \mathbb{Z}_n$ in $y \in k\mathbb{Z}_n$ poljubna. Imamo

$$y = k\tau,\ \tau \in \mathbb{Z}_n \Rightarrow xy = yx = k \cdot (x\tau) \in k\mathbb{Z}_n.$$

Torej je $I = k\mathbb{Z}_n$ za vsak tak $k \in \mathbb{N}$, za katerega velja $k|n$.

4. Dokazati moramo naslednji dve lastnosti: $(I,+) \leq (R,+)$ in $IR, RI \subseteq I$.

   - Naj bosta $a,b \in I$ poljubna. Od tod sledi, da sta $f(a), f(b) \in I'$. Ker je I' ideal sledi, da je $f(a) - f(b) \in I'$. Z druge strani, ker je f homomorfizem kolobarjev, je $f(a-b) \in I'$. To pomeni, da je $a - b \in f^{-1}(I') = I$.
   - Naj bosta $a \in I$ in $r \in R$ poljubna. Ker sta $f(a) \in I', f(r) \in R'$ in je I' ideal v R' je $f(r)f(a) \in I',\ f(a)f(r) \in I'$. Ker je f homomorfizem, sta tudi $f(ra), f(ar) \in I'$. Torej $ra, ar \in f^{-1}(I') = I$.

   Od tod sledi, da je I ideal v R.

5. (a) Naj bo $x \in f(\sqrt{I})$ poljuben. To pomeni, da obstaja takšen $a \in \sqrt{I}$, da je $f(a) = x$. Ker je $a \in \sqrt{I}$, obstaja takno pozitivno celo število $n \in \mathbb{N}$, da je $a^n \in I$. Torej, ker je f homomorfizem sledi, da je $x^n = f(a)^n = f(a^n) \in f(I)$. Z drugimi besedami $x \in \sqrt{f(I)}$, torej $f(\sqrt{I}) \subseteq \sqrt{f(I)}$.

   (b) $\boxed{\subseteq}$ Naj bo $x \in \sqrt{f^{-1}(I')}$ poljuben. Sledi:

   $$\begin{aligned}(\exists n \in \mathbb{N})\ x^n \in f^{-1}(I') &\Rightarrow f(x^n) \in I' \\ &\Rightarrow f(x)^n \in I'\ (f \text{ homomorfizem}) \\ &\Rightarrow f(x) \in \sqrt{I'}\end{aligned}$$

   $\boxed{\supseteq}$ Naj bo $x \in f^{-1}(\sqrt{I'})$ poljuben. Sledi:

   $$\begin{aligned}f(x) \in \sqrt{I'} &\Rightarrow (\exists n \in \mathbb{N})\ f(x)^n \in I' \\ &\Rightarrow f(x^n) \in I' \\ &\Rightarrow x^n \in f^{-1}(I') \Rightarrow x \in \sqrt{f^{-1}(I')}\end{aligned}$$

   Torej, $f^{-1}(\sqrt{I'}) = \sqrt{f^{-1}(I')}$.

   (c) $\boxed{\subseteq}$ Sledi iz (a).

   $\boxed{\supseteq}$ Naj bo $x \in \sqrt{f(I)} \subseteq R'$ poljuben. To pomeni, da obstaja takšen $n \in \mathbb{N}$, da je $x^n \in f(I)$, tj., obstaja takšen element $a \in I$, da velja $x^n = f(a)$. Ker je f surjekcija, vemo da obstaja takšen element $y \in R$ za katerega je $f(y) = x$.

Z drugimi besedami

$$f(a) = x^n = f(y)^n = f(y^n) \Rightarrow f(a) - f(y^n) = 0 \Rightarrow f(a - y^n) = 0 \Rightarrow a - y^n \in \ker(f) \subseteq I.$$

Ker je $a \in I$, je $y^n \in I$, torej $y \in \sqrt{I}$. Od tod sledi, da je $f(y) = x \in f(\sqrt{I})$, tj. $\sqrt{f(I)} \subseteq f(\sqrt{I})$. Torej, $f(\sqrt{I}) = \sqrt{f(I)}$.

6. Označimo z $N(R) = \{x \in R : (\exists n \in \mathbb{N})\ x^n = 0\}$ množico vseh nilpotentnih elementov v R. Očitno je $0 \in N(R)$. Naj bosta $x \in N(R)$ in $a \in R$ poljubna. Torej, obstaja takšno naravno število $n \in \mathbb{N}$, da je $x^n = 0$. Ampak potem je tudi $a^n x^n = 0 \Leftrightarrow (ax)^n = (xa)^n = 0$ (R komutativen). Z drugimi besedami, $ax, xa \in N(R)$. Naj bosta $x, y \in N(R)$ poljubna. Torej je $x^n = 0$ in $y^m = 0$ za neka $n, m \in \mathbb{N}$. Ker je R komutativen velja binomski izrek in dobimo:

$$(x-y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k}(-1)^k y^k = 0,$$

če je $p - k \geq n$ in $k \geq m$. Z drugimi besedami, $p \geq n + m$. Torej, $(x-y)^{n+m} = 0$, tj., $x - y \in N(R)$. To pomeni, da je $N(R)$ res ideal v R.

Če R ni komutativen, potem $N(R)$ ni nujno ideal v R. Proti primer: Naj bo R kolobar vseh matrik velikosti 2×2 nad poljem realnih števil. Vzemimo

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R.$$

Očitno sta $A^2 = 0$ in $B^2 = 0$, tj. $A, B \in N(R)$. Ampak, $A + B$ ni nilpotent, saj je

$$(A+B)^n = \begin{cases} A+B, & n = 2k+1 \\ I_2, & n = 2k \end{cases},\ k \in \mathbb{N}$$

7. Naj bo $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$ naraščajoča veriga idealov v R'. Iz naloge 4 sledi, da so praslike $f^{-1}(I_k)$ idealov I_k pod homomorfizmom f ideali v R. Torej imamo naraščajočo verigo idealov v R:

$$f^{-1}(I_1) \subseteq f^{-1}(I_2) \subseteq \ldots \subseteq f^{-1}(I_k) \ldots$$

Ker je R noetherski, obstaja takšno število $N \in \mathbb{N}$, da je

$$f^{-1}(I_N) = f^{-1}(I_{N+1}) = \ldots$$

Ker je f epimorfizem je

$$f(f^{-1}(I_k)) = I_k,$$

za vsak $k \in \mathbb{N}$. To pomeni, da je

$$I_N = I_{N+1} = \dots$$

Z drugimi besedami, R' je noetherski.

8.

$$\begin{aligned} R/I \text{ komutativen} &\Leftrightarrow (r+I)(s+I) = (s+I)(r+I),\ \forall r,s \in R \\ &\Leftrightarrow rs+I = sr+I,\ \forall r,s \in R \\ &\Leftrightarrow (rs+I)-(sr+I) = I,\ \forall r,s \in R\ (0_{K/I} = I) \\ &\Leftrightarrow (rs-sr)+I = I,\ \forall r,s \in R \\ &\Leftrightarrow rs-sr \in I,\ \forall r,s \in R \end{aligned}$$

9. Naj bo I levi ideal v R in naj bo $a \in I$ enota. Torej, obstaja $a^{-1} \in R$. Ker je I levi ideal velja $aa^{-1} = 1 \in I$. Iz naloge 2a sledi, da je $I = R$.

10. Naj bosta

$$\alpha = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \beta = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in I$$

poljubna. Ker sta $0, \alpha - \beta \in I$ sledi, da je I aditivna grupa. Naj bo

$$\gamma = \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} \in R$$

poljuben. Ker sta

$$\begin{aligned} \gamma\alpha &= \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & ua \\ 0 & 0 \end{bmatrix} \in I \text{ in} \\ \alpha\gamma &= \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} = \begin{bmatrix} 0 & au \\ 0 & 0 \end{bmatrix} \in I \end{aligned}$$

sledi, da je I ideal v R. Definirajmo funkcijo $\phi : R \to \mathbb{Q}$ s

$$\phi\left(\begin{bmatrix} u & v \\ 0 & u \end{bmatrix}\right) = u.$$

Za bralca: Dokaži, da je ϕ homomorfizem.

Izračunajmo $\ker(\phi)$ in $\mathrm{im}(\phi)$. **Trditev:** $\ker(\phi) = I$.

$\boxed{\subseteq}$ Naj bo

$$\rho = \begin{bmatrix} u & v \\ 0 & u \end{bmatrix} \in \ker(\phi)$$

poljuben. Potem je $\phi(\rho) = u = 0$. Torej,

$$\rho = \begin{bmatrix} 0 & v \\ 0 & 0 \end{bmatrix} \in I \Rightarrow \ker(\phi) \subseteq I.$$

$\boxed{\supseteq}$ Naj bo

$$\begin{bmatrix} 0 & v \\ 0 & 0 \end{bmatrix} \in I$$

poljuben. Ker je $\phi(\rho) = 0$ sledi, da je $\rho \in \ker(\phi)$. To pomeni, $I \subseteq \ker(\phi)$.

Torej, $I = \ker(\phi)$. Ker je ϕ surjekcija, sledi da je $\mathrm{im}(\phi) = \mathbb{Q}$. Po izreku 2.4 zaključimo, da je

$$R/\ker(\phi) \cong \mathrm{im}(\phi) \Leftrightarrow R/I \cong \mathbb{Q}.$$

Dodatne naloge

1. Naj bo R komutativen kolobar in $a \in R$. Dokaži, da je $I_a = \{x \in R : ax = 0\}$ ideal v R.
2. Dokaži, da je presek števno mnogo idealov v R ideal v R.
3. Naj bo $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \right\}$. Dokaži, da je funkcija

$$f : \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mapsto a$$

homomorfizem kolobarja S na $\mathbb{R}$. Poišči $\ker(f)$ in kvocienti kolobar $S/\ker(f)$.

4. Dokaži, da kvocientni kolobar $R/N(R)$, kjer je $N(R)$ ideal nilpotentnih elementov v R, ne vsebuje nilpotentnih elementov.
5. Naj bo R kolobar in I ideal v R ter $a \in R$. Dokaži, da je $A = \{r \in R : ra - ar \in I\}$ podkolobar kolobarja R.
6. Naj bo R komutativen kolobar z enoto v katerem je vsak element bodisi nilpotent bodisi enota. Dokaži, da je $R/N(R)$ polje, kjer je $N(R)$ ideal nilpotentnih elementov v R.

7. Dokaži, da kolobar $F^{n\times n}$ matrik velikosti $n\times n$, $n\geq 2$, nad poljem F vsebuje samo trivialne ideale.

8. Naj bo R kolobar brez deliteljev niča v katerem je vsak podkolobar hkrati ideal. Dokaži, da je R komutativen.

9. Naj bo I ideal v komutativnem kolobarju R.

   (a) Dokaži, da je tudi $\sqrt{I}=\{r\in R : (\exists n\in\mathbb{N})\ r^n\in I\}$ ideal v R.

   (b) Določi ali naslednje enakosti držijo: $\sqrt{\sqrt{I}}=\sqrt{I}$, $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$ in $\sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}$.

2.2. Maksimalni in glavni ideali. Praideali

Definicija 2.3

Naj bo R kolobar. Za ideal $P\neq R$ pravimo, da je je ***praideal***, če za vsaka $a,b\in R$ velja:

$$ab\in P\Rightarrow a\in P\ \vee\ b\in P.$$

Zgled 2.2.1. Ničla ideal je praidel v poljubnem celem kolobarju, ker je $ab=0$ natako tedaj, ko je $a=0$ ali $b=0$. Če je p praštevilo, je ideal $p\mathbb{Z}$ praideal, saj iz $ab\in p\mathbb{Z}$ sledi $p|ab$, kar pomeni, da bodisi $p|a$ bodisi $p|b$, tj., $a\in p\mathbb{Z}$ ali $b\in p\mathbb{Z}$.

Definicija 2.4

Pravi ideal $M\subset R$ kolobarja $R\neq 0$ je ***maksimalen***, če za poljuben ideal I v R, kjer je $M\subseteq I\subseteq R$, velja, da je bodisi $I=M$ bodisi $I=R$.

Zgled 2.2.2. Ideal $3\mathbb{Z}$ je maksimalen v $\mathbb{Z}$, vendar ideal $4\mathbb{Z}$ ni maksimalen v $\mathbb{Z}$, saj je $4\mathbb{Z}\subset 2\mathbb{Z}\subset\mathbb{Z}$.

Izrek 2.5

Naj bo R komutativen kolobar z enoto. Potem velja naslednje:

1. R/P je cel kolobar natanko tedaj, ko je P praideal v R.
2. R/M je polje natanko tedaj, ko je M maksimalen ideal v R.
3. Vsak maksimalen ideal v R je hkrati praideal.

Definicija 2.5

Če je R komutativen kolobar z enoto in $a \in R$, potem ideal $\{ra : r \in R\}$ vseh večkratnikov od a imenujemo ***glavni ideal generiran z*** a inga označimo z $\langle a \rangle$. Za ideal N v R pravimo, da je ***glavni ideal***, če je $N = \langle a \rangle$ za nek $a \in R$.

Definicija 2.6

Cel kolobar v katerem je vsak ideal glavni imenujemo ***glavni kolobar*** (***GK***).

Izrek 2.6

Naj bo F polje. Potem velja naslednje:

1. Vsak ideal v $F[x]$ je glavni.
2. Ideal $\langle p(x) \rangle \neq \{0\}$ v $F[x]$ je maksimalen natanko tedaj, ko je $p(x)$ nerazcepen nad F.

Noehterski izreki o izomorfizmu:

Izrek 2.7

Če je $f : R \to R'$ homomorfizem kolobarja, potem je:

1. $\ker(f)$ ideal v R,
2. $\mathrm{im}(f)$ podkolobar v R',
3. $R/\ker(f) \cong \mathrm{im}(f)$.

V primeru, ko je f surjekcija velja tudi: $R/\ker(f) \equiv R'$.

Izrek 2.8

Naj bo R kolobar, S podkolobar od R in I ideal v R. Potem je:

1. vsota $S+I = \{s+i : s \in S, i \in I\}$ podkolobar v R,
2. $S \cap I$ ideal v S,
3. $(S+I)/I \cong S/(S \cap I)$.

Izrek 2.9

Naj bo R kolobar in A, B ideala v R ($B \subseteq A \subseteq R$). Potem je:

1. množica A/B ideal v kvocientnem kolobarju R/B,

2. $(R/B)/(A/B) \cong R/A$.

Naloge

1. Poišči vse praideale in maksimalne ideale v $\mathbb{Z}_6$.
2. Poišči vse praideale in maksimalne ideale v $\mathbb{Z}_{12}$.
3. Poišči vse praideale in maksimalne ideale v $\mathbb{Z}_2 \times \mathbb{Z}_2$.
4. Poišče vse $c \in \mathbb{Z}_3$ za katere je $\mathbb{Z}_3[x]/\langle x^3 + c \rangle$ polje.
5. Poišči vse $c \in \mathbb{Z}_3$ za katere je $\mathbb{Z}_3[x]/\langle x^3 + x^2 + c \rangle$ polje.
6. Naj bo F polje in $f(x), g(x) \in F[x]$. Dokaži, da $f(x)$ deli $g(x)$ natanko tedaj, ko je $g(x) \in \langle f(x) \rangle$.
7. Dokaži, da je v komutativnem kolobarju z enoto R pravi ideal M maksimalen natanko tedaj, ko za vsak $r \notin M$ obstaja tak element $x_r \in R$, da je $1 + rx_r \in M$.
8. Naj bo R komutativen kolobar z enoto $1 \neq 0$. Naj za vsak element $a \in R$ obstaja tako pozitivno celo število n, da je $a^n = a$. Dokaži, da je vsak praideal maksimalen.
9. Dokaži, da je ideal $P = \langle 2, \sqrt{10} \rangle = \{a + b\sqrt{10} | a, b \in \mathbb{Z}, 2|a\}$ kolobarja $\mathbb{Z}[\sqrt{10}]$ praideal.
10. Naj bo R glavni kolobar in naj bo $a \in R$ poljuben, neničelen element, ki ni enota. Dokaži, da so naslednje trditve ekvivalentne:
    (a) Ideal $\langle a \rangle$ je maksimalen.
    (b) Ideal $\langle a \rangle$ je praideal.
    (c) Element a je nerazcepen.
11. Dokaži, da je v glavnem kolobarju vsak nerazcepen element tudi praelement.

Rešitve

1. Vemo, da je vsak ideal v $\mathbb{Z}_n$ oblike $k\mathbb{Z}_n$, pri čemer $k|n$. Ker je končen cel kolobar polje, praideal in maksimalni ideal sovpadata.

Ideali v $\mathbb{Z}_6$	Praideal	Maksimalni ideal
$\mathbb{Z}_6$	DA	NE
$2\mathbb{Z}_6 = \{0,2,4\}$	DA	NE
$3\mathbb{Z}_6 = \{0,3\}$	DA	NE
$6\mathbb{Z}_6 = \{0\}$	DA	NE

Od tod sledi naslednji uporaben izrek:

Izrek 2.10

$\mathbb{Z}_n/\langle d\rangle$ je cel kolobar natanko tedaj, ko je $d \neq n$ praštevilo.

2.

Ideali v $\mathbb{Z}_{12}$	Praideal	Maksimalni ideal
$\mathbb{Z}_{12}$	NE	NE
$2\mathbb{Z}_{12}$	DA	DA
$3\mathbb{Z}_{12}$	DA	DA
$4\mathbb{Z}_{12}$	NE	NE
$6\mathbb{Z}_{12}$	NE	NE
$12\mathbb{Z}_{12} = \{0\}$	NE	NE

3. Če sta R in S kolobarja z enoto, je vsak ideal v $R \times S$ oblike $I \times J$, kjer je I ideal v R in J ideal v S.

Ideai v $\mathbb{Z}_2 \times \mathbb{Z}_2$	Praideal	Maksimalen ideal
$\{0\} \times \{0\}$	NE	NE
$\{0\} \times \mathbb{Z}_2$	DA	DA
$\mathbb{Z}_2 \times \{0\}$	DA	DA
$\mathbb{Z}_2 \times \mathbb{Z}_2$	NE	NE

Komentar 2.3

Naj bosta R in S kolobarja, ter I in J njuna ideala. Potem velja:

$$(R \times S)/(I \times J) \cong (R/I) \times (S/J). \tag{2.2.1}$$

Iz (2.2.1) sledi, da je $(\mathbb{Z}_2 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2) \cong \mathbb{Z}_2$ in $(\mathbb{Z}_2 \times \mathbb{Z}_2)/(\mathbb{Z}_2 \times \{0\}) \cong \mathbb{Z}_2$. Ker je $\mathbb{Z}_2$ polje, z uporabo izreka 2.5 sledi, da sta $\mathbb{Z}_2 \times \{0\}$ in $\{0\} \times \mathbb{Z}_2$ maksimalna ideala in hkrati praideala.

4. Iz izreka 2.6 in izreka 2.5 velja: če je F polje in $f(x) \in F[x]$ je

$$F/\langle f(x)\rangle \text{ je polje } \Leftrightarrow \langle f(x)\rangle \text{ je maksimalen } \Leftrightarrow f(x) \text{ je nerazcepen nad } F.$$

Torej moramo poiskati vse elemente $c \in \mathbb{Z}_3$ za katere je $f(x) = x^3 + c$ nerazcepen nad $\mathbb{Z}_3$. Če preverimo za $c = 0, 1$ in 2, opazimo da noben polinom ni razcepen nad $\mathbb{Z}_3$.

5. Podobno kot v prejšnjem problemu moramo določiti vse $c \; in \; zZ_3$, za katere je polinom $f(x) = x^3 + x^2 + c$ nerazcepen nad zZ_3. Pogoj je izpolnjen le za $c = 2$.

6.

$$f(x)|g(x) \Leftrightarrow (\exists q(x) \in F[x])g(x) = f(x)q(x) \Leftrightarrow g(x) \in \langle f(x)\rangle .$$

Komentar 2.4

Vsak neničelen polinom $g(x) \in \langle f(x)\rangle$ je stopnje najmanj $\deg(f)$.

7. $\boxed{\Rightarrow}$ Naj bo M maksimalen ideal. Potem za poljuben $r \notin M$ velja $M + rR = R$, saj je $M + rR$ ideal, ki popolnoma vsebuje M. Tako moramo za nek $m \in M$ in $x \in R$ imeti $m + rx = 1$, z drugimi besedami, če označimo z $x_r = -x$, dobimo $1 + rx_r = m \in M$.

   $\boxed{\Leftarrow}$ Recimo, da za vsak $r \notin M$ obstaja tak element $x_r \in M$, da je $1 + rx_r = m \in M$. Ker ideal $M + rR$ vsebuje 1, moramo držati naslednje: $M + rR = R$ (glej nalogo 2a). Torej, če je $M \subseteq I$ in $M \neq I$, potem za $r \in I \setminus M$ velja $rR \subseteq I$ (ker je I ideal) in $M + rR = R \subseteq I$, tj. $I = R$. Torej je M maksimalen.

8. Naj bo I praideal kolobarja R. Za dokaz, da je I maksimalni ideal, zadostuje, da pokažemo, da je kvocientni kolobar R/I polje. Naj bo $\bar{a} = a + I$ neničelni element od R/I, kjer je $a \in R$. Iz predpostavke sledi, da obstaja celo število $n > 1$, tako da je $a^n = a$. Potem imamo

$$\bar{a}^n = a^n + I = a + I = \bar{a}.$$

Tako je

$$\bar{a}(\bar{a}^{n-1} - 1) = 0$$

v R/I. Upoštevajmo, da je R/I cel kolobar, saj je I praideal. Ker je $\bar{a} \neq 0$, zgornja enakost daje, da je $\bar{a}^{n-1} - 1 = 0$ in s tem

$$\bar{a} \cdot \bar{a}^{n-2} = 1.$$

Iz tega sledi, da ima $\bar{a}$ multiplikativni inverz $\bar{a}^{n-2}$. To dokazuje, da je vsak

neničelni element R/I enota, zato je R/I polje.

9. Recimo, da so $a+b\sqrt{10}, c+d\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ in produkt $(a+b\sqrt{10})(c+d\sqrt{10}) \in P$. Nato razširimo produkt, imamo

$$ac+10bd+(ad+bc)\sqrt{10} \in P.$$

Ker mora biti $ac+10bd$ sodo število, je bodisi a bodisi c sodo. Zato je bodisi

$$a+b\sqrt{10} \in P \text{ bodisi } c+d\sqrt{10} \in P,$$

in sklepamo, da je P praideal.

10.

$\boxed{(a) \Rightarrow (b)}$ Sledi iz Izreka 2.5.

$\boxed{(b) \Rightarrow (c)}$ Predpostavimo sedaj, da je ideal $\langle a \rangle$ praideal. Naj bo $a = bc$ za neka $b, c \in R$. Potem je $a = bc$ v praidealu $\langle a \rangle$ in od tod sledi, da je bodisi b bodisi c v $\langle a \rangle$. Brez izgube za splošnost lahko predpostavimo, da je $b \in \langle a \rangle$. Potem je $b = ad$ za nek $d \in R$. Sledi, da je

$$a = bc = adc$$

in ker je R cel kolobar, imamo

$$1 = dc.$$

Torej je c enota. To pomeni, da je a nerazcepen.

$\boxed{(c) \Rightarrow (a)}$ Recimo, da je a nerazcepen element. Naj bo I takšen ideal kolobarja R, za katerega je

$$\langle a \rangle \subseteq I \subseteq R.$$

Ker je R GK, obstaja tak $b \in R$, da je $I = \langle b \rangle$. Sedaj, ker je $\langle a \rangle \subseteq \langle b \rangle$, sledi, da je $a = bc$ za nek $c \in R$. Nerazcepnost elementa a pomeni, da je bodisi b bodisi c enota. Če je b enota, potem je $I = R$. Če je c enota, potem je $\langle a \rangle = I$. Torej je ideal $\langle a \rangle$ maksimalen.

11. Naj bo p nerazcepen element v R in R GK. Iz prejšnje naloge sledi, da je ideal $\langle p \rangle$ praideal. Pokazali bomo, da je to enakovredno trditvi, da je p praelement.

Naj bo $\langle p \rangle$ paideal. Predpostavimo, da $p|ab$. Potem obstaja tak element

$r \in R$, da je $pr = ab$. To pomeni, da je $ab \in \langle p \rangle$. Ker je $\langle p \rangle$ praideal, je bodisi $a \in \langle p \rangle$ bodisi $b \in \langle p \rangle$, z drugimi besedami, $p|a$ ali $p|b$. Na podoben način lahko pokažemo še drugo implikacijo.

Komentar 2.5

Vsak GK je tudi kolobar z enolično faktorizacijo (KEF). Obrat trditve ne drži.

Dodatne naloge

1. Naj bo R cel kolobar, v katerem vsaka množica idealov S vsebuje takšen ideal I, ki ni vsebovan v nobenem drugem idealu $J \in S$ (v tem primeru pravimo idealu I minimalen element množice S). Dokaži, da je R polje.

2. Naj bo R kolobar z enoto, ki vsebuje enoličen, maksimalen levi ideal M. Dokaži:

   (a) M je množica vseh elementov v R, ki nimajo levega multiplikativnega inverza.

   (b) Noben element v M nima desnega multiplikativnega inverza.

3. Naj bo R kolobar z enoto, ki ima enoličen, maksimalen levi ideal M. Dokaži:

   (a) M je dvostranski ideal, ki vsebuje vse prave leve in desne ideale kolobarja R.

   (b) R/M je obseg.

4. Naj bo M maksimalen ideal v komutativnem kolobarju R z enoto, v katerem je multipklitavni inverz poljubnega elementa $x \in M$ element $1+x$. Dokaži, da je M enoličen, maksimalen ideal v R. (Namig: uporabi prejšnjo nalogo.)

5. Naj bo R kolobar z enoto, ki vsebuje enoličen, maksimalen levi ideal M. Pokažite, da sta elementa 0 in 1 edina idempotenta R.

2.3. Razširitev polj. Algebraični in transcendentni elementi.

Iz Pitagorovega izreka sledi, da je dolžina diagonale kvadrata s stranico dolžine 1 enaka $\sqrt{2}$. To število pa ni racionalno. Od tod sledi, da za vsako racionalno število q velja $q^2 \neq 2$. To je bilo znano že v antični Grčiji. Spomnimo se dokaza.

Dokaz iracionalnosti števila $\sqrt{2}$. Privzemimo, da je pogoj $q^2 = 2$ izpolnjen za nek $q \in \mathbb{Q}$. Naj bo $q = \frac{m}{n}$, pri čemer je $\gcd(m,n) = 1$. Enakost $q^2 = 2$ lahko zapišemo kot $m^2 = 2n^2$. Torej je m^2 sodo število, kar pomeni, da je m sodo in je oblike $m = 2k$. Ker sta m in n tuja, je n liho. Ampak, iz $2n^2 = m^2$ sledi, da je $n^2 = 2k^2$, torej je n^2 sodo. Toda to je protislovje, saj je kvadrat lihega števila n liho število.

Za opis najbolj osnovnih geometrijskih opažanj tako potrebujemo tudi števila, ki niso racionalna. To spoznanje je sčasoma vodilo do vpeljave realnih števil. Zakaj bi širili tudi polje realnih števil? Tu je morda težje podati kratek odgovor, ki se zdi že na prvi pogled prepričljiv. Največkrat izhajamo iz dejstva, da enačba $x^2 = -1$ nima rešitve v množici realnih števil. Kompleksna števila vpeljemo tako, da to enačbo lahko rešimo. Tako najprej definiramo imaginarno enoto i, že po imenu torej nekakšno namišljeno število, za katero velja $i^2 = -1$. Zatem na znani način vpeljemo množico vseh kompleksnih števil in jo na naraven način opremimo s seštevanjem in množenjem. Kot vemo, s tem dobimo polje.

Vpeljave racionalnih, realnih in kompleksnih števil imajo skupno značilnost. Pri vseh je bil osnovni vzvod nerešljivost polinomskih enačb, torej neobstoj ničel polinomov, v dotlej znanih množicah števil. Racionalna števila so ničle linearnih polinomov $kx+n$, ki nimajo (nujno) ničel v $\mathbb{Z}$. Polinomi kot na primer x^2-2 nimajo ničel v $\mathbb{Q}$, kar je vodilo do vpeljave realnih števil. Podobno polinom x^2+1 nima ničle v $\mathbb{R}$, kar je napeljalo h konstrukciji kompleksnih števil. Reševanje polinomskih enačb je torej odigralo eno ključnih vlog v zgodovini matematike. Torej je študij razširitev polj tesno povezan s študijem polinomov, še zlasti s študijem njihovih ničel.

Definicija 2.7

Za polje E pravimo, da je razširitev polja F, če je $F \leq E$.

Naslednji izrek je velikega pomena, saj pravi, da ima vsak nekonstanten polinom ničlo v nekem polju.

Izrek 2.11: Kronecker

Naj bo F polje in $f(x) \in F[x]$ nekonstanten polinom. Potem obstaja razširitev E polja F in takšen element $\alpha \in E$, da velja $f(\alpha) = 0$.

Zgled 2.3.1. Naj bo $F = \mathbb{R}$ in $f(x) = x^2+1$. Očitno kvadratni polinom f nima ničel v $\mathbb{R}$ in je torej nerazcepen nad $\mathbb{R}$. To pomeni, da je $\langle x^2+1 \rangle$ maksimalen ideal v $\mathbb{R}$ oziroma, da je $E = \mathbb{R}/\langle x^2+1 \rangle$ polje. Očitno je $F \leq E$. Naj bo $\alpha = x + \langle x^2+1 \rangle \in E$. V E

velja naslednje

$$f(\alpha) = \alpha^2 + 1 = (x + \langle x^2+1 \rangle)^2 + (1 + \langle x^2+1 \rangle) = (x^2+1) + \langle x^2+1 \rangle = 0.$$

Torej je α ničla polinoma x^2+1. Lahko se pokaže, da je $E \cong \mathbb{C}$.

Ker bomo preučevali ničle polinomov, bo naslednja definicija za nas zelo pomembna.

Definicija 2.8

Naj bo α element iz neke razširitve E polja F. Pravimo, da je α ***algebraičen nad*** F, če obstaja tak neničelen polinom $f(x) \in F[X]$, da je $f(\alpha) = 0$. Če α ni algebraičen nad F pravimo, da je α ***transcendenten nad*** F.

Zgled 2.3.2. $\mathbb{C}$ je razširitev polja $\mathbb{Q}$. Ker je $\sqrt{2}$ ničla polinoma $x^2 - 2 \in \mathbb{Q}[x]$, je $\sqrt{2}$ algebraičen nad $\mathbb{Q}$. Znano je (ampak ni enostavno dokazati), da sta π in e transcendentna nad $\mathbb{Q}$.

Opazimo, da je zelo pomembno, da napišemo "nad poljem F".

Zgled 2.3.3. π je transcendenten nad $\mathbb{Q}$, vendar velja, da je π algebraičen nad $\mathbb{R}$, ker je rešitev polinoma $x - \pi \in \mathbb{R}[x]$.

Neničelnih polinomov, katerih ničla je algebraičen element, je več; en pa ima prav posebno vlogo.

Definicija 2.9

Polinomu $p(x) \in F[x]$ pravimo ***minimalni polinom*** algebraičnega elementa $\alpha \in E$, če je $p(\alpha) = 0$, $p(x)$ ima vodilni koeficient enak 1 in izmed vseh neničelnih polinomov iz $F[x]$, katerih ničla je α, ima $p(x)$ najnižjo stopnjo. Če je $\deg(p(x)) = n$, rečemo, da je α algebraičen ***stopnje*** n ***(nad*** F***).***

Naslednji izrek nam da celovitejši pogled na pojem minimalnega polinoma.

Izrek 2.12

Naj bo element $\alpha \in E$ algebraičen nad F in naj bo $p(x) \in F[x]$ tak polinom z vodilnim koeficientom 1, da je $p(\alpha) = 0$. Naslednje trditve so ekvivalentne:

1. $p(x)$ je minimalen polinom elementa α.
2. $p(x)$ je nerazcepen v $F[x]$.
3. $p(x)$ deli vsak polinom $f(x) \in F[x]$, za katerega je $f(\alpha) = 0$.

Komentar 2.6

Minimalni polinom elementa α nad poljem F bomo označevali z $m_{\alpha,F}$. V angleški literaturi je pogosto uporabljena oznaka $\mathrm{irr}(\alpha, F)$.

Naj bo E razširitev polja F in naj bo $\alpha \in E$. Označimo z $\phi_\alpha \colon F[x] \to E$ evalvacijski homomorfizem.

Če je α **algebraičen nad** F, potem je $\phi_\alpha(F[x]) = F[x]/\langle m_{\alpha,F}\rangle := F(\alpha)$ polje, kjer je $\phi_\alpha(x) = \alpha$ in $F(\alpha)$ vsebuje α. To je najmanjša razširitev polja F v E, ki vsebuje α (po inkluziji).

Če je α **transcedenten nad** F, potem je $\ker(\phi_\alpha) = \{0\}$ in je slika od $F[x]$ pod ϕ_α cel kolobar izomorfen $F[x]$. Ta cel kolobar bomo označili z $F[\alpha]$ in $F(\alpha)$ bo podpolje polja E, ki je izomorfen polju ulomkov $F[\alpha]$.

Definicija 2.10

Razširitev E polja F je ensotavna razširitev (polja F), če je $E = F(\alpha)$ za nek $\alpha \in E$.

Izrek 2.13

Naj bo E razširitev polja F in naj bo $\alpha \in E$ algebraičen nad F, kjer je $\deg(\alpha, F) = n \geq 1$. Potem lahko vsak elelemt $\beta \in F(\alpha)$ enolično zapišemo v obliki

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

kjer so elementi $b_0, \ldots, b_{n-1} \in F$.

Dokaz: Naj bo $p(x) = m_{\alpha,F}$ takšen polinom, za katerega velja $F(\alpha) \equiv F[x]/\langle p(x)\rangle$. Ker je $\phi_\alpha(p(x)) = 0$ in $0 \neq \beta \in F(\alpha)$ poljuben, obstaja takšen $f(x) \in F[x]$, da je $\phi_\alpha(f(x)) = \beta$. Ker je $\beta \neq 0$ vemo, da $f(x) \notin \langle p(x)\rangle$. Zato algoritem deljenja vrne enoličen neničelen polinom $r(x)$ nižje stopnje od $p(x)$, da je $f(x) = h(x)p(x) + r(x)$ za nek $h(x) \in F[x]$. To pomeni, da je

$$\beta = \phi_\alpha(f(x)) = \phi_\alpha(h(x)p(x)) + \phi_\alpha(r(x)) = \phi_\alpha(r(x)).$$

Če zapišemo $r(x) = b_{n-1}x^{n-1} + \cdots + b_0$, imamo $\beta = \phi_\alpha(r(x)) = b_0 + \cdots + b_{n-1}\alpha^{n-1}$. Če bi obstajali takšni elementi $b'_0, \ldots, b'_{n-1} \in F$, da je $\beta = b'_0 + \ldots + b'_{n-1}\alpha^{n-1}$, potem bi dobili

$$\beta - \beta = 0 = (b_0 - b'_0) + \ldots + (b_{n-1} - b'_{n-1})\alpha^{n-1},$$

kar bi pomenilo, da je $g(x) = (b_0 - b'_0) + \ldots + (b_{n-1} - b'_{n-1})x^{n-1} \in \ker(\phi_\alpha)$. Ker je $p(x)$

polinom najnižje stopnje v $ker(\phi_\alpha)$ velja, da je $g(x) = 0$, tj. $b_i = b_i'$ za $i = 0, \ldots, n-1$.

♠

Naloge

1. Pokaži, da je dano število $\alpha \in \mathbb{C}$ algebraično nad $\mathbb{Q}$:

   (a) $\alpha = 1 + \sqrt{2}$

   (b) $\alpha = 1 + i$

   (c) $\alpha = \sqrt{1 + \sqrt[3]{2}}$

2. Naj bo E razširitev polja F in $\alpha \in E$ algebraičen nad F. Dokaži naslednje: če je polinom $f(x) \in F[x]$ nerazcepen in je $f(\alpha) = 0$, potem je $f = c \cdot m_{\alpha,F}$ za nek $c \in F$.

3. Poišči minimalen polinom elementa α nad poljem $\mathbb{Q}$ in mu določi stopnjo:

   (a) $\alpha = \sqrt{3 - \sqrt{6}}$

   (b) $\alpha = \sqrt{2} + \sqrt{3}$

4. Pokaži, da sta π^2 in $\pi + 2$ transcedentna nad $\mathbb{Q}$.

5. Določi ali je $\alpha \in \mathbb{C}$ algebraičen ali transcedenten nad F. Če je algebraičen mu določi stopnjo.

   (a) $\alpha = \sqrt{\pi},\ F = \mathbb{Q}$

   (b) $\alpha = \sqrt{\pi},\ F = \mathbb{R}$

   (c) $\alpha = \pi^2,\ F = \mathbb{Q}(\pi^3)$

6. Naj bo $\mathbb{Z}_2(\alpha)$ razširitev polja $\mathbb{Z}_2$, kjer je α ničla polinoma $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Dokaži, da je dan polinom nerazcepen nad $\mathbb{Z}_2$ in zapiši elemente polja $\mathbb{Z}_2(\alpha)$. Faktoriziraj dani polinom v $\mathbb{Z}_2(\alpha)[x]$.

7. Naj bo E razširitev polja F in $|F| = q$. Naj bo $\alpha \in E$, stopnje $\deg(\alpha, F) = n$, algebraičen nad F. Dokaži: $|F(\alpha)| = q^n$.

8. Dokaži, da je $f(x) = x^3 + 9x + 6$ nerazcepen nad $\mathbb{Q}$. Naj bo θ ničla polinoma f v neki razširitvi E polja $\mathbb{Q}$. Poišči $(1 + \theta)^{-1}$ v $\mathbb{Q}(\alpha)$.

Rešitve

1. Element α želimo "spremeniti" v element, ki vsebuje potence α in koeficiente v polju F (v našem primeru $\mathbb{Q}$).

   (a)

   $$\begin{aligned} \alpha &= 1+\sqrt{2} \\ \alpha - 1 &= \sqrt{2} \\ (\alpha-1)^2 &= 2 \\ \alpha^2 - 2\alpha - 1 &= 0 \end{aligned}$$

   Torej je α ničla polinoma $x^2-2x-1 \in \mathbb{Q}[x]$ in je algebraičen nad $\mathbb{Q}$ z $\deg(\alpha,\mathbb{Q}) = 2$.

   (b) Podobno kot v prejšnji nalogi lahko enostavno pokažemo, da je α ničla polinoma $x^2-2x+2 \in \mathbb{Q}[x]$ s stopnjo $\deg(\alpha,\mathbb{Q}) = 2$.

   (c) α je ničla polinoma $x^6-3x^4+3x^2-1 \in \mathbb{Q}[x]$ in $\deg(\alpha,\mathbb{Q}) = 6$.

2. Naj bo $m_{\alpha,F}$ minimalen polinom elementa α nad F. Potem je $m_{\alpha,F}(\alpha) = 0$. Ker je $f(\alpha) = 0$ velja, da je $\deg(f) \geq \deg(\alpha,F)$. Iz minimalnosti sledi dejstvo, da f vsebuje $m_{\alpha,F}$ kot faktor. Ker je f nerazcepen, je edina možnost $f = c \cdot m_{\alpha,F}$ za $c \in F$.

3. Podobno kot v prvi nalogi poišemo polinom v $\mathbb{Q}[x]$, ki ima α za ničlo. Potem moramo pokazati, da je ta polinom res minimalen polinom za α nad $\mathbb{Q}$.

   (a) α je ničla polinoma $x^4+6x^2+3 = f(x) \in \mathbb{Q}[x]$. Ker $3|3,6,\ 3 \nmid 1$ in $3^2 \nmid 3$, po Eisensteinevem kriteriju je polinom nerazcepen. Ker je f moničen, je $f = m_{\alpha,F}$ in je $\deg(\alpha,F) = 4$.

   (b) α je ničla polinoma $x^4-10x^2+1 = f(x) \in \mathbb{Q}[x]$. Bralcu prepuščamo, da dokaže da je polinom f res minimalen za elemnet α nad $\mathbb{Q}$.

4. Če predpostavimo, da je π^2 algebraičen nad $\mathbb{Q}$, potem obstaja takšen polinom $p(x)$ z racionalnimi koeficienti, da je $p(\pi^2) = 0$. Od tod sledi, da je $p(x^2) = q(x)$ prav tako polinom z racionalnim koeficienti in velja $p(\pi^2) = q(\pi) = 0$. To pomeni, da je π algebraičen nad $\mathbb{Q}$, kar ni res. Torej je π^2 transcedenten nad $\mathbb{Q}$. Bralcu prepuščamo, da preveri transcedentnost elementa $\pi+2$ nad $\mathbb{Q}$.

5. (a) Predpostavimo, da je $\sqrt{\pi}$ algebraičen nad $\mathbb{Q}$. Potem obstaja takšen $p(x) \in \mathbb{Q}[x]$, da je $\pi(\sqrt{\pi}) = 0$. V produktu $p(x)p(-x)$ se vsi členi z liho stonjo

pokrajšajo. Torej lahko obravnavamo produkt $p(x)p(-x)$, kot polinom z neznanko x^2. Trej, velja:

$$p(x)p(-x) = q(x^2) \to q(\pi) = q(\sqrt{pi}^2) = p(\sqrt{\pi})p(-\sqrt{\pi}) = 0,$$

kar pomeni da je π algebraičen nad $\mathbb{Q}$, kar nas privede do protislovja. Torej je $\sqrt{\pi}$ transcedenten nad $\mathbb{Q}$.

(b) $\sqrt{\pi} \in \mathbb{R}$ je algebraičen nad $\mathbb{R}$. Torej je ničla polinoma $x - \sqrt{\pi} \in \mathbb{R}[x]$ in posledično $\deg(\sqrt{\pi}, \mathbb{R}) = 1$.

(c) Polinom $x^3 - (\pi^3)^2$ je v $\mathbb{Q}(\pi^3)[x]$, z ničlo π^2. Torej je π^2 algebraičen nad $\mathbb{Q}(\pi^3)$ s stopnjo $\deg(\alpha, F) = 3$.

6. Polinom x^2+x+1 je nerazcepen nad $\mathbb{Z}_2$, saj je 2. stopnje in nima ničel v $\mathbb{Z}_2$. Torej je $x^2+x+1 = m_{\alpha,\mathbb{Z}_2}$ in $\deg(\alpha, \mathbb{Z}_2) = 2$. Iz izreka 2.13 sledi

$$\mathbb{Z}_2(\alpha) = \{0+0\alpha, 1+0\alpha, 0+1\alpha, 1+1\alpha\} = \{0, 1, \alpha, 1+\alpha\},$$

pri čemer sta množenje in seštevanje v $\mathbb{Z}_2(\alpha)$ definirana v spodnjih tabelah.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Ker je α ničla polinoma x^2+x+1, je $x^2+x+1 = (x-\alpha)\cdot f(x)$. Ko delimo dani polinom z linearnim fakotrjem, s pomočjo zgornjih tabel, dobimo, da je $g(x) = x+1+\alpha$. Torej je

$$x^2+x+1 = (x-\alpha)(x+\alpha+1) = (x+\alpha)(x+\alpha+1),$$

kjer je $-\alpha = \alpha \in \mathbb{Z}_2(\alpha)$.

7. Iz izreka 2.13 sledi, da lahko vsak element od $F(\alpha)$ enolično zapišemo kot $b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$, pri čemer so $b_0, \ldots, b_{n-1} \in F$. Ker ima F natnko q elementov, imamo q možnosti za b_0, q možnosti za b_1 in tako naprej. Torej imamo q^n možnosti za koeficiente $b_0, \ldots, b_{n-1}$. Zaradi enoličnosti reprezentacije lahko sklepamo, da ima $F(\alpha)$ natanko q^n elementov.

8. Očitno je $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Opazimo, da je

$$(\sqrt{2}+\sqrt{3})^{-1} = \frac{1}{\sqrt{2}+\sqrt{3}} \cdot \frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}} = \sqrt{3}-\sqrt{2},$$

kar pomeni, da je $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Ker je seštevanje zaprta operacija, je

$$(\sqrt{3}-\sqrt{2})+(\sqrt{3}+\sqrt{2}) = 2\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Po drugi strani vemo, da je $\frac{1}{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, kar pomeni, da je $\frac{1}{2} \cdot 2\sqrt{3} = \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Podobno pokažemo, da je $\sqrt{2} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$. Torej je $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Od tod sledi $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

9. Polinom $f(x)$ je nerazcepen nad $\mathbb{Q}$ po Eisensteinevem kriteriju za $p=3$. Ko delimo polinom $f(x)$ z $1+x$ dobimo

$$x^3+9x+6 = (1+x)(x^2-x+10)-4.$$

V primeru, ko je polje $\mathbb{Q}(\theta) \equiv \mathbb{Q}[x]/\langle f(x)\rangle$ (opazimo, da je $f = m_{\theta,\mathbb{Q}}$) dobimo:

$$\begin{aligned} 0 &= (1+\theta)(\theta^2-\theta+10)-4 \\ 4 &= (1+\theta)(\theta^2-\theta+10) \\ 1 &= \frac{1}{4}(1+\theta)(\theta^2-\theta+10) \\ (1+\theta)^{-1} &= \frac{1}{4}(\theta^2-\theta+10) \end{aligned}$$

2.4. Vektorski prostori

Definicija 2.11

Naj bo F polje. Vektorski prostor nad F (F-vektorski prostor) je sestavljen iz abelske grupe $(V,+)$ skupaj s skalarnim množenjem elementov iz V z elementi iz F, z leve strani, tako da za vsaka $a,b \in F$ in vsaka $\alpha,\beta \in V$ drži naslednje:

(V1) $a\alpha \in V$

(V2) $a(b\alpha) = (ab)\alpha$

(V3) $(a+b)\alpha = (a\alpha)+(b\alpha)$

(V4) $a(\alpha+\beta) = (a\alpha)+(a\beta)$

(V5) $1\alpha = \alpha$

Elementi v V se imenujejo vektorji, elementi v F skalari.

Zgled 2.4.1. Naj bo E razširitev polja F. Potem lahko na E gledamo kot F-vektorski prostor, pri čemer je seštevanje vektorjev definirano kot običajno seštevanje v E in

skalarni produkt $a\alpha$ običajno množenje nad poljem, elementa $a \in F$ z elementom $\alpha \in E$.

Definicija 2.12

F-vektorski prostor V je končnodimenzionalen, če obstaja končna podmnožica vektorjev v V, ki raztezajo prostor V.

Zgled 2.4.2. Če je $F \leq E$ in $\alpha \in E$ algebraičen nad F, potem je $F(\alpha)$ kočnodimenzionalen vektorski prostor nad F.

Definicija 2.13

Množica vektorjev $\{\alpha_i : i \in I\}$ je linearno neodvisna, če iz $\sum_{i \in I} a_i \alpha_i = 0$, sledi da so vsi $a_i = 0, i \in I$. V nasprotnem primeru pravimo, da je množica linearno odvisna.

Zgled 2.4.3. Če je E razširitev polja F in $\alpha \in E$ takšen algebraičen element nad F, da je $\deg(\alpha, F) = n$, potem lahko vsak element v $F(\alpha)$ enolično zapišemo kot linearno kombinacijo elementov v $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Torej je množica potenc elementa α linearno neodvisna.

Definicija 2.14

Baza vektorskega prostora je linearno neodvisna množica, ki razteza ta vektorski prostor. Če je V končno-dimenzionalen nad F, potem je dimenzija prostora V nad F enaka številu elementov v njegovi bazi.

Izrek 2.14

Naj bo $F \leq E$ in $\alpha \in E$ algebraičen nad F. Če je $\deg(\alpha, F) = n$, potem je $F(\alpha)$ vektorski prostor nad F dimenzije n z bazo $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Definicija 2.15

Za razširitev E polja F pravimo, da je algebraična razširitev, če je vsak element v E algebraičen nad F.

Definicija 2.16

Naj bo E razširitev polja F. Če je E končnodimenzionalen vektorski prostor nad F z dimenzijo n, potem je E končna razširitev dimenzije n polja F. Z $[E : F] = n$ označimo stopnjo n polja E nad F.

Komentar 2.7

To je le končna razširitev, ne trdimo, da so vpletena polja končna. Poleg tega moramo upoštevati, da je $[E : F] = 1$ natanko tedaj, ko je $E = F$.

Izrek 2.15

Vsaka končna razširitev je tudi algebraična.

Izrek 2.16

Če je E končna razširitev nad F in K končna razširitev nad E, potem je K kočna razšititev nad F in velja

$$[K : F] = [K : E] \cdot [E : F].$$

Naloge

1. Poišči bazo vektorskega prostora nad danim poljem:
   (a) $\mathbb{R}(\sqrt{2})$ nad $\mathbb{R}$
   (b) $\mathbb{C}$ nad $\mathbb{R}$
   (c) $\mathbb{Q}(\sqrt[4]{2})$ nad $\mathbb{Q}$
2. Izračunaj $[E : \mathbb{Q}]$ in poišči bazo vektorskega prostora E nad $\mathbb{Q}$, če je:
   (a) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
   (b) $E = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$
3. Pokaži, da je $x^2 - 3$ nerazcepen nad $\mathbb{Q}(\sqrt[3]{2})$.
4. Naj bo α algebraičen element lihe stopnje nad poljem F. Pokaži, da je $F(\alpha) = F(\alpha^2)$.
5. Dokaži, da sta $\mathbb{Q}(i)$ in $\mathbb{Q}(\sqrt{2})$ izomorfna kot vektorska prostora, ampak ne kot polja.
6. Če je E končna razširitev of F in $[E : F]$ praštevilo, potem je E enostavna razširitev od F in $E = F(\alpha)$, za vsak $\alpha \in E/F$.
7. Naj bo E končna razširitev polja F in polinom $p(x)$ nerazcepen nad F, stopnje $d \nmid [E : F]$. Dokaži, da $p(x)$ nima ničel v E.

Rešitve

1. (a) Ker je $\sqrt{2} \in \mathbb{R}$ in je ničla polinoma $x - \sqrt{2} \in \mathbb{R}[x]$ prve stopnje, je baza $\{1\}$.

   (b) Opazimo, da je $\mathbb{C} = \mathbb{R}(i)$. Velja, da je i ničla nerazcepnega polinoma $x^2 + 1 \in \mathbb{R}[x]$ druge stopnje. Torej je $\deg(i, \mathbb{R}) = 2$ in je $\{1, i\}$ baza $\mathbb{C}$ nad $\mathbb{R}$.

   (c) $\sqrt[4]{2}$ je koren nerazcepnega polinoma $x^4 - 2$ nad $\mathbb{Q}$ in je četrte stopnje. Torej je $\deg(\sqrt[4]{2}, \mathbb{Q}) = 4$ in je $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$ baza $\mathbb{Q}(\sqrt[4]{2})$ nad $\mathbb{Q}$.

2. (a) Opazimo, da je $E = K(\sqrt{3})$, pri čemer je $K = \mathbb{Q}(\sqrt{2})$. $\sqrt{2}$ je koren nerazcepnega polinoma $x^2 - 2$ nad $\mathbb{Q}$. Torej je $B = \{1, \sqrt{2}\}$ baza K nad $\mathbb{Q}$. To pomeni, da lahko vsak element $u \in K$ zapišemo kot $u = a + b\sqrt{2}$, za neka $a, b \in \mathbb{Q}$. Po drugi strani je $\sqrt{3}$ ničla od $irr(\sqrt{3}, K) = x^2 - 3$. Torej je $B' = \{1, \sqrt{3}\}$ je baza E nad K. To pomeni, da lahko vsak element $v \in E$ zapišemo kot $v = u_1 + u_2\sqrt{3}$ za neka $u_1, u_2 \in K$. Od tod sledi, da je

   $$v = a_1 + b_1\sqrt{2} + (a_2 + b_2\sqrt{2})\sqrt{3} = a_1 + b_1\sqrt{2} + a_2\sqrt{3} + b_2\sqrt{6}$$

   za neke $a_1, b_1, a_2, b_2 \in \mathbb{Q}$. Torej je v linearna kombinacija vektorjev

   $$U = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}.$$

   Iz $v = 0$ sledi, da je $a_1 = a_2 = b_1 = b_2 = 0$. Torej je U baza E nad $\mathbb{Q}$ in $[E : \mathbb{Q}] = 4$.

   (b) Potobno kot v prejšnjem primeru upoštevamo enostavne razdiritve E nad K in K nad $\mathbb{Q}$, pri čemer je $K = \mathbb{Q}(\sqrt[3]{5})$. Očitno je $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ baza K nad $\mathbb{Q}$ in $\{1, \sqrt{-2}\}$ baza E nad K. Torej je baza E nad $\mathbb{Q}$ produkt elementov predhodnih dveh baz. Torej, $\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{-2}, \sqrt[3]{5}\sqrt{-2}, \sqrt[3]{25}\sqrt{-2}\}$ in $[E : \mathbb{Q}] = 6$.

3. Če je $x^2 - 3$ razcepen nad $\mathbb{Q}(\sqrt[3]{2})$, ga lahko zapišemo kot produkt linearnih fakotrjev nad $\mathbb{Q}(\sqrt[3]{2})$. To pomeni, da $\sqrt{3}$ leži v $\mathbb{Q}(\sqrt[3]{2})$ in velja $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt[3]{2})$. Po drugi strani vemo, da je

   $$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \Rightarrow 2|3$$

   kar ni možno. Od tod sledi, da je $x^2 - 3$ nerazcepen nad $\mathbb{Q}(\sqrt[3]{2})$.

4. Ker je $\alpha^2 \in F(\alpha)$, je $F \leq F(\alpha^2) \leq F(\alpha)$. α je ničla polinoma $p(x) = x^2 - \alpha^2$ druge stopnje nad $F(\alpha^2)$. To pomeni, da je $[F(\alpha) : F(\alpha^2)] \leq 2$. Od tod sledi

   $$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)] \cdot [F(\alpha^2) : F(\alpha)]$$

in $[F(\alpha):F]$ je liho. To pomeni, da je $[F(\alpha):F(\alpha^2)]=1$, oziroma $F(\alpha)=F(\alpha^2)$.

5. Vemo, da je i ničla nerazcepnega polinoma x^2+1 nad $\mathbb{Q}$. To pomeni, da je $[\mathbb{Q}(i):\mathbb{Q}]=2$. Podobno je $\sqrt{2}$ ničla nerazcepnega polinoma x^2-2 nad $\mathbb{Q}$, kar pomeni, da je $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. Ker sta $\mathbb{Q}(i)$ in $\mathbb{Q}(\sqrt{2})$, kot vektorska prostora nad $\mathbb{Q}$, enake dimenzije, sta kot takšna izomorfna.

   Predpostavimo, da obstaja izomorfizem $f:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(i)$. To pomeni, da za neka $a,b\in\mathbb{Q}$ velja $f(\sqrt{2})=a+ib$. Vsak homomorfizem med polji nad $\mathbb{Q}$ fiksira elemente iz $\mathbb{Q}$, torej $f(q)=q$, za vse $q\in\mathbb{Q}$.

$$2=f(2)=f(\sqrt{2}\cdot\sqrt{2})=f(\sqrt{2})^2=a^2-b^2+2abi,$$

   kar pomeni, da je

$$a^2-b^2=2,\ 2ab=0.$$

   Edini rešitvi sta $(a,b^2)=(0,2)$ in $(a^2,b)=(2,0)$, kar ni mogoče, ker 2 ni kvadrat v $\mathbb{Q}$. Torej lahko zaključimo, da takšen izomorfizem ne more obstajati.

6. Iz $F\leq E$ in $\alpha\in E$ sledi, da je $F(\alpha)\leq E$. To pomeni, da je $[E:F]=[E:F(\alpha)]\cdot[F(\alpha):F]=p$. Ker $\alpha\notin F$, je $[F(\alpha):F]>1$. Torej je $[E:F(\alpha)]=1$, oziroma $E=F(\alpha)$.

7. Predpostavimo, da je $\alpha\in E$ ničla polinoma $p(x)$. Ker je $p(x)$ nerzacepen nad F, je $[F(\alpha):F]=\deg(p(x))=d$. Iz $[E:F]=[E:F(\alpha)]\cdot[F(\alpha):F]$ sledi, da je $[F(\alpha):F]=d|[E:F]$, kar je protislovje. Torej polinom $p(x)$ nima ničel v E.

Dodatne naloge

- Naj bo $f(x)$ nerazcepen v $K[x]$. Dokaži: če je F takšna razširitev polja K, da je $\gcd(\deg(f(x)),[F:K])=1$, potem je $f(x)$ nerazcepen nad K.
- Dokaži, da je $\mathbb{Q}(\sqrt{3},\sqrt[4]{3},\sqrt[8]{3},\ldots)$ algebraična razširitev od $\mathbb{Q}$, ampak ne končna.
- Dokaži ali ovrži: π je algebraičen nad $\mathbb{Q}(\pi^3)$.
- Dokaži, da sta polji $\mathbb{Q}(\sqrt[4]{3})$ in $\mathbb{Q}(\sqrt[4]{3}i)$ izomorfni, ampak nista enaki.

KONČNA POLJA

Definicija 3.1

Polje F, ki ima končno število elementov, se imenuje končno polje. Številu elementov v končnemu polju pravimo red polja in ga označujemo z $|F|$.

Končno polje F ima praštevilsko karakteristiko $char(F) = p$ in p^n elementov, $n \in \mathbb{N}$. Po navadi ga označimo z $GF(p^n)$ ali $\mathbb{F}_{p^n}$.

Nekaj lastnosti konlnih polj:

(i) Grupa neničelnih elementov F^* končnega polja F z operacijo množenja je ciklična.

(ii) Če je F končno polje, potem za poljuben $n \in \mathbb{N}$ obstaja nerazcepen polinom v $F[x]$ stopnje n.

(iii) Poljubni končni polji, ki imata enako število elementov, sta izomorfni.

(iv) Za vsako praštevilo p in poljuben $n \in \mathbb{N}$ obstaja polje, ki ima p^n elementov.

Izrek 3.1

Naj bo E končno polje s p^n elementov v $\overline{\mathbb{Z}_p}$, algebraičnem zaprtju polja $\mathbb{Z}_p$. Elementi polja E so ničle polinoma $x^{p^n} - x \in \mathbb{Z}_p[x]$ v $\mathbb{Z}_p$.

Definicija 3.2

Elementu α končnega polja pravimo primitivni n-ti koren identitete, če velja:

$$\alpha^n = 1 \quad \wedge \quad \alpha^m \neq 1 \ (0 < m < n).$$

Lema 3.1

Naj bo z primitivni n-ti koren identitete. t je red elementa z^k, $k \in \mathbb{N}$, natanko tedaj, ko je $t = \frac{n}{\gcd(n,k)}$.

Dokaz: Predpostavimo, da je t red elementa z^k, za nek $k \in \mathbb{N}$. To pomeni, da je t najmanjše takšno število, da velja $1 = (z^k)^t = z^{kt}$. Z drugimi besedam; kt je najmanjši

večkratnik od k, ki je tudi večkratnik od n, tj.

$$kt = lcm(k,n) = \frac{kn}{\gcd(k,n)}).$$

Torej je $t = \frac{n}{\gcd(k,n)}$.

♠

Naloge

1. Poišči število primitivnih 8-ih korenov identitete v $GF(9)$.
2. Poišči število primitivnih 10-ih korenov identitete v $GF(23)$.
3. Naj bo $\overline{\mathbb{Z}_2}$ algebraično zaprtje polja $\mathbb{Z}_2$, $\alpha \in \overline{\mathbb{Z}_2}$ ničla polinoma $p(x) = x^3 + x^2 + 1$ in $\beta \in \overline{\mathbb{Z}_2}$ ničla polinoma $q(x) = x^3 + x + 1$. Dokaži, da je $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2(\beta)$.
4. Dokaži, da končno polje s p^n elementi premore natančno eno podpolje s p^m elementi za vsak $m|n$.
5. Naj bo F končno polje karakteristike p. Naj bo $f : F \to F$ funkcija podana s predpisom $f(\alpha) = \alpha^p$. Dokaži, da je f automorfizem.
6. Naj bo F končno polje. Pokaži, da je vsak element v F vsota dveh kvadratov iz F.

Rešitve

1. Ker je z primitivni n-ti koren v $GF(m)$ je z tudi generator grupe $(GF(m)^*, \cdot)$. Vsi elementi v $GF(n)^*$ so oblike z^k za nek $k \in \mathbb{N}$. Predpostavimo, da je z^k generator grupe $GF(m)^*$. To pomeni da je reda n. Po prejšnji lemi je potem $n = \frac{n}{\gcd(k,n)}$, kar pomeni, da je $\gcd(k,n) = 1$. Torej je število primitivnih n-tih korenov identitete enako številu elementov, ki so tuja z n, tj. $\varphi(n)$. V našem primeru je $n = 8$ in $m = 9$. Ker 8 deli $|GF(9)^*|$, zaključimo, da takšen primitiven koren res obstaja. Število primitivnih 8-ih korenov identitete je potem $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$.
2. Ker 10 ne deli $|GF(23)^*| = 22$ sledi, da ne obstaja element reda 10 v $GF(23)$. Kar pomeni, da $GF(23)$ nima primitivnih 10-ih korenov identitete.
3. Polinoma p in q sta nerazcepna nad $\mathbb{Z}_2$ (saj sta stopnje 3 in nimata ničel v $\mathbb{Z}_2$), kar pomeni da sta $\mathbb{Z}_2(\alpha)$ in $\mathbb{Z}_2(\beta)$ stopnje razširitve 3 in kot takšna sta podpolja v $\overline{\mathbb{Z}_2}$ z 2^3 elementi. Po prejšnjem izreku sledi, da je $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2(\beta) = \{\omega \in \overline{\mathbb{Z}_2} : \omega^8 - \omega = 0\}$.

4. Naj bo $m \in \mathbb{N}$ poljuben delitelj števila n in naj bo $S_m(F) = \{\omega \in F : \omega^{p^m} = \omega\}$. Ni težko pokazati, da je $S_m(F)$ podpolje polja F ($|F| = p^n$). Vemo, da je $S_m(F)$ sestavljen iz ničel polinoma $x^{p^m} - x \in F[x]$. To pomeni, da je $|S_m(F)| \leq p^m$ oziroma $|S_m(F)^*| \leq p^m - 1$. Opazimo, da je $S_m(F)^*$ sestavljen iz ničel polinoma $x^{p^m-1} - 1 = 0$.

   Ker m deli n je $n = md$ za nek $d \in \mathbb{N}$. Torej

   $$p^n - 1 = p^{md} - 1 = (p^m - 1)(p^{d(m-1)} + \ldots + p^{2m} + p^m + 1)$$

   in posledično velja, da mora $p^m - 1$ deliti $p^n - 1$. Ker je F^* ciklična grupa reda $p^n - 1$ lahko sklepamo, da F^* vsebuje ciklično podgrupo reda $p^m - 1$. Bolj natančno, F^* vsebuje podgrupo, ki je sestavljena iz takšnih elementov α za katere je $\alpha^{p^m-1} = 1$. To pomeni, da ima $S_m(F)^*$ natanko $p^m - 1$ elementov, oziroma da ima $S_m(F)$ natanko p^m elementov in je torej podpolje reda p^m. Enoličnost sledi iz enoličnosti ciklične podgrupe ali iz lastnosti (iii) iz uvodnega dela poglavja.

5. Če je $char(F) = p$, potem je $(a+b)^p = a^p + b^p$ za vsaka $a, b \in F$. Velja tudi:

   $$\begin{aligned} f(1) &= 1 \\ f(a+b) &= (a+b)^p = a^p + b^p = f(a) + f(b) \\ f(ab) &= (ab)^p = a^p b^p = f(a)f(b) \end{aligned}$$

   Torej je f homomorfizem. Iz ejstva, da je $|F| < \infty$ sledi, da je f surjekcija. Ker je $\ker(f)$ ideal v F in je F polje, je $\ker(f) = \{0\}$ in posledično je f injekcija. Torej je f automorfizem.

6. Če je $char(F) = 2$ je $\phi : F \to F$ s predpisom $\phi(\alpha) = \alpha^2$ automorfizem (5. naloga). Torej za vsak $\alpha \in F$ velja $\phi(\alpha) = \alpha^2 = \alpha^2 + 0^2$. Naj bo $char(F) = p > 2$. Definirajmo $\phi : F^* \to F^*$ s $\phi(\alpha) = \alpha^2$. Iz $\phi(\alpha) = \phi(\beta)$ sledi, da je $\alpha^2 = \beta^2$. Torej je $\alpha = \beta$ ali $\alpha = -\beta$. Ker je $\beta \neq 0$ in $char(F) > 2$ sledi, da je $\beta \neq -\beta$. To pomeni, da je ϕ preslikava 2-na-1 in posledično obstaja $|F^*|/2 = (|F| - 1)/2$ kvadratov v F^*. Ni se težko prepričati, da je tudi 0 kvadrat. Torej imamo $(|F| - 1)/2 + 1 = (|F| + 1)/2$ kvadratov v F.

   Označimo z $A = \{a^2 : a \in F\}$ in $B_x = \{x - b^2 : b \in F\}$, kjer je x poljuben, ampak fiksen, element iz F. Če je $A \cap B = \emptyset$, je $|A \cup B| = |A| + |B| = |F| + 1 > |F|$, kar ni možno. Torej velja $A \cap B \neq \emptyset$. To pomeni, da obstajata takšna $\alpha, \beta \in F$, da je $\alpha^2 = x - \beta^2$, oziroma $x = \alpha^2 + \beta^2$. Ker je bil x poljuben element, trditev drži za celotno polje F.

Dodatne naloge

1. Dokaži, da vsak nerazcepen polinom v $\mathbb{Z}_p[x]$ deli $x^{p^n} - x$ za nek $n \in \mathbb{N}$.

DODATEK - VPRAŠANJA IZ TEORIJE

1. Podaj definicijo kolobarja.
2. Če je R kolobar, potem dokaži, da za poljubna $a,b \in R$ velja $0a = a0 = 0$, $a(-b) = (-a)b = -(ab)$ in $(-a)(-b) = ab$.
3. Definiraj homomorfizem kolobarjev. Kaj sta jedro in slika homomorfizma kolobarjev? Kaj lahko rečemo o povezavi med homomorfizmi kolobarjev in grup?
4. Definiraj avtomorfizem, epimorfizem, monomorfizem in izomorfizem.
5. Podaj definicijo obsega, celega kolobarja in polja.
6. Podaj definicijo podkolobarja. Zapiši Izrek o testiranju podkolobarjev.
7. Kaj so idempotentni in nilpotentni elementi v kolobarju?
8. Podaj definicijo deliteljev niča v kolobarju.
9. Kaj so delitelji niča v $\mathbb{Z}_n$? Dokaži.
10. Dokaži, da zakona krajšanja veljata v kolobarju R natanko tedaj, ko R nima deliteljev niča.
11. Ali je vsako polje cel kolobar? Dokaži svojo trditev ali podaj protiprimer.
12. Ali je vsak cel kolobar polje? Dokaži svojo trditev ali podaj protiprimer.
13. Podaj definicijo karakteristike kolobarja.
14. Napiši Fermatov mali izrek.
15. Definiraj Eulerjevo funkcijo.
16. Napiši Eulerjev izrek.
17. Kako definiramo elemente v polju ulomkov celega kolobarja?
18. Kako definiramo seštevanje in množenje v $R[x]$?
19. Definiraj evaluacijski homomorfizem. Kako definiramo ničle polinoma?

20. Napiši in dokaži Faktorski izrek.
21. Dokaži, da ima neničelni polinom stopnje n nad poljem F največ n ničel v F.
22. Podaj definicijo nerazcepnega polinoma.
23. Napiši in dokaži izrek, ki govori o razcepnosti polinomov stopnje 2 ali 3 nad poljem F.
24. Napiši Eisensteinov kriterij.
25. Podaj definicijo asociranih elementov, nerazcepnih elementov ter praelementov v celem kolobarju.
26. Kdaj rečemo, da je cel kolobar Gaussov?
27. V celem kolobarju je element nerazcepen natanko tedaj, ko je praelement. Dokaži ali podaj protiprimer.
28. Definiraj pojem ideala.
29. Napiši (precizno) definicijo kvocentnega kolobarja R po idealu N.
30. Napiši osnovni izrek homomorfizmov.
31. Naj bo R kolobar z enoto in N ideal v R, ki vsebuje enoto. Dokaži, da je potem $N = R$.
32. Podaj definicijo maksimalnega ideala.
33. Podaj definicijo praideala.
34. Kaj so ideali v $\mathbb{Z}$ in $\mathbb{Z}_n$? Utemelji svoj odgovor.
35. Podaj definicijo glavnega ideala.
36. Podaj definicijo glavnega kolobarja.
37. Napiši prvi izrek izomorfizmov.
38. Napiši drugi izrek izomorfizmov.
39. Napiši tretji izrek izomorfizmov.
40. Podaj definicijo razširitve polja.
41. Napiši Kronecker-jev izrek.
42. Podaj definicijo algebraičnega in transcedentnega elementa nad poljem F.

43. Podaj definicijo minimalnega polinoma za nek algebraični element α nad poljem F.

44. Podaj definicijo enostavne razširitve. Navedi izrek, ki poda natančen opis elementov v enostavni razširitvi.

45. Podaj definicijo algebraične razširitve.

46. Pokaži, da je vsaka končna razširitev algebraična razširitev. Navedi izreke, uporabljene v dokazu.

47. Navedi izrek o stolpu za razširitve polj.

48. Podaj definicijo algebraičnega zaprtja. Kdaj pravimo, da je polje algebraično zaprto?

49. Navedi osnovni izrek algebre.

50. Podaj definicijo primitivnega n-tega korena enote.

51. Utemelji, zakaj je končna razširitev E končnega polja F enostavna razširitev.

LITERATURA

1. A. Clark. Elements of abstract algebra. Dover Publications, New York, 1984.

2. J.B. Fraleigh. A first course in abstract algebra. Addison-Wesley, Reading, 1999.

3. S. Lang. Algebra. Addison-Wesley, Reading, 1965.

4. S. Lang. Undergraduate algebra. Springer-Verlag, 1990.

5. Z. Stojaković in Đ. Paunić. Zbirka zadataka iz algebre : grupe, prsteni, polja. Građevinska knjiga, Beograd, 1988.

6. I. Vidav. Algebra. DMFA, Ljubljana, 1972.