TEORIE GRUP PRO TEORII ČÍSEL

DAVID STANOVSKÝ

stanovsk@karlin.mff.cuni.cz

Tento text je vytažen z připravovaných skript pro předmět Algebra. Měl by pokrývat vše, co je nutné znát pro kurz Teorie čísel. Jde o několik vybraných sekcí, didakticky to není dokonalé, ale k základní orientaci to snad stačí.

Z kapitoly o komutativních okruzích je potřeba pouze základní definice (zjednodušeně řečeno, komutativní okruh je těleso bez podmínky na existenci inverzů), pojem invertibilního prvku (prvek a je invertibilní, pokud existuje prvek b takový, že $ab = 1$, značíme jej a^{-1}, je jednoznačně určen) a základní příklady: okruh celých čísel $\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0)$ a odvozené okruhy $\mathbb{Z}_n$, jejichž prvky jsou pouze čísla $0, ..., n-1$ a operace provádíme modulo n. V okruzích $\mathbb{Z}_n$ jsou invertibilní právě ty čísla k, která jsou nesoudělná s n, inverz lze spočítat pomocí Eulerovy věty nebo pomocí Bézoutovy rovnosti.

1. Pojem grupy

1.1. Definice a příklady.

Hlavní motivací teorie grup je studium nejrůznějších typů symetrií a transformací matematických objektů. Pojem pochází z Galoisovy teorie a původně označoval množinu (skupinu) permutací G uzavřenou na skládání, tj. splňující $\pi \circ \sigma \in G$ pro všechna $\pi, \sigma \in G$. Abstrakcí tohoto pojmu vznikla rozsáhlá větev algebry, zvaná teorie grup. Aplikace nachází všude, kde se vyskytuje pojem symetrie či transformace, především v kombinatorice (konečné grupy) a geometrii (lineární grupy).

Definice. *Grupou* rozumíme čtveřici $\mathbf{G} = (G, *, ', e)$, kde G je množina, na které jsou definovány binární operace $*$, unární operace $'$ a konstanta e splňující pro každé $a, b, c \in G$ následující podmínky:

$$a * (b * c) = (a * b) * c, \qquad a * e = e * a = a, \qquad a * a' = a' * a = e.$$

Grupu nazýváme *abelovskou*, pokud navíc pro všechna $a, b \in G$ platí

$$a * b = b * a.$$

Prvku e se říká *jednotka*, prvku a' *inverzní prvek* k prvku a.

Formálně rozlišujeme mezi množinou G, tzv. *nosnou množinou*, a čtveřicí $\mathbf{G} = (G, *, ', e)$, která navíc obsahuje informaci o algebraické struktuře definované na množině G. V konkrétních příkladech bývá typickou trojicí operací buď $+, -, 0$, pak hovoříme o *aditivním zápise* (a místo $x + (-y)$ píšeme $x - y$), anebo trojice $\cdot, ^{-1}, 1$, čemuž říkáme *multiplikativní zápis*.

Date: 15. února 2021.

Definice. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $H \subseteq G$ podmnožina její nosné množiny taková, že $e \in H$ a pro každé $a, b \in H$ platí

$$a' \in H \quad \text{a} \quad a * b \in H.$$

Říkáme, že H je *uzavřena na grupové operace* a že *tvoří podgrupu* grupy $\mathbf{G}$. Čtveřici $\mathbf{H} = (H, *|_H, '|_H, e)$ pak nazýváme *podgrupou*, přičemž $|_H$ značí restrikci operací na množinu H. Značíme $\mathbf{H} \leq \mathbf{G}$. Podgrupy $\mathbf{G}$ a $\{e\}$ nazýváme *nevlastní*.

Základním zdrojem příkladů abelovských grup jsou grupy odvozené od komutativních okruhů, zejména pak *číselné grupy*, odvozené od číselných oborů.

Příklad. Buď $\mathbf{R}$ okruh. Pak $(R, +, -, 0)$ je abelovská grupa, tzv. *aditivní grupa* okruhu $\mathbf{R}$. Důležité jsou zejména číselné grupy $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, a také grupy $\mathbb{Z}_n$ sestávající z čísel $0, \ldots, n-1$ s operacemi modulo n.

V matematice se vyskytují nejrůznější příklady grup. Kromě číselných grup nacházejí asi největší využití permutační grupy, maticové grupy a grupy geometrických zobrazení.

Příklad. Buď $\mathbf{R}$ komutativní okruh s jednotkou, označme R^* množinu všech invertibilních prvků v $\mathbf{R}$. Pak $\mathbf{R}^* = (R^*, \cdot, ^{-1}, 1)$ je abelovská grupa, tzv. *multiplikativní grupa* okruhu $\mathbf{R}$. Skutečně jde o grupu: inverz invertibilního prvku je invertibilní (protože $(a^{-1}) \cdot a = 1$), součin dvou invertibilních prvků a, b je invertibilní (protože $(ab)(b^{-1}a^{-1}) = 1$) a grupové axiomy jsou obsaženy v definici okruhu.

- Je-li $\mathbf{R}$ těleso, pak $\mathbf{R}^* = (R \setminus \{0\}, \cdot, ^{-1}, 1)$.
- Pro polynomiální okruhy platí $\mathbf{R}[x]^* = \mathbf{R}^*$, protože invertibilní jsou právě konstantní polynomy invertibilní v $\mathbf{R}$.
- $\mathbb{Z}^* = (\{1, -1\}, \cdot, ^{-1}, 1)$.
- Prvky grupy $\mathbb{Z}_n^*$ jsou právě všechna čísla $a \in \{1, \ldots, n-1\}$ nesoudělná s n. Soudělná čísla invertibilní nejsou: je-li $d \nmid 1$ společný dělitel a, n, pak $d \mid (ab \bmod n)$ pro libovolné b, takže součin ab nikdy nemůže být 1. Naopak, jsou-li a, n nesoudělná, uvažujme Bézoutovy koeficienty u, v splňující $1 = \mathrm{NSD}(a, n) = ua + vn$. Podíváme-li se na rovnost modulo n, dostaneme $1 \equiv ua \pmod{n}$, a tedy $a^{-1} = u \bmod n$.

Příklad. *Permutační grupy.* Základním příkladem je *symetrická grupa* sestávající z permutací na dané neprázdné množině X s operacemi $\circ$ skládání permutací, $^{-1}$ invertování permutací a konstantou $id : x \mapsto x$ (identické zobrazení), tj.

$$\mathbf{S}_X = (\{\pi : \ \pi \text{ je permutace na množině } X\}, \circ, ^{-1}, id).$$

Je-li $X = \{1, \ldots, n\}$, pak místo $\mathbf{S}_X$ píšeme $\mathbf{S}_n$. Podgrupy symetrických grup se nazývají *permutační grupy*, např.

- *alternující grupa* $\mathbf{A}_n \leq \mathbf{S}_n$ všech sudých permutací na n prvcích;
- *dihedrální grupa* $\mathbf{D}_{2n} \leq \mathbf{S}_n$ všech permutací, které odpovídají symetriím pravidelného n-úhelníka vztaženým na jeho vrcholy očíslované po směru hodinových ručiček. Tyto permutace odpovídají n rotacím a n reflexím, proto značení $\mathbf{D}_{2n}$.
- nejrůznější grupy symetrií geometrických těles, automorfismů grafů a dalších matematických struktur.

Příklad. *Maticové grupy.* Základním příkladem je *obecná lineární grupa* nad tělesem $\mathbf{T}$ sestávající z regulárních matic dané velikosti s operacemi $\cdot$ maticového násobení, $^{-1}$ maticového invertování a jednotkovou maticí jako jednotkou, tj.

$$\mathbf{GL}_n(\mathbf{T}) = (\{A : \ A \text{ je regulární matice } n \times n \text{ nad tělesem } \mathbf{T}\}, \cdot, ^{-1}, I),$$

Podgrupy lineárních grup se nazývají *maticové grupy*, např.

- *speciální lineární grupa* $\mathbf{SL}_n(\mathbf{T})$ všech matic s determinantem 1;
- *ortogonální grupa* $\mathbf{O}_n(\mathbf{T})$ všech ortogonálních matic, tj. takových A, které splňují $AA^T = I$ (nad tělesem $\mathbb{R}$ jde o matice, jejichž řádky, resp. sloupce, jsou ortonormální vektory vzhledem k standardnímu skalárnímu součinu).

Existuje řada dalších geometrických i algebraických konstrukcí abelovských grup, například grupy odvozené od eliptických křivek nebo třídové grupy prvoideálů v číselných tělesech. Některé z těchto konstrukcí mají významné aplikace v kryptografii, v praxi se hojně využívá například Diffie-Hellmanův protokol s grupami na eliptických křivkách nad konečnými tělesy.

Důležitou konstrukcí grup je direktní součin.

Definice. *Direktním součinem* grup $\mathbf{G}_i = (G_i, *_i, {}'^i, e_i)$, $i = 1, \ldots, n$, rozumíme grupu

$$\prod_{i=1}^{n} \mathbf{G}_i = \mathbf{G}_1 \times \cdots \times \mathbf{G}_n = (G_1 \times \cdots \times G_n, *, ', e),$$

jejíž operace jsou definovány po složkách, tj.

$$\begin{aligned}(a_1, \ldots, a_n) * (b_1, \ldots, b_n) &= (a_1 *_1 b_1, \ldots, a_n *_n b_n),\\ (a_1, \ldots, a_n)' &= ((a_1)'^1, \ldots, (a_n)'^n),\\ e &= (e_1, \ldots, e_n).\end{aligned}$$

pro všechna $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \ldots \times G_n$. Je snadné ověřit, že direktní součin splňuje všechny axiomy grup.

V případě, kdy $\mathbf{G}_1 = \ldots = \mathbf{G}_n = \mathbf{G}$, hovoříme o *direktní mocnině* a značíme ji $\mathbf{G}^n$.

Definice grupy obsahuje pouze minimální množství podmínek. Následující tvrzení ukazuje několik aritmetických pravidel (mj. krácení, jednoznačnost jednotky a jednoznačnost inverzních prvků), které z definice snadno plynou a v dalším textu je budeme volně používat.

Tvrzení 1.1 (základní vlastnosti grup)**.** *Buď $\mathbf{G} = (G, *, ', e)$ grupa a $a, b, c \in G$. Pak*

(1) *jestliže $a * c = b * c$ nebo $c * a = c * b$, pak $a = b$;*
(2) *jestliže $a * u = a$ nebo $u * a = a$ pro nějaké $u \in G$, pak $u = e$;*
(3) *jestliže $a * u = e$ nebo $u * a = e$ pro nějaké $u \in G$, pak $u = a'$;*
(4) *$(a')' = a$;*
(5) *$(a * b)' = b' * a'$.*

Důkaz. (1) Je-li $a * c = b * c$, pak také $(a * c) * c' = (b * c) * c'$ a použitím všech tří axiomů dostaneme $(a * c) * c' = a * (c * c') = a * e = a$ a podobně $(b * c) * c' = b$. Tedy $a = b$. Analogicky pro $c * a = c * b$.

(2) Je-li $a * u = a = a * e$, krácením dostáváme $u = e$. Analogicky pro $u * a = a$.

(3) Je-li $a * u = e = a * a'$, krácením dostáváme $u = a'$. Analogicky pro $u * a = e$.

(4) Protože $a' * a = e$, z jednoznačnosti inverzních prvků dostáváme $a = (a')'$.

(5) Protože $(a*b)*(b'*a') = a*(b*b')*a' = a*e*a' = a*a' = e$, z jednoznačnosti inverzních prvků dostáváme $(a*b)' = b'*a'$. □

1.2. **Mocniny a řád prvku.**

Čtenář si snad již zažil, že se grupové operace značí nejrůznějšími způsoby. Nadále se budeme držet multiplikativního zápisu. Nebude-li výslovně uvedeno jinak, uvažujeme-li grupu $\mathbf{G}$, implicitně rozumíme $\mathbf{G} = (G, \cdot, ^{-1}, 1)$. Ze začátku je dobré si u všech výrazů rozmýšlet, jak bychom je přepsali do ostatních značení.

Nyní definujeme *mocniny*. Buď $\mathbf{G}$ grupa, $a \in G$, $n \in \mathbb{Z}$. Označme

$$a^n = \begin{cases} 1 & n = 0 \\ \underbrace{a \cdot a \cdot \ldots \cdot a}_{n} & n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{-n} & n < 0 \end{cases}$$

Tvrzení 1.2 (mocniny)**.** *Buď $\mathbf{G}$ grupa, $a, b \in G$ a $k, l \in \mathbb{Z}$. Pak*

$$a^{k+l} = a^k \cdot a^l, \qquad a^{kl} = (a^k)^l = (a^l)^k$$

a je-li $\mathbf{G}$ abelovská, pak navíc $(ab)^k = a^k b^k$.

Důkaz. Pokud $k, l > 0$, ihned vidíme, že počet prvků a ve výrazech na obou stranách každé rovnosti je stejný. V případě záporných exponentů je třeba vzít v úvahu, že a a a^{-1} se navzájem pokrátí. Např. v první rovnosti, pro $k > 0 > l$, $|l| < |k|$, máme na levé straně součin $k + l$ prvků a, zatímco na pravé straně součin k prvků a a $-l$ prvků a^{-1}. Po vykrácení dostaneme rovnost obou výrazů. Ostatní případy se rozeberou podobně. □

V aditivním značení je mocninou výraz $a + \ldots + a$, resp. $(-a) + \ldots + (-a)$; tyto výrazy zkracujeme jako $n \cdot a$. Tvrzení 1.2 se pak přepíše jako

$$(k + l) \cdot a = k \cdot a + l \cdot a, \qquad (kl) \cdot a = k \cdot (l \cdot a), \qquad k \cdot (a + b) = k \cdot a + k \cdot b,$$

poslední rovnost samozřejmě platí pouze pro abelovské grupy. Pokud vám tyto podmínky připomínají definici vektorového prostoru, jste na správně stopě. Teorie abelovských grup je do značné míry teorií „vektorových prostorů nad $\mathbb{Z}$“, neboli $\mathbb{Z}$-modulů, s řadou aplikací v teorii čísel. Tímto směrem se však v úvodním kurzu ubírat nebudeme.

Definice. *Řádem grupy* $\mathbf{G}$ se rozumí počet prvků její nosné množiny, značíme jej $|\mathbf{G}|$ (tj., formálně vzato, $|\mathbf{G}| = |G|$).

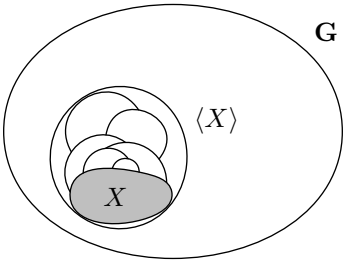
Řádem prvku a v grupě $\mathbf{G}$ se rozumí nejmenší $n \in \mathbb{N}$ takové, že $a^n = 1$, pokud takové n existuje, resp. ∞ v opačném případě. Značíme jej $\operatorname{ord}(a)$.

V Tvrzení 2.5 si ukážeme, že řád prvku je roven řádu jisté podgrupy, ale zatím si vystačíme s definicí pomocí mocnin.

Příklad. Pokud mluvíme o řádu jistého prvku, je třeba říci, v které grupě!

- $\operatorname{ord}(2) = 7$ v grupě $\mathbb{Z}_7$, protože $7 \cdot 2 \equiv 0 \pmod 7$, ale $n \cdot 2 \not\equiv 0 \pmod 7$ pro $n = 1, \ldots, 6$;
- $\operatorname{ord}(2) = 3$ v grupě $\mathbb{Z}_7^*$, protože $2^3 \equiv 1 \pmod 7$, ale $2^n \not\equiv 1 \pmod 7$ pro $n = 1, 2$.

Příklad. V nekonečných grupách mohou řády vycházet všelijak:



Obrázek 1. Ilustrace generování podgrupy $\langle X\rangle_{\mathbf{G}}$.

- v grupě $\mathbb{Q}$ je $\mathrm{ord}(0) = 1$ a $\mathrm{ord}(a) = \infty$ pro všechna $a \neq 0$;
- v grupě $\mathbb{Q}^*$ je $\mathrm{ord}(1) = 1$, $\mathrm{ord}(-1) = 2$ a $\mathrm{ord}(a) = \infty$ pro všechna $a \neq \pm 1$;
- v grupě $\mathbb{C}^*$ existuje prvek libovolného řádu: $\mathrm{ord}(e^{2\pi i/k}) = k$.

Příklad. V konečných grupách řády nevycházejí všelijak:

- v grupě $\mathbb{Z}_6$ je $\mathrm{ord}(0) = 1$, $\mathrm{ord}(1) = 6$, $\mathrm{ord}(2) = 3$, $\mathrm{ord}(3) = 2$, $\mathrm{ord}(4) = 3$ a $\mathrm{ord}(5) = 6$, čili vyskytují se řády $1, 2, 3, 6$;
- v grupě $\mathbf{S}_3$ je $\mathrm{ord}(id) = 1$, $\mathrm{ord}((i\ j)) = 2$, $\mathrm{ord}((i\ j\ k)) = 3$, čili vyskytují se řády $1, 2, 3$.

Všimněte si, že řád každého prvku dělí řád celé grupy. To není náhoda, nýbrž pravidlo, které je speciálním případem Lagrangeovy věty (Věta 2.8), která je náplní příští sekce.

2. Podgrupy

2.1. Generátory.

Lemma 2.1. *Průnik podgrup je podgrupa.*

Důkaz. Buď $\mathbf{G}$ grupa, uvažujme podgrupy $\mathbf{H}_i$, $i \in I$, a označme $H = \bigcap_{i\in I} H_i$. Dokážeme, že je množina H uzavřená na grupové operace. Protože $1 \in H_i$ pro všechna $i \in I$, bude 1 náležet i jejich průniku. Nyní uvažujme $a, b \in H$. Tyto leží v každém H_i a díky uzavřenosti na operace tam leží také prvky a^{-1} a $a \cdot b$. Takže tyto prvky leží i v průniku všech H_i, čili v H. □

Definice. Uvažujme podmnožinu $X \subseteq G$ grupy $\mathbf{G}$. Podgrupou *generovanou množinou* X rozumíme nejmenší podgrupu (vzhledem k inkluzi) grupy $\mathbf{G}$ obsahující podmnožinu X, značíme ji $\langle X\rangle_{\mathbf{G}}$.

Taková podgrupa jistě existuje: stačí vzít průnik všech podgrup obsahujících množinu X, tj.

$$\langle X\rangle_{\mathbf{G}} = \bigcap\{H :\ X \subseteq H,\ \mathbf{H} \leq \mathbf{G}\}.$$

Podle předchozího lemmatu jde skutečně o podgrupu, mezi všemi podgrupami obsahujícími množinu X bude jistě nejmenší.

Jak najít podgrupu generovanou danou množinou? Pro konečné grupy lze v principu použít následující postup: začneme s prvky množiny X a postupně přidáváme všemožné součiny a inverzy. Ve chvíli, kdy nejsme schopni získat žádné nové prvky, naše množina je uzavřená na grupové operace a podgrupa je nalezena (viz obrázek). Leckdy je však efektivnější použít následující tvrzení.

Tvrzení 2.2. *Buď* $\mathbf{G}$ *grupa a* $\emptyset \neq X \subseteq G$. *Pak*

$$\langle X\rangle_{\mathbf{G}} = \{a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n} :\ n \in \mathbb{N},\ a_1, \ldots, a_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Důkaz. Označme M množinu na pravé straně rovnosti. Je potřeba dokázat, že množina M

(1) tvoří podgrupu,
(2) obsahuje X,
(3) je nejmenší podmnožinou grupy $\mathbf{G}$ splňující tyto podmínky.

(1) Součin dvou prvků z M je jistě v M, jednotka $1 = a^0$ je tam také, a uzavřenost na inverzy plyne ze vztahu $(a_1^{k_1} \cdot \ldots \cdot a_n^{k_n})^{-1} = a_n^{-k_n} \cdot \ldots \cdot a_1^{-k_1} \in M$.
(2) Volbou $n = 1, k_1 = 1$ dostaneme libovolný prvek X.
(3) Uvažujme libovolnou podgrupu $\mathbf{H}$ obsahující X. Tato podgrupa musí obsahovat všechny mocniny a^i, $a \in X$, i jejich libovolné násobky, čili celé M. □

Obecné tvrzení o tvaru podgrup generovaných danou podmnožinou má dva důležité speciální případy.

Důsledek 2.3. *Buď* $\mathbf{G}$ *grupa a* $a \in G$. *Pak* $\langle a\rangle_{\mathbf{G}} = \{a^k :\ k \in \mathbb{Z}\}$.

Důsledek 2.4. *Buď* $\mathbf{G}$ *abelovská grupa a* $u_1, \ldots, u_n \in G$. *Pak*

$$\langle u_1, \ldots, u_n\rangle_{\mathbf{G}} = \{u_1^{k_1} \cdot u_2^{k_2} \cdot \ldots \cdot u_n^{k_n} :\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Vidíme, že v abelovských grupách je generování podgrup podobné jako generování vektorových prostorů: v aditivním zápise, tj. pro abelovskou grupu $\mathbf{G} = (G, +, -, 0)$, dostáváme

$$\langle u_1, \ldots, u_n\rangle_{\mathbf{G}} = \{k_1u_1 + k_2u_2 + \ldots + k_nu_n :\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

(S nezávislostí a jednoznačností zápisu je to složitější, ale tím se v této učebnici zabývat nebudeme.)

Příklad. Důležitým typem úlohy je zjistit, jakou podgrupu generuje daná podmnožina. Například:

- $\langle \frac{3}{4}, \frac{1}{3}\rangle_{\mathbb{Q}} = \{k\frac{3}{4} + l\frac{1}{3} :\ k, l \in \mathbb{Z}\} = \{\frac{k}{12} :\ k \in \mathbb{Z}\} = \langle \frac{1}{12}\rangle_{\mathbb{Q}}$. První a poslední rovnost plynou z Důsledku 2.4. K důkazu prostřední je potřeba si uvědomit, že na jednu stranu $\frac{3}{4}, \frac{1}{3} \in \langle \frac{1}{12}\rangle_{\mathbb{Q}}$, a na druhou stranu $\frac{1}{12} = \frac{3}{4} - 2 \cdot \frac{1}{3}$, a tedy $\frac{1}{12} \in \langle \frac{3}{4}, \frac{1}{3}\rangle_{\mathbb{Q}}$.
- $\langle \frac{3}{4}, \frac{1}{3}\rangle_{\mathbb{Q}^*} = \{(\frac{3}{4})^k \cdot (\frac{1}{3})^l :\ k, l \in \mathbb{Z}\} = \{3^k \cdot 4^l :\ k, l \in \mathbb{Z}\}$.

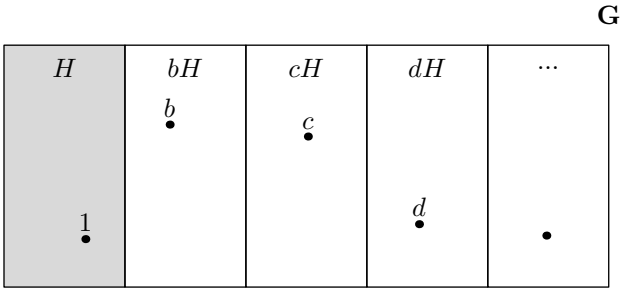
Příklad. Jiným důležitým typem úlohy je, najít k dané grupě $\mathbf{G}$ co nejmenší množinu generátorů, tj. podmnožinu $X \subseteq G$ takovou, že $\mathbf{G} = \langle X\rangle_{\mathbf{G}}$. Například:

- $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$, $\mathbb{Z}^* = \langle -1\rangle$, $\mathbb{Q}^* = \langle -1, \text{prvočísla}\rangle$.
- $\mathbb{Z}_n = \langle 1\rangle$, ale najít malou generující množinu grupy $\mathbb{Z}_n^*$ není obecně snadné. Například, $\mathbb{Z}_7^* = \langle 3\rangle$, ale $\mathbb{Z}_8^* = \langle 3, 5\rangle$ a nelze ji nagenerovat jedním prvkem.
- Pro některé grupy neexistuje minimální množina generátorů. Např. $\mathbb{Q} = \langle \frac{1}{n} : n \in \mathbb{N}\rangle$, libovolné konečné množství generátorů lze vypustit, ale minimální podmnožina neexistuje.

Na závěr dokážeme, že řád prvku (definovaný pomocí mocnin) je roven řádu podgrupy jím generované.

Tvrzení 2.5 (řád prvku vs. řád podgrupy)**.** *Buď* $\mathbf{G}$ *grupa a* $a \in G$. *Pak*

$$\operatorname{ord}(a) = |\langle a\rangle_{\mathbf{G}}|.$$



Obrázek 2. Rozklad grupy $\mathbf{G}$ podle podgrupy $\mathbf{H}$ a jeho transverzála.

Důkaz. Podle Důsledku 2.3 je $\langle a\rangle_{\mathbf{G}} = \{a^k :\ k \in \mathbb{Z}\}$. Všimněte si, že $a^i = a^j$ právě tehdy, když $a^{i-j} = 1$. Je-li $\mathrm{ord}(a) = \infty$, pak žádné $n \neq 0$ s vlastností $a^n = 1$ neexistuje, čili mocniny a^k jsou po dvou různé a podgrupa $\langle a\rangle$ je nekonečná. Je-li $\mathrm{ord}(a) = n < \infty$, pak jsou mocniny $a^0, a^1, \ldots, a^{n-1}$ po dvou různé, ovšem další mocniny nové prvky nepřidají: $a^n = a^0 = 1$, $a^{n+1} = a^n \cdot a^1 = a^1$, $a^{n+2} = a^n \cdot a^2 = a^2$ atd., obecně $a^{qn+r} = (a^n)^q \cdot a^r = a^r$. Tedy $\langle a\rangle_{\mathbf{G}} = \{a^0, a^1, \ldots, a^{n-1}\}$ obsahuje přesně n prvků. □

2.2. **Lagrangeova věta.**

Základní aritmetickou vlastností konečných grup je fakt, že řády podgrup dělí řád celé grupy, tj.

$$\mathbf{H} \leq \mathbf{G} \quad \Rightarrow \quad |\mathbf{H}| \text{ dělí } |\mathbf{G}|.$$

Speciálně, díky Tvrzení 2.5, řád prvku dělí řád celé grupy.

Myšlenka důkazu Lagrangeovy věty není složitá: celou grupu $\mathbf{G}$ rozložíme na několik podmnožin, které jsou po dvou disjunktní a stejně velké jako daná podgrupa $\mathbf{H}$. Počet prvků grupy $\mathbf{G}$ tak bude roven počtu prvků $\mathbf{H}$ krát počet těchto podmnožin. Nesamozřejmou částí důkazu je konstrukce tohoto rozkladu.

Definice. Buď $\mathbf{G}$ grupa a $\mathbf{H}$ její podgrupa:

- množiny $aH = \{ah :\ h \in H\}$, kde $a \in G$, se nazývají *rozkladové třídy* podgrupy $\mathbf{H}$;
- podmnožina $T \subseteq G$ s vlastností $|T \cap aH| = 1$ pro každé $a \in G$ se nazývá *transverzála* rozkladu $\mathbf{G}$ podle $\mathbf{H}$;
- počet rozkladových tříd se nazývá *index* podgrupy $\mathbf{H}$ v grupě $\mathbf{G}$ a značí se
$$[\mathbf{G} : \mathbf{H}] = |\{aH :\ a \in G\}|.$$

Příklad. Buď $\mathbf{G} = \mathbb{Z}$ a $\mathbf{H} = \{h \in \mathbb{Z} :\ n \mid h\}$. Rozkladovou třídu určenou prvkem $a \in \mathbb{Z}$ můžeme vyjádřit

$$aH = \{a + h :\ h \in H\} = \{a + nk :\ k \in \mathbb{Z}\} = \{u \in \mathbb{Z} :\ u \equiv a \pmod n\}.$$

Dvě rozkladové třídy aH, bH jsou buď stejné, nebo disjunktní, přičemž $aH = bH$ právě tehdy, když $a \equiv b \pmod n$. Dostáváme tak n různých po dvou disjunktních rozkladových tříd, $[\mathbf{G} : \mathbf{H}] = n$. Jako transverzálu lze zvolit např. $T = \{0, \ldots, n-1\}$, množinu všech možných zbytků po dělení n.

Lagrangeovu větu dokážeme pomocí dvou základních vlastností rozkladů: za prvé, různé rozkladové třídy jsou disjunktní, a za druhé, všechny rozkladové třídy jsou stejně velké. Analogická tvrzení platí i pro pravé rozkladové třídy.

Lemma 2.6 (disjunkce rozkladových tříd)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pro každé* $a, b \in G$ *platí buď* $aH = bH$*, nebo* $aH \cap bH = \emptyset$*.*

Důkaz. Předpokládejme $aH \cap bH \neq \emptyset$, dokážeme, že $aH = bH$. Uvažujme $c \in aH \cap bH$ a napišme $c = ah_1 = bh_2$ pro nějaká $h_1, h_2 \in H$. Pak pro každé $ah \in aH$ platí

$$ah = ch_1^{-1}h = b\underbrace{h_2h_1^{-1}h}_{\in H} \in bH$$

a podobně pro každé $bh \in bH$ platí

$$bh = ch_2^{-1}h = a\underbrace{h_1h_2^{-1}h}_{\in H} \in aH.$$

Tedy $aH = bH$. □

Lemma 2.7 (velikost rozkladových tříd)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pro každé* $a \in G$ *platí* $|aH| = |H|$*.*

Důkaz. Uvažujme zobrazení $f : G \to G$ definované $f(x) = ax$. Toto zobrazení je prosté: kdyby $ax = f(x) = f(y) = ay$, krácením dostaneme $x = y$. Přitom $f(H) = aH$, tedy $f|_H$ je bijekce mezi H a aH, takže jsou tyto množiny stejně velké. □

Lagrangeovu větu lze formulovat i pro nekonečné grupy, s použitím kardinálních čísel pro označení velikostí množin. Čtenáři, který kardinální čísla neviděl, postačí k porozumění tvrzení vlastnost, že součin velikostí množin je roven velikosti kartézského součinu, tj. $|X| \cdot |Y| = |X \times Y|$. Důkaz věty je pro konečné i nekonečné množiny stejný.

Věta 2.8 (Lagrangeova věta)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pak*

$$|\mathbf{G}| = |\mathbf{H}| \cdot [\mathbf{G} : \mathbf{H}].$$

Důkaz. Zvolme nějakou transverzálu T a napišme

$$G = \bigcup_{a \in T} aH.$$

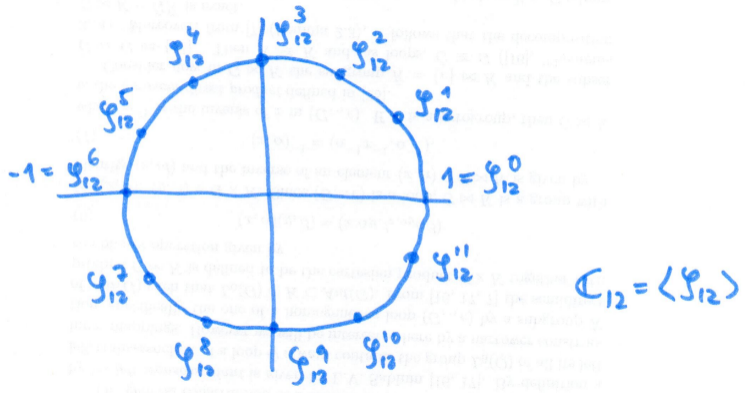
Podle Lemmatu 2.6 jde o disjunktní sjednocení, takže počet prvků lze spočítat jako součet velikostí jednotlivých podmnožin:

$$|\mathbf{G}| = \sum_{a \in T} |aH| = \sum_{a \in T} |H| = |T| \cdot |H| = [\mathbf{G} : \mathbf{H}] \cdot |\mathbf{H}|.$$

V druhé rovnosti jsme použili Lemma 2.7 a ve čtvrté rovnosti jsme použili vztah $|T| = [\mathbf{G} : \mathbf{H}]$, který plyne z Lemmatu 2.6. □

Příklad. Speciálním případem Lagrangeovy věty je *Eulerova věta* z elementární teorie čísel, která říká, že pro a, m nesoudělné platí $a^{\varphi(m)} \equiv 1 \pmod{m}$, kde φ je Eulerova funkce. Důkaz: buď $\mathbf{G} = \mathbb{Z}_m^*$ a $a \in \mathbb{Z}_m^*$ (tj. a je celé číslo nesoudělné s m), pak $\operatorname{ord}(a)$ dělí $|\mathbb{Z}_n^*| = \varphi(m)$, čili $\varphi(m) = k \cdot \operatorname{ord}(a)$ pro nějaké k, takže v grupě $\mathbb{Z}_m^*$ platí

$$a^{\varphi(m)} = (a^{\operatorname{ord}(a)})^k = 1^k = 1.$$



Obrázek 3. Ilustrace faktu, proč se cyklické grupy nazývají cyklické.

3. Cyklické grupy

3.1. Podgrupy, generátory, řády prvků.

Grupa $\mathbf{G}$ se nazývá *cyklická*, pokud je generovaná jedním prvkem, tj.

$$\mathbf{G} = \langle a \rangle_{\mathbf{G}}$$

pro nějaké $a \in G$. Její prvky lze díky Důsledku 2.3 vyjádřit jako mocniny generátoru,

$$G = \{a^k : \ k \in \mathbb{Z}\},$$

z čehož je vidět, že je to nutně grupa abelovská. Z Tvrzení 2.5 plyne, že je-li řád a nekonečný, pak jsou tyto mocniny po dvou různé, a je-li $\mathrm{ord}(a) = n$ konečný, pak $G = \{a^0, a^1, \ldots, a^{n-1}\}$. Odsud pochází název pro cyklické grupy: při násobení daným prvkem a cyklicky procházíme přes všechny prvky grupy $\mathbf{G}$.

Příklady.

- Grupy $\mathbb{Z}$ a $\mathbb{Z}_n$, $n \in \mathbb{N}$, jsou cyklické, generované prvkem 1.
- Grupy $\mathbb{C}_n \leq \mathbb{C}^*$ sestávající ze všech komplexních kořenů polynomu $x^n - 1$ jsou cyklické, $\mathbb{C}_n = \langle e^{2\pi i/n} \rangle$.
- V této sekci si dokážeme, že grupy $\mathbb{Z}_p^*$ jsou cyklické pro každé prvočíslo p (Věta 3.7). Například $\mathbb{Z}_5^* = \langle 2 \rangle$, $\mathbb{Z}_7^* = \langle 3 \rangle$, $\mathbb{Z}_{11}^* = \langle 2 \rangle$.
- Některé grupy $\mathbb{Z}_n^*$, n složené, jsou cyklické, např. $\mathbb{Z}_6^* = \{1, 5\} = \langle 5 \rangle$, ale některé ne, např. grupa $\mathbb{Z}_8^*$ cyklická není.
- Každá grupa $\mathbf{G}$ prvočíselného řádu je cyklická. Uvažujme podgrupu $\langle a \rangle$, $a \neq 1$. Podle Lagrangeovy věty je $|\langle a \rangle|$ dělí $|\mathbf{G}|$, přitom $|\langle a \rangle| > 1$, tedy $|\langle a \rangle| = |\mathbf{G}|$ a prvek a tuto grupu generuje.

Nejprve se podíváme, jak vypadají podgrupy cyklických grup.

Tvrzení 3.1. *Každá podgrupa cyklické grupy je cyklická.*

Důkaz. Buď $\mathbf{H}$ podgrupa cyklické grupy $\mathbf{G} = \langle a \rangle$. Je-li $H = \{1\}$, pak $\mathbf{H} = \langle 1 \rangle$. V opačném případě označme k nejmenší kladné číslo takové, že $a^k \in H$ (takové jistě existuje: je-li $1 \neq b \in H$, pak $b = a^l$ pro nějaké l a buď b nebo b^{-1} má

exponent kladný). Dokážeme, že $\mathbf{H} = \langle a^k \rangle$. Inkluze $\langle a^k \rangle \subseteq H$ je zřejmá. Pro spor tedy předpokládejme, že existuje nějaký prvek $a^n \in H \setminus \langle a^k \rangle$. Nutně $k \nmid n$, jinak bychom měli $a^n = (a^k)^{n/k} \in \langle a^k \rangle$. Napišme $n = kq + r$, kde $0 < r < k$. Pak

$$a^r = a^{n-kq} = a^n \cdot (a^k)^{-q} \in H,$$

protože a^n i a^k leží v H, což je spor s volbou k jako nejmenšího kladného čísla s vlastností $a^k \in H$. □

Příklad. Grupa $\mathbb{Z}$ je cyklická, čili její podgrupy jsou cyklické, tedy tvaru

$$\mathbf{H} = \langle k \rangle = k\mathbb{Z} = \{a \in \mathbb{Z} : \ k \mid a\}.$$

Přitom $k\mathbb{Z} = l\mathbb{Z}$ právě tehdy, když $k = \pm l$. Podgrupy jsou tedy ve vzájemně jednoznačné korepondenci s nezápornými čísly a $k\mathbb{Z} \subseteq l\mathbb{Z}$ právě tehdy, když $l \mid k$. Čili podgrupy jsou uspořádány vzhledem k inkluzi opačně než množina $\mathbb{N} \cup \{0\}$ dělitelností.

Pro konečné cyklické grupy je situace složitější, mnoho různých prvků může generovat stejné podgrupy.

Lemma 3.2 (podgrupy cyklických grup)**.** *Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa. Pak*

(1) $\langle a^k, a^l \rangle = \langle a^{\mathrm{NSD}(k,l)} \rangle$,
(2) *je-li $|\mathbf{G}| = n$, pak $\langle a^k \rangle = \langle a^{\mathrm{NSD}(k,n)} \rangle$.*

Důkaz. (1) Protože $\mathrm{NSD}(k,l)$ dělí k i l, platí $a^k, a^l \in \langle a^{\mathrm{NSD}(k,l)} \rangle$, čímž máme prokázánu inkluzi $\subseteq$. Naopak, podle Bézoutovy rovnosti je $\mathrm{NSD}(k,l) = uk + vl$ pro nějaká $u, v \in \mathbb{Z}$, a tedy

$$a^{\mathrm{NSD}(k,l)} = a^{uk+vl} = (a^k)^u \cdot (a^l)^v \in \langle a^k, a^l \rangle,$$

čímž máme prokázánu inkluzi $\supseteq$.

(2) Dosadíme $l = n$: pak $\langle a^{\mathrm{NSD}(k,n)} \rangle = \langle a^k, a^n \rangle = \langle a^k \rangle$, protože $a^n = 1$. □

Tvrzení 3.3 (generátory cyklických grup)**.** *Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa.*

(1) *Pokud je $\mathbf{G}$ nekonečná, generátorem jsou pouze prvky a, a^{-1}.*
(2) *Pokud je $\mathbf{G}$ konečná řádu n, generátorem jsou právě prvky a^k, kde $k \in \{1, \ldots, n-1\}$ je nesoudělné s n.*

Důkaz. (1) Oba prvky a, a^{-1} grupu $\mathbf{G}$ generují, protože $\{a^k : \ k \in \mathbb{Z}\} = \{a^{-k} : k \in \mathbb{Z}\}$. Žádný jiný generátor grupa $\mathbf{G}$ nemá: kdyby $\mathbf{G} = \langle a^n \rangle$ pro nějaké n, pak by existovalo $m \in \mathbb{Z}$ takové, že $a = (a^n)^m$, a dostali bychom $1 = (a^n)^m \cdot a^{-1} = a^{mn-1}$; řád a je ovšem nekonečný, a tedy $mn = 1$, čili $n = \pm 1$.

(2) Podle Lemmatu 3.2 je $\langle a^k \rangle = \langle a^{\mathrm{NSD}(k,n)} \rangle$. Pokud $\mathrm{NSD}(k,n) = 1$, pak $\langle a^k \rangle = \langle a \rangle = \mathbf{G}$. Pokud $\mathrm{NSD}(k,n) = d \neq 1$, pak $\langle a^k \rangle = \langle a^d \rangle = \{a^d, a^{2d}, \ldots, a^{\frac{n}{d}d}\}$ je vlastní podgrupa. □

Příklad (podgrupy grupy $\mathbb{Z}_n$)**.** Grupa $\mathbb{Z}_n$ je cyklická, čili její podgrupy jsou cyklické, tedy tvaru

$$\langle k \rangle = k\mathbb{Z}_n = \{ku \bmod n : \ u = 0, \ldots, n-1\},$$

pro nějaké $k \in \{0, \ldots, n-1\}$. Z Lemmatu 3.2(2) s volbou $a = 1$ plyne, že $k\mathbb{Z}_n = \mathrm{NSD}(k,n)\mathbb{Z}_n$, tedy $k\mathbb{Z}_n = l\mathbb{Z}_n$ právě tehdy, když $\mathrm{NSD}(k,n) = \mathrm{NSD}(l,n)$. Podgrupy jsou tedy ve vzájemně jednoznačné korepondenci s děliteli čísla n. Pro $k, l \mid n$ pak platí, že $k\mathbb{Z}_n \subseteq l\mathbb{Z}_n$ právě tehdy, když $l \mid k$. Čili podgrupy jsou uspořádány vzhledem

k inkluzi opačně než množina všech dělitelů čísla n dělitelností. Podle Tvrzení 3.3 je $\mathbb{Z}_n = \langle k \rangle$ právě tehdy, když jsou k, n nesoudělná.

Příklad (podgrupy grupy $\mathbb{Z}_p^*$)**.** Grupa $\mathbb{Z}_{11}^* = \langle 2 \rangle$ je cyklická řádu 10, čili její podgrupy jsou cyklické, tedy tvaru

$$\langle 2^k \rangle = \{2^{uk} \bmod 11 : \ u = 0, \ldots, 10\},$$

pro nějaké $k \in \{0, \ldots, 9\}$. Z Lemmatu 3.2(2) plyne, že $\langle 2^k \rangle = \langle 2^l \rangle$ právě tehdy, když $\mathrm{NSD}(k, n) = \mathrm{NSD}(l, n)$. Podgrupy jsou tedy ve vzájemně jednoznačné korepondenci s děliteli čísla 10, máme tedy čtyři podgrupy,

$$\langle 2^1 \rangle = \mathbb{Z}_{11}^*, \ \langle 2^2 \rangle = \{1, 4, 5, 9, 3\}, \ \langle 2^5 \rangle = \{1, 10\}, \ \langle 2^{10} \rangle = \{1\}.$$

Generátory jsou prvky 2^k takové, že k je nesoudělné s 10, tedy prvky $2^1 = 2$, $2^3 = 8$, $2^6 = 7$ a $2^9 = 6$. Všimněte si, že to jsou právě čísla, která nepatří do žádné z vlastních podgrup vypsaných výše.

Úloha se přímočaře zobecní na libovolnou grupu $\mathbb{Z}_p^*$, p prvočíslo, o které si ukážeme, je vždy cyklická, byť není zřejmé, který prvek a je generátorem. Podgrupy pak budou právě $\langle a^k \rangle$, kde $k \mid p-1$, generátory budou právě prvky a^k, kde $\mathrm{NSD}(k, p-1) = 1$.

Z Tvrzení 3.3 plyne, že cyklická grupa řádu n má právě $\varphi(n)$ generátorů, kde φ značí Eulerovu funkci. Tohoto faktu využijeme k řešení obecnější úlohy: spočítáme počet prvků každého řádu. V nekonečných cyklických grupách mají všechny prvky kromě jednotky řád nekonečný. V konečných grupách dává Lagrangeova věta omezení na přípustné řády. Ukážeme si, že v cyklických grupách prvky všech přípustných řádů existují a jejich počet je dán Eulerovou funkcí.

Tvrzení 3.4 (řády prvků cyklických grup)**.** *Cyklická grupa konečného řádu n obsahuje právě $\varphi(d)$ prvků řádu d pro každé $d \mid n$.*

Důkaz. Buď $\mathbf{G}$ cyklická grupa konečného řádu n. Každý prvek řádu $d \mid n$ je generátorem nějaké cyklické podgrupy řádu d. Taková podgrupa však v $\mathbf{G}$ existuje pouze jedna: podle Lemmatu 3.2 jsou všechny podgrupy v $\mathbf{G}$ tvaru $\langle a^k \rangle$, $k \mid n$. Přitom $|\langle a^k \rangle| = \frac{n}{k}$, čili $\langle a^{\frac{n}{d}} \rangle$ je jediná podgrupa řádu d. Ta má podle Tvrzení 3.3 právě $\varphi(d)$ generátorů. □

Tvrzení o počtu prvků daného řádu lze použít k důkazu následující kombinatorické identity.

Tvrzení 3.5. *Pro každé $n \in \mathbb{N}$ platí $\sum_{d \mid n} \varphi(d) = n$.*

Důkaz. Budeme počítat počet prvků grupy $\mathbb{Z}_n$ dvěma způsoby. Jeden způsob je triviální: grupa obsahuje čísla $0, \ldots, n-1$, tedy $|\mathbb{Z}_n| = n$. Podruhé spočítáme prvky podle řádů: podle Lagrangeovy věty jsou přípustné řády $d \mid n$, tedy $|\mathbb{Z}_n| = \sum_{d \mid n} u_d$, kde u_d značí počet prvků řádu d. Tvrzení 3.4 říká, že $u_d = \varphi(d)$. □

3.2. **Multiplikativní grupy konečných těles jsou cyklické.**

Tvrzení uvedené v názvu podsekce má dalekosáhlé důsledky v teorii konečných těles. K jeho důkazu použijeme následující kritérium cykličnosti.

Lemma 3.6. *Buď $\mathbf{G}$ konečná grupa a předpokládejme, že pro každé k grupa $\mathbf{G}$ obsahuje nejvýše k prvků a splňujících $a^k = 1$. Pak je grupa $\mathbf{G}$ cyklická.*

Důkaz. Označme $n = |\mathbf{G}|$ a u_k počet prvků řádu k v grupě $\mathbf{G}$. Podle Lagrangeovy věty je $u_k = 0$ pro všechna $k \nmid n$, a tedy $n = \sum_{d|n} u_d$ (počítáme prvky $\mathbf{G}$ podle jejich řádu jako v Tvrzení 3.5).

Uvažujme nějaký prvek a řádu k v $\mathbf{G}$. Podgrupa $\langle a \rangle$ je cyklická řádu k a všechny prvky $b \in \langle a \rangle$ splňují $b^k = 1$. Podle předpokladu v $\mathbf{G}$ žádné jiné prvky s touto vlastností nejsou, takže $\langle a \rangle$ je jediná cyklická podgrupa řádu k v $\mathbf{G}$. Podle Tvrzení 3.3 má $\varphi(k)$ generátorů, a tedy $u_k = \varphi(k)$.

Čili pro každé $d \mid n$ platí $u_d = 0$ nebo $u_d = \varphi(d)$. Dokážeme, že vždy nastane druhá možnost: podle Tvrzení 3.5 je $\sum_{d|n} \varphi(d) = n = \sum_{d|n} u_d$, takže $u_d = \varphi(d)$ pro všechna $d \mid n$. Speciálně $u_n \neq 0$, a tedy v $\mathbf{G}$ existuje prvek řádu n, neboli generátor. □

Věta 3.7. *Buď $\mathbf{T}$ těleso a $\mathbf{G}$ konečná podgrupa grupy $\mathbf{T}^*$. Pak $\mathbf{G}$ je cyklická.*

Důkaz. Polynom $x^k - 1$ má nejvýše k kořenů v tělese $\mathbf{T}$. Tedy grupa $\mathbf{G} \leq \mathbf{T}^*$ může obsahovat nejvýše k prvků a splňujících $a^k = 1$ a můžeme aplikovat předchozí kritérium. □

Speciálně, multiplikativní grupy konečných těles jsou cyklické. Jejich generátorům se říká *primitivní prvky*. Pozor, prvek α v tělese $\mathbb{Z}_p[\alpha]/(m)$ být primitivní může, ale nemusí: pozitivním příkladem $\mathbb{F}_4 = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$, negativním příkladem je $\mathbb{F}_9 = \mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$, kde α generuje pouze čtyřprvkovou podgrupu grupy $\mathbb{F}_9^*$. Primitivní prvky se používají například v algoritmu rychlé Fourierovy transformace, která umí vyhodnocovat a interpolovat polynomy v bodech $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ v čase $O(n \log n)$ (zatímco pro n náhodně zvolených bodů bychom standardními metodami potřebovali kvadratický čas).

Není bez zajímavosti, že pro grupy $\mathbb{Z}_p^*$ lze znění Věty 3.7 interpretovat čistě v jazyce elementární teorie čísel: pro každé prvočíslo p existuje číslo a (generátor té grupy) takové, že každé $b \in \{1, \ldots, p-1\}$ lze vyjádřit právě jedním způsobem jako $b = a^k \bmod p$ pro nějaké $k \in \{0, \ldots, p-2\}$.