

Diskrétní matematika II

5. května 2020

Obsah

Obsah	1
1 Diferenční rovnice	2
1.1 Motivační úlohy	2
2 Lineární diferenční rovnice	7
2.1 Prostor komplexních posloupností	8
2.2 Homogenní lineární diferenční rovnice	11
2.3 Lineární diferenční rovnice s pravou stranou	19
3 Příklady jiných diferenčních rovnic	28
3.1 Rekurence s nekonstantními koeficienty	28
3.2 Invertovací formule	30
4 Josefův problém a související úlohy	33
4.1 Zjednodušený Josefův problém	33
4.2 Zobecněný Josefův problém	35
5 Kořeny polynomů	38
6 Konečné grupy a konečná tělesa	41
6.1 Grupy	42
6.2 Podgrupa	44
6.3 Cyklické grupy	46
6.4 Izomorfizmy grup	49
Literatura	52

1 Diferenční rovnice

1.1 Motivační úlohy

Příklad 1.1. Králíci:

Kolik párů potomků bude mít v n -tém roce jediný pár králíků, když

- Králíci dospívají po jednom měsíci.
- Každý dospělý pár má v každém měsíci jeden pár potomků.
- Nedochází k úhynu.

Dojdeme k rekurenci

$$F_{n+2} = F_{n+1} + F_n, \quad n \geq 0, \quad F_0 = 0, \quad F_1 = 1. \quad (1.1)$$

Příklad 1.2. Hanojské věže: Máme tři kolíčky a na jednom z nich je nasunutá věž z koleček od největšího vespodu až k nejmenšímu navrch. Jaký je minimální počet kroků ve k přesunutí věže o n -kolečkách na jiný kolík, když

- V jednom tahu přesouváme jedno kolečko.
- Smíme položit jen menší na větší.

Označíme H_n . Vyzkoušíme a zjistíme $H_1 = 1$, $H_2 = 3$, $H_3 = 7$. Závislost H_n na H_{n-1} dvodíme následujícím postupem: Máme-li věž výšky n , přesuneme nejdříve horních $n - 1$ kroužků na jiný kolík. To lze provést nejméně H_{n-1} kroky. Potom přesuneme největší n -té kolečko na prázdný kolík. Nakonec opět přesuneme věž výšky $n - 1$, tentokrát na kolík s největším kolečkem, k čemuž potřebujeme dalších H_{n-1} kroků. Celkem $H_n = 2H_{n-1} + 1$.

Teď bychom chtěli vyřešit rekurentní vztah, tedy zjistit H_n v závislosti na n , nikoliv na předcházejících členech posloupnosti.

1. řešení: Uděláme si tabulku několika prvních hodnot posloupnosti napočítaných z rekurence,

n	1	2	3	4	5	6	7	...
H_n	1	3	7	15	31	63	127	...

Zkusíme uhodnout řešení. V tomto případě to není nijak složité, pro prvních sedm hodnot n platí $H_n = 2^n - 1$. Musíme ale dokázat, že to platí pro všechna přirozená n . Protože máme k dispozici vztah, převádějící H_n na výraz v předchozích členech posloupnosti, vhodným nástrojem k důkazu je matematická indukce. Platnost prvního kroku je zjevná z tabulky hodnot. Předpokládejme, že pro indexy $k < n$ platí $H_k = 2^k - 1$. Pak $H_n = 2H_{n-1} + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 1$.

2. řešení: Kdyby se stalo, že nás nenapadne možné pokračování posloupnosti 1, 3, 7, 15, 31, ..., můžeme zkusit metodu postupného dosazování:

$$\begin{aligned} H_n &= 2H_{n-1} + 1 = 2(2H_{n-2} + 1) + 1 = 2^2H_{n-2} + 2 + 1 = \\ &= 2^2(2H_{n-3} + 1) + 2 + 1 = 2^3H_{n-3} + 2^2 + 2 + 1 = \dots = \\ &= 2^{n-1}H_1 + 2^{n-2} + \dots + 2 + 1 = \sum_{j=0}^{n-1} 2^j = 2^n - 1, \end{aligned}$$

kde jsme využili, že $H_1 = 1$ a vzorec pro součet členů geometrické posloupnosti.

3. řešení: Stejně jako v případě soustav lineárních rovnic je někdy je přehlednější místo postupného dosazování napsat všechny rovnice pod sebe a eliminovat neznáme sčítáním vhodných násobků rovnic:

$$\begin{aligned} H_n - 2H_{n-1} &= 1 \quad / \times 2^0 \\ H_{n-1} - 2H_{n-2} &= 1 \quad / \times 2^1 \\ &\vdots \\ H_3 - 2H_2 &= 1 \quad / \times 2^{n-3} \\ H_2 - 2H_1 &= 1 \quad / \times 2^{n-2} \end{aligned}$$

V našem případě sečtením všech naznačených násobků rovnic vypadnou neznámé členy $H_{n-1}, \dots, H_2$ a získáme

$$H_n - 2^{n-1}H_1 = \sum_{j=0}^{n-2} 2^j,$$

což vede ke stejnému výsledku jako prve.

Příklad 1.3. Krájení pizzy: Jaký je nejvyšší počet dílů, na který lze rozkrojit pizzu n -rovnými řezy? Po úvaze brzy zjistíme, že k získání maximálního počtu má smysl dělat řezy pouze tak, aby každý nový řez protínal v šechny předchozí na ploše pizzy. Předpokládáme-li, že řezy umíme dělat s libovolnou přesností, můžeme vlastně uvažovat pizzu libovolně velkou a úlohu pak zjednodušit následovně: Hledáme nejvyšší počet částí, na které lze rozdělit rovinu n přímkami. Označme tento počet P_n .

Zkusme opět určit P_n pro několik počátečních hodnot n . Zjevně $P_0 = 1$, $P_1 = 2$. Při určování $P_2 = 4$ a $P_3 = 7$ si uvědomíme, že je třeba n -tou přímkou volit různoběžnou s předchozími. Při umísťování každé další přímky je třeba dbát na to, aby žádné tři neprocházely jedním společným bodem.

Rekurentní vztah pro P_n vznikne, když si uvědomíme, že oproti P_{n-1} vznikne tolik nových částí, kolik je průsečíků nové přímky s předchozími, a ještě jedna navíc, tedy celkem n . Máme proto $P_n = P_{n-1} + n$.

Tento rekurentní vztah chceme opět vyřešit. Vytvoříme tabulku prvních několika hodnot posloupnosti,

n	0	1	2	3	4	5	6	...
P_n	1	2	4	7	11	16	22	...

Tentokrát je výrazně obtížnější odhadnout výsledek pouze z této tabulky. Napíšeme proto rovnice pod sebe.

$$P_n - P_{n-1} = n$$

$$P_{n-1} - P_{n-2} = n - 1$$

$$\vdots$$

$$P_2 - P_1 = 2$$

$$P_1 - P_0 = 1$$

Prostým sečtením získáme rovnost $P_n - P_0 = \sum_{j=1}^n j = \frac{1}{2}n(n+1)$, takže

$$P_n = 1 + \frac{n(n+1)}{2} = \frac{n^2 + n + 2}{2}.$$

Příklad 1.4. Krájení másla: Zkoumejme nyní trojrozměrnou analogii předchozí úlohy, tedy otázku, jaký je nejvyšší počet dílů, na který lze rozkrojit n -rovnými řezy kostku másla. Stejně jako v příkladu 1.3 problém zidealizujeme a převedeme na zjišťování maximálního počtu částí, na které lze rozdělit prostor n rovinami. Označme tento počet R_n .

Tabulku R_n pro několik počátečních hodnot n je sestavujeme teď bez obrázku poněkud obtížněji, máme $R_0 = 1$, $R_1 = 2$, $R_2 = 4$, $R_3 = 8$, $R_4 = 15$, ... Při umísťování rovin je třeba dodržovat následující pravidla:

- Roviny klademe tak, aby jejich průsečnice byly mimoběžné;
- žádným bodem prostoru neprochází více než tři roviny.

Při splnění těchto podmínek se v n -té rovině zobrazí průsečnice s předchozími $n - 1$ rovinami jako $n - 1$ různoběžek, které se nikdy nesetkávají tři v jednom bodě. To se

nápadně podobá úloze o pizze. Když chceme sestavit pro posloupnost $(R_n)_{n \geq 1}$ rekurentní vztah, uvědomíme si, že přidáním n -té roviny rozdělíme na dvě každý díl z dělení z $(n-1)$ -ního kroku, kterým n -tá rovina prochází, a těch je právě tolik, kolik je oblastí v n -té rovině vytyčených průsečnicemi s předchozími přímkami. Těch je ale P_{n-1} . Proto pro každé n platí

$$R_n = R_{n-1} + P_{n-1}.$$

Rekurenci opět řešíme zapsáním pod sebe,

$$\begin{aligned} R_n - R_{n-1} &= P_{n-1} \\ R_{n-1} - R_{n-2} &= P_{n-2} \\ &\vdots \\ R_2 - R_1 &= P_1 \\ R_1 - R_0 &= P_0 \end{aligned}$$

Sečtením získáme rovnost

$$R_n - R_0 = \sum_{j=0}^{n-1} P(j) = \sum_{j=0}^{n-1} \left(1 + \frac{n(n+1)}{2}\right) = n + \frac{1}{2} \sum_{j=0}^{n-1} j + \frac{1}{2} \sum_{j=0}^{n-1} j^2,$$

odkud odvodíme

$$R_n = \frac{n^3 + 5n - 6}{6}.$$

Příklad 1.5. Pro pořádek odvodíme vztah $\sum_{j=1}^n j^2 = \frac{1}{6}(n(n+1)(2n+1))$.

1. řešení: Jedním ze způsobů je zkoumání rozdílu $\sum_{j=1}^n (j+1)^3 - \sum_{j=1}^n j^3$. Na jedné straně je zjevné, že

$$\sum_{j=1}^n (j+1)^3 - \sum_{j=1}^n j^3 = \sum_{j=2}^{n+1} j^3 - \sum_{j=1}^n j^3 = (n+1)^3 - 1. \quad (1.2)$$

Na druhé straně můžeme vyjádřit

$$\sum_{j=1}^n (j+1)^3 - \sum_{j=1}^n j^3 = \sum_{j=1}^n (3j^2 + 3j + 1) = 3 \sum_{j=1}^n j^2 + \frac{3}{2}n(n+1) + n. \quad (1.3)$$

Porovnáním (1.2) a (1.3) dostaneme

$$\sum_{j=1}^n j^2 = \frac{1}{3} \left(n^3 + 3n^2 + 3n - \frac{3}{2}(n^2 + n) - n \right) = \frac{1}{6}(2n^3 + 3n^2 + n),$$

což odpovídá uváděnému vzorci.

2. řešení: Čtenář možná zná odvození pomocí jiného zajímavého triku, totiž převedení na součet dvojnásobné sumy. Zapišeme-li $j = \sum_{k=1}^j 1$, máme

$$\begin{aligned} \sum_{j=1}^n j^2 &= \sum_{j=1}^n \sum_{k=1}^j j = \sum_{k=1}^n \sum_{j=k}^n j = \sum_{k=1}^n \frac{(n+k)(n+1-k)}{2} = \\ &= \frac{1}{2} \sum_{k=1}^n (n(n+1) + k - k^2) = \frac{n^2(n+1)}{2} + \frac{n(n+1)}{4} - \frac{1}{2} \sum_{k=1}^n k^2. \end{aligned}$$

Porovnáním levé a pravé strany dostaneme

$$\frac{3}{2} \sum_{j=1}^n j^2 = \frac{n^2(n+1)}{2} + \frac{n(n+1)}{4},$$

což vede ke kýženému výsledku.

Příklad 1.6. QuickSort

2 Lineární diferenční rovnice

Všechny v úvodu uvedené úlohy vedly na řešení tzv. lineárních rekurentních vztahů, totiž takových, v nichž n -tý člen posloupnosti je lineární kombinací pevného počtu předchozích členů. Přesněji tento pojem uvedeme v následující definici.

Definice 2.1. Necht $k \in \mathbb{N}$, $(f(n))_{n \geq 1}$, $(\alpha_0(n))_{n \geq 1}$, $\dots$, $(\alpha_{k-1}(n))_{n \geq 1}$ jsou komplexní posloupnosti takové, že $\alpha_0(n)$ není rovna nulové posloupnosti. Vztah

$$a_{n+k} + \alpha_{k-1}(n)a_{n+k-1} + \alpha_{k-2}(n)a_{n+k-2} + \dots + \alpha_1(n)a_{n+1} + \alpha_0(n)a_n = f(n), \quad n \geq 1, \quad (2.1)$$

se nazývá lineární diferenční rovnice k -tého řádu (nebo lineární rekurentní vztah k -tého řádu) pro posloupnost $(a_n)_{n \geq 1}$.

Poznámka 2.2. 1. Všimněte si, že pro každé n je závislost na předchozích k členech daná jinou rovnicí, protože posloupnosti $(\alpha_0(n))_{n \geq 1}$, $\dots$, $(\alpha_{k-1}(n))_{n \geq 1}$ nejsou obecně konstantní. Když $\alpha_0(n) = \alpha_0 \neq 0$, $\dots$, $\alpha_{k-1}(n) = \alpha_{k-1}$ pro všechna $n \geq 1$, nazýváme (2.1) lineární diferenční rovnice k -tého řádu s konstantními koeficienty.

2. Podmínka, aby posloupnost $(\alpha_0(n))_{n \geq 1}$ nebyla identicky nulová, zaručuje, že diferenční rovnice je právě k -tého a nikoliv nižšího řádu.
3. Aby byla posloupnost $(a_n)_{n \geq 1}$ vztahem (2.1) jednoznačně určena, je třeba zadat k počátečních podmínek, tj. hodnot $a_0, \dots, a_{k-1}$. Ostatní členy pak ze vztahu (2.1) lze dopočítat. Posléze uvidíme, že ve skutečnosti stačí zadat libovolných k členů posloupnosti.
4. Nejjednodušším případem pravé strany $(f(n))_{n \geq 1}$ diferenční rovnice (2.1) je nulová posloupnost. Pokud $f(n) = 0$ pro každé $n \geq 1$, nazýváme (2.1) homogenní lineární diferenční rovnice.

Příklad 2.3. Rekurence $F_{n+2} = F_{n+1} + F_n$ zapsána jako $F_{n+2} - F_{n+1} - F_n = 0$ je homogenní lineární diferenční rovnice druhého řádu s konstantními koeficienty, kde $\alpha_0(n) = \alpha_1(n) = -1$ pro $n \geq 0$.

Příklad 2.4. Ačkoliv v rekurenci $a_n = a_{n-2}$ závisí n -tý člen vždy pouze na jednom z předchozích členů, je to rekurence druhého řádu, protože k jednoznačnému určení všech členů posloupnosti $(a_n)_{n \geq 0}$ je třeba zadat dvě počáteční podmínky, a_1 a a_2 .

2.1 Prostor komplexních posloupností

Pro naše pozdější úvahy je podstatné si připomenout vektorový prostor ℓ komplexních posloupností. Na množině posloupností $\{(a_n)_{n \geq 1} : a_n \in \mathbb{C}\}$ jsou definovány operace $\oplus : \ell \times \ell \rightarrow \ell$, $\odot : \mathbb{C} \times \ell \rightarrow \ell$, člen po členu, tedy

$$(a_n)_{n \geq 1} \oplus (b_n)_{n \geq 1} = (a_n + b_n)_{n \geq 1}, \quad \text{and} \quad \alpha \odot (a_n)_{n \geq 1} = (\alpha a_n)_{n \geq 1}.$$

Roli nulového vektoru hraje nulová posloupnost $(0)_{n \geq 1}$. Čtenář si snadno ověří, že trojice $(\ell, \oplus, \odot)$ splňuje všechny axiomy vektorového prostoru nad tělesem $\mathbb{C}$. Protože jsou operace definované přirozeně a z kontextu je vždy jasné, kdy se jedná o sčítání a násobení skalárem v ℓ , budeme je brzy značit obyčejným $+$ a $\cdot$.

Tento prostor má nekonečnou dimenzi, protože pro každé $m \in \mathbb{N}$ existuje m -tice lineárně nezávislých vektorů. Tu lze volit například z posloupností $e^{(j)} = (e_n^{(j)})_{n \geq 1}$, $j = 1, \dots, m$, kde $e_n^{(j)} = \delta_{jn}$ je dáno Kroneckerovým delta. Symbolicky zapsáno,

$$\begin{aligned} e^{(1)} &= (1, 0, 0, \dots, 0, 0, \dots), \\ e^{(2)} &= (0, 1, 0, \dots, 0, 0, \dots), \\ &\vdots \\ e^{(m)} &= (0, 0, 0, \dots, 1, 0, \dots). \end{aligned}$$

Lineární nezávislost těchto posloupností se ověří přímo z definice. Zjišťujeme, zda jediná lineární kombinace $e^{(1)}, \dots, e^{(m)}$ rovná nulové posloupnosti je triviální, tedy zda

$$\alpha_1 \odot e^{(1)} \oplus \dots \oplus \alpha_m \odot e^{(m)} = (\alpha_1 e_n^{(1)} + \dots + \alpha_m e_n^{(m)})_{n \geq 1} = (0)_{n \geq 1} \quad (2.2)$$

implikuje $\alpha_1 = \dots = \alpha_m = 0$. Vztah (2.2) lze vidět jako nekonečně mnoho rovnic pro neznámé $\alpha_1, \dots, \alpha_m$, z nichž prvních m udává právě $\alpha_j = 0$, další jsou triviální, $0 = 0$. Lineární nezávislost posloupností $e^{(1)}, \dots, e^{(m)}$ je tedy potvrzena.

Využijme tento algebraický pohled na posloupnosti k vyřešení nejjednoduššího případu lineární diferenční rovnice druhého řádu, tedy na rekurenci pro Fibonacciho čísla (1.1).

Označme M množinu posloupností splňujících stejnou rekurenci,

$$M = \{(a_n)_{n \geq 1} \in \ell : a_{n+2} - a_{n+1} - a_n = 0, \text{ pro } n \geq 1\},$$

a zkoumejme její strukturu. Především si všimneme, že M je neprázdná, obsahuje například posloupnost Fibonacciho čísel a samozřejmě také nulovou posloupnost. Snadno rovněž vidíme, že M je uzavřená na sčítání $\oplus$ a násobení číslem z tělesa $\mathbb{C}$. Pro posloupnosti $(a_n)_{n \geq 1}, (b_n)_{n \geq 1} \in M$ a komplexní číslo α totiž můžeme dosadit posloupnost $(c_n)_{n \geq 1} := \alpha \odot (a_n)_{n \geq 1} \oplus (b_n)_{n \geq 1} = (\alpha a_n + b_n)_{n \geq 1}$ do rekurence a zjistit, že

$$\begin{aligned} c_{n+2} - c_{n+1} - c_n &= (\alpha a_{n+2} + b_{n+2}) - (\alpha a_{n+1} + b_{n+1}) - (\alpha a_n + b_n) = \\ &= \alpha \underbrace{(a_{n+2} - a_{n+1} - a_n)}_{=0 \text{ protože } (a_n)_{n \geq 1} \in M} + \underbrace{(b_{n+2} - b_{n+1} - b_n)}_{=0 \text{ protože } (b_n)_{n \geq 1} \in M} = 0. \end{aligned}$$

Množina M s operacemi $\oplus, \odot$ tedy tvoří podprostor vektorového prostoru ℓ .

Protože k jednoznačnému určení posloupnosti z M je třeba znát dva její členy, odhadujeme, že dimenze prostoru M je rovna 2. Abychom toto dokázali, potřebujeme najít dvoučlennou bázi prostoru M , tedy dvě lineárně nezávislé posloupnosti $a^{(1)}, a^{(2)}$ z M takové, že každá posloupnost z M je jejich lineární kombinací. Tentokrát smíme volit pouze dva členy v bazických posloupnostech. Ostatní je třeba dopočítat z rekurence $a_{n+2}^{(j)} - a_{n+1}^{(j)} - a_n^{(j)}$ tak, aby bylo zaručeno, že $a^{(1)}, a^{(2)}$ jsou prvky množiny M . Volíme-li $a_1^{(1)} = 1, a_2^{(1)} = 0, a_1^{(2)} = 0, a_2^{(2)} = 1$, dostaneme

$$\begin{aligned} a^{(1)} &= (1, 0, 1, 1, 2, 3, 5, \dots), \\ a^{(2)} &= (0, 1, 1, 2, 3, 5, 8, \dots), \end{aligned}$$

tedy posunutá Fibonacciho čísla. Snadno se přesvědčíme, že tyto posloupnosti jsou opravdu lineárně nezávislé, protože

$$\alpha_1 a_1^{(1)} + \alpha_2 a_1^{(2)} = \alpha_1 = 0, \quad \alpha_1 a_2^{(1)} + \alpha_2 a_2^{(2)} = \alpha_2 = 0.$$

Ověřme fakt, že $a^{(1)}, a^{(2)}$ generují celou množinu M . Necht' $(a_n)_{n \geq 1} \in M$. Najdeme $\alpha_1, \alpha_2 \in \mathbb{C}$ tak, aby $(a_n)_{n \geq 1} = \alpha_1 \odot a^{(1)} + \alpha_2 \odot a^{(2)}$. Porovnáním po složkách získáme pro $n = 1, 2$,

$$\begin{aligned} a_1 &= \alpha_1 a_1^{(1)} + \alpha_2 a_1^{(2)} = \alpha_1, \\ a_2 &= \alpha_1 a_2^{(1)} + \alpha_2 a_2^{(2)} = \alpha_2. \end{aligned}$$

Ještě musíme ověřit, že $a_n = \alpha_1 a_n^{(1)} + \alpha_2 a_n^{(2)}$ pro každé $n \geq 1$. To provedeme matematickou indukcí. Pro $n = 1, 2$ to zjevně platí. Předpokládejme, že $a_k = \alpha_1 a_k^{(1)} + \alpha_2 a_k^{(2)}$ pro $k < n$. Z rekurence pro $(a_n)_{n \geq 1}$ máme

$$\begin{aligned} a_n &= a_{n-1} + a_{n-2} = (\alpha_1 a_{n-1}^{(1)} + \alpha_2 a_{n-1}^{(2)}) + (\alpha_1 a_{n-2}^{(1)} + \alpha_2 a_{n-2}^{(2)}) = \\ &= \alpha_1 (a_{n-1}^{(1)} + a_{n-2}^{(1)}) + \alpha_2 (a_{n-1}^{(2)} + a_{n-2}^{(2)}) = \alpha_1 a_n^{(1)} + \alpha_2 a_n^{(2)}, \end{aligned}$$

kde jsme využili indukční předpoklad a rekurenci pro posloupnosti $a^{(1)}$ a $a^{(2)}$. Tím jsme vlastně dokázali následující tvrzení.

Tvrzení 2.5. *Nechť $M = \{(a_n)_{n \geq 1} \in \ell : a_{n+2} - a_{n+1} - a_n = 0, \text{ pro } n \geq 1\}$. Pak M je podprostor prostoru ℓ a platí $\dim M = 2$.*

Sice jsme ukázali, že posloupnosti $a^{(1)}, a^{(2)}$ tvoří bázi prostoru M , nicméně k vyřešení Fibonacciho rekurentního vztahu nám to zatím nepomohlo. Potřebujeme najít vhodnější bázi, tak, aby n -tý člen bazických posloupností jednoduchým způsobem závisel na n . Vyzkoušíme, jestli bázi nemůžeme sestavit z posloupností tvaru $(\lambda^n)_{n \geq 1}$, pro nějaké $\lambda \in \mathbb{C}$. Především musí být $(\lambda^n)_{n \geq 1} \in M$, tedy splňovat rekurenci,

$$\lambda^{n+2} - \lambda^{n+1} - \lambda^n = 0, \quad n \geq 1.$$

Při $\lambda = 0$ to je jistě pravda, nicméně výsledkem je nulová posloupnost, která nemůže být prvkem báze. Proto předpokládáme $\lambda \neq 0$ a vykrátíme λ^n . Aby posloupnost $(\lambda^n)_{n \geq 1}$ splňovala Fibonacciho rekurenci, je pak nutné a stačí, aby λ byla kořenem rovnice $x^2 - x - 1$. Získáme následující fakt.

Tvrzení 2.6. *Nechť $\lambda \neq 0$. Pak $(\lambda^n)_{n \geq 1} \in M$, právě když $\lambda = \frac{1}{2}(1 \pm \sqrt{5})$.*

Dostali jsme tedy právě dvě posloupnosti tvaru $(\lambda^n)_{n \geq 1}$ v prostoru M . Byli bychom rádi, kdyby $((\frac{1+\sqrt{5}}{2})^n)_{n \geq 1}$ a $((\frac{1-\sqrt{5}}{2})^n)_{n \geq 1}$ tvořily bázi M . K tomu již stačí ověřit jejich lineární nezávislost, tedy platnost implikace

$$\alpha_1 \left(\frac{1+\sqrt{5}}{2} \right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2} \right)^n = 0 \text{ pro každé } n \in \mathbb{N} \quad (2.3)$$

$\Downarrow$

$$\alpha_1 = \alpha_2 = 0.$$

Jednou z možností je použít dvě z nekonečně mnoha rovnic (2.3) pro neznámé α_1, α_2 , např. pro $n = 1$ a $n = 2$, a vyjádřit α_1, α_2 . Platnost implikace lze ale také ověřit použitím vlastností limit posloupností. Protože $\frac{1+\sqrt{5}}{2} > 1$ a $|\frac{1-\sqrt{5}}{2}| < 1$, je limita

$$\lim_{n \rightarrow \infty} \left(\alpha_1 \left(\frac{1+\sqrt{5}}{2} \right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2} \right)^n \right) = \begin{cases} +\infty & \text{když } \alpha_1 > 0, \\ 0 & \text{když } \alpha_1 = 0, \\ -\infty & \text{když } \alpha_1 < 0, \end{cases}$$

takže (2.3) platí pouze pro $\alpha_1 = 0$. Odtud už přímo plyne, že i $\alpha_2 = 0$ a tedy naše posloupnosti $((\frac{1+\sqrt{5}}{2})^n)_{n \geq 1}$ a $((\frac{1-\sqrt{5}}{2})^n)_{n \geq 1}$ jsou lineárně nezávislé. Jelikož $\dim M = 2$, tvoří bázi prostoru M . Každý prvek z M , a tedy i posloupnost $(F_n)_{n \geq 1}$ Fibonacciho čísel je tedy jejich lineární kombinací. Nalezneme tedy $\alpha, \beta \in \mathbb{C}$ takové, že pro každé n platí

$$F_n = \alpha \left(\frac{1+\sqrt{5}}{2} \right)^n + \beta \left(\frac{1-\sqrt{5}}{2} \right)^n.$$

K tomu použijeme soustavu rovnic danou počátečními podmínkami $F_1 = 1, F_2 = 1$,

$$\begin{aligned} F_1 = 1 &= \alpha \frac{1 + \sqrt{5}}{2} + \beta \frac{1 - \sqrt{5}}{2}, \\ F_2 = 1 &= \alpha \left(\frac{1 + \sqrt{5}}{2} \right)^2 + \beta \left(\frac{1 - \sqrt{5}}{2} \right)^2. \end{aligned}$$

Jednoduchým výpočtem dostaneme $\alpha = -\beta = \frac{1}{\sqrt{5}}$. Odvodili jsme tak tzv. Binetovu formuli.

Tvrzení 2.7. *Nechť $(F_n)_{n \in \mathbb{N}}$ je dána rekurencí $F_{n+2} = F_{n+1} + F_n$ pro $n \geq 1$ s počátečními podmínkami $F_1 = F_2 = 1$. Pak*

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n, \quad n \in \mathbb{N}.$$

Protože posloupnost $\left(\frac{1 - \sqrt{5}}{2} \right)^n$ má za limitu nulu, snadno nahlédneme, že F_n je vlastně nejbližší celé číslo k číslu $\frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n$.

2.2 Homogenní lineární diferenční rovnice

Postup ilustrovaný v předchozím paragrafu na případu rekurence pro Fibonacciho čísla nyní aplikujeme k řešení obecných homogenních lineárních rekurencí k -tého řádu s konstantními koeficienty,

$$a_{n+k} + \alpha_{k-1}a_{n+k-1} + \alpha_{k-2}a_{n+k-2} + \cdots + \alpha_1a_{n+1} + \alpha_0a_n = 0, \quad n \geq 1. \quad (2.4)$$

Věta 2.8. *Označme*

$$M = \{(a_n)_{n \geq 1} \in \ell : (a_n)_{n \geq 1} \text{ splňuje (2.4)}\}.$$

Množina M je podprostor prostoru ℓ a platí $\dim M = k$.

Důkaz. Protože M obsahuje nulovou posloupnost, je $M \neq \emptyset$. Musíme ještě ověřit uzavřenost na operace $\oplus$ a $\odot$ z prostoru ℓ nad tělesem $\mathbb{C}$. Ověření je přímočaré, takže ho necháme na čtenáři. $\square$

V prostoru M budeme opět hledat vhodnou bázi. Protože je M prostor dimenze k , stačí zvolit k lineárně nezávislých posloupností. Stejně jako v příkladě s Fibonacciho rekurencí vyzkoušíme posloupnosti typu $(\lambda^n)_{n \geq 1}$.

Věta 2.9. *Nechť $\lambda \neq 0$. Pak $(\lambda^n)_{n \geq 1} \in M$, právě když λ je kořenem polynomu*

$$P(x) = x^k + \alpha_{k-1}x^{k-1} + \alpha_{k-2}x^{k-2} + \cdots + \alpha_1x + \alpha_0. \quad (2.5)$$

Definice 2.10. Polynom (2.5) v předchozí definici se nazývá charakteristický polynom diferenční rovnice (2.4). Rovnice $P(\lambda) = 0$ je charakteristická rovnice (2.4).

Důkaz věty 2.9. celé provést obecně. □

Všimněme si, že až po větu 2.8 bylo možné uvažovat diferenční rovnice s nekonstantními koeficienty. Teprve když jsme odvozovali důkaz věty 2.9, bylo nutné vzít v potaz konstantnost koeficientů $\alpha_i(n)$.

Poznámka 2.11. Vzhledem k tomu, že bude třeba pracovat s kořeny charakteristického polynomu diferenční rovnice, je vhodné připomenout některá fakta o polynomech. Z kurzů matematické analýzy a lineární algebry by čtenář měl vědět, že

- Polynom s komplexními koeficienty stupně k má v $\mathbb{C}$ právě k kořenů, tj. existují komplexní čísla $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ tak, že

$$P(x) = \alpha_k x^k + \dots + \alpha_1 x + \alpha_0 = \alpha_k (x - \lambda_1) \cdots (x - \lambda_k).$$

- Jestliže má polynom reálné koeficienty, pak s každým kořenem $\lambda_0 \in \mathbb{C}$ má za kořen i číslo $\bar{\lambda}_0$ komplexně sdružené k λ . Kořeny $\lambda_0, \bar{\lambda}_0$ mají stejnou násobnost. Toto tvrzení lze snadno odvodit z faktu, že $P(\bar{\lambda}) = \overline{P(\lambda)} = 0$.
- Jestliže má polynom P kořen λ násobnosti $\gamma \geq 1$, pak jeho derivace P' má kořen λ násobnosti $\gamma - 1$. Je-li totiž $P(x) = (x - \lambda)^\gamma Q(x)$, kde $Q(\lambda) \neq 0$, pak $P'(x) = (x - \lambda)^{\gamma-1} Q(x) + (x - \lambda)^\gamma Q'(x) = (x - \lambda)^{\gamma-1} (Q(x) + (x - \lambda) Q'(x)) = (x - \lambda)^{\gamma-1} R(x)$. Násobnost kořene λ je tedy alespoň γ_1 . Dosadíme-li $x = \lambda$, zjistíme, že $R(\lambda) = Q(\lambda) + (\lambda - \lambda) Q'(\lambda) = Q(\lambda) \neq 0$. Proto je násobnost kořene λ právě $\gamma - 1$.
- Jestliže polynom $P(\lambda) = \sum_{j=0}^k \alpha_j \lambda^j$ má kořeny $\lambda_1, \dots, \lambda_k$, a $C \in \mathbb{C}$ je nějaká nenulová konstanta, pak polynom

$$\tilde{P}(\lambda) = \sum_{j=0}^k \tilde{\alpha}_j \lambda^j, \quad \text{kde} \quad \tilde{\alpha}_j = C^{j-k} \alpha_j \quad \text{pro } j = 0, \dots, k,$$

má kořeny $C^{-1} \lambda_1, \dots, C^{-1} \lambda_k$. Platí totiž

$$\begin{aligned} P(\lambda) &= \sum_{j=0}^k \alpha_j \lambda^j = 0 \\ &\Downarrow \\ \tilde{P}(C^{-1} \lambda) &= \sum_{j=0}^k \tilde{\alpha}_j (C^{-1} \lambda)^j = \sum_{j=0}^k C^{j-k} \alpha_j \frac{\lambda^j}{C^j} = C^{-k} \sum_{j=0}^k \alpha_j \lambda^j = C^{-k} P(\lambda) = 0. \end{aligned}$$

Při vyšetřování kořenů polynomu P mohou nastat dvě situace:

1. Pokud máme štěstí, kořeny $\lambda_1, \dots, \lambda_k$ charakteristického polynomu jsou navzájem různé. Tyto kořeny jsou navíc nenulové, což je zaručeno podmínkou $\alpha_0 \neq 0$. V prostoru M tedy máme k posloupností $(\lambda_1^n)_{n \geq 1}, \dots, (\lambda_k^n)_{n \geq 1}$. Když ověříme jejich lineární nezávislost, budeme mít vhodnou bázi prostoru M .
2. Může se ale stát, že některé kořeny polynomu P mají násobnost ≥ 2 . Polynom P má pak pouze $l < k$ navzájem různých nenulových kořenů $\lambda_1, \dots, \lambda_l$, a i kdyby posloupnosti $(\lambda_1^n)_{n \geq 1}, \dots, (\lambda_l^n)_{n \geq 1}$ byly lineárně nezávislé, není jich dost, aby tvořily bázi prostoru M , který má dimenzi k . Bude tedy nutné soubor doplnit o další lineárně nezávislé posloupnosti.

Každou ze situací rozebereme zvlášť.

2.2.1 Charakteristický polynom s různými kořeny

Nechť charakteristický polynom P ze vztahu (2.5) má k navzájem různých kořenů $\lambda_1, \dots, \lambda_k$. Ověříme lineární nezávislost posloupností $(\lambda_1^n)_{n \geq 1}, \dots, (\lambda_k^n)_{n \geq 1}$, tj. platnost implikace

$$\beta_1 \lambda_1^n + \dots + \beta_k \lambda_k^n = 0 \text{ pro } n \in \mathbb{N} \quad \Rightarrow \quad \beta_1 = \dots = \beta_k = 0.$$

Zapišme matici soustavy prvních k rovnic pro neznámé $\beta_1, \dots, \beta_k$,

$$A = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \dots & \lambda_k \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \dots & \lambda_k^2 \\ \lambda_1^3 & \lambda_2^3 & \lambda_3^3 & \dots & \lambda_k^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_1^k & \lambda_2^k & \lambda_3^k & \dots & \lambda_k^k \end{pmatrix} \quad (2.6)$$

Chceme ukázat, že soustava homogenních lineárních rovnic s takovou maticí má pouze triviální řešení. Čtenář obeznámený s pojmem determinantu jistě rozpoznal Vandermondu matici, jejíž determinant je roven $\det A = \prod_{1 \leq i < j \leq k} (\lambda_j - \lambda_i)$, a proto je v případě navzájem různých nenulových $\lambda_1, \dots, \lambda_k$ různý od nuly. Matice A je tedy regulární a soustava má pouze triviální řešení. Protože ale nepředpokládáme znalost látky kurzu Lineární algebra 2, pokusíme se přesvědčit i čtenáře s determinantů neznalé. Můžeme provést ekvivalentní úpravy matice A , tj. ty, které nezmění řešení příslušné soustavy rovnic. Takovou úpravou je například přičítání λ_1 -násobku předchozího řádku k následujícímu,

kteřé vyrobí v prvním sloupci nuly,

$$A \sim \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \dots & \lambda_k \\ 0 & \lambda_2(\lambda_2 - \lambda_1) & \lambda_3(\lambda_3 - \lambda_1) & \dots & \lambda_k(\lambda_k - \lambda_1) \\ 0 & \lambda_2^2(\lambda_2 - \lambda_1) & \lambda_3^2(\lambda_3 - \lambda_1) & \dots & \lambda_k^2(\lambda_k - \lambda_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \lambda_2^{k-1}(\lambda_2 - \lambda_1) & \lambda_3^{k-1}(\lambda_3 - \lambda_1) & \dots & \lambda_k^{k-1}(\lambda_k - \lambda_1) \end{pmatrix} \quad (2.7)$$

V následujícím kroku bychom chtěli vydělit všechny sloupce tak, aby podmatice $k - 1 \times k - 1$ byla stejného typu jako původní matice A . Dostaneme matici

$$B = \begin{pmatrix} \lambda_1 & \frac{\lambda_2}{\lambda_2 - \lambda_1} & \lambda_3(\lambda_3 - \lambda_1)^{-1} & \dots & \lambda_k(\lambda_k - \lambda_1)^{-1} \\ 0 & \lambda_2 & \lambda_3 & \dots & \lambda_k \\ 0 & \lambda_2^2 & \lambda_3^2 & \dots & \lambda_k^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \lambda_2^{k-1} & \lambda_3^{k-1} & \dots & \lambda_k^{k-1} \end{pmatrix}. \quad (2.8)$$

Tato úprava už ovšem nepatří mezi ekvivalentní úpravy. Z našeho hlediska to ale nevadí, protože soustava s maticí B má pouze triviální řešení, právě když soustava s maticí A má pouze triviální řešení. Zavedeme-li totiž

$$\gamma_1 = \beta_1, \quad \gamma_2 = \beta_2(\lambda_2 - \lambda_1), \quad \dots, \quad \gamma_k = \beta_k(\lambda_k - \lambda_1),$$

pak $\beta_1, \dots, \beta_k$ splňují homogenní soustavu s maticí A , právě když $\gamma_1, \dots, \gamma_k$ splňují homogenní soustavu s maticí B , a z jejich vztahu je jasné, že $\beta_1 = 0$, právě když $\gamma_i = 0$.

Je zjevné, že úpravami obdobnými těm z (2.7) a (2.8) obdržíme matici v horním trojúhelníkovém tvaru s diagodálou $(\lambda_1, \lambda_2, \dots, \lambda_k)$, takže příslušná homogenní soustava má pouze triviální řešení. Odtud vyplývá, že nutně $\beta_1 = \beta_2 = \dots = \beta_k = 0$.

V prostoru M dimenze k tudíž máme k lineárně nezávislých posloupností $(\lambda_1^n)_{n \geq 1}, \dots, (\lambda_k^n)_{n \geq 1}$, které tedy tvoří bázi. Libovolná posloupnost $(a_n)_{n \geq 1} \in M$ je tedy jejich lineární kombinací. Přesněji:

Tvrzení 2.12. *Nechť charakteristický polynom (2.5) lineární rekurence (2.4) má k navzájem různých kořenů $\lambda_1, \dots, \lambda_k$. Pak ke každé posloupnosti $(a_n)_{n \geq 1}$, která je řešením (2.4), existují komplexní čísla $\beta_1, \dots, \beta_k$ tak, že pro každé $n \geq 1$ platí*

$$a_n = \beta_1 \lambda_1^n + \dots + \beta_k \lambda_k^n. \quad (2.9)$$

Koeficienty $\beta_1, \dots, \beta_k$ získáme porovnáním (2.9) s počátečními podmínkami pro posloupnost $(a_n)_{n \geq 1}$, obvykle zadanými určením hodnot $a_1, \dots, a_k$. Dostáváme soustavu k lineárních rovnic pro neznámé $\beta_1, \dots, \beta_k$. Matice této soustavy je regulární, takže soustava má jednoznačné řešení. V případě zadání právě hodnot $a_1, \dots, a_k$ je maticí soustavy

matice A ze vztahu (2.6). Je ale zřejmé, že zadáním jiných k hodnot posloupnosti $(a_n)_{n \geq 1}$ bychom opět dostali soustavu lineárních rovnic, jejímž řešením bychom získali koeficienty $\beta_1, \dots, \beta_k$ do (2.9).

2.2.2 Charakteristický polynom s násobnými kořeny

Příklad 2.13. Motivací příklad: Řešme diferenční rovnici $a_{n+2} - 2a_{n+1} + a_n = 0$ s počátečními podmínkami $a_1 = 1$, $a_2 = -1$. Charakteristický polynom této rovnice je $P(\lambda) = \lambda^2 - 2\lambda + 1 = (\lambda - 1)^2$. Kořen máme tedy pouze jeden, $\lambda_1 = \lambda_2 = 1$. Ke konstantní posloupnosti $(1^n)_{n \geq 1} = (1)_{n \geq 1}$ tedy musíme dodat ještě jednu jinou tak, aby společně tvořily bázi prostoru $M = \{(a_n)_{n \geq 1} \in \ell : a_{n+2} - 2a_{n+1} + a_n = 0, \text{ pro } n \geq 1\}$. Protože lze naši rekurenci přepsat $a_{n+2} - a_{n+1} = a_{n+1} - a_n$, snadno nás napadne jiné možné řešení, třeba $(a_n)_{n \geq 1} = (n)_{n \geq 1}$. Vyzkoušíme, zda posloupnosti $(1)_{n \geq 1}$ a $(n)_{n \geq 1}$ jsou lineárně nezávislé, jako obvykle přímo z definice. Musíme ověřit, že $\alpha + \beta n = 0$ pro každé $n \geq 1$ implikuje $\alpha = \beta = 0$. To je ovšem pravda, protože už pro $n = 1$ a $n = 2$ máme soustavu

$$\alpha + \beta = 0$$

$$\alpha + 2\beta = 0$$

která má samozřejmě pouze triviální řešení. Posloupnosti $(1)_{n \geq 1}$ a $(n)_{n \geq 1}$ tedy tvoří bázi prostoru M a každé řešení naší rekurence musí být jejich lineární kombinací. Přesněji řečeno, pro každé $(a_n)_{n \geq 1} \in M$ existují komplexní čísla α, β taková, že

$$a_n = \alpha + \beta n \quad \text{pro } n \geq 1.$$

Prostor M tedy obsahuje právě všechny aritmetické posloupnosti. Koeficienty $\alpha, \beta \in \mathbb{C}$ spočítáme z počátečních podmínek,

$$\alpha + \beta = 1$$

$$\alpha + 2\beta = -1$$

kde vidíme, že $\beta = -2$ a $\alpha = 3$. Řešením naší úlohy je proto posloupnost $(a_n)_{n \geq 1} = (3 - 2n)_{n \geq 1}$.

Podívejme se, jak obecně řešit situaci, když některé kořeny charakteristického polynomu P mají násobnost ≥ 2 . Označme navzájem různé nenulové kořeny $\lambda_1, \dots, \lambda_l$ a jejich násobnosti postupně $\gamma_1, \dots, \gamma_l$. Jak tedy doplnit soubor $(\lambda_1^n)_{n \geq 1}, \dots, (\lambda_l^n)_{n \geq 1}$ o dalších $k - l$ posloupností, aby vznikla báze prostoru M ?

Ke každému λ_i uvažujme následujících γ_i posloupností:

$$(\lambda_i^n)_{n \geq 1}, \quad (n\lambda_i^n)_{n \geq 1}, \quad (n^2\lambda_i^n)_{n \geq 1}, \quad \dots, (n^{\gamma_i-1}\lambda_i^n)_{n \geq 1}.$$

První, co je třeba dokázat, je fakt, že uvedené posloupnosti všechny patří do M , tedy že splňují rekurenci (2.4). To odvodíme následující úvahou o charakteristickém polynomu $P(\lambda)$. Zderivujeme-li polynom $\lambda^n P(\lambda)$ pro pevné $n \in \mathbb{N}$ podle proměnné λ , dostaneme

$$\begin{aligned} (\lambda^n P(\lambda))' &= (\lambda^{n+k} + \alpha_{k-1}\lambda^{n+k-1} + \dots + \alpha_1\lambda^{n+1} + \alpha_0\lambda^n)' = \\ &= (n+k)\lambda^{n+k-1} + \alpha_{k-1}(n+k-1)\lambda^{n+k-2} + \dots + \alpha_1(n+1)\lambda^n + \alpha_0n\lambda^{n-1} \end{aligned}$$

Když předchozí polynom vynásobíme λ , dostaneme

$$\lambda(\lambda^n P(\lambda))' = (n+k)\lambda^{n+k} + \alpha_{k-1}(n+k-1)\lambda^{n+k-1} + \dots + \alpha_1(n+1)\lambda^{n+1} + \alpha_0n\lambda^n. \quad (2.10)$$

Chceme-li ověřit, zda posloupnost $(n\lambda_i^n)_{n \geq 1}$ splňuje (2.4), stačí zjistit, zda polynom (2.10) má kořen λ_i . Pokud má polynom $P(\lambda)$ kořen λ_i násobnosti $\gamma_i \geq 2$, totéž platí i pro polynom $\lambda^n P(\lambda)$ (přibude jen n -násobný kořen 0). Vzhledem k poznámce 2.11, má polynom $(\lambda^n P(\lambda))'$ a tedy i $\lambda(\lambda^n P(\lambda))'$ kořen λ_i násobnosti $\gamma_i - 1 \geq 1$. Proto pro každé pevné $n \geq 1$ platí

$$(n+k)\lambda_i^{n+k} + \alpha_{k-1}(n+k-1)\lambda_i^{n+k-1} + \dots + \alpha_1(n+1)\lambda_i^{n+1} + \alpha_0n\lambda_i^n = 0,$$

což není nic jiného než dosazení posloupnosti $(n\lambda_i^n)_{n \geq 1}$ do (2.4). $(n\lambda_i^n)_{n \geq 1}$ proto patří do prostoru M .

Pro ověření $(n^2\lambda_i^n)_{n \geq 1} \in M$ uvažujeme polynom

$$\lambda\left(\lambda(\lambda^n P(\lambda))'\right)' = (n+k)^2\lambda^{n+k} + \alpha_{k-1}(n+k-1)^2\lambda^{n+k-1} + \dots + \alpha_1(n+1)^2\lambda^{n+1} + \alpha_0n^2\lambda^n,$$

který má kořen λ_i , právě když násobnost λ_i v polynomu $P(\lambda)$ je $\gamma_i \geq 3$.

Stejným způsobem bychom odvodili, že $(n^k\lambda_i^n)_{n \geq 1} \in M$ pro všechna $k = 0, \dots, \gamma_i - 1$. Zároveň vidíme, že posloupnost $(n^\gamma\lambda_i^n)_{n \geq 1}$ už rekurenci (2.4) nesplňuje.

Protože ke každému kořenu λ_i máme tolik posloupností, kolik je jeho násobnost, máme celkem $k = \sum_{i=1}^l \gamma_i$ posloupností jako kandidáty na bázi prostoru M . Nyní je třeba zjistit, zda jsou tyto posloupnosti lineárně nezávislé. Postup by byl obdobný jako v předcházejících případech, jen o poznání techničtější. Zapišme tedy, co jsme odvodili:

Tvrzení 2.14. *Nechť charakteristický polynom (2.5) lineární rekurence (2.4) má l navzájem různých kořenů $\lambda_1, \dots, \lambda_l$, násobností po řadě $\gamma_1, \dots, \gamma_l$. Pak každá posloupnost $(a_n)_{n \geq 1}$, která je řešením (2.4), je komplexní lineární kombinací posloupností*

$$(\lambda_i^n)_{n \geq 1}, \quad (n\lambda_i^n)_{n \geq 1}, \quad (n^2\lambda_i^n)_{n \geq 1}, \quad \dots, (n^{\gamma_i-1}\lambda_i^n)_{n \geq 1}, \quad i \in \{1, \dots, l\}. \quad (2.11)$$

2.2.3 Charakteristický polynom s komplexními kořeny

Příklad 2.15. Vyřešme rekurenci $a_{n+2} + 2a_{n+1} + 4a_n = 0$, $a_0 = a_1 = 1$. Charakteristický polynom $P(\lambda) = \lambda^2 + 2\lambda + 4$ má tentokrát dva navzájem komplexně sdružené kořeny $\lambda_{1,2} = -1 \pm i\sqrt{3}$. Naše posloupnost $(a_n)_{n \geq 0}$ je tedy lineární kombinací posloupností $(\lambda_i^n)_{n \geq 0}$, tedy musí existovat komplexní α, β tak, že pro každé $n \geq 0$ platí

$$a_n = \alpha(-1 + i\sqrt{3})^n + \beta(-1 - i\sqrt{3})^n.$$

Dosažením počátečních podmínek dostaneme soustavu lineárních rovnic

$$a_1 = 1 = \alpha + \beta, \quad a_2 = 1 = \alpha(-1 + i\sqrt{3}) + \beta(-1 - i\sqrt{3})$$

jejímž řešením je $\alpha = \frac{2+i\sqrt{3}}{2i\sqrt{3}} = \frac{3-2i\sqrt{3}}{6}$, $\beta = \frac{2-i\sqrt{3}}{-2i\sqrt{3}} = \frac{3+2i\sqrt{3}}{6}$. Máme proto následující vyjádření n -tého členu posloupnosti a_n :

$$a_n = \frac{3 - 2i\sqrt{3}}{6}(-1 + i\sqrt{3})^n + \frac{3 + 2i\sqrt{3}}{6}(-1 - i\sqrt{3})^n.$$

Vzhledem k tomu, že ze zadání je posloupnost $(a_n)_{n \geq 0}$ zjevně celočíselná, tento výsledek zapsaný pomocí komplexních čísel se nám moc nelíbí. Pokusme se tedy najít vyjádření pro a_n , které by používalo pouze reálná čísla. Protože $\lambda_2 = \overline{\lambda_1}$, je také $\lambda_2^n = \overline{\lambda_1^n} = \overline{\lambda_1}^n$. Protože také $\beta = \overline{\alpha}$, je a_n vlastně reálnou složkou výrazu $\frac{3-2i\sqrt{3}}{6}(-1 + i\sqrt{3})^n$. Pro její určení použijeme zápis komplexních čísel v goniometrickém tvaru a Moivreovu větu. Máme $-1 + i\sqrt{3} = 2(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 2(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3})$. Proto

$$(-1 + i\sqrt{3})^n = 2^n (\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3})^n = 2^n (\cos \frac{2\pi n}{3} + i \sin \frac{2\pi n}{3}).$$

Odtud odvodíme

$$a_n = 2\Re\left(\frac{3 - 2i\sqrt{3}}{6}(-1 + i\sqrt{3})^n\right) = 2^n \cos \frac{2\pi n}{3} + \frac{2^{n+1}}{\sqrt{3}} \sin \frac{2\pi n}{3}.$$

Toto vyjádření už nevyužívá komplexní jednotku. Čtenáře může napadnout, zda nelze pro ještě hezčí zápis a_n využít faktu, že posloupnosti $\sin \frac{2\pi n}{3}$ a $\cos \frac{2\pi n}{3}$ jsou periodické s periodou 3. Máme

$$\begin{aligned} \sin \frac{2\pi(3k)}{3} &= 0, & \sin \frac{2\pi(3k+1)}{3} &= \frac{\sqrt{3}}{2}, & \sin \frac{2\pi(3k+2)}{3} &= -\frac{\sqrt{3}}{2}, \\ \cos \frac{2\pi(3k)}{3} &= 1, & \cos \frac{2\pi(3k+1)}{3} &= -\frac{1}{2}, & \cos \frac{2\pi(3k+2)}{3} &= -\frac{\sqrt{3}}{2}, \end{aligned}$$

a proto

$$a_{3k} = 2^{3k}, \quad a_{3k+1} = -2^{3k} + 2^{3k+1} = 2^{3k}, \quad a_{3k+2} = -2^{3k+1} - 2^{3k+2} = -3 \cdot 2^{3k+1}.$$

Získáním takto jednoduchého vyjádření vyvstane otázka, jestli jsme si všechnu práci nemohli ušetřit a dospět k němu z rekurence rovnou. Jak se snado ukáže, toto možné bylo, pokud bychom provedli hned na začátku jednoduchý trik: Protože požadujeme platnost rekurence $a_{n+2} + 2a_{n+1} + 4a_n = 0$ pro každé n , napíšeme si tento vztah pod sebe pro dva po sobě jdoucí indexy,

$$a_{n+2} + 2a_{n+1} + 4a_n = 0,$$

$$a_{n+3} + 2a_{n+2} + 4a_{n+1} = 0.$$

Odečtením dvojnásobku první rovnice od druhé získáme vztah $a_{n+3} = 8a_n = 2^3 a_n$. S použitím počáteční podmínky $a_0 = 1$ odtud plyne $a_{3k} = 2^{3k}$, z podmínky $a_1 = 1$ odvodíme $a_{3k+1} = 2^{3k}$ a protože $a_2 = -2a_1 - 4a_0 = -6$, dostaneme také $a_{3k+2} = -6 \cdot 2^{3k} = -3 \cdot 2^{3k+1}$.

Ve skutečnosti každý polynom s reálnými koeficienty má s komplexním kořenem λ_0 za kořen i číslo $\bar{\lambda}_0$ komplexně sdružené, a to oba se stejnou násobností. Můžeme se stejně jako příkladu 2.15 ptát, zda řešení příslušné diferenční rovnice nelze zapsat pomocí reálné báze, tedy nahradit posloupnosti $(n^j \lambda_0^n)_{n \geq 1}$, $(n^j \bar{\lambda}_0^n)_{n \geq 1}$ dvěma jinými posloupnostmi v prostoru M , které by byly lineárně nezávislé. Využijeme následující tvrzení z lineární algebry.

Tvrzení 2.16. *Pokud $\vec{x}$, $\vec{y}$, $\vec{z}_1, \dots, \vec{z}_k$ je báze vektorového prostoru V nad $\mathbb{C}$, pak i $\frac{1}{2}(\vec{x} + \vec{y})$, $\frac{1}{2i}(\vec{x} - \vec{y})$, $\vec{z}_1, \dots, \vec{z}_k$ je báze vektorového prostoru V .*

Důkaz. Toto tvrzení dokážeme, když ověříme, že z lineární nezávislosti $\vec{x}$, $\vec{y}$, $\vec{z}_1, \dots, \vec{z}_k$ plyne lineární nezávislost $\frac{1}{2}(\vec{x} + \vec{y})$, $\frac{1}{2i}(\vec{x} - \vec{y})$, $\vec{z}_1, \dots, \vec{z}_k$. $\square$

Důsledek 2.17. *Nechť mezi kořeny charakteristického polynomu (2.5) lineární rekurence (2.4) jsou $\lambda_0 = r(\cos \varphi + i \sin \varphi)$, $\bar{\lambda}_0 = r(\cos \varphi - i \sin \varphi)$ s násobností γ_0 . Pak posloupnosti $(n^j \lambda_0^n)_{n \geq 1}$, $(n^j \bar{\lambda}_0^n)_{n \geq 1}$, $0 \leq j < \gamma_0$, v bázi (2.11) prostoru M lze nahradit posloupnostmi $(n^j r^n \cos n\varphi)_{n \geq 1}$, $(n^j r^n \sin n\varphi)_{n \geq 1}$, $0 \leq j < \gamma_0$.*

Důkaz. Máme

$$\begin{aligned} \frac{1}{2} \odot ((n^j \lambda_0^n)_{n \geq 1} \oplus (n^j \bar{\lambda}_0^n)_{n \geq 1}) &= \left(\frac{1}{2} (n^j \lambda_0^n + n^j \bar{\lambda}_0^n) \right)_{n \geq 1} = \\ &= \left(\Re(n^j \lambda_0^n) \right)_{n \geq 1} = \left(n^j \Re(\lambda_0^n) \right)_{n \geq 1} \\ \frac{1}{2i} \odot ((n^j \lambda_0^n)_{n \geq 1} \ominus (n^j \bar{\lambda}_0^n)_{n \geq 1}) &= \left(\frac{1}{2i} (n^j \lambda_0^n - n^j \bar{\lambda}_0^n) \right)_{n \geq 1} = \\ &= \left(\Im(n^j \lambda_0^n) \right)_{n \geq 1} = \left(n^j \Im(\lambda_0^n) \right)_{n \geq 1} \end{aligned}$$

Protože $\lambda_0 = r(\cos \varphi + i \sin \varphi)$, podle Moivreovy věty odvodíme $\lambda_0^n = r^n(\cos \varphi + i \sin \varphi)^n = r^n(\cos n\varphi + i \sin n\varphi)$, takže $\Re(\lambda_0^n) = r^n \cos n\varphi$ a $\Im(\lambda_0^n) = r^n \sin n\varphi$. $\square$

2.3 Lineární diferenční rovnice s pravou stranou

Podívejme se nyní na řešení lineární rekurence k -tého řádu s konstantními koeficienty ale nenulovou pravou stranou,

$$a_{n+k} + \alpha_{k-1}a_{n+k-1} + \alpha_{k-2}a_{n+k-2} + \cdots + \alpha_1a_{n+1} + \alpha_0a_n = f(n), \quad n \geq 1. \quad (2.12)$$

Přidruženým charakteristickým polynomem je polynom $P(\lambda) = \lambda^k + \alpha_{k-1}\lambda^{k-1} + \cdots + \alpha_1\lambda + \alpha_0$. Abychom naznačili obecný postup řešení nehomogenní diferenční rovnice, prozkoumejme nejprve na příkladě nejjednodušší případ pravé strany, kdy $f(n) \equiv 1$ je konstantní.

Příklad 2.18. Řešme diferenční rovnici druhého řádu s nenulovou pravou stranou,

$$a_{n+2} - 3a_{n+1} + 2a_n = 1. \quad (2.13)$$

Protože požadujeme platnost tohoto vztahu pro každé přirozené n , můžeme využít, že i $a_{n+3} - 3a_{n+2} + 2a_{n+1} = 1$. Odečtením obou rovností dostaneme

$$a_{n+3} - 4a_{n+2} + 5a_{n+1} - 2a_n = 0. \quad (2.14)$$

To už je homogenní diferenční rovnice, ovšem třetího řádu. Zkusme ji řešit metodou, kterou jsme se naučili. Charakteristický polynom (2.14) je

$$P(\lambda) = \lambda^3 - 4\lambda^2 + 5\lambda - 2 = (\lambda - 1)^2(\lambda - 2),$$

proto každé řešení (2.14) je lineární kombinací posloupností $(1)_{n \in \mathbb{N}}$, $(n)_{n \in \mathbb{N}}$ a $(2^n)_{n \in \mathbb{N}}$, a tedy n -tý člen je tvaru

$$a_n = \alpha + \beta n + \gamma 2^n, \quad \text{pro nějaké } \alpha, \beta, \gamma \in \mathbb{C}. \quad (2.15)$$

Je zřejmé, že pro jednoznačné určení řešení (2.13) stačí dvě počáteční podmínky, proto jistě ne každá trojice komplexních koeficientů α, β, γ povede k řešení původní rovnice. Dosadíme (2.15) do (2.13),

$$\begin{aligned} \alpha + \beta(n+2) + \gamma 2^{n+2} - 3(\alpha + \beta(n+1) + \gamma 2^{n+1}) + 2(\alpha + \beta n + \gamma 2^n) &= 1, \\ \underbrace{(1-3+2)}_{=0}\alpha + \underbrace{(n+2-3(n+1)+2n)}_{=-1}\beta + \underbrace{(2^{n+2}-3 \cdot 2^{n+1}+2 \cdot 2^n)}_{=0} &= 1, \end{aligned}$$

z čehož odvodíme $\beta = -1$. Obecným řešením rovnice (2.13) je tedy posloupnost $(a_n)_{n \geq 1}$, kde $a_n = \alpha - n + \gamma 2^n$.

Čtenáře možná už napadlo, proč závislost na parametrech α a γ zmizela. Je to tím, že právě posloupnosti tvaru $\alpha + \gamma 2^n$ jsou řešením rovnice (2.13) bez pravé strany. Charakteristickým polynomem je totiž $P(\lambda) = \lambda^2 - 3\lambda + 2 = (\lambda - 1)(\lambda - 2)$, takže příslušnou homogenní rovnici řeší všechny lineární kombinace posloupností $(1^n)_{n \geq 1}$ a $(2^n)_{n \geq 1}$. Z toho je vidět, že řešení nehomogenní rovnice (2.13) lze rozložit na součet řešení a_n^h přidružené homogenní rovnice a jednoho partikulárního řešení a_n^p k pravé straně. V našem případě $a_n = a_n^h + a_n^p$, kde $a_n^h = \alpha + \gamma 2^n$ a $a_n^p = -n$.

Snadno si uvědomíme, že linearita diferenční rovnice umožňuje rozklad na homogenní a partikulární řešení i v případě obecné pravé strany.

Tvrzení 2.19. *Nechť posloupnost $(a_n^p)_{n \geq 1}$ je libovolné řešení diferenční rovnice (2.12). Pak všechna řešení této rovnice najdeme ve tvaru $a_n = a_n^h + a_n^p$, $n \geq 1$, kde $(a_n^h)_{n \geq 1}$ je nějaké řešení přidružené homogení diferenční rovnice (2.4).*

Otázkou zůstává, jak nalézt nějaké partikulární řešení k dané pravé straně. Probereme několik typů posloupností $(f(n))_{n \geq 1}$, u kterých lze dát k hledání partikulárního řešení návod.

2.3.1 Polynomiální pravá strana

Prvním případem nenulové pravé strany pro nás byla konstantní posloupnost. Ukážeme si, že postup lze zobecnit. To, co se v příkladě 2.18 dělo, totiž nebylo náhodou.

Zkoumejme nyní obecnější případ, kdy na pravé straně diferenční rovnice bude polynom

$$f(n) = c_0 + c_1 n + \cdots + c_t n^t,$$

kde st $f = t \geq 0$, $c_0, \dots, c_t$ jsou obecně komplexní koeficienty a $c_t \neq 0$. Podíváme se, co se stane, když stejně jako v příkladě provedeme posunutí indexu a odečtení. Na pravé straně nové rekurence máme polynom

$$\begin{aligned} \tilde{f}(n) &:= f(n+1) - f(n) = c_0 + c_1(n+1) + \cdots + c_t(n+1)^t - (c_0 + c_1 n + \cdots + c_t n^t) = \\ &= c_1 + \cdots + c_{t-1}((n+1)^{t-1} - n^{t-1}) + c_t((n+1)^t - n^t) = \\ &= c_1 + \cdots + c_t(tn^{t-1} + \binom{t}{2}n^{t-2} + \cdots + tn + 1) \end{aligned}$$

Polynom $\tilde{f}$ je tedy stupně právě $t-1$, protože u nejvyšší mocniny n^{t-1} stojí koeficient $c_t \neq 0$. Situace je tedy zlepšila, nicméně abychom získali homogenní diferenční rovnici, budeme muset tento posun s odečtením znovu a znovu, celkem $(t+1)$ -krát. Po t krocích

dostaneme polynom stupně nula, tedy konstantu, po posledním, $(t + 1)$ -ním kroku bude na pravé straně opravdu nulový polynom.

Musíme ovšem vyzkoumat, co se při těchto operacích děje na levé straně rekurence. Už po jednom kroku tam stojí komplikovaný výraz

$$\begin{aligned} a_{n+k+1} + \alpha_{k-1}a_{n+k} + \cdots + \alpha_0a_{n+1} - (a_{n+k} + \alpha_{k-1}a_{n+k-1} + \cdots + \alpha_0a_n) = \\ = a_{n+k+1} + (\alpha_{k-1} - 1)a_{n+k} + (\alpha_{k-2} - \alpha_{k-1})a_{n+k-1} \cdots + (\alpha_0 - \alpha_1)a_n - \alpha_0a_n. \end{aligned} \quad (2.16)$$

Ve skutečnosti ale tento výraz zkoumat nepotřebujeme. Potřebujeme totiž znát jen charakteristický polynom $\tilde{P}$ přidružený k nové rovnici. Ten získáváme dosazením posloupnosti λ^n . Uvědomíme-li si, že posun v indexu pak znamená pouze vynásobí proměnnou λ , vidíme, že polynom $\tilde{P}(\lambda)$ vznikne odečtením původního charakteristického polynomu $P(\lambda)$ od jeho λ -násobku, tedy $\tilde{P}(\lambda) = \lambda P(\lambda) - P(\lambda) = (\lambda - 1)P(\lambda)$.

Jak jsme si řekli, operaci posunu indexu a odečtení potřebujeme provést $(t + 1)$ -krát. Na konci tak budeme mít homogenní diferenční rovnici

$$b_{n+k+t+1} + \tilde{\alpha}_{k+t}b_{n+k+t} + \cdots + \tilde{\alpha}_1b_{n+1} + \tilde{\alpha}_0b_0 = 0, \quad n \geq 1, \quad (2.17)$$

s charakteristickým polynomem $(\lambda - 1)^{t+1}P(\lambda)$. Řšení této nové homogenní rekurence umíme najít postupem z předchozích kapitol jako lineární kombinací posloupností získaných z kořenů polynomu $(\lambda - 1)^{t+1}P(\lambda)$. Označme $\lambda_1 = 1$ a nechť $r \geq 0$ je násobnost λ_1 jako kořene v původním polynomu $P(\lambda)$. Pak podprostor $\tilde{M}$ posloupností, které řeší homogenní rekurenci (2.17), má bázi

$$\begin{aligned} (1)_{n \geq 1}, \quad (n)_{n \geq 1}, \quad \dots \quad (n^{r-1})_{n \geq 1}, \quad (n^r)_{n \geq 1}, \quad \dots, \quad (n^{r+t})_{n \geq 1}, \\ (\lambda_i^n)_{n \geq 1}, \quad (n\lambda_i^n)_{n \geq 1}, \quad \dots \quad (n^{\gamma_i-1}\lambda_i^n)_{n \geq 1}, \quad i \in \{2, \dots, l\}. \end{aligned} \quad (2.18)$$

Poznamenejme, že pokud polynom P neměl kořen $\lambda_1 = 1$, pak $(1)_{n \geq 1}, (n)_{n \geq 1}, \dots, (n^{r-1})_{n \geq 1}$ je prázdný seznam.

Odvodili jsme, že každé řešení nehomogenní diferenční rovnice (2.12) je řešením homogenní rovnice (2.17). Naopak to ovšem neplatí. Ne každá lineární kombinace prvků báze (2.18) prostoru $\tilde{M}$ splňuje rovnici (2.12). Posloupnosti $(n^r)_{n \geq 1}, \dots, (n^{r+t})_{n \geq 1}$ jsou v bázi $\tilde{M}$ díky faktoru $(\lambda - 1)^{t+1}$ polynomu $\tilde{P}(\lambda)$. Zbytek uvedených posloupností tedy tvoří bázi prostoru M všech řešení homogenní diferenční rovnice přidružené k původní rovnici (2.12). Každá jejich lineární kombinace proto odpovídá homogennímu řešení $(a_n^h)_{n \geq 1}$. Naopak lineární kombinací posloupností $(n^r)_{n \geq 1}, \dots, (n^{r+t})_{n \geq 1}$ získáme partikulární řešení k dané pravé straně. Toto partikulární řešení je ve tvaru

$$a_n^p = d_0n^r + d_1n^{r+1} + \cdots + d_tn^{r+t} = n^r(d_0 + d_1n + \cdots + d_tn^t), \quad n \geq 1.$$

Koeficienty $d_0, \dots, d_t$ zjistíme dosazením $(a_n^p)_{n \geq 1}$ do (2.12). Shrňme uvedené poznatky do tvrzení.

Tvrzení 2.20. *Je-li pravá strana $(f(n))_{n \geq 1}$ diferenční rovnice (2.12) dána polynomem $f(n)$ stupně $t \geq 0$, pak partikulární řešení rovnice (2.12) je ve tvaru $a_n^p = n^r g(n)$, kde $r \geq 0$ je násobnost kořene $\lambda = 1$ v charakteristickém polynomu $P(\lambda)$ přidružené homogenní diferenční rovnice a $g(n)$ je nějaký polynom stupně $\text{st}(g) = \text{st}(f) = t$.*

Příklad 2.21. Metodu použijeme k výpočtu sumy $\sum_{k=1}^n k^2$ ještě jiným způsobem než v příkladu 1.5. Označíme-li například $S_n := \sum_{k=1}^n k^2$, snadno získáme pro posloupnost $(S_n)_{n \geq 1}$ rekurentní vztah $S_{n+1} - S_n = (n+1)^2$. Protože $\sum_{k=1}^1 k^2 = 1$, součtem naší sumy je tedy právě řešení této rekurence s počáteční podmínkou $S_1 = 1$. Řešení homogenní soustavy $S_{n+1}^h - S_n^h = 0$ jsou samozřejmě konstantní posloupnosti, $S_n^h = \alpha \in \mathbb{C}$. Abychom určili partikulární řešení, uvědomíme si, že na pravé straně rekurence je polynom stupně $t = 2$, a charakteristický polynom rekurence $P(\lambda) = \lambda - 1$ má kořen 1 násobnosti $r = 1$. Proto partikulární řešení hledáme ve tvaru $S_n^p = n(d_0 + d_1 n + d_2 n^2)$. Koeficienty d_0, d_1, d_2 získáme dosazením do rekurence s pravou stranou,

$$\begin{aligned} S_{n+1}^p - S_n^p &= (n+1)(d_0 + d_1(n+1) + d_2(n+1)^2) - n(d_0 + d_1 n + d_2 n^2) = \\ &= d_0 + d_1(2n+1) + d_2(3n^2 + 3n + 1) = (n+1)^2. \end{aligned}$$

Protože potřebujeme rovnost pro všechna $n \geq 1$, stačí porovnat koeficienty u jednotlivých mocnin n .

$$\begin{array}{ll} n^0 : & d_0 + d_1 + d_2 = 1 \\ n^1 : & 2d_1 + 3d_2 = 2 \\ n^2 : & 3d_2 = 1 \end{array}$$

To je soustava tří lineárních rovnic o třech neznámých d_0, d_1, d_2 , kterou snadno vyřešíme. Řešením je trojice

$$d_2 = \frac{1}{3}, \quad d_1 = \frac{1}{2}, \quad d_0 = \frac{1}{6}.$$

Partikulární řešení proto nacházíme ve tvaru $S_n^p = n(\frac{1}{6} + \frac{1}{2}n + \frac{1}{3}n^2) = \frac{1}{6}(2n^3 + 3n^2 + n)$. Obecné řešení rekurence $S_{n+1} - S_n = (n+1)^2$ je tedy $S_n = S_n^h + S_n^p = \alpha + \frac{1}{6}(2n^3 + 3n^2 + n)$. Koeficient α , který odpovídá právě řešení udávajícímu součet sumy $\sum_{k=1}^n k^2$, vypočítáme dosazením počáteční podmínky $S_1 = 1$. Máme $S_1 = 1 = \alpha + \frac{1}{6}(2 + 3 + 1)$, takže $\alpha = 0$. Můžeme tedy uzavřít, že $\sum_{k=1}^n k^2 = \frac{1}{6}(2n^3 + 3n^2 + n)$, což samozřejmě odpovídá výsledku z příkladu 1.5.

2.3.2 Kvazipolynomiální pravá strana

Uvažujme ještě obecnější pravou stranu diferenční rovnice ve tvaru tzv. kvazipolynomu, tj. $f(n) = C^n p(n)$, kde $p(n)$ je polynom a $0 \neq C \in \mathbb{C}$. Podívejme se, jakým způsobem řešení úlohy převedeme na známý případ. Vydělíme-li celou rovnici

$$a_{n+k} + \alpha_{k-1}a_{n+k-1} + \cdots + \alpha_1 a_{n+1} + \alpha_0 a_n = C^n p(n). \quad (2.19)$$

číslem C^{n+k} , dostaneme při šikovném zápisu

$$\frac{a_{n+k}}{C^{n+k}} + \frac{\alpha_{k-1}}{C} \frac{a_{n+k-1}}{C^{n+k-1}} + \cdots + \frac{\alpha_1}{C^{k-1}} \frac{a_{n+1}}{C^{n+1}} + \frac{\alpha_0}{C^k} \frac{a_n}{C^n} = \frac{p(n)}{C^k}.$$

Zavedeme-li novou posloupnost $\tilde{a}_n = \frac{a_n}{C^n}$, získali jsme vlastně diferenční rovnici

$$\tilde{a}_{n+k} + \tilde{\alpha}_{k-1}\tilde{a}_{n+k-1} + \cdots + \tilde{\alpha}_1\tilde{a}_{n+1} + \tilde{\alpha}_0\tilde{a}_n = \tilde{p}(n). \quad (2.20)$$

s koeficienty $\tilde{\alpha}_j = C^{j-k}\alpha_j$, $j \in \{0, \dots, k-1\}$, a na pravé straně je polynom $\tilde{p}(n) = C^{-k}p(n)$. (Je třeba si uvědomit, že k je pevné, je to řád diferenční rovnice.) Vyřešíme rekurenci (2.20) postupem výše uvedeným, kde $\tilde{a}_n = \tilde{a}_n^h + \tilde{a}_n^p$. Řešení diferenční rovnice (2.19) dostaneme ve tvaru

$$a_n = C^n \tilde{a}_n = C^n \tilde{a}_n^h + C^n \tilde{a}_n^p. \quad (2.21)$$

Zkoumejme vztah dvou výše uvedených rekurencí (2.19) a (2.20). Charakteristický polynom homogenní rekurence přidružené k (2.19) označme $P(\lambda)$, polynom příslušný k (2.20) označme $\tilde{P}(\lambda)$. Podle poznámky 2.11 jsou kořeny $\tilde{\lambda}_i$ polynomu $\tilde{P}$ jen C^{-1} -násobky kořenů polynomu $P(\lambda)$, tj. $C^{-1}\lambda_i$. Proto víme, že když

$$(\lambda_i^n)_{n \geq 1}, (n\lambda_i^n)_{n \geq 1}, \dots, (n^{\gamma_i-1}\lambda_i^n)_{n \geq 1}, \quad i \in \{1, \dots, l\}.$$

je báze prostoru řešení původní homogenní rovnice přidružené k (2.19), pak bázi

$$(\tilde{\lambda}_i^n)_{n \geq 1}, (n\tilde{\lambda}_i^n)_{n \geq 1}, \dots, (n^{\gamma_i-1}\tilde{\lambda}_i^n)_{n \geq 1}, \quad i \in \{1, \dots, l\},$$

prostoru řešení homogenní rovnice přidružené k (2.20) lze zapsat pomocí kořenů polynomu $P(\lambda)$ jako

$$(C^{-n}\lambda_i^n)_{n \geq 1}, (nC^{-n}\lambda_i^n)_{n \geq 1}, \dots, (n^{\gamma_i-1}C^{-n}\lambda_i^n)_{n \geq 1}, \quad i \in \{1, \dots, l\}.$$

Odvodíme tak, že $C^n \tilde{a}_n^h$ ve vztahu (2.21) je vlastně řešením a_n^p homogenní rovnice přidružené k (2.19). Partikulární řešení a_n^p získáme jako $a_n^p = C^n \tilde{a}_n^p$. Připomeňme, že $\tilde{a}_n^p$ jsme podle předpisu z tvrzení 2.20 hledali ve tvaru $\tilde{a}_n^p = n^r g(n)$, kde $g(n)$ je polynom stupně $\text{st}g = \text{st}\tilde{p} = \text{st}p$ a r je násobnost kořene 1 v polynomu $\tilde{P}$. Ta je ale stejná jako násobnost kořene C v polynomu P . Odvodili jsme tak následující tvrzení.

Tvrzení 2.22. Je-li pravá strana $(f(n))_{n \geq 1}$ diferenční rovnice (2.12) dána kvazipolynommem $f(n) = C^n p(n)$, kde $0 \neq C \in \mathbb{C}$ a p je polynom stupně $t \geq 0$, pak partikulární řešení rovnice (2.12) je ve tvaru $a_n^p = C^n n^r g(n)$, kde $r \geq 0$ je násobnost kořene $\lambda = C$ v charakteristickém polynomu $P(\lambda)$ přidružené homogenní diferenční rovnice a $g(n)$ je nějaký polynom stupně $\text{st}(g) = \text{st}(f) = t$.

Příklad 2.23. Vypočítáme součet $\sum_{k=1}^n (-1)^k k^2$. Obdobně jako v příkladu 2.21 označíme $S_n = \sum_{k=1}^n (-1)^k k^2$. Posloupnost $(S_n)_{n \geq 1}$ splňuje rekurenci $S_{n+1} - S_n = (-1)^{n+1} (n+1)^2$. Řešení bude dáno jednoznačně, pokud zadáme počáteční podmínku $S_1 = -1$. Obecné řešení této rekurence s kvazipolynomiální pravou stranou je součtem obecného řešení homogenní rovnice, což je opět $S_n^h = \alpha$ a partikulárního řešení S_n^p . Podle tvrzení 2.22 lze partikulární řešení hledat ve tvaru $S_n^p = C^n n^r g(n)$, kde $C = -1$, r je násobnost kořene -1 v polynomu $P(\lambda) = \lambda - 1$, tj. $r = 0$. Polynom g je stupně stejného jako $(n+1)^2$, tj. $\text{st}g = 2$. Je tedy $S_n^p = (-1)^n (d_0 + d_1 n + d_2 n^2)$. Koeficienty d_0, d_1, d_2 zjistíme, když S_n^p dosadíme do původní rekurence s pravou stranou.

$$\begin{aligned} S_{n+1}^p - S_n^p &= (-1)^{n+1} (d_0 + d_1(n+1) + d_2(n+1)^2) - (-1)^n (d_0 + d_1 n + d_2 n^2) = \\ &= (-1)^{n+1} (2d_0 + d_1(2n+1) + d_2(2n^2 + 2n + 1)) = (-1)^{n+1} (n+1)^2. \end{aligned}$$

Porovnáme koeficienty u jednotlivých mocnin n ,

$$\begin{aligned} n^0 : \quad & 2d_0 + d_1 + d_2 = 1 \\ n^1 : \quad & 2d_1 + 2d_2 = 2 \\ n^2 : \quad & 2d_2 = 1 \end{aligned}$$

Řešením této soustava rovnic je trojice

$$d_2 = \frac{1}{2}, \quad d_1 = \frac{1}{2}, \quad d_0 = 0.$$

Partikulární řešení proto nacházíme ve tvaru $S_n^p = (-1)^n (\frac{1}{2}n + \frac{1}{2}n^2) = \frac{(-1)^n}{2} (n^2 + n)$. Obecné řešení rekurence $S_{n+1} - S_n = (-1)^{n+1} (n+1)^2$ je tedy $S_n = S_n^h + S_n^p = \alpha + \frac{(-1)^n}{2} (n^2 + n)$. Koeficient α , který odpovídá právě řešení udávajícímu součet sumy $\sum_{k=1}^n (-1)^k k^2$, vypočítáme dosazením počáteční podmínky $S_1 = -1$. Máme $S_1 = -1 = \alpha + \frac{-1}{2} (1 + 1) = \alpha - 1$, takže opět $\alpha = 0$. Můžeme tedy uzavřít, že $\sum_{k=1}^n (-1)^k k^2 = \frac{(-1)^n}{2} (n^2 + n)$.

Příklad 2.24. Sečtěme sumu $\sum_{k=1}^n k \binom{n}{k}$. Tentokrát už samotné sestavení rekurence není úplně přímočaré. Označíme-li opět $S_n = \sum_{k=1}^n k \binom{n}{k}$, pak $S_{n+1} = \sum_{k=1}^{n+1} k \binom{n+1}{k}$. Když chceme vyjádřit S_{n+1} pomocí předchozích členů posloupnosti, použijeme identitu $\binom{n+1}{k} =$

$\binom{n}{k} + \binom{n}{k-1}$, která platí pro $1 \leq k \leq n$. Je proto

$$\begin{aligned} S_{n+1} &= \sum_{k=1}^{n+1} k \binom{n+1}{k} = \sum_{k=1}^n k \binom{n+1}{k} + (n+1) \binom{n+1}{n+1} = \sum_{k=1}^n k \left(\binom{n}{k} + \binom{n}{k-1} \right) + n+1 = \\ &= \sum_{k=1}^n k \binom{n}{k} + \sum_{k=1}^n k \binom{n}{k-1} + n+1 = \sum_{k=1}^n k \binom{n}{k} + \sum_{k=0}^{n-1} (k+1) \binom{n}{k} + n+1 = \\ &= 2 \sum_{k=1}^n k \binom{n}{k} + \sum_{k=0}^n \binom{n}{k} = 2S_n + 2^n, \end{aligned}$$

kde jsme využili, že $\binom{n}{n} = 1$ a $\sum_{k=0}^n \binom{n}{k} = 2^n$. Odvodili jsme tedy rekurenci

$$S_{n+1} - 2S_n = 2^n, \quad S_1 = 1.$$

Víme, že $S_n = S_n^h + S_n^p$. Protože charakteristický polynom přidružené homogenní rovnice je $P(\lambda) = \lambda - 2$, je obecné řešení $S_n^h = \alpha \cdot 2^n$. Partikulární řešení hledáme ve tvaru $S_n^p = 2^n n d_0$. Dosazením do rekurence zjistíme

$$S_{n+1}^p - 2S_n^p = 2^{n+1}(n+1)d_0 - 2^n n d_0 = 2^n,$$

odkud snadno odvodíme, že $2d_0 = 1$, tudíž $d_0 = \frac{1}{2}$. Je tedy $S_n = S_n^h + S_n^p = \alpha \cdot 2^n + 2^{n-1}n$.

S využitím počáteční podmínky máme $S_1 = 1 = 2\alpha + 1$, takže $\alpha = 0$. Celkově tedy $\sum_{k=1}^n k \binom{n}{k} = 2^{n-1}n$.

Tento příklad ovšem zaslouží drobný komentář. Ke stejnému výsledku bychom totiž mohli dojít na základě jednoduché kombinatorické úvahy. Zjistíme počet možností, jak ze třídy o n žácích vybrat výbor s předsedou. Při pevném k je počet různých k -členných komisí v n -členné třídě roven $\binom{n}{k}$. V každé z těchto komisí máme k možností výběru předsedy. Proto $k \binom{n}{k}$ je počet k -členných komisí s předsedou. Abychom získali počet všech možností, musíme sečíst přes $1 \leq k \leq n$. Naše suma $\sum_{k=1}^n k \binom{n}{k}$ tedy označuje počet různých komisí s předsedou v n -členné třídě. Stejný počet ovšem zjistíme, když nejprve určíme ve třídě předsedu - tu máme n možností. Pak komisi libovolně doplníme, a to tak, že každému ze zbývajících $n-1$ žáků řekneme, jestli v komisi bude nebo ne. To provedeme 2^{n-1} způsoby. Celkem $n2^{n-1}$.

2.3.3 Algebraický přístup

Na problém řešení lineárních diferenčních rovnic lze nahlédnout ještě více algebraicky.

Uvažujme operátor A na prostoru ℓ , zadaný předpisem

$$A(a_n)_{n \geq 1} = (a_{n+k} + \alpha_{k-1}a_{n+k-1} + \cdots + \alpha_1 a_{n+1} + \alpha_0 a_n)_{n \geq 1}.$$

Snadno ověříme, že tento operátor je lineární, totiž že pro dvě komplexní posloupnosti $(a_n)_{n \geq 1}$, $(b_n)_{n \geq 1}$ a komplexní číslo α platí $A(\alpha(a_n)_{n \geq 1} + (b_n)_{n \geq 1}) = \alpha A(a_n)_{n \geq 1} + A(b_n)_{n \geq 1}$.

Řešení diferenční rovnice (2.12) je vlastně hledání posloupnosti $(a_n)_{n \geq 1}$ takové, že $A(a_n)_{n \geq 1} = (f(n))_{n \geq 1}$. Z lineární algebry víme, že množina všech řešení takové rovnice, tj. množina $A^{-1}((f(n))_{n \geq 1})$ má tvar

$$A^{-1}((f(n))_{n \geq 1}) = (a_n^p)_{n \geq 1} + \ker A,$$

kde posloupnost $(a_n^p)_{n \geq 1}$ splňuje $A(a_n^p)_{n \geq 1} = (f(n))_{n \geq 1}$ je nějaké partikulární řešení a $\ker A = A^{-1}((0)_{n \geq 1})$ je jádro operátoru A , tj. množina všech řešení homogenní rovnice (2.4). My jsme již dříve viděli, že $\ker A = M$ je podprostor prostoru ℓ . Množina všech řešení nehomogenní rovnice (2.12) je tedy lineární varieta v ℓ .

Předpokládejme, že je dáno více pravých stran $(f_i(n))_{n \geq 1}$, pro $i \in \{1, \dots, m\}$, a k nim partikulární řešení $(a_n^{p,i})_{n \geq 1}$, tj. takové posloupnosti, že $A(a_n^{p,i})_{n \geq 1} = (f_i(n))_{n \geq 1}$. Protože operátor A je lineární je množina řešení rovnice

$$A(a_n)_{n \geq 1} = (f_1(n))_{n \geq 1} + (f_2(n))_{n \geq 1} + \dots + (f_m(n))_{n \geq 1}$$

rovna

$$\begin{aligned} A^{-1}\left((f_1(n))_{n \geq 1} \oplus \dots \oplus (f_m(n))_{n \geq 1}\right) &= A^{-1}\left((f_1(n))_{n \geq 1} \oplus \dots \oplus A^{-1}((f_m(n))_{n \geq 1})\right) = \\ &= (a_n^{p,1})_{n \geq 1} \oplus \dots \oplus (a_n^{p,m})_{n \geq 1} + \ker A. \end{aligned}$$

Pravou stranu lineární diferenční rovnice (2.12) si tedy můžeme rozložit na součet dílčích pravých stran tak, aby se nám snáze hledala partikulární řešení. Tuto myšlenku posléze využijeme.

2.3.4 Pravá strana $\sin(n\gamma)$, $\cos(n\gamma)$

Posledním případem pravé strany, kterým se budeme zabývat, jsou posloupnosti typu $(\sin n\varphi g(n))_{n \geq 1}$, $(\cos n\varphi g(n))_{n \geq 1}$, kde $\varphi \in \mathbb{R}$ a g je nějaký polynom. Ve skutečnosti je tento případ snadno převoditelný na předchozí úlohu. Stačí si totiž uvědomit vzorce

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}, \quad \cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \text{pro } z \in \mathbb{C}.$$

Příklad 2.25. Řešte rekurenci $a_{n+1} - 3a_n = 2^n \cos \frac{n\pi}{3}$. Řešením homogenní rovnice je $a_n^h = \alpha 3^n$. Protože $\cos \frac{n\pi}{3} = \frac{1}{2}(e^{\frac{n\pi i}{3}} + e^{-\frac{n\pi i}{3}})$, můžeme hledat partikulární řešení jako součet posloupností $(a_n^{p,1})$, $(a_n^{p,2})$, pro které

$$a_{n+1}^{p,1} - 3a_n^{p,1} = 2^{n-1}e^{\frac{n\pi i}{3}}, \quad a_{n+1}^{p,2} - 3a_n^{p,2} = 2^{n-1}e^{-\frac{n\pi i}{3}}.$$

Tyto rekurence už mají pravé strany ve tvaru (navzájem komplexně sdružených) kvazipolynomů $\frac{1}{2}(2e^{\pm \frac{\pi i}{3}})^n$. Protože stupeň polynomu je $t = 0$ a násobnost konstanty $K = 2e^{\pm \frac{\pi i}{3}}$ jako kořene charakteristického polynomu je $r = 0$, partikulární řešení hledáme ve tvaru $a_n^{p,1} = d_1(2e^{\frac{\pi i}{3}})^n$, $a_n^{p,2} = d_2(2e^{-\frac{\pi i}{3}})^n$. Dosazení provedeme pro $a_n^{p,1}$,

$$a_{n+1}^{p,1} - 3a_n^{p,1} = d_1(2e^{\frac{\pi i}{3}})^{n+1} - 3d_1(2e^{\frac{\pi i}{3}})^n = d_1(2e^{\frac{\pi i}{3}})^n(2e^{\frac{\pi i}{3}} - 3) = 2^{n-1}e^{\frac{n\pi i}{3}},$$

odkud snadno plyne $d_1 = \frac{1}{2(2e^{\frac{\pi i}{3}} - 3)}$. Podobně odvodíme, že $d_2 = \frac{1}{2(2e^{-\frac{\pi i}{3}} - 3)}$. I partikulární řešení jsou tedy k sobě navzájem komplexně sdružená, takže $a_n^p = a_n^{p,1} + a_n^{p,2} = 2\Re a_n^{p,1}$.

Protože

$$d_1 = \frac{1}{2(2e^{\frac{\pi i}{3}} - 3)} \frac{2e^{-\frac{\pi i}{3}} - 3}{2e^{-\frac{\pi i}{3}} - 3} = \frac{2e^{-\frac{\pi i}{3}} - 3}{14},$$

vypočítáme

$$\begin{aligned} a_n^p &= 2\Re \frac{2e^{-\frac{\pi i}{3}} - 3}{14} (2e^{\frac{\pi i}{3}})^n = \frac{2^n}{7} \Re(2e^{-\frac{\pi i}{3}} - 3)e^{\frac{n\pi i}{3}} = \\ &= \frac{2^n}{7} (2 \cos \frac{\pi}{3} - 2i \sin \frac{\pi}{3} - 3) (\cos \frac{n\pi}{3} + i \sin \frac{n\pi}{3}) = \frac{2^n}{7} (-2 - i\sqrt{3}) (\cos \frac{n\pi}{3} + i \sin \frac{n\pi}{3}) = \\ &= \frac{2^n}{7} (-2 \cos \frac{n\pi}{3} + \sqrt{3} \sin \frac{n\pi}{3}) = -\frac{2^{n+1}}{7} \cos \frac{n\pi}{3} + \frac{2^n \sqrt{3}}{7} \sin \frac{n\pi}{3} \end{aligned}$$

Celkové řešení původní rekurence získáme součtem tohoto partikulárního řešení s řešením homogenní rovnice, tj.

$$a_n = \alpha 3^n - \frac{2^{n+1}}{7} \cos \frac{n\pi}{3} + \frac{2^n \sqrt{3}}{7} \sin \frac{n\pi}{3}.$$

3 Příklady jiných diferenčních rovnic

3.1 Rekurence s nekonstantními koeficienty

Příklad 3.1. Vyřešme rekurenci

$$a_{n+1} = n(a_n + a_{n-1} + \cdots + a_1), \quad n \geq 2, \quad a_1 = 1.$$

Na první pohled je to rekurence, která nezapadá do našeho standardu. Provedeme-li ale jednoduchý trik, na známý případ ji převedeme. Stačí totiž označit $s_n = a_1 + \cdots + a_n$. Pak a_{n+1} je rovno rozdílu $s_{n+1} - s_n = a_{n+1}$, takže platí $s_{n+1} - s_n = ns_n$. Přepsáno ve standardním tvaru $s_{n+1} - (n+1)s_n = 0$. Vidíme, že to je jednoduchá homogenní rekurence prvního řádu, a i když má nekonstantní koeficient, snadno odvodíme, že $s_n = n!s_1$. Protože $s_1 = a_1 = 1$, je $s_n = n!$ a odtud pro $n \geq 2$

$$a_n = s_n - s_{n-1} = n! - (n-1)! = (n-1)(n-1)!.$$

Příklad 3.2. Řešme homogenní lineární rekurenci druhého řádu s nekonstantními koeficienty,

$$2a_{n+2} + 2na_{n+1} + n(n-1)a_n = 0, \quad n \geq 2.$$

Tvar nekonstantních koeficientů v této rekurenci může směřovat k nápadu, abychom celou rovnici vydělili $n!$. Potom

$$2\frac{a_{n+2}}{n!} + 2\frac{n}{n} \frac{a_{n+1}}{(n-1)!} + \frac{n(n-1)}{n(n-1)} \frac{a_n}{(n-2)!} = 0, \quad n \geq 2.$$

Po substituci $b_n = \frac{a_n}{(n-2)!}$ pro $n \geq 2$ máme

$$2b_{n+2} + 2b_{n+1} + b_n = 0, \quad n \geq 2,$$

což už je homogenní rekurence druhého řádu s konstantními koeficienty. K dořešení stačí určit kořeny charakteristického polynomu $2\lambda^2 + 2\lambda + 1$. Těmi jsou navzájem komplexně

sdružená čísla $\frac{1}{2} \pm \frac{i}{2}$. Abychom dostali řešení vyjádřeno jako lineární kombinaci reálných posloupností, použijeme postup z důsledku 2.17, zapíšeme číslo $\frac{1}{2} + \frac{i}{2}$ v goniometrickém tvaru

$$\frac{1}{2} + \frac{i}{2} = \frac{1}{\sqrt{2}} \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right) = \frac{1}{\sqrt{2}} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right).$$

Odtud $b_n = \alpha \frac{1}{\sqrt{2}^n} \cos \frac{\pi n}{4} + \beta \frac{1}{\sqrt{2}^n} \sin \frac{\pi n}{4}$. Přejdeme-li zpět k posloupnosti a_n , máme

$$a_n = \alpha \frac{(n-2)!}{\sqrt{2}^n} \cos \frac{\pi n}{4} + \beta \frac{(n-2)!}{\sqrt{2}^n} \sin \frac{\pi n}{4}, \quad n \geq 2.$$

Příklad 3.3. Řešme rekurenci

$$r_n - (n-1)r_{n-1} - (n-1)r_{n-2} = 0, \quad n \geq 2, \quad (3.1)$$

s počátečními podmínkami $r_0 = 1$, $r_1 = 0$. To je homogenní lineární rekurence druhého řádu, ovšem s nekonztantními koeficienty. Trik z příkladu 3.2 tady nevede k cíli, jak si čtenář může sám vyzkoušet. Zadááme-li se na rovnici pečlivě, všimneme si, že lze snadno přepsat do tvaru

$$r_n - nr_{n-1} = -(r_{n-1} - (n-1)r_{n-2}).$$

Označíme-li $s_n = r_n - nr_{n-1}$, dostáváme jednoduchý vztah pro posloupnost $(s_n)_{n \geq 1}$, totiž $s_n = -s_{n-1}$. Zkušené oko okamžitě zjistí, že obecné řešení této rovnice je $s_n = (-1)^n c$. Konstantu c můžeme zjistit z počátečních podmínek, protože $s_1 = -c = r_1 - r_0 = -1$, tudíž $c = 1$. Zbývá tedy určit, jak pomocí s_n zjistíme r_n . Dosazením máme pro $n \geq 1$

$$r_n - nr_{n-1} = (-1)^n.$$

Zavzpomínáme na kapitolu 1.1, kde jsme viděli, jak řešit libovolnou lineární rekurenci prvního řádu. Pro jednoduchost označme posloupnost $t_n = \frac{r_n}{n!}$, pro kterou máme $t_n - t_{n-1} = \frac{(-1)^n}{n!}$ pro $n \geq 1$. S použitím $t_0 = r_0 = 1$ snadno odvodíme, že $t_n = \sum_{k=0}^n \frac{(-1)^k}{k!}$, odkud dále

$$r_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}. \quad (3.2)$$

Tím jsme získali vyjádření pro n -tý člen posloupnosti $(r_n)_{n \geq 0}$ bez použití předcházejících členů této posloupnosti. Úplně spokojení ale zatím nejsme, protože bychom nejraději měli vztah pro n pomocí konečného počtu elementárních operací. Vypomůžeme si následující úvahou: Výraz (3.2) nám může připomenout Taylorův rozvoj funkce $e^x = \sum_{k=0}^{+\infty} \frac{x^k}{k!}$. Pro $x = -1$ je tedy $\sum_{k=0}^n \frac{(-1)^k}{k!} = e^{-1}$. V rovnosti (3.2) ovšem máme pouze konečnou sumu. Protože rozvoj řada $\sum_{k=0}^n \frac{(-1)^k}{k!}$ má členy se střídavými znaménky, odhadneme chybu

$$\left| \sum_{k=0}^n \frac{(-1)^k}{k!} - e^{-1} \right| < \frac{1}{(n+1)!},$$

takže po vynásobení $n!$ dostáváme

$$|r_n - n!e^{-1}| = \left| n! \sum_{k=0}^n \frac{(-1)^k}{k!} - n!e^{-1} \right| < \frac{1}{n+1} \leq \frac{1}{2}. \quad (3.3)$$

Na závěr si uvědomíme, že všechny členy posloupnosti $(r_n)_{n \geq 0}$ jsou ze zadání nutně celočíselné, tudíž r_n lze podle (3.3) určit jako nejbližší celé číslo k číslu $n!e^{-1}$. To lze ekvivalentně zapsat pomocí celé části,

$$r_n = \left\lfloor n!e^{-1} + \frac{1}{2} \right\rfloor. \quad (3.4)$$

3.2 Invertovací formule

Zkoumejme následující úlohu: Na konci školního roku si děti ve třídě chtějí vzájemně dávat dárky. Protože jsou ale některé děti oblíbenější než jiné, aby to těm druhým nebylo líto, učitelka rozhodla, že budou losovat, kdo komu dárek donese. Kolika způsoby může losování dopadnout?

Losování odpovídá permutacím na množině $\{1, 2, \dots, n\}$, kde n je počet dětí ve třídě. Je ale jasné, že při losování nechceme, aby dítě mělo donést dárek samo sobě, takže vyloučíme ty permutace π , kdy pro nějaké $1 \leq i \leq n$ platí $\pi(i) = i$. Takové permutace můžeme nazvat permutace bez pevného bodu. Jejich počet označme d_n .

Pro malá n určíme d_n přímo. Zjevně

$$d_1 = 0, \quad d_2 = 1, \quad d_3 = 2,$$

protože jediná permutace jednoho prvku je identita, na dvou prvcích už máme jednu transpozici, a na třech prvcích cyklické permutace (231) a (312). Zbylé čtyři permutace na $\{1, 2, 3\}$ jsou identita a tři transpozice, kde pevným bodem je postupně $i = 1$, $i = 2$ a $i = 3$. Zkusme odvodit počet d_n obecně. Roztřídíme všechny permutace na $\{1, 2, \dots, n\}$, kterých je $n!$, do tříd podle toho, kolik mají pevných bodů. Hledané číslo d_n označuje počet těch, které nemají žádný pevný bod. Těch, které mají pevný bod právě jeden, je nd_{n-1} . Je totiž n způsobů, jak zvolit pevný bod, a pak d_{n-1} způsobů, jak zamíchat ostatní prvky množiny $\{1, 2, \dots, n\}$. Obdobně $\binom{n}{2}d_{n-2}$ je počet prmutací s právě dvěma pevnými body. Můžeme tedy zapsat

$$n! = d_n + nd_{n-1} + \binom{n}{2}d_{n-2} + \dots + \binom{n}{n-2}d_2 + \binom{n}{n-1}d_1 + 1,$$

kde poslední jednička zastupuje jedinou permutaci, kdy jsou pevnými body všechny prvky množiny $\{1, 2, \dots, n\}$, a to identitu. Dodefinujeme-li $d_0 = 1$, pak tento vztah lze přepsat

na

$$n! = \sum_{i=0}^n \binom{n}{i} d_{n-i}. \quad (3.5)$$

Takový vztah je vlastně taky rekurencí pro posloupnost $(d_n)_{n \geq 0}$, naše úvahy o lineárních diferenčních rovnicích pro řešení této rekurence nefungují. Nástrojem nám v tomto případě bude následující invertovací formule.

Věta 3.4. *Nechť $(f_n)_{n \geq 0}$, $(g_n)_{n \geq 0}$ jsou posloupnosti takové, že pro každé $n \in \mathbb{N}_0$ platí $g_n = \sum_{k=0}^n \binom{n}{k} f_{n-k}$. Pak pro každé $n \in \mathbb{N}_0$ platí $f_n = \sum_{k=0}^n \binom{n}{k} (-1)^k g_{n-k}$.*

Důkaz. Do pravé strany vztahu, který chceme dokázat, dosadíme předpoklad

$$PS = \sum_{k=0}^n \binom{n}{k} (-1)^k g_{n-k} = \sum_{k=0}^n \binom{n}{k} (-1)^k \sum_{j=0}^{n-k} \binom{n-k}{j} f_{n-k-j}.$$

Ve vnitřní sumě zaměníme pořadí sčítanců, takže

$$PS = \sum_{k=0}^n \binom{n}{k} (-1)^k \sum_{j=0}^{n-k} \binom{n-k}{n-k-j} f_j.$$

V tomto výrazu zaměníme sumy,

$$PS = \sum_{k=0}^n \sum_{j=0}^{n-k} \binom{n}{k} (-1)^k \binom{n-k}{n-k-j} f_j = \sum_{j=0}^n \sum_{k=0}^{n-j} \binom{n}{k} (-1)^k \binom{n-k}{n-k-j} f_j,$$

a dále rozepíšeme kombinační čísla,

$$PS = \sum_{j=0}^n \sum_{k=0}^{n-j} (-1)^k \frac{n!}{k!(n-k)!} \frac{(n-k)!}{(n-k-j)!j!} f_j.$$

Zkrátíme $(n-k)!$ a z vnitřní sumy vytkneme vše, co nezávisí na jejím sčítacím indexu k ,

$$PS = \sum_{j=0}^n f_j \frac{n!}{j!} \sum_{k=0}^{n-j} (-1)^k \frac{1}{k!(n-k-j)!} = \sum_{j=0}^n f_j \frac{n!}{j!(n-j)!} \sum_{k=0}^{n-j} (-1)^k \frac{(n-j)!}{k!(n-k-j)!},$$

přičemž jsme rozšířili vynásobením $(n-j)!/(n-j)!$. Tak získáme

$$PS = \sum_{j=0}^n f_j \binom{n}{j} \sum_{k=0}^{n-j} \binom{n-j}{k} (-1)^k.$$

Vnitřní sumu teď upravíme podle binomické věty $\sum_{k=0}^{n-j} \binom{n-j}{k} (-1)^k = (1-1)^{n-j} = \delta_{nj}$, tj. tato suma je nulová pro všechna j kromě $j = n$, kdy má hodnotu 1. Proto můžeme uzavřít

$$PS = \sum_{j=0}^n f_j \binom{n}{j} \delta_{nj} = f_n \binom{n}{n} = f_n,$$

což jsme chtěli ukázat. □

Předvedme použití této invertovací formule na příkladu permutací bez pevného bodu.

Příklad 3.5. Chceme-li aplikovat větu 3.4 na vztah (3.5), položíme $g_n = n!$ a $f_n = d_n$. Z věty potom dostaneme

$$d_n = \sum_{k=0}^n \binom{n}{k} (-1)^k (n-k)! = \sum_{k=0}^n \frac{n!}{k!} (-1)^k.$$

To ale přesně odpovídá výrazu (3.2). S použitím řešení příkladu 3.3 tedy zjistíme, že počet permutací množiny $\{1, 2, \dots, n\}$ bez pevného bodu je $d_n = \lfloor n!e^{-1} + \frac{1}{2} \rfloor$. Čtenáři ponecháváme jako cvičení, aby si rozmyslel kombinatorické zdůvodnění, proč posloupnost $(d_n)_{n \geq 0}$ splňuje rekurenci (3.1).

4 Josefův problém a související úlohy

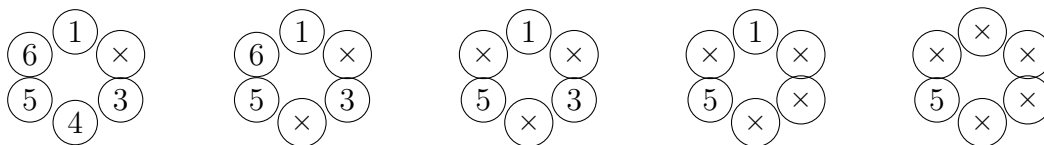
Josefův problém patří mezi tzv. rozpočítávací úlohy. Jmenuje se podle římského historika židovského původu Josefa Flavia, který ho popsal ve svých zápiscích o první židovské válce. Podle Josefova popisu obléhání města Jodfatu byli on a dalších 40 bojovníků uvězněni v jeskyni římskými vojáky. Nechtěli se nechat Římany zajmout, a tak se rozhodli spáchat hromadnou sebevraždu. Shodli se, že se zabijí navzájem tak, aby nikdo nezahynul vlastní rukou. První vylosovaný bude zabit druhým vylosovaným, ten zase třetím, atd. a až poslední se vydá obléhatelům. Losování proběhlo rozpočítáváním tak, že si bojovníci stoupli do kruhu a los padl na každého třetího. Josef popisuje, že shodou náhod nebo možná Božím řízením zůstal on a jeho přítel jako poslední na řadě. Josef byl tedy zajat, ale protože vojevůdci Vespasianovi předpověděl, že se stane císařem, nejenže přežil, ale dokonce byl propuštěn a ve službách Říma udělal poměrně slušnou kariéru.

Podíváme se na tuto rozpočítávací úlohu, ale ve zjednodušené verzi.

4.1 Zjednodušený Josefův problém

Nejdříve zformulujeme úlohu. Postavíme n lidí do kola, přičemž jednotlivé osoby jsou označeny číslem od 1 do n podle pořadí. Postupně vyřazujeme každého druhého (tj. osobu s číslem 2, 4, 6, atd.) a takto projdeme celý kruh. Při dalším vyřazování postupujeme stejně, jen už není na první pohled jasné, kterých osob se zbavujeme. Na konci přežije jediná osoba a my označíme $J(n)$ číslo, kterým tato osoba byla od začátku označena. Řešení našeho problému tedy spočívá v popisu posloupnosti $(J(n))_{n \geq 1}$.

Na příkladě si můžeme vyzkoušet



takže přeživší je číslo $J(6) = 5$.

Můžeme si všimnout jistých zákonitostí. Je samozřejmé, že všechny osoby se sudým pořadím vypadnou hned v prvním kole. V následujícím kole pak škrtneme jako první osobu č. 1 nebo 3 podle toho, jestli původní počet osob byl lichý nebo sudý. Rozlišme si proto tyto dva případy.

Nechť nejdřív $n = 2m$ pro nějaké $m \geq 1$. Po prvním kole nám zbyde m osob, přičemž poslední vyřazená byla osoba s číslem $2m$. Než začneme další kolo vyřazování, všechny zbylé osoby (tj. $1, 3, 5, \dots, 2m-1$) dostanou nové označení (tj. $1, 2, 3, \dots, m$), takže osoba s původním číslem $2k-1$, pro $k = 1, \dots, m$, dostane nové označení k , protože je teď k -tá v pořadí. Předpokládejme, že známe hodnotu $J(m)$, což je nové označení osoby, která přežije. Stačí už jen zjistit, jaké bylo její původní označení. To je zjevně $2J(m) - 1$.

Uvažujme nyní případ, kdy $n = 2m+1$ pro $m \geq 1$. Po vyřazení $m+1$ osob zbyde osob m , přičemž poslední jsme vyřadili osoby s číslem $2m$ a pak 1. Opět všechny zbylé osoby $3, 5, \dots, 2m+1$ přechíslovujeme na $1, 2, 3, \dots, m$, takže tentokrát osoba s původním číslem $2k+1$, pro $k = 1, \dots, m$, dostává nové označení k . Hodnotu $J(2m+1)$ pak vypočítáme z $J(m)$ podle $J(2m+1) = 2J(m) + 1$.

Celkově jsme tedy odvodili následující rekurentní vztah pro posloupnost $(J(n))_{n \geq 1}$,

$$\begin{aligned} J(1) &= 1, \\ J(2m) &= 2J(m) - 1, \quad m \geq 1, \\ J(2m+1) &= 2J(m) + 1, \quad m \geq 1. \end{aligned} \tag{4.1}$$

1. řešení: Vypišme si několik počátečních hodnot posloupnosti:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1	...

Pozorováním této tabulky nás může napadnout, že hodnoty 1 posloupnost nabývá právě pro argumenty ve tvaru 2^k . Dále se zdá, že mezi jednotlivými jedničkami jsou posloupnosti po sobě jdoucích lichých čísel. To lze jednoduše zapsat, pokud si uvědomíme, že všechna přirozená čísla lze zapsat ve tvaru $n = 2^k + l$, kde $k \geq 0$ a $0 \leq l < 2^k$, přičemž různým párům (k, l) odpovídají různá n . Pak

$$J(n) = J(2^k + l) = 2l + 1. \tag{4.2}$$

Platnost uhodnutého vzorce ověříme matematickou indukcí na k . Pro $k = 0$ je jediné $l = 0$, a tudíž $J(2^0 + 0) = J(1) = 1 = 2 \cdot 0 + 1$. Předpokládejme, že pro kladné exponenty $< k$ už vzorec (4.2) platí. Protože v indukci budeme používat rekurentní vztah (4.1), rozlišíme

případ sudého a lichého l . Je-li $k \geq 1$ a $0 \leq l < 2^k$ je sudé, pak $2^k + l = 2(2^{k-1} + \frac{l}{2})$, kde $0 \leq \frac{l}{2} < 2^{k-1}$. Proto s použitím rekurentního vztahu a indukčního předpokladu máme

$$J(2(2^{k-1} + \frac{l}{2})) = 2J(2^{k-1} + \frac{l}{2}) - 1 = 2(2^{\frac{l}{2}} + 1) - 1 = 2l + 1.$$

Pro $k \geq 1$ a $0 \leq l < 2^k$ liché je $2^k + l = 2(2^{k-1} + \frac{l-1}{2}) + 1$, kde $0 \leq \frac{l-1}{2} < 2^{k-1}$. Proto je

$$J(2(2^{k-1} + \frac{l-1}{2}) + 1) = 2J(2^{k-1} + \frac{l-1}{2}) + 1 = 2(2^{\frac{l-1}{2}} + 1) + 1 = 2l + 1.$$

Tím jsme platnost vzorce (4.2) ověřili.

2. řešení: Ukažme si, že ke stejnému výsledku bychom mohli dojít i bez použití rekurentního vztahu (4.1). Nejprve se podívejme na případ, kdy počet osob v kruhu je $n = 2^k$ pro $k \geq 1$. Když začneme rozpočítávat od prvního a projdeme jedno kolo, zbyde právě polovina, tedy 2^{k-1} , lidí a počítat v dalším kole se bude opět od osoby č. 1. Po k kolech zbyde ‘v kruhu’ jen jeden člověk, a to právě osoba č. 1. Proto $J(2^k) = 1$.

V případě, že lidí v kruhu stojí $2^k + l$, začneme tím, že vyřadíme l osob, takže v kruhu zbývá 2^k lidí. Z předchozího víme, že v takové situaci přežívá ten, od kterého začneme počítat. Protože poslední z l lidí, kterého jsme škrtili, byla osoba č. $2l$, máme nově počítat od osoby č. $2l + 1$. Vidíme, že $J(2^k + l) = 2l + 1$.

Tím jsme ověřili, že řešením rekurence (4.1) je opravdu posloupnost (4.2).

4.2 Zobecněný Josefův problém

Zkusíme předchozí úlohu lehce zobecnit. Uvažujeme reálné parametry α, β_0, β_1 . Budeme hledat posloupnost $(J(n))_{n \geq 1}$, která splňuje rekurenci

$$\begin{aligned} J(1) &= \alpha, \\ J(2n) &= 2J(n) + \beta_0, \quad n \geq 1, \\ J(2n+1) &= 2J(n) + \beta_1, \quad n \geq 1. \end{aligned} \tag{4.3}$$

Ve výsledku předchozího příkladu byla důležitá nejvyšší mocnina dvojky obsažená v argumentu n . Zkusme zkoumat rekurenci (4.3) v závislosti na dvojkovém zápisu čísla n . Předpokládejme, že

$$n = (b_k \cdots b_0)_2 = b_k 2^k + \cdots + b_1 \cdot 2^1 + b_0.$$

Uvědomíme si, že ve dvojkovém zápisu o paritě čísla rozhoduje poslední cifra b_0 , speciálně

$$n \text{ je } \begin{cases} \text{sudé,} & \text{pokud } b_0 = 0, \\ \text{liché,} & \text{pokud } b_0 = 1. \end{cases}$$

Poslední cifra tedy rozhodne, kterou rovnici z rekurence (4.1) máme použít. Když $b_0 = 0$, tedy $n = 2m = (b_k \cdots b_1 0)_2$, pak dvojkový zápis čísla m , tedy poloviny z n , je $m = (b_k \cdots b_1)_2$. Podobně když $b_0 = 1$, tedy $n = 2m + 1 = (b_k \cdots b_1 1)_2$, pak dvojkový zápis čísla $m = (n-1)/2$, je opět $m = (b_k \cdots b_1)_2$. Rekurenci (4.3) tedy můžeme jednotně zapsat

$$J((b_k \cdots b_1 b_0)_2) = 2J((b_k \cdots b_1)_2) + \beta_{b_0}, \quad J(1) = \alpha.$$

Tady jsme využili, že v rekurenci je β_0 při $b_0 = 0$ a β_1 při $b_0 = 1$. Nyní můžeme tuto rekurenci opakovaně použít,

$$\begin{aligned} J(n) &= J((b_k \cdots b_1 b_0)_2) = 2J((b_k \cdots b_1)_2) + \beta_{b_0} = 2\left(2J((b_k \cdots b_2)_2) + \beta_{b_1}\right) + \beta_{b_0} = \\ &= 2^2 J((b_k \cdots b_2)_2) + 2^1 \beta_{b_1} + \beta_{b_0} = 2^2 \left(2J((b_k \cdots b_3)_2) + \beta_{b_2}\right) + 2^1 \beta_{b_1} + \beta_{b_0} = \cdots = \\ &= 2^k J((b_k)_2) + 2^{k-1} \beta_{b_{k-1}} + \cdots + 2^1 \beta_{b_1} + \beta_{b_0}. \end{aligned}$$

Protože standardně volíme nejvyšší cifru nenulovou, tedy $b_k = 1$, máme ve finále

$$J(n) = 2^k \alpha + 2^{k-1} \beta_{b_{k-1}} + \cdots + 2^1 \beta_{b_1} + \beta_{b_0},$$

což by při mírném zneužití značení mohlo být zapsáno

$$J(n) = (\alpha \beta_{b_{k-1}} \cdots \beta_{b_1} \beta_{b_0})_2.$$

Příklad 4.1. V naší původní rekurenci (4.1) určíme tímto způsobem $J(70)$. Nyní platí $\alpha = 1$, $\beta_0 = -1$, $\beta_1 = 1$. Protože dvojkový zápis čísla 78 je $78 = (1001110)_2$, bude výsledkem číslo

$$J(78) = (\alpha \beta_0 \beta_0 \beta_1 \beta_1 \beta_1 \beta_0)_2 = (1\bar{1}\bar{1}111\bar{1})_2,$$

přičemž jsme pro cifry v “zobecněné dvojkové soustavě” použili zápis $\bar{1} = -1$. Výsledkem je tedy

$$J(78) = (1\bar{1}\bar{1}111\bar{1})_2 = 2^6 - 2^5 - 2^4 + 2^3 + 2^2 + 2 - 1 = 29.$$

Původní metodou bychom dostali stejný výsledek, protože $78 = 2^6 + 14$, takže $J(78) = 2 \cdot 14 + 1 = 29$.

Předchozí úvahy můžeme zobecnit ještě dále, totiž na rekurence, v nichž je předpis rozlišen v závislosti na zbytku po dělení jiným číslem než 2. Je už jednoduché ověřit, že platí následující tvrzení.

Tvrzení 4.2. *Nechť $d \in \mathbb{N}$, $d \geq 2$, a necht dále $c, \alpha_1, \dots, \alpha_{d-1}, \beta_0, \dots, \beta_{d-1} \in \mathbb{C}$ jsou libovolná čísla. Je-li $n = (b_k \cdots b_1 b_0)_d$ zápis čísla n v soustavě se základem d , pak řešením rekurence*

$$J(1) = \alpha_1,$$

$$\vdots$$

$$J(d-1) = \alpha_{d-1},$$

$$J(dn+j) = cJ(n) + \beta_j, \quad j \in \{0, \dots, d-1\}, \quad n \geq 1,$$

je

$$J(n) = (\alpha_{b_k} \beta_{b_{k-1}} \cdots \beta_{b_1} \beta_{b_0})_c = c^k \alpha_{b_k} + c^{k-1} \beta_{b_{k-1}} + \cdots + c^1 \beta_{b_1} + \beta_{b_0}.$$

Příklad 4.3. Najdeme hodnotu $f(135)$ posloupnosti $(f(n))_{n \geq 1}$, která je řešením rekurence

$$f(1) = 0, \quad f(2) = 1, \quad f(3) = 2,$$

$$f(4n) = 3f(n) + 2,$$

$$f(4n+1) = 3f(n) - 5,$$

$$f(4n+2) = 3f(n) + 1,$$

$$f(4n+3) = 3f(n) - 1.$$

Budeme řešit rekurenci podle tvrzení 4.2. V našem případě máme $d = 4$, $c = 3$ a dále

$$\alpha_1 = 0, \quad \alpha_2 = 1, \quad \alpha_3 = 2, \quad \beta_0 = 2, \quad \beta_1 = -5, \quad \beta_2 = 1, \quad \beta_3 = -1.$$

Nejprve zapíšeme číslo 135 v soustavě se základem $d = 4$. Platí $135 = 2 \cdot 4^3 + 1 \cdot 4^1 + 3 = (2013)_4$. Cifry tohoto rozvoje použijeme jako indexy koeficientů α , resp. β pro získání výsledku. Podle tvrzení 4.2 je

$$f(n) = c^3 \alpha_2 + c^2 \beta_0 + c^1 \beta_1 + \beta_3 = 3^3 \cdot 1 + 3^2 \cdot 2 + 3 \cdot (-5) - 1 = (12\overline{5}\overline{1})_3 = 29.$$

Výsledek jsme zapsali i pomocí zneužitého značení, přičemž jsme pro cifry v “zobecněné trojkové soustavě” použili zápis $\overline{5} = -5$ a $\overline{1} = -1$.

5 Kořeny polynomů

Podstatou řešení lineárních rekurencí je určení kořenů charakteristického polynomu. To může být zapeklitá otázka, pokud je polynom vyššího stupně. Exaktně (takzvaně v radikálech) totiž lze určit pouze kořeny polynomů lineárních, kvadratických, kubických a kvartických. Následující tvrzení nám alespoň dává metodu, jak najít všechny racionální kořeny polynomu, pokud má celočíselné koeficienty.

Věta 5.1. *Je-li $f(x) = a_n x^n + \dots + a_1 x + a_0$, $n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{Z}$, pak všechny jeho racionální kořeny leží v množině*

$$\left\{ \frac{r}{s} : r \in \mathbb{Z}, s \in \mathbb{N}, r|a_0, s|a_n \right\}.$$

Důkaz. Předpokládejme, že polynom f má racionální kořen $\frac{r}{s}$, $r \in \mathbb{Z}$, $s \in \mathbb{N}$, kde zlomek je zapsán v základním tvaru, tedy r je nesoudělné s s . Proto platí $f(\frac{r}{s}) = 0$. Dosadíme-li, vidíme

$$0 = f\left(\frac{r}{s}\right) = a_n \frac{r^n}{s^n} + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + \dots + a_1 \frac{r}{s} + a_0.$$

Vynásobením obou stran rovnosti číslem s^n , obdržíme

$$0 = a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n.$$

Odtud snadno odvodíme, že

$$a_n r^n \equiv 0 \pmod{s} \quad \text{a} \quad a_0 s^n \equiv 0 \pmod{r}.$$

Proto s dělí $a_n r^n$ a r dělí $a_0 s^n$. Nyní využijeme nesoudělnosti r a s . Jestliže totiž s dělí $a_n r^n$ a je nesoudělné s r , nutně dělí a_n . Podobně odvodíme, že r dělí a_0 . Tím je důkaz hotov. $\square$

Příklad 5.2. Určete kořeny polynomu $f(x) = 5x^4 + 4x^3 + 4x^2 + 4x - 1$. Podle věty 5.1 může být racionální číslo $\frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, kořenem polynomu f , pouze pokud $p|1$ a $q|5$. To znamená, že jedinými kandidáty na racionální kořen polynomu f jsou

$$\frac{p}{q} \in \left\{ \pm 1, \pm \frac{1}{5} \right\}.$$

Stačí tedy ověřit pro každý prvek $\frac{p}{q}$ této množiny, zda $f(\frac{p}{q}) = 0$. Máme

$$\begin{aligned} f(1) &= 5 + 4 + 4 + 4 - 1 = 16 \neq 0, \\ f(-1) &= 5 - 4 + 4 - 4 - 1 = 0, \\ f\left(\frac{1}{5}\right) &= 5\frac{1}{5^4} + 4\frac{1}{5^3} + 4\frac{1}{5^2} + 4\frac{1}{5} - 1 = 0, \\ f\left(-\frac{1}{5}\right) &= 5\frac{1}{5^4} - 4\frac{1}{5^3} + 4\frac{1}{5^2} - 4\frac{1}{5} - 1 = -\frac{208}{125} \neq 0. \end{aligned}$$

Racionálními kořeny polynomu f jsou tedy -1 a $\frac{1}{5}$. Pokud vydělíme polynom f polynomem $(x+1)(5x-1) = 5x^2 + 4x - 1$, získáme $x^2 + 1$, takže zbývajících kořeny polynomu f jsou $\pm i$. Polynom f lze tedy rozložit na kořenové činitele

$$f(x) = 5x^4 + 4x^3 + 4x^2 + 4x - 1 = (x+1)(5x-1)(x+i)(x-i).$$

Na předchozím příkladu můžeme pozorovat, že všechny racionální kořeny polynomu s celočíselnými koeficienty lze určit vyčíslením polynomu v konečném počtu bodů. Předvedeme si proto způsob, jak toto zjednodušit.

Uvažujme opět polynom $f(x) = a_n x^n + \dots + a_1 x + a_0$. Naším cílem je vyčíslit f v bodě c . K tomu použijeme vhodný přepis f ,

$$f(c) = a_0 + c(a_1 + c(a_2 + \dots c(a_{n-2} + c(a_{n-1} + ca_n)) \dots)).$$

Polynom tedy můžeme vyčíslovat postupně od vnitřní závorky. Formálně postupujeme takto:

$$\begin{aligned} b_n &:= a_n \\ b_{n-1} &:= a_{n-1} + cb_n \\ &\vdots \\ b_1 &:= a_1 + cb_2 \\ b_0 &:= a_0 + cb_1 \end{aligned} \tag{5.1}$$

Snadno si uvědomíme, že $b_0 = f(c)$. Při takovém postupu vyčíslování polynomu stupně n pak použijeme nejvýše n násobení a n sčítání. Tím se počet operací oproti výpočtu pouhým dosazením výrazně snižuje. Tento postup se nazývá Hornerovo schéma a lze zapsat do tzv. syntetického diagramu, do kterého vyplníme v prvním řádku koeficienty polynomu od nejvyššího k nejnižšímu a do druhého řádku postupně dopočítáváme $b_n, \dots, b_0$ podle (5.1)

$$\begin{array}{c|c|c|c|c|c} & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ \hline c & b_n & b_{n-1} & \cdots & b_1 & b_0 \end{array}$$

Příklad 5.3. Vyčíslíme polynom $f(x) = 5x^4 + 4x^3 + 4x^2 + 4x - 1$ v bodě $c = \frac{1}{5}$ s pomocí Hornerova schematu. Máme

$$f(c) = -1 + c(4 + c(4 + c(4 + c5)))$$

Vyplníme tedy do tabulky

$$\begin{array}{c|c|c|c|c} & 5 & 4 & 4 & -1 \\ \hline \frac{1}{5} & 5 & 5 & 5 & 0 \end{array}$$

Vyšlo nám tedy, že $f(\frac{1}{5}) = 0$. Pro zajímavost uvedme, že nová posloupnost 5, 5, 5, 5 tvoří posloupnost koeficientů v polynomu, který získáme vydělením polynomu f kořenovým činitelem $x - \frac{1}{5}$, což si čtenář může rozmyslet. Platí tedy

$$f(x) = (x - \frac{1}{5})(5x^3 + 5x^2 + 5x + 5).$$

6 Konečné grupy a konečná tělesa

V lineární algebře jste zavedli pojem těleso. Definici tělesa splňují množiny $\mathbb{R}$ a $\mathbb{C}$ reálných a komplexních čísel. S těmito tělesy jste pak pracovali v kontextu vektorových prostorů, ale i posloupností a funkcí. Kromě $\mathbb{R}$ a $\mathbb{C}$ jste se setkali s tělesem $\mathbb{Q}$ racionálních čísel. Stejně vlastnosti ale splňuje celá řada dalších množin.

Příklad 6.1. Př. Uvažujme množinu prvků $\{a, b, c\}$ a na ní definované operace $+$ a $*$ pomocí tabulek

$+$	a	b	c	$*$	a	b	c
a	a	b	c	a	a	a	a
b	b	c	a	b	a	b	c
c	c	a	b	c	a	c	b

Poznamenejme, že výsledek operace $x \circ y$ je v tabulce $\circ$ v řádku označeném x a sloupci označeném y . Snadno se přesvědčíte, že množina $\{a, b, c\}$ s takto definovanými operacemi splňuje všechny vlastnosti požadované od tělesa. Speciálně prvek $a = 0$ je neutrální vzhledem ke sčítání, $b = 1$ je neutrální vzhledem k násobení. Prvek b je opačný k prvku c , a prvek c je inverzní sám k sobě. Přejmenujeme-li ještě $c = 2$, je jasné vidět, že operace $+$ a $*$ jsou právě sčítání a násobení modulo 3.

Předvedeme, jak takové těleso může být užitečné v kontextu rekurentních posloupností, například když zkoumáme dělitelnost jejich členů.

Příklad 6.2. Určete, které členy Fibonacciho posloupnosti jsou dělitelné třemi. Místo $(F_n)_{n \geq 0}$ nám stačí uvažovat posloupnost $(R_n)_{n \geq 0}$, kde R_n je zbytek po dělení čísla F_n třemi. Pak $R_n \in \{0, 1, 2\}$ a číslo F_n je dělitelné třemi, právě když $R_n = 0$.

Nová posloupnost splňuje rekurenci $R_{n+2} = R_{n+1} + R_n$ pro $n \geq 0$, ve které nyní operace $+$ je sčítání modulo 3, s počátečními podmínkami $R_0 = 0$, $R_1 = 1$.

Snadno napočítáme několik prvních členů posloupnosti $(R_n)_{n \geq 0}$

n	0	1	2	3	4	5	6	7	8	9	...
R_n	0	1	1	2	0	2	2	1	0	1	...

Protože jsme získali $R_8 = R_0 = 0$, $R_9 = R_1 = 1$, bude posloupnost $(R_n)_{n \geq 0}$ periodická s periodou délky 8. Dělitelné třemi jsou právě Fibonacciho čísla, jejichž index je dělitelný čtyřmi, tedy

$$3|F_n \iff 4|n.$$

V tomto výkladu nás budou zajímat právě konečná tělesa. Jejich plnou sílu uvidíte v kurzu Teorie kódování [4].

6.1 Grupy

Struktura tělesa pracuje se dvěma binárními operacemi. Ještě elementárnější strukturou je tzv. grupa, množina vybavená jednou binární operací s určitými vlastnostmi.

Definice 6.3. Nechť G je neprázdná množina a $\circ : G \times G \rightarrow G$ binární operace na G s vlastnostmi:

- $a \circ (b \circ c) = (a \circ b) \circ c$ pro každé $a, b, c \in M$ (asociativita),
- existuje $e \in M$ takové, že $e \circ a = a$ pro každé $a \in M$ (e je neutrální prvek),
- pro každé $a \in M$ existuje $b \in M$ takové, že $a \circ b = e$ (b je inverzní prvek k prvku a).

Množinu G spolu s operací $\circ$ značíme $(G, \circ)$ a nazýváme *grupa*. Pokud je z kontextu zřejmé, jakou operaci $\circ$ uvažujeme, mluvíme o grupě G . Pokud operace $\circ$ navíc splňuje

- $a \circ b = b \circ a$ pro každé $a, b \in M$ (komutativita),

řekneme, že grupa G je abelovská.

Pojem grupa zachycuje obecnou podstatu řady matematických struktur. Nejmenší grupou je tzv. triviální grupa E obsahující pouze jediný prvek. Nejčastěji se setkáváme s grupami, jejichž nosné množiny jsou podmnožiny komplexních čísel a operace jsou běžné sčítání a násobení. Tyto operace jsou asociativní a komutativní.

Příklad 6.4. Množina celých čísel s operací sčítání $(\mathbb{Z}, +)$ je abelovská grupa, neutrálním prvkem je 0 a opačným k m je $-m$. Naopak množina $(\mathbb{N}, +)$ grupou není. Neobsahuje totiž ani neutrální prvek, ani inverze. Dalšími jednoduchými příklady grup jsou $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$.

Množina reálných čísel vybavená násobením vlastnosti grupy nesplňuje. Neutrálním prvkem vzhledem k násobení by mohla být 1, ale pak nemá číslo 0 inverzi. Nicméně struktura $(\mathbb{R} \setminus \{0\}, \cdot)$ už grupou je, stejně tak $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Pod pojem grupa ovšem spadá i řada méně běžných struktur.

Příklad 6.5. Necht G je množina všech spojitých bijekcí $f : \mathbb{R} \rightarrow \mathbb{R}$ a $\circ$ je operace skládání zobrazení. Operace $\circ$ je asociativní, neutrálním prvkem je identické zobrazení a ke každé spojitě bijekci f je její inverzí vzhledem ke skládání spojitá funkce f^{-1} . Proto $(G, \circ)$ je grupa. Tato grupa ovšem není abelovská. Jako příklad si můžeme uvést funkce $f(x) = 2x$, $g(x) = x + 1$. Platí

$$(f \circ g)(x) = f(g(x)) = 2x + 2, \text{ ale } (g \circ f)(x) = g(f(x)) = 2x + 1.$$

Příklad 6.6. Necht G je množina všech matic $A \in \mathbb{R}^{n \times n}$ s nenulovým determinanem a $\circ$ je operace maticového násobení. Pak $(G, \circ)$ je grupa, která není abelovská. Příklad můžeme najít už u matic 2×2 . Označíme-li

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix},$$

pak

$$A \cdot B = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}, \text{ ale } B \cdot A = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}.$$

Nejzásadnějším příkladem konečných grup jsou grupy získané pomocí operací sčítání a násobení modulo $m \in \mathbb{N}$. Tyto operace jsou opět asociativní a komutativní. V dalším textu je pro rozlišení od sčítání a násobení v $\mathbb{C}$ budeme značit $\oplus$, $\odot$.

Příklad 6.7. Necht $m = 5$. Pak množina $\mathbb{Z}_5 = \{0, 1, \dots, 4\}$ s operací sčítání modulo 5 je grupa. Neutrálním prvkem je 0, a protože $1 \oplus 4 = 0$, $2 \oplus 3 = 0$, jsou prvky 1 a 4, resp. 2 a 3, navzájem opačné. Proto $(\mathbb{Z}_5, \oplus \text{ mod } 5)$ je grupa.

Vybavíme-li množinu $\mathbb{Z}_5$ operací násobení modulo 5, bude 1 neutrálním prvkem, ale narazíme na problém, že 0 nemá inverzi. Každý nenulový prvek ale inverzi má, protože $1 \odot 1 = 1$, $2 \odot 3 = 1$, $4 \odot 4 = 1$. Struktura $(\mathbb{Z}_5 \setminus \{0\}, \odot \text{ mod } 5)$ je tedy grupa.

Příklad 6.8. Necht $m = 6$. Množina $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$ s operací sčítání modulo 6 je opět grupa. Neutrálním prvkem je 0, a páry opačných prvků jsou $1 \oplus 5 = 0$, $2 \oplus 4 = 0$, $3 \oplus 3 = 0$.

Vyzkoušejme, zda násobení modulo 6 opět vytvoří grupu na množině nenulových zbytků modulo 6. $\mathbb{Z}_6 \setminus \{0\} = \{1, 2, 3, 4, 5\}$. Neutrálním prvkem může být jedině 1. Mají ale všechny prvky inverze? Zjevně 1 je inverzní sama k sobě a také platí $5 \odot 5 = 1$. Ale

$$2 \odot 2 = 4, \quad 2 \odot 3 = 0, \quad 2 \odot 4 = 2, \quad 2 \odot 5 = 4.$$

Proto prvek 2 nemá v množině $\mathbb{Z}_6 \setminus \{0\}$ inverzi. Stejně tak bychom nenalezli inverzi k prvkům 3 a 4. Je to tím, že 2, 3, 4 jsou čísla soudělná s 6.

Situace z předchozích dvou příkladů se dá zobecnit do následujícího tvrzení.

Tvrzení 6.9. *Nechť $m \in \mathbb{N}$ a nechť $\oplus$ a $\odot$ značí operace modulo m . Pak platí*

1. $(\mathbb{Z}_m, \oplus)$ je grupa pro každé $m \in \mathbb{N}$.
2. $(\mathbb{Z}_m \setminus \{0\}, \odot)$ je grupa, právě když m je prvočíslo.

Důkaz. V množině $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ vybavené sčítáním modulo m je neutrálním prvkem 0. K prvku $k \in \mathbb{Z}_m$ je inverzí prvek $m-k \in \mathbb{Z}_m$, protože $k \oplus (m-k) = 0$. Proto $(\mathbb{Z}_m, \oplus)$ je grupa.

Uvažujme množinu $\{1, 2, \dots, m-1\}$ s násobením modulo m . Neutrálním prvkem je 1. Jestliže m není prvočíslo, pak existuje $d \in \{1, 2, \dots, m-1\}$, které je dělitelem čísla m . Kdyby toto d mělo v množině $\{1, 2, \dots, m-1\}$ inverzi k vzhledem k násobení, pak by platilo $d \odot k = 1$. To ale znamená, že existuje $j \in \mathbb{Z}$ takové, že $d \cdot k = 1 + j \cdot m$. To ale není možné, protože číslo d dělí levou stranu, ale nedělí pravou stranu této rovnice.

Pro důkaz opačné implikace druhého tvrzení využijeme znalost z prvního semestru diskrétní matematiky [3]. Nechť m je prvočíslo. Pak jsou všechna čísla $d \in \{1, 2, \dots, m-1\}$ nesoudělná s m . K danému d tedy existují $k, j \in \mathbb{Z}$ tak, že platí $d \cdot k + m \cdot j = 1$, navíc k je určeno až na posun o násobek čísla m . Lze tedy volit $k \in \{1, 2, \dots, m-1\}$. To ovšem znamená, že $d \odot k = 1$, takže k je inverze k prvku d . □

Poznámka 6.10. Stejně jako jsme z množiny $\mathbb{Z}_m$ odebrali 0, která neměla inverzi vzhledem k násobení, lze v případě, že m není prvočíslo, odebrat z množiny $\mathbb{Z}_m$ i další prvky bez inverzí tak, aby vznikla grupa. Lze odvodit, že invertibilní prvky v $\mathbb{Z}_m$ jsou právě taková k , která jsou nesoudělná s m . Množinu invertibilních prvků modulo m značíme

$$\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m : \text{nsd}(k, m) = 1\}.$$

Spolu s operací násobení modulo m tvoří $\mathbb{Z}_m^*$ grupu. To je v souladu s faktem, že pro m prvočíslo, tato množina splývá se $\mathbb{Z}_m \setminus \{0\}$.

6.2 Podgrupa

Protože nejčastějším typem operace $\circ$ je sčítání nebo násobení, používá se jedno ze dvou typů značení.

Aditivní značení: Pro operaci $\circ$ používáme značku $+$, neutrální prvek se značí 0 , inverznímu prvku k prvku a se říká opačný prvek a značí se $-a$ a zavádíme $\underbrace{a + a + \cdots + a}_{n\text{krát}} = na$ pro $n \in \mathbb{N}$, a také $0a = 0$ a $(-n)a = n(-a)$.

Multiplikativní značení: Značku $\cdot$ pro operaci $\circ$ často vynecháváme, tedy pro $a, b \in G$ píšeme $a \circ b = ab$. Neutrální prvek se značí 1 , někdy se mu také říká jednotka. Inverzní prvek k prvku a značíme a^{-1} a zavádíme $\underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{krát}} = a^n$, přičemž $a^0 = 1$ a $a^{-n} = (a^{-1})^n$. Z asociativity operace snadno vidíme, že platí očekávaný vztah

$$a^k \circ a^j = a^{k+j} \quad \text{pro každé } k, j \in \mathbb{Z}.$$

V následujícím textu budeme využívat multiplikativní značení.

Definice 6.11. Nechť G s operací $\circ$ je grupa a nechť G' je neprázdna podmnožina množiny G . Pokud G' s operací $\circ$ je sama grupou, řekneme, že G' je podgrupa grupy G .

Poznámka 6.12. Aby neprázdna podmnožina $G' \subset G$ byla podgrupou grupy G , je nutné a stačí, aby byla uzavřená na operaci $\circ$ a na inverze všech prvků. Každá grupa má jako svou podgrupu triviální grupu E a taky sebe samu.

Tvrzení 6.13. Nechť G je grupa a nechť G' je její podgrupa. Pak počet prvků v G' dělí počet prvků v G , tedy $\#G' \mid \#G$.

Důkaz. Pro každé $a \in G$ uvažujeme množinu $aG' = \{ax : x \in G'\}$. Ukážeme, že platí tato tři fakta:

- (a) Pro každé $x \in G$ existuje $a \in G$ tak, že $x \in aG'$;
- (b) pro každé $a \in G$ je $\#(aG') = \#G'$;
- (c) pro každé $a, b \in G$ platí $aG' = bG'$ nebo $aG' \cap bG' = \emptyset$.

Jinými slovy, množina G je disjunktním sjednocením stejně velkých podmnožin o velikosti $\#G'$. Proto $\#G' \mid \#G$. Zbývá tedy dokázat fakta (a)–(c).

Bod (a) je zřejmý, protože podgrupa G' obsahuje neutrální prvek. Je tedy $x = x1 \in xG'$. Pro bod (b) vezměme $x, y \in G'$. Jestliže $ax = ay$, pak vynásobením prvkem a^{-1} zleva získáme $x = y$. Přiřazení $x \mapsto ax$ je tedy bijekce mezi G' a aG' . Tudíž $\#(aG') = \#G'$.

Pro bod (c) uvažujme prvek x v průniku $aG' \cap bG'$. To znamená, že existují prvky $y, z \in G'$ tak, že $x = ay = bz$. Zjistíme, že $b = ayz^{-1}$. Protože G' je podgrupa grupy G , leží prvek yz^{-1} v G' , a proto $b \in aG'$. Teď ukážeme, že $bG' \subset aG'$. Libovolný prvek $bw \in bG'$ můžeme totiž napsat $bw = ayz^{-1}w \in aG'$, opět z uzavřenosti G' vůči operacím.

Ze symetrie ale platí $aG' \subset bG'$. Pokud tedy průnik množin aG' , bG' obsahuje alespoň jeden prvek, pak jsou obě množiny shodné. $\square$

Příklad 6.14. Najděte minimální množinu G tak, aby obsahovala matici $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ a tvořila spolu s maticovým násobením grupu. Potom rozhodněte, zda G je grupa abelovská a najděte všechny podgrupy grupy G .

Řešení: Víme, že všechny mocniny matice A musí patřit do množiny G ,

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Je zřejmé, že množina $G = \{I, A, A^2, A^3\}$ s maticovým násobením tvoří grupu. Mocniny stejné matice spolu komutují, proto je grupa G abelovská. Protože $\#G = 4$, podle tvrzení 6.13 mohou mít podgrupy pouze 1, 2 nebo 4 prvky. Jednoprvková podgrupa je pouze triviální $G' = \{I\}$. Čtyřprvková podgrupa je pak celé $G' = G$. Netriviální nevlastní podgrupa grupy G bude tedy dvouprvková a kromě identické matice I bude obsahovat prvek B takový, že $B^2 = I$. Jedinou možností je $G' = \{I, B = A^2\}$.

6.3 Cyklické grupy

Lemma 6.15. *Nechť G je konečná grupa. Pak pro každé $a \in G$ existuje $n \in \mathbb{N}$ takové, že $a^n = 1$.*

Důkaz. Uvažujme posloupnost prvků $1 = a^0, a^1, a^2, a^3, \dots$. Protože grupa G je konečná, musí existovat $k, j \in \mathbb{N}$ tak, že $a^k = a^j$. Vynásobíme-li rovnici prvkem $(a^{-1})^j$, dostaneme $a^{k-j} = 1$. $\square$

Definice 6.16. Nechť G je konečná grupa, $a \in G$. Minimální $n \in \mathbb{N}$ s vlastností $a^n = 1$ se nazývá řád prvku a v grupě G .

Příklad 6.17. Určete řády všech prvků v grupě G z příkladu 6.14. Protože $A^4 = I$, $(A^2)^2 = I$, $(A^3)^4 = I$, jsou řády jednotlivých matic v grupě G rovny $r(I) = 1$, $r(A) = r(A^3) = 4$, $r(A^2) = 2$.

Tvrzení 6.18. *Nechť G je konečná grupa, $a \in G$. Označme r řád prvku a v grupě G . Potom $G' = \{a, a^2, a^3, \dots, a^r = 1\}$ je podgrupa grupy G , přičemž r dělí počet $\#G$ prvků v grupě G .*

Důkaz. Fakt, že G' je podgrupou grupy G je zřejmý. Protože $\#G' = r$, platí podle tvrzení 6.13, že $r \mid \#G$. $\square$

Definice 6.19. Grupa G se nazývá cyklická, pokud existuje prvek $a \in G$ tak, že $G = \{1, a, a^2, a^3, \dots, a^{r-1}\}$, kde r je řád prvku a v grupě G . Řekneme, že G je generovaná prvkem a a prvek a je generátor grupy G .

Poznámka 6.20. Protože mocniny stejného prvku spolu komutují, je každá cyklická grupa abelovská.

Příklad 6.21. Uvažujme grupu $(\mathbb{Z}_5^* = \{1, 2, 3, 4\}, \odot)$. Protože

$$\{2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1\} = \mathbb{Z}_5^*,$$

je prvek 2 generátorem této grupy. Podobně

$$\{3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1\} = \mathbb{Z}_5^*,$$

takže prvek 3 je také generátor grupy. Je to proto, že řady prvků 2 a 3 jsou $r(2) = r(3) = 4$. Naopak $4^2 = 1$, takže řád prvku 4 je $r(4) = 2$ a prvek 4 není generátorem.

Poznámka 6.22. Nechť $G = \{a, a^2, \dots, a^r = 1\}$ je cyklická grupa s generátorem a řádu r . Každý dělitel d čísla r je řádem některého prvku grupy G . Označme $k = r/d$. Pak prvek $b = a^k$ má řád d , protože $b^d = a^{kd} = a^r = 1$. Zároveň platí, že $G' = \{b, b^2, \dots, b^d = 1\}$ je podgrupa grupy G .

Následující věta určuje, jak nalézt všechny generátory cyklické grupy.

Tvrzení 6.23. *Nechť G je cyklická grupa s r prvky a nechť a je její generátor, tj. $G = \{a, a^2, \dots, a^{r-1}, a^r = 1\}$. Pak prvek a^k je taky generátor grupy G , právě když $\text{nsd}(k, r) = 1$. Speciálně to znamená, že počet různých generátorů grupy G je $\varphi(r)$, kde φ je Eulerova funkce.*

Důkaz. Nejdříve si uvědomíme, že pro každý násobek $n = jr$ čísla r platí $a^n = (a^r)^j = 1^j = 1$. Platí i opačná implikace, totiž jakmile $a^n = 1$ pro nějaké $n \in \mathbb{N}$, pak $r|n$. Při dělení čísla n číslem r máme $n = jr + i$, kde $j \in \mathbb{N}_0$ a $0 \leq i < r$. Pak $1 = a^n = (a^r)^j a^i = a^i$. A protože r je minimální exponent s touto vlastností, nutně $i = 0$.

Uvažujme nyní exponent k a označme $d = \text{nsd}(k, r)$. Pak pro prvek $b = a^k$ platí

$$b^{r/d} = (a^k)^{r/d} = (a^r)^{k/d} = 1.$$

Proto je řád $r(b)$ prvku b nejvýše roven r/d .

Kdyby $d = \text{nsd}(k, r) > 1$, pak $\{b, b^2, \dots, b^{r(b)} = 1\} \subsetneq G$. Předpokládejme naopak, že $d = 1$. Pak pro řád $r(b)$ prvku $b = a^k$ platí $r(b) \leq r$. Platí $1 = b^{r(b)} = (a^k)^{r(b)} = a^{kr(b)}$. Podle výše uvedeného nutně máme $r|kr(b)$. Ale $\text{nsd}(k, r) = 1$, takže $r|r(b)$. To dohromady znamená, že $r = r(b)$, takže prvek b je generátorem grupy G . $\square$

Přiopomeňme, že Eulerova funkce $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ určuje pro každé n počet přirozených čísel menších nebo rovných n nesoudělných s n . Vlastnosti Eulerovy funkce i vzorec, jak určit $\varphi(n)$ z prvočíselného rozkladu čísla n , může čtenář najít v [3].

Příklad 6.24. Vraťme se k příkladu 6.21. V grupě $\mathbb{Z}_5^* = \{2, 2^2 = 4, 2^3 = 3, 2^4 = 1\}$ je generátorem prvek 2^j , kde j je nesoudělné s $r = 4$. Takové j je pouze $j = 1, j = 3$, takže $2^1 = 2$ a $2^3 = 3$.

Příklad 6.25. Najděme generátory v grupě $(\mathbb{Z}_{17}^* = \{1, 2, 3, \dots, 16\}, \odot)$. Výpočtem zjistíme

$$\begin{aligned} 3^1 &= 3, 3^2 = 9, 3^3 = 10, 3^4 = 13, 3^5 = 5, 3^6 = 15, 3^7 = 11, 3^8 = 16, \\ 3^9 &= 14, 3^{10} = 8, 3^{11} = 7, 3^{12} = 4, 3^{13} = 12, 3^{14} = 2, 3^{15} = 6, 3^{16} = 1. \end{aligned}$$

To znamená, že 3 je generátorem grupy. Protože řád prvku 3 je 16, budou dalšími generátory grupy čísla $3^3 = 10, 3^5 = 5, 3^7 = 11, 3^9 = 14, 3^{11} = 7, 3^{13} = 12$ a $3^{15} = 6$. Generátorů je celkem 8, což odpovídá počtu $\varphi(16)$ čísel menších nebo rovných 16 nesoudělných s 16.

Poznámka 6.26. V grupě $(\mathbb{Z}_n, \oplus)$ je generátorem vždy 1, protože

$$\{1, 1 \oplus 1 = 2, \dots, \underbrace{1 \oplus 1 \oplus \dots \oplus 1}_{(n-1)\text{krát}} = n-1, \underbrace{1 \oplus 1 \oplus \dots \oplus 1}_{n\text{krát}} = 0\} = \mathbb{Z}_n.$$

Příklad 6.27. Najdeme všechny generátory grupy $(\mathbb{Z}_6, \oplus)$. Protože $\mathbb{Z}_6$ je cyklická grupa s generátorem 1, můžeme k nalezení všech dalších generátorů použít tvrzení 6.23. Musíme jen dát pozor, že nyní máme aditivní značení. Dalšími generátory jsou tedy prvky $\underbrace{1 \oplus 1 \oplus \dots \oplus 1}_{j\text{krát}} = j$, kde j je nesoudělné s 6. Kromě 1 je tedy generátorem $\mathbb{Z}_6$ ještě 5. Můžeme si ověřit:

$$5, 5 \oplus 5 = 4, 5 \oplus 5 \oplus 5 = 3, 5 \oplus 5 \oplus 5 \oplus 5 = 2, 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 = 1, 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 = 0.$$

Ale třeba 4 není generátorem, protože

$$\{4, 4 \oplus 4 = 2, 4 \oplus 4 \oplus 4 = 0\} \subsetneq \mathbb{Z}_6.$$

6.4 Izomorfizmy grup

Jak jsme viděli na některých příkladech, grupou mohou být různé matematické objekty - množiny čísel, matic, funkcí, atd. Přesto jejich struktura může být v zásadě stejná. V případě, že u grupy G stačí prvky a operaci „přejmenovat“, abychom dostali grupu G' , budeme říkat, že grupy G a G' jsou izomorfní. Přesněji to vystihuje následující definice.

Definice 6.28. Nechtě $(G, \circ)$ a $(G', \circ')$ jsou grupy. Řekneme, že grupa G je izomorfní s grupou G' , pokud existuje bijekce $\psi : G \rightarrow G'$ taková, že pro všechny $x, y \in G$ platí

$$\psi(x \circ y) = \psi(x) \circ' \psi(y). \quad (6.1)$$

Nejlépe ilustrujeme izomorfii grup, pokud porovnáme jejich tabulku operace.

Příklad 6.29. Uvažujme grupu $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ s operací sčítání modulo 4 a grupu $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ s operací násobení modulo 5. Mají stejný počet prvků, což je první podmínka k tomu, aby mezi nimi existoval izomorfismus. Z tabulek jejich operací zkusíme vyčíst, která bijekce mezi $\mathbb{Z}_4$ a $\mathbb{Z}_5^*$ je izomorfismem.

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_5^*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Na první pohled se tabulky operací nepodobají. Přesto jsou tyto grupy izomorfní. Snadno si rozmyslíme, že při izomorfismu se musí zobrazovat neutrální prvek na neutrální prvek a prvek x v grupě G musí mít stejný řád jako prvek $\psi(x)$ v grupě G' . Z tabulek lze snadno vyčíst, že řády prvků jsou

$$\text{v } \mathbb{Z}_4 : \quad r(0) = 1, \quad r(1) = 4, \quad r(2) = 2, \quad r(3) = 4;$$

$$\text{v } \mathbb{Z}_5^* : \quad r(1) = 1, \quad r(2) = 4, \quad r(3) = 4, \quad r(4) = 2.$$

Poznamenejme, že prvky řádu 4 jsou právě generátory příslušné grupy. Kandidáty na izomorfizmy máme dva

$$\psi_1 : \quad 0 \mapsto 1, \quad 1 \mapsto 2, \quad 2 \mapsto 4, \quad 3 \mapsto 3;$$

$$\psi_2 : \quad 0 \mapsto 1, \quad 1 \mapsto 3, \quad 2 \mapsto 4, \quad 3 \mapsto 2.$$

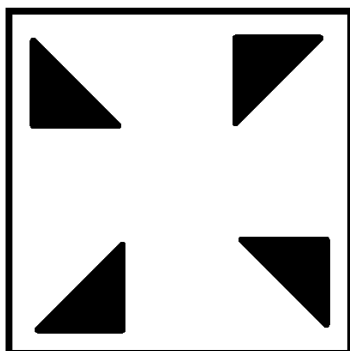
Po příslušném zpermutování prvků v tabulce $\mathbb{Z}_5^*$ dostaneme tabulky

$\mathbb{Z}_5^*$	1	2	4	3
$\psi_1(0) = 1$	1	2	4	3
$\psi_1(1) = 2$	2	4	3	1
$\psi_1(2) = 4$	4	3	1	2
$\psi_1(3) = 3$	3	1	2	4

$\mathbb{Z}_5^*$	1	3	4	2
$\psi_2(0) = 1$	1	3	4	2
$\psi_2(1) = 3$	3	4	2	1
$\psi_2(2) = 4$	4	2	1	3
$\psi_2(3) = 2$	2	1	3	4

V obou případech vznikne tabulka, v níž každý řádek je jen cyklickým posunem oproti řádku předchozímu tak, jak je tomu u tabulky sčítání v $\mathbb{Z}_4$.

Stejnou strukturu cyklické grupy jako $\mathbb{Z}_4$ mají i další čtyřprvkové grupy, jako například grupa matic $\{I, A, A^2, A^3\}$ pro $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ z příkladu 6.14, grupa $(\{\pm 1, \pm i\}, \cdot)$ všech komplexních kořenů polynomu $x^4 - 1$ s operací násobení komplexních čísel, nebo grupa symetrií takového obrázku:



Čtenář si jako cvičení může zkusit nalézt příslušné izomorfizmy.

Na příkladě si každý může uvědomit následující zjevný fakt.

Tvrzení 6.30. *Každé dvě cyklické grupy se stejným počtem prvků jsou izomorfní.*

Důkaz. Necht G je cyklická grupa s generátorem a , $G = \{a, a^2, \dots, a^r = 1\}$ a G' je grupa s generátorem b , $G' = \{b, b^2, \dots, b^r = 1\}$. Definujeme zobrazení $\psi : G \rightarrow G'$ tak, že $\psi(a) = b$ a pro každý prvek $a^j \in G$, $j = 2, \dots, r$ dále $\psi(a^j) = \psi(a)^j = b^j$. Z předpisu je jasné, že ψ je bijekce a navíc splňuje vlastnost izomorfizmu (6.1). $\square$

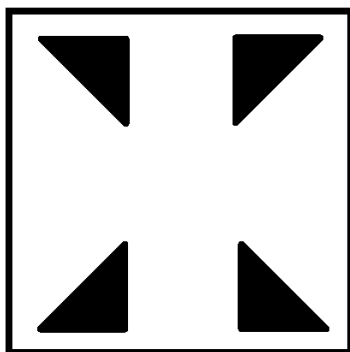
Příklad 6.31. Najdeme minimální množinu obsahující matice $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ a $C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, která spolu s maticovým násobením tvoří grupu.

Postupně máme

$$B^2 = I, C^2 = I, BC = CB = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ a } (BC)^2 = (CB)^2 = I.$$

Celkově tedy máme čtyřprvkovou grupu $G = \{I, B, C, BC\}$, v níž mají všechny prvky kromě identity I řád 2. Tato grupa tedy není cyklická, a nemůže tedy být izomorfní grupě $\mathbb{Z}_4$.

Snadno si rozmyslíme, že je ale izomorfní grupě $\{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$, ve které je operací násobení dvojic po složkách, potažmo grupě $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$, jejíž operací je sčítání modulo 2 opět po složkách. Tato poslední grupa je vlastně „direktním součinem“ grup $\mathbb{Z}_2 \times \mathbb{Z}_2$ a odpovídá symetriím obrázku



Poznamenejme, že existují právě dvě čtyřprvkové grupy (až na izomorfismus), jak jsou popsány v příkladech 6.29 a 6.31. Ta první je cyklická grupa $\mathbb{Z}_4$, grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ se nazývá Kleinova grupa.

Literatura

- [1] J. Herman, R. Kučera, J. Šimša, *Equations and Inequalities: Elementary Problems and Theorems in Algebra and Number Theory*. 1. vyd. New York : Springer-Verlag, 2000. 355 s. Canadian Mathematical Society Books in Math.
- [2] L. Lovász, J. Pelikán, K. Vesztergombi, *Discrete mathematics: Elementary and Beyond, Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.
- [3] Z. Masáková, *Diskrétní matematika I*, učební text FJFI ČVUT v Praze
http://people.fjfi.cvut.cz/masakzuz/dim_soubory/dim.pdf
- [4] E. Pelantová, *Teorie kódování*, učební text FJFI ČVUT v Praze
<http://people.fjfi.cvut.cz/pelannedi/TK0/komplet2020.pdf>