

21. LINEÁRNE REKURENTNÉ POSTUPNOSTI NAD TELESAMI

Z predchádzajúcej kapitoly vyplýva, že ak máme teleso F , potom v F môžeme uskutočňovať operácie sčítania, násobenia, odčítania a delenia, podobne ako v množine racionálnych, reálnych alebo komplexných čísel. Podobne tam môžeme rozvinúť aj analogickú teóriu o lineárnych rekurentných postupnostiach.

Nech $\{x_n\}$ je postupnosť prvkov z F . Potom ju budeme nazývať *lineárne rekurentná postupnosť*, ak existujú také prvky $A, B \in F$, že pre $n = 0, 1, 2, \dots$ platí

$$x_{n+2} = Ax_{n+1} + Bx_n. \quad (28)$$

Úloha 468.

- a) Ak $\{x_n\}, \{y_n\}$ sú také postupnosti, ktoré spĺňajú vzťah (28), potom pre $a, b \in F$ aj postupnosť $\{ax_n + by_n\}$ spĺňa vzťah (28).
 b) Ak $x_0 = y_0$ a $x_1 = y_1$, potom $x_n = y_n$ pre $n = 0, 1, 2, \dots$.
 Dokážte.

Budeme sa snažiť nájsť explicitný vzorec pre n -tý člen lineárnej rekurentnej postupnosti. Na to však budeme potrebovať vedieť vyriešiť kvadratickú rovnicu podobne, ako sme to robili aj v predchádzajúcom prípade.

Úloha 469. Nech $\lambda \in F$ je riešením rovnice

$$(\lambda - \lambda_1)(\lambda - \lambda_2) = 0.$$

Potom $\lambda = \lambda_1 \vee \lambda = \lambda_2$. Dokážte.

Úloha 470. Dokážte, že v telese platí vzorec

$$(a + b)(a - b) = a^2 - b^2.$$

Ak n je prirodzené číslo a $a \in F$, potom symbolom na budeme označovať prvok $a + \dots + a$ ($n \times$ sčítame prvok a). Je to aditívna analógia definície mocniny. Nazýva sa aj *vonkajší súčin* alebo *vonkajšie násobenie*.

Úloha 471. Dokážte, že pre všetky $m, n \in \mathbb{N}$, $a, b \in F$ platí

$$\begin{aligned} n(ab) &= (na)b = a(nb), \\ (m + n)a &= ma + na, \\ m(a + b) &= ma + mb. \end{aligned}$$

Teraz opäť urobíme isté zjednodušenie. Pre prirodzené číslo n budeme symbolom n označovať aj súčet n jednotiek telesa F .

Úloha 472. Dokážte, že v telese $\mathbb{Z}_p$, kde p je prvočíslo, platí $p \cdot 1 = 0$.

Úloha 473. Dokážte, že v telese $\mathbb{Z}_p$, kde p je prvočíslo, platí $n \cdot 1 = 0$ práve vtedy, ak $p|n$.

Úloha 474. Dokážte, že v telese $\mathbb{Z}_p$, kde p je prvočíslo, platí pre všetky $m, n \in \mathbb{N}$, že $m \cdot 1 = n \cdot 1$ práve vtedy, ak $m \equiv n \pmod{p}$.

Namiesto $m \cdot 1$ môžeme skrátene písať iba m . Ako vidíme z predchádzajúcich troch úloh, v tomto prípade sa kongruencie menia na rovnosti.

Úloha 475. Dokážte, že v ľubovoľnom telese platí

$$(a+b)^2 = a^2 + 2ab + b^2,$$

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

Ak $a, b \in F$, potom symbolom $\frac{a}{b}$ budeme označovať súčin $a \frac{1}{b}$.

Úloha 476. Nech v telese F platí, že $2 \neq 0$. Potom pre $a, b \in F$ platí, že

$$\lambda^2 + a\lambda + b = \left(\lambda + \frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2 + b.$$

Dokážte.

(Návod: Použite úlohu 475 a.)

Úloha 477. Ak $a, b \in F$ a $2 \neq 0$ a ak existuje taký prvok $c \in F$, že $c^2 = \left(\frac{a}{2}\right)^2 - b$, potom rovnica

$$\lambda^2 + a\lambda + b = 0$$

má korene $\lambda_1 = -\frac{a}{2} + c$, $\lambda_2 = -\frac{a}{2} - c$. Dokážte. (Hodnotu $\left(\frac{a}{2}\right)^2 - b$ nazývame diskriminant.)

(Návod: Použite úlohy 476, 470 a 469.)

Teraz budeme postupovať podobným spôsobom ako sme postupovali pri lineárnych rekurentných postupnostiach celých čísel.

Úloha 478. Ak postupnosť prvkov telesa F v tvare $\{aq^n\}$ spĺňa vzťah (28), kde $a, q \neq 0$, potom q je koreňom rovnice

$$\lambda^2 - A\lambda - B = 0. \tag{29}$$

Dokážte.

Úloha 479. Ak q_1, q_2 sú dva rôzne prvky telesa F , potom pre každé $x_0, x_1 \in F$ vždy existujú také prvky $a, b \in F$, že

$$\begin{aligned} a + b &= x_0, \\ aq_1 + bq_2 &= x_1. \end{aligned}$$

Dokážte.

Úloha 480. Ak rovnica (29) má dva rôzne korene q_1, q_2 a postupnosť $\{x_n\}$ spĺňa vzťah (28), potom existujú také prvky $a, b \in F$, že

$$x_n = aq_1^n + bq_2^n$$

pre $n = 0, 1, \dots$. Dokážte.

Úloha 481. Nech $\{x_n\}$ je taká postupnosť celých čísel, v ktorej $x_0 = 2, x_1 = 5$ a $x_{n+2} = 5x_{n+1} + x_n \pmod{7}$. Dokážte, že n -tý člen tejto postupnosti je zvyšok po delení čísla $2^n + 3^n$ číslom 7.

Úloha 482. Nech $\{x_n\}$ je postupnosť z úlohy 481. Dokážte, že $x_n = x_{n+6}$ pre všetky $n = 0, 1, 2, \dots$

(Návod: Použite úlohu 481 a malú Fermatovu vetu.)

Teraz sa budeme zaoberať lineárnymi rekurentnými postupnosťami modulo 7.

Úloha 483. Nech $x_{n+2} = Ax_{n+1} + Bx_n \pmod{7}$ a číslo $A^2 + 4B$ je kvadratický zvyšok modulo 7. Potom $x_n = x_{n+6}$ pre všetky $n = 0, 1, 2, \dots$

Vidíme, že problém dokážeme vyriešiť, ak je diskriminant príslušnej kvadratickej rovnice kvadratickým zvyškom modulo 7. Ale čo ak nie je? Všimnime si podobnosť s prípadom nezáporného a záporného diskriminantu kvadratickej rovnice s reálnymi koeficientami.

Uvažujme takú postupnosť prirodzených čísel $\{x_n\}$, v ktorej

$$x_0 = 2, x_1 = 1 \tag{30}$$

a

$$x_{n+2} = x_{n+1} + x_n \pmod{7}. \tag{31}$$

Úloha 484. Dokážte, že kvadratická rovnica $\lambda^2 + 6\lambda + 6 = 0$ nemá riešenie v $\mathbb{Z}_7$.

Teraz pridajme k $\mathbb{Z}_7$ taký prvok ϑ , pre ktorý $\vartheta^2 = 5$!

Úloha 485. Dokážte, že $4(1 + \vartheta)$ a $4(1 - \vartheta)$ sú koreňmi rovnice $\lambda^2 + 6\lambda + 6 = 0$.

Úloha 486. Nech $\{x_n\}$ je postupnosť prvkov zo $\mathbb{Z}_7$ definovaná pomocou vzťahov (30) a (31). Dokážte, že

$$x_n = 4^n(1 + \vartheta)^n + 4^n(1 - \vartheta)^n, \quad n = 0, 1, \dots$$

Úloha 487. Nech $\{x_n\}$ je postupnosť prvkov $\mathbb{Z}_7$ definovaná pomocou vzťahov (30) a (31). Dokážte, že

$$x_n = 4^n \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2l} \pmod{7}, \quad n = 0, 1, \dots$$

(Návod: Upravte vzorec z úlohy 486 pomocou binomickej vety.)

Všetko by teraz bolo v poriadku. Ale odkiaľ sme vzali taký prvok ϑ , že $\vartheta^2 = 5$. To si práve teraz ukážeme.

Musíme si všimnúť, že prvok ϑ má podobné vlastnosti ako komplexné číslo i . Pripomeňme si, ako vytvárame komplexné čísla pomocou reálnych čísel. Nasledujúci postup bude analogický.

Uvažujme karteziánsky súčin $\mathbb{Z}_7 \times \mathbb{Z}_7$. Budeme ho označovať $\mathbb{Z}_7^2$. Definujme operácie $+$ a $\cdot$ nasledovne:

$$\begin{aligned} [a_1, b_1] + [a_2, b_2] &= [a_1 + a_2, b_1 + b_2], \\ [a_1, b_1] \cdot [a_2, b_2] &= [a_1 a_2 + 5b_1 b_2, a_1 b_2 + b_1 a_2]. \end{aligned}$$

Úloha 488. Dokážte, že $(\mathbb{Z}_7^2, +, \cdot)$ je komutatívny okruh s jednotkou.

Úloha 489. Dokážte, že pre $a \in \mathbb{Z}_7$ platí

$$[a, 0] \cdot [a_2, b_2] = a[a_2, b_2],$$

kde posledné násobenie je vonkajšie násobenie, ktoré sme definovali pred úlohou 471.

Úloha 490. Dokážte, že pre $a, b \in \mathbb{Z}_7$ platí

$$\begin{aligned} [a, 0] + [b, 0] &= [a + b, 0], \\ [a, 0] \cdot [b, 0] &= [ab, 0]. \end{aligned}$$

Vidíme, že prvky $[a, 0]$ majú rovnaké vlastnosti ako prvky telesa $\mathbb{Z}_7$. Preto budeme stotožňovať prvky a a $[a, 0]$.

Úloha 491. Označme $\vartheta = [0, 1]$. Dokážte, že $\vartheta^2 = 5$.

Úloha 492. Dokážte, že každý prvok zo $\mathbb{Z}_7^2$ môžeme vyjadriť v tvare $a + b\vartheta$, $a, b \in \mathbb{Z}_7$.

Označme pre $a + b\vartheta \in \mathbb{Z}_7^2$

$$N(a + b\vartheta) = (a + b\vartheta)(a - b\vartheta) = a^2 - 5b^2.$$

Hodnotu $N(a + b\vartheta)$ nazývame normou prvku $a + b\vartheta$.

Úloha 493. Dokážte, že pre $z_1, z_2 \in \mathbb{Z}_7^2$ platí

$$N(z_1 \cdot z_2) = N(z_1)N(z_2).$$

Úloha 494. Dokážte, že $N(z) = 0$ práve vtedy, keď $z = 0$.

Úloha 495. Dokážte, že $(\mathbb{Z}_7^2, +, \cdot)$ je oborom integrity.

(Návod: Použite úlohy 493 a 494.)

Úloha 496. Dokážte, že $(\mathbb{Z}_7^2, +, \cdot)$ je telesom.

(Návod: Použite úlohy 495 a 463.)

Toto teleso nazývame *kvadratickým rozšírením* telesa $\mathbb{Z}_7$. V závere tejto kapitoly si ukážeme, ako môžeme uvedený postup zovšeobecniť pre konečné teleso F . Nech $q \in F$ je taký prvok, pre ktorý $a^2 \neq q$ pre každé $a \in F$. Na množine $F^2 = F \times F$ si definujeme operácie $+$, $\cdot$ takto:

$$[a_1, b_1] + [a_2, b_2] = [a_1 + a_2, b_1 + b_2],$$

$$[a_1, b_1] \cdot [a_2, b_2] = [a_1a_2 + qb_1b_2, a_1b_2 + b_1a_2],$$

pre každé $a_1, a_2, b_1, b_2 \in F$.

Úloha 497. Dokážte, že $(F^2, +, \cdot)$ je komutatívny okruh s jednotkou.

Označme pre $[a, b] \in F^2$

$$N([a, b]) = [a, b] \cdot [a, -b] = a^2 - qb^2.$$

Túto hodnotu môžeme opäť nazvať normou prvku $[a, b]$.

Úloha 498. Dokážte, že

$$N([a_1, b_1] \cdot [a_2, b_2]) = N([a_1, b_1]) \cdot N([a_2, b_2])$$

pre všetky $a_1, a_2, b_1, b_2 \in F$.

Úloha 499. Dokážte, že pre všetky $a, b \in F$

$$N([a, b]) = 0 \iff a = 0 = b.$$

Úloha 500. Dokážte, že F^2 je obor integrity a aj teleso.

(Návod: Použite úlohy 498, 499 a 463.)

Úloha 501. Dokážte, že v telese F platí pre všetky prvky $a, b \in F$

$$a^2 = b^2 \Rightarrow a = b \vee a = -b.$$

Úloha 502. Nech v konečnom telese F platí $2 \neq 0$. Potom existuje taký prvok $q \in F$, pre ktorý $a^2 \neq q$ pre každé $a \in F$.

(Návod: $a^2 = (-a)^2$ a teda množina $\{a^2; a \in F\}$ má menej prvkov ako F .)

Úloha 503. Nech v konečnom telese F platí $2 \neq 0$. Potom existuje teleso s mohutnosťou $|F|^2$.

(Návod: Použite úlohy 500 a 502.)

Úloha 504. Nech p je nepárne prvočíslo. Potom pre každé $n \in \mathbb{N}$ existuje teleso s mohutnosťou p^{2^n} .

(Návod: Postupujte matematickou indukciou a použite úlohy 502, 503 a 457.)

Teleso F^2 z úlohy 500 nazývame *kvadratickým rozšírením* telesa F . Vzniklo ako teleso, ktoré obsahuje F a koreň polynomu $x^2 - q$. V algebre je dokázané (pozri napríklad [KOL]), že k F môžeme pridať koreň ľubovoľného polynomu s koeficientami z F . V takomto prípade hovoríme o *algebrickom rozšírení* telesa F , ktoré skúma algebra a algebrická teória čísel. V literatúre možno nájsť množstvo elegantných výsledkov o algebrických rozšíreniach telies.