NI-MPI cvičení 7 handout 13. února 2025
Problémy, návrhy apod. hlaste v GitLabu.
Verze souboru: 2023-02-15 12:19.

Obsah

Co byste si měli z tohoto cvičení odnést:

- jak najít podgrupy generované množinami,
- jak najít efektivně generátory multiplikativních grup modulo prvočíslo p.

A co byste se měli doučit, pokud to ještě/už neumíte:

- stačí znát z přednášky definice a základní vlastnosti výše zmíněných pojmů.

18 Cyklické grupy a generátory

Cvičení 18.1 Najděte všechny generátory a všechny podgrupy grupy $\mathbb{Z}_{15}^+$. Najděte také inverzní prvky ke všem prvkům. ■ ?

Cvičení 18.2 Najděte konečnou grupu, která má podgrupy řádu $3, 5$ a 7. ■ ?

Cvičení 18.3 Najděte podgrupu grupy $(\mathbb{Z}, +)$ generovanou množinou ?

(a) $\{2\}$,

(b) $\{2, 3\}$,

(c) $\{2, 5\}$,

(d) $\{6, 15\}$,

(e) $\{n, m\}$, kde $n \neq m$ jsou kladná přirozená čísla.

Cvičení 18.4 Popište jak vypadají podgrupy cyklické grupy $(\mathbb{Z}, +)$. ?

Známe z přednášky: Je-li $(G, \circ)$ cyklická grupa řádu n a a nějaký její generátor, potom a^k je také generátor tehdy a jen tehdy, když k a n jsou nesoudělná (tj. $\gcd(k, n) = 1$).

Cvičení 18.5 Najděte všechny generátory a všechny podgrupy grupy $\mathbb{Z}_{11}^\times$. Najděte také inverzní prvky ke všem prvkům. ■ ?

Cvičení 18.6 Najděte všechny generátory a všechny podgrupy grupy $\mathbb{Z}_{17}^{\times}$. Najděte také inverzní prvky ke všem prvkům. ■

Cvičení 18.7 Najděte nejmenší podgrupu grupy regulárních matic z $\mathbb{R}^{3,3}$ s klasickým maticovým násobením, která obsahuje matici

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(a) Je tato podgrupa cyklická?

(b) Je cyklická výše zmíněná grupa všech regulárních matic z $\mathbb{R}^{3,3}$?

■

Cvičení 18.8 Najděte všechny generátory a podgrupy aditivní grupy modulo 22, tj. grupy $\mathbb{Z}_{22}^{+}$.

Cvičení 18.9 Najděte všechna kladná $n \in \mathbb{Z}$ taková, že grupa $\mathbb{Z}_n^{\times}$ má řád 12.

Cvičení 18.10 Najděte nejmenší podgrupu grupy $(\mathbb{R}^{+}, \cdot)$ kladných reálných čísel s klasickým násobením, která obsahuje

(a) čísla 5 a 10;

(b) všechna prvočísla.

Cvičení 18.11 Buďte f a g dvě permutace z S_9, kde

$$f = (2,4,5,6,3,1,8,9,7) \quad \text{a} \quad g = (8,1,5,2,6,3,7,9,4)\,.$$

(a) Čemu se rovná $f \circ g$?

(b) Čemu se rovná $\langle f \rangle$, tzn. nejmenší podgrupa S_n obsahující f?

(c) Čemu se rovná $f^{100} \circ g^{100}$?

Cvičení 18.12 Nalezněte grupu G a dva její prvky a, b řádu 3 takové, že prvek $c = a \circ b$ nemá řád 3 a není neutrální. Může být grupa G abelovská? ■

19 Generátory grup $\mathbb{Z}_p^{\times}$

Cvičení 19.1 Jaká je pravděpodobnost, že náhodně zvolený prvek grupy $\mathbb{Z}_{23}^{\times}$ je generátor?

Základní cvičení 19.2

(a) Je 5 generátor grupy $\mathbb{Z}_{23}^{\times}$? (Pokuste se toto ověřit či vyvrátit bez nutnosti výčtu množiny generované prvkem 5.)

(b) Je 2 generátor grupy $\mathbb{Z}_{23}^{\times}$?

(c) Nalezněte všechny generátory grupy $\mathbb{Z}_{23}^{\times}$.

Základní cvičení 19.3 Ukažte že množina $H = \{a^{11} : a \in \mathbb{Z}_{23}^{\times}\}$ je podgrupa grupy $\mathbb{Z}_{23}^{\times}$ a zjistěte její řád. ■

Cvičení 19.4 Mějme libovolná přirozená čísla k a n. Ukažte že množina $H = \{a^k : a \in \mathbb{Z}_n^{\times}\}$ je podgrupa grupy $\mathbb{Z}_n^{\times}$ a zjistěte (popiště a zdůvodněte), pro která k se jedná o vlastní podgrupu. ■

Cvičení 19.5 Nalezněte nosnou množinu grupy $\mathbb{Z}_{18}^{\times}$ a všechny její generátory.

Cvičení 19.6 Nalezněte nosnou množinu grupy $\mathbb{Z}_{30}^{\times}$ a všechny její generátory.

Řešení

Řešení Cvičení 18.3: (a) sudá čísla, (b) $(\mathbb{Z}, +)$, (c) $(\mathbb{Z}, +)$, (d) násobky tří, (e) násobky $\gcd(n, m)$

Řešení Cvičení 18.4: Z předchozího cvičení lze odvodit, že se bude jednat vždy o podgrupy tvaru $\langle k \rangle$, $k \in \mathbb{Z}$.

Řešení Cvičení 18.8: Obecný postup je následující. Najdeme nějaký generátor g: v grupě $\mathbb{Z}_{22}^{+}$ je to snadné, neboť očividným generátorem je 1. Potom využijeme větu, která říká, že g^k je generátor právě když k je nesoudělné s řádem grupy: v grupě $\mathbb{Z}_{22}^{+}$ se používá aditivní značení, takže místo g^k píšeme $k \times g$ a generátory jsou tedy čísla $k \times 1 = k$ nesoudělná s řádem grupy 22. Takových čísel je $\varphi(22) = \varphi(2)\varphi(11) = 1 \cdot 10 = 10$ (Eulerova funkce): $\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$.

Řešení Cvičení 18.9: Odpovědí je samozřejmě číslo 42, ale není samo. Všechna možná hledaná n můžeme najít díky tomu, že řád grupy $\mathbb{Z}_n^{\times}$ je roven $\varphi(n)$, kde φ je Eulerova funkce. Hledání n takových, že $\mathbb{Z}_n^{\times}$ má řád 12 tedy odpovídá řešení rovnice

$$\varphi(n) = 12.$$

Postupovat můžeme buď tak, že využijeme faktu, že pro hodnotu $\varphi(n)$ existují spodní odhady (vizte např. zde), a pak projdeme všechna n, pro která je tento odhad menší než 12. Tento postup je ale zoufale nematematický, a proto jej tady nebudeme rozpitvávat.

Zajímavější je postup analytický. Vyjdeme z toho, že $\varphi(n)$ se dá napsat jako součin výrazů tvaru $(p^k - p^{k-1})$, kde p^k je nejvyšší mocnina prvočísla p, která dělí n. Číslo 12 se dá napsat jako součin celých kladných čísel pouze osmi způsoby:

$$12 = 1 \cdot 12 = 2 \cdot 6 = 1 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 3 = 1 \cdot 2 \cdot 2 \cdot 3 = 4 \cdot 3 = 1 \cdot 4 \cdot 3.$$

Hledáme tedy prvočísla p a kladná celá čísla k taková, že výraz $(p^k - p^{k-1})$ se rovná 1, 2, 3, 4, 6 nebo 12. Snadno ověříme, že pro všechna uvažovaná p a k platí $(p^k - p^{k-1}) \geq p - 1$ a že $(p^k - p^{k-1})$ je rostoucí posloupností (vzhledem ke k). Proto platí $(p^k - p^{k-1}) = 1$ pouze pro $p = 2$ a $k = 1$, $(p^k - p^{k-1}) = 2$ pouze pro $p = 3$ a $k = 1$ resp. $p = 2$ a $k = 2$ (pro větší hodnoty p a k už je výraz nutně větší než 2). Podobně dostaneme, že $(p^k - p^{k-1}) = 3$ nemá řešení. Z toho je zřejmé, že není třeba uvažovat poslední čtyři součiny ve výčtu výše:

$$2 \cdot 2 \cdot 3 = 1 \cdot 2 \cdot 2 \cdot 3 = 4 \cdot 3 = 1 \cdot 4 \cdot 3.$$

A zbývá tedy vyřešit rovnici $(p^k - p^{k-1}) = 6$ opět stačí uvažovat pouze prvočísla ostře menší než 8 a prvních pár hodnot k. Dostaneme pouhá dvě řešení: $p = 7$ a $k = 1$ resp. $p = 3$ a $k = 2$.

Celkově tedy dostáváme pro hledaná n násl. možnosti prvočíselných rozkladů:

$$n = 13, n = 2 \cdot 13, n = 3 \cdot 7, n = 2 \cdot 3 \cdot 7, n = 2^2 \cdot 7, n = 2^2 \cdot 3^2,$$

tedy čísla $13, 26, 21, 42, 28, 36$.

Řešení Cvičení 18.10: (a) Budeme doplňovat čísla do množiny $\{5, 10\}$ tak, aby byly splněny všechny požadavky na grupu.

1. Abychom zajistili uzavřenost vůči operaci násobení, musíme přidat $5 \cdot 5, 5 \cdot 5 \cdot 5, \ldots$ neboli všechny mocniny pětky $5^k, k = 1, 2, 3, \ldots$. Podobně pro 10 musíme přidat $10^\ell, \ell = 1, 2, 3, \ldots$. Množina ale stále není uzavřená, neb tam chybí např. součin $5^2 10^3$, proto musíme přidat všechna čísla tvaru $5^k 10^\ell$, kde alespoň jedno z nezáporných čísel k a ℓ je nenulové. Taková množina již je uzavřená.

2. Asociativita je vlastnost operace a operace násobení čísel je samozřejmě asociativní.

3. Neutrální prvek je číslo jedna a to nám tam stále chybí, proto umožníme i případ, kdy v $5^k 10^\ell$ jsou nulové k i ℓ, a tím získáme monoid: i po přidání čísla 1 množina zůstává uzavřená.

4. Inverze k prvku $5^k 10^\ell$ je číslo $5^{-k} 10^{-\ell}$, přidáme tam tedy i tato čísla a výsledek je množina

$$\{5^k 10^\ell \mid k, \ell \in \mathbb{Z}\},$$

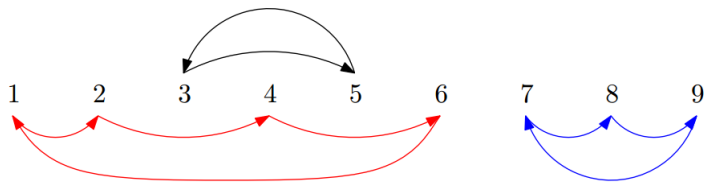
   která je uzavřená vůči násobení (to je třeba zkontrolovat pokaždé, když tam něco přidáme, neb by se uzavřenost mohla narušit), a tedy se již jedná o grupu. Z konstrukce je jasné, že se jedná o nejmenší možnou grupu.

(b) U množiny prvočísel postupujeme podobně: musíme přidat všechny kladné mocniny všech prvočísel, a pak také všechny jejich vzájemné součiny. Tím ale dostaneme všechna celá čísla ostře větší než 1 (každé takové číslo se dá napsat jako součin mocnin prvočísel!). Tak dostaneme grupoid. Asociativita opět platí a po přidání jedničky dostáváme monoid. Abychom dostali grupu, přidáme ke všem kladným celým číslům inverze: v množině tak máme čísla $1, 2, 3, \ldots$ a $1/2, 1/3, 1/4, \ldots$. Tato množina ale není uzavřená (např. chybí $3 \cdot 1/5$), proto musíme přidat i všechny vzájemné součiny a tím dostaneme $\mathbb{Q}^+$, množinu všech kladných racionálních čísel, která již tvoří grupu.

Řešení Cvičení 18.11: část (i): Zápis $f = (2, 4, 5, 6, 3, 1, 8, 9, 7)$ vlastně znamená, že $f(1) = 2, f(2) = 4, f(3) = 5$, a tak dále. Složení $f \circ g$ se pak konstruuje jako standardní složení zobrazení. Například $(f \circ g)(1) = f(g(1))$ a jelikož $g(1) = 8$ a $f(8) = 9$, je $(f \circ g)(1) = 9$. Opakováním této úvahy dostaneme, že

$$f \circ g = (9, 2, 3, 4, 1, 5, 8, 7, 6).$$

část (ii): Abychom lépe pochopili strukturu permutace f, nakreslíme si následující orientovaný graf: vrcholy budou čísla 1 až 9, tedy definiční obor f, a z vrcholu k povede vždy právě jedna šipka do vrcholu $f(k)$. Např. z 1 vedeme šipku do 2, z 2 do 4 atd. Výsledek vypadá takto:



Snadno si rozmyslíme, že pro každý vrchol platí, že z něho vede právě jedna šipka (neb f je zobrazení), a také že do něho vede právě jedna šipka (neb f je bijekce!). To nutně znamená, že se graf skládá z uzavřených nezávislých cyklů. Pro permutaci f jsou to cykly na vrcholech $1, 2, 4, 6$ (červené šipky), $3, 5$ (černé šipky)

a $7, 8, 9$ (modré šipky). S pomocí tohoto grafu snadno zjistíme, jak vypadají mocniny f. Např. f^2 získáme tak, že vždy uděláme po šipkách dva kroky: 1 se zobrazí na 4, 2 na 6, 3 na 3 atd. Celkově

$$f^2 = (4, 6, 3, 1, 5, 2, 9, 7, 8).$$

Víme, že obecně platí

$$\langle f \rangle = \{f^k \ : \ k \in \mathbb{Z}\}.$$

Díky obrázku výše ovšem víme o permutaci f důležitou věc: mocnění f znamená pohyb po cyklech délky 4, 2 a 3. Nejmenší společný násobek těchto čísel je 12 a tak platí, že $f^{12} = f^0 = \mathrm{id}$. Z toho již plyne, že

$$\langle f \rangle = \{f^k \ : \ k \in \mathbb{Z}\} = \{f^0, f^1, f^2, \ldots, f^{11}\}.$$

Jak přesně tyto permutace vypadají získáme snadno z obrázku výše.
část (*iii*): Z předchozího bodu víme, že f^{100} se rovná f^4, protože $100 \equiv 4 \pmod{12}$. Abychom si zjednodušili podobně g^{100}, nakreslíme si opět příslušný orientovaný graf a z něho zjistíme, že g obsahuje cykly délek 5, 3 a 1. Nejmenší společný násobek těchto čísel je 15, a tedy platí $g^{100} = g^{10}$. Nyní už jednoduše zjistíme, že

$$f^{100} \circ g^{100} = f^4 \circ g^{10} = (1, 2, 3, 4, 5, 6, 8, 9, 7) \circ (1, 2, 5, 4, 6, 3, 7, 8, 9) = (1, 2, 5, 4, 6, 3, 8, 9, 7)\,.$$

Řešení Cvičení 19.1: Jelikož počet generátorů je $\varphi(22) = 10$, je pravděpodobnost rovna $10/22 = 0,45454545\cdots$.

Řešení Cvičení 19.2: (a) ano, je, (b) ne, není, (c) $\{5^k \mod 23 : gcd(k, 22) = 1\}$.

Řešení Cvičení 19.5: Nosná množina je $\{1, 5, 7, 11, 13, 17\}$ a generátory jsou prvky 5 a 11.

Řešení Cvičení 19.6: Nosná množina grupy $\mathbb{Z}_{30}^{\times}$ je množina $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Dle věty z přednášky (30 není tvaru 2, 4, p^k, nebo $2p^k$, kde p je liché prvočíslo a k je kladné přirozené číslo) se nejedná o cyklickou grupu a proto její množina generátorů je prázdná.

ChangeLog

Verze	Datum	Autor	Log
1.11	15.2.23	ŠS	Oprava překlepu v řešení příkladu se 2 permutacemi.
1.1	15.10.18	ŠS	Vyhozena část příkladu hovořící o izomorfismech.
1.0	3.10.18	ŠS	Verze z roku 2017/2018.