DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Polinomu algebra

2.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis - vispārināt dalāmības, pirmskaitļu, LKD, MKD, Eiklīda algoritma jēdzienus patvaļīgu gredzenu un polinomu gredzenu gadījumā.

Lekcijas kopsavilkums:

- polinomu gredzenos virs lauka var izmantot Eiklīda algoritmu;
- polinomu gredzeniem ir spēkā aritmētikas pamatteorēmas analogs;

- LKD un MKD analogi eksistē, ja gredzenam ir spēkā vienozīmīgās faktorizācijas īpašība, polinomu gredzeniem tas ir spēkā.

Svarīgākie jēdzieni: asociācijas attiecība, LKD un MKD patvaļīgos gredzenos, nedalāms elements, pirmelements, galīgas faktorizācijas gredzens (GFG), Eiklīda gredzens, Eiklīda algoritms, vienozīmīgās faktorizācijas gredzens (VFG),

Svarīgākie fakti un metodes: asociācijas attiecība ir ekvivalence, dalāmības īpašības, nedalāmo elementu īpašības, GFG piemēri, secinājumi no Eiklīda algoritma, Eiklīda gredzens ir VFG, LKD un MKD aprēķināšana VFG.

1. Dalāmība patvaļīgos gredzenos

1.1. Invertējamie elementi un asociācija

Šajā lekcijā visi gredzeni ir unitāri IG.

Saka, ka $b \in R$ dala $a \in R$ $(b|a)$, ja $\exists\ q \in R$: $a = bq$.

Ja $b|a$ un $a|b$, tad a un b sauc par *asociētiem elementiem*, apzīmē ar $a \sim b$ ($\sim$ ir binära attiecība kopā R).

1.1. piemērs. $\mathbb{Z}$ - $\pm a$. $k[X]$ - uf, kur $u \in k$, $u \neq 0$.

1.1. teorēma.

1. $\sim$ ir ekvivalences attiecība (refleksīva, simetriska, tranzitīva).
2. $a \sim b \iff \exists u \in \mathcal{U}(R) : a = ub$.

PIERĀDĪJUMS

1. Refleksivitāte $a = 1 \cdot a$.

Simetrija Seko no definīcijas.

Tranzitivitāte

$$\left\{\begin{array}{l} a\sim b \\ b\sim c \end{array}\right. \iff \left\{\begin{array}{l} \left\{\begin{array}{l} a|b \\ b|a \end{array}\right. \\ \left\{\begin{array}{l} b|c \\ c|b \end{array}\right. \end{array}\right. \iff \left\{\begin{array}{l} \left\{\begin{array}{l} a|b \\ b|a \end{array}\right. \\ \left\{\begin{array}{l} b|c \\ c|b \end{array}\right. \end{array}\right.$$

$$\Longrightarrow \quad a\sim c.$$

2. $a\sim b \Longrightarrow a=cb=c\underbrace{(c'a)}_{=b}=(cc')a \Longrightarrow$

$$cc'=1 \Longrightarrow c,c'\in\mathcal{U}(R).$$

$$a=ub \Longrightarrow \left\{\begin{array}{l} b|a \\ b=u^{-1}a \end{array}\right. \Longrightarrow \left\{\begin{array}{l} b|a \\ a|b \end{array}\right. \Longrightarrow a\sim b. \ \blacksquare$$

1.1. piezīme. Tā kā $\sim$ ir ekvivalence, ir definētas atbilstošās ekvivalences klases.

1.2. piemērs. $R[X]$, ekvivalences klases $\{uf|$ kur $u \in \mathcal{U}(R)\}$.

1.2. Dalāmības īpašības

1.2. teorēma. R - IG, unitārs.

1. $a|b_1,\ a|b_2,\ ...,\ a|b_n \implies a|(b_1 + ... + b_n)$.
2. $\left\{ \begin{array}{l} a|b \\ b|c \end{array} \right. \implies a|c.$
3. $a|b \implies \forall c \in R:\ a|bc.$
4. $\left\{ \begin{array}{l} a|b \\ c|d \end{array} \right. \implies ac|bd.$
5. $u \in \mathcal{U}(R) \iff u|1.$

PIERĀDĪJUMS

1.-4.Pierādām līdzīgi veselo skaitļu gredzena gadījumam.

5. $u \in \mathcal{U}(R) \iff \exists\, u' \in R:\ uu' = 1 \iff u|1.$ ■

1.3. LKD un MKD

1.3.1. Dalītāji

$a \in R$ sauc par $\{b_1, ..., b_m\} \subseteq R$ *kopīgu dalītāju*, ja $\forall\ i : \quad a|b_i$. $\{b_1, ..., b_n\}$ dalītāju kopu apzīmē ar $D(b_1, ..., b_n)$.

Par kopas $\{b_1, ..., b_m\}$ *lielāko kopīgo dalītāju (LKD)* sauksim to kopīgo dalītāju, kurš dalās ar jebkuru šīs kopas kopīgo dalītāju. Citiem vārdiem sakot, $d \in D(b_1, ..., b_n)$ ir LKD, ja

$$d' \in D(b_1, ..., b_n) \implies d'|d.$$

1.2. piezīme. LKD ir noteikts ar precizitāti līdz asociācijai:
$d = LKD(a, b) \implies ud = LKD(a, b)$, kur $u \in \mathcal{U}(R)$.

Var izmainīt LKD definīciju tā, lai tas būtu viennozīmīgi noteikts. Piemēram, polinomu gredzenu gadījumā var pieprasīt, lai vecākais koeficients būtu vienāds ar 1.

1.3. piemērs. $\mathbb{Z}[X]$, $LKD(2X+2, X^2-1) \sim X+1$.

1.3. teorēma. R - IG.

1. $\forall\, b \in R:\ LKD(b,0) \sim b.$
2. $\forall\, a,b \in R:\ a|b \implies D(a,b) = D(a)$ un $LKD(a,b) \sim a.$
3. $\forall\, a,b,k \in R:$

$$D(a,b) = D(a-kb,b) \text{ un } LKD(a,b) \sim LKD(a-kb,b).$$

PIERĀDĪJUMS Tāds pats kā $\mathbb{Z}$ gadījumā. ■

1.3.2. Daudzkārtņi

$c \in R$ sauc par $\{b_1, ..., b_m\} \subseteq R$ *kopīgu daudzkārtni*, ja $\forall\, i$ izpildās $b_i|c$. $b_1, ..., b_n$ daudzkārtņu kopu apzīmē ar $M(b_1, ..., b_n)$.

Par kopas $\{b_1, ..., b_m\}$ *mazāko kopīgo daudzkārtni (MKD)* sauc to kopīgo daudzkārtni, kurš dala jebkuru šīs kopas kopīgo daudzkārtni. Citiem vārdiem sakot, c ir mazākais kopīgais daudzkārtnis, ja

$$c' \in M(b_1, ..., b_n) \implies c|c'.$$

1.3. piezīme. MKD ir noteikts ar precizitāti līdz asociācijai:
$c = MKD(a,b) \iff uc = MKD(a,b)$, kur $u \in \mathcal{U}(R)$.

1.4. piemērs. $\mathbb{Z}[X]$, $MKD(2X+2, X^2-1) \sim 2(X^2-1)$.

1.4. Nedalāmie elementi un pirmelementi

1.4.1. Pamatfakti

$p \in R$, $p \neq 0$, sauc par *nedalāmu*, ja

$$\begin{cases} p \notin \mathcal{U}(R) \\ p = ab \implies a \in \mathcal{U}(R) \ \vee \ b \in \mathcal{U}(R). \end{cases}$$

R nedalāmo elemenu kopu apzīmē ar $\mathcal{I}(R)$.

$R[X]$ nedalāmos elementus sauc par *nedalāmiem polinomiem*.

$p \in R$ sauc par *pirmelementu*, ja

$$p|ab \implies p|a \vee p|b.$$

R pirmelementu kopu apzīmē ar $\mathcal{P}(R)$.

1.5. piemērs. Laukā nav nedalāmu elementu.

$\mathbb{Z}$ nedalāmie elementi ir $\pm$ pirmskaitļi.

Lineāri polinomi (ar pakāpi 1) virs lauka ir nedalāmi, tas seko no īpašības $\deg(fg) = \deg(f) + \deg(g)$.

1.4. teorēma. R- IG.

1. $p \in \mathcal{P}(R) \implies p \in \mathcal{I}(R)$ (kopu terminos - $\mathcal{P}(R) \subseteq \mathcal{I}(R)$).
2. $\left\{ \begin{array}{l} p \in \mathcal{I}(R) \\ u \in \mathcal{U}(R) \end{array} \right. \implies up \in \mathcal{I}(R).$
3. $\left\{ \begin{array}{l} a, b \in \mathcal{I}(R) \\ a|b \end{array} \right. \implies a \sim b.$

PIERĀDĪJUMS

1. $p \notin \mathcal{I}(R) \implies p = ab$, kur $a, b \notin \mathcal{U}(R)$. Pierādīsim, ka $p \nmid a$ un $p \nmid b$.

$p|a \implies a = qp = qab = a(qb) \implies qb = 1 \implies b \in \mathcal{U}(R)$ - pretruna. Līdzīgi, ja $p|b$.

2. $up \notin \mathcal{I}(R) \implies up = p_1p_2 \implies p = (u^{-1}p_1)p_2 \implies p \notin \mathcal{I}(R)$.

3. $a|b \implies b = qa$. $q \notin \mathcal{U}(R) \implies b \notin \mathcal{I}(R) =$ pretruna. ■

1.4.2. Galīgas faktorizācijas gredzeni

IG R sauc par *galīgas faktorizācijas gredzenu (GFG, atomisku gredzenu)*, ja $\forall\ r \in R\backslash\mathcal{U}(R)$, $r \neq 0$, ir izsakāms galīga nedalāmu elementu reizinājuma veidā:

$$\exists\ \{x_1, ..., x_n\} \subseteq \mathcal{I}(R) :\ r = x_1...x_n.$$

1.5. teorēma.

1. $\mathbb{Z}$ ir GFG.
2. R - IG $\implies$ $R[X]$ ir GFG.

PIERĀDĪJUMS

1. Seko no aritmētikas pamatteorēmas.

2. Izmantosim matemātisko indukciju pēc polinoma pakāpes.

Indukcijas bāze Ja $\deg(f) \in \{0, 1\}$, tad apgalvojums ir acīmredzams, jo lineārie polinomi ir nedalāmi.

Indukcijas solis Pieņemsim, ka apgalvojums ir patiess $\forall\, f \in R[X]$: $\deg(f) < n$ un pierādīsim, ka tad apgalvojums ir patiess, ja $\deg(f) = n$.

$f \in \mathcal{I}(R[X]) \implies$ nekas nav jāierāda.

$f \notin \mathcal{I}(R[X]) \implies f = f_1 f_2$, kur $\deg f_i < n \implies$

f_i izsakās galīga nedalāmu elementu reizinājuma veidā saskaņā ar indukcijas pieņēmumu:

$$\begin{cases} f_1 = p_1 \ldots p_m \\ f_2 = q_1 \ldots q_l \end{cases} \implies f = f_1 f_2 = p_1 \ldots p_m q_1 \ldots q_l \implies$$

f izsakās galīga reizinājuma veidā. ■

1.6. piemērs. $\mathbb{Q}[X]$, $X^2 - 1 = (X-1)(X+1)$.

2. Eiklīda algoritms patvaļīgos gredzenos

2.1. Norma un Eiklīda gredzeni

IG R sauksim par *Eiklīda gredzenu*, ja eksistē *normas funkcija*

$$\mathbf{N} : R\backslash\{0\} \to \mathbb{N} \cup \{0\},$$

kas apmierina šādus nosacījumus:

- $\forall\ a, b \in R,\ b \neq 0,\ \exists\ q, r \in R$:
  - $a = qb + r$,
  - $\mathbf{N}(r) < \mathbf{N}(b)$ vai $r = 0$;
- $\mathbf{N}(ab) \geq \mathbf{N}(a)$ visiem $\{a, b\} \subseteq R\backslash\{0\}$.

2.1. piemērs. $R = \mathbb{Z}$, $\mathbf{N}(a) = |a|$ - teorēma par veselo skaitļu dalīšanu ar atlikumu.

$R = k[X]$, k - lauks, $\mathbf{N}(a) = \deg(a)$ - pakāpes īpašība, teorēma par polinomu dalīšanu ar atlikumu.

$\mathbb{Z}[X]$ nav Eiklīda gredzens.

R ir lauks, $\mathbf{N}(a) = 1$, $\forall\ a \neq 0$.

2.1. teorēma. R - Eiklīda gredzens.

1. $\forall\ a, b \in R\backslash\{0\}:\ a \sim b \implies \mathbf{N}(a) = \mathbf{N}(b)$.
2. $\forall\ a \in R\backslash\{0\}, \forall\ b \in R\backslash(\mathcal{U}(R) \cup \{0\}):\ \mathbf{N}(ab) > \mathbf{N}(a)$.
3. R - GFG.

PIERĀDĪJUMS

1. $a \sim b \implies \begin{cases} a = ub, \text{ kur } u \in \mathcal{U}(R) \\ b = u^{-1}a \end{cases} \implies$

$$\begin{cases} \mathbf{N}(a) = \mathbf{N}(ub) \geq \mathbf{N}(b) \\ \mathbf{N}(b) = \mathbf{N}(u^{-1}a) \geq \mathbf{N}(a) \end{cases} \implies \mathbf{N}(a) = \mathbf{N}(b)$$

2. Izdalīsim a ar ab:

$$a = q(ab) + r, \text{ kur } \mathbf{N}(ab) > \mathbf{N}(r) \ \vee \ r = 0.$$

$r = 0 \implies a = a(qb) \implies 1 = qb \implies b \in \mathcal{U}(R)$ - pretruna.

$\mathbf{N}(ab) > \mathbf{N}(r) \implies \mathbf{N}(ab) > \mathbf{N}(a - qab) =$
$\mathbf{N}(a(1 - qb)) \geq \mathbf{N}(a) \implies \mathbf{N}(ab) > \mathbf{N}(a).$

3. $a = b_1 ... b_k$, kur $\forall\ b_i \notin \mathcal{U}(R) \implies$

$$\mathbf{N}(a) = \mathbf{N}(b_1 ... b_k) > \mathbf{N}(b_1 ... b_{k-1}) > ... > \mathbf{N}(b_1)$$

Esam ieguvuši dilstošu nenegatīvu skaitļu virkni, kuras garums nepārsniedz $\mathbf{N}(a)$.

Elementam a apskatīsim sadalījumu ar garāko iespējamo šādu dilstošo virkni. Tas ir sadalījums ar nedalāmiem elementiem, jo pretējā gadījumā virkni varētu padarīt garāku. ■

2.2. Eiklīda algoritms Eiklīda gredzenos

R ir Eiklīda gredzens ar normas funkciju $\mathbf{N}$.

2.2.1. Algoritms

Rīkojamies tāpat kā $\mathbb{Z}$ gadījumā, veicam pēctecīgu dalīšanu ar atlikumu gredzenā $R[X]$.

Iegūsim dalīšanas atlikumu virkni $r_1, r_2, ..., r_{n-1}, 0$ ar īpašību

$$\mathbf{N}(r_1) > \mathbf{N}(r_2) > ... > \mathbf{N}(r_{n-1}).$$

Virkne $\mathbf{N}(r)$, kad r mainās algoritma izpildes gaitā, ir stingri dilstoša virkne, tāpēc šī algoritma realizācijā soļu skaits ir galīgs.

2.2. piemērs. $R = \mathbb{Q}[X]$. $a = X^3 - 5X + 2$, $b = X^2 - X - 2$.

1. $a = (X + 1)b + (-2X + 4)$,
2. $b = (-\frac{1}{2}X - \frac{1}{2})(-2X + 4) + 0$.

$R = \mathbb{F}_2[X]$. $a = X^4 + X^2 + 1$, $b = X^2 + 1$.

1. $a = (X^2 + 1)b + X$,
2. $b = X \cdot X + 1$,
3. $X = X \cdot 1 + 0$.

2.2.2. Eiklīda algoritma saistība ar LKD

2.2. teorēma. R - Eiklīda gredzens. Pieņemsim, ka tiek realizēts Eiklīda algoritms ar sākuma datiem (a, b), $b \nmid a$, tiek veikti n soļi, pēdējais nenulles atlikums ir r_{n-1}.

1. $D(a, b) = D(r_{n-1})$.
2. $LKD(a, b) \sim r_{n-1}$.

PIERĀDĪJUMS Tāds, pats kā $\mathbb{Z}$ gadījumā. ■

2.3. piemērs. $R = \mathbb{Q}[X]$. $a = X^3 - 5X + 2$, $b = X^2 - X - 2$.
Redzam, ka $LKD(a, b) \sim -2X + 4 \sim X - 2$.

$R = \mathbb{F}_2[X]$. $a = X^4 + X^2 + 1$, $b = X^2 + 1$.
Redzam, ka $LKD(a, b) \sim 1$.

2.2.3. Secinājumi no Eiklīda algoritma

2.3. teorēma. R - Eiklīda gredzens.

1. $\forall\, \{a, b\} \subseteq R \;\exists\; LKD(a, b)$.
2. $\forall\, \{a, b\} \subseteq R \;\exists\; \{x, y\} \subseteq R : LKD(a, b) = xa + yb$.
   ($LKD(a, b)$ ir a un b *R-lineāra kombinācija*)
3. $\left\{ \begin{array}{l} a|bc \\ LKD(a, b) = 1 \end{array} \right. \implies a|c$.
4. Katrs nedalāms R elements ir pirmelements:
$$p \in \mathcal{I}(R) \implies \Big(p|ab \implies p|a \text{ vai } p|b\Big).$$
5. $\forall\, \{a, b\} \subseteq R \;\exists\; MKD(a, b) : \; MKD(a, b) \sim \frac{ab}{LKD(a,b)}$.

PIERĀDĪJUMS

1. Seko no Eiklīda algoritma.

2. Pierādījums līdzīgs $\mathbb{Z}$ gadījumam: jāapskata visas Eiklīda algoritma dalīšanas un jāizsaka LKD kā sākotnējo elementu lineāra kombinācija.

3. $\left\{ \begin{array}{l} bc = qa \\ 1 = xa + yb \end{array} \right. \Longrightarrow c = cxa + cyb =$
$= acv + y\underbrace{bc}_{qa} = a(cx + yq) \Longrightarrow a|c.$

4. Pieņemsim, ka $ab \neq 0$. Definēsim $d = LKD(a, p)$.
$d|p \Longrightarrow d|1$ vai $d \sim p$.

$d|1 \Longrightarrow d = xa + yp \Longrightarrow$

$1 = d^{-1}d = d^{-1}(xa + yp) = x'a + y'p \Longrightarrow LKD(p, a) = 1.$

Saskaņā ar iepriekš pierādītu apgalvojumu $p|b$.

$d \sim p \Longrightarrow d = up \Longrightarrow up|a \Longrightarrow p|a.$

5. Pierādījums līdzīgs $\mathbb{Z}$ gadījumam. ■

2.4. piemērs. $R = \mathbb{Q}[X]$. $a = X^3 - 5X + 2$, $b = X^2 - X - 2$.

1. $a = (X+1)b + (-2X+4)$,
2. $b = (-\frac{1}{2}X - \frac{1}{2})(-2X+4) + 0$.

$LKD(a,b) = -2X+4$, $-2X+4 = 1 \cdot a - (X+1)b$.

3. Factorizācija patvaļīgos gredzenos

3.1. Pamatfakti

IG R ir *viennozīmīgas faktorizācijas gredzens (VFG, faktoriāls gredzens)*, ja $\forall\, a \in R\backslash\{0\}$ ir izsakāms formā

$$a = \underbrace{u}_{\in \mathcal{U}(R)} \underbrace{p_1 p_2 ... p_k}_{p_i \in \mathcal{I}(R)}, \text{ kur}$$

šāds sadalījums ir noteikts viennozīmīgi ar precizitāti līdz elementu kārtībai un aizvietošanai ar asociētiem elementiem, citiem vārdiem sakot, ja

$$a = up_1p_2...p_k = u'p'_1p'_2...p'_m,$$

tad $k = m$ un pēc elementu p'_i pārkārtošanas $\forall\ i\ \exists\ u_i \in \mathcal{U}(R)$ tāds, ka $p_i = u_ip'_i$.

3.1. piemērs. Jebkurš lauks ir VFG. $\mathbb{Z}$ ir VFG.

3.2. piemērs. Gredzenā $\mathbb{Z}[\sqrt{-5}]$ elements 9 ir izsakāms reizinājumā divos dažādos veidos

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

Var pierādīt, ka 3 ir nedalāms, bet nav pirmelements.

3.2. Eiklīda gredzenu viennozīmīgās faktorizācijas īpašība

3.1. teorēma. R - Eiklīda gredzens $\Longrightarrow$ R - VFG.

PIERĀDĪJUMS R ir Eiklīda gredzens $\Longrightarrow$ R ir GFG. Jāpierāda, ka faktorizācija ir viennozīmīga ar precizitāti līdz invertējamiem reizinātājiem un kārtībai.

Pieņemsim, ka $r \in R$ var izteikt kā nedalāmu elementu reizinājumu divos veidos:

$$r = p_1 p_2 ... p_n = p'_1 p'_2 ... p'_l.$$

$p_n | r \Longrightarrow p_n$ dala vismaz vienu no nedalāmajiem elementiem $p'_1, ..., p'_l$, pieņemsim, ka $p_n | p'_l$.

$$\Longrightarrow p'_l = u_n p_n, \text{ kur } u_n \in \mathcal{U}(R), \text{ jo } p'_l \in \mathcal{I}(R) \Longrightarrow$$

$$p_1 p_2 ... p_{n-1} p_n = u_n p'_1 p'_2 ... p'_{l-1} p_n.$$

Izmantojot IG saīsināšanas īpašību, saīsinām ar p_n abas puses:

$$p_1 p_2 ... p_{n-1} = u_n p'_1 p'_2 ... p'_{l-1}.$$

Turpinām saīsināt reizinātājus šādā veidā. Var secināt, ka

- abās pusēs reizinātāji beigsies vienlaicīgi, jo pretējā gadījumā vienā pusē būtu neinvertējams elements, bet otrā invertējams $\Longrightarrow$ $n = l$
- $\forall\ p'_i\ \exists\ p_j :\ p'_i = u_j p_j$.■

3.1. piezīme. Seko, ka $k[X]$ ir VFG, ja k ir lauks.

3.2. piezīme. Svarīgs fakts (pagaidām bez pierādījuma) - R - VFG $\Longrightarrow$ $R[X]$ - VFG. Piemēram, $\mathbb{Z}[X]$ ir VFG.

3.3. LKD un MKD viennozīmīgās faktorizācijas gredzenos

R - VFG. Fiksēsim kopu $\mathcal{P}_0 \subseteq \mathcal{P}(R)$ tādu, ka katrs R pirmelements ir asociēts ar kādu kopas $\mathcal{P}_0$ elementu (*pirmelementu asociācijas klašu pārstāvju kopu*).

3.3. piemērs. $R = \mathbb{Z} \Longrightarrow \mathcal{P}_0$ var būt (pozitīvo) pirmskaitļu kopu.

3.2. teorēma. R - VFG, $a, b \in R$, $\begin{cases} a = up_1^{\alpha_1}...p_k^{\alpha_k} \\ b = vp_1^{\beta_1}...p_k^{\beta_k}, \text{ kur } p_i \in \mathcal{P}_0. \end{cases}$

Tad

$$\begin{cases} LKD(a,b) \sim p_1^{\delta_1}...p_k^{\delta_k}, \text{ kur } \delta_i = \min(\alpha_i, \beta_i) \\ MKD(a,b) \sim p_1^{\lambda_1}...p_k^{\lambda_k}, \text{ kur } \lambda_i = \max(\alpha_i, \beta_i). \end{cases}$$

PIERĀDĪJUMS Pierāda līdzīgi veselo skaitļu gadījumam.■

3.4. piemērs. $LKD(X^2-1, X^3-1) \sim X-1$,
$MKD(X^2-1, X^3-1) \sim (X^2-1)(X^2+X+1)$.

4. 2.mājasdarbs

4.1. Obligātie uzdevumi

2.1 Pierādīt, ka gredzenā $k[X]$, kur k ir lauks, polinomi ar pakāpi 0 dala visus polinomus.

2.2 Pierādīt, ka bezgalīgā gredzenā neinvertējamu (nenulles) elementu kopa ir bezgalīga.

2.3 Atrast $LKD(f,g)$ un izteikt to lineāras kombinācijas veidā, atrast $MKD(f,g)$.

(a) $f = X^3 - X^2 - 3X + 3$, $g = X^2 - 1$, virs $\mathbb{Q}[X]$,
(b) $f = X^4 + X^2 + 1$, $g = X^3 + 1$, virs $\mathbb{F}_2[X]$,
(c) $f = X^3 + X + 1$, $g = X^3 + 2$, virs $\mathbb{F}_3[X]$.

4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.4 Atrast IG, kas nav GFG.

2.5 Pierādīt, ka $\mathbb{Z}[X]$ nav Eiklīda gredzens.

2.6 Vai $k[[X]]$, kur k ir lauks, ir Eiklīda gredzens?

2.7 Visiem naturāliem n un m polinomiem $f(X) = X^n$ un $g(X) = (1-X)^m$ virs $\mathbb{Q}[X]$ atrast tādus polinomus a un b, lai izpildītos vienādība $a(X)f(X) + b(X)g(X) = 1$.