Algebra 2 (NMAG 202)

poznámky k streamu

Jan Šťovíček

6. 4. 2020

Katedra algebry MFF UK

Cyklické grupy – připomenutí

- Cyklická grupa je grupa tvaru $G = \langle a \rangle$, tj. generovaná jediným prvkem.
- Každá cyklická grupa je isomorfní
  - grupě $(\mathbb{Z}, +, -, 0)$, je-li $\mathrm{ord}(a) = \infty$, nebo
  - grupě $(\mathbb{Z}_n, +, -, 0)$, je-li $\mathrm{ord}(a) = n < \infty$.
- Cílem je ukázat větu 4.6:

  Je-li T těleso a G konečná podgrupa T^*, pak je G cyklická.

Podgrupy cyklických grup

Tvrzení 4.1
Každá podgrupa cyklické grupy je cyklická.

Důkaz:

- Buď $H \leq G$ a BÚNO G je $(\mathbb{Z}, +, -, 0)$ nebo $(\mathbb{Z}_n, +, -, 0)$.
- Je-li $H \neq \{0\}$, vybereme nejmenší kladné $a \in H$.
- Tj. $\langle a \rangle = \{na \mid n \in \mathbb{Z}\} \subseteq H$.
- Kdyby $b \in H \setminus \langle a \rangle$, můžeme psát $b = qa + r$ pro nějaké $q \in \mathbb{Z}$ a $0 < r < a$.
- Pak ale $r = b - qa \in H$ a $0 \neq r < a$ je ve sporu s volbou a.

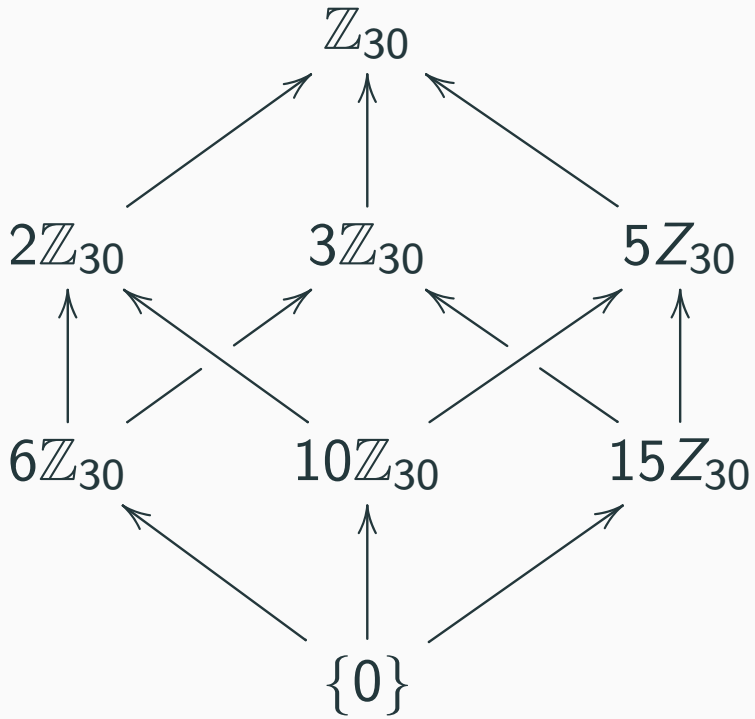
Lemma 4.2
Je-li $G = \langle a \rangle$ cyklická grupa, pak

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

Důkaz: Určitě $a^k, a^l \in \langle a^{\mathrm{NSD}(k,l)} \rangle$. Vyjádříme-li $\mathrm{NSD}(k, l) = uk + vl$, pak $a^{\mathrm{NSD}(k,l)} = (a^k)^u \cdot (a^l)^v$.

Příklady

- Podgrupy $\mathbb{Z}$ jsou přesně $k\mathbb{Z} = \{nk \mid n \in \mathbb{Z}\}$, $k \geq 0$.
- Svaz podgrup $\mathbb{Z}_{30}$:



Kolik různých generátorů má cyklická grupa?

Tvrzení 4.3

1. Nekonečná cyklická grupa má přesně 2 různé generátory.
2. Konečná cyklická grupa řádu n má přesně $\varphi(n)$ různých generátorů (Eulerova funkce).

Důkaz:

1. BÚNO $G = \mathbb{Z}$. Generátory jsou přesně 1 a $-1 \in \mathbb{Z}$.
2. BÚNO $G = \mathbb{Z}_n$. Generátory jsou přesně $k \in \mathbb{Z}_n$ nesoudělné s n (vizte lemma 4.2).

Hrátky s Eulerovou funkcí

Tvrzení 4.4
Cyklická grupa konečného řádu n obsahuje pro každé $d|n$ právě $\varphi(d)$ prvků řádu d.

Důkaz:

- Ať $d|n$ a BÚNO $G = \mathbb{Z}_n$.
- Každý prvek řádu d generuje podgrupu G řádu d.
- Ale podle lemmatu 4.2 obsahuje G jedinou podgrupu řádu d:

$$H = \left\langle \frac{n}{d} \right\rangle = \left\{ 0, \frac{n}{d}, \frac{2n}{d}, \frac{3n}{d}, \dots \right\}.$$

- Čili G má tolik prvků řádu d, kolik má H generátorů.

Tvrzení 4.5
Pro každé $n \in \mathbb{N}$ platí $\sum_{d|n} \varphi(d) = n$.

Charakterizace cyklických grup (klíč k důkazu věty 4.6)

Lemma 4.7
Je-li G konečná grupa taková, že pro každé k existuje nejvýše k prvků $a \in G$ splňujících $a^k = 1$, pak je G cyklická.

Důkaz:

- Označme $n = |G|$ a pro každé k, $u_k :=$ počet prvků řádu k.
- Pokud $k \nmid n$, pak $u_k = 0$ (Lagrangeova věta). Tj. $n = \sum_{d|n} u_d$.
- Je-li $u_d \neq 0$, pak existuje prvek $a \in G$ řádu d, který nutně generuje podgrupu $\langle a \rangle \subseteq G$ řádu d.
- Ovšem každé $b \in \langle a \rangle$ splňuje $b^d = 1$, takže $\langle a \rangle$ je nutně jediná cyklická podgrupa G řádu d.
- Z tvrzení 4.4 je tedy u_d buď $\varphi(d)$ nebo 0.
- Z tvrzení 4.5 ale $n = \sum_{d|n} \varphi(d)$ a odtud $u_d = \varphi(d) \ \ \forall d|n$.
- Speciálně $u_n = \varphi(n) > 0$, tj. G má prvek a řádu n a $G = \langle a \rangle$.

Konečné podgrupy multiplikativní grupy tělesa jsou cyklické

Věta 4.6
Je-li T těleso a G konečná podgrupa T^*, pak je G cyklická.

Důkaz: Prvky $a \in T^*$ splňující $a^k = 1$ jsou přesně kořeny polynomu $x^k - 1 \in T[x]$ a je jich tedy nejvýše k.

Faktory obecně

- Idea faktorů je ztotožnit objekty, které chceme považovat za stejné.
- Princip jsme viděli například
  - u Burnsideovy věty (věchny prvky orbity pro nás byly stejné),
  - v teorii dělitelnosti (asociované prvky oboru integrity pro nás byly z pohledu dělitelnosti stejné),
  - u kongruencí (u čísel nás zajímal jen zbytek po dělení m).
- Obecný postup při "ztotožňování objektů":
  - máme nějakou množinu prvků, která nás zajímá (např. $\mathbb{Z}$),
  - máme na ní nějakou relaci ekvivalence, která říká, které prvky jsou stejné (např. $\equiv_m$),
  - uvažujeme množinu bloků ekvivalence (např. $(\mathbb{Z}/\equiv_m) = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$).

Faktorgrupy

- Začneme s grupou $(G, \cdot, ^{-1}, 1)$ a relací ekvivalence $\sim$ na G.
- Chtěli bychom definovat grupu $(G/\!\sim, \cdot, ^{-1}, e)$ předpisem

$$[a]_\sim \cdot [b]_\sim := [ab]_\sim, \quad [a]_\sim^{-1} := [a^{-1}]_\sim \quad \text{a} \quad e := [1]_\sim.$$

- Potenciální problém: operace nemusí být dobře definované! Aby byly, musí platit

$$a_1 \sim a_2 \quad \& \quad b_1 \sim b_2 \implies a_1 b_1 \sim a_2 b_2,$$
$$a \sim b \implies a^{-1} \sim b^{-1}.$$

- Relace ekvivalence na grupě, která tyto 2 podmínky splňuje, se říká kongruence.
- Je-li $\sim$ kongruence na G, pak $G/\!\sim$ s operacemi výše je automaticky grupa, např.

$$([a]_\sim \cdot [b]_\sim) \cdot [c]_\sim = [(ab)c]_\sim = [a(bc)]_\sim = [a]_\sim \cdot ([b]_\sim \cdot [c]_\sim).$$

Kongruence versus normální podgrupy

Buď $(G, \cdot, ^{-1}, 1)$ grupa a $\sim$ kongruence na G, tj.

$$a_1 \sim a_2 \;\&\; b_1 \sim b_2 \Rightarrow a_1 b_1 \sim a_2 b_2 \quad \text{a} \quad a \sim b \Rightarrow a^{-1} \sim b^{-1}.$$

Pozorování: $N := [1]_\sim$ je normální podgrupa G.

- $1 \in [1]_\sim$,
- $g \sim 1$ a $h \sim 1 \implies gh \sim 1$ a $g^{-1} \sim 1$.
- $g \sim 1$ a $a \in G \implies aga^{-1} \sim a \cdot 1 \cdot a^{-1} = 1$.

Pozorování: Bloky $\sim$ jsou přesně rozkladové třídy N, tj.

$$(G/\sim) = \{aN \mid a \in G\} = \{Na \mid a \in G\}.$$

- Máme totiž $g \sim h \Leftrightarrow h^{-1}g \in N \Leftrightarrow gN = hN$.

Kongruence versus normální podgrupy – pokračování

Tvrzení
Buď $(G, \cdot, ^{-1}, 1)$ grupa. Pak existuje bijekce mezi

1. kongruencemi na G a
2. normálními podgrupami $N \trianglelefteq G$.

Důkaz:

- Je-li $\sim$ kongruence, položíme $N := [1]_\sim$.
- Je-li naopak $N \trianglelefteq G$, definujeme

  $$g \sim_N h \quad \text{pokud} \quad h^{-1}g \in N \quad (\Leftrightarrow gN = hN \Leftrightarrow Ng = Nh).$$

- Ověříme, že $\sim_N$ je kongruence:
  - Pokud $a_2^{-1}a_1 \in N$ a $b_2^{-1}b_1 \in N$, pak
    $(a_2b_2)^{-1}(a_1b_1) = b_2^{-1}(a_2^{-1}a_1)b_1 = (b_2^{-1}b_1)b_1^{-1}(a_2^{-1}a_1)b_1 \in N.$
  - $b^{-1}a \in N \implies a(b^{-1}a)^{-1}a^{-1} = a(a^{-1}b)a^{-1} = ba^{-1} \in N.$
- Nakonec $[1]_{\sim_N} = N$.

Shrnutí

- Buď $(G, \cdot, ^{-1}, 1_G)$ grupa a $N \trianglelefteq G$ normální podgrupa.
- Pak máme tzv. faktorgrupu G podle N s nosnou množinou

$$G/N = \{aN \mid a \in G\} = \{Na \mid a \in G\}$$

a operacemi

$$aN \cdot bN := (ab)N, \quad (aN)^{-1} := a^{-1}N \quad \text{a} \quad 1_{G/N} := 1N = N.$$

Příklady faktorgrup

1. Pro $G = \mathbb{Z}$, $N = m\mathbb{Z}$ máme isomorfismus

$$\begin{aligned} \mathbb{Z}_m &\xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}, \\ a &\mapsto a + m\mathbb{Z}. \end{aligned}$$

2. Je-li $G = S_n$ a $N = A_n$ ($n \geq 2$), pak máme rozklad

$$S_n/A_n = \{A_n, \{\text{liché permutace}\}\}$$

   a isomorfismus

$$\begin{aligned} S_n/A_n &\xrightarrow{\sim} \mathbb{Z}_2, \\ A_n &\mapsto 0, \\ \{\text{liché permutace}\} &\mapsto 1. \end{aligned}$$

3. Na rozmyšlení: Jak vypadá faktorgrupa $\mathbb{R}/\mathbb{Z}$?