ZÁKLADNÍ ALGEBRAICKÉ KONSTRUKCE

DAVID STANOVSKÝ

1. Obecné algebry

Cíl. *Zavedeme obecný pojem algebry jakožto množiny s danou sadou operací. Budeme diskutovat pojem podalgebry, generující množiny a direktního součinu.*

1.1. Algebraické struktury.

Dosud se čtenář seznámil se základy tří klasických algebraických teorií: lineární algebry, komutativní algebry a teorie grup. Objektem studia těchto disciplín je vždy speciální typ *algebraické struktury* (vektorový prostor, komutativní okruh, grupa), popsaný jako *množina*, na níž jsou definovány nějaké *operace*, přičemž každá teorie na tyto objekty klade nějaké podmínky, tzv. *axiomy*, které vycházejí z vlastností, které sdílejí důležité příklady (např. v komutativní algebře obory polynomů a číselné obory). Tyto společné znaky jsou abstrahovány v definici obecného pojmu *algebry*, který formalizuje představu, co rozumíme algebraickou strukturou.

Definice. *n-ární operací* na množině A rozumíme zobrazení z kartézské mocniny $A^n = A \times \ldots \times A$ do A. Speciálně, 0-ární operace je zobrazení z jednoprvkové množiny do A, tedy *konstanta*. Místo 1-ární říkáme *unární*, místo 2-ární říkáme *binární*. Číslu n se říká *arita* operace.

Jazykem rozumíme množinu Σ spolu se zobrazením $ar : \Sigma \to \mathbb{N} \cup \{0\}$. Význam této definice je následující: Σ je množina operačních symbolů, které budeme v dané teorii používat, a zobrazení ar udává aritu každého symbolu. Pro binární symboly se zpravidla používají infixové znaky $+, \cdot, *, \circ$ apod., pro unární symboly se někdy používají postfixové znaky $'$,$^{-1}$ apod.

Definice. *Algebra* v jazyce Σ je dvojice $\mathbf{A} = (A, \Phi)$, kde A je neprázdná množina, zvaná *nosná množina*, a Φ je zobrazení z množiny Σ do množiny všech operací na A přiřazující symbolu σ nějakou $ar(\sigma)$-ární operaci $\sigma^{\mathbf{A}}$.

Algebry budeme značit tučným písmenem, jejich nosné množiny tenkým, s výjimkou standardních značení pro běžné číselné obory ($\mathbb{Z}$, $\mathbb{Q}$ apod.). Nebude-li výslovně uvedeno jinak, nosnou množinu algebry $\mathbf{A}$ budeme značit A apod. V běžné mluvě se rozdíl mezi algebrou a její nosnou množinou často stírá a v ručním zápise je (nedobrým) zvykem značit algebru i její nosnou množinu stejně, byť, formálně vzato, jde o různé věci.

Nyní si ukážeme, jak lze v právě zavedeném smyslu definovat algebraické struktury, které již znáte.

Příklady.

- *Grupa* je algebra $\mathbf{G} = (G, \Phi)$ v jazyce $\{*, ', e\}$, kde $ar(*) = 2$, $ar(') = 1$, $ar(e) = 0$, splňující následující podmínky pro všechny prvky $a, b, c \in G$:
$$a *^{\mathbf{G}} (b *^{\mathbf{G}} c) = (a *^{\mathbf{G}} b) *^{\mathbf{G}} c,$$
$$a *^{\mathbf{G}} e^{\mathbf{G}} = e^{\mathbf{G}} *^{\mathbf{G}} a = a,$$
$$a *^{\mathbf{G}} a'^{\mathbf{G}} = a'^{\mathbf{G}} *^{\mathbf{G}} a = e^{\mathbf{G}}.$$
Algebra v jazyce $\{*, e\}$ splňující první dvě podmínky se nazývá *monoid*, algebra v jazyce $\{*\}$ splňující první podmínku se nazývá *pologrupa*.
- *Komutativní okruh s jednotkou* je algebra $\mathbf{R} = (R, \Phi)$ v jazyce $\{+, -, \cdot, 0, 1\}$, kde $ar(+) = ar(\cdot) = 2$, $ar(-) = 1$, $ar(0) = ar(1) = 0$, taková, že $(R, +, -, 0)$ je abelovská grupa, $(R, \cdot, 1)$ je komutativní monoid a pro všechna $a, b, c \in R$ platí
$$a \cdot^{\mathbf{R}} (b +^{\mathbf{R}} c) = (a \cdot^{\mathbf{R}} b) +^{\mathbf{R}} (a \cdot^{\mathbf{R}} c).$$

Je-li z kontextu zřejmé, zda mluvíme o symbolu nebo příslušné operaci, budeme pro přehlednost vynechávat horní index. Algebry v konečném jazyce $\{\sigma_1, \ldots, \sigma_n\}$ budeme zapisovat ve tvaru
$$\mathbf{A} = (A, \sigma_1, \ldots, \sigma_n).$$

Příklady.

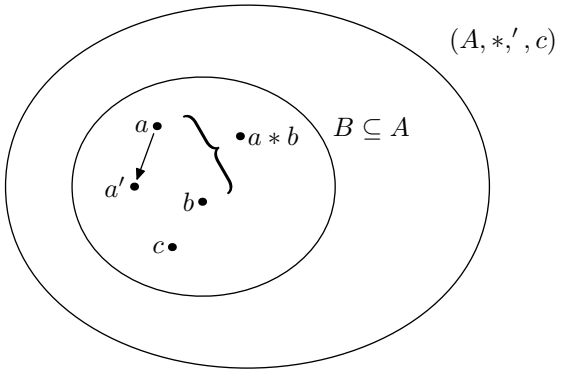
- *Těleso* je komutativní okruh s jednotkou $\mathbf{T} = (T, +, -, \cdot, 0, 1)$ splňující navíc podmínku, že pro všechna $0 \neq a \in T$ existuje právě jedno $b \in T$ takové, že $a \cdot b = 1$. Toto b sice značíme a^{-1}, ale pozor: formálně vzato, $^{-1}$ není unární operace na T, protože není definována pro 0.
- *Vektorový prostor* nad tělesem $\mathbf{T}$ je algebra $\mathbf{V}$ v jazyce $\{+, -, 0, f_\alpha : \alpha \in T\}$, kde $ar(+) = 2$, $ar(-) = 1$, $ar(0) = 1$ a $ar(f_\alpha) = 1$ pro všechna $\alpha \in T$, taková, že $(V, +, -, 0)$ je abelovská grupa a pro všechna $a, b \in V$, $\alpha, \beta \in T$, platí
$$f_{(\alpha +^{\mathbf{T}} \beta)}(a) = f_\alpha(a) + f_\beta(a), \quad f_{\alpha \cdot^{\mathbf{T}} \beta}(a) = f_\alpha(f_\beta(a)),$$
$$f_\alpha(a + b) = f_\alpha(a) + f_\alpha(b), \quad f_1(a) = a.$$
Symboly f_α interpretujeme jako skalární násobení prvkem α, tj. $f_\alpha(v) = \alpha \cdot v$. Striktně vzato, skalární součin není binární operace, neboť jde o zobrazení $T \times V \to V$.

Další příklady algebraických teorií uvidíme v poslední kapitole. Za všechny zmiňme následující dva:

Příklady.

- *Svaz* je algebra v jazyce $\{\vee, \wedge\}$, kde $ar(\vee) = ar(\wedge) = 2$, splňující jisté axiomy, které umožňují interpretovat operace $\vee, \wedge$ jako supremum a infimum dvouprvkové množiny v nějaké svazově uspořádané množině. Detaily viz Sekce **??**.
- *Booleova algebra* je algebra v jazyce $\{\vee, \wedge, \neg, 0, 1\}$, kde $ar(\vee) = ar(\wedge) = 2$, $ar(\neg) = 1$ a $ar(0) = ar(1) = 0$, splňující jisté axiomy, které vycházejí z výrokové logiky. Detaily viz Sekce **??**.

Ve zbytku kapitoly se seznámíme s několika pojmy, které se opakují ve všech výše uvedených teoriích, a dáme jim společný rámec. Jde především o pojmy podalgebry, direktního součinu, homomorfismu a faktoralgebry.



Obrázek 1. Podalgebra $\mathbf{B}$ algebry $\mathbf{A}$.

1.2. **Podalgebry.**

Definice. Buď f n-ární operace na množině A a $B \subseteq A$. Řekneme, že podmnožina B je *uzavřena na operaci* f, pokud

$$f(b_1, \ldots, b_n) \in B$$

pro všechna $b_1, \ldots, b_n \in B$.

Stojí za to explicitně uvést, že podmnožina $B \subseteq A$ je *uzavřena* na

- binární operaci $*$, pokud pro každé $a, b \in B$ platí $a * b \in B$;
- unární operaci $'$, pokud pro každé $b \in B$ platí $b' \in B$;
- nulární operaci (konstantu) c, pokud $c \in B$.

Definice. Buď $\mathbf{A}$ algebra v jazyce Σ. Řekneme, že neprázdná podmnožina $B \subseteq A$ *tvoří podalgebru* algebry $\mathbf{A}$, pokud je uzavřená na všechny operace algebry $\mathbf{A}$. *Podalgebrou* algebry $\mathbf{A}$ pak rozumíme algebru $\mathbf{B}$ ve stejném jazyce, jejíž nosná množina tvoří podalgebru algebry $\mathbf{A}$ a jejíž operace jsou restrikce operací algebry $\mathbf{A}$, tj. $\sigma^{\mathbf{B}} = \sigma^{\mathbf{A}}|_B$ pro všechna $\sigma \in \Sigma$. Značíme $\mathbf{B} \leq \mathbf{A}$.

Uvědomte si, že tato definice je kompatibilní s analogickými definicemi, které jsme již slyšeli: podalgebra vektorového prostoru je totéž co podprostor, podalgebra komutativního okruhu je podokruh, podalgebra grupy je podgrupa.

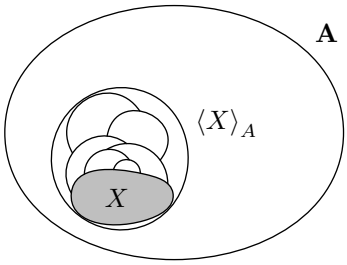
Příklad. Na operacích dané algebry záleží:

- podmnožina $\mathbb{N}$ tvoří podalgebru algebry $(\mathbb{Z}, +)$, ale nikoliv $(\mathbb{Z}, +, -)$;
- podmnožina $\{z \in \mathbb{C} : |z| = 1\}$ tvoří podalgebru algebry $(\mathbb{C}, \cdot)$, ale nikoliv $(\mathbb{C}, +)$.

Tvrzení 1.1. *Buď $\mathbf{A}$ algebra a $\mathbf{B}_i$, $i \in I$, její podalgebry. Pak $\bigcap_{i\in I} B_i$ je buď prázdná množina, nebo tvoří podalgebru algebry $\mathbf{A}$.*

Jde-li o podalgebru, budeme ji značit $\bigcap_{i\in I} \mathbf{B}_i$.

Důkaz. Označme $B = \bigcap_{i\in I} B_i$ a předpokládejme $B \neq \emptyset$. Buď σ symbol arity n a $b_1, \ldots, b_n \in B$. Pak $b_1, \ldots, b_n \in B_i$ pro všechna $i \in I$, tedy $\sigma^{\mathbf{A}}(b_1, \ldots, b_n) \in B_i$ pro všechna $i \in I$, neboť každá množina B_i je na tuto operaci uzavřena, a tedy $\sigma^{\mathbf{A}}(b_1, \ldots, b_n) \in \bigcap_{i\in I} B_i = B$. □



Obrázek 2. Podalgebra algebry $\mathbf{A}$ generovaná množinou X.

Pro sjednocení obdobné tvrzení neplatí: např. v algebře $(\mathbb{Z}, +)$ uvažujte podmnožinu A sudých čísel a podmnožinu B čísel dělitelných třemi. Sjednocení není uzavřeno na sčítání, třeba $2 + 3 \notin A \cup B$. Pro posloupnost do sebe zanořených algeber je však situace jiná.

Tvrzení 1.2. *Buď* $\mathbf{A}$ *algebra a* $\mathbf{B}_1 \leq \mathbf{B}_2 \leq \mathbf{B}_3 \leq \ldots$ *její podalgebry. Pak* $\bigcup_{i\in\mathbb{N}} B_i$ *tvoří podalgebru algebry* $\mathbf{A}$.

Tuto podalgebru budeme značit $\bigcup_{i\in\mathbb{N}} \mathbf{B}_i$.

Důkaz. Označme $B = \bigcup_{i\in\mathbb{N}} B_i$. Buď σ symbol arity n a $b_1, \ldots, b_n \in B$. Pak existuje $k \in \mathbb{N}$ takové, že $b_1, \ldots, b_n \in B_k$: vzhledem k tomu, že $b_j \in B_{k_j}$ pro nějaké $k_j \in \mathbb{N}$, stačí zvolit $k = \max(k_1, \ldots, k_n)$. Pro toto k pak platí $\sigma^{\mathbf{A}}(b_1, \ldots, b_n) \in B_k$, a tedy $\sigma^{\mathbf{A}}(b_1, \ldots, b_n) \in \bigcup_{i\in\mathbb{N}} B_i = B$. □

Uvažujme podmnožinu $\emptyset \neq X \subseteq A$ v algebře $\mathbf{A}$. Podalgebrou *generovanou množinou* X rozumíme nejmenší podalgebru (vzhledem k inkluzi) algebry $\mathbf{A}$ obsahující podmnožinu X, značíme ji $\langle X\rangle_{\mathbf{A}}$. Taková podalgebra jistě existuje: stačí vzít průnik všech podalgeber obsahujících množinu X, tj.

$$\langle X\rangle_{\mathbf{A}} = \bigcap_{X\subseteq B,\ \mathbf{B}\leq\mathbf{A}} \mathbf{B}.$$

Podle Tvrzení 1.1 je tento průnik skutečně podalgebrou, jistě obsahuje množinu X a mezi všemi takovými podalgebrami je nejmenší.

Prvky podalgebry $\langle X\rangle_{\mathbf{A}}$ zpravidla počítáme tak, že začneme s prvky množiny X a aplikováním operací algebry $\mathbf{A}$ získáváme postupně další prvky. Postup se zastaví ve chvíli, kdy již žádné nové prvky nevznikají, tedy když je výsledná podmnožina uzavřena na všechny operace algebry $\mathbf{A}$. Tento postup lze formalizovat podobně jako pro grupy ve Tvrzení **??**, ale tím se zde zabývat nebudeme.

Podalgebry generované konečnou množinou často zapisujeme zkráceně $\langle a_1, \ldots, a_n\rangle$ místo $\langle\{a_1, \ldots, a_n\}\rangle$.

Příklad. Na operacích dané algebry záleží: pro dané $n \in \mathbb{Z}$

- $\langle n\rangle_{(\mathbb{Z},+)} = \{k \cdot n : k \in \mathbb{N}\}$,
- $\langle n\rangle_{(\mathbb{Z},\cdot)} = \{n^k : k \in \mathbb{N}\}$.

Příklad. Užitečnou úlohou je nalézt co nejmenší množinu generátorů dané algebry:

- $(\mathbb{N}, +) = \langle 1\rangle$, $(\mathbb{Z}, +) = \langle 1, -1\rangle$, $(\mathbb{Z}, +, -) = \langle 1\rangle$.
  V první algebře každý prvek nagenerujeme jako součet konečně mnoha jedniček. U celých čísel potřebujeme nagenerovat i záporná čísla a k tomu

potřebujeme prvek -1 (nulu dostaneme jako $1+(-1)$). V poslední algebře však máme operaci $-$, takže prvek -1 nagenerujeme z jedničky.
- $(\mathbb{N},\cdot) = \langle 1, p : p \text{ je prvočíslo}\rangle$ díky základní větě aritmetiky. Je vidět, že tato generující množina je nejmenší možná: žádné prvočíslo není možné nagenerovat pomocí jiných prvků.

1.3. **Direktní součiny.**

Definice. *Direktním součinem* algeber $\mathbf{A}_1,\dots,\mathbf{A}_m$ ve stejném jazyce Σ rozumíme algebru $\mathbf{A}_1\times\cdots\times\mathbf{A}_m$ v témže jazyce, jejíž nosnou množinou je kartézský součin $A_1\times\cdots\times A_m$ a její operace jsou definovány po složkách, tedy

$$\sigma^{\mathbf{A}_1\times\cdots\times\mathbf{A}_m}((a_1^1,\dots,a_m^1),\dots,(a_1^n,\dots,a_m^n)) = (\sigma^{\mathbf{A}_1}(a_1^1,\dots,a_1^n),\dots,\sigma^{\mathbf{A}_m}(a_m^1,\dots,a_m^n)$$

pro každý n-ární symbol $\sigma\in\Sigma$ a všechna $a_1^k,\dots,a_n^k\in A_k$, $k=1,\dots,m$.

Stojí za to explicitně uvést, že pro binární symbol $*$ definujeme operaci předpisem

$$(a_1,\dots,a_m)*(b_1,\dots,b_m) = (a_1 *^{\mathbf{A}_1} b_1,\dots,a_m *^{\mathbf{A}_m} b_m),$$

pro unární symbol $'$ definujeme operaci $(a_1,\dots,a_m)' = (a_1'^{\mathbf{A}_1},\dots,a_m'^{\mathbf{A}_m})$ a pro konstantní symbol c definujeme konstantu $(c^{\mathbf{A}_1},\dots,c^{\mathbf{A}_m})$.

2. Homomorfismy

Cíl. *Zavedeme pojem homomorfismu, tedy zobrazení zachovávajícího strukturu dané algebry. Speciální pozornost budeme věnovat bijektivním homomorfismům, tzv. izomorfismům, které formálně popisují jev, kdy jsou dvě algebry „stejné až na přejmenování prvků“.*

2.1. **Homomorfismy.**

Zobrazením mezi dvěma matematickými objekty, která zachovávají jejich strukturu, se říká homomorfismy. Tento pojem by měl čtenář znát např. z diskrétní matematiky pro grafy, nebo z lineární algebry pro vektorové prostory. Pod jinými názvy pak tento princip najdeme v řadě dalších disciplín: např. pro metrické prostory hraje podobnou roli izometrie, tj. zobrazení zachovávající vzdálenosti (metriku). Nyní zavedeme pojem homomorfismu pro obecné algebry.

Definice. Buďte $\mathbf{A}$, $\mathbf{B}$ algebry ve stejném jazyce Σ. Zobrazení $\varphi : A\to B$ se nazývá *homomorfismus* algeber $\mathbf{A}$, $\mathbf{B}$, pokud

$$\varphi(\sigma^{\mathbf{A}}(a_1,\dots,a_n)) = \sigma^{\mathbf{B}}(\varphi(a_1),\dots,\varphi(a_n))$$

pro každý n-ární symbol $\sigma\in\Sigma$ a všechna $a_1,\dots,a_n\in A$. Říkáme, že φ *zachovává operace* těchto algeber. Píšeme $\varphi:\mathbf{A}\to\mathbf{B}$.

Stojí za to explicitně uvést, že φ zachovává binární symbol $*$, pokud

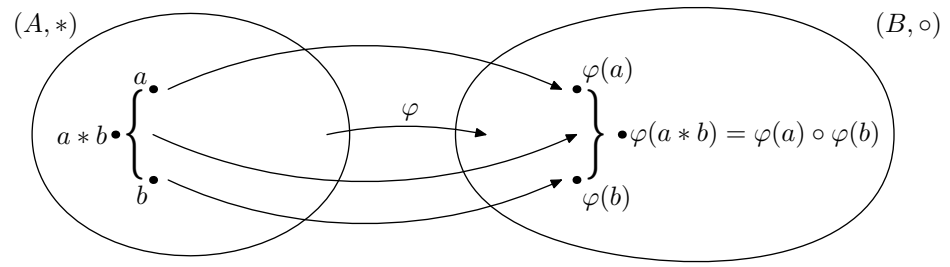
$$\varphi(a *^{\mathbf{A}} b) = \varphi(a) *^{\mathbf{B}} \varphi(b)$$

pro všechna $a,b\in A$; zachovává unární symbol $'$, pokud

$$\varphi(a'^{\mathbf{A}}) = \varphi(a)'^{\mathbf{B}}$$

pro všechna $a\in A$; zachovává konstantu c, pokud $\varphi(c^{\mathbf{A}}) = c^{\mathbf{B}}$.

Pro speciální typy homomorfismů se používá následující terminologie:



Obrázek 3. Homomorfismus $\varphi : \mathbf{A} \to \mathbf{B}$.

- *monomorfismus*, neboli *vnoření*, je prostý homomorfismus (někdy se užívá značení $\mathbf{A} \hookrightarrow \mathbf{B}$),
- *epimorfismus* je homomorfismus na (značení $\mathbf{A} \twoheadrightarrow \mathbf{B}$),
- *izomorfismus* je homomorfismus, který je bijekcí (značení $\mathbf{A} \simeq \mathbf{B}$),

a dále

- *endomorfismem* algebry $\mathbf{A}$ rozumíme homomorfismus z $\mathbf{A} \to \mathbf{A}$,
- *automorfismem* algebry $\mathbf{A}$ rozumíme izomorfismus z $\mathbf{A} \to \mathbf{A}$.

Uvědomte si, že uvedená definice homomorfismu je v případě vektorových prostorů totožná s definicí lineárního zobrazení, tak jak jej znáte z lineární algebry.

Příklad. Identické zobrazení $id : \mathbf{A} \to \mathbf{A}$, $x \mapsto x$, je vždy homomorfismem.

Příklad. Uvažujme zobrazení

$$\varphi : \mathbb{R} \to \mathbb{R}, \quad x \mapsto e^x.$$

Zobrazení φ je homomorfismem $(\mathbb{R}, +) \to (\mathbb{R}, \cdot)$, neboť $\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y)$.

Příklad. Uvažujme zobrazení

$$\varphi : \mathbb{C} \to \mathbb{R}, \quad z \mapsto |z|.$$

Zobrazení φ je homomorfismem $(\mathbb{C}, \cdot) \to (\mathbb{R}, \cdot)$, ale nikoliv $(\mathbb{C}, +) \to (\mathbb{R}, +)$.

Oboru hodnot daného homomorfismu $\varphi : \mathbf{A} \to \mathbf{B}$ se v algebře říká *obraz* a značí se

$$\mathrm{Im}(\varphi) = \{b \in B : b = \varphi(a) \text{ pro nějaké } a \in A\}.$$

Obraz vždy tvoří podalgebru algebry $\mathbf{B}$: je-li σ n-ární symbol a $b_1, \ldots, b_n \in \mathrm{Im}(\varphi)$, pak $b_1 = \varphi(a_1), \ldots, b_n = \varphi(a_n)$ pro nějaká $a_1, \ldots, a_n \in A$ a platí

$$\sigma^{\mathbf{B}}(b_1, \ldots, b_n) = \sigma^{\mathbf{B}}(\varphi(a_1), \ldots, \varphi(a_n)) = \varphi(\sigma^{\mathbf{A}}(a_1, \ldots, a_n)) \in \mathrm{Im}(\varphi).$$

Důležitou úlohou je určit, jak vypadají všechny homomorfismy mezi dvěma danými algebrami. Jedna metoda řešení vychází z toho, že homomorfismy jsou určeny svými hodnotami na generátorech (podobně jako u vektorových prostorů). Obecný princip vysvětlíme na konkrétním příkladě.

Úloha. Najděte všechny homomorfismy $(\mathbb{N}, +) \to (\mathbb{N}, +)$.

Řešení. Uvažujme homomorfismus φ. Protože $(\mathbb{N},+)=\langle 1\rangle$, z hodnoty v bodě 1 lze spočítat hodnoty ve všech ostatních bodech: je-li $\varphi(1)=k$, pak

$$\varphi(n)=\varphi(\underbrace{1+\ldots+1}_{n})=\underbrace{\varphi(1)+\ldots+\varphi(1)}_{n}=kn.$$

Tedy každý homomorfismus $(\mathbb{N},+)\to(\mathbb{N},+)$ je jedním ze zobrazení φ_k definovaných $\varphi_k(n)=kn$ pro všechna $n\in\mathbb{N}$. Zbývá ověřit, že všechna zobrazení φ_k jsou skutečně homomorfismy, což je snadné: $\varphi_k(x+y)=k(x+y)=kx+ky=\varphi_k(x)+\varphi_k(y)$ pro všechna $x,y\in\mathbb{N}$. □

Pokud nejsme schopni efektivně použít generující množinu, jako třeba v následující úloze, můžeme zkusit využít prvků se zvláštními vlastnostmi, které jsou zachovány každým homomorfismem (viz též diskuse invariantů v Sekci 2.2).

Úloha. Najděte všechny homomorfismy $(\mathbb{Z},\cdot)\to(\mathbb{Z},+)$.

Řešení. Uvažujme homomorfismus φ. Ze zachování operace plyne, že $\varphi(0)=\varphi(0\cdot 0)=\varphi(0)+\varphi(0)$, tedy $\varphi(0)=0$ a dostáváme $0=\varphi(0)=\varphi(n\cdot 0)=\varphi(n)+\varphi(0)=\varphi(n)$ pro každé $n\in\mathbb{Z}$. Existuje tedy jediný homomorfismus $n\mapsto 0$. □

Tvrzení 2.1. *Buď $\mathbf{A},\mathbf{B},\mathbf{C}$ algebry ve stejném jazyce a $\varphi:\mathbf{A}\to\mathbf{B}$ a $\psi:\mathbf{B}\to\mathbf{C}$ homomorfismy. Pak*

(1) *složené zobrazení $\psi\circ\varphi$ je homomorfismus $\mathbf{A}\to\mathbf{C}$;*
(2) *je-li φ izomorfismus, pak inverzní zobrazení φ^{-1} je izomorfismus $\mathbf{B}\to\mathbf{A}$.*

Důkaz. (1) Ověříme, že složené zobrazení $\psi\circ\varphi$ zachovává všechny operace. Pro přehlednost důkaz provedeme pro binární symbol $*$, pro symboly ostatní arity se důkaz provede analogicky. Protože φ,ψ jsou homomorfismy, platí

$$\varphi(a_1 *^{\mathbf{A}} a_2)=\varphi(a_1)*^{\mathbf{B}}\varphi(a_2),\quad \psi(b_1 *^{\mathbf{B}} b_2)=\psi(b_1)*^{\mathbf{C}}\psi(b_2)$$

pro všechna $a_1,a_2\in A$ a $b_1,b_2\in B$, a tedy

$$\begin{aligned}(\psi\circ\varphi)(a_1 *^{\mathbf{A}} a_2)&=\psi(\varphi(a_1 *^{\mathbf{A}} a_2))=\psi(\varphi(a_1)*^{\mathbf{B}}\varphi(a_2))\\&=\psi(\varphi(a_1))*^{\mathbf{C}}\psi(\varphi(a_2))=(\psi\circ\varphi)(a_1)*^{\mathbf{C}}(\psi\circ\varphi)(a_2)\end{aligned}$$

pro všechna $a_1,a_2\in A$.

(2) Ověříme, že inverzní zobrazení φ^{-1} zachovává všechny operace. Pro přehlednost důkaz opět provedeme pouze pro binární symbol $*$. Pro všechna $b_1,b_2\in B$ platí

$$b_1 *^{\mathbf{B}} b_2=\varphi(\varphi^{-1}(b_1))*^{\mathbf{B}}\varphi(\varphi^{-1}(b_2))=\varphi(\varphi^{-1}(b_1)*^{\mathbf{A}}\varphi^{-1}(b_2)),$$

a tedy

$$\varphi^{-1}(b_1 *^{\mathbf{B}} b_2)=\varphi^{-1}(\varphi(\varphi^{-1}(b_1)*^{\mathbf{A}}\varphi^{-1}(b_2)))=\varphi^{-1}(b_1)*^{\mathbf{A}}\varphi^{-1}(b_2).$$

□

Připomeňme, že automorfismy algebry $\mathbf{A}$ jsou bijektivní homomorfismy $\mathbf{A}\to\mathbf{A}$, tj. permutace na nosné množině A, které zachovávají všechny operace. Z Tvrzení 2.1 plyne, že složení automorfismů dané algebry je opět automorfismem, a že inverzní zobrazení k automorfismu je také automorfismem. Vidíme, že všechny automorfismy dané algebry $\mathbf{A}$ tvoří podgrupu symetrické grupy $\mathbf{S}_A$. Tuto podgrupu nazýváme *grupa automorfismů* a značíme

$$\mathbf{Aut}(\mathbf{A})=(\{\varphi:\mathbf{A}\to\mathbf{A}\text{ automorfismus}\},\circ,^{-1},id)\leq\mathbf{S}_A.$$

Tato grupa popisuje symetrie dané algebry a je velmi důležitá v řadě situací. Příklady si ukážeme v Sekci 3.4.

2.2. **Izomorfní algebry.**

Řekneme, že algebry $\mathbf{A}$ a $\mathbf{B}$ jsou *izomorfní*, značíme $\mathbf{A} \simeq \mathbf{B}$, pokud existuje izomorfismus $\mathbf{A} \to \mathbf{B}$, tj. vzájemně jednoznačné zobrazení mezi nosnými množinami, které zachovává všechny operace. Tento pojem si lze představit jako „kopírování algeber“: máme-li algebru $\mathbf{A}$, pro jednoduchost uvažujme binární $\mathbf{A} = (A, *)$, a bijektivní zobrazení $\varphi : A \to B$, můžeme na množinu B „překopírovat“ operaci $*$ předpisem

$$a \circ b = \varphi(\varphi^{-1}(a) * \varphi^{-1}(b)).$$

Vidíme, že zobrazení φ^{-1}, a tedy podle Tvrzení 2.1 i zobrazení φ, bude izomorfismus algeber $(A, *)$ a $(B, \circ)$. Navíc každý izomorfismus si lze představit tímto způsobem. Izomorfní algebry mají stejné „algebraické vlastnosti“ (nebudeme se pouštět do toho, co to přesně znamená). Jedna je kopií druhé, došlo pouze k přejmenování prvků popsaném kopírovacím zobrazením φ.

Je dobré si uvědomit, že relace $\simeq$ je ekvivalencí na třídě všech algeber v daném jazyce, jak plyne z Tvrzení 2.1. Reflexivita relace je důsledkem toho, že identita je izomorfismus. Symetrie toho, že inverzní zobrazení k izomorfismu je izomorfismus. A tranzitivita toho, že složení izomorfismů je izomorfismus.

Pojem izomorfismu má širší kontext. Z diskrétní matematiky znáte pojem izomorfismus grafů: dva grafy jsou izomorfní, pokud existuje bijekce mezi jejich vrcholy, která zachovává hrany, tj. vrcholy x, y jsou spojeny hranou v jednom grafu právě tehdy, když jsou jejich obrazy spojeny hranou v druhém grafu; tedy druhý graf je kopií prvního, pouze s jiným označením vrcholů. Podobný pojem najdete v každé matematické strukturní teorii.

Příklad. Algebry

$$(\{0,1\}, +_{\bmod 2}) \quad \text{a} \quad (\{1,-1\}, \cdot)$$

jsou izomorfní. Podívejme se na tabulky těchto operací:

$+$	0	1
0	0	1
1	1	0

$\cdot$	1	-1
1	1	-1
-1	-1	1

Tyto tabulky vypadají podobně: jedna je kopií druhé, pokud přepíšeme $0 \mapsto 1$, $1 \mapsto -1$. Není těžké ověřit, že toto zobrazení je skutečně izomorfismem uvedených algeber.

Příklad. Algebry

$$(\mathbb{C}, +) \quad \text{a} \quad (\mathbb{R}, +) \times (\mathbb{R}, +)$$

jsou izomorfní. Intuitivně, komplexní čísla se sčítají tak, že se sčítají jejich reálné složky, jednu algebru z druhé dostaneme přepisem $a + bi \mapsto (a, b)$. Není těžké ověřit, že toto zobrazení je skutečně izomorfismem uvedených algeber.

K důkazu, že jsou dané dvě algebry izomorfní, stačí explicitně uvést nějaký izomorfismus. Těžší úloha je prokázat, že dané algebry izomorfní nejsou, tedy že žádný izomorfismus mezi nimi neexistuje.

Příklad. Algebry $(\mathbb{Z}, \cdot)$ a $(\mathbb{Z}, +)$ *nejsou* izomorfní, protože, jak jsme ukázali v Sekci 2.1, jediný homomorfismus mezi těmito algebrami je $n \mapsto 0$ a to není bijekce.

Spočítat všechny homomorfismy mezi dvěma algebrami nebývá vůbec snadné a ani to není potřeba. Neexistence izomorfismu se obvykle prokazuje pomocí tzv. invariantů. *Invariantem* rozumíme vlastnost V takovou, že kdykoliv jsou dvě algebry $\mathbf{A}, \mathbf{B}$ izomorfní a $\mathbf{A}$ má vlastnost V, pak $\mathbf{B}$ má také vlastnost V. Příkladem invariantů jsou:

- velikost nosné množiny (mezi různě velkými množinami neexistuje bijekce, tedy ani izomorfismus);
- minimální počet generátorů;
- rovnosti, např. komutativita, asociativita, apod.;
- existence prvků s význačnými vlastnostmi, např. existence tzv. *nulového prvku*, tedy prvku z splňujícího „$\forall x\ z * x = z$“;
- počty prvků daného řádu v dané grupě, viz Tvrzení 3.4.

Nebudeme se zde pouštět do systematického studia invariantů, detailně tuto problematiku pokrývá matematická logika. Obecně lze říci, že invariantem je jakákoliv vlastnost, kterou lze vyjádřit pomocí pomocí tzv. *formulí* v daném jazyce, tj. výrazů používajících kvantifikátory, proměnné, logické spojky, rovnítko a operace z daného jazyka. Metodu ilustrujeme na několika příkladech.

Příklad. Algebry

$$(\mathbb{C}, \cdot) \quad \text{a} \quad (\mathbb{R}, \cdot) \times (\mathbb{R}, \cdot)$$

nejsou izomorfní. (Zobrazení $a+bi \mapsto (a, b)$ evidentně izomorfismus není, komplexní čísla se nenásobí po složkách.) Invariantem je např. vlastnost „$\forall x\ \exists y\ y \cdot y = x$“, která říká, že pro každý prvek existuje jeho druhá odmocnina. Algebra $(\mathbb{C}, \cdot)$ tuto vlastnost má, zatímco v algebře $(\mathbb{R}, \cdot) \times (\mathbb{R}, \cdot)$ jsou prvky, které odmocnit nelze, např. $(-1, -1)$.

Zbývá dokázat, že to je skutečně invariant. Mějme tedy algebry $\mathbf{A} = (A, \cdot)$, $\mathbf{B} = (B, \cdot)$, izomorfismus $\varphi : \mathbf{A} \to \mathbf{B}$ a předpokládejme, že algebra $\mathbf{A}$ má uvedenou vlastnost. Zvolme prvek $a \in B$. Jak najít prvek $b \in B$ splňující $b \cdot b = a$? Protože je φ bijekce, existuje $x \in A$ takové, že $\varphi(x) = a$. K němu existuje $y \in A$ s vlastností $y \cdot y = x$, položme tedy $b = \varphi(y)$. Pak $a = \varphi(x) = \varphi(y \cdot y) = \varphi(y) \cdot \varphi(y) = b \cdot b$.

Příklad. Algebry

$$(\mathbb{N}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +)$$

nejsou navzájem izomorfní, hned z několika důvodů. Předně, nosná množina algebry $(\mathbb{R}, +)$ je striktně větší, než ostatní nosné množiny. Dále $(\mathbb{N}, +) = \langle 1 \rangle$, zatímco druhé dvě algebry nelze nagenerovat jedním prvkem. Jiný argument lze provést použitím invariantu „$\exists x\ \forall y\ y + x = y$“, který postuluje existenci nulového prvku, který v $(\mathbb{N}, +)$ není, ale v ostatních algebrách je. (Dokažte sami, že jsou uvedené vlastnosti invariantem!)

3. Grupové homomorfismy

Cíl. *V této sekci vztáhneme obecnou teorii homomorfismů na případ grup. Na grupách ilustrujeme obecný fenomén klasifikačních a reprezentačních vět. Na závěr se podíváme na grupy automorfismů grup.*

3.1. **Základní vlastnosti.**

Buď $\mathbf{G}$, $\mathbf{H}$ dvě grupy. Abychom se vyhnuli psaní horních indexů u operací, označme je různou sadou symbolů, třeba $\mathbf{G} = (G, *, ', e)$ a $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ (tohoto značení se budeme držet v celé sekci). Podle definice z předchozí sekce, zobrazení $\varphi : G \to H$ je *homomorfismem* těchto grup, pokud pro každé $a, b \in G$ platí

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \quad \varphi(a') = \varphi(a)^{-1} \quad \text{a} \quad \varphi(e) = 1.$$

Je dobré si uvědomit, že druhé dvě podmínky plynou z té první, což znatelně zjednoduší práci při ověřování, zda je dané zobrazení homomorfismem.

Lemma 3.1. *Buď $\mathbf{G} = (G, *, ', e)$, $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ grupy a $\varphi : G \to H$ zobrazení. Pak φ je homomorfismem těchto grup právě tehdy, když*

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b)$$

pro všechna $a, b \in G$.

Důkaz. Musíme dokázat, že φ zachovává také invertování a jednotku. Nejprve dokážeme, že $\varphi(e) = 1$. Protože $\varphi(e) = \varphi(e * e) = \varphi(e) \cdot \varphi(e)$, krácením dostaneme $\varphi(e) = 1$. Dále dokážeme $\varphi(a') = \varphi(a)^{-1}$ pro každé $a \in G$. Protože $1 = \varphi(e) = \varphi(a * a') = \varphi(a) \cdot \varphi(a')$, z jednoznačnosti inverzních prvků v grupě $\mathbf{H}$ plyne $\varphi(a') = \varphi(a)^{-1}$. □

Připomeňme *obraz homomorfismu*

$$\mathrm{Im}(\varphi) = \{b \in H : b = \varphi(a) \text{ pro nějaké } a \in G\}$$

a definujme *jádro homomorfismu* φ předpisem

$$\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = 1\}.$$

Tvrzení 3.2. *Buď $\mathbf{G} = (G, *, ', e)$, $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ grupy a $\varphi : \mathbf{G} \to \mathbf{H}$ homomorfismus. Pak*

(1) $\mathrm{Ker}(\varphi)$ *tvoří podrupu grupy* $\mathbf{G}$ *a* $\mathrm{Im}(\varphi)$ *tvoří podgrupu grupy* $\mathbf{H}$*;*
(2) φ *je prostý právě tehdy, když* $\mathrm{Ker}(\varphi) = \{e\}$.

Důkaz. (1) Uzavřenost obrazu na operace jsme ověřili v Sekci 2.1, nyní dokážeme uzavřenost jádra. Buď $a, b \in \mathrm{Ker}(\varphi)$, tedy $\varphi(a) = \varphi(b) = 1$. Pak $\varphi(a * b) = \varphi(a) \cdot \varphi(b) = 1 \cdot 1 = 1$ a dále $\varphi(a') = \varphi(a)^{-1} = 1^{-1} = 1$ a $\varphi(e) = 1$, tedy $\mathrm{Ker}(\varphi)$ tvoří podgrupu grupy $\mathbf{G}$.

(2) Je-li φ prosté, dva různé prvky se nemohou zobrazovat na 1, takže $\mathrm{Ker}(\varphi)$ musí obsahovat jen prvek, a tím je e. Naopak, není-li φ prosté, tedy $\varphi(a) = \varphi(b)$ pro nějaká $a \neq b$, pak $1 = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a * b')$, takže máme $e \neq a * b' \in \mathrm{Ker}(\varphi)$. □

Důležitým příkladem grupového homomorfismu je modulární zobrazení z čínské věty o zbytcích.

Tvrzení 3.3. *Buďte $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla a označme $M = m_1 \cdot \ldots \cdot m_n$. Zobrazení*

$$\begin{aligned} \varphi : \mathbb{Z}_M &\to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \\ x &\mapsto (x \bmod m_1, \ldots, x \bmod m_n). \end{aligned}$$

je izomorfismem těchto grup.

Důkaz. Ověříme, že to je homomorfismus. Podle Lemmatu 3.1 stačí následující:

$$\begin{aligned}\varphi(x) +^{\mathbb{Z}_{m_1}\times\ldots\times\mathbb{Z}_{m_n}} \varphi(y) &= (x \bmod m_1, \ldots, x \bmod m_n) + (y \bmod m_1, \ldots, y \bmod m_n)\\ &= ((x+y) \bmod m_1, \ldots, (x+y) \bmod m_n) = \varphi(x +^{\mathbb{Z}_M} y),\end{aligned}$$

přičemž v poslední rovnosti využíváme faktu, že všechna m_i dělí M. Pohledem do důkazu čínské věty o zbytcích **??** zjistíme, že je zobrazení φ bijektivní. □

Z tvrzení vidíme, že pro m, n nesoudělná platí $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. Naopak, pro m, n soudělná tyto grupy izomorfní nejsou. To se nejsnáze prokáže tak, že grupa $\mathbb{Z}_{mn}$ je cyklická, zatímco $\mathbb{Z}_m \times \mathbb{Z}_n$ není, protože všechny její prvky mají řád nejvýše $\mathrm{NSN}(m, n)$. Myšlenku prokazování neizomorfnosti pomocí řádu prvků lze zobecnit.

Tvrzení 3.4. *Buď $\varphi : \mathbf{G} \to \mathbf{H}$ izomorfismus grup. Pak*

$$\mathrm{ord}(a) = \mathrm{ord}(\varphi(a))$$

pro každé $a \in G$.

Důkaz. Všimněte si, že $\varphi(x^k) = \varphi(x)^k$ pro všechna $k \in \mathbb{Z}$, protože $\varphi(x * \ldots * x) = \varphi(x) \cdot \ldots \cdot \varphi(x)$ a analogicky $\varphi(x' * \ldots * x') = \varphi(x)^{-1} \cdot \ldots \cdot \varphi(x)^{-1}$, pro každé $x \in G$. Protože φ je bijekce, platí $a^k = e$ právě tehdy, když $\varphi(a^k) = \varphi(e)$, tedy když $\varphi(a)^k = 1$. □

Z tvrzení plyne, že existence daného počtu prvků daného řádu je invariantem. Jinými slovy, jsou-li dvě grupy izomorfní, pak mají stejný počet prvků každého řádu. Opačná implikace neplatí, ale konečné protipříklady jsou řídké.

Příklady.

- Grupy $\mathbb{Q}$ a $\mathbb{Q}^*$ nejsou izomorfní, neboť grupa $\mathbb{Q}^*$ obsahuje prvek -1 řádu 2, zatímco grupa $\mathbb{Q}$ žádný prvek řádu 2 neobsahuje.
- Grupy $\mathbb{Q}$ a $\mathbb{Q}^+$ (podgrupa $\mathbb{Q}^*$ sestávající z kladných čísel) nejsou izomorfní, přestože v obou grupách mají všechny prvky kromě jednotky řád nekonečno. Není těžké dokázat, že invariantem je např. vlastnost „$\forall y\ \exists x\ x * x = y$“, která platí pouze v $(\mathbb{Q}, +)$.
- Kvaternionová grupa $\mathbf{Q}$ a dihedrální grupa $\mathbf{D}_8$ nejsou izomorfní, neboť grupa $\mathbf{Q}$ obsahuje šest prvků řádu 4, zatímco grupa $\mathbf{D}_8$ pouze dva. (Obě grupy obsahují prvky řádů 1, 2, 4 a žádný řádu 8.)

3.2. Klasifikační věty.

Jedním ze základních cílů každé algebraické teorie je tzv. *klasifikace* objektů, tj. *úplný seznam* všech příkladů *až na izomorfismus*. To zpravidla není možné provést v úplnosti, ale často je možné klasifikovat objekty s nějakou speciální, nicméně důležitou vlastností. Asi nejjednodušší větou svého druhu je klasifikace cyklických grup: každá cyklická grupa je izomorfní právě jedné z grup $\mathbb{Z}$ nebo $\mathbb{Z}_n$, $n \in \mathbb{N}$, tj. tyto jsou, až na izomorfismus, všechny příklady cyklických grup.

Věta 3.5. *Buď $\mathbf{G}$ cyklická grupa. Je-li $\mathbf{G}$ nekonečná, pak je izomorfní grupě $\mathbb{Z}$. Je-li $\mathbf{G}$ konečná řádu n, pak je izomorfní grupě $\mathbb{Z}_n$.*

Důkaz. Označme $\mathbf{G} = (G, \cdot, ^{-1}, 1) = \langle a \rangle$. Nejprve předpokládejme, že je $\mathbf{G}$ nekonečná, tedy $\mathrm{ord}(a) = \infty$, a uvažujme zobrazení

$$\mathbb{Z} \to \mathbf{G}, \qquad k \mapsto a^k.$$

Toto zobrazení je homomorfismus, neboť $a^k \cdot a^l = a^{k+l}$. Přitom jádro je triviální, protože $a^k \neq 1$ pro všechna $k \neq 0$, takže podle Tvrzení 3.2 jde o prosté zobrazení. Tvrzení **??** o vyjádření prvků podgrup generovaných danou množinou pak říká, že je toto zobrazení na $\mathbf{G}$.

Nyní předpokládejme, že je $\mathbf{G}$ řádu n, tedy $\mathrm{ord}(a) = n$, a uvažujme zobrazení

$$\mathbb{Z}_n \to \mathbf{G}, \qquad k \mapsto a^k.$$

Toto zobrazení je homomorfismus, neboť $a^k \cdot a^l = a^{k+l} = a^{k+l \bmod n}$, přičemž druhá rovnost plyne z následující úvahy: pokud $k + l < n$, tvrzení je triviální. Pokud $k + l \geq n$, pak $k + l \bmod n = k + l - n$, a tedy $a^{k+l \bmod n} = a^{k+l} \cdot a^{-n} = a^{k+l}$, protože $a^n = 1$. Podobně jako pro nekonečnou grupu dostáváme, že jádro je triviální a že jde o zobrazení na $\mathbf{G}$. □

Poznámka. Z důkazu předchozího tvrzení je vidět, že pro libovolnou grupu $\mathbf{G}$ a její prvek a je zobrazení

$$\varphi_a : \mathbb{Z} \to \mathbf{G}, \qquad k \mapsto a^k$$

homomorfismem. Jeho obrazem je cyklická podgrupa $\mathbf{Im}(\varphi_a) = \langle a \rangle_{\mathbf{G}}$, jeho jádrem je $\mathbf{Ker}(\varphi_a) = n\mathbb{Z}$, kde $n = \mathrm{ord}(a)$ v konečném případě a $n = 0$ v případě $\mathrm{ord}(a) = \infty$.

Mnohem silnější větou je klasifikace konečných abelovských grup, která říká, že každá konečná abelovská grupa je, až na izomorfismus, direktním součinem konečných cyklických grup. Navíc, díky čínské větě o zbytcích ve formě Tvrzení 3.3, stačí uvažovat pouze cyklické grupy řádu mocniny prvočísla, neboť

$$\mathbb{Z}_{p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}} \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}},$$

kdykoliv jsou $p_1, \ldots, p_m$ po dvou různá prvočísla. Navíc platí, že jednotlivé komponenty direktního součinu jsou určeny jednoznačně (až na pořadí).

Věta 3.6. *Buď $\mathbf{G}$ konečná abelovská grupa, $|\mathbf{G}| > 1$. Pak existují prvočísla $p_1, \ldots, p_m$ (ne nutně po dvou různá) a přirozená čísla $k_1, \ldots, k_m$ taková, že*

$$\mathbf{G} \simeq \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

Čísla $p_1, \ldots, p_m$ a $k_1, \ldots, k_m$ jsou určena jednoznačně až na pořadí.

Důkaz této věty je relativně elementární, ale přesto dosti dlouhý. Bude obsahem Sekce **??** na konci skript.

Příklad. Grupy $\mathbb{Z}_5^*$ i $\mathbb{Z}_{12}^*$ jsou čtyřprvkové, a tedy izomorfní buď grupě $\mathbb{Z}_4$, nebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$. Vidíme, že $\mathbb{Z}_5^* \simeq \mathbb{Z}_4$, protože $\mathbb{Z}_5^* = \langle 2 \rangle$. Na druhou stranu $\mathbb{Z}_{12}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, protože všechny prvky $\mathbb{Z}_{12}^*$ mají řád 1 nebo 2, tedy nejde o cyklickou grupu.

Příklad. Grupa $\mathbb{Z}_{21}^*$ je dvanáctiprvková. Je tedy izomorfní buď grupě $\mathbb{Z}_3 \times \mathbb{Z}_4$, nebo grupě $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Podle čínské věty o zbytcích je $\mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$. Protože grupa $\mathbb{Z}_{21}^*$ neobsahuje žádný prvek řádu 12, platí $\mathbb{Z}_{21}^* \simeq \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Oblíbenou kratochvílí je hledání malých grup, což je svým způsobem také klasifikační věta. Následující tabulka obsahuje klasifikaci všech grup řádu n pro $n \leq 11$ a pro $n = p$, $2p$, p^2, kde p je prvočíslo. V současné době je znám seznam všech grup až do velikosti $2047 = 2^{11} - 1$.

n	grupy řádu n
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ \mathbf{S}_3 = \mathbf{D}_6$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbf{D}_8,\ \mathbf{Q}$
	$\dots$
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p$
$2p$	$\mathbb{Z}_{2p},\ \mathbf{D}_{2p}$

Elementární důkaz pro $n \leq 6$ není těžký. Pro n prvočíslo je klasifikace důsledkem Lagrangeovy věty a klasifikace cyklických grup: grupy prvočíselného řádu nemohou mít vlastní podgrupy, a tedy jsou generovány každým svým prvkem kromě jednotky. Důkazy ostatních tvrzení jsou znatelně obtížnější.

3.3. **Reprezentace grup.**

Jiným, slabším, typem věty popisující objekty v dané třídě, jsou tzv. *reprezentační věty*. Každý objekt je popsán, až na izomorfismus, jako podobjekt objektu nějakého konkrétního typu. Formálně, existuje vnoření (prostý homomorfismus) do tohoto objektu. Reprezentační věty ukazují, že zkoumání obecné teorie je stejně těžké, jako zkoumání podobjektů těchto konkrétních objektů.

V úvodu kapitoly o grupách jsme zmínili, že dvěma základními příklady grup jsou grupy permutací a grupy regulárních matic. To proto, že každou grupu lze reprezentovat jako grupu permutací a každou *konečnou* grupu jako grupu regulárních matic. Tyto dvě reprezentační věty si nyní ukážeme.

Věta 3.7 (Cayleyova reprezentace)**.** *Každou grupu lze vnořit do nějaké symetrické grupy.*

Formálně, pro každou grupu $\mathbf{G}$ existuje množina X a prostý homomorfismus $\varphi : \mathbf{G} \to \mathbf{S}_X$. Čili $\mathbf{G}$ je izomorfní s permutační grupou $\mathbf{Im}(\varphi) \leq \mathbf{S}_X$.

Důkaz. Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa a uvažujme pro každé $a \in G$ zobrazení

$$L_a : G \to G, \quad x \mapsto a \cdot x$$

(těmto zobrazením se říká *levé translace*). Tato zobrazení jsou permutace: jediné řešení rovnice $L_a(x) = a \cdot x = y$ je prvek $x = a^{-1} \cdot y$, tedy zobrazení L_a je jak prosté, tak na. Uvažujme nyní zobrazení

$$\lambda : \mathbf{G} \to \mathbf{S}_G, \quad a \mapsto L_a.$$

Dokážeme, že λ je homomorfismus. Podle Lemmatu 3.1 stačí ověřit, že $\lambda(a \cdot b) = \lambda(a) \circ \lambda(b)$, tj. že zobrazení $L_{a \cdot b}$ je totožné se složením zobrazení $L_a \circ L_b$. Dosazením $x \in G$ vidíme, že

$$L_{a \cdot b}(x) = (a \cdot b) \cdot x = a \cdot (b \cdot x) = L_a(b \cdot x) = L_a(L_b(x)) = (L_a \circ L_b)(x).$$

K ověření prostosti stačí spočítat jádro: kdyby $L_a = id$, pak $a = L_a(1) = id(1) = 1$. Tedy $\mathbf{Ker}(\lambda) = \{1\}$ a λ je prostý homomorfismus. □

Věta 3.8 (Lineární reprezentace)**.** *Každou konečnou grupu lze vnořit do nějaké obecné lineární grupy, nad libovolným tělesem.*

Důkaz. Buď $\mathbf{T}$ libovolné těleso, $\mathbf{G}$ daná konečná grupa a označme $n = |G|$. Bez újmy na obecnosti předpokládejme, že nosná množina G sestává z čísel $1, \dots, n$ (přejmenování prvků odpovídá izomorfismu). Protože máme k dispozici Cayleovu reprezentaci $\lambda : \mathbf{G} \to \mathbf{S}_n$, stačí nalézt vnoření ψ grupy $\mathbf{S}_n$ do $\mathbf{GL}_n(\mathbf{T})$, hledaným vnořením pak bude složení $\psi \circ \lambda$. Uvažujme

$$\psi : \mathbf{S}_n \to \mathbf{GL}_n(\mathbf{T}), \quad \sigma \mapsto \big(\delta_{i,\sigma(j)}\big)_{i,j=1}^{n},$$

kde $\delta_{u,v} = 1$ pokud $u = v$ a $\delta_{u,v} = 0$ v opačném případě. Tedy $\psi(\sigma)$ je matice, ve které je v každém řádku a každém sloupci právě jedna jednička a jinak samé nuly, přičemž ta jednička na i-tém řádku je v $\sigma^{-1}(i)$-tém sloupci. Evidentně jde o prosté zobrazení, zbývá tedy dokázat, že to je homomorfismus, tedy že platí

$$\psi(\pi \circ \sigma) = \psi(\pi) \cdot \psi(\sigma)$$

pro všechny permutace $\pi, \sigma \in S_n$. Pravá strana je rovna

$$\big(\delta_{i,\pi(j)}\big)_1^n \cdot \big(\delta_{i,\sigma(j)}\big)_1^n = \big(\sum_k \delta_{i,\pi(k)} \cdot \delta_{k,\sigma(j)}\big)_1^n.$$

Přitom $\delta_{i,\pi(k)} \cdot \delta_{k,\sigma(j)} = 1$ právě tehdy, když $i = \pi(k)$ a $k = \sigma(j)$, což je právě tehdy, když $i = \pi(\sigma(j))$ a $k = \sigma(j)$. Tedy celá suma je rovna jedné pro $i = \pi(\sigma(j))$ a nule v opačném případě. Tím pádem je to přesně matice $\psi(\pi \circ \sigma)$. □

Příklad. Rozebereme si reprezentaci grupy $\mathbf{S}_3$ v grupě $\mathbf{GL}_3(\mathbf{T})$. Podle návodu uvedeného v důkazu Věty 3.8 zkonstruujeme

$$\psi(id) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \psi((1\ 2\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \psi((1\ 3\ 2)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$
$$\psi((1\ 2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \psi((2\ 3)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \psi((1\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

3.4. **Automorfismy grup.**

V Sekci 2.2 jsme definovali pojem grupy automorfismů dané algebry. Nyní se podíváme na speciální případ, kde je touto algebrou grupa. Začneme tím, že spočteme, jak vypadají automorfismy cyklických grup.

Tvrzení 3.9. *Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa.*

1. *Endomorfismy $\mathbf{G}$ jsou právě všechna zobrazení $x \mapsto x^k$, $k \in \mathbb{Z}$.*
2. *Automorfismy $\mathbf{G}$ jsou právě všechna zobrazení $x \mapsto x^k$ pro $k \in \mathbb{Z}$ splňující $\mathbf{G} = \langle a^k \rangle$.*

Důkaz. Buď φ endomorfismus a $k \in \mathbb{Z}$ takové, že $\varphi(a) = a^k$ (každý prvek grupy $\mathbf{G}$ je takového tvaru). Pro dané $x = a^l$ dostáváme

$$\varphi(x) = \varphi(a^l) = \varphi(a)^l = a^{kl} = x^k.$$

Tato zobrazení jsou skutečně endomorfismy, protože pro $x = a^l$, $y = a^m$ platí

$$\varphi(x \cdot y) = \varphi(a^l \cdot a^m) = \varphi(a^{l+m}) = a^{(l+m)\cdot k} = a^{lk} \cdot a^{mk} = x^k \cdot y^k = \varphi(x) \cdot \varphi(y).$$

Které z těchto endomorfismů jsou permutace? Vidíme, že

$$\mathrm{Im}(\varphi) = \{x^k : x \in G\} = \{a^{kl} : l \in \mathbb{Z}\} = \langle a^k \rangle_{\mathbf{G}},$$

tedy podmínka $\mathbf{G} = \langle a^k \rangle$ je ekvivalentní požadavku, že je homomorfismus φ na. Je-li $\mathbf{G}$ konečná, φ je prostý podle Lemmatu **??**. Je-li $\mathbf{G}$ nekonečná, jediná možnost, jak splnit tuto podmínku, je $k = \pm 1$, přičemž obě volby dají prostá zobrazení. □

Příklad. Endomorfismy grupy $\mathbb{Z}_n$ jsou právě zobrazení $x \mapsto kx$, $k = 0, \ldots, n-1$. Automorfismy jsou pouze ty z nich, kde $\mathrm{NSD}(k, n) = 1$ (viz Lemma **??**). Vidíme, že $\mathbf{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$, kde prvku $k \in \mathbb{Z}_n^*$ odpovídá zobrazení $\varphi_k(x) = kx$, neboť $(\varphi_k \circ \varphi_l)(x) = k \cdot (l \cdot x) = (k \cdot l) \cdot x = \varphi_{kl}(x)$.

Příklad. Endomorfismy grupy $\mathbb{Z}$ jsou právě zobrazení $x \mapsto kx$, $k \in \mathbb{Z}$. Automorfismy jsou pouze dva, $x \mapsto \pm x$. Vidíme, že $\mathbf{Aut}(\mathbb{Z}) \simeq \mathbb{Z}^*$, ze stejného důvodu, jako v předchozím příkladě.

Pro grupy s více než jedním generátorem je situace v obecnosti komplikovaná, není snadné určit, které hodnoty na generátorech určují endomorfismus. Důležitou roli při určování grupy automorfismů hraje konjugace: zobrazení

$$\kappa_a : \mathbf{G} \to \mathbf{G}, \quad x \mapsto a \cdot x \cdot a^{-1}$$

je vždy automorfismem grupy $\mathbf{G}$, pro každé $a \in G$, protože $\kappa_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \kappa_a(x) \cdot \kappa_a(y)$. Těmto automorfismům se říká *vnitřní*. Je snadné ověřit, že vnitřní automorfismy tvoří podgrupu grupy $\mathbf{Aut}(\mathbf{G})$, značíme ji $\mathbf{Inn}(\mathbf{G})$. Toto pozorování nám může pomoci najít potřebný příklad automorfismu dané grupy, aniž bychom museli hledat složitou konstrukci.

Příklad. Dokážeme, že $\mathbf{Aut}(\mathbf{S}_3) = \mathbf{Inn}(\mathbf{S}_3) \simeq \mathbf{S}_3$. Protože je $\mathbf{S}_3 = \langle (1\ 2), (2\ 3) \rangle$, každý její automorfismus je určený hodnotami na těchto dvou transpozicích. Ty se přitom mohou zobrazit jen na transpozice (Tvrzení 3.4), které navíc musí být navzájem různé, takže $\mathbf{Aut}(\mathbf{S}_3)$ je nejvýše šestiprvková grupa. Není těžké ověřit, že vnitřní automorfismy jsou po dvou různé, tedy $\mathbf{Aut}(\mathbf{S}_3) = \mathbf{Inn}(\mathbf{S}_3)$, a dále, že spolu vnitřní automorfismy nekomutují, takže z tabulky malých grup vyčteme, že jde, až na izomorfismus, o grupu $\mathbf{S}_3$.

Poznamenejme, že podobné tvrzení platí i pro větší symetrické grupy, ale je o dost těžší to dokázat: $\mathbf{Aut}(\mathbf{S}_n) = \mathbf{Inn}(\mathbf{S}_n) \simeq \mathbf{S}_n$, s jedinou výjimkou $n = 6$.