

LINEARNA ALGEBRA 2020/21

12. VAJE: 23. 12. 2020

1. Pokaži, da je grupa $\mathbb{Z}_2 \times \mathbb{Z}_3$ izomorfna $\mathbb{Z}_6$. Pokaži, da $\mathbb{Z}_9$ ni izomorfna $\mathbb{Z}_3 \times \mathbb{Z}_3$.
2. Naj bo G grupa, v kateri velja $g^2 = 1$ za vsak $g \in G$. Pokaži, da je G abelova.
3. Naj bo $(R, +, \cdot)$ (asociativen) kolobar pokaži, da je $r0 = 0r = 0$ za vsak $r \in R$.
Dokaži: če je $1 = 0$, potem je $R = \{0\}$.
Pokaži, da je $-(rs) = (-r)s = r(-s)$.
4. Naj bosta R_1 in R_2 kolobarja. Potem je $R_1 \times R_2$ kolobar za operaciji po komponentah. Določi obrnljive elemente $R_1 \times R_2$. Pokaži, da za obsega D_1, D_2 kolobar $D_1 \times D_2$ ni obseg.
5. (Razširjen Evklidov algoritem)

Data: Neničelni celi števili a, b . (Ali neničelna polinoma.)

Result: d, x, y , kjer je $d = \gcd(a, b)$ in $xa + yb = d$.

$(r_0, x_0, y_0) = (a, 1, 0);$

$(r_1, x_1, y_1) = (b, 0, 1);$

while $r_{i+1} \neq 0$ **do**

$k_i = r_{i-1} // r_i;$ ▷ celoštevilsko deljenje (polinomsko deljenje)
 $(r_{i+1}, x_{i+1}, y_{i+1}) = (r_{i-1}, x_{i-1}, y_{i-1}) - k_i(r_i, x_i, y_i);$

end

return (r_i, x_i, y_i)

Pokaži, da algoritem deluje pravilno.

a.) Pokaži, da je $\gcd(r_j, r_{j+1}) = \gcd(r_{j+1}, r_{j+2}) = \gcd(r_{i-1}, r_i) = r_i$

b.) Pokaži, da je $x_i a + y_i b = r_i$ za vsak i .

6. Pokaži, da je celoštevilska enačba $ax + by = c$ rešljiva natanko tedaj, ko je c večkratnik $\gcd(a, b)$.
7. Reši celoštevilsko enačbo $4333x + 623y = 21$
8. Poišči (multiplikativni) inverz 7 v $\mathbb{Z}_{13}$ in reši enačbi $66x = 84$ in $66y = 14$ v $\mathbb{Z}_{105}$.
9. Izračunaj največja skupna delitelja polinomov

$$x^4 + 1, x^3 - 2x + 2$$

in

$$x^6 - 3x^5 - 15x^4 + 87x^3 - 162x^2 + 132x - 40, x^4 - 4x^3 + 3x^2 + 4x - 4$$

1. Pokaži, da je grupa $\mathbb{Z}_2 \times \mathbb{Z}_3$ izomorfna $\mathbb{Z}_6$. Pokaži, da $\mathbb{Z}_9$ ni izomorna $\mathbb{Z}_3 \times \mathbb{Z}_3$.

homomorfizem

$$f: G_1 \rightarrow G_2$$

$$f(gh) = f(g) \cdot f(h) \text{ - homomorfizem}$$

+ bijektivnost

$$f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \begin{pmatrix} 0,1 \\ 0,1,2 \end{pmatrix}$$

homomorfizem je possem določen z $f(1)$

$$f(n) = n \cdot f(1) = \underbrace{f(1) + \dots + f(1)}_{n\text{-krat}}$$

$$f(1) = (1, 2)$$

$$f(2) = (0, 4) = (0, 1)$$

$$f(3) = (1, 0)$$

$$f(4) = (0, 2)$$

$$f(5) = (1, 1)$$

$$f(0) = (0, 0)$$

Delovalo bi tudi

$$f(1) = (1, 1)$$

V splošnem velja

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{n \cdot m}$$

$(\Leftrightarrow)$

$$\gcd(n, m) = 1$$

$\mathbb{Z}_9$ ni izomorfna $\mathbb{Z}_3 \times \mathbb{Z}_3$

Priznamo da izomorfizem obstaja.

$$|\mathbb{Z}_9| = |\mathbb{Z}_3 \times \mathbb{Z}_3|$$

$\parallel$
9

$\parallel$
9

$$f: \mathbb{Z}_9 \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$f \text{ injektivna} \Leftrightarrow (f(n) = 0 \Rightarrow n = 0)$$

$$f(1) \neq 0 \quad f(3) = 3 \cdot f(1) = (3a, 3b) = (0, 0) \text{ ampak } 3 \neq 0.$$

f ni injektivna! ~~ne~~

2. Naj bo G grupa, v kateri velja $\underline{g^2 = 1}$ za vsak $g \in G$. Pokaži, da je G abelova.

$$\underline{g_1 \cdot g_2 = g_2 \cdot g_1} \quad \forall g_1, g_2 \in G$$

$\forall \mathbb{R} \setminus \{0\}$ ne velja $x^2 = 1 \quad \forall x \in \mathbb{R} \setminus \{0\}$.

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = I \quad - GL_2(\mathbb{R})$

$\mathbb{Z}_2 \quad \forall g \in \mathbb{Z}_2 \quad 2 \cdot g = 0$

$$(g_1 \cdot g_2)(g_1 \cdot g_2) = 1 \quad \Rightarrow \quad g_1 \cdot g_2 \cdot g_1 \cdot g_2 = 1 \quad / \cdot g_2 \text{ iz desne}$$

$$g_1 \cdot g_1 = 1$$

$$g_2 \cdot g_2 = 1$$

$$g_1 g_2 g_1 \underline{g_2 g_1} = g_2 \quad / \cdot g_1 \text{ iz leve}$$

$$\underline{g_1 \cdot g_1} g_2 g_1 = g_1 g_2$$

$$\underline{g_2 \cdot g_1 = g_1 \cdot g_2} \quad \checkmark$$

• Kolobarji (Rings) Vsi kolobarji so asociativni

$$(R, +, \cdot)$$

• $(R, +)$ abelova grupa Enoto ^{povzadi} označujemo z 0

• $(R, \cdot)$ polgrupa (potencialno enoto (povzadi) označimo z 1.

• Kolobar je komutativen, če je množenje komutativno

- (levo in desna) distributivnost
 $r(s+t) = rs+rt \quad \forall r,s,t \in R$
 $(r+s)t = rt+st$

Primeri:

$$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot) \dots (\mathbb{H}, +, \cdot)$$

$$(\mathbb{Z}_n, +, \cdot), (M_n(\mathbb{R}), +, \cdot).$$

3. Naj bo $(R, +, \cdot)$ (asociativen) kolobar pokaži, da je $r0 = 0r = 0$ za vsak $r \in R$.

Dokaži: če je $1 = 0$, potem je $R = \{0\}$.

Pokaži, da je $-(rs) = (-r)s = r(-s)$.

- $r0 = 0r = 0 \quad \forall r \in R$

$$r0 = 0 \quad 0+0=0$$

$$r0 = r(0+0) = \underline{r0 + r0} \quad / - r0 \text{ (abelova grupa za seštevanje)}$$

$$0 = r \cdot 0$$

analogno $0 \cdot r = 0$

- (Aksiomi za $\mathbb{R}$ PG $1 \neq 0$)

če je $1=0$, potem $R = \{0\}$

$$\underline{r=0}$$

$$\underline{0} = r0 = r \cdot 1 = r \rightarrow 0 = r$$

- $r, -r$ - inverz za seštevanje

$$-(ab) = (-a) \cdot b = a(-b) \quad \text{Pozorati moramo}$$

$$\underline{ab} + \underline{(-a) \cdot b} = 0$$

$$ab + (-a)b = (a-a) \cdot b = 0 \cdot b = 0$$

$$ab + a(-b) = a(b-b) = a \cdot 0 = 0$$

4. Naj bosta R_1 in R_2 kolobarja. Potem je $R_1 \times R_2$ kolobar za operaciji po komponentah. Določi obrnljive elemente $R_1 \times R_2$. Pokaži, da za obsega D_1, D_2 kolobar $D_1 \times D_2$ ni obseg.

obseg $(D, +, \cdot)$ je kolobar, kjer je vsak nenulčni element obrnljiv.

$\forall d \in D \setminus \{0\} \exists d^{-1} \in D$ $\xrightarrow{\text{multiplikativni inverz}}$

$(D \setminus \{0\}, \cdot)$ je grupa

- komutativen obseg imenujemo polje

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ $\xrightarrow{\text{Galoisova polja}}$ $\mathbb{GF}(p^n)$ $\left| \begin{array}{l} \mathbb{H} - \text{kvaternioni} \\ \searrow \text{obseg, ki ni komutativen} \end{array} \right.$
 $\downarrow$ p -primitivno

$D_1 \times D_2$ ni obseg

kaj so obrnljivi elementi v $D_1 \times D_2$? $(1, 1)$ - lasta za množenje

$$(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

(r_1, r_2) - obrnljiv $\Leftrightarrow r_1$ in r_2 obrnljiva

$$(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

$$\parallel \parallel$$

$$(s_1, s_2)(r_1, r_2) = (s_1 r_1, s_2 r_2)$$

$$\parallel \parallel$$

$$(1, 1) = (1, 1)$$

$$r_1 s_1 = s_1 r_1 = 1 \quad \bullet \quad s_1 = r_1^{-1}$$

$$r_2 s_2 = s_2 r_2 = 1 \quad \bullet \quad s_2 = r_2^{-1}$$

$$r_1 \neq 0, r_2 \neq 0 \quad (0, r_2) \cdot (r_1, 0) = (0r_1, r_2 \cdot 0) = (0, 0) \quad \text{delitelji nič}$$

- koloburju brez deliteljev nič ne moremo cel kolobar.

$D_1 \times D_2$ ima elemente $\neq (0, 0)$, ki niso obratljivi

$(d_1, 0)$ $d_1 \neq 0$ niso obratljivi $\Rightarrow D_1 \times D_2$ ni obseg

- $r \in (R, +, \cdot)$ r - delitelj nič $\Rightarrow$ r ni obratljiv

$s \neq 0$ $r \cdot s = 0$ • recimo, da je r obratljiv (r^{-1})

Poten dobimo $r^{-1} \cdot r \cdot s = r^{-1} \cdot 0 = 0$

$$\parallel \\ 1 \cdot s = s = 0 \quad \text{---}$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = 0 \\ (M_2(\mathbb{R}), +, \cdot)$$

$\mathbb{Z}_{p_1 p_2}$ RSA - kriptirni algoritem

$$n \in \mathbb{Z}_{p_1 p_2} \quad n \text{ tu}^o p_1 p_2 \\ \downarrow \\ \text{tu}^o p_1 p_2 \quad \frac{(p_1-1)(p_2-1)}{n} = 1 \quad \text{--- Mali Fermatov izrek}$$

$$\frac{(p_1-1)(p_2-1)+1}{n} = n$$

$$\frac{n}{n} \text{ --- } n\text{-sporočilo} \\ m = n^{(p_1-1)} \text{ --- kodirano sporočilo}$$

$$m^{(p_1-1)+1} = n \\ \text{--- desifriranje}$$

5. (Razširjen Evklidov algoritem) Deljivo nad $\mathbb{Z}$ in polinomi $F[x]$

Data: Neničelni celi števili a, b . (Ali neničelna polinoma.)

Result: d, x, y , kjer je $d = \gcd(a, b)$ in $xa + yb = d$.

$(r_0, x_0, y_0) = (a, 1, 0);$

$(r_1, x_1, y_1) = (b, 0, 1);$

while $r_{i+1} \neq 0$ **do**

$k_i = r_{i-1} // r_i;$

 ▷ celoštevilsko deljenje (polinomsko deljenje)

$(r_{i+1}, x_{i+1}, y_{i+1}) = (r_{i-1}, x_{i-1}, y_{i-1}) - k_i(r_i, x_i, y_i);$

end

return (r_i, x_i, y_i)

Evklidske danene so
kolobarji, kjer imamo algoritme
deljenja.

$$\begin{array}{lcl}
 (4333, 1, 0) & & 4333 // 623 = 6 \\
 (623, 0, 1) & \hookleftarrow & 623 \cdot 6 = 3738 \\
 (595, 1, -6) & \hookleftarrow & 4333 - 3738 = 595 \\
 (28, -1, 7) & \hookleftarrow & 623 // 595 = 1 \\
 & & 595 // 28 = 21 \\
 & & 595 - 21 \cdot 28 = 7 \\
 7 = \gcd(4333, 623) & \swarrow & (7, 22, -153) \\
 & & \hline
 & & (0, 1, -) \\
 & \swarrow & 22 \cdot 4333 + (-153) \cdot 623 = 7 \quad / \cdot 3
 \end{array}$$

$$66 \cdot 4333 - 459 \cdot 623 = 21 \quad - \text{Rešitev ni evklidska}$$

8. Poišči (multiplikativni) inverz 7 v $\mathbb{Z}_{13}$ in reši enačbi $66x = 84$ in $66y = 14$ v $\mathbb{Z}_{105}$.

Računamo v $\mathbb{Z}$

$$x \cdot 7 + y \cdot 13 = 1 \quad \begin{array}{l} n \in \mathbb{Z}_m \\ \text{ostatek} \Leftrightarrow n \bmod m \\ \gcd(7, m) = 1 \end{array}$$

$$\overline{x \cdot 7} = \overline{1} \in \mathbb{Z}_{13}$$

„ $\overline{x \cdot 7}$ - ostatek pri deljenju s 13“

$$\begin{array}{rcl}
 \begin{array}{c} 7, 1, 0 \\ \hline (13, 0, 1) \end{array} & 7 // 13 = 0 & \\
 (7, 1, 0) & 13 // 7 = 1 & \\
 (6, -1, 1) & 7 // 1 & \\
 \begin{array}{c} (1, 2, -1) \\ \hline (0, *, *) \end{array} & \begin{array}{l} 2 \cdot 7 - 13 = 1 \\ 2 \text{ invers } 7 \text{ v } \mathbb{Z}_{13} \end{array} &
 \end{array}$$

$$\begin{array}{l}
 66x = 84 \\
 66y = 14
 \end{array}
 \quad \vee \quad \mathbb{Z}_{105}$$

$$\begin{array}{rcl}
 66x + 105a = 84 \\
 \hline
 66y + 105b = 14 \\
 \hline
 \end{array}$$

$$\begin{array}{l}
 \bullet (105, 1, 0) \\
 \bullet (66, 0, 1) \\
 (39, 1, -1) \\
 (27, -1, 2) \\
 (12, 2, -3) \quad 27 // 12 = 2 \\
 (3, -5, 8) \quad 8 \cdot 66 + 5 \cdot 105 = 3 \quad \checkmark
 \end{array}$$

$$8 \cdot 66 - 5 \cdot 105 = 3 \quad \cdot / 28 \quad 84/3 = 28$$

$$\underline{224 \cdot 66 - 140 \cdot 105 = 84}$$

$$\begin{array}{l}
 224 \cdot 66 = 84 \quad \vee \quad \mathbb{Z}_{105} \Rightarrow 14 \cdot 66 = 84 \\
 224 - 2 \cdot 105 = 14 \quad \vee \quad \mathbb{Z}_{105}
 \end{array}$$

$$66y + 105b = 14 \quad 3+14$$

$$66y = 14 \text{ nima rešitev v } \mathbb{Z}_{105}$$

Tudi zelo enostavne enačbe imajo lahko več rešitev npr.:

$$4 \cdot x = 0 \quad \mathbb{Z}_8$$

$$x=0, x=2, x=4, x=6$$

9. Izračunaj največja skupna delitelja polinomov

$$x^4 + 1, x^3 - 2x + 2$$

in

$$x^6 - 3x^5 - 15x^4 + 87x^3 - 162x^2 + 132x - 40, x^4 - 4x^3 + 3x^2 + 4x - 4$$

obseg

$F[x]$

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

$F[x]/(p) \rightarrow$ ostanki pri deljenju s p | če je p -necelcepu, potem je $F[x]/(p)$ -obseg

$$\left| \mathbb{R}[x]/_{x^2+1} \cong \mathbb{C} \right|$$

(Analogija z $\mathbb{Z}_p$,
necelcupna števila so praštevila)

$$\left(\underline{x^4+1}, 1, 0 \right)$$

$$\left(\underline{x^3-2x+2}, 0, 1 \right)$$

$$\left(2x^2-2x+1, 1, -x \right)$$

$$\left(-\frac{3}{2}(x+1), -, - \right) \circ$$

$$\left(1, -, - \right)$$

$$\left(0, 0, 0 \right)$$

$$\gcd() = 1$$

$$x^4+1 \parallel x^3-2x+2 = x$$

$$-x^4+2x^2-2x$$

$$2x^2-2x+1$$

$$x^3-2x+2 \parallel 2x^2-2x+1 = \underline{\underline{\frac{1}{2}x + \frac{1}{2}}}$$

$$-x^3+x^2-\frac{1}{2}x$$

$$x^2-\frac{5}{2}x+2$$

$$-x^2+x-\frac{1}{2}$$

$$-\frac{3}{2}x+\frac{3}{2}$$

$$-\frac{3}{2}(x+1)$$

$$\begin{array}{r} 2x^2 - 2x + 1 \\ - 2x^2 + 2x \\ \hline 1 \end{array} \quad // \quad \left(-\frac{3}{2}\right)(x+1) = -\frac{4}{3}x$$

$$\mathbb{Q}[x] / (x^4 + 1) \quad \hookrightarrow \quad x^3 - 2x + 2 \text{ ist invertierbar}$$

$$\gcd(x^4 + 1, x^3 - 2x + 2) = 1$$

Dodatno

5. (Razširjen Evklidov algoritem)

Data: Neničelni celi števili a, b . (Ali neničelna polinoma.)

Result: d, x, y , kjer je $d = \gcd(a, b)$ in $xa + yb = d$.

$(r_0, x_0, y_0) = (a, 1, 0);$

$(r_1, x_1, y_1) = (b, 0, 1);$

while $r_{i+1} \neq 0$ **do**

$k_i = r_{i-1} // r_{i+1};$ $\triangleright$ celoštevilsko deljenje (polinomsko deljenje)

$(r_{i+1}, x_{i+1}, y_{i+1}) = (r_{i-1}, x_{i-1}, y_{i-1}) - k_i(r_i, x_i, y_i);$

end

return (r_i, x_i, y_i)

Pokaži, da algoritem deluje pravilno.

a.) Pokaži, da je $\gcd(r_j, r_{j+1}) = \gcd(r_{j+1}, r_{j+2}) = \gcd(r_{i-1}, r_i) = r_i$

b.) Pokaži, da je $x_i a + y_i b = r_i$ za vsak i .

6. Pokaži, da je celoštevilska enačba $ax + by = c$ rešljiva natanko tedaj, ko je c večkratnik $\gcd(a, b)$.

a) Naj bo $n = \gcd(r_j, r_{j+1})$ in $m = \gcd(r_{j+1}, r_{j+2})$

Pokazali bomo, da $n \mid r_{j+2}$ in $m \mid r_j$, potem bo $n \mid m$ in $m \mid n$
in $m = n$.

• $r_j = a \cdot n$ $r_{j+1} = b \cdot n$, a, b tuji

$$r_{j+2} = r_j - k_{j+1} r_{j+1} = (a - k_{j+1} b) n \Rightarrow n \mid r_{j+2}$$

• $r_{j+1} = c \cdot m$, $r_{j+2} = d \cdot m$

$$r_j = r_{j+2} + k_{j+1} r_{j+1} = (c + k_{j+1} d) m \quad m \mid r_j$$

b) Indukcija

$$\begin{aligned} x_0 \cdot a + y_0 \cdot b &= 1a + 0b = a \\ x_1 \cdot a + y_1 \cdot b &= 0 \cdot a + 1b = b \end{aligned} \quad \left. \vphantom{\begin{aligned} x_0 \cdot a + y_0 \cdot b &= 1a + 0b = a \\ x_1 \cdot a + y_1 \cdot b &= 0 \cdot a + 1b = b \end{aligned}} \right\} \text{ baza}$$

$$x_{i-1} \cdot a + y_{i-1} \cdot b = r_{i-1}$$

$$x_i \cdot a + y_i \cdot b = r_i$$

$$x_{i+1} \cdot a + y_{i+1} \cdot b = (x_{i-1} - k_i x_i) a + (y_{i-1} - k_i y_i) b$$

$$= (x_{i-1} \cdot a + y_{i-1} \cdot b) - k_i (x_i \cdot a + y_i \cdot b) = r_{i-1} - k_i r_i = r_{i+1}$$

(6.) $ax + by = c$

Naj bo $c = n \cdot \gcd(a, b)$. $\rightarrow$ z algoritmom dobimo rešitev $ax' + by' = \gcd(a, b)$
potem $x = n \cdot x'$ $y = n \cdot y'$ rešita našo enačbo.

Naj bo $ax + by = c$, potem je leva stran deljiva z $\gcd(a, b) \Rightarrow$ torej je tudi desna $\gcd(a, b) \mid c$.