Teorie čísel: Cvičení 10 – výsledky a vybraná řešení

25. dubna 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@gmail.com

Výsledky a řešení:

-2. $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$. Zřejmě $a \in \mathbb{Z}_{12}$ generuje $\mathbb{Z}_{12}$ právě tehdy když $\mathbb{Z}_{12} = \{na \mid n \in \mathbb{Z}\}$. Vzhledem k tomu, že navíc $12a = 0$, tak se ekvivalentně ptáme, kdy $\mathbb{Z}_{12} = \{na \mid n = 0, 1, \ldots, 11\}$.

Dále si všimněme, že pokud $d = NSD(a, 12) > 1$, tak $d \mid na$ pro všechna n, tedy se nikdy nemůže stát $na = 1$ a a negeneruje celou $\mathbb{Z}_{12}$. Zbývá dokázat, že všechny zbylé $a \in \mathbb{Z}_{12}$, $NSD(a, 12) = 1$ jsou generátory $\mathbb{Z}_{12}$.

Zřejmě $\langle 1 \rangle = \mathbb{Z}_{12}$. Pro $a \in \{5, 7, 11\}$ si jde buď vypsat celou množinu $\{na \mid n = 0, 1, \ldots, 11\}$ (např. pro $a = 5$ vyjde $0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7$, tedy $\langle 5 \rangle = \mathbb{Z}_{12}$), nebo můžeme najít odpověď na otázku, zda má kongruence $na \equiv b \pmod{12}$ řešení $n \in \mathbb{Z}$ pro libovolné $b \in \mathbb{Z}$.

Pro $a = 5$ z Bézoutovy rovnosti díky $NSD(5, 12) = 1$ najdeme $n, m \in \mathbb{Z}$, že $5n + 12m = 1$, tedy $5n \equiv 1 \pmod{12}$. Neboli 5 má inverz modulo 12 a kongruence $5n \equiv 1 \pmod{12}$ má řešení. Rovněž pak má řešení i kongruence $b \equiv 5(nb) \pmod{12}$, a tedy $\langle 5 \rangle = \mathbb{Z}_{12}$.

Rozmyslete si, že podobný argument lze použít i pro $a = 7, 11$. V úloze 1 si rozmyslíte, že tento argument jde zobecnit pro libovolné $\mathbb{Z}_n$.

Generátory $\mathbb{Z}_{12}$ jsou $1, 5, 7, 11$.

-1. Při určování homomorfismů je klíčové pozorování, že pokud $a^k = 1$, tak $1 = \varphi(1) = \varphi(a^k) = \varphi(a \cdot a \cdots a) = \varphi(a)^k$ neboli pokud má prvek a řád k, tak řád prvků $\varphi(a)$ dělí k. (Pro sčítací grupy jde tohle pozorování přepsat jako $na = 0 \Rightarrow n\varphi(a) = 0$.)

a) Uvažujme nějaký homomorfismus $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_6$. Vidíme, že $\mathbb{Z}_3 = \langle 1 \rangle$, jako důsledek tak $\varphi(a) = a\varphi(1)$ pro libovolné $a \in \mathbb{Z}_3$. Pokud tedy určíme $\varphi(1)$, tak už máme vynucené podmínky pro to, jak musí celé zobrazení vypadat. Dále si všimněme, že $3 \cdot 1 = 0$ v $\mathbb{Z}_3$ (řád 1 v $\mathbb{Z}_3$ je 3), a tedy podle výše uvedeného pozorování rovněž $3\varphi(1) = 0$ v $\mathbb{Z}_6$ (neboli $\varphi(1)$ má v $\mathbb{Z}_6$ řád 1 nebo 3). Rovnost $3n = 0$ v $\mathbb{Z}_6$ splňují pouze prvky $\{0, 2, 4\}$, a tedy $\varphi(1) \in \{0, 2, 4\}$.

Dostáváme, tak tři potenciální zobrazení:

(a) φ_0: $\varphi_0(0) = \varphi_0(1) = \varphi_0(2) = 0$, což je triviální homomorfismus,
(b) $\varphi_2 : \varphi_2(0) = 0$, $\varphi_2(1) = 2$, $\varphi_2(2) = 2 \cdot 2 = 4$,
(c) $\varphi_4 : \varphi_2(0) = 0$, $\varphi_4(1) = 4$, $\varphi_4(2) = 2 \cdot 4 = 2$.

Ověřte si, že skutečně všechna tato tři zobrazení jsou dobře definované homomorfismy (tj. vztah $\varphi(g \cdot h) = \varphi(g) * \varphi(h)$ je zachován po složkách pro všechna $g, h \in \mathbb{Z}_3$). Buď to jde vyloženě po prvcích nebo si uvědomte, jak jsou homomorfismy definované pomocí $\varphi(1)$.

Dohromady tak máme triviální homomorfismus (ten existuje vždy) a dva netriviální.

b) Podobně jako v a) si uvědomíme, že 1 je generátor $\mathbb{Z}_5$ a φ je určené obrazem $\varphi(1)$. Vzhledem k tomu, že řád 1 v $\mathbb{Z}_5$ je 5 ($5 \cdot 1 = 0$), tak máme, že $5 \cdot \varphi(1) = 0$ neboli řád $\varphi(1)$ v $\mathbb{Z}_6$ dělí 5. Prvek $\varphi(1)$ má tedy buď řád 1 (pak $\varphi(1) = 0$ a dostáváme triviální homomorfismus), nebo má řád 5. Nicméně v grupě $\mathbb{Z}_6$ není žádný prvek řádu 5, neboť z Lagrangeovy věty musí řád prvku dělit řád grupy ($|\mathbb{Z}_6| = 6$). Tento případ tak nemůže nastat.

Jediný homomorfismus mezi zadanými grupami je triviální.

0. a) Protože 11 je prvočíslo, tak z přednášky víme, že grupa je cyklická. Pojďme tedy najít nějaký primitivní prvek. $|\mathbb{Z}_{11}^*| = 10$, řád libovolného prvku $a \in \mathbb{Z}_{11}^*$ tak z Lagrangeovy věty dělí 10, tedy je to jedno z čísel 1 (jednotka), 2, 5 nebo 10 (primitivní prvky). Takže na ověření, že je a primitivní prvek, stačí ukázat, že $a, a^2, a^5 \neq 1$.

Zkusme například $a = 2$. Pak $a = 2 \neq 1$, $a^2 = 2^2 = 4 \neq 1$ a $a^5 = 10 \neq 1$. Řád 2 je tak nutně 10 a 2 je primitivní prvek.

b) $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, hledáme prvek řádu 4. Nicméně 1 má řád 1 a pro zbylé prvky platí $3^2 = 5^2 = 7^2 = 1$, a tedy mají řád 2. Vidíme tedy, že žádný prvek negeneruje celou $\mathbb{Z}_8^*$ a grupa není cyklická.

1. a) $\mathbb{Z}_{18} = \{0, 1, \ldots, 17\}$. Analogicky k úloze -2. pro $a \in \mathbb{Z}_{18}$ platí, že pokud $NSD(a, 18) > 1$, tak $NSD(a, 18) \mid na$ pro všechna n a $\langle a \rangle \subsetneq \mathbb{Z}_{18}$.

   Pro $NSD(a, 18) = 1$, tedy $a \in \{1, 5, 7, 11, 13, 17\}$, lze stejně jako v -2. ukázat, že skutečně generují celou $\mathbb{Z}_{18}$.

   b) Pokud pro $a \in \mathbb{Z}_n$ platí $d = NSD(a, n) > 1$, tak $d \mid na$ pro všechna n, $1 \notin \langle a \rangle \subsetneq \mathbb{Z}_{18}$ a a tak negeneruje celou $\mathbb{Z}_n$.

   c) V návaznosti na část b) si rozmyslíme, že všechny prvky splňující $NSD(a, n) = 1$ už jsou generátory. Jde o přímé zobecnění důkazu provedeného v příkladu -2.

   Z Bézoutovy rovnosti díky $NSD(a, n) = 1$ najdeme $x, y \in \mathbb{Z}$, že $xa + yn = 1$, tedy $xa \equiv 1 \pmod{n}$. Neboli a má inverz modulo n a kongruence $ax \equiv 1 \pmod{n}$ má řešení. Rovněž pak má řešení i kongruence $b \equiv a(xb) \pmod{n}$, a tedy $\langle a \rangle = \mathbb{Z}_n$.

2. a) Na to, aby byl φ homomorfismus, tak musíme ukázat, že pro všechna $a, b \in \mathbb{Z}_6$ platí

$$\varphi((a + b) \mod 6) = (\varphi(a) + \varphi(b)) \mod 3.$$

   Z definice ϕ, tak chceme ukázat, že

$$((a + b) \mod 6) \mod 3 =^{?} ((a \mod 3) + (b \mod 3)) \mod 3 = a + b \mod 3.$$

   Pokud si označíme $c = (a + b) \mod 6$, tak chceme vlastně říct, že $c \equiv a + b \pmod{3}$. Nicméně víme, že $a + b \equiv c \pmod{6}$ a protože 3 dělí 6, tak i $a + b \equiv c \pmod{3}$. Tedy se skutečně jedná o homomorfismus. (Podmínku bychom přirozeně mohli ověřit i po prvcích, ale to je zbytečně pracné.)

   b) V tomto případě nejde o homomorfismus. Speciálně si můžeme všimnout, že například

$$0 = \varphi(0) = \varphi(1 + 4) \neq \varphi(1) + \varphi(4) = 2$$

   .

   Poznámka: To, že to takto vyšlo není v nějakém smyslu náhoda. Jde v podstatě o to, že v $\mathbb{Z}_6$ ztotožňujeme prvky se stejným zbytkem modulo 3 a dostaneme kopii $\mathbb{Z}_3$, (což odpovídá struktuře faktorgrupy, jak uvidíte nebo jste již viděli na Algebře), což v $\mathbb{Z}_5$ nejde.

3. a) $\varphi(1)$ se musí zobrazit na prvek řádu 1, 2 nebo 4, tedy $\varphi(1) \in \{0, 2, 4, 6\}$. Všechny tyto možnosti dají homomorfismus definovaný po prvcích jako $\varphi(a) = a\varphi(1)$. (To, že jsou to skutečně homomorfismy je třeba ověřit – buď ručně, nebo to dokázat obecně).

   b) Podobně jako výše se $\varphi(1)$ musí zobrazit na prvek řádu 1, 2 nebo 4. Prvky řádu 4 v $\mathbb{Z}_6$ nejsou, pro ostatní dostaneme možnosti $\varphi(1) \in \{0, 3\}$, oba opět dají funkční homomorfismy.

   c) Podobně jako výše se $\varphi(1)$ musí zobrazit na prvek řádu 1, 2 nebo 4. Nicméně z těchto řádů existuje v $\mathbb{Z}_7$ pouze prvek řádu 1 (je jím 0), a tedy dostaneme pouze možnost $\varphi(1) = 0$ a triviální homomorfismus.

4. a) Z Lagrangeovy věty platí, že řády prvků jsou buď 1 nebo 7. Očividně jediný prvek řádu 1 je 0 (jednotka v této grupě) a ostatní prvky budou mít řád 7.

   b) $\mathbb{Z}_7^*$ je cyklická, jak víme. Buď můžeme řády spočítat pro každý prvek zvlášť, nebo si pro zjednodušení práce můžeme najít nějaký primitivní prvek modulo 7. S trochou snahy zjistíme, že je jím například 3 (nebo si vzpomeneme na minulé cvičení). Každý prvek jde potom tedy zapsat ve tvaru 3^k a hledáme nejmenší n takové, že $(3^k)^n = 1$ neboli $nk \equiv 0 \pmod{6}$, neboť $3^6 = 1$. Z toho už snadno odvodíme, že $n = \frac{6}{NSD(6,k)}$.

   Speciálně tak vidíme, že řád 1 má přesně $3^0 = 1$, řád 2 má přesně $3^3 = 6$, řád 3 mají přesně $3^2 = 2$, $3^4 = 4$ a řád 6 mají $3^1 = 3$, $3^5 = 5$.

5. Cyklické jsou právě $\mathbb{Z}_5^*$ (generátory $2, 3$), $\mathbb{Z}_6^*$ (generátor 5) a $\mathbb{Z}_9^*$ (generátory $2, 5$). Grupa $\mathbb{Z}_{12}^*$ naopak cyklická není, neboť v ní všechny prvky mají řád nanejvýš 2.

6. a) 3 (primitivní prvek 2)

   5 (primitivní prvky $2, 3$)

   7 (primitivní prvky $3, 5$)

   b) Hledáme homomorfismus, který bude zároveň bijekce. Protože jsou velikosti grup shodné, tak stačí ukázat, že bude homomorfismus na celou grupu $\mathbb{Z}_6$. Toho lze docílit tím, že zobrazíme generátor $\mathbb{Z}_7^*$ (primitivní prvek modulo 7, např. 3) na generátor $\mathbb{Z}_6$ (např. 1). Chceme tak $\varphi(3) = 1$ a definujme tedy po prvcích bijekci $\varphi(3^k) = k$ pro $k \in \{0, \ldots, 5\}$. Zbývá ověřit, že je to bijekce (to jste viděli například ve skriptech nebo na minulém cviku při počítání charakterů).

7. a) Chceme právě prvky $a \in \mathbb{Z}_p$ nesoudělné s p, to jsou jistě všechny kromě 0, a tak $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ a $|\mathbb{Z}_p^*| = p - 1$.

   b) Označme řád a jako k, tedy $a^k = 1$. Jistě $k \leq p - 1$, neboť řád prvku dělí řád grupy. Nicméně prvky generované a jsou v množině $1, a, a^2, \ldots a^{k-1}$ (libovolné jiné (i záporné) mocniny umíme přenásobením dostat na jednu z těchto). Prvek a má ale generovat celou $\mathbb{Z}_p^*$, tedy alespoň $p - 1$ prvků. Z toho už dostaneme i $k \geq p - 1$ a nutně $k = p - 1$.

   c) Podobně jako v předchozím případě definujeme zobrazení po prvcích jako $\varphi(a^k) = k$ a ověříme, že jde skutečně o dobře definovaný izomorfismus.

8. Stačí si uvědomit, že to jsou přesně prvky $\mathbb{Z}_7^*$ s řádek 6, což jsme už v úloze 4. určili, že jsou 3 a 5.

   Obecně, pokud už zvládneme najít jeden primitivní prvek (v tomto případě například 3), tak z postupu z příkladu 4 vyplývá, že ostatní získáme přesně tak, že tento prvek umocníme na čísla nesoudělná s řádem grupy. Speciálně v našem případě chceme umocnit 3 na čísla nesoudělná s 6, což jsou přesně $3^1 = 3$ a $3^5 = 5$.