Sbírka příkladů

z odborné soutěže pro předmět Algebra I konané v semestru Jaro 2014

Autorský kolektiv: Radan Kučera, Ondřej Klíma a Jaromír Kuben

Příklady jsou určeny těm studentům, kteří mají hlubší zájem o algebru. Jsou tedy zamýšleny nejen pro studenty Obecné matematiky nebo studenty Statistiky a analýzy dat, ale také pro všechny ostatní studenty včetně studentů učitelství matematiky, tedy bez ohledu na studijní obor – zkrátka pro všechny, kterým je blízký abstraktní styl myšlení a kteří budou, například při volbě tématu bakalářské práce, inklinovat ke studiu abstraktních matematických oborů.

První část sbírky obsahuje zadání 10 příkladů, jež byly v semestru Jaro 2014 pravidelně zadávány v rámci soutěže podpořené FRMU a jsou proto označeny jako kolo 1 až 10. Druhá část sestává ze vzorových řešení k jednotlivým kolům, které jsou někdy rozšířeny o zadání souvisejících příkladů řešených na semináři, který byl nepovinnou součástí soutěže. U každého kola jsou v úvodu uvedeny doporučené znalosti, odkazy míří na přednášky o grupách probírané v Algebře I v jarním semestru 2014; tyto přednášky jsou k dispozici na stránce
https://is.muni.cz/el/1431/jaro2014/M2150/um/Algebra2014grupy.pdf.

Část I – Zadání

1. kolo – Zápis permutací pomocí druhých mocnin

Doporučené znalosti: permutace – po str. 9 v přednášce.

Zadání: Buď $n > 1$ přirozené číslo, pro které uvažujme permutační grupu $(\mathbb{S}_n, \circ)$. Pro libovolnou permutaci $\sigma \in \mathbb{S}_n$ označme $\mathsf{r}_1(\sigma)$ počet pevných bodů permutace σ, tj. takových čísel i, $1 \leq i \leq n$, která splňují $\sigma(i) = i$. Dále pro libovolné přirozené číslo $k > 1$ označme $\mathsf{r}_k(\sigma)$ počet cyklů délky k v rozkladu permutace σ na součin nezávislých cyklů a položme $\mathsf{r}(\sigma) = \sum_{k=1}^{n} \mathsf{r}_k(\sigma)$.

a) (1 bod) Vysvětlete, proč pro libovolnou permutaci σ platí $\sum_{k=1}^{n} k \cdot \mathsf{r}_k(\sigma) = n$.

b) (2 body) Dokažte, že pro paritu permutace $\mathsf{p}(\sigma)$ permutace σ platí $\mathsf{p}(\sigma) = (-1)^{n-\mathsf{r}(\sigma)}$.

c) (3 body) Nalezněte podmínku, ve které vystupují čísla $\mathsf{r}_k(\sigma)$, ale nikoliv sama permutace σ, aby nalezená podmínka byla ekvivalentní s podmínkou

$$\exists \tau \in \mathbb{S}_n \,:\, \sigma = \tau^2 \,.$$

Dokažte ekvivalenci těchto podmínek.

d) (4 body) Určete, pro které permutace $\sigma \in \mathbb{S}_n$ existují $\tau, \rho \in \mathbb{S}_n$ splňující $\sigma = \tau^2 \circ \rho^2$. Tuto charakterizaci dokažte.

Komentář: Terminologie není zcela ustálena, někdy se pevné body permutací považují za cykly délky jedna (a v tomto pojetí je pak $\mathsf{r}(\sigma)$ počet všech cyklů v rozkladu permutace σ na součin nezávislých cyklů). My jsme však na přednášce v souladu se skripty definovali jen cykly délky $k \geq 2$, proto se v zadání vyhýbáme pojmu „cyklus délky jedna“.

Pro první seznámení s použitými pojmy položme $n = 8$ a uvažme permutaci

$$\alpha = (1,2)(4,5,6,7) \in \mathbb{S}_8.$$

Pro tuto permutaci ihned vidíme, že $\mathsf{r}_2(\alpha) = 1$ a $\mathsf{r}_4(\alpha) = 1$. Dále $\mathsf{r}_1(\alpha) = 2$, protože prvky 3 a 8 se zobrazují v permutaci α samy na sebe a každý z nich je tedy pevným bodem permutace α. Pro ostatní k je potom hodnota $\mathsf{r}_k(\alpha)$ rovna 0. Proto vidíme, že rovnost v části a) platí: $1 \cdot 2 + 2 \cdot 1 + 4 \cdot 1 = 8$. Podle definice funkce r je dále $\mathsf{r}(\alpha) = 4$. Odtud dostáváme, že hodnota $(-1)^{8-4}$ v části b) je skutečně rovna paritě premutace α, která je sudou permutací. Poznamenejme ještě, že pro permutaci α vhodná permutace τ v části c) neexistuje, ovšem dvojice permutací τ, ρ v části d) naopak existuje.

Při práci s paritou nemusíte používat přímo definici, ale můžete využít některý ekvivalentní způsob výpočtu, který se používá ve skriptech nebo byl dokázán na přednášce. Při řešení se snažte příslušné použité věty z teorie vhodně citovat. (Např. „dle základní definice“, „dle věty číslo $x.y$ ze skript“, „dle poznámky na straně x ze slajdů k přednášce“ apod.)

Druhou mocninou permutace τ použitou v částech c) a d) se rozumí, v souladu s obvyklým značením v teorii grup, permutace $\tau \circ \tau$.

Řešení – str. 16.

2. kolo – Exponent permutační grupy

Doporučené znalosti: řád prvků a exponent grupy – po str. 28 v přednášce.

Zadání:

a) (2 body) Určete, která komplexní čísla α mají v grupě $(\mathbb{C}^*, \cdot)$ konečný řád.

b) (2 body) Pro libovolné přirozené číslo n určete, kolik existuje v grupě $(\mathbb{C}^*, \cdot)$ prvků řádu n.

c) (3 body) Pro každé přirozené číslo $n \leq 12$ zjistěte, jaký největší řád může mít prvek grupy $(\mathbb{S}_n, \circ)$, a napište jeden prvek, který tento maximální řád má. Pro tato přirozená čísla $n \leq 12$ spočítejte také exponent grupy $(\mathbb{S}_n, \circ)$.

d) (3 body) Pro libovolné přirozené číslo n označme e_n exponent grupy $(\mathbb{S}_n, \circ)$. Nalezněte vhodný vzorec popisující rozklad čísla e_n na součin prvočísel. Nalezený vzorec dokažte.

Komentář: Protože se někdy objevuje i jiná definice, připomeňme, že jsme definovali přirozená čísla jako *kladná* celá čísla, nulu tedy nepovažujeme za přirozené číslo.

Na přednášce jsme definovali množinu $\mathbb{C}^*$ jako množinu všech nenulových komplexních čísel, tedy $(\mathbb{C}^*, \cdot)$ je grupa na této množině vzhledem k operaci násobení komplexních čísel.

Pro libovolné přirozené číslo n označme m_n největší z řádů prvků grupy $(\mathbb{S}_n, \circ)$. Podle definice je $(\mathbb{S}_1, \circ)$ grupa všech bijekcí na množině $\{1\}$, tedy $\mathbb{S}_1 = \{\mathrm{id}\}$. Jediný prvek této grupy, identita, má tedy řád $m_1 = 1$, exponent této grupy je také $e_1 = 1$. Vaším úkolem v části c) je určit největší možný řád m_n prvku i exponent e_n grupy $(\mathbb{S}_n, \circ)$ pro všechna přirozená $n \leq 12$. Naproti tomu v části d) máte najít vzorec jen pro e_n, nikoli pro m_n.

Připomeňme ještě Moivreovu větu, která by mohla být při řešení užitečná. Každé nenulové komplexní číslo z lze psát ve tvaru

$$z = r \cdot (\cos\alpha + i \sin\alpha)$$

pro vhodná $r \in \mathbb{R}$, $r > 0$, $\alpha \in \mathbb{R}$, přičemž $r = |z|$ je dáno jednoznačně a α je dáno jednoznačně až na přičtení celočíselného násobku 2π. Pak pro libovolné celé číslo n platí

$$z^n = r^n \cdot (\cos n\alpha + i \sin n\alpha).$$

Řešení – str. 18.

3. kolo – Grupy s exponentem 2

Doporučené znalosti: exponent konečné grupy a homomorfismus grup – po str. 36 v přednášce.

Zadání:

a) (1 bod) Nechť $\varphi : G \to H$ je surjektivní homomorfismus konečných grup. Dokažte, že pokud má grupa G exponent 2, potom je exponent grupy H roven 1 nebo 2.

b) (1 bod) Dokažte, že každá konečná grupa s exponentem 2 je komutativní.

c) (4 body) Nechť m a n jsou přirozená čísla. Uvažujme předpis

$$\varphi : \mathbb{Z}_m^\times \to \mathbb{Z}_n^\times,\ \varphi([a]_m) = [a]_n,\ \text{kde } a \in \mathbb{Z}.$$

Dokažte, že tento předpis definuje korektně zobrazení $\varphi : \mathbb{Z}_m^\times \to \mathbb{Z}_n^\times$ právě tehdy, když $n \mid m$. Dále dokažte, že za tohoto předpokladu je φ surjektivní homomorfismus grupy $(\mathbb{Z}_m^\times, \cdot)$ do grupy $(\mathbb{Z}_n^\times, \cdot)$.

d) (2 body) Určete, pro které mocniny prvočísel $n = p^k$, kde p je prvočíslo a k je číslo přirozené, má grupa $(\mathbb{Z}_n^\times, \cdot)$ exponent 2.

e) (2 body) Určete všechna přirozená čísla n taková, že grupa $(\mathbb{Z}_n^\times, \cdot)$ má exponent 2.

Komentář: Pro zisk kladného počtu bodů není nezbytně nutné odevzdávat kompletní řešení jednotlivých úloh. Například v části c) je třeba dokázat více faktů a za každý z nich lze získat nějaké body. Zde důkaz nejobtížnější části, tj. surjektivity zobrazení φ, je možné provést například vhodným využitím tzv. *čínské zbytkové věty.* Tato věta říká, že pro libovolná *nesoudělná* přirozená čísla k a ℓ a libovolná celá čísla a, b existuje celé číslo c takové, že $[c]_k = [a]_k$ a $[c]_\ell = [b]_\ell$. Navíc je toto c určeno jednoznačně modulo $k\ell$. (Jinými slovy $[a]_k \cap [b]_\ell = [c]_{k\ell}$.) Její důkaz plyne okamžitě z důkazu věty na straně 21 slajdů z přednášky, neboť jediné tvrzení, které potřebujeme, je fakt, že tam definované zobrazení f je bijektivní. Proto čínskou zbytkovou větu již nemusíte dokazovat, ale můžete ji použít při důkaze v části c) – i se znalostí této nápovědy není úplně jednoduché surjektivitu zobrazení φ uvidět.

Podobně se nebojte v řešení jedné části zadání použít tvrzení z jiné části, přestože jste potřebné tvrzení sami nedokázali.

Řešení – str. 20.

4. kolo – Maximální podgrupy v permutačních grupách

Doporučené znalosti: podgrupy a Lagrangeova věta – po str. 40 v přednášce.

Zadání: Řekneme, že podgrupa H grupy G je *maximální*, pokud $H \neq G$ a zároveň neexistuje podgrupa M grupy G s vlastnostmi $H \subseteq M$ a $H \neq M \neq G$.

a) (2 body) Nechť $f\colon G_1 \to G_2$ je surjektivní homomorfismus grup a $H \leq G_1$ je maximální podgrupa grupy G_1 taková, že $\ker f \subseteq H$. Dokažte, že potom $f(H)$ je maximální podgrupa grupy G_2.

b) (2 body) Nechť $f\colon G_1 \to G_2$ je surjektivní homomorfismus grup a $K \leq G_2$ je maximální podgrupa grupy G_2. Dokažte, že potom $f^{-1}(K)$ je maximální podgrupa grupy G_1.

c) (1 bod) Pro libovolné $n \in \mathbb{N}$, $n \geq 2$ ukažte, že libovolná podgrupa grupy $\mathbb{S}_n$, která obsahuje některou lichou permutaci, má sudý počet prvků.

d) (1 bod) Pro libovolné $n \in \mathbb{N}$, $n \geq 4$ dokažte, že každá maximální podgrupa $\mathbb{S}_n$ má sudý počet prvků.

e) (4 body) Nechť $n \in \mathbb{N}$, $n \geq 2$. Hráči A a B hrají následující hru: hráči střídavě vybírají prvky grupy $\mathbb{S}_n$ (v každém tahu vždy jeden prvek), přičemž nelze vybrat prvek, který už byl vybrán dříve (tzn. jde o výběr bez vracení). Jako první vybírá hráč A. Hra končí v momentě, kdy množina všech vybraných prvků generuje celou grupu $\mathbb{S}_n$. Hráč, který vybíral naposledy, prohrává, ten druhý vyhrává.

   a) Dokažte, že pro $n = 2$ a $n = 3$ má hráč A vítěznou strategii.

   b) Dokažte, že pro $n \geq 4$ má hráč B vítěznou strategii.

Komentář: Nemusíte odevzdávat kompletní řešení jednotlivých úloh – například v části e) se bude hodnotit i dokázání jednotlivých případů. Lze také řešit pouze jednotlivé úlohy – můžete například řešit pouze části a) nebo b), jež nijak nesouvisí se zbývajícími částmi.

Pojem maximální podgrupa je samozřejmě motivován terminologií z uspořádaných množin. Uspořádanou množinou, která se zde uvažuje, je množina všech podgrup grupy G. Zde je evidentně největším, a tudíž jediným maximálním prvkem sama grupa G. Toto triviální pozorování vede k otázce, co se stane, když tento prvek z uspořádané množiny odstraníme. Proto se uvažují pouze tzv. *vlastní* podgrupy grupy G (tedy podgrupy grupy G různé od G) a mezi nimi nás pak zajímají maximální prvky v uspořádnání inkluzí. Proto bychom správně měli definovat pojem *maximální vlastní podgrupa*, nicméně slůvko vlastní se v této definici vypouští, neboť termín pouze zbytečně prodlužuje. Poznamenejme ještě, že pro některé (nekonečné) grupy maximální podgrupy neexistují. V našem případě, vzhledem ke konečnosti uvažovaných grup, můžeme dokonce tvrdit, že pro libovolnou vlastní podgrupu grupy $\mathbb{S}_n$ existuje maximální podgrupa, která ji obsahuje.

Předchozí odstavec tedy můžeme shrnout: maximální podgrupy jsou právě ty, které jsou v uspořádané množině všech podgrup těsně pod největší podgrupou G.

Řešení – str. 21.

5. kolo – Podgrupy

Doporučené znalosti: rozklady grup a normální podgrupy – po str. 43 v přednášce.

Zadání:

a) (2 body) Nechť $(G, \cdot)$ je libovolná grupa a X, Y jsou libovolné podmnožiny nosné množiny G grupy $(G, \cdot)$. Zjistěte, které inkluze

   (i) mezi podmnožinami $\langle X \rangle \cap \langle Y \rangle$ a $\langle X \cap Y \rangle$ množiny G

   (ii) mezi podmnožinami $\big\langle \langle X \rangle \cup \langle Y \rangle \big\rangle$ a $\langle X \cup Y \rangle$ množiny G

   jsou obecně platné, tj. platí pro každé podmnožiny X, Y v každé grupě $(G, \cdot)$.

b) (2 body) Nechť G je libovolná grupa a H je její podgrupa taková, že index podgrupy H v grupě G je roven dvěma. Dokažte, že H je normální podgrupa grupy G.

c) (3 body) Nechť G je libovolná grupa a H je její normální podgrupa, která je cyklická. Dokažte, že libovolná podgrupa K podgrupy H je normální podgrupa grupy G.

d) (3 body) Nechť $\mathcal{R}$ je libovolný rozklad nosné množiny grupy $(G, \cdot)$ takový, že pro každý prvek $g \in G$ a každou třídu rozkladu $A \in \mathcal{R}$ platí $\{g \cdot a;\, a \in A\} \in \mathcal{R}$. Dokažte, že rozklad $\mathcal{R}$ je rozkladem grupy G podle vhodné podgrupy H.

Komentář: Úloha a) se týká čtyř možných inkluzí, z nichž každou máte buď obecně dokázat anebo naopak vyvrátit nějakým konkrétním příkladem. Uvědomte si, že jsme dokazovali, že průnik podgrup grupy G je podgrupa grupy G, a že tedy všechny čtyři zmiňované podmnožiny jsou podgrupy. Také se Vám může hodit následující postřeh plynoucí ihned z definice podgrupy $\langle M \rangle$ grupy G generované množinou M: pro každou podgrupu H grupy G jsou výroky $M \subseteq H$ a $\langle M \rangle \subseteq H$ ekvivalentní (promyslete si proč).

Řešení – str. 22.

6. kolo – Polopřímý součin grup

Doporučené znalosti: věty o faktorových grupách a Burnsidovo lemma – po str. 55 v přednášce.

Zadání:

a) (7 bodů) Připomeňme, že $\mathrm{Aut}(H)$ značí grupu automorfismů grupy H.

(i) Nechť $(H,\cdot)$ a $(K,\cdot)$ jsou grupy, $\varphi : K \to \mathrm{Aut}(H)$ homomorfismus grup. Na množině $G = H \times K$ definujeme operaci $\cdot$ takto: pro libovolné $h_1, h_2 \in H$ a libovolné $k_1, k_2 \in K$ klademe

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot (\varphi(k_1)(h_2)), k_1 \cdot k_2).$$

Dokažte, že $(G,\cdot)$ je grupa. Dále dokažte, že její podmnožiny $\{(h,1)\colon h \in H\}$ resp. $\{(1,k)\colon k \in K\}$ tvoří podgrupy grupy G izomorfní s H resp. K, a navíc ta první z nich je normální podgrupa grupy G.

Grupu $(G,\cdot)$ definovanou v části (i) nazýváme *polopřímý součin grup* $(H,\cdot)$ a $(K,\cdot)$ vzhledem k akci φ a značíme ji $H \rtimes_\varphi K$.

(ii) Nechť $n \in \mathbb{N}$, $n \geq 3$. Dokažte, že dihedrální grupa $\mathbb{D}_n$ je izomorfní grupě $\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$, kde $\varphi\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ je dáno vztahem $\varphi([b]_2)([a]_n) = [(-1)^b a]_n$ pro všechna $a, b \in \mathbb{Z}$.

(iii) Uvažujme polopřímý součin grup $\mathbb{Z} \rtimes_\varphi \mathbb{Z}_2$, kde akce $\varphi\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$ je určena vztahem $\varphi([b]_2)(a) = (-1)^b a$ pro všechna $a, b \in \mathbb{Z}$ a zobrazení $f\colon \mathbb{Z} \times \mathbb{Z}_2 \to \mathbb{Z}$ dané předpisem $f((a,[b]_2)) = 2a + \frac{1-(-1)^b}{2}$ pro všechna $a, b \in \mathbb{Z}$. Dokažte, že f je izomorfismus grupy $\mathbb{Z} \rtimes_\varphi \mathbb{Z}_2$ a grupy $(\mathbb{Z}, \circ)$, v níž pro libovolné $x, y \in \mathbb{Z}$ je definováno $x \circ y = x + (-1)^x y$.

b) (3 body) Nechť konečná grupa G má tranzitivní akci (definice viz níže) na konečné množině X, kde $|X| \geq 2$, je tedy dán homomorfismus $\varphi : G \to \mathbb{S}(X)$. Dokažte, že potom existuje $g \in G$ takové, že pro všechna $x \in X$ platí $\varphi(g)(x) \neq x$ (tj. permutace $\varphi(g)$ množiny X indukovaná prvkem g nemá žádný pevný bod).

Komentář: Je-li H grupa, pak grupa automorfismů grupy H je podgrupou grupy permutací $\mathbb{S}(H)$ množiny H, protože každý automorfismus $H \to H$ je bijekce, tedy permutace množiny H, a v obou grupách $\mathrm{Aut}(H)$ a $\mathbb{S}(H)$ je operací skládání zobrazení. Proto homomorfismus $\varphi : K \to \mathrm{Aut}(H)$ zadává akci grupy K na množině H, v níž je dokonce každá užitá permutace automorfismem.

Polopřímý součin, který jsme definovali v úloze a)-(i), zobecňuje součin grup, který jsme definovali na přednášce a kterému se (pro odlišení od polopřímého součinu) říká také přímý součin: promyslete si, že jej dostaneme, pokud homomorfismus φ je definován tak, že $\varphi(k)$ je identita na H pro každé $k \in K$.

V úloze a)-(iii) považujte skutečnost, že $(\mathbb{Z}, \circ)$ je grupa, za dokázanou – viz. příklad 2.1.3 ze sbírky ke cvičení.

Vysvětleme ještě použitý pojem tranzitivní akce: o akci grupy G na množině X řekneme, že je tranzitivní, pokud pro libovolné $x, y \in X$ existuje $g \in G$ tak, že $\varphi(g)(x) = y$, což lze ekvivalentně vyjádřit tím, že orbita libovolného prvku $x \in X$ je rovna celé množině X.

Řešení – str. 23.

7. kolo – Permutační grupy a vnitřní automorfismy grup

Doporučené znalosti: vnitřní automofismy grup – po str. 57 v přednášce.

Zadání:

a) (6 bodů)

(i) Nechť G je konečná grupa řádu n a $a \in G$ je prvek řádu k. Uvažme homomorfismus $r\colon G \to \mathbb{S}(G)$ z Cayleyho věty (definici připomínáme v komentáři dole). Určete (v závislosti na n a k) délky cyklů v rozkladu permutace r_a na nezávislé cykly a určete také paritu této permutace.

(ii) Nechť G je konečná grupa řádu $2m$, kde m je liché. Dokažte, že existuje podgrupa grupy G indexu 2.

b) (4 body)

(i) Nechť G je grupa. Dokažte, že množina $\mathrm{Inn}(G)$ vnitřních automorfismů grupy G je normální podgrupa grupy $(\mathrm{Aut}(G), \circ)$ automorfismů grupy G.

(ii) Dokažte, že $\mathrm{Aut}(\mathbb{S}_3) = \mathrm{Inn}(\mathbb{S}_3)$.

Komentář: Připomeňme, že homomorfismus $r\colon G \to \mathbb{S}(G)$ z Cayleyho věty byl definován takto: pro každé $x \in G$ je $r(x) = r_x$, kde bijekce $r_x : G \to G$ je definována předpisem $r_x(g) = x \cdot g$ pro libovolné $g \in G$.

Připomeňme také, že pro libovolnou grupu $(G, \cdot)$ platí, že množina $\mathrm{Aut}(G)$ všech automorfismů grupy G (tj. izomorfismů $G \to G$) vzhledem k operaci skládání zobrazení tvoří grupu: vždyť z toho, že identita na G je automorfismus, že složení dvou izomorfismů je izomorfismus a že inverzní zobrazení k izomorfismu je izomorfismus, plyne, že $\mathrm{Aut}(G)$ je podgrupou grupy $(\mathbb{S}(G), \circ)$.

Symbolem $\mathrm{Inn}(G)$ rozumíme množinu všech vnitřních automorfismů grupy G, tedy $\mathrm{Inn}(G) = \{\rho_a;\ a \in G\}$, kde pro libovolný prvek $a \in G$ je vnitřní automorfismus $\rho_a : G \to G$ definován předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro libovolné $g \in G$.

Z tvrzení uvedeného v úloze b)(i) vyplývá, že pro každou grupu G existuje faktorgrupa $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. Tato grupa se nazývá *grupa vnějších automorfismů grupy* G a značí se $\mathrm{Out}(G)$ (nicméně její prvky nejsou automorfismy G, ale množiny těchto automorfismů, které jsou třídy rozkladu grupy $\mathrm{Aut}(G)$ podle podgrupy $\mathrm{Inn}(G)$). Tvrzení v úloze b)(ii) je tedy ekvivalentní tomu, že grupa $\mathrm{Out}(\mathbb{S}_3)$ vnějších automorfismů grupy $(\mathbb{S}_3, \circ)$ má jediný prvek, t.j. je triviální.

Řešení – str. 25.

8. kolo – Normalizér a centralizér množiny v grupě a automorfismy součinu grup

Doporučené znalosti: centrum grupy – po str. 57 v přednášce.

Zadání: Definice centralizéru a normalizéru jsou uvedeny v komentáři. Připomeňme, že $\mathrm{Aut}(K)$ značí grupu automorfismů grupy K.

a) (4 body) Nechť G a H jsou grupy.

   (i) Dokažte, že grupa $\mathrm{Aut}(G \times H)$ obsahuje podgrupu, která je izomorfní grupě $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

   (ii) Ukažte na příkladu, že grupa $\mathrm{Aut}(G \times H)$ nemusí být grupě $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ izomorfní.

   (iii) Jestliže navíc G a H jsou konečné a $(|G|, |H|) = 1$, dokažte, že $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

b) (3 body) Nechť G je grupa a $H \leq G$ je její podgrupa.

   (i) Dokažte, že $H \subseteq N_G(H)$.

   (ii) Dokažte, že H je normální podgrupa grupy G, právě když $N_G(H) = G$.

   (iii) Na vhodném příkladu ukažte, že je-li A pouze podmnožinou G, pak $A \subseteq N_G(A)$ platit nemusí.

c) (3 body) Nechť G je grupa a $H \leq G$ je její podgrupa. Dokažte, že centralizér $C_G(H)$ je normální podgrupa normalizéru $N_G(H)$ a že faktorgrupa $N_G(H)/C_G(H)$ je izomorfní vhodné podgrupě grupy $\mathrm{Aut}(H)$.

Komentář: Nechť $(G, \cdot)$ je grupa, $A \subseteq G$ podmnožina množiny G. Centralizérem množiny A v grupě G rozumíme množinu

$$C_G(A) = \{g \in G;\ \forall a \in A :\ g \cdot a \cdot g^{-1} = a\}.$$

Pro libovolné $g \in G$ definujeme $g \cdot A \cdot g^{-1} = \{g \cdot a \cdot g^{-1};\ a \in A\}$. Normalizérem množiny A v grupě G rozumíme množinu

$$N_G(A) = \{g \in G;\ g \cdot A \cdot g^{-1} = A\}.$$

Uvědomte si, že ihned z definice plyne:

- $C_G(A) \subseteq N_G(A)$;
- $C_G(A)$ i $N_G(A)$ jsou podgrupy grupy G;
- pro centrum $Z(G)$ grupy G platí $Z(G) = C_G(G)$;
- je-li G komutativní, pak $C_G(A) = N_G(A) = G$.

Řešení – str. 27.

9. kolo – Jednoduchost alternujících grup

Doporučené znalosti: vnitřní automofismy – po str. 56 v přednášce.

Zadání:

a) (3 body)

(i) Dokažte, že pro každé $n \in \mathbb{N}$ množina všech cyklů v $\mathbb{A}_n$ délky 3 generuje celou grupu $\mathbb{A}_n$.

(ii) Popište třídy konjugace grupy $\mathbb{A}_5$ (definice viz níže).

b) (7 bodů) Cílem tohoto příkladu je dokázat, že pro každé $n \geq 5$ je grupa $\mathbb{A}_n$ jednoduchá (definice viz níže). Budeme postupovat indukcí vzhledem k n.

(i) Dokažte, že $\mathbb{A}_5$ je jednoduchá grupa.

Nyní předpokládejme, že $n \geq 6$ a že grupa $\mathbb{A}_{n-1}$ je jednoduchá. Pro každé $i \in \{1, \ldots, n\}$ označme $H_i = \{\sigma \in \mathbb{A}_n \colon \sigma(i) = i\}$. Nechť dále H je libovolná netriviální normální podgrupa grupy $\mathbb{A}_n$. Potřebujeme ukázat, že $H = \mathbb{A}_n$.

(ii) Dokažte, že pro každé $i \in \{1, \ldots, n\}$ je H_i podgrupa grupy $\mathbb{A}_n$ izomorfní grupě $\mathbb{A}_{n-1}$. Dále dokažte, že $H \cap H_i$ je normální podgrupa grupy H_i.

(iii) Dokažte, že existuje $i \in \{1, \ldots, n\}$ takové, že $H \cap H_i \neq \{\mathrm{id}\}$.
[Návod: Vezměte si libovolné $\sigma \in H$, $\sigma \neq \mathrm{id}$. Ukažte, že existuje $\sigma' \in H$ takové, že $\sigma \neq \sigma'$ a $\sigma(i) = \sigma'(i)$ pro nějaké i (můžete rozlišit případy, kdy σ obsahuje cyklus délky aspoň 3 a kdy nikoliv).]

(iv) Dokažte, že $H = \mathbb{A}_n$.

Komentář: Prvky g, h grupy $(G, \cdot)$ se nazývají *konjugované*, jestliže existuje prvek $a \in G$ tak, že $g = a \cdot h \cdot a^{-1}$. Snadno se vidí, že relace „být konjugované“ je relací ekvivalence na množině G; třídy rozkladu podle této ekvivalence se nazývají *třídy konjugace* grupy G.

Třídy konjugace grupy G můžeme popsat také jinak. Nechť $\rho : G \to \mathbb{S}(G)$ je akce grupy G na sobě vnitřními automorfismy, tedy pro libovolný prvek $a \in G$ je $\rho(a) = \rho_a$, kde $\rho_a : G \to G$ je vnitřní automorfismus grupy G definovaný předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro libovolné $g \in G$. Pak pro libovolné prvky g, h grupy G platí, že jsou konjugované, právě když patří v akci ρ do stejné orbity; třídy konjugace grupy G jsou tedy právě orbity v této akci.

Dále si ukážeme, jak funguje konjugace v grupě $\mathbb{S}_n$. Nechť $\sigma \in \mathbb{S}_n$ je permutace, jejíž rozklad na nezávislé cykly je

$$(a_{1,1}, \ldots, a_{1,\ell_1}) \circ (a_{2,1}, \ldots, a_{2,\ell_2}) \circ \ldots \circ (a_{k,1}, \ldots, a_{k,\ell_k}).$$

Zvolme libovolné $\tau \in \mathbb{S}_n$. Pro každé $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots \ell_i\}$ platí $\sigma(a_{i,j}) = a_{i,j+1}$ (přičemž druhý index chápeme cyklicky modulo ℓ_i, tedy $a_{i,\ell_i+1} = a_{i,1}$), z čehož vyplývá $(\tau \circ \sigma \circ \tau^{-1})(\tau(a_{i,j})) = \tau(\sigma(\tau^{-1}(\tau(a_{i,j})))) = \tau(\sigma(a_{i,j})) = \tau(a_{i,j+1})$. Odtud je snadno vidět, že rozklad permutace $\tau \circ \sigma \circ \tau^{-1}$ na nezávislé cykly je

$$(\tau(a_{1,1}), \ldots, \tau(a_{1,\ell_1})) \circ (\tau(a_{2,1}), \ldots, \tau(a_{2,\ell_2})) \circ \ldots \circ (\tau(a_{k,1}), \ldots, \tau(a_{k,\ell_k})).$$

Zejména tedy platí, že konjugované permutace v $\mathbb{S}_n$ mají stejné délky cyklů v rozkladu na nezávislé cykly (permutace, jež mají stejné délky cyklů v rozkladu na nezávislé cykly, se někdy stručně nazývají *permutace stejného typu*). Naopak nechť $\sigma' \in \mathbb{S}_n$ má stejné délky cyklů v rozkladu na nezávislé cykly jako σ. Z předchozího výpočtu je potom snadno vidět, že existuje (pro $n > 1$ ne jediné) $\tau \in \mathbb{S}_n$ takové, že platí $\sigma' = \tau \circ \sigma \circ \tau^{-1}$. Celkem jsme tedy dokázali, že permutace v $\mathbb{S}_n$ jsou konjugované právě tehdy, když jsou stejného typu.

Zkoumejme nyní stejnou otázku v grupě $\mathbb{A}_n$. Stejným výpočtem jako výše se ukáže, že konjugované permutace v $\mathbb{A}_n$ jsou stejného typu. Opačná implikace ovšem obecně neplatí (důvod je ten, že žádné příslušné τ nemusí být sudé). Například permutace $(1, 2, 3)$ a $(1, 3, 2)$ jsou stejného typu, ale nejsou v grupě $\mathbb{A}_3$ konjugované, neboť $\mathbb{A}_3$ je komutativní grupa, tedy každý její prvek je konjugovaný pouze sám se sebou.

Grupa se nazývá *jednoduchá*, pokud je netriviální a nemá žádnou vlastní netriviální normální podgrupu. Jednoduché grupy hrají důležitou roli v teorii grup, významným hlubokým výsledkem je klasifikace konečných jednoduchých grup, jejíž kompletní důkaz má několik tisíc stran a samotná formulace tvrzení této klasifikace je velmi netriviální.

Snadno se ale odvodí, jak vypadají všechny komutativní jednoduché grupy. Zřejmě pro každé prvočíslo p je grupa $\mathbb{Z}_p$ jednoduchá, neboť dokonce nemá žádné vlastní netriviální podgrupy. Naopak zřejmě pro každou komutativní jednoduchou grupu platí, že nemůže mít žádnou vlastní netriviální podgrupu (neboť v komutativní grupě je každá podgrupa normální), proto každý nenulový prvek takové grupy musí generovat celou tuto grupu. Tudíž jde o cyklickou grupu. Každá cyklická grupa je izomorfní buď $\mathbb{Z}$ nebo $\mathbb{Z}_n$ pro nějaké $n \in \mathbb{N}$; snadno se uvidí, že $\mathbb{Z}$ není jednoduchá a $\mathbb{Z}_n$ je jednoduchá právě pro prvočíselné n.

Řešení – str. 28.

10. kolo – Nástin pojmu prezentace grup

Doporučené znalosti: předchozí kola soutěže.

Zadání:

a) (7 bodů) Nechť jsou dány konstanty $k, \ell, r \in \mathbb{N}$. Řekneme, že grupa $(G, \cdot)$ *splňuje prezentaci*

$$\langle x, y \mid x^k = 1, y^\ell = 1, xy = y^r x \rangle\,, \qquad (*)$$

jestliže existují v grupě G prvky a, b takové, že grupa G je jimi generována a platí $a^k = 1, b^\ell = 1, a \cdot b = b^r \cdot a$.

i) Dokažte, že každá grupa G splňující prezentaci $(*)$ je konečná a platí pro ni $|G| \leq k \cdot \ell$.

ii) Dokažte, že pokud existuje grupa G velikosti $k \cdot \ell$ splňující prezentaci $(*)$, potom platí $r^k \equiv 1 (\mathrm{mod}\ \ell)$.

iii) Dokažte, že pokud platí $r^k \equiv 1 (\mathrm{mod}\ \ell)$, pak existuje grupa G velikosti $k \cdot \ell$, která splňuje prezentaci $(*)$.

iv) Ukažte, že pro libovolné dvě grupy G a H splňující prezentaci $(*)$ existuje grupa K splňující prezentaci $(*)$ a surjektivní homomorfismy grup $\alpha : K \to G$ a $\beta : K \to H$.

v) Ukažte, že existuje grupa K splňující prezentaci $(*)$ taková, že pro libovolnou grupu G splňující prezentaci $(*)$ existuje surjektivní homomorfismus grup $\alpha : K \to G$.

b) (3 body) Nechť je pevně zvoleno číslo $m \in \mathbb{N}$. Řekneme, že grupa $(G, \cdot)$ *splňuje prezentaci*

$$\langle x, y \mid x^2 = 1, y^2 = 1, (xy)^m = 1 \rangle\,, \qquad (**)$$

jestliže existují v grupě G prvky a, b takové, že grupa G je jimi generována a platí $a^2 = 1, b^2 = 1, (a \cdot b)^m = 1$.

i) Dokažte, že každá grupa G splňující prezentaci $(**)$ je konečná a platí pro ni $|G| \leq 2m$.

ii) Dokažte, že existuje grupa G velikosti $2m$ splňující prezentaci $(**)$.

Komentář: Při řešení části a)-iii) může být užitečné si všimnout, že z předpokladu $r^k \equiv 1 (\mathrm{mod}\ \ell)$ plyne nesoudělnost čísel r a ℓ.

V částech a)-iii) a b)-ii) samozřejmě dokazujte existenci příslušné grupy tak, že dáte příklad všeobecně známé grupy, která má požadované vlastnosti. Za všeobecně známé mějte grupy, s kterými jste se seznámili ve výuce nebo v naší soutěži.

Poznamenejme, že grupa K, jejíž existenci máte za úkol dokázat v části a)-v), je dána jednoznačně až na izomorfismus. Skutečně, pokud K_1 a K_2 jsou grupy splňující podmínku z a)-v), pak máme k dispozici dva surjektivní homomorfismy $\alpha : K_1 \to K_2$ a $\beta : K_2 \to K_1$, jejichž existence implikuje $|K_1| = |K_2|$ a jedná se tedy o izomorfismy grup. Podobně by se stejné tvrzení dokázalo i v případě prezentace $(**)$. Říkáme potom, že grupa K má prezentaci $(*)$ resp. $(**)$. V obou případech ovšem argumentace dokazující existenci a jednoznačnost grupy K vhodně využívá konečnosti uvažovaných grup a obecně se pojem *prezentace grup* musí zavést jiným způsobem. Stejně jako v zadání se prezentací grupy rozumí seznam generátorů grupy a seznam relací, které mají být v grupě splněny. (Relace vyjadřuje, že prvek, zapsaný pomocí generátorů v jistém tvaru,

lze zapsat pomocí generátorů i dalším způsobem.) Grupa K s touto prezentací se konstruuje za pomocí abstraktní grupy sestávající ze všech možných výrazů vytvořených z generátorů, která se vhodně faktorizuje. Takto zkonstruovaná grupa K má potom vlastnosti popsané v bodě a)-v), tj. libovolná grupa G, která splňuje stejnou prezentaci, je homomorfním obrazem K. Nicméně v této obecné podobě se s prezentacemi grup seznámíme až v kurzu Algebra II.

Řešení – str. 32.

Část II – Řešení

1. kolo — řešení

Za účelem zjednodušení formulací v následujícím řešení budeme pevné body permutace považovat za cykly délky jedna, čemuž jsme se v zadání vyhnuli (viz komentář k zadání). Při tomto pojetí lze také modifikovat definici rozkladu na nezávislé cykly, tak, že cykly délky jedna jsou jeho součástí. Věta o jednoznačnosti rozkladu (věta 2.5 ve skriptech, resp. str. 7 na slajdech) pak zůstává v platnosti a navíc je ji možné rozšířit i na případ identické permutace. Přesněji, rozklad na nezávislé cykly identické permutace id je součin n cyklů délky jedna. Zejména charakteristiky definované v zadání nabývají hodnot: $\mathsf{r}_1(\mathsf{id}) = n$, $\mathsf{r}_k(\mathsf{id}) = 0$ pro všechna $k > 1$ a následně $\mathsf{r}(\mathsf{id}) = n$.

a) Buď $\sigma \in \mathbb{S}_n$. Číslo n na pravé straně dokazované rovnosti značí počet prvků množiny $X_n = \{1, \ldots, n\}$, kterou permutujeme. Pro zadanou permutaci $\sigma : X_n \to X_n$ je každý prvek množiny X_n prvkem právě jednoho cyklu v rozkladu na součin nezávislých cyklů. Pro každé k, včetně případu $k = 1$, je součin $k \cdot \mathsf{r}_k(\sigma)$ roven počtu prvků množiny X_n, které jsou součástí některého cyklu délky k, neboť k jako délka cyklu je počet prvků vyskytujících se v daném cyklu, a $\mathsf{r}_k(\sigma)$ je počet cyklů délky k. Levá strana rovnosti je proto počet prvků množiny X_n, které jsou součásti některého cyklu v rozkladu na součin nezávislých cyklů. Tento počet je ovšem n, neboť již víme, že každý prvek množiny X_n je prvkem právě jednoho cyklu.

b) Podle druhého důsledku na straně 9 slajdů z přednášky je parita permutace σ rovna $(-1)^{\mathsf{s}(\sigma)}$, kde $\mathsf{s}(\sigma)$ je počet cyklů sudé délky v rozkladu permutace σ na součin nezávislých cyklů. Tedy dle námi zavedeného značení máme $\mathsf{s}(\sigma) = \sum_{\ell=1}^{n} \mathsf{r}_{2\ell}(\sigma)$. Všimněme si, že pokud $2\ell > n$, pak dle definice platí $\mathsf{r}_{2\ell}(\sigma) = 0$. Pokusme se tedy výraz v zadání $(-1)^{n-\mathsf{r}(\sigma)}$ upravit do tvaru $(-1)^{\mathsf{s}(\sigma)}$. Nejdříve upravíme exponent $n-\mathsf{r}(\sigma)$, kde n nahradíme vztahem z části a) a $\mathsf{r}(\sigma)$ nahradíme definicí $\mathsf{r}(\sigma) = \sum_{k=1}^{n} \mathsf{r}_k(\sigma)$. Dostaneme tak $n - \mathsf{r}(\sigma) = \sum_{k=1}^{n} (k-1) \cdot \mathsf{r}_k(\sigma)$ a tedy

$$(-1)^{n-\mathsf{r}(\sigma)} = \prod_{k=1}^{n} (-1)^{(k-1)\cdot \mathsf{r}_k(\sigma)} \ . \qquad (*)$$

Protože pro lichá k jsou čísla $k-1$ sudá, dostáváme $(-1)^{(k-1)\cdot \mathsf{r}_k(\sigma)} = 1$. Můžeme tedy v součinu $(*)$ násobit jen přes sudé indexy k. Navíc pro tato sudá k je $k-1$ liché číslo a tedy parita $(k-1)\cdot \mathsf{r}_k(\sigma)$ je stejná jako parita $\mathsf{r}_k(\sigma)$. Tudíž pro sudá k můžeme v součinu $(*)$ činitel $(-1)^{(k-1)\cdot \mathsf{r}_k(\sigma)}$ nahradit výrazem $(-1)^{\mathsf{r}_k(\sigma)}$. Celkem tedy

$$(-1)^{n-\mathsf{r}(\sigma)} = \prod_{k=1}^{n} (-1)^{(k-1)\cdot \mathsf{r}_k(\sigma)} = \prod_{\ell=1}^{n} (-1)^{\mathsf{r}_{2\ell}(\sigma)} = (-1)^{\sum_{\ell=1}^{n} \mathsf{r}_{2\ell}(\sigma)} = (-1)^{\mathsf{s}(\sigma)} = \mathsf{p}(\sigma) \ .$$

Alternativní řešení: Permutace σ se napíše jako součin nezávislých cyklů $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{\mathsf{r}(\sigma)}$ a parita σ se určí jako součin parit jednotlivých permutací σ_i, které jsou $\mathsf{p}(\sigma_i) = (-1)^{k_i - 1}$, kde k_i je délka cyklu σ_i. Potom

$$\mathsf{p}(\sigma) = (-1)^{\sum_{i=1}^{\mathsf{r}(\sigma)} (k_i - 1)} = (-1)^{n - \mathsf{r}(\sigma)} \ ,$$

neboť dle části a) víme, že $\sum_{i=1}^{\mathsf{r}(\sigma)} k_i = n$.

c) Hledaná ekvivalence pro zadanou permutaci σ je tato:

$$\exists \tau \in \mathbb{S}_n \ : \ \sigma = \tau^2 \quad \Longleftrightarrow \quad \forall \ell \in \mathbb{N} \ : \ 2 \mid \mathsf{r}_{2\ell}(\sigma) \ .$$

"$\Longrightarrow$" : Nechť tedy $\sigma = \tau^2$. Pokud použijeme rozklad permutace τ na nezávislé cykly, tj. $\tau = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_j$, tak z nezávislosti jednotlivých cyklů plyne, že $\sigma = \tau^2 = \tau_1^2 \circ \tau_2^2 \circ \cdots \circ \tau_j^2$. Pokud je τ_i cyklus liché délky, pak τ_i^2 je cyklus stejné liché délky. Pokud je τ_i cyklus sudé délky, pak τ_i^2

má rozklad na nezávislé cykly ve tvaru součinu dvou cyklů téže sudé délky, která je polovinou délky cyklu τ_i. Nás zajímají cykly sudé délky v rozkladu permutace σ na nezávislé cykly. Pro libovolné ℓ je tedy $\mathsf{r}_{2\ell}(\sigma)$ rovno dvojnásobku počtu cyklů délky 4ℓ v rozkladu permutace τ, tj. $\mathsf{r}_{2\ell}(\sigma) = 2 \cdot \mathsf{r}_{4\ell}(\tau)$, tudíž $2 \mid \mathsf{r}_{2\ell}(\sigma)$.

"$\Longleftarrow$" Nejdříve vyřešíme případ, kdy σ je součinem dvou nezávislých cyklů stejné sudé délky. Tedy buď $\sigma = (x_1, x_2, \ldots, x_{2\ell})(y_1, y_2, \ldots, y_{2\ell})$. Pokud vytvoříme cyklus τ délky 4ℓ, kde se pravidelně a přitom postupně střídají čísla z dané dvojice cyklů, tj. cyklus $\tau = (x_1, y_1, x_2, y_2, \ldots, x_{2\ell}, y_{2\ell})$, pak platí $\tau^2 = \sigma$. Této konstrukce později ještě využijeme.

Nechť je nyní dána permutace σ splňující předpoklad $\forall \ell \in \mathbb{N} : 2 \mid \mathsf{r}_{2\ell}(\sigma)$. Můžeme přepokládat, že σ není identická permutace, pro niž je hledaná permutace τ ona sama. Uvažujme rozklad σ na nezávislé cykly

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_m \circ \rho_1 \circ \rho'_1 \circ \rho_2 \circ \rho'_2 \circ \cdots \circ \rho_r \circ \rho'_r \ ,$$

kde pro $i = 1, \ldots, m$ je σ_i cyklus liché délky p_i, a pro $j = 1, \ldots, r$ jsou oba cykly ρ_j i ρ'_j cyklem stejné sudé délky q_j. Označíme-li pro $i = 1, \ldots, m$ permutaci $\tau_i = \sigma_i^{\frac{p_i+1}{2}}$, pak platí $\tau_i^2 = \sigma_i^{p_i+1} = \sigma_i$. Pro libovolné $j = 1, \ldots, r$, dle úvodní poznámky v důkazu, existuje cyklus δ_j délky $2q_j$ s vlastností $\delta_j^2 = \rho_j \circ \rho'_j$. Uvažme nyní permutaci

$$\tau = \tau_1 \circ \cdots \circ \tau_m \circ \delta_1 \circ \cdots \circ \delta_r \ .$$

Protože cykly v rozkladu σ jsou nezávislé, tak také cykly v předchozím součinu jsou nezávislé a jedná se tedy o rozklad permutace τ na nezávislé cykly. Z toho důvodu

$$\tau^2 = \tau_1^2 \circ \cdots \circ \tau_m^2 \circ \delta_1^2 \circ \cdots \circ \delta_r^2 = \sigma \ .$$

d) Protože pro libovolnou permutaci τ je permutace τ^2 sudá, je zřejmě každá permutace tvaru $\tau^2 \circ \sigma^2$ sudou permutací. Tím dostáváme hypotézu, že taková dvojice permutací τ, σ existuje právě pro sudou permutaci σ. Přitom je třeba dokázat opačnou implikaci, tedy, že pro každou sudou permutaci σ existují vhodné permutace τ, ρ splňující $\sigma = \tau^2 \circ \rho^2$.

Buď tedy σ sudá permutace. Uvažujme rozklad σ na nezávislé cykly

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_m \circ \rho_1 \circ \rho_2 \circ \cdots \circ \rho_r \ ,$$

kde pro $i = 1, \ldots, m$ je σ_i cyklus liché délky p_i, a pro $j = 1, \ldots, r$ je ρ_j cyklus sudé délky q_j. Přitom r je sudé číslo, neboť σ je sudá permutace. Cyklus $(x_1, x_2, \ldots, x_q)$ sudé délky q lze psát jako $(x_1, \ldots, x_{q-1}) \circ (x_{q-1}, x_q)$, tedy jako součin cyklu liché délky a transpozice. Tedy pro libovolné $j = 1, \ldots, r$ máme $\rho_j = \sigma_{m+j} \circ \rho'_j$, kde σ_{r+j} je cyklus liché délky p_{r+j} a ρ'_j je transpozice. Navíc jsou všechny tyto cykly po dvou nezávislé s vyjímkou dvojic σ_{m+j}, ρ'_j. Proto můžeme psát

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_{m+r} \circ \rho'_1 \circ \rho'_2 \circ \cdots \circ \rho'_r \ .$$

Položme $\gamma = \sigma_1 \circ \cdots \circ \sigma_{m+r}$ a $\delta = \rho'_1 \circ \rho'_2 \circ \cdots \circ \rho'_r$. Víme, že v rozkladu na nezávislé cykly obsahuje γ pouze cykly liché délky a δ pouze r transpozic. Protože r je sudé číslo, dle části c) existují permutace $\tau, \rho \in \mathbb{S}_n$ takové, že $\tau^2 = \gamma$ a $\rho^2 = \delta$. Tudíž $\tau^2 \rho^2 = \gamma \circ \delta = \sigma$.

Seminář: 1. Rozhodněte, kdy pro permutaci σ platí následující podmínka

$$\exists \tau \in \mathbb{S}_n : \ \sigma = \tau^3 \ .$$

2. Určete, pro které permutace $\sigma \in \mathbb{S}_n$ existují $\tau, \rho \in \mathbb{S}_n$ splňující $\sigma = \tau^3 \circ \rho^3$.

3. Pro dané n, k uvažujme zobrazení $\varphi_{n,k} : \mathbb{S}_n \to \mathbb{S}_n$ dané předpisem $\varphi_{n,k}(\sigma) = \sigma^k$. Určete pro které dvojice čísel n, k je zobrazení $\varphi_{n,k}$ bijekce.

2. kolo — řešení

Na přednášce jsme definovali množinu $\mathbb{C}^*$ jako množinu všech nenulových komplexních čísel, tedy $(\mathbb{C}^*, \cdot)$ je grupa na této množině vzhledem k operaci násobení komplexních čísel.

a-b) Užijeme Moivreovu větu: Každé nenulové komplexní číslo α lze psát ve tvaru

$$\alpha = r \cdot (\cos\gamma + i \sin\gamma)$$

pro vhodná $r \in \mathbb{R}$, $r > 0$, $\gamma \in \mathbb{R}$, přičemž $r = |\alpha|$ je dáno jednoznačně a γ je dáno jednoznačně až na přičtení celočíselného násobku 2π. Pak pro libovolné celé číslo n platí

$$\alpha^n = r^n \cdot (\cos n\gamma + i \sin n\gamma).$$

Jestliže má $\alpha \in \mathbb{C}^*$ konečný řád v grupě $(\mathbb{C}^*, \cdot)$, existuje $n \in \mathbb{N}$ tak,že platí $\alpha^n = 1$. To pak znamená, že $r^n = 1$ a že existuje $k \in \mathbb{Z}$ splňující $n\gamma = 2k\pi$. Odtud $r = 1$, neboť r je kladné reálné číslo, a $\gamma = \frac{2k}{n}\pi$ je součinem racionálního čísla $\frac{k}{n}$ a čísla 2π. Tedy každé číslo $\alpha \in \mathbb{C}^*$, které má konečný řád v grupě $(\mathbb{C}^*, \cdot)$, je tvaru $\alpha = \cos(u \cdot 2\pi) + i \sin(u \cdot 2\pi)$ pro vhodné $u \in \mathbb{Q}$. Protože jsou funkce cos a sin periodické s periodou 2π, je možné ještě přidat požadavek $0 \leq u < 1$.

Naopak, libovolné racionální číslo u lze jednoznačně zapsat ve tvaru $u = \frac{p}{q}$, kde $p \in \mathbb{Z}$, $q \in \mathbb{N}$ a čísla p, q jsou nesoudělná. Označme $\beta = \cos(\frac{p}{q} \cdot 2\pi) + i \sin(\frac{p}{q} \cdot 2\pi)$. Pro každé $t \in \mathbb{N}$ pak podle Moivreovy věty platí

$$\beta^t = \cos(\tfrac{pt}{q} \cdot 2\pi) + i \sin(\tfrac{pt}{q} \cdot 2\pi).$$

Platí tedy $\beta^t = 1$, právě když $\frac{pt}{q} \in \mathbb{Z}$, což je ekvavalentní s $q \mid pt$. Protože jsou čísla p, q nesoudělná, je poslední podmínka ekvivalentní s $q \mid t$. Dokázali jsme, že číslo β má řád q v grupě $(\mathbb{C}^*, \cdot)$.

Dostali jsme tedy řešení úlohy a): Množinou všech komplexních čísel, které mají konečný řád v grupě $(\mathbb{C}^*, \cdot)$, je

$$\big\{\cos(u \cdot 2\pi) + i \sin(u \cdot 2\pi);\ u \in \mathbb{Q},\ 0 \leq u < 1\big\}.$$

Rovněž odvodíme řešení úlohy b): číslo β má řád n, právě když

$$\beta = \cos(\tfrac{p}{n} \cdot 2\pi) + i \sin(\tfrac{p}{n} \cdot 2\pi),$$

kde $p \in \mathbb{Z}$, $(p, n) = 1$. Přidáme-li podmínku $0 < p \leq n$, dostaneme tak každé takové β jednoznačně. V grupě $(\mathbb{C}^*, \cdot)$ tedy existuje prvků řádu n právě tolik, kolik je takových p, tj. právě $\varphi(n)$, kde φ je Eulerova funkce.

c) Označme m_n největší z řádů všech prvků grupy $(\mathbb{S}_n, \circ)$. Probírkou všech možných permutací snadno dostaneme, že pro $n \leq 4$ platí $m_n = n$, přičemž největší řád má cyklus $(1, 2, \ldots, n)$. Pro $n \geq 5$ mají grupy příliš mnoho prvků, nebudeme tedy procházet všechny možné prvky, ale budeme postupovat jinak:

Libovolná neidentická permutace $\sigma \in \mathbb{S}_n$ je složením nezávislých cyklů délky alespoň 2, přičemž součet jejich délek je nejvýše n. Je-li mezi nimi cyklus délky k, přičemž $k = rs$ pro nesoudělná čísla $r \geq 2$, $s \geq 3$, je k nejmenší společný násobek čísel r, s a platí $r + s < rs = k$, neboť $1 < (r-1)(s-1) = 1 - r - s + rs$. Je-li tedy $k = p_1^{e_1} \cdots p_t^{e_t}$, kde $p_1 < \cdots < p_t$ jsou prvočísla a $e_1, \ldots, e_t \in \mathbb{N}$, lze cyklus délky k nahradit nezávislými cykly délek $p_1^{e_1}$, …, $p_t^{e_t}$, přičemž na to ani nevyužijeme všech k prvků zmiňovaného cyklu. Tím získáme permutaci $\tau \in \mathbb{S}_n$, $\tau \neq \sigma$, přičemž τ a σ mají stejný řád. Provedeme-li to se všemi cykly permutace σ, jejichž délka není mocnina prvočísla, dostaneme nakonec permutaci, jejíž každý nezávislý cyklus má délku, která je mocninou prvočísla, přičemž tato permutace má stále stejný řád jako permutace σ. Zřejmě se její řád nezmění, pokud pro každé prvočíslo p ponecháme jen ten z nejdelší z cyklů, jejichž délka je mocninou prvočísla p. Tím jsme dostali, že m_n je největší možný součin činitelů, které jsou

mocninami různých prvočísel, přičemž součet těchto mocnin prvočísel nepřevýší n. V následující tabulce je uveden vždy takový největší součin, spolu spříkladem permutace řádu m_n:

$$\begin{aligned}
m_5 &= 2 \cdot 3 = 6, && (1,2) \circ (3,4,5);\\
m_6 &= 2 \cdot 3 = 6, && (1,2) \circ (3,4,5);\\
m_7 &= 2^2 \cdot 3 = 12, && (1,2,3,4) \circ (5,6,7);\\
m_8 &= 3 \cdot 5 = 15, && (1,2,3) \circ (4,5,6,7,8);\\
m_9 &= 2^2 \cdot 5 = 20, && (1,2,3,4) \circ (5,6,7,8,9);\\
m_{10} &= 2 \cdot 3 \cdot 5 = 30, && (1,2) \circ (3,4,5) \circ (6,7,8,9,10);\\
m_{11} &= 2 \cdot 3 \cdot 5 = 30, && (1,2) \circ (3,4,5) \circ (6,7,8,9,10);\\
m_{12} &= 2^2 \cdot 3 \cdot 5 = 60, && (1,2,3,4) \circ (5,6,7) \circ (8,9,10,11,12).
\end{aligned}$$

Exponenty grup $\mathbb{S}_n$ pro $n \leq 12$ spočítáme odvozeným vzorcem v následující části.

d) Protože grupa $\mathbb{S}_n$ obsahuje cykly všech délek 2, 3, …, n a cyklus délky k má řád k v grupě $\mathbb{S}_n$, je hledaný exponent dělitelný každým z čísel 2, 3, …, n, a tedy je dělitelný i jejich nejmenším společným násobkem.

Na druhou stranu je libovolná neidentická permutace z $\mathbb{S}_n$ složením nezávislých cyklů, z nichž každý má délku nejvýše n. Řád této permutace je pak nejmenší společný násobek délek použitých cyklů, a tedy dělitelem nejmenšího společného násobku čísel 2, 3, …, n.

Dostali jsme, že hledaný exponent e_n je nejmenší společný násobek čísel 2, 3, …, n. Zbývá ještě nalézt vzorec popisující rozklad čísla e_n na součin prvočísel. Číslo e_n je dělitelné jen prvočísly dělícími některé z čísel 2, 3, …, n, tedy prvočísly $p \leq n$. Navíc z jednoznačného rozkladu na součin prvočísel plyne, že pro libovolné $k \in \mathbb{N}$ platí $p^k \mid e_n$, právě když p^k je dělitelem některého z čísel 2, 3, …, n, tedy právě když $p^k \leq n$. Platí tedy

$$e_n = \prod_{\text{prvočíslo } p \leq n} p^{k_p},$$

kde k_p je největší celé číslo splňující $p^{k_p} \leq n$, tedy $k_p \leq \frac{\ln n}{\ln p}$. Je tedy $k_p = \left[\frac{\ln n}{\ln p}\right]$, kde $[x]$ je celá část reálného čísla x, tj. $[x] \in \mathbb{Z}$, $[x] \leq x < [x] + 1$.

Speciálně

$$\begin{aligned}
e_1 &= 1,\\
e_2 &= 2,\\
e_3 &= 2 \cdot 3 = 6,\\
e_4 &= 2^2 \cdot 3 = 12,\\
e_5 &= 2^2 \cdot 3 \cdot 5 = 60,\\
e_6 &= 2^2 \cdot 3 \cdot 5 = 60,\\
e_7 &= 2^2 \cdot 3 \cdot 5 \cdot 7 = 420,\\
e_8 &= 2^3 \cdot 3 \cdot 5 \cdot 7 = 840,\\
e_9 &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520,\\
e_{10} &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520,\\
e_{11} &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27720,\\
e_{12} &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27720.
\end{aligned}$$

Seminář: 1. Nalezněte exponent grupy $\mathbb{D}_n$ pro každé $n \in \mathbb{N}$, $n \geq 3$.

2. Nalezněte exponent grupy všech rotací čtyřstěnu, resp. krychle.
3. Nalezněte exponent grupy všech shodností čtyřstěnu, resp. krychle.

3. kolo — řešení

a) Vezměme si libovolné $b \in H$. Jelikož je homomorfismus φ surjektivní, existuje $a \in G$ takové, že $b = \varphi(a)$. Dále víme, že grupa G má exponent 2, a tak platí $a^2 = 1$. Odtud plyne $b^2 = \varphi(a)^2 = \varphi(a^2) = \varphi(1) = 1$, a tak má b řád 1 nebo 2. Toto platí pro všechny prvky H, a tedy H má exponent 1 nebo 2.

b) Vezměme si libovolné prvky a, b zadané grupy. Pak platí $a^2 = b^2 = (ab)^2 = 1$, a tak $ab = a(ab)^2b = a^2bab^2 = ba$ a tedy zadaná grupa je komutativní.

c) Předpokládejme nejprve, že předpis korektně zadává zobrazení. Platí $[1]_m = [m+1]_m \in \mathbb{Z}_m^\times$, a tak musí být $[1]_n = \varphi([1]_m) = \varphi([m+1]_m) = [m+1]_n$, což zřejmě platí právě tehdy, když $n \mid m$. Nyní naopak předpokládejme, že $n \mid m$. Pokud pro $a, b \in \mathbb{Z}$ platí $[a]_m = [b]_m$, pak zřejmě $[a]_n = [b]_n$, a tak předepsaná hodnota nezáleží na volbě reprezentanta dané zbytkové třídy. Dále $(a, m) = 1$ implikuje $(a, n) = 1$, a tedy pro každé $[a]_m \in \mathbb{Z}_m^\times$ platí $[a]_n \in \mathbb{Z}_n^\times$, předpis tedy skutečně zadává korektně definované zobrazení $\mathbb{Z}_m^\times \to \mathbb{Z}_n^\times$.

Odteď tedy předpokládejme, že $n \mid m$. Nejprve ukážeme, že je φ homomorfismus grup. To plyne z toho, že pro libovolné $[a]_m, [b]_m \in \mathbb{Z}_m^\times$ platí $\varphi([a]_m \cdot [b]_m) = \varphi([ab]_m) = [ab]_n = [a]_n \cdot [b]_n = \varphi([a]_m) \cdot \varphi([a]_m)$. Zbývá ukázat, že je φ surjektivní. Nechť

$$m = \prod_{p \mid m} p^{\alpha_p}$$

je prvočíselný rozklad čísla m, kde $\alpha_p \in \mathbb{N}$ pro všechna prvočísla p dělící m. Označme $\mathcal{P}$ množinu všech prvočísel, které dělí m a zároveň nedělí n, a $\mathcal{Q}$ množinu všech prvočísel dělících n. Dále označme

$$r = \prod_{p \in \mathcal{P}} p^{\alpha_p}, s = \prod_{p \in \mathcal{Q}} p^{\alpha_p}.$$

Potom zřejmě $m = rs$, $(r, s) = (r, n) = 1$, a tak $n \mid s$. Vezměme si libovolné $[a]_n \in \mathbb{Z}_n^\times$. Potom $(a, n) = 1$, a tak $(a, s) = 1$, neboť n a s jsou dělitelné stejnými prvočísly. Podle čínské zbytkové věty existuje $x \in \mathbb{Z}$ takové, že $x \equiv 1 \pmod{r}$ a $x \equiv a \pmod{s}$. Potom $(x, r) = 1$ a $(x, s) = (a, s) = 1$, a tak $(x, m) = 1$. Navíc platí $x \equiv a \pmod{n}$. Tudíž $[x]_m \in \mathbb{Z}_m^\times$ a $\varphi([x]_m) = [x]_n = [a]_n$, a tedy φ je surjektivní.

d) Předpokládejme nejprve, že $p \geq 5$. Potom $[3]_{p^k} \in \mathbb{Z}_{p^k}^\times$ ale $[3]_{p^k}^2 \neq [1]_{p^k}$ (neboť $p^k \nmid 8$) a tak $\mathbb{Z}_{p^k}^\times$ nemá exponent 2.

Nyní předpokládejme, že $p = 3$. Přímým ověřením se snadno zjistí, že $\mathbb{Z}_3^\times$ má exponent 2, ale $\mathbb{Z}_9^\times$ má exponent větší než 2, a tak z tvrzení v částech a) a c) plyne, že $\mathbb{Z}_{3^k}^\times$ nemá exponent 2 ani pro žádné $k \geq 2$.

Nakonec předpokládejme, že $p = 2$. Opět přímým ověřením snadno zjistíme, že $\mathbb{Z}_2^\times$ má exponent 1, $\mathbb{Z}_4^\times$ a $\mathbb{Z}_8^\times$ mají exponent 2 a $\mathbb{Z}_{16}^\times$ má exponent větší než 2, z čehož stejně jako výše plyne, že $\mathbb{Z}_{2^k}^\times$ nemá exponent 2 pro žádné $k \geq 4$.

Celkem jsme tedy dostali, že $\mathbb{Z}_{p^k}^\times$ má exponent 2 pro $p^k \in \{3, 4, 8\}$.

e) Nechť

$$n = \prod_{p \mid n} p^{\alpha_p}$$

je prvočíselný rozklad čísla n, kde $\alpha_p \in \mathbb{N}$ pro všechna prvočísla p dělící n. Z čínské zbytkové věty potom plyne

$$(\mathbb{Z}_n^\times, \cdot) \cong \prod_{p|n} \left(\mathbb{Z}_{p^{\alpha_p}}^\times, \cdot\right).$$

Snadno se uvidí, že exponent součinu konečně mnoha konečných grup je roven nejmenšímu společnému násobku exponentů těchto grup, a tak $(\mathbb{Z}_n^\times, \cdot)$ bude mít exponent 1 nebo 2 právě tehdy, když grupy $(\mathbb{Z}_{p^{\alpha_p}}^\times, \cdot)$ budou mít exponent 1 nebo 2 pro všechna prvočísla p dělící n. Grupa $(\mathbb{Z}_{p^k}^\times, \cdot)$ má exponent 1 (tj. je triviální) pouze pro $p = 2$ a $k = 1$, neboť ve všech ostatních případech je $|\mathbb{Z}_{p^k}^\times| = \varphi(p^k) = (p-1)p^{k-1} > 1$, a má exponent 2 pro $p^k \in \{3, 4, 8\}$ podle části d). Z toho je snadno vidět, že $(\mathbb{Z}_n^\times, \cdot)$ má exponent 1 nebo 2 právě tehdy, když $n \mid 24$. Pro $n = 1$ a $n = 2$ je $(\mathbb{Z}_n^\times, \cdot)$ triviální, tedy má exponent 1, v ostatních případech, tj. pro $n \in \{3, 4, 6, 8, 12, 24\}$, má exponent 2.

Poznámka: Na závěr zmíníme jednu aplikaci předchozího výsledku. Dirichletova věta o prvočíslech v aritmetických posloupnostech říká, že pro každé $a \in \mathbb{Z}$, $n \in \mathbb{N}$ takové, že $(a, n) = 1$, existuje nekonečně mnoho prvočísel p takových, že $p \equiv a \pmod{n}$. Důkaz tohoto tvrzení v plné obecnosti je relativně obtížný, v některých speciálních případech jej ale lze dokázat elementárnějším způsobem. Konkrétně platí, že pro danou dvojici a, n existuje elementární (ve smyslu, který lze exaktně definovat) důkaz tvrzení právě tehdy, když $a^2 \equiv 1 \pmod{n}$. Zejména pro dané n lze tvrzení dokázat elementárně pro všechna a s ním nesoudělná právě tehdy, když má grupa $(\mathbb{Z}_n^\times, \cdot)$ exponent 1 nebo 2, což jak jsme ukázali je právě tehdy, když $n \mid 24$.

4. kolo — řešení

a) Ukážeme nejprve, že $f(H) \neq G_2$. Předpokládejme sporem, že tomu tak není. Vezměme si libovolné $g \in G_1 \setminus H$. Jelikož $f(H) = G_2$, existuje $h \in H$ takové, že $f(h) = f(g)$. Potom $f(gh^{-1}) = 1$, tedy $gh^{-1} \in \ker f$, a tudíž $gh^{-1} \in H$. Pak $g = (gh^{-1})h \in H$, což je spor. Předpokládejme nyní, že existuje podgrupa $M \leq G_2$ taková, že $f(H) \subseteq M$ a $f(H) \neq M \neq G_2$. Pak zřejmě $f^{-1}(f(H)) \subseteq f^{-1}(M)$. Platí $H \subseteq f^{-1}(f(H))$, a tak $H \subseteq f^{-1}(M)$. Ze surjektivity f snadno plyne, že $f(f^{-1}(M)) = M$. Kdyby bylo $H = f^{-1}(M)$, pak $f(H) = f(f^{-1}(M)) = M$, což je spor. Kdyby bylo $f^{-1}(M) = G_1$, pak $M = f(f^{-1}(M)) = f(G_1) = G_2$, opět spor. Celkem tedy $H \neq f^{-1}(M) \neq G_1$, což je spor s maximalitou H v G_1. Žádná taková podgrupa M tedy neexistuje, a tedy $f(H)$ je maximální podgrupa G_2.

b) Ze surjektivity f snadno plyne, že $f(f^{-1}(K)) = K$. Kdyby bylo $f^{-1}(K) = G_1$, pak $K = f(f^{-1}(K)) = f(G_1) = G_2$, což je spor. Předpokládejme nyní, že existuje podgrupa $M \leq G_1$ taková, že $f^{-1}(K) \subseteq M$ a $f^{-1}(K) \neq M \neq G_1$. Pak $K = f(f^{-1}(K)) \subseteq f(M)$. Kdyby bylo $K = f(M)$, pak si vezměme libovolné $m \in M \setminus f^{-1}(K)$. Potom ze surjektivity f plyne, že existuje $k \in f^{-1}(K)$ takové, že $f(k) = f(m)$. Pak $f(mk^{-1}) = 1 \in K$, a tedy $mk^{-1} \in f^{-1}(K)$. Pak $m = (mk^{-1})k \in f^{-1}(K)$, spor. Analogicky kdyby $f(M) = G_2$, pak si vezměme libovolné $g \in G_1 \setminus M$. Potom existuje $n \in M$ takové, že $f(n) = f(g)$. Pak $f(gn^{-1}) = 1 \in K$, a tedy $gn^{-1} \in f^{-1}(K)$, tudíž $gn^{-1} \in M$. Pak $g = (gn^{-1})n \in M$, opět spor. Celkem tedy $K \neq f(M) \neq G_2$, což je spor s maximalitou K v G_2. Žádná taková podgrupa M tedy neexistuje, a tedy $f^{-1}(K)$ je maximální podgrupa G_1.

c) Nechť σ je lichá permutace obsažená v dané podgrupě. Uvažme homomorfismus parity $p\colon \mathbb{S}_n \to \{\pm 1\}$. Permutaci σ lichá, tedy $p(\sigma) = -1$. Řád $p(\sigma)$ musí dělit řád σ. Zřejmě řád prvku

-1 v grupě $\{\pm 1\}$ je 2, a tak je řád σ sudý. Podle Lagrangeovy věty je pak i řád dané podgrupy sudý.

d) Pokud daná maximální podgrupa grupy $\mathbb{S}_n$ obsahuje nějakou lichou permutaci, pak je její řád sudý podle části c). Jediná maximální podgrupa grupy $\mathbb{S}_n$ obsahující pouze sudé permutace je evidentně podgrupa $\mathbb{A}_n$, jejíž řád je $n!/2$, což je sudé číslo pro $n \geq 4$.

e) 1. Pro $n = 2$ hráč A vyhraje, pokud v prvním tahu vybere identitu. Pro $n = 3$ si může hráč A zaručit výhru následujícím způsobem. V prvním tahu vybere $(1, 2, 3)$. Potom hráč B musí vybrat sudou permutaci, jinak by prohrál. V následujícím tahu vybere A zbývající sudou permutaci (grupa $\mathbb{S}_3$ obsahuje 3 sudé permutace) a B v následujícím tahu nutně prohraje.

2. Předpokládejme nyní, že $n \geq 4$. Potom má hráč B následující vítěznou strategii. Pokaždé, když je B na tahu, vybere si nějakou maximální podgrupu $M \leq \mathbb{S}_n$, která obsahuje všechny již vybrané prvky (taková zřejmě existuje). Jelikož podle části d) má M sudý řád a počet vybraných prvků v daný moment musí být lichý, existuje prvek podgrupy M, který ještě nebyl vybrán. Pokud hráč B vybere libovolný takový prvek, tak má zaručeno, že neprohraje, neboť i po jeho tahu budou všechny vybrané prvky obsaženy v M, a tak nemůžou generovat celou $\mathbb{S}_n$. Jelikož hra může trvat jenom konečný počet tahů, hráč B musí při této strategii po dostatečně velkém počtu tahů vyhrát.

5. kolo — řešení

a) Jsou-li A, B libovolné podmnožiny nosné množiny G grupy $(G, \cdot)$, pak z inkluze $A \subseteq B$ plyne $\langle A \rangle \subseteq \langle B \rangle$, vždyť $\langle A \rangle$ je nejmenší podgrupa grupy G obsahující množinu A a $\langle B \rangle$ je (nejmenší) podgrupa grupy G obsahující množinu B, a tedy $\langle B \rangle$ obsahuje i množinu A.

(i) Inkluze $\langle X \rangle \cap \langle Y \rangle \subseteq \langle X \cap Y \rangle$ neplatí. Protipříkladem jsou například množiny $X = \{1\}$ a $Y = \{-1\}$ v grupě $(\mathbb{Z}, +)$, kdy $\langle X \rangle \cap \langle Y \rangle = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$ a $\langle X \cap Y \rangle = \langle \emptyset \rangle = \{0\}$.

Z inkluze $X \cap Y \subseteq X$ plyne $\langle X \cap Y \rangle \subseteq \langle X \rangle$. Podobně z $X \cap Y \subseteq Y$ plyne $\langle X \cap Y \rangle \subseteq \langle Y \rangle$. Dohromady $\langle X \cap Y \rangle \subseteq \langle X \rangle \cap \langle Y \rangle$.

(ii) Z inkluze $X \subseteq X \cup Y$ plyne $\langle X \rangle \subseteq \langle X \cup Y \rangle$. Podobně z $Y \subseteq X \cup Y$ plyne $\langle Y \rangle \subseteq \langle X \cup Y \rangle$. Dohromady $\langle X \rangle \cup \langle Y \rangle \subseteq \langle X \cup Y \rangle$. Odtud $\big\langle \langle X \rangle \cup \langle Y \rangle \big\rangle \subseteq \big\langle \langle X \cup Y \rangle \big\rangle$. Protože $\langle X \cup Y \rangle$ je podgrupa grupy G, je $\big\langle \langle X \cup Y \rangle \big\rangle = \langle X \cup Y \rangle$.

Z inkluzí $X \subseteq \langle X \rangle$ a $Y \subseteq \langle Y \rangle$ plyne $X \cup Y \subseteq \langle X \rangle \cup \langle Y \rangle$, odtud $\langle X \cup Y \rangle \subseteq \big\langle \langle X \rangle \cup \langle Y \rangle \big\rangle$.

b) Uvažme grupu $(\{1, -1\}, \cdot)$ a zobrazení $f : G \to \{1, -1\}$ určené předpisem

$$f(x) = \begin{cases} 1 & \text{jestliže } x \in H, \\ -1 & \text{jestliže } x \in G - H. \end{cases}$$

Ukážeme, že f je homomorfismus. Zvolme libovolné $a, b \in G$ a rozlišme čtyři případy:

- Jestliže $a \in H$, $b \in H$, pak i $a \cdot b \in H$, protože H je podgrupa. Pak $f(a) \cdot f(b) = 1 \cdot 1 = 1 = f(a \cdot b)$.
- Jestliže $a \in H$, $b \notin H$, pak $a \cdot b \notin H$, neboť z $a \cdot b \in H$ by plynulo $b = a^{-1} \cdot (a \cdot b) \in H$. Je tedy $f(a) \cdot f(b) = 1 \cdot (-1) = -1 = f(a \cdot b)$.
- Jestliže $a \notin H$, $b \in H$, pak $a \cdot b \notin H$, neboť z $a \cdot b \in H$ by plynulo $a = (a \cdot b) \cdot b^{-1} \in H$. Je tedy $f(a) \cdot f(b) = (-1) \cdot 1 = -1 = f(a \cdot b)$.

- Jestliže $a \notin H$, $b \notin H$, pak $a^{-1} \notin H$, neboť z $a^{-1} \in H$ by plynulo $a \in H$. Proto obě levé třídy $a^{-1} \cdot H$ a $b \cdot H$ jsou různé od H. Protože je index podgrupy H v grupě G roven dvěma, existují jen dvě levé třídy, proto $a^{-1} \cdot H = b \cdot H$, což je ekvivalentní s $a \cdot b \in H$. Je tedy $f(a) \cdot f(b) = (-1) \cdot (-1) = 1 = f(a \cdot b)$.

Je tedy f homomorfismus. Jeho jádro $\ker f = H$ je normální podgrupa grupy G.

c) Označme h generátor podgrupy H, tj. $H = \langle h \rangle = \{h^n;\, n \in \mathbb{Z}\}$. Nechť $g \in G$ a $k \in K$ jsou libovolné, existuje tedy $n \in \mathbb{Z}$ tak, že $k = h^n$. Protože H je normální podgrupa grupy G, je $g \cdot h \cdot g^{-1} \in H$, a proto existuje $m \in \mathbb{Z}$ tak, že $g \cdot h \cdot g^{-1} = h^m$. Použitím níže dokázané rovnosti $(g \cdot h \cdot g^{-1})^n = g \cdot h^n \cdot g^{-1}$ dostáváme

$$g \cdot k \cdot g^{-1} = g \cdot h^n \cdot g^{-1} = (g \cdot h \cdot g^{-1})^n = (h^m)^n = (h^n)^m = k^m \in K.$$

Dokažme nyní slibovanou rovnost $(g \cdot h \cdot g^{-1})^n = g \cdot h^n \cdot g^{-1}$ pro každé $n \in \mathbb{Z}$. Pro $n = 0$ zřejmě platí, stačí tedy dokázat pro libovolné přirozené číslo n, že

$$(g \cdot h \cdot g^{-1})^n = g \cdot h^n \cdot g^{-1}, \qquad (g \cdot h \cdot g^{-1})^{-n} = g \cdot h^{-n} \cdot g^{-1}.$$

To uděláme indukcí. Pro $n = 1$ je první rovnost zřejmá a druhá plyne z odvozeného vzorce pro inverzní prvek k součinu. Předpokládejme tedy, že rovnosti platí pro libovolné dané přirozené n a dokažme jej pro $n + 1$. Užitím indukčního předpokladu

$$\begin{aligned}(g \cdot h \cdot g^{-1})^{n+1} &= (g \cdot h \cdot g^{-1})^n \cdot (g \cdot h \cdot g^{-1}) = g \cdot h^n \cdot g^{-1} \cdot g \cdot h \cdot g^{-1} = g \cdot h^{n+1} \cdot g^{-1},\\ (g \cdot h \cdot g^{-1})^{-(n+1)} &= (g \cdot h \cdot g^{-1})^{-n} \cdot (g \cdot h \cdot g^{-1})^{-1} = g \cdot h^{-n} \cdot g^{-1} \cdot g \cdot h^{-1} \cdot g^{-1} = g \cdot h^{-(n+1)} \cdot g^{-1}.\end{aligned}$$

d) Nechť $H \in \mathcal{R}$ je ta třída rozkladu $\mathcal{R}$, která obsahuje neutrální prvek 1 grupy G. Dokážeme, že H je podgrupa grupy G.

Pro libovolný prvek $a \in H$ je $A = \{a \cdot h;\, h \in H\} \in \mathcal{R}$. Protože $1 \in H$, platí $a \in A$. Tedy $a \in A \cap H$ a z toho, že $\mathcal{R}$ je rozklad, plyne $A = H$. Proto $a \cdot h \in H$ pro každé $a, h \in H$. Podobně pro libovolný prvek $b \in H$ je $B = \{b^{-1} \cdot h;\, h \in H\} \in \mathcal{R}$. Pak $1 = b^{-1} \cdot b \in B$, tedy $B = H$, odkud $b^{-1} = b^{-1} \cdot 1 \in B = H$. Je tedy H podgrupa grupy G.

Ze zadání je každá levá třída grupy G podle podgrupy H prvkem $\mathcal{R}$. Ukažme také, že každá třída $T \in \mathcal{R}$ je levou třídou grupy G podle podgrupy H. Třídy rozkladu jsou podle definice neprázdné, existuje tedy $t \in T$. Pak levá třída $t \cdot H \in \mathcal{R}$ a platí $t \in T \cap (t \cdot H)$, tedy $T = t \cdot H$.

6. kolo — řešení

a) (i) Je zřejmé, že operace na G je korektně definovaná. Nejprve ověříme, že je tato operace asociativní. Nechť $h_1, h_2, h_3 \in H$, $k_1, k_2, k_3 \in K$. Potom platí

$$\begin{aligned}&((h_1, k_1) \cdot (h_2, k_2)) \cdot (h_3, k_3)\\ &\quad = (h_1(\varphi(k_1)(h_2)), k_1k_2) \cdot (h_3, k_3)\\ &\quad = (h_1(\varphi(k_1)(h_2))(\varphi(k_1k_2)(h_3)), (k_1k_2)k_3)\\ &\quad = (h_1(\varphi(k_1)(h_2))(\varphi(k_1)(\varphi(k_2)(h_3))), k_1k_2k_3) \quad \textit{(φ je homomorfismus $K \to \mathrm{Aut}(H)$)}\\ &\quad = (h_1(\varphi(k_1)(h_2(\varphi(k_2)(h_3)))), k_1(k_2k_3)) \quad \textit{($\varphi(k_1)$ je automorfismus H)}\\ &\quad = ((h_1, k_1) \cdot (h_2(\varphi(k_2)(h_3)), k_2k_3)\\ &\quad = (h_1, k_1) \cdot ((h_2, k_2) \cdot (h_3, k_3)),\end{aligned}$$

skutečně tedy jde o asociativní operaci. Dále pro každé $h \in H$, $k \in K$ platí $(h,k)\cdot(1_H,1_K) = (h(\varphi(k)(1_H)), k\cdot 1_K) = (h\cdot 1_H, k) = (h,k)$ (neboť $\varphi(k)$ je automorfismus H, a tak $\varphi(k)(1_H) = 1_H$) a $(1_H,1_K)\cdot(h,k) = (1_H\cdot\varphi(1_K)(h), 1_K\cdot k) = (h,k)$ (protože φ je homomorfismus $K \to \mathrm{Aut}(H)$, a tedy $\varphi(1_K) = \mathrm{Id}_H$), takže $(1_H,1_K)$ je neutrální prvek této operace. Navíc ukážeme, že prvek $(\varphi(k^{-1})(h^{-1}), k^{-1})$ je inverzní prvek k prvku (h,k) (to, že inverzi máme hledat zrovna v tomto tvaru, se snadno nahlédne ze vzorce pro operaci $\cdot$). Skutečně platí

$$\begin{aligned}
&(h,k)\cdot(\varphi(k^{-1})(h^{-1}), k^{-1})\\
&\qquad = (h(\varphi(k)(\varphi(k^{-1})(h^{-1}))), kk^{-1})\\
&\qquad = (h(\varphi(kk^{-1})(h^{-1})), 1_K) \quad \textit{(φ je homomorfismus $K \to \mathrm{Aut}(H)$)}\\
&\qquad = (h(\varphi(1_K)(h^{-1})), 1_K)\\
&\qquad = (hh^{-1}, 1_K) \quad \textit{(φ je homomorfismus $K \to \mathrm{Aut}(H)$, tudíž $\varphi(1_K) = \mathrm{Id}_H$)}\\
&\qquad = (1_H, 1_K),
\end{aligned}$$

$$\begin{aligned}
&(\varphi(k^{-1})(h^{-1}), k^{-1})\cdot(h,k)\\
&\qquad = ((\varphi(k^{-1})(h^{-1}))(\varphi(k^{-1})(h)), k^{-1}k)\\
&\qquad = (\varphi(k^{-1})(h^{-1}h), 1_K) \quad \textit{($\varphi(k^{-1})$ je automorfismus H)}\\
&\qquad = (\varphi(k^{-1})(1_H), 1_K)\\
&\qquad = (1_H, 1_K) \quad \textit{($\varphi(k^{-1})$ je automorfismus H, a tedy $\varphi(k^{-1})(1_H) = 1_H$).}
\end{aligned}$$

$(G,\cdot)$ je tedy grupa.

Označme $H' = \{(h,1_K)\colon h \in H\}$ a $K' = \{(1_H,k)\colon k \in K\}$. Uvažme zobrazení $i\colon H \to G$ a $j\colon K \to G$ dané předpisy $i(h) = (h,1_K)$ a $j(k) = (1_H,k)$. Pro každé $h_1,h_2 \in H$, $k_1,k_2 \in K$ platí $i(h_1)\cdot i(h_2) = (h_1,1_K)\cdot(h_2,1_K) = (h_1(\varphi(1_K)(h_2)), 1_K\cdot 1_K) = (h_1h_2, 1_K) = i(h_1h_2)$ a $j(k_1)\cdot j(k_2) = (1_H,k_1)\cdot(1_H,k_2) = (1_H\cdot\varphi(k_1)(1_H), k_1k_2) = (1_H,k_1k_2) = j(k_1k_2)$, takže i a j jsou homomorfismy. Navíc jsou oba zřejmě injektivní a jejich obrazy jsou H' resp. K', takže H' a K' jsou podgrupy G izomorfní H resp. K.

Ukážeme ještě, že H' je normální podgrupa G. Nechť $h \in H$. Pro každé $x \in H$, $y \in K$ platí $(x,y) = (x,1_K)\cdot(1_H,y)$, a tak $(x,y)\cdot(h,1_K)\cdot(x,y)^{-1} = (x,1_K)\cdot(1_H,y)\cdot(h,1_K)\cdot((x,1_K)\cdot(1_H,y))^{-1} = (x,1_K)\cdot(1_H,y)\cdot(h,1_K)\cdot(1_H,y)^{-1}\cdot(x,1_K)^{-1} = (x,1_K)\cdot(1_H,y)\cdot(h,1_K)\cdot(1_H,y^{-1})\cdot(x^{-1},1_K) = (x,1_K)\cdot((1_H,y)\cdot(h,1_K)\cdot(1_H,y^{-1}))\cdot(x^{-1},1_K) = (x,1_K)\cdot((\varphi(y)(h),y)\cdot(1_H,y^{-1}))\cdot(x^{-1},1_K) = (x,1_K)\cdot(\varphi(y)(h),1_K)\cdot(x^{-1},1_K) = (x(\varphi(y)(h))x^{-1},1_K) \in H'$, tudíž podgrupa H' je opravdu normální (všimněte si, že z tohoto výpočtu je vidět, že vnitřní automorfismy grupy G indukované prvky podgrupy K' působí na podgrupě H' jako automofismy určené homomorfismem φ).

Alternativně lze normalitu podgrupy H' ukázat tak, že ověříme, že projekce z G do K je homomorfismus, jehož jádro je H'. Uvažme tedy zobrazení $p\colon G \to K$ dané předpisem $p((h,k)) = k$. Potom pro každé $h_1,h_2 \in H$, $k_1,k_2 \in K$ platí $p((h_1,k_1)\cdot(h_2,k_2)) = p((h_1(\varphi(k_1)(h_2)), k_1k_2)) = k_1k_2 = p((h_1,k_1))p((h_2,k_2))$. Zobrazení p je tedy skutečně homomorfismus (navíc evidentně surjektivní) a zřejmě platí $\mathrm{Ker}\, p = H'$, opět tedy dostáváme, že H' je normální podgrupa (rozmyslete si, že projekce z G do H je homomorfismus pouze tehdy, když je φ triviální homomorfismus, v tom případě je zřejmě G přímý součin grup H a K).

(ii) Snadno se uvidí, že předpis pro φ zadává korektně definovaný homomorfismus $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$. Označme r rotaci pravidelného n-úhelníku o úhel $2\pi/n$ proti směru hodinových ručiček a s jeho libovolnou (ale pevně zvolenou) osovou souměrnost. Definujme zobrazení $f\colon \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2 \to \mathbb{D}_n$ předpisem $f(([a]_n,[b]_2)) = r^a \circ s^b$. Řád r je n a řád s je 2, f je proto korektně definované.

Navíc prvky $\mathbb{D}_n$ jsou právě r^i a $r^i \circ s$, kde $i \in \{0, \dots, n-1\}$, z čehož je snadno vidět, že f je bijekce. Ukážeme, že f je také homomorfismus. Snadno se nahlédne, že platí $s \circ r = r^{-1} \circ s$ (nakreslete si obrázek), a tak pro všechna $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ je $f(([a_1]_n, [b_1]_2)) \circ f(([a_2]_n, [b_2]_2)) = r^{a_1} \circ s^{b_1} \circ r^{a_2} \circ s^{b_2} = r^{a_1} \circ r^{(-1)^{b_1} a_2} \circ s^{b_1} \circ s^{b_2} = r^{a_1 + (-1)^{b_1} a_2} \circ s^{b_1 + b_2} = f(([a_1 + (-1)^{b_1} a_2]_n, [b_1 + b_2]_2)) = f(([a_1]_n + \varphi([b_1]_2)([a_2]_n), [b_1]_2 + [b_2]_2)) = f(([a_1]_n, [b_1]_2) \cdot ([a_2]_n, [b_2]_2))$. Tudíž f je izomorfismus, a proto $\mathbb{D}_n \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$.

(iii) Opět se snadno zkontroluje, že předpis pro φ zadává korektně definovaný homomorfismus $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$. Stejně tak se snadno ověří, že zobrazení f je korektně definované. Ukážeme, že f je homomorfismus. Platí, že pro každé $b \in \mathbb{Z}$ mají čísla b a $(1 - (-1)^b)/2$ stejnou paritu, proto pro každé $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ platí $f((a_1, [b_1]_2)) \circ f((a_2, [b_2]_2)) = (2a_1 + (1 - (-1)^{b_1})/2) \circ (2a_2 + (1 - (-1)^{b_2})/2) = 2a_1 + (1 - (-1)^{b_1})/2 + (-1)^{2a_1 + (1-(-1)^{b_1})/2}(2a_2 + (1 - (-1)^{b_2})/2) = 2a_1 + (1 - (-1)^{b_1})/2 + (-1)^{b_1}(2a_2 + (1 - (-1)^{b_2})/2) = 2(a_1 + (-1)^{b_1} a_2) + (1 - (-1)^{b_1} + (-1)^{b_1} - (-1)^{b_1 + b_2})/2 = 2(a_1 + (-1)^{b_1} a_2) + (1 - (-1)^{b_1 + b_2})/2 = f((a_1 + (-1)^{b_1} a_2, [b_1 + b_2]_2)) = f((a_1 + \varphi([b_1]_2)(a_2), [b_1]_2 + [b_2]_2)) = f((a_1, [b_1]_2) \cdot (a_2, [b_2]_2))$. Zobrazení f je tedy skutečně homomorfismus, navíc je snadno vidět, že má triviální jádro (neutrální prvek grupy $(\mathbb{Z}, \circ)$ je 0), a tudíž je injektivní. Pro každé $a \in \mathbb{Z}$ platí $f((a, [0]_2)) = 2a$ a $f((a, [1]_2)) = 2a + 1$, a tak je f taky surjektivní, a celkem je to tedy izomorfismus.

b) Pro každé $g \in G$ označme $X_g = \{x \in X \colon \varphi(g)(x) = x\}$ množinu pevných bodů permutace množiny X indukované prvkem g. Předpokládejme sporem, že pro všechna $g \in G$ platí $X_g \neq \emptyset$, tedy $|X_g| \geq 1$. Podle Burnsidova lemmatu je počet orbit dané akce roven aritmetickému průměru čísel $|X_g|$ (přes všechna $g \in G$). Tato akce je ale tranzitivní, tudíž orbita je jenom jedna. Čísla $|X_g|$ jsou tedy všechna větší nebo rovny než 1 a jejich aritmetický průměr je 1. To je možné jedině tak, že $|X_g| = 1$ pro všechna $g \in G$. Platí ale $X_1 = X$, a tak $|X_1| = |X| \geq 2$, spor.

Poznámka: V situaci z příkladu b) si můžeme všimnout toho, že pokud jsou dva prvky grupy G konjugované, potom permutace množiny X indukované těmito prvky mají stejné délky cyklů v rozkladu na nezávislé cykly. Z dokázaného tvrzení tedy plyne, že nejenom existuje $g \in G$ takové, že $X_g = \emptyset$, ale dokonce existuje třída konjugace v G taková, že všechny její prvky mají tuto vlastnost.

Ukažme si ještě jednu aplikaci tohoto tvrzení, jejíž formulace je zcela elementární, nicméně její důkaz je hlubší. Nechť $f(x) \in \mathbb{Z}[x]$ je polynom s celočíselnými koeficienty stupně $n \geq 2$, který je ireducibilní (tj. nejde napsat jako součin dvou polynomů kladného stupně s koeficienty v $\mathbb{Z}$). Potom existuje nekonečně mnoho prvočísel p takových, že kongruence $f(x) \equiv 0 \pmod{p}$ nemá řešení (jinými slovy pro každé $x \in \mathbb{Z}$ je $p \nmid f(x)$). Naše tvrzení se zde využije tak, že za X vezmeme množinu všech kořenů polynomu $f(x)$ (ten má v tělese $\mathbb{C}$ komplexních čísel právě n různých kořenů) a za G tzv. Galoisovu grupu polynomu $f(x)$, kterou lze v tomto případě definovat jako grupu automorfismů nejmenšího podtělesa tělesa $\mathbb{C}$, která obsahuje všechny kořeny $f(x)$. Snadno se nahlédne, že G má kanonickým způsobem akci na X. Trochu těžší je dokázat, že je tato akce tranzitivní. Z našeho tvrzení potom plyne existence automorfismu z této Galoisovy grupy, který nezobrazuje žádný kořen polynomu $f(x)$ sám na sebe. Zbytek důkazu ale využívá věci, které jsou příliš nad rámec tohoto předmětu, zejména je potřeba tzv. Čebotarevova věta o hustotě.

7. kolo — řešení

a) (i) Poznamenejme, že ze zadání ihned plyne, že k dělí n. Protože prvek $a \in G$ je řádu k, jsou prvky $a^0 = 1, a, a^2, \dots, a^{k-1}$ po dvou různé. Pro libovolné $g \in G$ jsou po dvou různé tedy i prvky $g = 1 \cdot g, a \cdot g, a^2 \cdot g, \dots, a^{k-1} \cdot g$. Dále pro libovolné $i \in \{0, \dots, k-1\}$ platí $r_a(a^i g) = a^{i+1} g$, kde v případě $i = k-1$ dostáváme $r_a(a^{k-1} g) = a^k g = g$. Tudíž uvažujeme-li rozklad permutace r_a

na nezávislé cykly, pak libovolný prvek $g \in G$ je součástí cyklu $(g, ag, \ldots, a^{k-1}g)$ délky k. Proto je rozklad r_a tvořen $\frac{n}{k}$ nezávislými cykly délky k.

Parita cyklu délky k je $(-1)^{k-1}$ a tudíž je parita permutace r_a je rovna

$$(-1)^{(k-1)\cdot\frac{n}{k}} = (-1)^{n-\frac{n}{k}}\,.$$

(ii) Uvažujme opět injektivní homomorfismus $r\colon G \to \mathbb{S}(G)$ z Cayleyho věty a označme $H = r(G)$ podgrupu grupy $\mathbb{S}(G)$ izomorfní s grupou G. Nechť $a \in G$ je prvek řádu 2, jehož existence je zaručena dle Cauchyho věty (slajdy str. 62, učebnice věta 10.9). Dle předchozího příkladu je parita permutace $r_a \in H$ rovna $(-1)^m = -1$ a jedná se tedy o lichou permutaci. Stejně jako v řešení příkladu c) z 4. kola, uvažujeme přiřazení parity $\varphi : \mathbb{S}(G) \to \{1, -1\}$ o nemž víme, že je homomorfismus grup. Protože $\varphi(r_a) = -1$, je zúžení zobrazení φ na podmnožinu H, tj. $\varphi|_H : H \to \{1, -1\}$, surjektivní homomorfismus grup. Jeho jádro $K = \ker(\varphi|_H) = H \cap \mathbb{A}(G)$ je normální podgrupou grupy H. Protože $|\ker(\varphi|_H)| \cdot |\varphi(H)| = |H|$, vidíme, že K je podgrupou grupy H indexu 2. Grupa G tedy obsahuje podgrupu indexu 2, kterou je $r^{-1}(K)$.

Argumentaci lze vést i tak, že místo φ uvažujeme homomorfismus $\varphi \circ r : G \to \{1, -1\}$.

b) (i) Za dokázané mějme $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathbb{S}(G)$ – viz komentář k zadání a str. 57 slajdů.

Zbývá tedy dokázat, že podgrupa $\mathrm{Inn}(G)$ grupy $\mathrm{Aut}(G)$ je normální podgrupou. Nechť tedy $\alpha \in \mathrm{Aut}(G)$ je libovolný automorfismus grupy G a $a \in G$ je libovolný prvek G, který zadává vnitřní automorfismus ρ_a. Potřebujeme dokázat, že $\beta = \alpha \circ \rho_a \circ \alpha^{-1}$ je vnitřní automorfismus grupy G. Musíme tedy najít vhodný prvek $b \in G$ tak, aby $\beta = \rho_b$. Z toho důvodu pro libovolný prvek $x \in G$ určíme $\beta(x)$. Platí

$$\beta(x) = (\alpha \circ \rho_a \circ \alpha^{-1})(x) = \alpha(\rho_a(\alpha^{-1}(x))) = \alpha(a \cdot \alpha^{-1}(x) \cdot a^{-1})\,.$$

Protože α je automorfismus, je předchozí výraz dále roven

$$\alpha(a \cdot \alpha^{-1}(x) \cdot a^{-1}) = \alpha(a) \cdot \alpha(\alpha^{-1}(x)) \cdot \alpha(a^{-1}) = \alpha(a) \cdot x \cdot \alpha(a^{-1})\,.$$

Zde $\alpha(a^{-1}) = (\alpha(a))^{-1}$, neboť $\alpha \in \mathrm{Aut}(G)$. Proto označme $b = \alpha(a)$ a platí

$$\beta(x) = \alpha(a) \cdot x \cdot (\alpha(a))^{-1} = b \cdot x \cdot b^{-1} = \rho_b(x)\ .$$

Protože x byl libovolně zvolený prvek z G, dostáváme $\beta = \rho_b \in \mathrm{Inn}(G)$.

(ii) Pro libovolnou grupu G platí, že jádro homomorfismu $\rho : G \to \mathrm{Inn}(G)$ je rovno centru grupy G – podrobnosti na str. 57 slajdů. V případě grupy $G = \mathbb{S}_3$ víme, že $Z(\mathbb{S}_3) = \{\mathrm{id}\}$, neboť $(1,2) \circ (1,2,3) = (2,3) \neq (1,3) = (1,2,3) \circ (1,2)$ atd. Homomorfismus $\rho : \mathbb{S}_3 \to \mathrm{Aut}(\mathbb{S}_3)$ je tedy injektivní a obraz homomorfismu ρ, tj. podgrupa $\mathrm{Inn}(\mathbb{S}_3)$, má 6 prvků.

Ukážeme, že $\mathrm{Aut}(\mathbb{S}_3)$ má nejvýše 6 prvků, čímž bude, díky $\mathrm{Inn}(\mathbb{S}_3) \leq \mathrm{Aut}(\mathbb{S}_3)$, rovnost $\mathrm{Aut}(\mathbb{S}_3) = \mathrm{Inn}(\mathbb{S}_3)$ dokázána. Platí $\mathbb{S}_3 = \langle (1,2), (1,2,3) \rangle$, a proto je libovolný automorfismus α grupy $\mathbb{S}_3$ jednoznačně zadán hodnotami $\alpha((1,2))$ a $\alpha((1,2,3))$. Přitom $\alpha((1,2))$ musí být prvek řádu 2, tj. cyklus délky 2, a podobně $\alpha((1,2,3))$ musí být cyklus délky 3. Pro výběr hodnoty $\alpha((1,2))$ máme 3 možnosti a pro výběr hodnoty $\alpha((1,2,3))$ 2 možnosti. Skutečně tedy existuje nejvýše 6 automorfismů grupy $\mathbb{S}_3$.

Pro zdůvodnění $|\mathrm{Aut}(\mathbb{S}_3)| \leq 6$ lze místo generátorů vzít trojici transpozic, která v každém automorfismu musí být nějak zpermutována a tudíž je automorfismů nejvýše tolik, kolik je permutací této tříprvkové množiny.

Seminář: Dokažte $\mathrm{Aut}(\mathbb{S}_n) = \mathrm{Inn}(\mathbb{S}_n)$ pro všechna $n \neq 6$.

8. kolo — řešení

a) (i) Stačí sestrojit vnoření $\theta : \mathrm{Aut}(G) \times \mathrm{Aut}(H) \to \mathrm{Aut}(G \times H)$. Je tedy třeba libovolné dvojici $(\sigma, \rho) \in \mathrm{Aut}(G) \times \mathrm{Aut}(H)$ přiřadit automorfismus $\theta((\sigma, \rho))$ grupy $G \times H$. Na libovolný prvek $(g, h) \in G \times H$ necháme dvojici automorfismů působit po složkách, tedy $\theta((\sigma, \rho))((g, h)) = (\sigma(g), \rho(h))$. Pro stručnost označme $\alpha = \theta((\sigma, \rho))$. Snadno se ukáže, že α je homomorfismus grup: pro libovolné $(g_1, h_1), (g_2, h_2) \in G \times H$ je $g_1, g_2 \in G$, $h_1, h_2 \in H$, a tedy

$$\begin{aligned}\alpha((g_1, h_1) \cdot (g_2, h_2)) &= \alpha((g_1 \cdot g_2, h_1 \cdot h_2)) = (\sigma(g_1 \cdot g_2), \rho(h_1 \cdot h_2)) = \\ &= (\sigma(g_1) \cdot \sigma(g_2), \rho(h_1) \cdot \rho(h_2)) = (\sigma(g_1), \rho(h_1)) \cdot (\sigma(g_2), \rho(h_2)) = \\ &= \alpha((g_1, h_1)) \cdot \alpha((g_2, h_2)).\end{aligned}$$

Tuto konstrukci lze snadněji popsat komutativním diagramem: $\alpha = \theta((\sigma, \rho))$ je jediný homomorfismus, pro který komutuje následující diagram

$$\begin{array}{ccccc} G & \xleftarrow{\pi_1} & G \times H & \xrightarrow{\pi_2} & H \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \rho} \\ G & \xleftarrow{\pi_1} & G \times H & \xrightarrow{\pi_2} & H \end{array}$$

Odtud je také ihned vidět, že $\theta((\mathrm{id}_G, \mathrm{id}_H)) = \mathrm{id}_{G \times H}$ a že pro libovolné dvojice automorfismů $(\sigma_1, \rho_1), (\sigma_2, \rho_2) \in \mathrm{Aut}(G) \times \mathrm{Aut}(H)$ platí $\theta((\sigma_2, \rho_2)) \circ \theta((\sigma_1, \rho_1)) = \theta((\sigma_2 \circ \sigma_1, \rho_2 \circ \rho_1))$:

$$\begin{array}{ccccc} G & \xleftarrow{\pi_1} & G \times H & \xrightarrow{\pi_2} & H \\ \downarrow{\scriptstyle \sigma_1} & & \downarrow{\scriptstyle \theta((\sigma_1,\rho_1))} & & \downarrow{\scriptstyle \rho_1} \\ G & \xleftarrow{\pi_1} & G \times H & \xrightarrow{\pi_2} & H \\ \downarrow{\scriptstyle \sigma_2} & & \downarrow{\scriptstyle \theta((\sigma_2,\rho_2))} & & \downarrow{\scriptstyle \rho_2} \\ G & \xleftarrow{\pi_1} & G \times H & \xrightarrow{\pi_2} & H \end{array}$$

(with $\sigma_2 \circ \sigma_1$ connecting the left G's and $\rho_2 \circ \rho_1$ connecting the right H's)

Odtud plyne, že $\theta((\sigma^{-1}, \rho^{-1}))$ je inverzní zobrazení k $\theta((\sigma, \rho))$, a tedy $\theta((\sigma, \rho))$ je bijekce, proto $\theta((\sigma, \rho)) \in \mathrm{Aut}(G \times H)$. Rovnost

$$\theta((\sigma_2, \rho_2)) \circ \theta((\sigma_1, \rho_1)) = \theta((\sigma_2 \circ \sigma_1, \rho_2 \circ \rho_1)) = \theta((\sigma_2, \rho_2) \circ (\sigma_1, \rho_1))$$

znamená, že $\theta : \mathrm{Aut}(G) \times \mathrm{Aut}(H) \to \mathrm{Aut}(G \times H)$ je homomorfismus grup. Jestliže $\theta((\sigma, \rho)) = \mathrm{id}_{G \times H}$, pak pro každé $(g, h) \in G \times H$ platí $(\sigma(g), \rho(h)) = (g, h)$, a tedy $\sigma(g) = g$ a $\rho(h) = h$, je tedy $\sigma = \mathrm{id}_G$, $\rho = \mathrm{id}_H$. Dokázali jsme, že jádro $\ker \theta = \{(\mathrm{id}_G, \mathrm{id}_H)\}$ je jednoprvkové, a proto je θ vnoření.

(ii) Protože každý automorfismus dvojprvkové grupy $(\mathbb{Z}_2, +)$ musí zobrazit neutrální prvek $[0]_2$ opět na $[0]_2$, jediným automorfismem této grupy je identita, tedy $\mathrm{Aut}(\mathbb{Z}_2) = \{\mathrm{id}_{\mathbb{Z}_2}\}$. Odtud plyne, že součin $\mathrm{Aut}(\mathbb{Z}_2) \times \mathrm{Aut}(\mathbb{Z}_2)$ je také jednoprvkový. Ovšem grupa $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ obsahuje i neidentický automorfismus, například záměnu první a druhé složky, tj. $(u, v) \mapsto (v, u)$. (Pro úplnost dodejme, že $\mathbb{Z}_2 \times \mathbb{Z}_2$ je dvourozměrný vektorový prostor nad tělesem $\mathbb{Z}_2$, a tedy metodami lineární algebry snadno dostaneme, že $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathrm{GL}_2(\mathbb{Z}_2) \cong \mathbb{S}_3$.)

(iii) Zobrazení $i_1 : G \to G \times H$ a $i_2 : H \to G \times H$ definovaná pro libovolná $g \in G$, $h \in H$ předpisem $i_1(g) = (g, 1_H)$, $i_2(h) = (1_G, h)$, kde 1_G a 1_H značí neutrální prvky příslušných grup, jsou jistě vnoření. Pro libovolné $\alpha \in \mathrm{Aut}(G \times H)$ máme komutativní diagram

$$\begin{array}{ccccc} G & \xrightarrow{i_1} & G \times H & \xleftarrow{i_2} & H \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \rho} \\ G & \xleftarrow{\pi_1} & G \times H & \xrightarrow{\pi_2} & H \end{array}$$

kde $\sigma = \pi_1 \circ \alpha \circ i_1$ a $\rho = \pi_2 \circ \alpha \circ i_2$. Protože $\pi_2 \circ \alpha \circ i_1$ je homomorfismus grup, pro libovolné $g \in G$ je řád prvku $\pi_2(\alpha(i_1(g)))$ dělitelem řádu prvku g, tedy i řádu $|G|$ grupy G. Současně je to prvek grupy H, a tedy jeho řád je dělitelem řádu $|H|$ grupy H. Z předpokladu $(|G|, |H|) = 1$ plyne, že tímto řádem musí být 1, tedy $\pi_2(\alpha(i_1(g))) = 1_H$. Analogicky $\pi_1(\alpha(i_2(h))) = 1_G$ pro každé $h \in H$.

Z definice je $\ker \sigma$ množina všech prvků grupy G, které splní $\sigma(g) = 1_G$. Protože $\sigma = \pi_1 \circ \alpha \circ i_1$ a $\pi_2(\alpha(i_1(g))) = 1_H$, z $\sigma(g) = 1_G$ plyne $\alpha(i_1(g)) = (1_G, 1_H)$. Ovšem α je automorfismus, a tedy dostáváme $i_1(g) = (1_G, 1_H)$, tj. $g = 1_G$. Proto $\ker \sigma = \{1_G\}$ a σ je vnoření $G \to G$. Protože G je konečná grupa, je $\sigma \in \mathrm{Aut}(G)$. Analogicky $\rho \in \mathrm{Aut}(H)$.

Pro libovolná $g \in G$, $h \in H$ platí $(g, h) = (g, 1) \cdot (1, h) = i_1(g) \cdot i_2(h)$. Proto $\alpha((g, h)) = \alpha(i_1(g) \cdot i_2(h)) = (\alpha \circ i_1)(g) \cdot (\alpha \circ i_2)(h)$. Přitom $(\alpha \circ i_1)(g) = (\pi_1((\alpha \circ i_1)(g)), \pi_2((\alpha \circ i_1)(g))) = (\sigma(g), 1_H)$, protože $\pi_1 \circ \alpha \circ i_1 = \sigma$ a $(\pi_2 \circ \alpha \circ i_1)(g) = 1_H$. Podobně $(\alpha \circ i_2)(h) = (1_G, \rho(h))$, dohromady $\alpha((g, h)) = (\sigma(g), 1_H) \cdot (1_G, \rho(h)) = (\sigma(g), \rho(h))$. To znamená, že $\alpha = \theta((\sigma, \rho))$, a tedy θ je surjektivní. Dokázali jsme, že $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

b) (i) Protože H je podgrupa grupy G, pro každé $g, h \in H$ platí $g \cdot h \cdot g^{-1} \in H$, a tedy $g \cdot H \cdot g^{-1} \subseteq H$. Rovněž $g^{-1} \cdot h \cdot g \in H$, a proto $h \in g \cdot H \cdot g^{-1}$, tedy $H \subseteq g \cdot H \cdot g^{-1}$. To znamená $g \cdot H \cdot g^{-1} = H$, tedy $H \subseteq N_G(H)$.

(ii) Jestliže $N_G(H) = G$, pak pro každé $g \in G$ platí $g \cdot H \cdot g^{-1} = H$, a proto pro každé $h \in H$ je $g \cdot h \cdot g^{-1} \in H$, což znamená, že podgrupa H grupy G je normální.

Je-li naopak H normální podgrupa grupy G, pak pro každé $g \in G$ je $g \cdot H \cdot g^{-1} \subseteq H$. To musí ovšem platit i pro $g^{-1} \in G$, tedy rovněž $g^{-1} \cdot H \cdot g \subseteq H$, tedy $H \subseteq g \cdot H \cdot g^{-1}$, dohromady $H = g \cdot H \cdot g^{-1}$, odkud $g \in N_G(H)$, tedy $G \subseteq N_G(H)$. Opačná inkluze platí z definice.

(iii) Zvolme $G = \mathbb{S}_3$, $A = \{(1,2), (1,3)\}$. Pak platí $(1,2) \circ (1,2) \circ (1,2)^{-1} = (1,2)$ a $(1,2) \circ (1,3) \circ (1,2)^{-1} = (2,3)$, a tedy $(1,2) \circ A \circ (1,2)^{-1} = \{(1,2), (2,3)\} \neq A$. Proto $(1,2) \notin N_G(A)$.

c) Pro libovolné $g \in N_G(H)$ definujme zobrazení $\varphi_g : H \to H$ předpisem $\varphi_g(h) = g \cdot h \cdot g^{-1}$, což je skutečně prvek podgrupy H díky předpokladu $g \in N_G(H)$. Protože pro každé $h_1, h_2 \in H$ platí $\varphi_g(h_1) \cdot \varphi_g(h_2) = g \cdot h_1 \cdot g^{-1} \cdot g \cdot h_2 \cdot g^{-1} = g \cdot h_1 \cdot h_2 \cdot g^{-1} = \varphi_g(h_1 \cdot h_2)$, je φ_g homomorfismus grup. Přitom pro libovolné $g_1, g_2 \in G$ a libovolné $h \in H$ platí $\varphi_{g_1 \cdot g_2}(h) = g_1 \cdot g_2 \cdot h \cdot (g_1 \cdot g_2)^{-1} = g_1 \cdot g_2 \cdot h \cdot g_2^{-1} \cdot g_1^{-1} = \varphi_{g_1}(\varphi_{g_2}(h))$, a tedy $\varphi_{g_1 \cdot g_2} = \varphi_{g_1} \circ \varphi_{g_2}$. Odtud plyne jednak to, že $\varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}_H = \varphi_{g^{-1}} \circ \varphi_g$, a proto φ_g je bijekce, tedy $\varphi_g \in \mathrm{Aut}(H)$, jednak to, že předpis $\varphi(g) = \varphi_g$ zadává homomorfismus grup $\varphi : N_G(H) \to \mathrm{Aut}(H)$.

Jádro $\ker \varphi$ je množina všech těch $g \in N_G(H)$, které splňují $\varphi(g) = \mathrm{id}_H$, tj. takových $g \in N_G(H)$, že pro každé $h \in H$ platí $\varphi_g(h) = h$, což znamená $g \cdot h \cdot g^{-1} = h$. Takové g je podle definice prvkem $C_G(H)$. Na druhou stranu každý prvek $C_G(H)$ je prvkem $N_G(H)$, a tedy $\ker \varphi = C_G(H)$. Proto je centralizér $C_G(H)$ normální podgrupa normalizéru $N_G(H)$ a podle důsledku hlavní věty o faktorových grupách je $N_G(H)/C_G(H) \cong \varphi(N_G(H))$, což je podgrupa grupy $\mathrm{Aut}(H)$.

9. kolo — řešení

a) (i) Každá sudá permutace je složením sudého počtu transpozic, stačí tedy ukázat, že podgrupa $\mathbb{A}_n$ generovaná všemi cykly délky 3 obsahuje všechna složení dvou transpozic. Pokud prvky $a, b, c \in \{1, \ldots, n\}$ jsou po dvou různé, pak platí $(a,b) \circ (b,c) = (a,b,c)$, takže $(a,b) \circ (b,c)$ patří do této podgrupy. Analogicky pokud prvky $a, b, c, d \in \{1, \ldots, n\}$ jsou po dvou různé, pak platí $(a,b) \circ (c,d) = (a,c,d) \circ (a,b,d)$, takže $(a,b) \circ (c,d)$ rovněž patří do této podgrupy.

(ii) Zřejmě $\{\mathrm{id}\}$ je jedna třída konjugace. Uvažme libovolný cyklus (a,b,c) délky 3 v $\mathbb{A}_5$. Snadno se uvidí, že existuje $\tau \in \mathbb{A}_5$ takové, že $\tau(1) = a$, $\tau(2) = b$, $\tau(3) = c$, z textu v komentáři potom plyne, že všechny cykly délky 3 tvoří jednu třídu konjugace v $\mathbb{A}_5$. Dále pro libovolnou permutaci $(a,b) \circ (c,d) \in \mathbb{A}_5$, která je složením dvou nezávislých transpozic, existují permutace $\tau, \tau' \in \mathbb{S}_5$

takové, že $\tau(1)=a$, $\tau(2)=b$, $\tau(3)=c$, $\tau(4)=d$ a $\tau'(1)=a$, $\tau'(2)=b$, $\tau'(3)=d$, $\tau'(4)=c$. Tyto dvě permutace mají opačná znaménka, takže jedna z nich je sudá, proto všechny permutace, které jsou složením dvou nezávislých transpozic, tvoří jednu třídu konjugace v $\mathbb{A}_5$. Dále třída konjugace prvku $(1,2,3,4,5)$ obsahuje všechny permutace tvaru $(\tau(1),\tau(2),\tau(3),\tau(4),\tau(5))$, kde $\tau\in\mathbb{A}_5$. Zřejmě pokud τ nahradíme permutací $\tau\circ(1,2,3,4,5)^k$, $k\in\mathbb{Z}$, pak se výsledek nezmění, můžeme se tedy například omezit pouze na ta τ, pro které $\tau(1)=1$. Naopak pro různá taková τ dostaneme různé výsledky, takže tato třída konjugace obsahuje $4!/2=12$ cyklů délky 5. Analogicky se ukáže, že třída konjugace prvku $(1,2,3,5,4)$ obsahuje zbylých 12 cyklů délky 5. Celkem tedy třídy konjugace v $\mathbb{A}_5$ jsou $\{\mathrm{id}\}$, $\{(1,2,3),(1,2,4),(1,2,5),(1,3,4),(1,3,5),(1,4,5),(2,3,4),(2,3,5),(2,4,5),(3,4,5),(3,2,1),(4,2,1),(5,2,1),(4,3,1),(5,3,1),(5,4,1),(4,3,2),(5,3,2),(5,4,2),(5,4,3)\}$, $\{(1,2)\circ(3,4),(1,3)\circ(2,4),(1,4)\circ(2,3),(1,2)\circ(3,5),(1,3)\circ(2,5),(1,5)\circ(2,3),(1,2)\circ(4,5),(1,4)\circ(2,5),(1,5)\circ(2,4),(1,3)\circ(4,5),(1,4)\circ(3,5),(1,5)\circ(3,4),(2,3)\circ(4,5),(2,4)\circ(3,5),(2,5)\circ(3,4)\}$, $\{(1,2,3,4,5),(1,3,4,2,5),(1,3,5,4,2),(1,4,3,5,2),(1,2,4,5,3),(1,4,2,3,5),(1,5,2,4,3),(1,5,3,2,4),(1,2,5,3,4),(1,3,2,5,4),(1,4,5,2,3),(1,5,4,3,2)\}$, $\{(1,2,3,5,4),(1,3,4,5,2),(1,3,5,2,4),(1,4,3,2,5),(1,2,4,3,5),(1,4,2,5,3),(1,5,2,3,4),(1,5,3,4,2),(1,2,5,4,3),(1,3,2,4,5),(1,4,5,3,2),(1,5,4,2,3)\}$.

Pozn.: To, jak vypadají třídy konjugace v $\mathbb{A}_n$, lze popsat pro libovolné $n\in\mathbb{N}$. Pro libovolné permutace $\sigma,\sigma'\in\mathbb{S}_n$ stejného typu je množina všech $\tau\in\mathbb{S}_n$ takových, že $\sigma'=\tau\sigma\tau^{-1}$, rovna nějaké levé třídě rozkladu $\mathbb{S}_n$ podle centralizeru $C_{\mathbb{S}_n}(\sigma)$. Odtud se snadno nahlédne, že pro $\sigma\in\mathbb{A}_n$ platí, že pokud $C_{\mathbb{S}_n}(\sigma)$ obsahuje nějakou lichou permutaci, potom všechny permutace stejného typu jako σ tvoří jednu třídu konjugace v $\mathbb{A}_n$, v opačném případě permutace tohoto typu tvoří dvě (stejně velké) třídy konjugace. Nechť σ obsahuje k_i cyklů délky i pro každé $i\in\{1,\dots,n\}$ v rozkladu na nezávislé cykly, přičemž tyto cykly označme $c_{i,j}$, $1\le i\le n$, $1\le j\le k_i$, kde $c_{i,j}=(a_{i,j,1},\dots,a_{i,j,i})$. Potom lze ukázat, že

$$C_{\mathbb{S}_n}(\sigma)\cong\prod_{i=1}^{n}\left(\mathbb{Z}_i^{k_i}\rtimes_{\varphi_i}\mathbb{S}_{k_i}\right),$$

kde homomorfismy $\varphi_i\colon\mathbb{S}_{k_i}\to\mathrm{Aut}\left(\mathbb{Z}_i^{k_i}\right)$ jsou dány vztahy

$$\varphi_i(\theta)(([t_1]_i,\dots,[t_{k_i}]_i))=([t_{\theta^{-1}(1)}]_i,\dots,[t_{\theta^{-1}(k_i)}]_i),$$

přičemž izomorfismus $f\colon\prod_{i=1}^{n}\left(\mathbb{Z}_i^{k_i}\rtimes_{\varphi_i}\mathbb{S}_{k_i}\right)\to C_{\mathbb{S}_n}(\sigma)$ je dán vztahem

$$\begin{aligned}f((([t_{1,1}]_1,\dots,[t_{1,k_1}]_1),\theta_1),\dots,(([t_{n,1}]_n,\dots,[t_{n,k_n}]_n),\theta_n))=\\=c_{1,1}^{t_{1,1}}\circ\ldots\circ c_{1,k_1}^{t_{1,k_1}}\circ\tau_{1,\theta_1}\circ\ldots\circ c_{n,1}^{t_{n,1}}\circ\ldots\circ c_{n,k_n}^{t_{n,k_n}}\circ\tau_{n,\theta_n},\end{aligned}$$

kde $\tau_{i,\theta}\in\mathbb{S}_n$ je dáno vztahy $\tau_{i,\theta}(a_{i,j,k})=a_{i,\theta(j),k}$ a $\tau_{i,\theta}(a_{i',j,k})=a_{i',j,k}$ pro $i'\neq i$. Odtud se snadno nahlédne (neboť $\mathrm{sgn}(c_{i,j})=(-1)^{i-1}$ a $\mathrm{sgn}(\tau_{i,\theta})=\mathrm{sgn}(\theta)^i$), že pokud σ obsahuje v rozkladu na nezávislé cykly buď cyklus sudé délky nebo dva stejně dlouhé cykly liché délky, pak $C_{\mathbb{S}_n}(\sigma)$ obsahuje nějakou lichou permutaci, v opačném případě $C_{\mathbb{S}_n}(\sigma)$ obsahuje pouze sudé permutace.

b) (i) Nechť $H\le\mathbb{A}_5$ je normální podgrupa grupy $\mathbb{A}_5$. Z části a)(ii) víme, že třídy konjugace grupy $\mathbb{A}_5$ mají velikosti $1,20,15,12,12$. Jelikož H je normální podgrupa $\mathbb{A}_5$, musí být sjednocením některých z těchto tříd, přičemž musí určitě obsahovat třídu $\{\mathrm{id}\}$. Snadno se ověří, že takové sjednocení bude mít počet prvků dělící $|\mathbb{A}_5|=5!/2=60$ pouze pokud buď vezmeme pouze třídu $\{\mathrm{id}\}$ nebo když vezmeme všechny třídy, a tak z Lagrangeovy věty plyne, že $H=\{\mathrm{id}\}$ nebo $H=\mathbb{A}_5$, a tudíž $\mathbb{A}_5$ je jednoduchá grupa.

(ii) Grupa H_n je zřejmě izomorfní $\mathbb{A}_{n-1}$ a grupy $H_1, \ldots, H_n$ jsou navzájem izomorfní, neboť pro každé $\sigma \in \mathbb{A}_n$ vnitřní automorfismus ρ_σ zobrazuje H_i na $H_{\sigma(i)}$. Dále ukážeme, že $H \cap H_i$ je normální podgrupa H_i. Nechť $\sigma \in H \cap H_i$ a $\tau \in H_i$. Zřejmě $\tau\sigma\tau^{-1} \in H_i$, a jelikož je H normální podgrupa $\mathbb{A}_n$, tak $\tau\sigma\tau^{-1} \in H$. Celkem tedy $\tau\sigma\tau^{-1} \in H \cap H_i$, a tedy $H \cap H_i$ je normální podgrupa H_i.

(iii) Vezměme si libovolné $\sigma \in H$, $\sigma \neq \mathrm{id}$.

Pokud σ obsahuje v rozkladu na nezávislé cykly cyklus délky aspoň 3, pak ho můžeme napsat jako $\sigma = (a_1, a_2, a_3, \ldots) \circ \theta$, kde cyklus $(a_1, a_2, a_3, \ldots)$ je disjunktní s permutací θ. Označme $\tau = (a_3, a_4, a_5) \in \mathbb{A}_n$, kde a_4, a_5 jsou libovolné navzájem různé prvky různé od a_1, a_2, a_3 (takové prvky existují, neboť $n \geq 6$). Potom $\sigma' = \tau \circ \sigma \circ \tau^{-1} \in H$. Platí $\sigma'(a_1) = \tau(\sigma(\tau^{-1}(a_1))) = \tau(\sigma(a_1)) = \tau(a_2) = a_2 = \sigma(a_1)$ a $\sigma'(a_2) = \tau(\sigma(\tau^{-1}(a_2))) = \tau(\sigma(a_2)) = \tau(a_3) = a_4 \neq \sigma(a_2)$, takže $\sigma'^{-1}\sigma \in H_{a_1} \cap H$, $\sigma'^{-1}\sigma \neq \mathrm{id}$.

Pokud σ obsahuje v rozkladu na nezávislé cykly pouze cykly délky nejvýše 2, pak musí obsahovat aspoň dva cykly délky 2, takže ho můžeme napsat jako $\sigma = (a_1, a_2) \circ (a_3, a_4) \circ \theta$, kde prvky a_1, a_2, a_3, a_4 jsou navzájem různé a permutace $(a_1, a_2) \circ (a_3, a_4)$ je disjunktní s permutací θ. Označme $\tau = (a_4, a_5, a_6) \in \mathbb{A}_n$, kde a_5, a_6 jsou libovolné navzájem různé prvky různé od a_1, a_2, a_3, a_4 (opět využíváme toho, že $n \geq 6$). Potom opět $\sigma' = \tau \circ \sigma \circ \tau^{-1} \in H$. Platí $\sigma'(a_1) = \tau(\sigma(\tau^{-1}(a_1))) = \tau(\sigma(a_1)) = \tau(a_2) = a_2 = \sigma(a_1)$ a $\sigma'(a_3) = \tau(\sigma(\tau^{-1}(a_3))) = \tau(\sigma(a_3)) = \tau(a_4) = a_5 \neq \sigma(a_3)$, takže $\sigma'^{-1}\sigma \in H_{a_1} \cap H$, $\sigma'^{-1}\sigma \neq \mathrm{id}$.

Dokázali jsme tedy, že existuje $i \in \{1, \ldots, n\}$ takové, že $H \cap H_i \neq \{\mathrm{id}\}$.

(iv) Vezměme si i z předchozí části. Podle části (ii) a indukčního předpokladu je H_i jednoduchá grupa. Víme, že $H \cap H_i$ je její netriviální normální podgrupa, tudíž $H \cap H_i = H_i$, a tak $H_i \subseteq H$. Jelikož H_i obsahuje cyklus délky 3, a stejně jako v části a)(ii) se ukáže, že všechny cykly délky 3 v $\mathbb{A}_n$ jsou v $\mathbb{A}_n$ konjugované, tak H obsahuje všechny cykly délky 3 v $\mathbb{A}_n$. Z tvrzení části a)(i) potom plyne, že $H = \mathbb{A}_n$.

Pozn.: Ukážeme si ještě jiný důkaz faktu, že grupa $\mathbb{A}_n$ je pro $n \geq 5$ jednoduchá. Nechť tedy $n \geq 5$ a H je netriviální normální podgrupa $\mathbb{A}_n$. Ukážeme, že H obsahuje cyklus délky 3. Opět si vezměme libovolné $\sigma \in H$, $\sigma \neq \mathrm{id}$.

Pokud σ obsahuje v rozkladu na nezávislé cykly cyklus délky aspoň 4, pak ho můžeme napsat jako $\sigma = (a_1, a_2, \ldots, a_r) \circ \theta$, kde $r \geq 4$ a cyklus $(a_1, a_2, \ldots, a_r)$ je disjunktní s permutací θ. Označme $\tau = (a_1, a_2, a_3)$. Potom je $\tau \circ \sigma \circ \tau^{-1} \in H$, a tak $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in H$. Jelikož τ je disjunktní s θ, tak platí $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (a_1, a_2, a_3) \circ (a_1, a_2, \ldots, a_r) \circ \theta \circ (a_3, a_2, a_1) \circ \theta^{-1} \circ (a_r, a_{r-1} \ldots, a_1) = (a_1, a_2, a_3) \circ (a_1, a_2, \ldots, a_r) \circ (a_3, a_2, a_1) \circ (a_r, a_{r-1} \ldots, a_1) \circ \theta \circ \theta^{-1} = (a_1, a_2, a_3) \circ (a_1, a_2, \ldots, a_r) \circ (a_3, a_2, a_1) \circ (a_r, a_{r-1} \ldots, a_1) = (a_1, a_2, a_4)$.

Pokud σ obsahuje v rozkladu na nezávislé cykly aspoň dva cykly délky 3, pak ho můžeme napsat jako $\sigma = (a_1, a_2, a_3) \circ (a_4, a_5, a_6) \circ \theta$, kde prvky $a_1, a_2, a_3, a_4, a_5, a_6$ jsou navzájem různé a permutace $(a_1, a_2, a_3) \circ (a_4, a_5, a_6)$ je disjunktní s permutací θ. Označme $\tau = (a_1, a_2, a_4)$. Opět platí $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in H$, přičemž $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (a_1, a_2, a_4) \circ (a_1, a_2, a_3) \circ (a_4, a_5, a_6) \circ \theta \circ (a_4, a_2, a_1) \circ \theta^{-1} \circ (a_6, a_5, a_4) \circ (a_3, a_2, a_1) = (a_1, a_2, a_4) \circ (a_1, a_2, a_3) \circ (a_4, a_5, a_6) \circ (a_4, a_2, a_1) \circ (a_6, a_5, a_4) \circ (a_3, a_2, a_1) \circ \theta \circ \theta^{-1} = (a_1, a_2, a_4) \circ (a_1, a_2, a_3) \circ (a_4, a_5, a_6) \circ (a_4, a_2, a_1) \circ (a_6, a_5, a_4) \circ (a_3, a_2, a_1) = (a_1, a_2, a_5, a_3, a_4)$. Na tento cyklus potom aplikujeme postup z předchozího odstavce a tím dostaneme cyklus délky 3 patřící do H.

Pokud σ obsahuje v rozkladu na nezávislé cykly jeden cyklus délky 3 a jinak pouze cykly délky 1 a 2, pak ho můžeme napsat jako $\sigma = (a_1, a_2, a_3) \circ \theta$, kde cyklus (a_1, a_2, a_3) je disjunktní s permutací θ a navíc $\theta^2 = \mathrm{id}$. Pak platí $\sigma^2 = ((a_1, a_2, a_3) \circ \theta)^2 = (a_1, a_2, a_3)^2 \circ \theta^2 = (a_1, a_3, a_2) \in H$.

Pokud σ obsahuje v rozkladu na nezávislé cykly pouze cykly délky 1 a 2, pak musí obsahovat aspoň dva cykly délky 2, takže ho můžeme napsat jako $\sigma = (a_1, a_2) \circ (a_3, a_4) \circ \theta$, kde prvky a_1, a_2, a_3, a_4 jsou navzájem různé a permutace $(a_1, a_2) \circ (a_3, a_4)$ je disjunktní s permutací θ.

Označme $\tau = (a_1, a_2, a_3)$. Opět platí $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in H$, přičemž $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (a_1, a_2, a_3) \circ (a_1, a_2) \circ (a_3, a_4) \circ \theta \circ (a_3, a_2, a_1) \circ \theta^{-1} \circ (a_4, a_3) \circ (a_2, a_1) = (a_1, a_2, a_3) \circ (a_1, a_2) \circ (a_3, a_4) \circ (a_3, a_2, a_1) \circ (a_4, a_3) \circ (a_2, a_1) \circ \theta \circ \theta^{-1} = (a_1, a_2, a_3) \circ (a_1, a_2) \circ (a_3, a_4) \circ (a_3, a_2, a_1) \circ (a_4, a_3) \circ (a_2, a_1) = (a_1, a_3) \circ (a_2, a_4)$. Dále označme $\psi = (a_1, a_3, a_5)$, kde a_5 je libovolný prvek různý od a_1, a_2, a_3, a_4 (zde využíváme toho, že $n \geq 5$). Potom platí $\psi \circ (a_1, a_3) \circ (a_2, a_4) \circ \psi^{-1} \circ ((a_1, a_3) \circ (a_2, a_4))^{-1} = (a_1, a_3, a_5) \circ (a_1, a_3) \circ (a_2, a_4) \circ (a_5, a_3, a_1) \circ (a_4, a_2) \circ (a_3, a_1) = (a_1, a_5, a_3) \in H$.

Ukázali jsme tedy, že H obsahuje cyklus délky 3, z čehož stejně jako v části b)(iv) plyne, že $H = \mathbb{A}_n$.

V části b)(iii) i v tomto druhém důkazu jsme několikrát našli permutaci s požadovanými vlastnostmi jako prvek tvaru $\alpha\beta\alpha^{-1}\beta^{-1}$, kde α, β byly nějaké vhodné permutace. Prvky tohoto tvaru hrají obecně v teorii grup důležitou roli, nyní si o nich řekneme něco více.

Mějme grupu G. Pro prvky $x, y \in G$ definujeme *komutátor prvků* x, y jako prvek $xyx^{-1}y^{-1}$ a značíme $[x, y]$. Snadno se nahlédne, že x a y spolu komutují právě tehdy, když $[x, y] = 1$ (což vysvětluje ten název). Potom definujeme *komutátorovou podgrupu grupy* G (anglicky se někdy používá název *derived subgroup*) jako podgrupu grupy G generovanou všemi komutátory prvků grupy G. Značíme ji $[G, G]$ (někdy se taky používá značení G' nebo $G^{(1)}$). Tedy

$$[G, G] = \langle \{[x, y] \colon x, y \in G\} \rangle = \langle \{xyx^{-1}y^{-1} \colon x, y \in G\} \rangle.$$

(Některé zdroje definují komutátor x, y jako $x^{-1}y^{-1}xy$. To sice obecně nemusí být stejný prvek jako $xyx^{-1}y^{-1}$, ale i při této definici bude platit, že x a y spolu komutují právě tehdy, když je jejich komutátor roven 1, a navíc podgrupa $[G, G]$ bude při obou definicích stejná, neboť komutátor x, y v tomto smyslu je roven komutátoru x^{-1}, y^{-1} ve smyslu definovaném výše. Pro tyto účely je tedy jedno, kterou z definic používáme.)

Značení $[G, G]$ vyvolává (bohužel) dojem, že prvky komutátorové podgrupy grupy G jsou právě všechny komutátory v G. Ukazuje se ale, že tomu tak obecně není, neboť součin dvou komutátorů nemusí být komutátorem. Nicméně platí to pro konečné grupy malých řádů, nejmenší konečná grupa, ve které to neplatí, má 96 prvků (přesněji existují dvě takové navzájem neizomorfní grupy řádu 96).

Není těžké ověřit, že $[G, G]$ je normální podgrupa G a že má následující vlastnost: pro každou normální podgrupu H grupy G platí, že grupa G/H je komutativní právě tehdy, když $[G, G] \subseteq H$. Grupa $[G, G]$ je tedy nejmenší normální podgrupa grupy G taková, že příslušná faktorgrupa je komutativní. Zejména tedy $[G, G] = \{1\}$ právě tehdy, když je G komutativní (což je vidět rovnou z definice). Grupa $G/[G, G]$ se potom nazývá *abelizace grupy* G a značí se G^{ab}.

Ukažme si pár příkladů. Pro $n \in \{1, 2, 3\}$ je $\mathbb{A}_n$ komutativní, takže její komutátorová podgrupa je triviální a $\mathbb{A}_n^{\mathrm{ab}} \cong \mathbb{A}_n$. Pro $n = 4$ není těžké přímo spočítat, že $[\mathbb{A}_4, \mathbb{A}_4] = V_4$, kde $V_4 = \{\mathrm{id}, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$, a tak $\mathbb{A}_4^{\mathrm{ab}} = \mathbb{A}_4/V_4 \cong \mathbb{Z}_3$. Pro $n \geq 5$ je $\mathbb{A}_n$ jednoduchá grupa, takže její jediné normální podgrupy jsou $\{\mathrm{id}\}$ a $\mathbb{A}_n$. Jelikož není komutativní, tak $[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n$ (grupa G taková, že $[G, G] = G$ se nazývá *perfektní grupa*) a $\mathbb{A}_n^{\mathrm{ab}} \cong \{1\}$. Pro symetrické grupy $\mathbb{S}_n$, kde $n \in \{1, 2, 3, 4\}$ se snadno spočítá, že $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$. Pro $n \geq 5$ není těžké dokázat (s využitím toho, že $\mathbb{A}_n$ je jednoduchá), že jediné normální podgrupy $\mathbb{S}_n$ jsou $\{\mathrm{id}\}$, $\mathbb{A}_n$ a $\mathbb{S}_n$, z čehož snadno plyne, že opět $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$. Pro všechna $n \in \mathbb{N}$ tedy platí $\mathbb{S}_n^{\mathrm{ab}} = \mathbb{S}_n/\mathbb{A}_n$, a tedy $\mathbb{S}_1^{\mathrm{ab}} \cong \{1\}$ a $\mathbb{S}_n^{\mathrm{ab}} \cong \mathbb{Z}_2$ pro $n \geq 2$. S trochou úsilí lze navíc dokázat, že pro všechny grupy $\mathbb{S}_n$ a $\mathbb{A}_n$ platí, že každý prvek jejich komutátorových podgrup je přímo komutátor.

Komutátorové podgrupy se rovněž používají k definici tzv. řešitelných grup. Mějme grupu G. Potom můžeme sestrojit posloupnost grup $G^{(0)}, G^{(1)}, G^{(2)}, \ldots$ rekurentně tak, že $G^{(0)} = G$ a $G^{(k+1)} = [G^{(k)}, G^{(k)}]$ (což vysvětluje, proč se $[G, G]$ někdy značí jako $G^{(1)}$). Potom řekneme, že G je *řešitelná grupa*, pokud existuje $k \in \mathbb{N}_0$ takové, že $G^{(k)}$ je triviální grupa.

Opět si ukážeme několik příkladů. Pro každou komutativní grupu G platí $G^{(1)} = \{1\}$, a tak je každá komutativní grupa řešitelná. Grupy $\mathbb{A}_1$ a $\mathbb{A}_2$ jsou triviální, takže $\mathbb{A}_1^{(0)} = \{\mathrm{id}\}, \mathbb{A}_2^{(0)} = \{\mathrm{id}\}$.

Grupa $\mathbb{A}_3$ je komutativní, takže $\mathbb{A}_3^{(1)} = \{\mathrm{id}\}$. Pro $n = 4$ platí $\mathbb{A}_4^{(1)} = V_4$ a $\mathbb{A}_4^{(2)} = [V_4, V_4] = \{\mathrm{id}\}$ (neboť V_4 je komutativní). Tudíž pro $n \leq 4$ je $\mathbb{A}_n$ je řešitelná grupa. Pro $n \geq 5$ platí $\mathbb{A}_n^{(k)} = \mathbb{A}_n$ pro všechna $k \in \mathbb{N}_0$, takže $\mathbb{A}_n$ není řešitelná. Dále $\mathbb{S}_1^{(0)} = \{\mathrm{id}\}$, $\mathbb{S}_2^{(1)} = \mathbb{A}_2 = \{\mathrm{id}\}$, $\mathbb{S}_3^{(1)} = \mathbb{A}_3$, $\mathbb{S}_3^{(2)} = \{\mathrm{id}\}$, $\mathbb{S}_4^{(1)} = \mathbb{A}_4$, $\mathbb{S}_4^{(2)} = V_4$, $\mathbb{S}_4^{(3)} = \{\mathrm{id}\}$. Tudíž pro $n \leq 4$ je $\mathbb{S}_n$ řešitelná grupa. Pro $n \geq 5$ je $\mathbb{S}_n^{(k)} = \mathbb{A}_n$ pro všechna $k \in \mathbb{N}$, takže $\mathbb{S}_n$ není řešitelná grupa.

Řešitelné grupy se využívají např. v tzv. Galoisově teorii, například to, že pro $n \geq 5$ grupa $\mathbb{S}_n$ není řešitelná úzce souvisí s tím, proč pro polynomy nad $\mathbb{C}$ stupně většího nebo rovno než 5 nelze obecně vyjádřit jeho kořeny z jeho koeficientů použitím aritmetických operací a odmocnin (obecněji platí, že to jde právě tehdy, když je tzv. Galoisova grupa tohoto polynomu řešitelná, odtud taky pochází ten název).

10. kolo — řešení

a) (i) Nechť grupa G splňuje prezentaci $(*)$ a $a, b \in G$ jsou její prvky vyhovující požadovaným rovnostem. Stačí dokázat, že podgrupa G generovaná prvky a, b je dána vztahem

$$\langle\{a, b\}\rangle = \{b^i \cdot a^j \mid i \in \{0, \ldots, \ell - 1\}, j \in \{0, \ldots, k - 1\}\},$$

protože z předpokladu $\langle\{a, b\}\rangle = G$ pak dostaneme požadované tvrzení ohledně řádu grupy G. Označme tedy $X = \{b^i \cdot a^j \mid i \in \{0, \ldots, \ell-1\}, j \in \{0, \ldots, k-1\}\}$ podmnožinu grupy G a dokažme, že 1) X obsahuje prvky a, b, 2) X je podgrupa grupy G a 3) X je nejmenší podgrupa grupy G obsahující prvky a, b.

Nejdříve poznamenejme, že ze vztahu $a^k = 1$ plyne, že pro libovolné $p \in \mathbb{Z}$ je prvek a^p roven a^d, kde $d \in \{0, \ldots, k - 1\}$ je zbytek po dělení čísla p číslem k. Podobně lze psát libovolnou mocninu prvku b jako b^d, kde $d \in \{0, \ldots, \ell - 1\}$. Zejména tedy platí rovnost $X = \{b^i \cdot a^j \mid i, j \in \mathbb{Z}\}$. Přistupme nyní k důkazu jednotlivých tvrzení 1-3).

1) Snadno vidíme, že $a = b^0 \cdot a^1 \in X$ a $b = b^1 \cdot a^0 \in X$.

2) Zřejmě $1 = b^0 \cdot a^0 \in X$. Abychom ukázali, že X je uzavřená vzhledem k násobení, ukážeme nejdříve, pro libovolné $p \in \mathbb{N}_0$ platí $a \cdot b^p \in X$. Skutečně, indukcí lze dokázat rovnost $a \cdot b^p = b^{rp} \cdot a$: pro $p = 0$ je rovnost zřejmá a pokud předpokládáme platnost tohoto vztahu pro p, pak pro $p + 1$ dostaneme

$$a \cdot b^{p+1} = a \cdot b^p \cdot b = b^{rp} \cdot a \cdot b = b^{rp} \cdot b^r \cdot a = b^{r(p+1)} \cdot a\,.$$

Ukážeme dále, že pro libovolná $j, p \in \mathbb{N}_0$ platí

$$a^j \cdot b^p = b^{r^j \cdot p} \cdot a^j\,. \qquad (\dagger)$$

Platnost rovnosti $(\dagger)$ dokazujeme indukcí vzhledem k j: pro $j = 0$ rovnost $(\dagger)$ zřejmě platí a pokud předpokládáme platnost tohoto vztahu pro j, pak pro $j + 1$ dostaneme

$$a^{j+1} \cdot b^p = a \cdot a^j \cdot b^p = a \cdot b^{r^j \cdot p} \cdot a^j = b^{r \cdot r^j \cdot p} \cdot a \cdot a^j = b^{r^{j+1} \cdot p} \cdot a^{j+1}\,.$$

Použitím rovnosti $(\dagger)$ dostáváme, že pro libovolná přirozená čísla $i, j, p, q \in \mathbb{N}_0$ platí

$$(b^i \cdot a^j) \cdot (b^p \cdot a^q) = b^i \cdot b^{r^j \cdot p} \cdot a^j \cdot a^p = b^{i + r^j \cdot p} \cdot a^{j+p}$$

a dokázali jsme, že X je uzavřená na násobení. Zbývá ukázat, že pro libovolný prvek $b^i \cdot a^j \in X$, kde $i \in \{0, \ldots, \ell - 1\}, j \in \{0, \ldots, k - 1\}$, platí $(b^i \cdot a^j)^{-1} \in X$. To plyne z následujících rovností: $(b^i \cdot a^j)^{-1} = a^{-j} \cdot b^{-i} = a^{k-j} \cdot b^{\ell-i}$, kde poslední prvek zřejmě náleží do množiny X, protože X je podmnožina uzavřená na násobení. Tím je dokončen důkaz bodu 2).

3) Nechť H je libovolná podgrupa grupy G, která obsahuje prvky a, b. Pak vzhledem k uzavřenosti H na násobení, obsahuje podgrupa H i prvky tvaru $b^j \cdot a^i$, kde $i, j \in \mathbb{N}$. Zejména tedy $X \subseteq H$ a důkaz bodu 3), a tím i části i), je dokončen.

(ii) Vzhledem k předchozí části znamená předpoklad $|G| = k \cdot \ell$, že jsou prvky $b^i \cdot a^j$, kde $i \in \{0, \ldots, \ell - 1\}, j \in \{0, \ldots, k - 1\}$, po dvou různé. Zejména je prvek b řádu ℓ. Prvek $b^1 \cdot a^0 = b = a^k \cdot b$ vyjádříme pomocí odvozeného vztahu pro násobení (†) jako $a^k \cdot b = b^{r^k} \cdot a^k = b^{r^k} = b^d$, kde d je zbytek po dělení čísla r^k číslem ℓ. Tudíž $b^{d-1} = 1$ a protože b má řád ℓ, tak dostáváme $\ell \mid d - 1$, tj. $d = 1$. Odtud $r^k \equiv 1 (\mathrm{mod}\ \ell)$.

(iii) Začněme neformálně: pokud budeme libovolný prvek $b^i \cdot a^j \in G$ uvažovat jako příslušnou uspořádanou dvojici exponentů pak vzhledem ke vztahům $a^k = 1$ a $b^\ell = 1$ lze hledanou grupu G reprezentovat jako množinu $\mathbb{Z}_\ell \times \mathbb{Z}_k$, kde prvek $b^i a^j$ bude reprezentován jako $([i]_\ell, [j]_k)$. Podle části i) pro operaci $\cdot$ platí $([i]_\ell, [j]_k) \cdot ([p]_\ell, [q]_k) = ([i + r^j p]_\ell, [j + q]_k)$. Místo toho, abychom dokazovali, že $(\mathbb{Z}_\ell \times \mathbb{Z}_k, \cdot)$ je grupa, popíšeme tuto grupu jako polopřímý součin grup $\mathbb{Z}_\ell$ a $\mathbb{Z}_k$, který známe z příkladu a)-i) z 6. kola soutěže.

Nyní tedy již formálně: nechť $k, \ell, r \in \mathbb{N}$ jsou taková, že platí $r^k \equiv 1 (\mathrm{mod}\ \ell)$. Nejdříve uvažujme grupu $\mathrm{Aut}(\mathbb{Z}_\ell)$. Víme, že každý homomorfismus z grupy $\mathbb{Z}_\ell$ do sebe je dán jako násobení pevně zvoleným prvkem. Přesněji, pro libovolné $x \in \mathbb{Z}_\ell$ je zobrazení $\omega_x : \mathbb{Z}_\ell \to \mathbb{Z}_\ell$, dané předpisem $\omega_x(g) = x \cdot g$, homomorfismus grup. Lze přitom dokázat, že jiné homomorfismy z grupy $\mathbb{Z}_\ell$ do sebe neexistují, protože každý homorfismus z grupy $\mathbb{Z}_\ell$ je jednoznačně dán obrazem prvku $[1]_\ell$. Dále pro libovolné $x, y \in \mathbb{Z}_\ell$ platí $\omega_x \circ \omega_y = \omega_{xy}$, $\omega_{[1]_\ell} = \mathrm{id}$ a ω_x je izomorfismus právě tehdy, když x je invertibilní prvek monoidu $(\mathbb{Z}_\ell, \cdot)$, tj. $x \in \mathbb{Z}_\ell^\times$. Proto je grupa $\mathrm{Aut}(\mathbb{Z}_\ell)$ izomorfní grupě $(\mathbb{Z}_\ell^\times, \cdot)$.

Z předpokladu $r^k \equiv 1 (\mathrm{mod}\ \ell)$ víme, že $(r, \ell) = 1$ a tedy $[r]_\ell \in \mathbb{Z}_\ell^\times$. Pro $x = [r]_\ell$ je proto ω_x automorfismus grupy $(\mathbb{Z}_\ell, +)$. Navíc pro libovolné $m \in \mathbb{N}$ platí $(\omega_x)^m = \omega_{x^m}$. Pro $m = k$ máme $x^k = [r^k]_\ell = [1]_\ell$ a tedy $(\omega_x)^k = \omega_{x^k} = id$. Definujme nyní zobrazení $\varphi : \mathbb{Z}_k \to \mathrm{Aut}(\mathbb{Z}_\ell)$ předpisem $\varphi([h]_k) = (\omega_x)^h$ pro libovolné $h \in \mathbb{Z}$. Toto zobrazení je korektně definováno, protože $(\omega_x)^k = id$. Snadno se také nahlédne, že φ je homomorfismus grup. Podle již zmíněného příkladu a)-i) z 6. kola soutěže tak máme definovánu grupu $(G, \cdot)$, pro niž platí $G = \mathbb{Z}_\ell \times \mathbb{Z}_k$ a operace $\cdot$ je dána vztahem

$$([i]_\ell, [j]_k) \cdot ([p]_\ell, [q]_k) = ([i]_\ell + (\omega_x)^j([p]_\ell), [j]_k + [q]_k) = ([i + r^j p]_\ell, [j + q]_k)\,, \text{ pro } i, j, p, q \in \mathbb{Z}.$$

Pokud nyní zvolíme v G dva prvky $b = ([1]_\ell, [0]_k)$ a $a = ([0]_\ell, [1]_k)$, pak se snadno ověří, že G splňuje prezentaci $(*)$. Skutečně, pro libovolné $m \in \mathbb{Z}$ platí $b^m = ([m]_\ell, [0]_k)$, protože $\mathbb{Z}_\ell \times \{[0]_k\}$ je podgrupa grupy G izomorfní grupě $\mathbb{Z}_\ell$, kde izomorfismem je projekce na první složku. Tedy $b^\ell = ([0]_\ell, [0]_k)$ a podobně $a^k = ([0]_\ell, [0]_k)$, protože podgrupa $\{[0]_\ell\} \times \mathbb{Z}_k$ grupy G je izomorfní s grupou $\mathbb{Z}_k$. Konečně

$$a \cdot b = ([0]_\ell, [1]_k) \cdot ([1]_\ell, [0]_k) = ([0 + r^1 \cdot 1]_\ell, [1]_k) = ([r]_\ell, [0]_k) \cdot ([0]_\ell, [1]_k) = b^r \cdot a\,.$$

Celkem je $G = \mathbb{Z}_\ell \rtimes_\varphi \mathbb{Z}_k$ grupa řádu $k \cdot \ell$, která splňuje prezentaci $(*)$.

Poznamenejme, že v případě $k = 1$ je $\mathbb{Z}_k$ triviální grupa a je zbytečné uvažovat polopřímý součin, protože ten je izomorfní grupě $\mathbb{Z}_\ell$ a lze tedy za grupy G vzít rovnou $\mathbb{Z}_\ell$. Podobně v případě $\ell = 1$. Také je dobré si uvědomit, že v případě $r = 1$ je každá grupa splňující prezentaci $(*)$ komutativní. V tomto případě je $\omega_x = \mathrm{id}$, čímž pádem homomorfismus φ zobrazuje každý prvek $\mathbb{Z}_k$ na $\mathrm{id} \in \mathrm{Aut}(\mathbb{Z}_\ell)$ a tedy polopřímý součin $\mathbb{Z}_\ell \rtimes_\varphi \mathbb{Z}_k$ je přímý součin $\mathbb{Z}_\ell \times \mathbb{Z}_k$.

(iv) Buďte G a H dvě grupy splňující prezentaci $(*)$ a v nich označme příslušné prvky $a, b \in G$ a $a', b' \in H$. Uvažujeme-li přímý součin grup $G \times H$, pak projekce na první a druhou složku $\pi_1 : G \times H \to G$, resp. $\pi_2 : G \times H \to H$, jsou homomorfismy grup. Označme v grupě

$G \times H$ prvky $A = (a, a')$ a $B = (b, b')$. Vzhledem k tomu, že operace násobení je v grupě $G \times H$ definována po složkách, snadno se nahlédne, že

$$A^k = (a^k, (a')^k) = (1_G, 1_H) = 1_{G\times H}\,,$$

a podobně $B^\ell = 1_{G\times H}$ a $A \cdot B = B^r \cdot A$. Označíme-li K podgrupu grupy $G \times H$ generovanou prvky A a B, pak K splňuje prezentaci $(*)$. Navíc $\{a, b\} \subseteq \pi_1(K)$ a tudíž π_1 je surjektivní homomorfismus z K na G. Stejně se ukáže, že i π_2 je surjektivní homomorfismus.

(v) Označme K některou grupu, která má největší řád ze všech grup splňujících prezentaci $(*)$. Její existence plyne z části i). Buď nyní G libovolná grupa splňující $(*)$. Podle části iv) existuje grupa N splňující prezentaci $(*)$ a surjektivní homomorfismy grup $\alpha : N \to K$ a $\beta : N \to G$. Protože K byla největší možná grupa splňující prezentaci $(*)$, platí pro velikosti grup K a N nerovnost $|K| \geq |N|$. Zároveň $|N| \geq |K|$, protože α je surjektivní zobrazení konečných množin. Tudíž $|K| = |N|$ a $\alpha : N \to K$ je bijekce, tj. izomorfismus grup. Proto $\beta \circ \alpha^{-1} : K \to G$ je surjektivní homomorfismus z grupy K na grupu G.

Poznamenejme, že v části ii) jsme ukázali, že vždy $b = b^{r^k}$, tj. $b^{r^k-1} = 1$. Vzhledem k $b^\ell = 1$ tak máme $b^d = 1$ pro největší společný dělitel d čísel $r^k - 1$ a ℓ. Lze dokázat, že jako největší grupu splňující prezentaci $(*)$, jejíž existenci jsme dokázali v části v), a která je určena jednoznačně až na izomorfismus, jak jsme si povšimli v komentáři zadání, lze vzít polopřímý součin grup $\mathbb{Z}_d$ a $\mathbb{Z}_k$. Z popsaného totiž plyne, že každá grupa splňující prezentaci $(*)$ pro trojici k, ℓ, r splňuje prezentaci $(*)$ i pro trojici k, d, r, přitom pro tuto trojici je předpoklad $r^k \equiv 1 (\mathrm{mod}\ d)$ již splněn.

b) (i) Nechť G splňuje prezentaci $(**)$ a $a, b \in G$ jsou příslušné prvky. Uvědomme si, že prvek a je inverzní sám k sobě a totéž platí pro prvek b. Z rovnosti $(ab)^m = 1$ pronásobením prvkem a zleva a prvkem b zprava dostaneme $a \cdot b = a \cdot (a \cdot b)^m \cdot b = (b \cdot a)^{m-1}$.

Stačí dokázat, že podgrupa G generovaná prvky a, b je dána vztahem

$$\langle\{a, b\}\rangle = \{(a \cdot b)^i \cdot a^j \mid i \in \{0, \ldots, m-1\}, j \in \{0, 1\}\}\,,$$

protože dle předpokladu $\langle\{a, b\}\rangle = G$ pak dostáváme požadované. Postupujme podobně jako v části a)-i): označme $X = \{(a \cdot b)^i \cdot a^j \mid i \in \{0, \ldots, m-1\}, j \in \{0, 1\}\}$ podmnožinu grupy G.

1) Zřejmě $a = (a \cdot b)^0 \cdot a^1 \in X$ a platí $b = (a \cdot b)^m \cdot b = (a \cdot b)^{m-1} \cdot a$.

2) Zřejmě $1 = (a \cdot b)^0 \cdot a^0 \in X$. Dále pro libovolné $i \in \{0, \ldots, m-1\}$ platí $((a \cdot b)^i)^{-1} = (a \cdot b)^{m-i}$ a lze vidět, že prvek $(a \cdot b)^i a$ je inverzní sám k sobě. Množina X tak obsahuje s každým prvkem i prvek k němu inverzní. Potřebujeme ještě ukázat, že X je uzavřená na násobení. Buď nyní $(a \cdot b)^i \cdot a^j \in X$ a $(a \cdot b)^p \cdot a^q \in X$ libovolné – zde předpokládáme $i, p \in \{0, \ldots, m-1\}$ a $j, q \in \{0, 1\}$. Pokud $j = 0$ pak $(a \cdot b)^i \cdot a^j \cdot (a \cdot b)^p \cdot a^q = (a \cdot b)^{i+p} \cdot a^q \in X$, protože v případě $i + p \geq m$ platí $(a \cdot b)^{i+p} \cdot a^q = (a \cdot b)^{i+p-m} \cdot a^q$. Pokud $j = 1$, pak použijeme v úvodu dokázanou rovnost $a \cdot b = (b \cdot a)^{m-1}$ a dostaneme

$$(a \cdot b)^i \cdot a^j \cdot (a \cdot b)^p \cdot a^q = (a \cdot b)^i \cdot a \cdot ((b \cdot a)^{m-1})^p \cdot a^q = (a \cdot b)^i \cdot a \cdot (b \cdot a)^{p(m-1)} \cdot a^q =$$

$$= (a \cdot b)^i (a \cdot b)^{p(m-1)} \cdot a \cdot a^q = (a \cdot b)^{i+p(m-1)} \cdot a^{1-q} = (a \cdot b)^d \cdot a^{1-q} \in X\,,$$

kde d je zbytek po dělení čísla $i + p(m-1)$ číslem m.

3) Dokáže se naprosto stejně jako v části a)-i).

(ii) Vhodnou grupou, pro pevně zvolené $m \geq 3$, která má řád $2m$, je $(\mathbb{D}_m, \circ)$, tj. grupa symetrií pravidelného m-úhelníku. V grupě $\mathbb{D}_m$ označme a některou osovou souměrnost. Platí $a^2 = \mathrm{id}$. Dále označme r rotaci kolem středu o úhel $\frac{2\pi}{m}$. Platí $|\langle\{r\}\rangle| = m$. Protože řád podgrupy $\langle\{a, r\}\rangle$ je větší než $|\langle\{r\}\rangle| = m$ a dělí $2m = |\mathbb{D}_m|$, platí $\langle\{a, r\}\rangle = \mathbb{D}_m$. Označme nyní $b = a \circ r$. Zjevně se jedná o nějakou osovou souměrnost, a proto $b^2 = \mathrm{id}$. Navíc $a \circ b = a \circ a \circ r = r$, a proto $(a \circ b)^m = \mathrm{id}$. Konečně z rovnosti $a \circ b = r$ plyne $\langle\{a, b\}\rangle = \langle\{a, r\}\rangle = \mathbb{D}_m$. Celkem dostáváme, že grupa $(\mathbb{D}_m, \circ)$ splňuje prezentaci $(**)$.

Pro $m = 1$ má platit $a \cdot b = 1$, tj. $a = b^{-1} = b$. Jako grupu řádu $2m = 2$ lze vzít cyklickou grupu $(\mathbb{Z}_2, +)$ a v ní prvky $a = b = [1]_2$.

Pro $m = 2$ má platit $(a \cdot b)^2 = 1$, tj. $b \cdot a = (a \cdot b)^{m-1} = a \cdot b$ (viz část i)). Uvažovaná grupa je tedy komutativní (pokud komutují generátory, pak komutují všechny prvky). Jako grupu řádu $2m = 4$ lze vzít komutativní grupu $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ a v ní prvky $a = ([1]_2, [0]_2)$ a $b = ([0]_2, [1]_2)$.

Poznamenejme, že úlohu b) lze řešit také převedením na úlohu a). Nechť G je grupa splňující prezentaci $(**)$ a a, b její vhodné prvky. Označíme-li $c = a \cdot b$, pak platí $b = a^{-1} \cdot c = a \cdot c$ a tedy G je generována dvojicí prvků a a c. Navíc $a^2 = 1$, $c^m = 1$ a protože pro $b = a \cdot c$ máme $b^2 = 1$, dostáváme $a \cdot c \cdot a \cdot c = 1$. Odkud plyne, pronásobením $c^{m-1} \cdot a$ zleva, rovnost $a \cdot c = c^{m-1} \cdot a$. Tedy G splňuje prezentaci $(*)$ pro trojici čísel $k = 2$, $\ell = m$, $r = m - 1$. Část a)-i) tak ihned dává b)-i) a část a-iii) implikuje b-ii), neboť předpoklad $r^k \equiv 1 (\mathrm{mod}\ \ell)$ je splněn. V řešení části a)-iii) popsaný polopřímý součin grup $\mathbb{Z}_m$ a $\mathbb{Z}_2$ je samozřejmě izomorfní grupě $\mathbb{D}_m$ (pro $m \geq 3$) popsané v řešení b-ii), což bylo dokázáno v příkladu a)-ii) v 6. kole.

Seminář: Určete grupy symetrií pravidelných těles (krychle, čtyřstěnu, dvanáctistěnu, atd.).