ALGEBRA I

JAN TRLIFAJ

Tento text pokrývá látku probíranou na přednášce Algebra I (NALG026) pro druhý ročník bakalářského studia obecné matematiky.

Hlavním tématem je teorie grup. Kromě základních vlastností grup se věnujeme jejich působení na množinách a pomocí nich dokazujeme dvě klasické strukturní věty pro konečné grupy. Druhým tématem jsou okruhy a moduly. Po probrání jejich základních vlastností prezentujeme na příkladě komutativních okruhů důležitou obecnou metodu lokalizace. Část o modulech zase slouží jako malý úvod do kategoriálních metod v algebře.

Text zachycuje podrobně základní pojmy, tvrzení a jejich důkazy. Některé partie – zejména příklady – jsou prezentovány stručněji, doplnění podrobností je ponecháno čtenáři jako cvičení. Některé poznámky přesahují rámec přednášky a slouží k náhledu do obecnějších souvislostí probíraného tématu.

Date: 12. ledna 2012.

1. Grupy a jejich reprezentace

Tato kapitola je věnována základním pojmům a výsledkům teorie grup a úvodu do teorie reprezentací grup. Hlavními výsledky jsou věta o struktuře grup řádu p^2, kde p je prvočíslo (Věta 1.62), a Frobenius-Stickelbergerova věta o struktuře konečných komutativních grup (Věta 1.66). Pojítkem výkladu jsou varianty Cayleyho věty o vnořitelnosti do transformačních monoidů resp. symetrických grup.

Nejprve zavedeme méně strukturované objekty: pologrupy a monoidy.

1.1. **Pologrupy a monoidy.**

Definice 1.1. Uspořádaná dvojice $\mathcal{G} = (G, \odot)$, kde G je neprázdná množina a $\odot$ je binární operace na G, se nazývá *grupoid*. Je-li operace $\odot$ asociativní na G, pak se $\mathcal{G}$ nazývá *pologrupa*. Množina G je *nosičem* grupoidu (pologrupy) $\mathcal{G}$.

Pokud nebude hrozit nedorozumění, nebudeme v dalším striktně rozlišovat mezi grupoidem a jeho nosičem, tj. budeme předpokládat, že G je již vybavena strukturou grupoidu zřejmou z daného kontextu. (Podobné zjednodušení provedeme později i pro grupy, okruhy a moduly).

Příklad 1.2. Příkladem grupoidu je $(\mathbb{Z}, -)$ (= množina všech celých čísel s operací odečítání). Příklady pologrup jsou $(\mathbb{N}, +)$ a $(\mathbb{Z}, +)$ (= množina všech přirozených resp. celých čísel s operací sčítání).

Pojem grupoidu je příliš málo strukturován na to, aby bylo možné vytvořit hlubší obecnou teorii. Obvykle se proto zkoumají grupoidy s dalšími vlastnostmi - my se zde zaměříme na pologrupy a monoidy, a pak především na grupy.

Konečné grupoidy často zadáváme pomocí tabulky operace $\odot$, tzv. Cayleyho tabulky. Všimněme si, že má-li množina G mohutnost $\mid G \mid = n$, máme n^{n^2} různých možností jak Cayleyho tabulku definovat. Už pro $n = 4$ je to $2^{32} \simeq 4.10^9$ možností.

Definice 1.3. Nechť $\mathcal{G} = (G, \odot)$ je grupoid. Prvek $e \in G$ se nazývá *levá resp. pravá jednotka* v $\mathcal{G}$ pokud $e \odot g = g$ resp. $g \odot e = g$ pro každé $g \in G$. Levá i pravá jednotka v $\mathcal{G}$ se nazývá *(oboustranná) jednotka* v $\mathcal{G}$.

Pokud v grupoidu $\mathcal{G}$ existuje aspoň jedna levá jednotka $e \in G$ a aspoň jedna pravá jednotka $f \in G$, pak jsou všechny levé i pravé jednotky totožné, neboť $e = e \odot f = f$.

Pokud v $\mathcal{G}$ žádná levá jednotka neexistuje, není obecně počet pravých jednotek v $\mathcal{G}$ nijak omezen: na libovolné neprázdné množině A můžeme definovat binární operaci $\odot$ vztahem $a \odot b = a$. Pak je každý prvek A pravou jednotkou, a $(A, \odot)$ je pologrupa.

Definice 1.4. Uspořádaná trojice $\mathcal{G} = (G, \odot, e)$, kde $(G, \odot)$ je pologrupa a e je (oboustranná) jednotka v $\mathcal{G}$, se nazývá *monoid*. Je-li operace $\odot$ komutativní, je $\mathcal{G}$ *komutativní monoid*.

Například $(\mathbb{N}, +, 0)$ a $(\mathbb{Z}, +, 0)$ jsou komutativní monoidy. V dalším budeme potřebovat komutativní monoid $(\mathbb{N}^m, \bar{\oplus}, \bar{0})$ tvořený všemi uspořádanými m-ticemi přirozených čísel se sčítáním po složkách a s $\bar{0} = (0, \ldots, 0) \in \mathbb{N}^m$.

Důležitým příkladem nekomutativního monoidu je tzv. transformační monoid:

Definice 1.5. Nechť X je neprázdná množina a $T(X)$ je množina všech transformací X (= zobrazení z X do X). Monoid $\mathcal{T}(X) = (T(X), \circ, \mathrm{id}_X)$, kde $\circ$ je operace skládání zobrazení a id_X je identická transformace na X, se nazývá *transformační monoid* na X.

(Konvence: zobrazení budeme skládat zprava doleva, tedy $(f \circ g)(x) = f(g(x))$ pro $x \in X$)

Má-li množina X n prvků, má transformační monoid $T(X)$ n^n prvků. Naším nejbližším cílem bude dokázat, že transformační monoidy jsou bohaté i po strukturní stránce: každý monoid je izomorfní podmonoidu vhodného transformačního monoidu. K tomu budeme potřebovat několik dalších základních pojmů:

Definice 1.6. Nechť $\mathcal{G} = (G, \odot)$ je grupoid a $g \in G$. Zobrazení $L_g : G \to G$ definované vztahem $L_g(h) = g \odot h$ se nazývá *levou translací* určenou prvkem g. Zobrazení $P_g : G \to G$ definované vztahem $P_g(h) = h \odot g$ se nazývá *pravou translací* určenou prvkem g.

Definice 1.7. Nechť $\mathcal{G} = (G, \odot, e)$ a $\mathcal{H} = (H, \odot', e')$ jsou monoidy. Pak $\mathcal{H}$ je *podmonoidem* v $\mathcal{G}$ (značení: $H \leq G$ nebo $\mathcal{H} \leq \mathcal{G}$) pokud $H \subseteq G$, $\odot'$ je restrikcí $\odot$ na H a $e' = e$.

Nosiče podmonoidů $\mathcal{G}$ jsou tedy právě podmnožiny G uzavřené na binární operaci $\odot$ a obsahující e. Všechny podmonoidy v $\mathcal{G}$ tvoří částečně uspořádanou množinu, jejímž nejmenším prvkem je monoid s nosičem $\{e\}$, a největším $\mathcal{G}$.

Definice 1.8. Nechť $\mathcal{G} = (G, \odot, e)$ a $\mathcal{G}' = (G', \odot', e')$ jsou monoidy a $\varphi : G \to G'$ je zobrazení. Pak φ je *monoidový homomorfismus* pokud $\varphi(g \odot h) = \varphi(g) \odot' \varphi(h)$ pro každá $g, h \in G$ a $\varphi(e) = e'$.

Je-li navíc φ bijekce, nazývá se φ *monoidovým izomorfismem*. Monoidy $\mathcal{G}$ a $\mathcal{G}'$ se pak nazývají *izomorfní* (označení: $G \simeq G'$ nebo $\mathcal{G} \simeq \mathcal{G}'$)

Je-li $H \leq G$, pak inkluze $H \hookrightarrow G$ je zřejmě prostým monoidovým homomorfismem.

Existence izomorfismu mezi dvěma monoidy říká, že tyto monoidy mají tytéž algebraické vlastnosti, tj. jsou nerozlišitelné algebraickými prostředky. Klasifikace až na izomorfismus je (obvykle velmi obtížně dosažitelným) cílem řady algebraických teorií.

S každým homomorfismem je spojen pojem *jádra* a *obrazu*. Všimněme si nejprve vlastností obrazu. Shrneme je v následujícím lemmatu, jehož důkaz plyne bezprostředně z 1.7 a 1.8:

Lemma 1.9. *Nechť $\mathcal{G} = (G, \odot, e)$ a $\mathcal{G}' = (G', \odot', e')$ jsou monoidy a $\varphi : G \to G'$ je monoidový homomorfismus. Pak Im $\varphi = \{g' \in G' \mid \exists g \in G : \varphi(g) = g'\}$ je nosičem podmonoidu v $\mathcal{G}'$. Je-li φ prosté zobrazení, je zobrazení $\psi : G \to$ Im φ definované pomocí $\psi(g) = \varphi(g)$ pro každé $g \in G$ monoidovým izomorfismem.*

Věta 1.10 (Cayleyho pro monoidy)**.** *Každý monoid je izomorfní podmonoidu vhodného transformačního monoidu.*

Důkaz. Nechť $\mathcal{G} = (G, \odot, e)$ je monoid. Položme $X = G$ a definujme zobrazení $\varphi : G \to T(X)$ vztahem $\varphi(g) = L_g$. Protože $L_g(e) = g$ pro každé $g \in G$, je φ prosté. Z asociativity operace $\odot$ plyne $L_{g \odot h} = L_g \circ L_h$ pro každé $g, h \in G$. Protože $e \in G$ je jednotkový prvek, je $L_e = \mathrm{id}_G$, tedy φ je prostý monoidový homomorfismus. Podle Lemmatu 1.9 je Im $\varphi \leq T(X)$ a $G \simeq$ Im φ. □

Reprezentace monoidu $\mathcal{G}$ v důkazu 1.10 zdaleka není optimální: je-li $\mathcal{G} = \mathcal{T}(X)$ již transformačním monoidem, je $\mathcal{G}$ reprezentováno jako podmonoid v $\mathcal{T}(T(X))$. Důležitou vlastností reprezentace v důkazu Věty 1.10 je ale fakt, že konečné monoidy jsou reprezentovány jako podmonoidy konečných transformačních monoidů.

Definice 1.11. Nechť $\mathcal{G} = (G, \odot, e)$ je monoid a $g \in G$. Pak g je *zleva invertibilní* pokud existuje $h_1 \in G$ tak, že $h_1 \odot g = e$. Pak h_1 se nazývá *levý inverzní* prvek ke g.

Podobně g je *zprava invertibilní* pokud existuje $h_2 \in G$ tak, že $g \odot h_2 = e$, a h_2 se nazývá *pravý inverzní* prvek ke g.

Je-li g zleva i zprava invertibilní, nazývá se g *(oboustranně) invertibilní*. Z asociativity operace $\odot$ pak plyne, že prvek $h_1 = h_1 \odot e = h_1 \odot (g \odot h_2) = (h_1 \odot g) \odot h_2 = e \odot h_2 = h_2$ je jednoznačně určen g; budeme jej značit g^{-1}.

Například v transformačním monoidu $\mathcal{T}(X)$ jsou zleva invertibilní právě všechna prostá zobrazení X do sebe, zprava invertibilní právě všechna zobrazení na, a invertibilní právě všechny bijekce X na sebe. Je-li X konečná, pak tyto pojmy splývají. Podle Věty 1.10 tedy pojmy zleva (resp. zprava, oboustranně) invertibilního prvku splývají i v každém konečném monoidu $\mathcal{G}$.

1.2. **Grupy.** Jedním z klíčových pojmů moderní algebry je pojem grupy.

Definice 1.12. Nechť $(G, \odot, e)$ je monoid na němž existuje unární operace $^{-1}$ taková, že pro každé $g \in G$ je g^{-1} oboustranně inverzním prvkem ke g.

Pak $\mathcal{G} = (G, \odot, ^{-1}, e)$ se nazývá *grupa*. Je-li navíc operace $\odot$ komutativní, pak $\mathcal{G}$ je *komutativní (= Abelova) grupa*.

Aditivní i multiplikativní grupy všech celých, racionálních, reálných a komplexních čísel, tj. $(\mathbb{Z}, +, -, 0)$, $(\mathbb{Q}, +, -, 0)$, $(\mathbb{R}, +, -, 0)$, $(\mathbb{C}, +, -, 0)$, $(\mathbb{Q} \setminus \{0\}, ., ^{-1}, 1)$, $(\mathbb{R} \setminus \{0\}, ., ^{-1}, 1)$ a $(\mathbb{C} \setminus \{0\}, ., ^{-1}, 1)$ jsou komutativní. Aditivní grupa kvaternionů $(\mathbb{H}, +, -, 0)$ je komutativní, ale jejich multiplikativní grupa $(\mathbb{H} \setminus \{0\}, ., ^{-1}, 1)$ není komutativní (*Kvaternionem* rozumíme 2×2-matici $\left(\begin{smallmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{smallmatrix}\right)$, kde z_1, z_2 jsou komplexní čísla, a $\bar{z}$ značí číslo komplexně sdružené s číslem $z \in \mathbb{C}$. Kvaterniony se sčítají a násobí jako komplexní matice typu 2×2).

Základním příkladem konečné grupy je, pro každé $n > 1$, aditivní grupa $\mathbb{Z}_n = (\{0, \dots, n-1\}, +_n, -_n, 0_n)$ všech zbytkových tříd celých čísel modulo n: operace $+_n$ je sčítání modulo n, $-_n$ je opačný prvek modulo n, jednotkou je $0_n = 0$. Tato grupa je zřejmě komutativní.

Základním příkladem nekomutativní grupy je symetrická grupa:

Definice 1.13. Nechť X je neprázdná množina a $S(X)$ je množina všech bijekcí X na sebe. Pak $(S(X), \circ, \mathrm{id}_X)$ je podmonoidem v transformačním monoidu $\mathcal{T}(X)$. Pro $f \in S(X)$ označme f^{-1} inverzní bijekci k f. Pak $\mathcal{S}(X) = (S(X), \circ, ^{-1}, \mathrm{id}_X)$ je grupa, tzv. *symetrická grupa* na množině X.

V pojmu grupy se setkává asociativita s možností dělení a krácení:

Definice 1.14. Nechť $\mathcal{G} = (G, \odot)$ je grupoid. Pak $\mathcal{G}$ je *s levým krácením (resp. dělením)*, pokud pro každé $g \in G$ je levá translace L_g prostá (resp. na). Pravé krácení resp. dělení je definováno analogicky pomocí pravé translace P_g.

Je-li $\mathcal{G}$ s levým i pravým krácením a s levým i pravým dělením, pak se $\mathcal{G}$ nazývá *kvazigrupa*. Kvazigrupa s jednotkovým prvkem se nazývá *lupa*.

Například v pologrupě $\mathcal{G} = (G, \odot)$ definované vztahem $g \odot h = h$ pro každé $g, h \in G$ je L_g identita na G, zatímco P_g je konstantní pro každé $g \in G$. Tedy má-li G aspoň dva prvky, je $\mathcal{G}$ s levým krácením i dělením, ale není s pravým krácením ani dělením. Naopak, grupoid $(\mathbb{Z}, -)$ je kvazigrupou, ale není pologrupou.

Věta 1.15. *Nechť $(G, \odot)$ je grupoid. Potom následující podmínky jsou ekvivalentní:*

(i) *$(G, \odot)$ je pologrupa a kvazigrupa.*

(ii) *Na G lze definovat unární operaci $^{-1}$ a (nulární operaci) $e \in G$ tak, že $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa.*

Důkaz. (i) ⇒ (ii). Nechť $g \in G$. Protože $(G, \odot)$ je kvazigrupa, existují prvky $g_1, g_2 \in G$ tak, že $g \odot g_1 = g = g_2 \odot g$. Dokážeme, že $e = g_1 = g_2$ je jednotkovým prvkem grupoidu $(G, \odot)$. Podle předpokladu existují pro libovolné $h \in G$ prvky $h_1, h_2 \in G$ tak, že $g \odot h_1 = h = h_2 \odot g$.

Pak $h \odot g_1 = (h_2 \odot g) \odot g_1 = h_2 \odot (g \odot g_1) = h_2 \odot g = h$, a podobně $g_2 \odot h = h$. Tedy $e = g_1 = g_2$ je jednotkovým prvkem grupoidu $(G, \odot)$.

Protože $(G, \odot)$ je kvazigrupa, existují pro každé $g \in G$ prvky $k_1, k_2 \in G$ tak, že $g \odot k_1 = e = k_2 \odot g$. Z asociativity $\odot$ plyne, že $k_1 = k_2 = g^{-1}$ je inverzní prvek ke g.

(ii) ⇒ (i). Zřejmě je $(G, \odot)$ pologrupou. Protože $L_g \circ L_{g^{-1}} = L_e = \mathrm{id}_G = L_{g^{-1}} \circ L_g$ a $P_g \circ P_{g^{-1}} = P_e = \mathrm{id}_G = P_{g^{-1}} \circ P_g$ pro každé $g \in G$, je $(G, \odot)$ kvazigrupa. □

Nyní budeme směřovat k důkazu verze Cayleyho věty 1.10 pro grupy. K tomu potřebujeme rozšířit pojmy podmonoidu a monoidového homomorfismu na grupy:

Definice 1.16. Nechť $\mathcal{G} = (G, \odot, {}^{-1}, e)$ a $\mathcal{H} = (H, \odot', {}^{-1'}, e')$ jsou grupy. Pak $\mathcal{H}$ je *podgrupou* v $\mathcal{G}$ (označení: $H \leq G$ nebo $\mathcal{H} \leq \mathcal{G}$; H se nazývá *nosičem* podgrupy $\mathcal{H}$) pokud $H \subseteq G$, $\odot'$ resp. ${}^{-1'}$ je restrikcí $\odot$ resp. ${}^{-1}$ na H a $e' = e$.

Podgrupy $\mathcal{G}$ tedy odpovídají podmonoidům v $(G, \odot, e)$, jejichž nosiče jsou uzavřené na unární operaci ${}^{-1}$. Podgrupy $\mathcal{G}$ tvoří částečně uspořádanou množinu, jejímž nejmenším prvkem je grupa s nosičem $\{e\}$ a největším $\mathcal{G}$ (tzv. *triviální* podgrupy v $\mathcal{G}$).

Definice 1.17. Nechť $1 < n < \omega$. Pak symbolem S_n značíme symetrickou grupu na množině $\{1, \ldots, n\}$. Nosičem této grupy jsou všechny permutace na $\{1, \ldots, n\}$ (viz. též 1.13). Výběrem všech sudých permutací dostáváme tzv. alternující grupu A_n, která je zřejmě podgrupou S_n. Jinou podgrupu, F_n, v S_n můžeme získat například tak, že uvažujeme pouze permutace fixující poslední složku, $F_n = \{f \in S_n \mid f(n) = n\}$.

Definice 1.18. Nechť $\mathcal{G} = (G, \odot, {}^{-1}, e)$ a $\mathcal{G}' = (G', \odot', {}^{-1'}, e')$ jsou grupy a $\varphi : G \to G'$ je zobrazení. Pak φ je *grupový homomorfismus* pokud φ je monoidový homomorfismus $(G, \odot, e)$ do $(G', \odot', e')$, a pro každé $g \in G$ je $\varphi(g^{-1}) = (\varphi(g))^{-1'}$.

Je-li navíc φ bijekce, nazývá se *grupovým izomorfismem*. Grupy $\mathcal{G}$ a $\mathcal{G}'$ se pak nazývají *izomorfní* (značení: $G \simeq G'$ nebo $\mathcal{G} \simeq \mathcal{G}'$)

Příklad 1.19. Je-li $H \leq G$, pak vnoření $\varphi\colon H \hookrightarrow G$ je zřejmě prostým grupovým homomorfismem. Zobrazení $f \mapsto f \restriction \{1, \ldots, n-1\}$ grupy F_n z 1.17 do symetrické grupy S_{n-1} je zřejmě grupovým izomorfismem.

Skutečnost, že nějaké zobrazení $\varphi\colon G \to G'$ je grupovým homomorfismem lze ověřit velmi jednoduše:

Lemma 1.20. *Nechť $\mathcal{G} = (G, \odot, {}^{-1}, e)$ a $\mathcal{G}' = (G', \odot', {}^{-1'} e')$ jsou grupy a $\varphi : G \to G'$ je zobrazení. Pak φ je grupový homomorfismus právě když $\varphi(g \odot h) = \varphi(g) \odot' \varphi(h)$ pro každé $g, h \in G$.*

Důkaz. Předpokládejme, že $\varphi(g \odot h) = \varphi(g) \odot' \varphi(h)$ pro každé $g, h \in G$. Protože jednotkový prvek grupy je jejím jediným idempotentním prvkem (tj. prvkem s vlastností $g \odot g = g$), je nutně $\varphi(e) = e'$. Podobně, inverzní prvek g^{-1} je jediným prvkem h takovým, že $h \odot g = g \odot h$ je jednotkovým prvkem. Tedy nutně $\varphi(g^{-1}) = (\varphi(g))^{-1'}$. □

Vlastnosti jádra a obrazu grupového homomorfismu shrneme v následujícím lemmatu, jehož důkaz plyne bezprostředně z Definic 1.16 a 1.18:

Lemma 1.21. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ a $\mathcal{G}' = (G', \odot', ^{-1'}, e')$ jsou grupy a $\varphi\colon G \to G'$ je grupový homomorfismus. Pak $Ker\,\varphi = \{g \in G \mid \varphi(g) = e'\}$ je nosičem podgrupy v $\mathcal{G}$ a $Im\,\varphi$ je nosičem podgrupy v $\mathcal{G}'$. Je-li φ prosté zobrazení, je zobrazení $\psi : G \to Im\,\varphi$ definované pomocí $\psi(g) = \varphi(g)$ pro každé $g \in G$ grupovým izomorfismem.*

Věta 1.22 (Cayleyho pro grupy)**.** *Každá grupa je izomorfní podgrupě vhodné symetrické grupy.*

Důkaz. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa. Položme $X = G$ a definujme zobrazení $\varphi\colon G \to S(X)$ vztahem $\varphi(g) = L_g$. Tato definice je korektní, neboť $(G, \odot)$ je kvazigrupa.

Podle 1.10 určuje φ prostý monoidový homomorfismus $(G, \odot, e)$ do $\mathcal{T}(X)$. Podle 1.20 je φ grupovým homomorfismem. Podle 1.21 je Im φ podgrupou v $\mathcal{S}(X)$ izomorfní s $\mathcal{G}$. □

Reprezentaci grupy $\mathcal{G}$ z 1.22 použijeme v následující sekci ke konstrukci tzv. regulární reprezentace grupy $\mathcal{G}$.

Definice 1.23. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $\mathcal{H} \leq \mathcal{G}$ a $g \in G$. Množina $gH = \{g \odot h \mid h \in H\}$ se nazývá *levou rozkladovou třídou* grupy $\mathcal{G}$ podle podgrupy $\mathcal{H}$ určenou prvkem g. Zřejmě $gH = L_g(H)$. Analogicky definujeme *pravou rozkladovou třídu*, $Hg = P_g(H)$.

Příklad 1.24. 1. Nechť $\mathcal{G} = S_n$ a $\mathcal{H} = A_n$. Pokud $g \in A_n$, pak $gA_n = A_ng = A_n$ (Obecně zřejmě platí, že $gH = H$ právě když $Hg = H$ právě když $g \in H$). Pokud $g \notin A_n$, pak $gA_n = S_n \setminus A_n$. Analogicky $A_ng = S_n \setminus A_n$. Tedy levá a pravá rozkladová třída libovolného prvku $g \in S_n$ podle A_n splývají.

2. Nechť $\mathcal{G} = S_n$ a $\mathcal{H} = F_n \cong S_{n-1}$ (viz 1.17). Pak pro $g \in S_n$ je $gF_n = \{f \in S_n \mid f(n) = g(n)\}$, zatímco $F_ng = \{f \in S_n \mid f^{-1}(n) = g^{-1}(n)\}$. Tyto rozkladové třídy obecně nesplývají.

Obecně je tedy nutné rozlišovat mezi levými a pravými rozkladovými třídami. Jak ale uvidíme za chvíli, počet levých a pravých rozkladových tříd je vždy stejný.

Lemma 1.25. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $g, g' \in \mathcal{G}$ a $\mathcal{H} \leq \mathcal{G}$. Potom buď $gH = g'H$ nebo $gH \cap g'H = \emptyset$ (a $gH = g'H$ právě když $g'^{-1} \odot g \in H$).*

Důkaz. Nechť $gH \cap g'H \neq \emptyset$ a $x \in gH \cap g'H$. Pak $x = g \odot h = g' \odot h'$, a tedy $g'^{-1} \odot g \in H$, což je ekvivalentní s $g^{-1} \odot g' \in H$. Protože $g = g' \odot g'^{-1} \odot g$, podmínka $g'^{-1} \odot g \in H$ implikuje $gH = L_g(H) \subseteq L_{g'}(H) = g'H$, a podobně $g'H \subseteq gH$. Naopak, $gH = g'H$ zřejmě implikuje $g'^{-1} \odot g \in H$, a tedy $gH \cap g'H \neq \emptyset$. □

Důsledek 1.26. *Ze souboru $\{gH \mid g \in G\}$ všech levých rozkladových tříd $\mathcal{G}$ podle $\mathcal{H}$ lze vybrat disjunktní rozklad množiny G. Tento rozklad se nazývá* levý rozklad *$\mathcal{G}$ podle $\mathcal{H}$. Jeho systém reprezentantů se nazývá* levá transverzála *grupy $\mathcal{G}$ podle $\mathcal{H}$. Analogicky definujeme pravý rozklad a pravou transverzálu $\mathcal{G}$ podle $\mathcal{H}$.*

Všimněme si, že všechny třídy levého (resp. pravého) rozkladu $\mathcal{G}$ podle $\mathcal{H}$ mají stejnou mohutnost, protože pro každé $g \in G$ je levá translace L_g, zúžená na H, bijekcí H na gH (resp. pravá translace P_g, zúžená na H, je bijekcí H na Hg). Navíc množina $H = eH = He$ je třídou levého i pravého rozkladu $\mathcal{G}$ podle $\mathcal{H}$.

Příklad 1.27. V příkladu 1.24.1 je $\{A_n, S_n \setminus A_n\}$ levý i pravý rozklad S_n podle A_n.

Lemma 1.28 (o indexu)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $\mathcal{H} \leq \mathcal{G}$. Potom mohutnost libovolné levé a libovolné pravé transverzály je stejná. Tato mohutnost se nazývá index $\mathcal{H}$ v $\mathcal{G}$ a značí se $[G : H]$.*

Důkaz. Nechť L je libovolná levá transverzála $\mathcal{G}$ podle $\mathcal{H}$. Stačí dokázat, že $P = \{g^{-1} \mid g \in L\}$ je pravou transverzálou.

Disjunktnost: Nechť $g, g' \in L$. Pak $Hg^{-1} \cap Hg'^{-1} = \emptyset$. Jinak existuje $x \in G$ tvaru $x = h \odot g^{-1} = h' \odot g'^{-1}$, kde $h, h' \in H$. Pak ale $x^{-1} = g \odot h^{-1} = g' \odot h'^{-1}$, a tedy $gH = g'H$, ve sporu s tím, že L je levá transverzála.

Pokrývání: Nechť $x \in G$. Pak $x^{-1} \in G$, a tedy $x^{-1} \in \bigcup_{g \in L} gH$, a existují $g_o \in L$ a $h \in H$ tak, že $x^{-1} = g_o \odot h$. Pak $x = h^{-1} \odot g_o^{-1}$ a $x \in Hg_o^{-1}$. Tím je dokázáno, že $\bigcup_{g \in L} Hg^{-1} = G$. □

Věta 1.29 (Lagrange)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $\mathcal{H} \leq \mathcal{G}$. Pak $|G| = |H| \cdot [G : H]$.*

Důkaz. Nechť L je levá transverzála $\mathcal{G}$ podle $\mathcal{H}$. Pak G je disjunktním sjednocením rozkladových tříd gH ($g \in L$). Jelikož $gH = L_g(H)$ a L_g je bijekce, je $|gH| = |H|$ a tudíž $|G| = |H| \cdot |L| = |H| \cdot [G : H]$ podle 1.28. □

Poznámka 1.30. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $(H_i \mid i \in I)$ je libovolný systém jejích podgrup. Pak $\bigcap_{i \in I} H_i$ je zřejmě podgrupou v $\mathcal{G}$.

Nechť X je neprázdná podmnožina G. Pak $\langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$ se nazývá *podgrupa generovaná* X v $\mathcal{G}$. Zřejmě $\langle X \rangle = X$ právě když $X \leq G$. Snadno se ověří, že

$$\langle X \rangle = \{x_1 \odot x_2 \odot \cdots \odot x_n \mid n < \omega,\, x_i \in X \cup X^{-1}\, (i \leq n)\},$$

kde $X^{-1} = \{g^{-1} \mid g \in X\}$: množina M na pravé straně rovnosti je totiž nosičem podgrupy v $\mathcal{G}$ obsahující X, a každá podgrupa $H \leq G$ obsahující X musí jistě obsahovat i M.

Definice 1.31. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, pak mohutnost $|G|$ se nazývá *řádem grupy* $\mathcal{G}$. Pro $g \in G$ se $\langle g \rangle$ nazývá *cyklickou grupou* generovanou g a $|\langle g \rangle|$ se nazývá *řádem prvku* g v $\mathcal{G}$; značíme jej $o(g)$. Je-li $\mathcal{G}$ konečná grupa, pak podle Lagrangeovy věty řád libovolného jejího prvku dělí řád grupy $\mathcal{G}$.

Lagrangeova věta je jednoduchým, ale velmi účinným nástrojem pro zkoumání struktury podgrup konečných grup. Například je-li $\mathcal{G}$ grupou prvočíselného řádu, má podle Lagrangeovy věty $\mathcal{G}$ pouze triviální podgrupy, a $\mathcal{G}$ je tedy cyklická, generovaná libovolným svým prvkem $g \neq e$.

Poznámka 1.32. Z 1.30 plyne, že $\langle g \rangle = \{g^z \mid z \in \mathbb{Z}\}$, kde definujeme $g^0 = e$, $g^n = \underbrace{g \odot \cdots \odot g}_{n}$ pro $n > 0$, a $g^n = \underbrace{g^{-1} \odot \cdots \odot g^{-1}}_{-n}$ pro $n < 0$. Pokud je řád prvku g *konečný* (tedy $|\langle g \rangle| = m$ pro nějaké $m < \omega$), potom zřejmě $\langle g \rangle = \{g^k \mid k \in \{0, 1, \ldots, m-1\}\}$, kde m je nejmenší přirozené číslo takové, že $g^m = e$.

Věta 1.33 (Poincaré)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $H_1, \ldots, H_n$ jsou podgrupy v $\mathcal{G}$ konečného indexu. Potom průnik $\bigcap_{i=1}^n H_i$ je podgrupa konečného indexu, a platí $[G : \bigcap_{i=1}^n H_i] \leq [G : H_1] \cdots [G : H_n]$.*

Důkaz. Tvrzení stačí dokázat pro $n = 2$, pro $n > 2$ pak snadno plyne indukcí.

Nejprve dokážeme, že pro libovolné $g \in G$ platí $g(H_1 \cap H_2) = gH_1 \cap gH_2$. Inkluze $\subseteq$ je zřejmá. Naopak, je-li $x \in gH_1 \cap gH_2$, pak $x = g \odot h_1 = g \odot h_2$ pro nějaká $h_1 \in H_1$ a $h_2 \in H_2$. Pak ale $h_1 \in H_1 \cap H_2$, a tedy $x \in g(H_1 \cap H_2)$.

Nyní definujme zobrazení φ z množiny všech levých rozkladových tříd podle $H_1 \cap H_2$ do množiny všech dvojic levých rozkladových tříd podle H_1 a levých rozkladových tříd podle H_2

následovně: $\varphi(g(H_1 \cap H_2)) = (gH_1, gH_2)$. Toto zobrazení je korektně definované, neboť pro libovolná $g, g' \in G$ taková, že $g(H_1 \cap H_2) = g'(H_1 \cap H_2)$ platí podle 1.25 $(g')^{-1} \odot g \in H_1 \cap H_2$, a tedy $gH_1 = g'H_1$ a $gH_2 = g'H_2$. Protože $g(H_1 \cap H_2) = gH_1 \cap gH_2$, je φ prosté, a tedy $[G : (H_1 \cap H_2)] \leq [G : H_1] \cdot [G : H_2]$. □

Příklad 1.34. $\mathcal{G} = (\mathbb{Z}, +, -, 0)$ je grupa celých čísel. Pro $n \in \mathbb{N}$ definujme podgrupu $H_n = \langle 2^n \rangle = \{z \cdot 2^n \mid z \in \mathbb{Z}\}$. Pak zřejmě $[G : H_n] = 2^n$, čili H_n je podgrupou konečného indexu v G. Podgrupa $H = \bigcap_{n<\infty} H_n = \{0\}$ má nekonečný index $[G : H] = |\mathbb{Z}|$. Větu 1.33 tedy nelze obecně rozšířit na nekonečné průniky.

Jedním ze základních způsobů konstrukce nových grup je faktorizace podle podgrup. Faktorizace je zobecněním konstrukce grupy $\mathbb{Z}_n$ (zbytkových tříd modulo n) z grupy $\mathbb{Z}$: $\mathbb{Z}_n$ je izomorfní faktoru grupy $\mathbb{Z}$ podle její cyklické podgrupy $\mathbb{Z}n = \{z.n \mid z \in \mathbb{Z}\}$. Jak uvidíme dále, obecně nelze faktorizovat podle každé podgrupy, ale jenom podle podgrupy, která je normální, tj. invariantní na všechny vnitřní automorfismy:

Definice 1.35. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $g \in \mathcal{G}$. Zobrazení $(\ )^g : G \to G$ takové, že $h \mapsto g \odot h \odot g^{-1}$ se nazývá *vnitřní automorfismus* $\mathcal{G}$ určený g. Platí, že $(\ )^{g^{-1}} \circ (\ )^g = (\ )^g \circ (\ )^{g^{-1}} = \mathrm{id}_G$ a $(\ )^g(h \odot h') = (\ )^g(h) \odot (\ )^g(h')$, tedy $(\ )^g$ je grupový izomorfismus. Prvek $(h)^g = g \odot h \odot g^{-1}$ se nazývá *konjugovaný* v $\mathcal{G}$ s prvkem h pomocí g.

Definice 1.36. Podgrupa $\mathcal{H} \leq \mathcal{G}$ se nazývá *normální* v $\mathcal{G}$ pokud H je invariantní na všechny vnitřní automorfismy určené prvky $g \in G$, tj. pokud pro každá $h \in H$, $g \in G$ platí $g \odot h \odot g^{-1} \in H$. Skutečnost, že podgrupa $\mathcal{H}$ je normální podgrupou v $\mathcal{G}$, značíme $\mathcal{H} \trianglelefteq \mathcal{G}$ resp. $H \trianglelefteq G$.

Příklad 1.37.
(1) Triviální podgrupy jsou zřejmě normální.
(2) $A_n \trianglelefteq S_n$, neboť znamení permutace se zachovává vnitřními automorfismy. Podobně každá podgrupa H grupy G taková, že $[G : H] = 2$ je normální – pak totiž $\{H, G \setminus H\}$ je levým i pravým rozkladem G podle H a normalita plyne z následujícího lemmatu 1.39.
(3) $F_n \not\trianglelefteq S_n$ pro $n \geq 3$, kde $F_n = \{f \in S_n \mid f(n) = n\}$, neboť F_n není invariantní na vnitřní automorfismus určený transpozicí prvků 1 a n.
(4) Je-li $\mathcal{G}$ komutativní, pak zřejmě každá podgrupa $\mathcal{G}$ je normální.

Lemma 1.38. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$, $\mathcal{G}' = (G', \odot', ^{-1'}, e')$ jsou grupy a $\varphi : G \mapsto G'$ je grupový homomorfismus. Pak pro jádro homomorfismu φ platí $\mathrm{Ker}\,\varphi \trianglelefteq G$.*

Důkaz. Podle 1.21 je $\mathrm{Ker}\,\varphi = \{g \in G \mid \varphi(g) = e'\} \leq G$. Navíc pro $h \in \mathrm{Ker}\,\varphi$ a $g \in G$ máme $\varphi(g \odot h \odot g^{-1}) = \varphi(g) \odot' \varphi(h) \odot' \varphi(g^{-1}) = \varphi(g) \odot' e' \odot' (\varphi(g))^{-1} = e'$, a tedy $\mathrm{Ker}\,\varphi \trianglelefteq G$. □

Lemma 1.39. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $H \leq G$. Pak $H \trianglelefteq G$ právě když levý a pravý rozklad $\mathcal{G}$ podle $\mathcal{H}$ splývají.*

Důkaz. Je-li H normální v G, pak pro každé $g \in G$ je $gH \subseteq Hg$, a tedy i $g^{-1}H \subseteq Hg^{-1}$, $Hg \subseteq gH$, a $gH = Hg$. Tedy levá a pravá rozkladová třída libovolného prvku $g \in G$ podle H splývají, a totéž platí i pro levý a pravý rozklad G podle H.

Naopak, pokud rozklady splývají a $g \in G$, pak $gH = Hg$, neboť $g \in gH \cap Hg$, a $H \trianglelefteq G$. □

Definice 1.40. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $H \trianglelefteq G$. Označme G/H množinu všech rozkladových tříd grupy $\mathcal{G}$ podle $\mathcal{H}$. Na G/H definujeme operace $\bar{\odot}$ $^{\bar{-1}}$, $\bar{e}$ pomocí grupových operací na reprezentantech: $gH \,\bar{\odot}\, g'H = (g \odot g')H$, $(gH)^{\bar{-1}} = g^{-1}H$ a $\bar{e} = eH = H$.

Potom $\mathcal{G}/\mathcal{H} = (G/H, \bar{\odot}, ^{\bar{-1}}, \bar{e})$ je grupa, nazývaná *faktorovou grupou* grupy $\mathcal{G}$ podle $\mathcal{H}$.

Vzhledem k tomu, že grupové operace na G/H jsou definovány pomocí grupových operací v G na reprezentantech rozkladových tříd, stačí k ověření faktu, že $\mathcal{G}/\mathcal{H}$ je grupa, ověřit nezávislost na volbě reprezentantů. K té stačí normalita H v G – např. pro binární operaci máme: $g_1H = g_2H$ a $g_1'H = g_2'H$ implikuje $(g_1 \odot g_1')H = g_1(g_1'H) = g_1(g_2'H) = (g_1H)g_2' = (g_2H)g_2' = g_2(g_2'H) = (g_2 \odot g_2')H$.

Příklad 1.41. Nechť $\mathcal{G} = (\mathbb{Z}, +, -, 0)$, $H = \mathbb{Z}n = \{z \cdot n \mid z \in \mathbb{Z}\}$ pro libovolné $n \in \mathbb{N}$. Pak $H \trianglelefteq G$ a $(G/H, \bar{+}; \bar{-}, \bar{0})$ je izomorfní grupě $\mathbb{Z}_n$ všech zbytkových tříd celých čísel modulo n.

Lemma 1.42. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $H \trianglelefteq G$. Definujme $\pi_H \colon G \to G/H$ tak, že $g \mapsto gH$. Pak π_H je grupový homomorfismus. Dále $Im\, \pi_H = G/H$ a $Ker\, \pi_H = H$.*

Důkaz. To, že π_H je grupový homomorfismus, plyne podle 1.20 z identity $\pi_H(g) \bar{\odot} \pi_H(g') = gH \bar{\odot} g'H = (g \odot g')H = \pi_H(g \odot g')$ pro každá $g, g' \in G$. Dále $G/H = \{gH \mid g \in G\} = \mathrm{Im}\, \pi_H$, a $\mathrm{Ker}\, \pi_H = \{g \in G \mid \pi_H(g) = H\} = \{g \in G \mid gH = H\} = H$. □

Definice 1.43. Homomorfismus π_H z lemmatu 1.42 se nazývá *kanonická projekce* grupy $\mathcal{G}$ podle podgrupy $\mathcal{H}$.

Každá normální podgrupa je tedy jádrem aspoň jednoho homomorfismu (a naopak, jádro každého homomorfismu z $\mathcal{G}$ je normální podgrupou v $\mathcal{G}$ podle 1.38). Následující věta ukazuje důležitou vlastnost kanonické projekce:

Věta 1.44 (o homomorfismu pro grupy)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ a $\mathcal{G}' = (G', \odot', ^{-1'}, e')$ jsou grupy, $H \trianglelefteq G$ a $\varphi \colon G \to G'$ je grupový homomorfismus takový, že $H \leq Ker\, \varphi$. Pak existuje jednoznačně určený grupový homomorfismus $\psi \colon G/H \to G'$ takový, že $\psi \circ \pi_H = \varphi$.*

Důkaz. Definujme $\psi \colon G/H \to G'$ tak, že $gH \mapsto \varphi(g)$. Tato definice je korektní, neboť $g_1H = g_2H$ implikuje $g_2^{-1} \odot g_1 \in H \subseteq \mathrm{Ker}\, \varphi$, a tedy $\varphi(g_2^{-1} \odot g_1) = e'$ a $\varphi(g_1) = \varphi(g_2)$.

ψ je grupový homomorfismus podle 1.20, neboť $\psi(g_1H \bar{\odot} g_2H) = \psi((g_1 \odot g_2)H) = \varphi(g_1 \odot g_2) = \varphi(g_1) \odot' \varphi(g_2) = \psi(g_1H) \odot' \psi(g_2H)$. Pro každé $g \in G$ navíc platí $(\psi\pi_H)(g) = \psi(gH) = \varphi(g)$, tj. $\psi \circ \pi_H = \varphi$.

Konečně, je-li $\eta \colon G/H \to G'$ takový, že $\eta \circ \pi_H = \varphi$, pak pro každé $g \in G$ je $(\eta\pi_H)(g) = \eta(gH) = \varphi(g)$, a $\eta = \psi$. □

Poznámka 1.45. Je-li $\mathcal{G}$ grupa a $\mathcal{H}$ je její normální podgrupa, pak kanonická projekce indukuje izomorfismus množiny všech podgrup K grupy G obsahujících H (částečně uspořádané inkluzí) na množinu všech podgrup faktorové grupy G/H (částečně uspořádané inkluzí) pomocí zobrazení $K \mapsto \pi_H(K) = \{kH \mid k \in K\}$. Přitom $K \trianglelefteq G$ právě když $\pi_H(K) \trianglelefteq G/H$.

Nyní dokážeme klasické věty o izomorfismu pocházející od Emmy Noether:

Věta 1.46 (1. věta o izomorfismu pro grupy)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$, $\mathcal{G}' = (G', \odot', ^{-1'}, e')$ jsou grupy a $\varphi \colon G \to G'$ je grupový homomorfismus. Potom $G/Ker\, \varphi \simeq Im\, \varphi$.*

Důkaz. Podle 1.44 existuje grupový homomorfismus $\psi \colon G/\mathrm{Ker}\, \varphi \to G'$ definovaný vztahem $g(\mathrm{Ker}\, \varphi) \mapsto \varphi(g)$. Zřejmě ψ je prostý a $\mathrm{Im}\, \psi = \mathrm{Im}\, \varphi$, tedy zobrazení $\xi : G/\mathrm{Ker}\, \varphi \to \mathrm{Im}\, \varphi$ definované vztahem $g\mathrm{Ker}\, \varphi \mapsto \varphi(g)$ je grupový izomorfismus. □

Důsledek 1.47. *Nechť $\mathcal{G}$ je grupa. Pak $\mathcal{G}$ je cyklická grupa právě když $\mathcal{G}$ je izomorfní grupě $\mathbb{Z}$ nebo grupě $\mathbb{Z}_n$ pro nějaké $n \geq 1$.*

Důkaz. Grupy $\mathbb{Z}$ a $\mathbb{Z}_n$ ($n \geq 1$) jsou zřejmě cyklické.

Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je cyklická, tj. existuje $g \in G$ takové, že $\mathcal{G} = \langle g \rangle = \{g^z \mid z \in \mathbb{Z}\}$ (g^z je definované v 1.32). Definujme $\varphi\colon \mathbb{Z} \to G$ vztahem $z \mapsto g^z$. Toto zobrazení je homomorfismus grupy $\mathbb{Z}$ na grupu $\mathcal{G}$ neboť $g^{z_1+z_2} = g^{z_1} \odot g^{z_2}$. Použitím Věty 1.46 dostáváme $\mathbb{Z}/\mathrm{Ker}\ \varphi \simeq \mathrm{Im}\ \varphi = G$. Rozlišíme dva případy.

(1) $\mathrm{Ker}\ \varphi = \{0\}$. Pak $G \simeq \mathbb{Z}$, $\mathcal{G}$ je nekonečná grupa a každý prvek G se dá právě jedním způsobem vyjádřit ve tvaru g^z.
(2) $\mathrm{Ker}\ \varphi \neq \{0\}$. Pak existuje nejmenší $n \geq 1$ takové, že $g^n = e$ a $\mathrm{Ker}\ \varphi = \mathbb{Z}n = \{z{\cdot}n \mid z \in \mathbb{Z}\} \leq \mathbb{Z}$, takže $G \simeq \mathbb{Z}/\mathbb{Z}n \simeq \mathbb{Z}_n$. Tedy $\mathcal{G}$ je konečná grupa řádu $|\ G\ | = o(g) = |\langle g \rangle| = n$.

□

Věta 1.48 (2. věta o izomorfismu pro grupy)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $H \trianglelefteq G$, $K \trianglelefteq G$ a $K \leq H$. Pak $(G/K)/(H/K) \simeq G/H$.*

Důkaz. Definujme zobrazení $\varphi\colon G/K \to G/H$ vztahem $gK \mapsto gH$. To je korektní definice, neboť $gK = g'K$ implikuje ${g'}^{-1} \odot g \in K \subseteq H$, a tedy $gH = g'H$. Navíc φ je grupový homomorfismus, neboť $\varphi(gK \mathbin{\bar{\odot}} g'K) = \varphi((g \odot g')K) = (g \odot g')H = gH \mathbin{\bar{\odot}} g'H = \varphi(gK) \mathbin{\bar{\odot}} \varphi(g'K)$. Zřejmě φ zobrazuje na G/H. Podle 1.38 a 1.46 máme $\mathrm{Ker}\ \varphi \trianglelefteq G/K$ a $(G/K)/\mathrm{Ker}\ \varphi \simeq \mathrm{Im}\ \varphi$. Nicméně $\mathrm{Ker}\ \varphi = \{gK \mid gH = H\} = \{gK \mid g \in H\} = H/K$, takže $(G/K)/(H/K) \simeq G/H$. □

Důsledek 1.49. *Nechť $\mathcal{G}$ je cyklická grupa, $H \leq G$, $\varphi\colon G \to G'$ je grupový homomorfismus na. Pak $\mathcal{H}$ i $\mathcal{G}'$ jsou cyklické grupy.*

Důkaz. Podle 1.47 je G homomorfním obrazem grupy $\mathbb{Z}$, tedy také G' je homomorfním obrazem grupy $\mathbb{Z}$, a proto G' je cyklická.

Je-li $G \cong \mathbb{Z}$, je H izomorfní podgrupě K v $\mathbb{Z}$. Je-li K nenulová podgrupa v $\mathbb{Z}$, pak K je generována svým nejmenším prvkem $0 < n \in K$, a tedy $K = \mathbb{Z}n \cong \mathbb{Z}$ je nekonečná cyklická a totéž platí pro grupu H. Jinak $K = \{0\}$, tj. $H = \{e\}$.

Je-li $G \simeq \mathbb{Z}_n = \mathbb{Z}/\mathbb{Z}n$ pro nějaké $n \geq 1$, pak podle 1.45 je H izomorfní grupě $K/\mathbb{Z}n$, kde K je podgrupa v $\mathbb{Z}$ obsahující $\mathbb{Z}n$. Pak $K = \mathbb{Z}m$, kde m je přirozené číslo dělící n, tedy existuje přirozené číslo p tak, že $n = m.p$, a $H \cong \mathbb{Z}m/\mathbb{Z}n \cong \mathbb{Z}_p$ (poslední izomorfismus je dán přiřazením $m + \mathbb{Z}n \mapsto 1 + \mathbb{Z}p$). □

Poznámka 1.50. Nechť $\mathcal{H}$, $\mathcal{K}$ jsou podgrupy grupy $\mathcal{G} = (G, \odot, ^{-1}, e)$. Definujeme $HK \overset{def.}{=} \{h \odot k \mid h \in H,\ k \in K\}$. Zřejmě HK obsahuje množiny H i K, obecně ale HK nemusí být nosičem podgrupy v G. Je tomu tak ale v následující větě, která je základním nástrojem pro zkoumání řetězců podgrup v grupách (tzv. Jordan–Hölderovy teorie):

Věta 1.51 (3. věta o izomorfismu pro grupy)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $H \trianglelefteq G$ a $K \leq G$. Pak $HK = KH$ je nosičem nejmenší podgrupy v $\mathcal{G}$ obsahující H i K, $(H \cap K) \trianglelefteq K$, a platí grupový izomorfismus $(HK)/H \simeq K/(H \cap K)$.*

Důkaz. Jelikož $H \trianglelefteq G$, dostáváme podle 1.39, že pro každé $g \in G$ je $gH = Hg$, a tedy $HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$.

Dokážeme, že HK je podgrupa v $\mathcal{G}$ (pak je HK zřejmě nejmenší ze všech podgrup obsahujících H i K): máme $e \odot e = e \in HK$, a je-li $(h \odot k) \in HK$ a $(h' \odot k') \in HK$, pak $(h \odot k) \odot (h' \odot k') = h \odot (k \odot h') \odot k'$ a jelikož $k \odot h' \in HK = KH$, existuje $h'' \in H$ takové, že

$k \odot h' = h'' \odot k$, tedy $(h \odot k) \odot (h' \odot k') = \underbrace{(h \odot h'')}_{\in H} \odot \underbrace{(k \odot k')}_{\in K} \in HK$. Dále, je-li $(h \odot k) \in HK$, pak $(h \odot k)^{-1} \in HK$, neboť $(h \odot k)^{-1} = k^{-1} \odot h^{-1} \in KH = HK$.

Nyní definujme zobrazení $\varphi\colon K \to (HK)/H$ vztahem $k \mapsto kH$. φ je grupový homomorfismus na HK/H neboť $\varphi(k \odot k') = (k \odot k')H = kH \,\bar{\odot}\, k'H = \varphi(k) \,\bar{\odot}\, \varphi(k')$. Jeho jádrem je $\operatorname{Ker}\varphi = \{k \in K \mid kH = H\} = \{k \in K \mid k \in H\} = K \cap H$. Tedy $K \cap H \trianglelefteq K$, a užitím 1.46 dostáváme $K/(K \cap H) \simeq HK/H$. □

1.3. **Působení grup na množinách.** Podle Cayleyho věty 1.22 si lze (až na izomorfismus) každou grupu představit jako grupu tvořenou permutacemi. Tato prezentace vychází z přiřazení $g \mapsto L_g$, kde L_g je levá translace určená prvkem g. Je jedním z příkladů pojmu akce grupy na množině:

Definice 1.52. Nechť $\mathcal{G}$ je grupa a X je neprázdná množina. Grupový homomorfismus ϕ z grupy $\mathcal{G}$ do symetrické grupy $\mathcal{S}(X)$ nazýváme *akcí (nebo působením) grupy $\mathcal{G}$ na množině X.*

Jiným příkladem je akce grupy $\mathcal{G}$ na sobě pomocí vnitřních automorfismů: $\phi : G \to S(G)$ je definováno vztahem $g \mapsto (\,)^g$. Dalším důležitým příkladem je lineární reprezentace grupy $\mathcal{G}$ (kde $\mathcal{G}$ působí na vektorovém prostoru pomocí jeho automorfismů - viz. následující sekci).

S akcí grupy na množině je přirozeně spojeno několik dalších pojmů:

Definice 1.53. Nechť $\mathcal{G}$ je grupa, X je neprázdná množina a ϕ je akce $\mathcal{G}$ na X.

Orbitou prvku $x \in X$ vzhledem k ϕ rozumíme množinu $O_x = \{(\phi(g))(x) \mid g \in G\} \subseteq X$. Protože ϕ je grupový homomorfismus, můžeme na X zavést ekvivalenci $\sim$ vztahem $x_1 \sim x_2 \overset{def}{\iff} \exists\, g \in G\colon x_2 = \phi(g)(x_1)$. Orbity pak odpovídají rozkladovým třídám ekvivalence $\sim$.

Stabilizátorem prvku $x \in X$ vhledem k ϕ rozumíme množinu $C_x = \{g \in G \mid (\phi(g))(x) = x\}$. Protože ϕ je grupový homomorfismus, je C_x nosičem podgrupy v $\mathcal{G}$.

V případě akce grupy $\mathcal{G}$ na sobě pomocí levých translací je orbitou libovolného prvku $h \in \mathcal{G}$ celá množina G a jeho stabilizátorem je triviální grupa $\{e\}$.

V případě akce grupy $\mathcal{G}$ na sobě pomocí vnitřních automorfismů je situace mnohem zajímavější, orbity prvků mohou být různě veliké. Tomuto případu se budeme podrobněji věnovat dále.

Nejprve ale dokážeme následující obecnou větu:

Věta 1.54. *Nechť $\mathcal{G}$ je grupa, X je neprázdná množina, ϕ je akce $\mathcal{G}$ na X a $x \in X$. Pak velikost orbity prvku x je rovna indexu jeho stabilizátoru, tj. $[G : C_x] = |O_x|$.*

Důkaz. Definujme zobrazení φ:

$$\begin{aligned} \varphi\colon O_x &\to \text{levé rozkladové třídy podle } C_x \\ \phi(g)(x) &\mapsto gC_x \end{aligned}$$

Podle 1.28 stačí dokázat, že φ je bijekce:

(1) φ je korektní. Nechť $g, g' \in G$ jsou taková, že $\phi(g)(x) = \phi(g')(x)$. Pak $(\phi(g'^{-1}) \circ \phi(g))(x) = x$, odkud $\phi(g'^{-1} \odot g)(x) = x$, $g'^{-1} \odot g \in C_x$, a $gC_x = g'C_x$.

(2) φ je prosté. To plyne obrácením předchozí úvahy: z $gC_x = g'C_x$ naopak plyne $(\phi(g'^{-1}) \circ \phi(g))(x) = x$, a $\phi(g)(x) = \phi(g')(x)$.

(3) φ je na: probíhá-li g celé G, pak gC_x zřejmě probíhá všechny levé rozkladové třídy G podle C_x.

□

Jako aplikaci Věty 1.54 uvedeme tzv. *Bursideovo lemma* pro počet orbit akce grupy na množině:

Důsledek 1.55. *Nechť $\mathcal{G}$ je konečná grupa, X je neprázdná množina a ϕ je akce $\mathcal{G}$ na X. Pro každé $g \in G$ označme $F_g = \{x \in X \mid \phi(g)(x) = x\}$. Pak pak počet orbit akce ϕ na X je roven*

$$\frac{1}{|G|}\sum_{g\in G}|F_g|\,.$$

Důkaz. Počet všech dvojic (g, x) takových, že $\phi(g)(x) = x$, můžeme vyjádřit dvojím způsobem: jako $\sum_{g\in G}|F_g|$ nebo jako $\sum_{x\in X}|C_x|$. Druhé vyjádření je podle Vět 1.29 a 1.54 též rovno $\sum_{x\in X}\frac{|G|}{[G:C_x]} = \sum_{x\in X}\frac{|G|}{|O_x|}$. Tedy

$$\frac{1}{|G|}\sum_{g\in G}|F_g| = \sum_{x\in X}\frac{1}{|O_x|} = \sum_{x\in R_1}\frac{1}{|O_x|} + \cdots + \sum_{x\in R_k}\frac{1}{|O_x|} = \underbrace{1+\cdots+1}_{k\times} = k,$$

kde $R_1, \ldots, R_k$ jsou orbity akce ϕ na X. □

Až do konce této sekce se omezíme na akce grup na sobě pomocí vnitřních automorfismů, tj. $\phi : G \to S(G)$ bude definováno vztahem $g \mapsto ()^g$. Zřejmě $h \in G$ má v této akci jednoprvkovou orbitu právě když pro každé $g \in G$ je $g \odot h = h \odot g$, tj. h je prvkem centra grupy G ve smyslu následující definice:

Definice 1.56. *Centrem* grupy $\mathcal{G}$ rozumíme množinu $\{h \in G \mid \forall\, g \in G\colon g \odot h = h \odot g\}$, tj. množinu všech prvků G, které komutují s každým prvkem grupy G. Centrum grupy $\mathcal{G}$ budeme značit $Z(G)$.

Lemma 1.57. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa. Pak $Z(G) \trianglelefteq G$.*

Důkaz. Zřejmě $e \in Z(G)$ a $Z(G)$ je uzavřené na $\odot$. Je-li $g \in Z(G)$, pak $g^{-1}\odot h = (h^{-1} \odot g)^{-1} = (g \odot h^{-1})^{-1} = h \odot g^{-1}$, takže $g^{-1} \in Z(G)$. Tedy $Z(G)$ je podgrupa v $\mathcal{G}$.

Zbývá dokázat, že $Z(G)$ je normální podgrupou v G. Nechť $g \in Z(G)$ a $h \in G$. Pak $h \odot g \odot h^{-1} = h \odot h^{-1} \odot g = e \odot g = g$, tj. $h \odot g \odot h^{-1} \in Z(G)$, a $Z(G)$ je invariantní na vnitřní automorfismy grupy $\mathcal{G}$. □

Poznámka 1.58. Zřejmě grupa $\mathcal{G}$ je komutativní právě když $Z_1 = Z(G) = G$. Je-li $Z(G)$ netriviální podgrupou v G, můžeme podle 1.57 vytvořit faktorovou grupu $G/Z(G)$ a určit její centrum: podle 1.45 je tvaru Z_2/Z_1 kde Z_2 je normální podgrupa G obsahující Z_1. Je-li $Z_1 \neq Z_2 \neq G$, můžeme pokračovat analogicky.

Grupy, pro které existuje přirozené číslo $n > 0$ takové, že $Z_n = G$ se nazývají *nilpotentní*. Nejmenší takové n se nazývá *stupeň nilpotence* grupy $\mathcal{G}$ a řada $\{e\} = Z_0 \leq Z_1 \leq Z_2 \leq \cdots \leq Z_n = G$ je *horní centrální řada* grupy $\mathcal{G}$.

Komutativní grupy jsou tedy právě grupami stupně nilpotence 1.

Je-li $\mathcal{G} = (G, \odot, ^{-1}, e)$ grupa, pak se její nosič dá napsat jako disjunktní sjednocení následujícím způsobem $G = Z(G) \cup^{disj.} \bigcup_{h\in I}^{disj.} O_h$, kde I je množina reprezentantů alespoň dvouprvkových orbit grupy $\mathcal{G}$. Z 1.54 máme okamžitý důsledek:

Důsledek 1.59. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je konečná grupa. Pak $|G| = |Z(G)| + \sum_{h\in I}[G : C_h]$, kde I je množina reprezentantů alespoň dvouprvkových orbit grupy $\mathcal{G}$.*

Konečná grupa může obecně mít triviální centrum - to je případ symetrické grupy S_n pro $n \geq 3$, a též každé jednoduché konečné nekomutativní grupy (viz dále Příklad 1.70). Naopak, pro p prvočíslo má každá konečná p-grupa netriviální centrum, a tedy je nilpotentní:

Důsledek 1.60. *Nechť p je prvočíslo.*

(1) *(Burnside) Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je p-grupa (tj. G je řádu $|G| = p^n$ pro nějaké $0 < n \in \mathbb{N}$). Pak $|Z(G)| > 1$.*
(2) *Každá konečná p-grupa je nilpotentní.*

Důkaz. (1) Předpokládejme, že $|Z(G)| = 1$. Z 1.57 a 1.29 plyne, že pro libovolné $h \in G$, $h \neq e$ platí, že $[G : C_h] \mid |G| = p^n$. Pak $[G : C_h] = p^{n_h}$ pro nějaké $1 \leq n_h < n$. Pak podle 1.59 $p^n = 1 + \sum_{h\in I}[G : C_h] = 1 + \sum_{h\in I} p^{n_h}$. To je spor, protože jak levá strana, tak i suma na pravé straně, jsou dělitelné p, ale $p \nmid 1$. Tedy $|Z(G)| > 1$. (2) Plyne z (1) podle Poznámky 1.58. □

Definice 1.61. *Součinem* konečně mnoha grup $\mathcal{G}_i = (G, \odot_i, ^{-1_i}, e_i)$ $(1 \leq i \leq m)$ rozumíme grupu $\mathcal{G}_1 \times \cdots \times \mathcal{G}_m$, jejímž nosičem je kartézský součin nosičů $G_1 \times \cdots \times G_m$, s grupovými operacemi definovanými po složkách: $(g_1, \ldots, g_m) \odot (g'_1, \ldots, g'_m) = (g_1 \odot_1 g'_1, \ldots, g_m \odot_m g'_m)$, $(g_1, \ldots, g_m)^{-1} = (g_1^{-1}, \ldots, g_m^{-1})$ a $e = (e_1, \ldots, e_m)$.

Pro každé $1 \leq i \leq m$ je grupa $\mathcal{G}_i$ izomorfní podgrupě $\mathcal{G}'_i$ v $\mathcal{G}$ s nosičem G'_i tvořeným všemi prvky tvaru $(e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n)$, kde $g_i \in G_i$. Tedy také $\mathcal{G} \cong \mathcal{G}'_1 \times \cdots \times \mathcal{G}'_m$. Podgrupy $\mathcal{G}'_i$ $(1 \leq i \leq m)$ spolu komutují (tj. $g'_i \odot g'_j = g'_j \odot g'_i$ pro každé $i \neq j \leq m$, $g'_i \in G'_i$ a $g'_j \in G'_j$), a každý prvek $g \in G$ lze jednoznačně vyjádřit jako součin $g = g'_1 \odot \cdots \odot g'_m$ kde $g'_i \in G'_i$ pro $1 \leq i \leq m$.

Posledně zmíněná vlastnost charakterizuje konečné součiny grup: je-li $\mathcal{G} = (G, \odot, ^{-1}, e)$ grupa a $\mathcal{H}_i$ $(1 \leq i \leq n)$ jsou její komutující podgrupy takové, že každý prvek $g \in G$ lze jednoznačně vyjádřit jako součin $g = h_1 \odot \cdots \odot h_n$ kde $h_i \in H_i$ pro každé $1 \leq i \leq n$, pak $\mathcal{G} \overset{\varphi}{\cong} \mathcal{H}_1 \times \cdots \times \mathcal{H}_n$, kde izomorfismus φ je definován přiřazením $g \mapsto (h_1, \ldots, h_n)$.

Ve speciálním případě kdy p je prvočíslo a $\mathcal{G}_i = \mathbb{Z}_p$ pro $1 \leq i \leq m$ je součin $\mathcal{G}$ dokonce lineárním prostorem nad tělesem $\mathbb{Z}_p$, podgrupy $\mathcal{G}'_i$ $(1 \leq i \leq m)$ jsou jeho nezávislými $\mathbb{Z}_p$-lineárními podprostory a $\mathcal{G}$ je součinem těchto svých podprostorů ve smyslu lineární algebry.

Předchozí řetězec snadných úvah nás nyní dovádí ke strukturním výsledkům, které už vůbec nejsou zřejmé na první pohled.

Pro první z nich připomeňme, že všechny grupy prvočíselného řádu jsou cyklické, a tedy komutativní, viz. Důsledek 1.47.

Věta 1.62. *Nechť $\mathcal{G}$ je grupa řádu p^2, kde p je prvočíslo. Pak $\mathcal{G}$ je komutativní, a buď $G \simeq \mathbb{Z}_{p^2}$ nebo $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Z 1.60 víme, že $|Z(G)| > 1$. Podle Lagrangeovy věty 1.29 k důkazu komutativity stačí vyloučit možnost, že $|Z(G)| = p$.

Pokud ale $|Z(G)| = p$, je $Z(G)$ cyklická grupa řádu p, a stejně tak i $G/Z(G)$. Uvažujme prvky $h, z \in G$ takové, že $e \neq z \in Z(G)$ a $h \notin Z(G)$. Pak pro každé $g \in G$ existuje $m < p$ tak, že $gZ(G) = h^m Z(G)$, a tedy pro každé $g \in G$ existují $m, n < p$ tak, že $(h^m)^{-1} \odot g =$

z^n, tj. $g = z^n \odot h^m$. Pro libovolná $g, g' \in G$ máme $g = z^n \odot h^m$, $g' = z^{n'} \odot h^{m'}$, odkud $g \odot g' = (z^n \odot h^m) \odot (z^{n'} \odot h^{m'}) = z^n \odot (h^m \odot z^{n'}) \odot h^{m'} = z^{n+n'} \odot h^{m+m'}$. Podobně $g' \odot g = z^{n+n'} \odot h^{m+m'}$, a $\mathcal{G}$ je tedy komutativní. To je spor s předpokladem, že $|Z(G)| = p$.

Pokud G obsahuje prvek řádu p^2, je $G \simeq \mathbb{Z}_{p^2}$. Pokud mají všechny prvky $e \neq g \in G$ řád p, je G lineárním prostorem dimenze 2 nad tělesem $\mathbb{Z}_p$. Libovolný rozklad G na součin jednodimenzionálních podprostorů pak indukuje izomorfismus $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

Poznámka 1.63. Grupy $\mathcal{G}$ řádu p^3, kde p je prvočíslo, už komutativní být nemusejí. Pro dané p jich existuje až na izomorfismus právě pět. Tři z nich jsou komutativní: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ a $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, a dvě nekomutativní:

Pro $p = 2$ je to dihedrální grupa Δ_4 (se dvěma generátory a, b, splňujícími definující relace $a^4 = 1$, $b^2 = 1$ a $bab = a^{-1}$) a grupa kvaternionů Q_8 (se dvěma generátory a, b, splňujícími definující relace $a^4 = 1$, $b^2 = a^2$ a $b^{-1}ab = a^{-1}$). Grupa Q_8 je izomorfní podgrupě multiplikativní grupy tělesa kvaternionů $\mathbb{H}$ sestávající z matic $\pm\mathbf{1}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$ (viz dále Příklad 2.5(4)).

Pro $p > 2$ je to grupa se dvěma generátory a, b, splňujícími definující relace $a^{p^2} = 1$, $b^p = 1$ a $b^{-1}ab = a^{1+p}$, a grupa se třemi generátory a, b, c, splňujícími definující relace $a^p = b^p = c^p = 1$, $a^{-1}b^{-1}ab = c$ a $a^{-1}c^{-1}ac = b^{-1}c^{-1}bc = 1$.

Podobně obecně nejsou komutativní ani grupy řádu $p.q$ kde $p \neq q$ jsou prvočísla - nejjednodušším příkladem je grupa S_3.

Následující věta o struktuře konečných komutativních grup je známa už od roku 1878, kdy ji publikovali Frobenius a Stickelberger. Její důkaz rozdělíme do dvou částí: první umožní rozklad grupy na součin tzv. p–primárních komponent, druhá dá úplný popis těchto komponent.

Lemma 1.64. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je konečná komutativní grupa řádu $n = p_1^{k_1} \dots p_m^{k_m}$ kde p_i jsou prvočísla a $k_i > 0$ pro každé $1 \leq i \leq m$. Pro $1 \leq i \leq m$ položme $G_i = \{g \in G \mid \exists l \geq 0 : o(g) = p_i^l\}$. Pak G_i je nosičem podgrupy v $\mathcal{G}$ (tzv. p_i–primární komponenty grupy $\mathcal{G}$) a existuje grupový izomorfismus $\mathcal{G} \cong \mathcal{G}_1 \times \dots \times \mathcal{G}_m$.*

Důkaz. To, že $G_i \leq G$ je zřejmé z definice řádu prvku v grupě 1.31. Protože $\mathcal{G}$ je komutativní, zbývá podle 1.61 jen dokázat, že každý prvek $g \in G$ lze jednoznačně vyjádřit ve tvaru $g = g_1 \odot \dots \odot g_m$ kde $g_i \in G_i$ pro $1 \leq i \leq m$.

Existence: Podle 1.29 máme $o(g) = p_1^{l_1} \dots p_m^{l_m}$ kde $l_i \leq k_i$ pro $1 \leq i \leq m$. Položme $q_i = p_1^{l_1} \dots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \dots p_m^{l_m}$. Protože čísla q_i $(1 \leq i \leq m)$ jsou nesoudělná, existují celá čísla z_i $(1 \leq i \leq m)$ taková, že $\sum_{1 \leq i \leq m} z_i q_i = 1$. Položme $g_i = g^{z_i q_i}$. Zřejmě $g^{q_i} \in G_i$, takže také $g_i \in G_i$, a platí $g_1 \odot \dots \odot g_m = g^{\sum_{1 \leq i \leq m} z_i q_i} = g$.

Jednoznačnost zřejmě stačí dokázat jen pro $g = e$. Nechť $e = g_1 \odot g_2 \odot \dots \odot g_m$ je netriviální vyjádření s minimálním počtem, r, indexů $1 \leq i \leq m$ takových, že $g_i \neq e_i$. Zřejmě $r \geq 2$. Nechť například $g_1 \neq e_1$, tj. $o(g) = p_1^l > 1$. Bylo-li $i \neq 1$ takové, že $e_i \neq g_i \in G_i$, pak také $g_i^{p_1^l} \neq e_i$, a tedy vyjádření $e = e_1 \odot g_2^{p_1^l} \odot \dots \odot g_m^{p_1^l}$ je netriviálním vyjádřením e, ve kterém je počet indexů $1 \leq i \leq m$ takových, že $g_i \neq e_i$, roven $r - 1$, ve sporu s minimalitou r. □

Lemma 1.65. *Nechť p je prvočíslo, $m > 0$ a $\mathcal{G} = (G, \odot, ^{-1}, e)$ je komutativní grupa, jejíž každý prvek má řád p^l pro nějaké $l \leq m$. Nechť $g \in G$ je maximálního řádu. Potom existuje podgrupa $\mathcal{H}$ v $\mathcal{G}$ taková, že $\mathcal{G} \cong \langle g \rangle \times \mathcal{H}$.*

Důkaz. Můžeme předpokládat, že $o(g) = p^m$. Podle Zornova lemmatu existuje podgrupa $H \leq G$ taková, že $H \cap \langle g \rangle = \{e\}$ a H je maximální s touto vlastností, tj. $H' \cap \langle g \rangle \neq \{e\}$ pro

každou podgrupu $H \subsetneq H' \leq G$. Zbývá dokázat, že nejmenší podgrupa G obsahující g i H je G, tj. $\langle g\rangle\, H = G$. (Pak lze každý prvek $g' \in G$ jednoznačně rozložit na součin $g' = g^n \odot h$ pro nějaké přirozené n a $h \in H$, a tedy $G \cong \langle g\rangle \times H$ podle 1.61.)

Předpokládejme, že existuje $g_1 \in G \setminus \langle g\rangle\, H$. Protože řád g_1 je mocninou p, můžeme též předpokládat, že $(g_1)^p = g^n \odot h$ pro nějaké n přirozené a $h \in H$ (jinak nahradíme g_1 prvkem $g_1^{p^k}$ kde k je největší takové, že $g_1^{p^k} \notin \langle g\rangle\, H$). Přitom $n > 0$, jinak by volba $H' = \langle g_1\rangle\, H$ dala $H \subsetneq H'$ a $H' \cap \langle g\rangle = \{e\}$, ve sporu s maximalitou H (pokud by totiž $g_1^k \odot h = g^r$ kde p nedělí k, pak by existovala celá čísla a, b taková, že $a.k + b.p = 1$, a $g_1^{a.k} \odot h^a = g^{a.r}$, odkud $g_1 = g_1^{a.k+b.p} \in \langle g\rangle\, H$).

Dále $e = (g_1)^{p^m} = (g^n)^{p^{m-1}} \odot h^{p^{m-1}}$, a protože $H \cap \langle g\rangle = \{e\}$, také $(g^n)^{p^{m-1}} = e = h^{p^{m-1}}$. Ale $o(g) = p^m$, takže $n = pn_1$ pro nějaké přirozené číslo $n_1 > 0$.

Označme $g_2 = g^{-n_1} \odot g_1$. Pak $(g_2)^p = g^{-n} \odot g^n \odot h = h \in H$, ale $g_2 \notin \langle g\rangle\, H$ protože $g_1 \notin \langle g\rangle\, H$. Položme $H' = \langle g_2\rangle\, H$. Pak opět $H \subsetneq H'$ a $H' \cap \langle g\rangle = \{e\}$, ve sporu s maximalitou podgrupy H. Tím je dokázáno, že $G = \langle g\rangle\, H$. □

Věta 1.66 (Frobenius-Stickelberger)**.** *Každá konečná komutativní grupa $\mathcal{G} \neq \{e\}$ je součinem konečně mnoha cyklických grup, z nichž každá má řád, který je mocninou nějakého prvočísla.*

Důkaz. Podle 1.64 je $\mathcal{G}$ izomorfní součinu svých primárních komponent: $\mathcal{G} \cong \mathcal{G}_1 \times \cdots \times \mathcal{G}_m$. Můžeme tedy předpokládat, že $\mathcal{G} = \mathcal{G}_1$ je rovna své p–primární komponentě. Podle 1.65 máme $\mathcal{G} \cong \mathcal{C} \times \mathcal{G}'$, kde $\mathcal{C}$ je cyklická podgrupa v $\mathcal{G}$ maximálního řádu, p^m, kde $m > 0$. Pokud $\mathcal{G}' \neq \{e\}$, použití 1.65 pro $\mathcal{G}'$ dává $\mathcal{G}' \cong \mathcal{C}' \times \mathcal{G}''$, kde $\mathcal{C}'$ je cyklická podgrupa v $\mathcal{G}'$ maximálního řádu, $p^{m'}$, kde $0 < m' \leq m$. Protože $\mathcal{G}$ je konečná a řády grup $\mathcal{G}$, $\mathcal{G}'$, $\mathcal{G}''$, ... tvoří ostře klesající posloupnost, dává tento postup po konečném počtu kroků požadovaný rozklad grupy $\mathcal{G}$ na součin cyklických grup. □

Poznámka 1.67. Z 1.47 a 1.66 plyne, že pro každou netriviální konečnou komutativní grupu G existuje izomorfismus

$$(*) \quad G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

kde $k > 0$, p_i jsou (ne nutně různá) prvočísla a $0 < n_i$ (ne nutně různá) přirozená čísla pro $1 \leq i \leq k$. Z Krull-Schmidtovy věty pak plyne, že každé vyjádření grupy G jako součinu cyklických grup řádů mocnin prvočísel má právě k členů, a navíc existuje bijekce množiny všech členů tohoto vyjadření na množinu všech členů vyjadření $(*)$ taková, že odpovídající si členy jsou izomorfními grupami.

Lemma 1.65 jsme zformulovali pro obecně nekonečné komutativní grupy, jejichž všechny prvky mají řád tvaru p^l $(l \leq m)$. Analogii Frobenius–Stickelbergerovy věty lze totiž dokázat i pro nekonečné komutativní grupy, které jsou *omezené* (tj. všechny jejich prvky mají řád $\leq n$ pro pevně dané přirozené číslo n, nebo-li jsou to $\mathbb{Z}_n$–moduly ve smyslu §2.3). I v tomto případě jsou všechny rozklady G jednoznačně určené podobně jako v předchozím paragrafu, jde tu ovšem o rozklady na nekonečné kosoučiny ve smyslu Příkladu 2.70.

1.4. **Maticové grupy a lineární reprezentace grup.** Důležitou částí teorie grup je zkoumání lineárních akcí grup na vektorových prostorech konečné dimenze. Toto zkoumání přirozeně spojuje abstraktní algebru s linearní algebrou a geometrií. Protože každý vektorový prostor konečné dimenze n nad tělesem K je izomorfní aritmetickému prostoru K^n všech n-tic prvků tělesa K, lze toto zkoumání redukovat na lineární akce grup na prostoru K^n,

tj. na grupové homomorfismy grup do obecné lineární grupy $GL(n,K)$ ve smyslu následující definice:

Definice 1.68. Nechť $0 < n \in \mathbb{N}$ a K je komutativní těleso. Označme $GL(n,K)$ množinu všech regulárních čtvercových matic stupně n nad K. Na $GL(n,K)$ definujme strukturu grupy následujícím způsobem

(1) $e = E_n$ (jednotková matice stupně n);
(2) $A \odot B = A \times B$, kde $\times$ značí násobení matic;
(3) A^{-1} = inverzní matice k A.

Grupu $\mathcal{GL}(n,K)$ nazýváme *obecnou lineární* grupou stupně n nad K.

Z lineární algebry víme, že $GL(n,K)$ je izomorfní grupě všech automorfismů vektorového prostoru K^n, a také známe pojem determinantu matice. Pro matice z $GL(n,K)$ dostáváme zobrazení $\det\colon GL(n,K) \to K^*$, $A \mapsto \det A$, kde K^* je multiplikativní grupa všech nenulových prvků tělesa K. Zobrazení *det* je grupovým homomorfismem grupy $GL(n,K)$ na K^* neboť $\det(A \times B) = \det A \cdot \det B$.

Definice 1.69. Jádro homomorfismu det, $\operatorname{Ker}\det = \{A \in GL(n,K) \mid \det A = 1\} \stackrel{def.}{=} SL(n,K)$ je podle 1.38 normální podgrupou v $GL(n,K)$. Tuto grupu značímée $\mathcal{SL}(n,K)$ a nazýváme *speciální lineární* grupou stupně n nad K.

Dále definujeme $PSL(n,K) \stackrel{def.}{=} SL(n,K)/Z(SL(n,K))$, kde $Z(SL(n,K))$ značí centrum grupy $\mathcal{SL}(n,K)$. Grupu $\mathcal{PSL}(n,K)$ nazýváme *projektivní speciální lineární* grupou stupně n nad K.

Grupa $\mathcal{G} = (G, \odot, ^{-1}, e)$ se nazývá *jednoduchá*, pokud triviální podgrupy G a $\{e\}$ jsou její jediné normální podgrupy.

Příklad 1.70. Základním příkladem jednoduché konečné grupy je cyklická grupa $\mathbb{Z}_p$, kde p je prvočíslo (viz. 1.31). Z 1.47 snadno plyne, že cyklické grupy prvočíselného řádu jsou jedinými komutativními jednoduchými grupami.

Dalšími příklady jednoduchých konečných grup jsou alternující grupa A_n pro $n \geq 5$ a projektivní speciální lineární grupa $\mathcal{PSL}(n,K)$ pro K konečné těleso a $n > 1$ (s výjimkou případu $\mathcal{PSL}(2,\mathbb{Z}_2)$ a $\mathcal{PSL}(2,\mathbb{Z}_3)$) - tyto dva netriviální výsledky pocházejí od Galoise resp. Jordana a Dixona. Jednoduchost alternující grupy A_n pro $n \geq 5$ je klíčová pro důkaz neexistence obecného řešení rovnice patého a vyššího stupně ,,v radikálech"(tj. pomocí konečného počtu běžných algebraických operací s koeficienty rovnice).

V roce 1981 bylo Gorensteinem oznámeno dokončení klasifikace všech jednoduchých konečných grup – kromě výše zmíněných existuje ještě několik dalších nekonečných řad těchto grup a 26 jednotlivých (tzv. sporadických) grup. Publikace úplného důkazu této klasifikace byla ale dokončena teprve nedávno, dvěma monografiemi Aschbachera a Smithe vydanými AMS roku 2004.

Definice 1.71. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, K je komutativní těleso a $1 \leq n \in \mathbb{N}$. *Reprezentací* grupy $\mathcal{G}$ stupně n nad K rozumíme grupový homomorfismus $\varphi\colon G \to GL(n,K)$. φ je *věrná* reprezentace, pokud $\operatorname{Ker}\varphi = \{e\}$.

Příklad 1.72. Příkladem reprezentace grupy $\mathcal{GL}(n,K)$ stupně 1 nad K je grupový homomorfismus $det\colon GL(n,K) \to K^* = GL(1,K)$. Tato reprezentace je ale věrná jen pro $n = 1$.

Je-li G podgrupou aditivní grupy $(K, +, -, 0)$ nějakého komutativního tělesa K, je příkladem věrné reprezentace grupy G stupně $n \geq 2$ nad K grupový homomorfismus $\varphi\colon G \to GL(n,K)$ definovaný vztahem

$$g \mapsto \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ g & 0 & \dots & 1 \end{pmatrix}$$

Poznámka 1.73. Z lineární algebry známe pojem stopy matice: stopa matice $A = (a_{ij})_{n\times n},\ A \in GL(n,K)$ se značí tr (A) a je definována jako tr $(A) \overset{def.}{=} \sum_{i\leq n} a_{ii}$.

Dvě matice A, B z $GL(n,K)$ jsou podle 1.35 konjugované právě tehdy, když existuje vnitřní automorfismus (určený některým prvkem z $GL(n,K)$), který převádí jednu matici na druhou. To nastává právě tehdy, když existuje matice $C \in GL(n,K)$: $A = C\times B\times C^{-1}$, neboli $A \sim B$ (tj. matice A je podobná matici B).

Podle 1.53 orbity prvků (při akci $\mathcal{GL}(n,K)$ na sobě pomocí vnitřních automorfismů) odpovídají třídám ekvivalence $\sim$ (podobnosti matic = konjugovanosti v $\mathcal{GL}(n,K)$). Matice s jednoprvkovými orbitami (tedy matice z centra $\mathcal{GL}(n,K)$) jsou právě diagonální matice s $0 \neq a_{ii} = a_{jj}$ pro všechna $i,j \leq n$. (Je-li K algebraicky uzavřené těleso, obsahuje každá orbita právě jednu matici v Jordanově kanonickém tvaru.)

Z lineární algebry také víme, že podobné matice mají tutéž stopu: protože K je komutativní, platí dokonce tr $(A\times B) = \sum_i \sum_j a_{ij}b_{ji} = \sum_j \sum_i b_{ji}a_{ij} =$ tr $(B\times A)$, a tedy tr $(C\times A\times C^{-1}) =$ tr (A) pro každou matici $C \in GL(n,K)$.

Definice 1.74. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a $\varphi\colon G \to GL(n,K)$ je její reprezentace stupně n nad K. Zobrazení $\chi_\varphi\colon G \to K$ definované $g \mapsto$ tr $(\varphi(g))$ se nazývá *charakterem* reprezentace φ.

Definice 1.75. Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $\varphi\colon G \to GL(n,K)$ a $\varphi'\colon G \to GL(n,K)$ jsou její reprezentace stupně n nad K. Pak φ je *ekvivalentní* s φ' pokud existuje $C \in GL(n,K)$ taková, že pro každé $g \in G$ je $\varphi'(g) = C \times \varphi(g) \times C^{-1}$

Poznámka 1.76. Při geometrickém pohledu, kdy místo $GL(n,K)$ uvažujeme grupu A všech automorfismů vektorového prostoru V dimenze n nad K a 'geometrickou reprezentaci' definujeme jako grupový homomorfismus G do A, odpovídají ekvivalentní reprezentace různým aritmetizacím (volbám K-báze ve V indukujícím izomorfismus $GL(n,K)$ na A) téže 'geometrické reprezentace'.

Lemma 1.77. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, $\varphi\colon G \to GL(n,K)$ je reprezentace grupy $\mathcal{G}$ stupně n nad K a g, g' jsou dva* konjugované *prvky z $\mathcal{G}$. Pak $\chi_\varphi(g) = \chi_\varphi(g')$.*

Důkaz. Z předpokladů víme, že existuje $h \in G$ takové, že $g' = h \odot g \odot h^{-1}$. Tedy $\varphi(g') = \varphi(h)\times\varphi(g)\times\varphi(h^{-1})$, a matice $\varphi(g)$ a $\varphi(g')$ jsou podobné. Z 1.73 a z toho, že $\chi_\varphi(g) =$ tr $(\varphi(g))$ plyne $\chi_\varphi(g) = \chi_\varphi(g')$. □

Předchozí lemma se někdy stručně formuluje větou, že charakter reprezentace je ,,třídová funkce"(,,třídou"se zde rozumí třída ekvivalence být konjugován).

Lemma 1.78. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa, φ, φ' jsou dvě ekvivalentní reprezentace grupy $\mathcal{G}$ stupně n nad K. Pak $\chi_\varphi = \chi_{\varphi'}$.*

Důkaz. Podle předpokladu existuje $C \in GL(n,K)$ takové, že pro každé $g \in G$ je $\varphi'(g) = C \times \varphi(g) \times C^{-1}$. Tedy pro každé $g \in G$ jsou $\varphi(g)$ a $\varphi(g')$ podobné. Z 1.73 a 1.74 nakonec plyne, že pro každé $g \in G$ je $\chi_\varphi(g) = \chi_{\varphi'}(g)$. □

Poznámka 1.79. Charakter reprezentace φ nahrazuje matici $\varphi(g)$ její stopou, a tedy ztrácí mnoho informací o této matici. Podle 1.78 nerozliší ekvivalentní reprezentace.

V klasickém případě reprezentací konečných grup nad tělesem, jehož charakteristika nedělí řád grupy, lze však překvapivě 1.78 částečně obrátit: charakter ireducibilní reprezentace určuje tuto reprezentaci až na ekvivalenci. To je důvodem, proč mají charaktery reprezentací v klasické teorii centrální roli.

Nyní použijeme Cayleyho větu ke konstrukci tzv. regulární reprezentace konečné grupy:

Věta 1.80 (Konstrukce regulární reprezentace)**.** *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je konečná grupa, $|G| = n$, K je komutativní těleso. Potom existuje věrná reprezentace grupy $\mathcal{G}$ stupně n nad K.*

Důkaz. Z věty 1.22 a jejího důkazu víme, že φ:

$$\begin{aligned} \varphi\colon G &\to S(G) \\ g &\mapsto L_g \end{aligned}$$

je prostý grupový homomorfismus. Zvolme bijekci (očíslování) $b\colon G \to \{1, \dots, n\}$, pak ξ_b:

$$\begin{aligned} \xi_b\colon S(G) &\to S_n \\ f &\mapsto b \circ f \circ b^{-1} \end{aligned}$$

je grupový izomorfismus. Zvolme dále zobrazení ψ:

$$\begin{aligned} \psi\colon S_n &\to GL(n, K) \\ p &\mapsto \text{permutační matice } p \end{aligned}$$

kde permutační matice p je matice $A = (a_{ij})_{n\times n}$, která má na místě a_{ij} hodnotu 1 pokud $p(j) = i$, jinak $a_{ij} = 0$. Jelikož $\psi(p \circ p') = \psi(p) \times \psi(p')$ pro každé dvě permutace $p, p' \in S_n$, je ψ grupový homomorfismus, jehož jádrem je $\operatorname{Ker}\psi = \{p \mid \psi(p) = E_n\} = \mathrm{id}_{S_n}$. Tedy ψ je prostý grupový homomorfismus a zobrazení $\varphi_b = \psi \circ \xi_b \circ \varphi$ je věrnou reprezentací grupy $\mathcal{G}$ stupně n nad K. □

Definice 1.81. Homomorfismus $\varphi_b : G \to GL(n, K)$ sestrojený v důkazu 1.80 se nazývá *regulární reprezentace* grupy G stupně n nad K.

Lemma 1.82. *Nechť $b, b'\colon G \to \{1, \dots, n\}$ jsou dvě bijekce z důkazu věty 1.80. Pak reprezentace φ_b a $\varphi_{b'}$ jsou ekvivalentní.*

Důkaz. Je třeba dokázat, že existuje $C \in GL(n, K)$ taková, že pro každé $g \in G$ je $\varphi_{b'}(g) = C \times \varphi_b(g) \times C^{-1}$. Z 1.80 víme, že $\varphi_b(g) = \psi(b \circ L_g \circ b^{-1})$ a $\varphi_{b'}(g) = \psi(b' \circ L_g \circ (b')^{-1})$.

Položme $C = \psi(b' \circ b^{-1})$. Pak $C \in GL(n, K)$, a pro každé $g \in G$ je

$$C \times \varphi_b(g) \times C^{-1} = \psi(b' \circ b^{-1}) \times \psi(b \circ L_g \circ b^{-1}) \times (\psi(b' \circ b^{-1}))^{-1} =$$

$$= \psi(b' \circ b^{-1} \circ b \circ L_g \circ b^{-1} \circ b \circ (b')^{-1}) = \psi(b' \circ L_g \circ (b')^{-1}) = \varphi_{b'}(g).$$

□

Poznámka 1.83. Předchozí lemma v podstatě říká, že nezáleží na tom, jakou bijekci si v důkazu věty 1.80 zvolíme. Vždy dostaneme, až na ekvivalenci, tutéž regulární reprezentaci grupy $\mathcal{G}$ stupně n nad K.

Podívejme se nakonec, jak vypadá charakter regulární reprezentace:

Lemma 1.84. *Nechť $\mathcal{G} = (G, \odot, ^{-1}, e)$ je grupa a φ_b je její regulární reprezentace stupně n nad K. Pak pro její charakter platí*

$$\chi_{\varphi_b}(g) = \begin{cases} 0, & g \neq e \\ n, & g = e \end{cases}$$

Důkaz. Především, pro libovolnou reprezentaci φ platí $\varphi(e) = E_n$, a tedy $\chi_{\varphi_b}(e) = \mathrm{tr}\,(E_n) = n$ (n zde značí n-krát sečtenou jednotku tělesa K).

Pro $g \neq e$ jsou na hlavní diagonále matice $\psi(b \circ L_g \circ b^{-1})$ vesměs nuly: jinak by totiž permutace $b \odot L_g \odot b^{-1}$ měla alespoň jeden pevný bod, a tedy levá translace L_g by měla alespoň jeden pevný bod. Ale $L_g(h) = h$ implikuje $g = e$, spor. Tím spíše je stopa matice $\psi(b \circ L_g \circ b^{-1})$ nulová, tj. $\chi_{\varphi_b}(g) = 0$. □

Poznámka 1.85. Klasická teorie reprezentací konečných grup (nad tělesem, jehož charakteristika nedělí řád grupy) má těžiště v teorii charakterů. Reprezentace nad tělesy konečné charakteristiky dělící řad grupy (tzv. modulární reprezentace) však vyžadují jiný přístup. V přednášce Algebra II uvidíme, že reprezentace grupy lze vždy ekvivalentně studovat jako moduly nad její grupovou algebrou.

V klasickém případě je podle Maschkeho věty grupová algebra totálně rozložitelná, a tedy stačí popsat reprezentanty tříd ekvivalence ireducibilních sčítanců regulární reprezentace. Těch je konečně mnoho, a každá reprezentace je ekvivalentní direktnímu součtu jejich kopií. Počet těchto kopií je přitom úplným invariantem (tj. určuje každou reprezentaci až na ekvivalenci).

V modulárním případě je situace podstatně složitější: grupová algebra je jen tzv. symetrickou algebrou. Teorie modulárních reprezentací je tak vlastně částí teorie modulů nad symetrickými konečně dimenzionálními algebrami ve smyslu následující kapitoly.

2. Okruhy a moduly

2.1. **Okruhy.** Pojem okruhu poskytuje obecný rámec pro několik klíčových algebraických pojmů: čísla, polynomy a matice.

Definice 2.1. $\mathcal{R} = (R, +, -, 0, ., 1)$, kde $0 \neq 1$ se nazývá *okruh* (asociativní, s jednotkovým prvkem), pokud

(1) $(R, +, -, 0)$ je komutativní grupa;
(2) $(R, ., 1)$ je monoid;
(3) Operace $\cdot$ je distributivní z obou stran k $+$, tedy pro všechna $r_1, r_2, r_3 \in R$ platí

$$\begin{aligned} (r_1 + r_2).r_3 &= r_1.r_3 + r_2.r_3 \\ r_3.(r_1 + r_2) &= r_3.r_1 + r_3.r_2 \end{aligned}$$

Pro každé $r \in R$ platí, že $r.0 + r.0 = r.(0 + 0) = r.0$, a tedy $r.0 = 0$, a podobně $0.r = 0$. Často budeme místo $r_1.r_2$ psát jen $r_1 r_2$.

Definice 2.2. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. *Centrem* okruhu $\mathcal{R}$ nazýváme množinu $\{r \in R \mid \forall s \in R\colon rs = sr\}$. Značení: Cen R. Okruh $\mathcal{R}$ je *komutativní* pokud Cen $R = R$.

Důležitými případy okruhů jsou tělesa, známá z lineární algebry:

Definice 2.3. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh, pak $\mathcal{R}$ je *těleso*, pokud $(R \setminus \{0\}, .)$ je kvazigrupa (tj. $(R \setminus \{0\}, ., ^{-1}, 1)$ je grupa).

Definice 2.4. Nechť K je komutativní těleso a $\mathcal{R} = (R, +, -, 0, ., 1)$ je okruh. Potom $\mathcal{R}$ je *K-algebra*, pokud platí

(1) $\mathcal{R}$ je vektorovým prostorem nad K, jehož aditivní grupou je $(R, +, -, 0)$, a
(2) pro každá $r, s \in R$ a $k \in K$ platí $(r.s)k = r.(sk) = (rk).s$ (tj. zobrazení $(r, s) \mapsto r.s$ je K-bilineární).

Ekvivalentně, K-algebra je okruh $\mathcal{R}$ obsahující ve svém centru kopii tělesa K (přiřazením $k \mapsto 1k$).

Příklad 2.5. S aditivními a multiplikativními grupami většiny následujících příkladů jsme se už setkali (viz. 1.12):

(1) $\mathcal{R} = (\mathbb{Z}, +, -, 0, ., 1)$, okruh všech *celých čísel* s obvyklými operacemi.
(2) $\mathcal{R} = \mathbb{Z}_n = (\{0, \dots, n-1\}, +_n, -_n, 0_n, .n, 1_n)$, okruh všech zbytků celých čísel modulo n s operacemi sčítání, násobení a vzetí opačného prvku modulo n, s nulou $0_n = 0$ a s jednotkou $1_n = 1$. . $\mathbb{Z}_n$ je (konečným) tělesem právě když n je prvočíslo. (Existují i jiné příklady konečných těles. Podle Wedderburnovy věty jsou všechna konečná tělesa komutativní; jejich strukturu úplně popíšeme v navazujícím textu Algebra II).
(3) Příkladem komutativních těles jsou tělesa všech racionálních, reálných a komplexních čísel s obvyklými operacemi, značená po řadě $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Každé z těchto těles je zároveň algebrou nad každým ze svých podtěles, např. $\mathbb{C}$ je $\mathbb{R}$-algebrou dimenze $\dim \mathbb{C}_{\mathbb{R}} = 2$.
(4) Množina všech kvaternionů

$$\mathbb{H} = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$$

s obvyklými operacemi pro matice je příkladem nekomutativního tělesa. $\mathbb{H}$ obsahuje kopii $\mathbb{C}$ jako podtěleso (je tvořena maticemi nulovými mimo hlavní diagonálu). Jako $\mathbb{R}$-algebra má $\mathbb{H}$ dimenzi 4, $\mathbb{R}$–bázi $\mathbb{H}$ tvoří matice $\mathbf{1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{i} = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $\mathbf{j} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ a $\mathbf{k} = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$.

Čtenář, očekávající nyní příklady těles vyšších konečných dimenzí nad $\mathbb{R}$, bude zklamán: podle Frobeniovy věty jsou $\mathbb{R}$, $\mathbb{C}$ a $\mathbb{H}$ až na izomorfismus jedinými konečně dimenzionálními $\mathbb{R}$-algebrami bez netriviálních dělitelů nuly.
(5) Nechť K je komutativní těleso, $0 < n \in \mathbb{N}$, pak $\mathcal{R} = \mathcal{M}_n(K) = (M_n(K), +, -, (0)_{n\times n}, \times, E_n)$ je *okruh všech čtvercových matic* stupně n nad K. Tento okruh je zároveň K-algebrou dimenze $\dim \mathcal{R}_K = n^2$. Pro $n \geq 2$ není $\mathcal{M}_n(K)$ komutativní.
(6) Nechť K je komutativní těleso, $1 < n \in \mathbb{N}$, pak $\mathcal{R} = \mathcal{UT}_n(K) = (UT_n(K), +, -, (0)_{n\times n}, \times, E_n)$ je *okruh všech horních trojúhelníkových matic* stupně n nad K. Zde $UT_n(K)$ značí množinu všech matic z $M_n(K)$, které jsou nulové všude pod hlavní diagonálou. $UT_n(K)$ je K-algebrou dimenze $\dim \mathcal{R}_K = n(n+1)/2$, která není komutativní.
(7) Nechť K je komutativní těleso. Pak $\mathcal{R} = (K[x], +, -, 0, ., 1)$ je *okruh polynomů* jedné neurčité x nad K. Tento okruh je komutativní; je K-algebrou nekonečné dimenze $\dim \mathcal{R}_K = \omega$ (K-bází této algebry je například množina $\{x^n \mid n \in \mathbb{N}_0\}$).

Podobně lze definovat okruh polynomů jedné neurčité nad libovolným okruhem S: $\mathcal{R} = (S[x], +, -, 0, ., 1)$. Indukcí tak můžeme definovat *okruh polynomů konečně mnoha komutujících neurčitých* $x_1, \dots, x_n$ nad komutativním tělesem K: $\mathcal{R} = K[x_1, \dots, x_n] = K[x_1, \dots, x_{n-1}][x_n]$.

Poznámka 2.6. Okruh polynomů je speciálním případem obecnější konstrukce tzv. monoidového okruhu, RG, monoidu G a okruhu R (kdy $R = K$ a G – volný komutativní monoid). Jiný speciální případ, kdy G je grupa a $R = K$, dává důležitý pojem grupové algebry grupy G (viz. Poznámku 1.85). Těmto pojmům, a zejména okruhům polynomů nad komutativními tělesy, se podrobněji věnuje přednáška Algebra II.

Nyní uvedeme příklad K-algebry jiného typu:

Příklad 2.7. Nechť K je komutativní těleso, G je graf s konečnou množinou vrcholů V a množinou (orientovaných, násobných) hran H. Symbolem $\langle KG\rangle$ značíme *algebru cest* grafu G.

$\langle KG\rangle$ je vektorovým prostorem nad K s bází tvořenou všemi vrcholy (= prvky V) a všemi cestami v grafu G (= konečnými posloupnostmi navazujících orientovaných hran). Zřejmě $\langle KG\rangle$ má konečnou dimenzi právě když graf G neobsahuje orientované cykly.

Multiplikativní strukturu stačí definovat na bázi prostoru $\langle KG\rangle$ – její jednoznačné (lineární) rozšíření na celý prostor je pak zřejmé. Na bázi je násobení definováno následovně: jsou-li c_1, c_2 dvě cesty v grafu G, pak $c_1 \cdot c_2$ je cesta vzniklá jejich složením pokud c_2 navazuje na c_1, a $c_1 \cdot c_2 = 0$ jinak. Jsou-li v_1, v_2 dva vrcholy grafu G, pak $v_1 \cdot v_2 = v_1$ pokud $v_1 = v_2$, a $v_1 \cdot v_2 = 0$ jinak. Je-li c cesta v G a v je vrchol G, pak $v \cdot c = c$ pokud v je počáteční vrchol cesty c, a $v \cdot c = 0$ jinak. Podobně $c \cdot v = c$ pokud v je koncový vrchol cesty c, a $c \cdot v = 0$ jinak.

Snadno se ověří, že $\langle KG\rangle$ s právě definovanými operacemi tvoří K-algebru.

Poznámka 2.8. Konstrukce algebry cest v 2.7 zahrnuje řadu známých konstrukcí algeber jako speciální případy. Například K-algebra polynomů $K[x]$ je izomorfní algebře cest grafu tvořeného pouze jedním vrcholem a jednou orientovanou hranou (smyčkou). Podobně K-algebra $UT_n(K)$ je izomorfní algebře cest následujícího grafu s n vrcholy a $n-1$ orientovanými hranami: $\bullet \to \bullet \to \cdots \to \bullet \to \bullet$.

(Je-li těleso K algebraicky uzavřené, lze – až na tzv. Moritovskou ekvivalenci – získat jako algebru cest každou dědičnou konečně dimenzionální K-algebru; navíc každá konečně dimenzionální K-algebra je Moritovsky ekvivalentní faktor-algebře nějaké algebry cest podle vhodného ideálu generovaného cestami délky aspoň 2).

Definice 2.9. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Pak $\mathcal{S} = (S, +', -', 0', \cdot', 1')$ je *podokruhem* v $\mathcal{R}$, pokud $(S, +', -', 0')$ je podgrupa v $(R, +, -, 0)$ a $(S, \cdot', 1')$ je podmonoid v $(R, \cdot, 1)$.

Je-li navíc K komutativní těleso a $\mathcal{R}$ je K-algebra, pak $\mathcal{S}$ je *podalgebrou* v $\mathcal{R}$ pokud $\mathcal{S}$ je podokruhem a zároveň K-podprostorem v $\mathcal{R}$.

Příklad 2.10.
(1) Je-li $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ okruh, pak $S = R$ je podokruhem v $\mathcal{R}$.
(2) Je-li $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ okruh, pak $S = \{\underbrace{1 + \cdots + 1}_{z\times} \mid z \in \mathbb{Z}\}$ (viz. 1.32) je podokruhem v $\mathcal{R}$, tzv. *prvookruhem* $\mathcal{R}$. Prvookruh je nejmenším podokruhem v $\mathcal{R}$; budeme ho značit $\mathcal{P}_R$.
(3) Je-li $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ okruh, pak jeho centrum Cen R je podokruhem v $\mathcal{R}$.
(4) K-algebra $UT_n(K)$ je podalgebrou K-algebry $M_n(K)$.

Definice 2.11. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. $I \subseteq R$ se nazývá levý (resp. pravý) *ideál* v $\mathcal{R}$ pokud $(I, +, -, 0)$ je podgrupa v $(R, +, -, 0)$ a pro každá $r \in R$ a $i \in I$ platí $r \cdot i \in I$ (resp. $i \cdot r \in I$). Je-li $I \subseteq R$ levý i pravý ideál, pak se I nazývá *oboustranný ideál* nebo prostě jen *ideál* v $\mathcal{R}$. (V komutativních okruzích samozřejmě pojmy levého, pravého a oboustranného ideálu splývají).

Příklad 2.12. (1) V každém okruhu R jsou $I = \{0\}$ a $I = R$ oboustrannými ideály, tzv. *triviálními* ideály. (Levé, pravé) ideály v okruhu tvoří částečně uspořádanou množinu (vzhledem k inkluzi), triviální ideály jsou jejím nejmenším resp. největším prvkem.

Okruh se nazývá *jednoduchý*, pokud má jen triviální oboustranné ideály (srovnej s 1.70). Například okruh $\mathcal{M}_n(K)$ ($n \geq 1$, K těleso) je jednoduchý. Struktura všech jednoduchých okruhů není obecně známá. Je však známa struktura všech jednoduchých okruhů bez nekonečných ostře klesajících řetězců pravých ideálů: podle Wedderburnovy věty jsou to až na izomorfismus právě okruhy všech čtvercových matic nad tělesy.

(2) Nechť R je okruh a $r \in R$. Pak $I = Rr = \{s.r \mid s \in R\}$ je levý ideál, tzv. *hlavní levý ideál* generovaný r. Podobně definujeme *hlavní pravý ideál* generovaný r.

(3) Nechť $R = \mathbb{Z}$, pak ideály splývají s podgrupami aditivní grupy $\mathbb{Z}$. Tedy libovolný ideál je hlavní, tvaru $\mathbb{Z}n$ pro nějaké $n \in \mathbb{N}$. Okruhy, v nichž je každý ideál hlavní, nazýváme *okruhy hlavních ideálů* – budeme se jim podrobněji věnovat později.

Následující věta charakterizuje tělesa jako okruhy, které mají jen triviální jednostranné ideály (a tedy komutativní tělesa jako jednoduché komutativní okruhy):

Věta 2.13. *Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Pak následující podmínky jsou ekvivalentní*

(i) *$\mathcal{R}$ je těleso.*
(ii) *$\mathcal{R}$ má jen triviální levé ideály.*
(iii) *$\mathcal{R}$ má jen triviální pravé ideály.*

Důkaz. Dokážeme pouze ekvivalenci (i) $\Leftrightarrow$ (ii), ekvivalence (i) $\Leftrightarrow$ (iii) se dokáže analogicky.

(i) $\Rightarrow$ (ii) Nechť I je nenulový levý ideál v $\mathcal{R}$. Vezměme $0 \neq x \in I$. Podle předpokladu existuje $y \in R$ takové, že $yx = 1$. Protože I je levý ideál, je $1 \in I$, a tedy pro každé $r \in R$ máme $r = r.1 \in I$ odkud $I = R$.

(ii) $\Rightarrow$ (i) Nechť $0 \neq x \in R$. Pak hlavní levý ideál $Rx = \{rx \mid r \in R\}$ je nenulový, tedy $Rx = R$ a existuje $x' \in R$ takové, že $x'.x = 1$. Jinými slovy, každý nenulový prvek z $\mathcal{R}$ je zleva invertibilní. Pak ale existuje $(x')' \in R$ takové, že $(x')'.x' = 1$, odkud $(x')' = (x')'.1 = ((x')'.x').x = x$, a tedy $x.x' = 1$ a každý nenulový prvek z $\mathcal{R}$ je oboustranně invertibilní. Tedy nenulové prvky v R tvoří multiplikativní grupu.

□

Definice 2.14. Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ a $\mathcal{R}' = (R', +', -', 0', .', 1')$ jsou okruhy. Zobrazení $\varphi\colon R \to R'$ je *okruhový homomorfismus* pokud φ je grupový homomorfismus $(R, +, -, 0)$ do $(R', +', -', 0')$ a zároveň φ je monoidový homomorfismus $(R, ., 1)$ do $(R', .', 1')$. Pojem *okruhový izomorfismus* značí okruhový homomorfismus, který je bijekcí.

Poznámka 2.15. Podle 1.20 je φ okruhový homomorfismus pokud pro každá $r, s \in R$ platí, že $\varphi(r + s) = \varphi(r) +' \varphi(s)$, $\varphi(r.s) = \varphi(r).'\varphi(s)$ a $\varphi(1) = 1'$.

Příklad 2.16. (1) Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ je okruh a $\mathcal{S} = (S, +, -, 0, ., 1)$ je jeho podokruh. Pak vnoření $\varphi\colon S \hookrightarrow R$ je okruhový homomorfismus.

(2) Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ je okruh. Pak zobrazení $\varphi : \mathbb{Z} \to R$ definované $z \mapsto \underbrace{1 + \cdots + 1}_{z\times}$ je okruhový homomorfismus, jehož obrazem je prvookruh okruhu $\mathcal{R}$.

Oboustranné ideály hrají v teorii okruhů stejnou roli jako normální podgrupy v teorii grup:

Lemma 2.17. *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ a $\mathcal{S} = (S, +', -', 0', .', 1')$ jsou okruhy a $\varphi\colon R \to S$ je okruhový homomorfismus. Pak $Ker\ \varphi = \{r \in R \mid \varphi(r) = 0'\}$ je oboustranný ideál v $\mathcal{R}$ a $Im\ \varphi = \{s \in S \mid \exists r \in R\colon \varphi(r) = s\}$ je podokruh v S.*

Důkaz. Dokážeme pouze tvrzení o Ker φ: protože φ je grupový homomorfismus, je Ker φ podgrupa v $\mathcal{R}$. Navíc pro libovolné $i \in \operatorname{Ker}\varphi$ a $r \in R$ máme $\varphi(r.i) = \varphi(r).'\varphi(i) = \varphi(r).'0' = 0'$ a podobně $\varphi(i.r) = 0'$, z čehož plyne, že $r.i \in \operatorname{Ker}\varphi$ a $i.r \in \operatorname{Ker}\varphi$. Tedy Ker φ je oboustranný ideál v $\mathcal{R}$. □

Definice 2.18. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh a I je jeho oboustranný ideál, $I \neq R$. Na faktorové grupě $(R/I, \bar{+}, \bar{-}, \bar{0})$ definujeme operaci $\bar{\cdot}$ a prvek $\bar{1}$ následovně

$$\begin{aligned}(r+I)\bar{\cdot}(s+I) &= r\cdot s + I\\ \bar{1} &= 1 + I\end{aligned}$$

Potom $\mathcal{R}/I = (R/I, \bar{+}, \bar{-}, \bar{0}, \bar{\cdot}, \bar{1})$ je okruh, který nazýváme *faktorový* okruh $\mathcal{R}$ podle I. Zobrazení $\pi_I : R \to R/I$ definované $r \mapsto r + I$ je okruhový homomorfismus *na* R/I, tzv. *kanonická projekce* podle I. Platí, že Ker $\pi_I = I$ a Im $\pi_I = R/I$.

Věta 2.19 (o homomorfismu pro okruhy)**.** *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ a $\mathcal{R}' = (R', +', -', 0', .', 1')$ jsou okruhy, $I \neq R$ je ideál v $\mathcal{R}$ a $\varphi : R \to R'$ je okruhový homomorfismus takový, že $\operatorname{Ker}\varphi \supseteq I$.*

Potom existuje právě jeden okruhový homomorfismus $\psi\colon R/I \to R'$ takový, že $\varphi = \psi \circ \pi_I$.

Důkaz. Podle 1.44 existuje právě jeden grupový homomorfismus aditivních grup, ψ, pro který platí $\varphi = \psi \circ \pi_I$, a ψ je definováno vztahem

$$\psi(r + I) = \varphi(r).$$

Protože $\psi((r+I)\bar{\cdot}(s+I)) = \varphi(r).'\varphi(s)$ a $\psi(1+I) = 1'$, je ψ okruhovým homomorfismem podle 2.15. □

Podobně, tj. ověřením, že izomorfismy aditivních grup jsou v dané situaci i okruhovými izomorfismy, se dokáží následující dvě věty o izomorfismu pro okruhy:

Věta 2.20 (1. věta o izomorfismu pro okruhy)**.** *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ a $\mathcal{R}' = (R', +', -', 0', .', 1')$ jsou okruhy a $\varphi : R \to R'$ je nenulový okruhový homomorfismus. Potom zobrazení $\psi : R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$ definované vztahem $\psi(r + \operatorname{Ker}\varphi) = \varphi(r)$ je okruhovým izomorfismem.*

Příklad 2.21. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Definujme okruhový homomorfismus $\varphi\colon \mathbb{Z} \to R$ vztahem $\varphi(z) = 1^z$ (viz. 2.16 a 1.32). Podle 2.20 platí, že Im $\varphi \simeq \mathbb{Z}/\operatorname{Ker}\varphi$. Z 2.16 víme, že Im φ je $\mathcal{P}_R$, prvookruh okruhu $\mathcal{R}$. Pro jádro φ platí

$$\operatorname{Ker}\varphi = \{z \mid 1^z = 0\} = \begin{cases}\{0\} & \text{pokud char } \mathcal{R} = 0\\ \mathbb{Z}n & \text{pokud char } \mathcal{R} = n\ (n \geq 2)\end{cases}$$

(kde char $\mathcal{R}$ je nejmenší $n \in \mathbb{N}$ takové, že $\underbrace{1 + \cdots + 1}_{n\times} = 0$; pokud takové $n \in \mathbb{N}$ neexistuje, definujeme char $\mathcal{R} = 0$).

Pro libovolný okruh $\mathcal{R}$ je tedy prvookruh $\mathcal{P}_R$ izomorfní s okruhem celých čísel „modulo char $\mathcal{R}$", tj. s faktorovým okruhem $\mathbb{Z}$ podle ideálu generovaného char $\mathcal{R}$.

Věta 2.22 (2. věta o izomorfismu pro okruhy)**.** *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ je okruh a $I \subseteq J \subsetneq R$ jsou ideály v $\mathcal{R}$. Potom J/I je ideál ve faktorovém okruhu R/I a platí okruhový izomorfismus $(R/I)/(J/I) \simeq R/J$.*

2.2. **Podílové okruhy a lokalizace.** Závěr této kapitoly věnujeme metodě lokalizace, jejíž různé variace tvoří důležitou součást moderní algebry, geometrie a topologie. Zde se budeme zabývat jen její základní formou pro komutativní okruhy: konstrukcí podílového okruhu komutativního okruhu. Idea je jednoduchá: rozšířit daný okruh tak, aby v rozšíření bylo možné snáze dělit; přesněji, aby bylo možné invertovat prvky z předem dané multiplikativní podmnožiny okruhu. (V obecnějších variantách této metody jde o invertování systémů matic nad okruhem R, a ještě obecněji, systémů morfismů mezi R-moduly či komplexy R-modulů.)

Nejprve zavedeme potřebné pojmy:

Definice 2.23. Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je komutativní okruh.

(i) Prvek $x \in R$ je *nilpotentní*, pokud existuje $n \in \mathbb{N}$, $n < \omega$ takové, že $x^n = \underbrace{x \cdots x}_{n\times} = 0$. Nejmenší takové $n \in \mathbb{N}$ se nazývá *index nilpotence* prvku x. (Například $x = 0$ má index nilpotence 1).

(ii) Prvek $x \in R$ je *regulární* (nebo též *nedělitel nuly*), pokud pro každé $y \in R$ platí, že $xy = 0$ implikuje $y = 0$.

(iii) Podmnožina $S \subseteq R$ je *multiplikativní*, pokud $1 \in S$, $0 \notin S$ a $s_1, s_2 \in S$ implikuje $s_1.s_2 \in S$ pro každá $s_1, s_2 \in S$.

(iv) $\mathcal{R}$ je *obor integrity*, pokud pro každá nenulová $x, y \in R$ platí, že $x.y \neq 0$ (tj. pokud $S = R \setminus \{0\}$ je multiplikativní množina v R).

Příklad 2.24. (1) $\mathcal{Z} = (\mathbb{Z}, +, -, 0, ., 1)$ je oborem integrity.

(2) Nechť p je prvočíslo a $n \geq 1$. Pak všechny prvky hlavního ideálu $\mathbb{Z}_{p^n}.p$ okruhu $\mathbb{Z}_{p^n}$ jsou nilpotentní stupně $\leq n$, zatímco všechny prvky množiny $\mathbb{Z}_{p^n} \setminus \mathbb{Z}_{p^n}.p$ jsou invertibilní.

(3) Nechť $\mathcal{R}$ je komutativní okruh. Označme S_{reg} množinu všech jeho regulárních prvků. Pak S_{reg} je multiplikativní, neboť $1 \in S_{reg}$, $0 \notin S_{reg}$ a pokud $s_1, s_2 \in S_{reg}$ a $y.(s_1.s_2) = 0$, pak $(y.s_1).s_2 = 0$, odkud $y.s_1 = 0$ a $y = 0$, tj. $s_1.s_2 \in S_{reg}$.

(4) Nechť $\mathcal{R}$ je komutativní okruh a $s \in R$ není nilpotentní. Pak $S = \{s^n \mid n \in \mathbb{N}\}$ je multiplikativní.

(5) Nechť $\mathcal{R}$ je komutativní okruh a $e \in R$ je *idempotent* (tj. $e \cdot e = e$). Je-li $e \neq 0$, pak množina $S = \{1, e\}$ je multiplikativní.

(6) Množina všech invertibilních prvků komutativního okruhu $\mathcal{R}$ (značení: S_{inv} nebo R^*) je multiplikativní.

Následující konstrukce zobecňuje známou konstrukci tělesa $\mathbb{Q}$ jako tělesa tříd ekvivalence zlomků nad $\mathbb{Z}$:

Definice 2.25 (Podílový okruh)**.** Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je komutativní okruh a $S \subseteq R$ je multiplikativní. Na množině $R \times S$ zavedeme ekvivalenci $\sim$ následovně :

$$(r, s) \sim (r', s') \Leftrightarrow \exists\, x \in S\colon (rs' - r's) \cdot x = 0$$

Označme $\overline{(r, s)}$ rozkladovou třídu prvku $(r, s) \in R \times S$ podle $\sim$. Na rozkladových třídách $(R \times S)/_\sim$ definujeme operace :

$$\begin{aligned}
\overline{(r,s)} \mathbin{\overline{+}} \overline{(r',s')} &= \overline{(rs'+r's, ss')} \\
\overline{-}\,\overline{(r,s)} &= \overline{(-r,s)} \\
\overline{(r,s)} \mathbin{\overline{\cdot}} \overline{(r',s')} &= \overline{(rr', ss')} \\
\overline{0} &= \overline{(0,1)} \\
\overline{1} &= \overline{(1,1)}
\end{aligned}$$

Věta 2.26. *Operace $\overline{+}$, $\overline{-}$, $\overline{0}$, $\overline{\cdot}$, $\overline{1}$ definují na $(R\times S)/_\sim$ z 2.25 strukturu okruhu, označovaného $\mathcal{R}S^{-1}$, a nazývaného* podílovým *okruhem okruhu $\mathcal{R}$ podle S.*

Zobrazení $\varphi\colon R \to RS^{-1}$ definované vztahem $\varphi(r) = \overline{(r,1)}$ je okruhový homomorfismus a pro každé $s \in S$ je $\varphi(s)$ invertibilní prvek v $\mathcal{R}S^{-1}$. Dále $Ker\,\varphi = \{r \in R \mid \exists\, s \in S\colon r \cdot s = 0\}$, a φ je prosté právě když $S \subseteq S_{reg}$.

Důkaz. To, že operace z 2.25 jsou korektně definované na množině $(R \times S)/_\sim$ a definují na této množině strukturu okruhu, přenecháme čtenáři jako snadné, byť zdlouhavé, cvičení. Dokážeme nyní, že φ je okruhový homomorfismus. Podle 2.25 stačí ověřit pro každá $r, r' \in R$

(1) $\varphi(r + r') = \overline{(r + r', 1)} = \overline{(r,1)} \mathbin{\overline{+}} \overline{(r',1)} = \varphi(r) \mathbin{\overline{+}} \varphi(r')$
(2) $\varphi(r \cdot r') = \overline{(r \cdot r', 1)} = \overline{(r,1)} \mathbin{\overline{\cdot}} \overline{(r',1)} = \varphi(r) \mathbin{\overline{\cdot}} \varphi(r')$
(3) $\varphi(1) = \overline{(1,1)} = \overline{1}$

Je-li $s \in S$, pak $\overline{(s,1)} \mathbin{\overline{\cdot}} \overline{(1,s)} = \overline{(1,1)}$, a tedy $\varphi(s)$ je invertibilní v $\mathcal{R}S^{-1}$.

Dále Ker $\varphi = \{r \in R \mid \overline{(r,1)} = \overline{(0,1)}\} = \{r \in R \mid \exists\, s \in S\colon r.s = 0\}$. Tedy Ker $\varphi = \{0\}$ právě když pro každé $s \in S$ a každé nenulové $r \in R$ je $r.s \neq 0$, tj. právě když $S \subseteq S_{reg}$. □

Zobrazení φ z 2.26 má následující univerzální vlastnost (srovnej s 1.44):

Lemma 2.27. *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ a $\mathcal{R}' = (R', +', -', 0', .', 1')$ jsou komutativní okruhy, $S \subseteq R$ je multiplikativní a $\psi : R \to R'$ je okruhový homomorfismus takový, že $\psi(s)$ je invertibilní v R' pro každé $s \in S$. Pak existuje právě jeden okruhový homomorfismus $\eta\colon RS^{-1} \to R'$ splňující $\eta \circ \varphi = \psi$.*

Důkaz. Pro $r \in R$ a $s \in S$ definujeme $\eta(\overline{(r,s)}) = \psi(r) \cdot' (\psi(s))^{-1'}$. Snadno se ověří, že η je (korektně definovaný) okruhový homomorfismus. Navíc $(\eta \odot \varphi)(r) = \eta(\overline{(r,1)}) = \psi(r)$.

Je-li $\eta'\colon RS^{-1} \to R'$ okruhový homomorfismus splňující $\eta' \odot \varphi = \psi$, pak pro každé $r \in R$ a $s \in S$ je $\eta'(\overline{(r,1)}) = \psi(r)$ a $\eta'(\overline{(s,1)}) = \psi(s)$, a tedy $\eta'(\overline{(r,s)}) = \eta'(\overline{(r,1)} \mathbin{\overline{\cdot}} \overline{(1,s)}) = \psi(r) \cdot' \eta'(\overline{(1,s)})$. Ale $\eta'(\overline{(1,s)}) \cdot' \psi(s) = \eta'(\overline{(s,s)}) = 1'$, takže $\eta'(\overline{(r,s)}) = \psi(r) \cdot' (\psi(s))^{-1'}$ a $\eta = \eta'$. □

Z jednoznačnosti zobrazení η v 2.27 plyne, že φ je tzv. epimorfismus okruhů, tj. $\tau = \tau'$ kdykoliv $\tau :: RS^{-1} \to R'$ a $\tau' :: RS^{-1} \to R'$ jsou okruhové homomorfismy splňující $\tau \circ \varphi = \tau' \circ \varphi$.

Speciálním případem konstrukce podílového okruhu je konstrukce tzv. klasického podílového okruhu:

Definice 2.28 (Klasický podílový okruh)**.** Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je komutativní okruh a $S = S_{reg}$. Potom $\mathcal{R}S^{-1}$ se nazývá *klasický* podílový okruh a značí se $Q_{cl}(R)$.

Podle 2.26 je v tomto případě zobrazení φ prosté, tedy R lze přirozeně ztotožnit s podokruhem v $Q_{cl}(R)$. Navíc, protože $S \subseteq S_{reg}$, je ekvivalence $\sim$ definována jednodušeji: $(r,s) \sim (r',s') \Leftrightarrow rs' = r's$.

Příklad 2.29. (1) Pro $R = \mathbb{Z}$ je $Q_{cl}(R) \simeq \mathbb{Q}$.

(2) Pro $R = \mathbb{Z}_{p^n}$, kde p je prvočíslo a $2 \leq n \in \mathbb{N}$ je podle 2.24.2 S_{reg} množinou všech invertibilních prvků v R, a tedy $Q_{cl}(R) \simeq R$ (neboť φ je v tomto případě i surjektivní).

Věta 2.30. *Nechť $\mathcal{R}$ je obor integrity. Potom $Q_{cl}(R)$ je komutativní těleso, tzv.* podílové *těleso oboru $\mathcal{R}$.*

Důkaz. Stačí ukázat, že pro libovolná $r \in R$ a $s \in R \setminus \{0\}$ taková, že $\overline{(r,s)} \neq \overline{(0,1)}$ je $\overline{(r,s)}$ invertibilní v $Q_{cl}(R)$. Ovšem $\overline{(r,s)} \neq \overline{(0,1)}$ právě když $r \neq 0$ právě když $r \in S_{reg}$. Inverzním prvkem k $\overline{(r,s)}$ v $Q_{cl}(R)$ je tedy zřejmě $\overline{(s,r)}$. □

Věta 2.30 říká, že klasický podílový okruh oboru integrity má nejjednodušší možnou strukturu ideálů. I v obecném případě dochází ke zjednodušení, neboť ideály, pro které $I \cap S \neq 0$, se stanou triviálními:

Věta 2.31. *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ je komutativní okruh a $S \subseteq R$ je multiplikativní.*

Pro každý ideál I v R je $IS^{-1} = \{\overline{(i,s)} \mid i \in I, s \in S\}$ ideálem v podílovém okruhu $\mathcal{R}S^{-1}$. Naopak, je-li J ideálem v podílovém okruhu $\mathcal{R}S^{-1}$, pak jeho vzor $I = \varphi^{-1}(J)$ v okruhovém homomorfismu φ je ideálem v R.

Každý ideál v podílovém okruhu $\mathcal{R}S^{-1}$ je tvaru IS^{-1} pro nějaký ideál I v R. Přitom $IS^{-1} = RS^{-1}$ právě když $I \cap S \neq \emptyset$.

Důkaz. První dvě tvrzení plynou přímo z definic.

Je-li J ideálem v podílovém okruhu $\mathcal{R}S^{-1}$, pak $I = \varphi^{-1}(J) = \{r \in R \mid \varphi(r) \in J\} = \{r \in R \mid \exists s \in S : \overline{(r,s)} \in J\} = \{r \in R \mid \forall s \in S : \overline{(r,s)} \in J\}$, odkud plyne, že $IS^{-1} = J$.

Nakonec, $IS^{-1} = RS^{-1}$ právě když $\overline{(1,1)} \in IS^{-1}$ právě když $I \cap S \neq \emptyset$. □

Je-li I ideál v R, pak IS^{-1} se nazývá *extenzí* ideálu I do $\mathcal{R}S^{-1}$. Je-li J ideálem v podílovém okruhu $\mathcal{R}S^{-1}$, pak $I = \varphi^{-1}(J)$ je *kontrakcí* ideálu J do R .

Z důkazu věty 2.31 plyne, že pro každý ideál J podílového okruhu $\mathcal{R}S^{-1}$ je extenze jeho kontrakce totožná s J (tj. $J = \varphi^{-1}(J)S^{-1}$). Naopak, kontrakce extenze ideálu I v R pouze obahuje I, ale je obecně větší než I (např. v případě, že $I \neq R$, ale $I \cap S \neq \emptyset$).

Dalším speciálním případem konstrukce podílového okruhu je lokalizace komutativního okruhu v prvoideálu.

Definice 2.32. Nechť $\mathcal{R}$ je komutativní okruh a $\mathcal{I}$ je ideál v $\mathcal{R}$. Potom

(i) $\mathcal{I}$ je *maximální*, pokud $I \neq R$ a pokud pro každý ideál $\mathcal{J}$ takový, že $I \subseteq J \subseteq R$ platí, že $J = I$ nebo $J = R$.

(ii) I je *prvoideál*, pokud $I \neq R$ a pro libovolná $x, y \in R$ platí implikace $x.y \in I \Rightarrow (x \in I) \vee (y \in I)$.

Skutečnost, že ideál I je prvoideálem nebo maximálním ideálem, lze snadno poznat podle faktorového okruhu R/I:

Lemma 2.33. *Nechť $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je komutativní okruh a I ideál v $\mathcal{R}$ takový, že $I \neq R$. Pak*

(i) *Kanonická projekce $\pi_I : R \to R/I$ indukuje izomorfismus částečně uspořádané množiny všech ideálů v okruhu R obsahujících ideál I na částečně uspořádanou množinu všech ideálů faktorového okruhu R/I.*

(ii) *I je maximální právě když faktorový okruh R/I je těleso.*

(iii) *I je prvoideál právě když faktorový okruh R/I je obor integrity.*

Tedy každý maximální ideál je prvoideálem.

Důkaz. (i) Snadno se ověří, že zobrazení $J \mapsto J/I = \{\pi_I(j) \mid j \in J\}$ je hledaným izomorfismem (srovnej s 1.45).

(ii) Podle definice maximálního ideálu je ideál I v okruhu R maximální právě když částečně uspořádaná množina všech ideálů v okruhu R obsahujících I je dvouprvková ($= \{I, R\}$). Podle části (i) a podle 2.13 je tato podmínka ekvivalentní s tím, že R/I je těleso.

(iii) Implikaci $x.y \in I \Rightarrow (x \in I) \vee (y \in I)$ z definice prvoideálu v 2.32 lze ekvivalentně napsat ve tvaru $(x+I)\dot{.}(y+I) = I \Rightarrow (x+I = I) \vee (y+I = I)$, což je přesně podmínka „R/I je obor integrity". □

Příklad 2.34. (1) Pokud $\mathcal{R} = K$, kde K je komutativní těleso, pak $\{0\}$ je jediný maximální ideál a jediný prvoideál v $\mathcal{R}$.

(2) Pokud $\mathcal{R} = \mathbb{Z}$, pak ideály jsou právě všechny podgrupy $\mathbb{Z}$, a tedy jsou tvaru $\mathbb{Z}n$, kde $n \in \mathbb{N}$ (viz. 2.12). Dále zřejmě platí, že $\mathbb{Z}m \subseteq \mathbb{Z}n$ právě když n dělí m. Tedy $\mathbb{Z}n$ je maximální ideál právě když n je prvočíslo. Podobně $\mathbb{Z}n$ je prvoideál právě když buď n je prvočíslo nebo $n = 0$ (neboť $\mathbb{Z}/0 = \mathbb{Z}$).

(3) Je-li $\mathcal{R}$ komutativní okruh a $J \neq R$ je ideál v R, pak existuje aspoň jeden maximální ideál I v R takový, že $J \subseteq I$. To lze dokázat jednoduše užitím Zornova lemmatu na množinu $\mathcal{A}$ všech ideálů v R různých od R a obsahujících J (částečně uspořádanou inkluzí). Platí totiž, že $J \in \mathcal{A}$ a $\mathcal{A}$ je uzavřená na sjednocení libovolných řetězců svých prvků (neboť pro každý ideál I platí $I = R$ právě když $1 \in I$), tedy $\mathcal{A}$ je induktivní. Maximální prvky množiny $\mathcal{A}$ pak podle definice 2.32 splývají s maximálními ideály okruhu R obsahujícími J.

Ve speciálním případě $J = \{0\}$ tak dostáváme existenci maximálních ideálů v libovolném komutativním okruhu R.

(4) Je-li I ideál v okruhu R, pak I je prvoideál v R právě když množina $S = R \setminus I$ je multiplikativní.

Definice 2.35 (Lokalizace v prvoideálu)**.** Nechť $\mathcal{R}$ je komutativní okruh a P je prvoideál v $\mathcal{R}$. Položme $S = R \setminus P$. Potom podílový okruh $\mathcal{R}S^{-1} = \mathcal{R}_{(P)}$ se nazývá *lokalizace* okruhu $\mathcal{R}$ v prvoideálu P.

Příklad 2.36. Nechť $\mathcal{R} = \mathbb{Z}$. Podle 2.34 jsou $I_0 = \{0\}$ a $I_p = \mathbb{Z}p$, kde p je prvočíslo, všechny prvoideály v $\mathbb{Z}$.

Máme $S_0 = \mathbb{Z} \setminus \{0\} = S_{reg}$, a tedy lokalizace $\mathbb{Z}$ v I_0 splývá s podílovým tělesem, tj. $\mathbb{Z}_{(I_0)} = \mathbb{Q}$. (Analogicky, lokalizace libovolného oboru integrity R v nulovém prvoideálu splývá s podílovým tělesem $Q_{cl}(R)$).

$S_p = \mathbb{Z} \setminus I_p$ je množinou všech celých čísel, která nejsou dělitelná prvočíslem p, a tedy $\mathbb{Z}_{(I_p)} \cong \{\frac{r}{s} \in \mathbb{Q} \mid p \nmid s,\ r, s \in \mathbb{Z}\}$ je podoborem integrity tělesa $\mathbb{Q}$.

Následující příklad vysvětluje název „lokalizace v prvoideálu", který má motivaci v algebraické geometrii (pojmy a výsledky uvedené v tomto příkladu budeme podrobněji studovat až v přednášce Algebra II):

Příklad 2.37. Nechť K je komutativní těleso. Označme $R = K[x_1, \ldots, x_n]$ okruh polynomů n komutujících neurčitých nad K (viz. 2.5.7).

Mějme $f_1, \ldots, f_m \in R$. *Algebraickou* množinou v K^n nazveme množinu $A = \{\overline{k} \in K^n \mid \forall\, i = 1, \ldots, m\colon f_i(\overline{k}) = 0\}$ (tj. množinu všech společných kořenů polynomů $f_1, \ldots, f_m$).

Značí-li I ideál v $\mathcal{R}$ generovaný $f_1, \ldots, f_m$, pak je také $A = \{\overline{k} \in K^n \mid \forall\, f \in I\colon f(\overline{k}) = 0\}$. Přitom I je prvoideálem právě když algebraická množina A je *ireducibilní*, tj. nelze vyjádřit jako sjednocení vlastních algebraických podmnožin.

Faktorový okruh $R/I = K[x_1, \ldots, x_n]/I$ se nazývá *souřadnicový* okruh A (je totiž jako okruh generován množinou rozkladových tříd „souřadnic" $\{x_1 + I, \ldots, x_n + I\}$).

Zvolme libovolně bod $a \in A$ na algebraické množině A a označme $I_a = \{g \in R \mid g(a) = 0\}$ (polynomy nulové v bodě a). Zřejmě $I \subseteq I_a$, a I_a je prvoideál v $\mathcal{R}$. Podle 2.22 a 2.33.3 je I_a/I prvoideálem v R/I. Označme $S = (R/I) \setminus (I_a/I)$. Pak podílový okruh $\mathcal{R}S^{-1}$ se nazývá lokalizace souřadnicového okruhu R/I v bodě a (v $\mathcal{R}S^{-1}$ jsou invertovány rozkladové třídy polynomů nenulových „lokálně", v bodě a, algebraické množiny A).

Lokalizace v prvoideálu je klíčovou metodou klasické komutativní algebry (a tedy i klasické algebraické geometrie). Korespondence mezi ideály z 2.31 funguje v tomto případě zvlášť dobře pro prvoideály:

Věta 2.38. *Nechť $\mathcal{R} = (R, +, -, 0, ., 1)$ je komutativní okruh a P je prvoideál v $\mathcal{R}$.*

Zobrazení $\ell : I \mapsto IS^{-1}$ z 2.31 definuje izomorfismus částečně uspořádané množiny všech prvoideálů okruhu R obsažených v P na částečně uspořádanou množinu všech prvoideálů okruhu $\mathcal{R}_{(P)}$.

Speciálně, $\mathcal{R}_{(P)}$ je lokální okruh *(tj. $\mathcal{R}_{(P)}$ má jediný maximální ideál).*

Důkaz. Z 2.31 víme, že zobrazení $\rho : J \mapsto \varphi^{-1}(J)$ zobrazuje množinu všech ideálů $\mathcal{R}_{(P)}$ do množiny všech ideálů okruhu R a splňuje $\ell \circ \rho = id$.

Přitom je-li J prvoideál v $\mathcal{R}_{(P)}$, je jeho vzor v okruhovém homomorfismu φ prvoideálem v R: je-li $x.y \in \rho(J)$, pak $\varphi(x).\varphi(y) \in J$, a tedy $\varphi(x) \in J$ nebo $\varphi(y) \in J$, tj. $x \in \rho(J)$ nebo $y \in \rho(J)$; přitom $\rho(J) \neq R$, neboť $\ell\rho(J) = J \neq \mathcal{R}_{(P)}$.

Podobně, je-li I prvoideál v R obsažený v P, pak $\ell(I)$ je prvoideálem v $\mathcal{R}_{(P)}$: je-li $\overline{(r,s)}.\overline{(r',s')} = \overline{(rr', ss')} \in \ell(I)$, pak existují $i \in I$ a $t, t' \in S$ taková, že $(rr't - ss'i)t' = 0$. Protože $ss't'i \in I$ a $tt' \notin I$, máme $rr' \in I$ a tedy $r \in I$ nebo $r' \in I$, tj. $\overline{(r,s)} \in \ell(I)$ nebo $\overline{(r',s')} \in \ell(I)$; přitom $\ell(I) \neq \mathcal{R}_{(P)}$, neboť $I \cap S = \emptyset$ (viz. 2.31).

Protože zobrazení ℓ a ρ zřejmě zachovávají částečné uspořádání inkluzí, zbývá jen dokázat, že pro každý prvoideál I okruhu R obsažený v P platí $\rho(\ell(I)) = I$. Protože $1 \in S$, je jistě $I \subseteq \rho(\ell(I))$. Naopak, je-li $r \in \rho(\ell(I))$, pak existují $i \in I$ a $s, s' \in S$ taková, že $(rs - i)s' = 0$. Protože $is' \in I$ a $ss' \notin I$, je $r \in I$.

Z předchozího a z 2.33 a 2.34.(3) plyne, že $\ell(P) = PS^{-1}$ je jediný maximální ideál okruhu $\mathcal{R}_{(P)}$. □

Speciálně, Věta 2.38 umožňuje zkoumat prvoideály obsažené v daném prvoideálu p okruhu R (zkoumáním prvoideálů v lokálním okruhu $R_{(p)}$). Naopak, prvoideály obsahující p odpovídají vzájemně jednoznačně prvoideálům faktorového okruhu R/p (viz. Lemma 2.33).

Na závěr se podívejme, jak se zjednoduší při lokalizaci struktura částečně uspořádané množiny ideálů okruhu celých čísel:

Příklad 2.39. Nechť $\mathcal{R} = \mathbb{Z}$, $I_0 = \{0\}$ a $I_p = \mathbb{Z}p$, kde p je prvočíslo. Podle 2.36 je $\mathbb{Z}_{(I_0)} = \mathbb{Q}$ těleso, tedy $\mathbb{Z}_{(I_0)}$ má jen triviální ideály (viz. 2.13).

Protože I_0 je kromě I_p jediný prvoideál v $\mathbb{Z}$ obsažený v I_p, má lokální obor integrity $\mathbb{Z}_{(I_p)} \subseteq \mathbb{Q}$ jen dva prvoideály: $\mathbb{Z}_{(I_p)}.0$ a $\mathbb{Z}_{(I_p)}.p$. Protože prvky $\mathbb{Z}$ nedělitelné p jsou invertibilní v $\mathbb{Z}_{(I_p)}$, jsou všechny nenulové ideály okruhu $\mathbb{Z}_{(I_p)}$ tvaru $\mathbb{Z}_{(I_p)}.p^n$ $(n \in \mathbb{N})$. Zobrazení ℓ tedy

převádí množinu všech (hlavních) ideálů okruhu celých čísel částečně uspořádanou inkluzí (dělitelností generátorů) na množinu $\{p^n \mid n \in \mathbb{N}\} \cup \{0\}$ lineárně uspořádanou dělitelností.

Poznámka 2.40. Podle 2.39 jsou $I_0 \subsetneq I_p$ jediné ostře rostoucí řetězce prvoideálů v $\mathbb{Z}$. Podobné lze ukázat, že všechny ostře rostoucí řetězce prvoideálů v polynomiálním okruhu $R = K[x_1, \dots, x_n]$ z 2.37 mají délku $\leq n$ (maximálním takovým řetězcem je například řetězec prvoideálů $0 \subsetneq Rx_1 \subsetneq \cdots \subsetneq \sum_{i \leq n} Rx_i$); totéž platí i pro souřadnicový okruh algebraické množiny A z 2.37. Maximální délka ostře rostoucích řetězců prvoideálů v komutativním okruhu se nazývá *Krullovou dimenzí* okruhu a je jedním ze základních invariantů zkoumaných v komutativní algebře.

2.3. **Moduly.**

Definice 2.41. Nechť $\mathcal{R} = (R, +_R, -_R, 0_R, \cdot_R, 1_R)$ je okruh. Pak $\mathcal{M} = (M, +, -, 0, \cdot r \ (r \in R))$ je *pravý R-modul*, pokud:

(1) $(M, +, -, 0)$ je komutativní grupa,

a pro každé $r \in R$ je $\cdot r$ unární operace na M splňující

(2) $\forall r \in R \, \forall m, m' \in M : (m + m') \cdot r = mr + m'r$;
(3) $\forall r, s \in R \, \forall m \in M : m(r +_R s) = mr + ms$;
(4) $\forall r, s \in R \, \forall m \in M : m(r \cdot_R s) = (m \cdot r) \cdot s$;
(5) $\forall m \in M : m \cdot 1_R = m$.

Poznámka 2.42. Pro každou komutativní grupu $(M, +, -, 0)$ tvoří vsechny grupové homomorfismy $f : M \to M$ *okruh endomorfismů* grupy M (značení: $\mathrm{End}(M)$): jeho jednotkovým prvkem je identický endomorfismus na M, a násobení je v něm definováno jako skládání zobrazení následovně: $f * g : m \mapsto ((m)f)g$.

Identity (2)–(5) z 2.41 platí právě tehdy když zobrazení $\varphi : R \to \mathrm{End}(M)$, přiřazující každému prvku $r \in R$ unární operaci $- \cdot r$, je okruhový homomorfismus $\mathcal{R}$ do $\mathrm{End}(M)$. Tedy moduly nad okruhem $\mathcal{R}$ jsou vlastně reprezentace okruhu $\mathcal{R}$ v okruzích endomorfismů komutativních grup.

Analogicky definujeme pojem *levého R-modulu*: unární operace příslušná prvku $r \in R$ je definována jako násobení zleva, a platí analogie identit (2)–(5) pro násobení $r \cdot -$. Pro zobrazení $\varphi\prime : R \to \mathrm{End}(M)$, přiřazující každému prvku $r \in R$ unární operaci $r \cdot -$, pak ovšem platí $\varphi'(r.s) = \varphi'(s) * \varphi'(r)$.

Pokud však na R definujeme nové násobení vztahem $r.'s = s.r$, bude $\mathcal{R}^{op} = (R, +, -, 0, .', 1)$ také okruhem, tzv. *opačným okruhem* k okruhu $\mathcal{R}$, a zobrazení $\varphi\prime : R \to \mathrm{End}(M)$ bude okruhovým homomorfismem $\mathcal{R}^{op}$ do $\mathrm{End}(M)$. Levé $\mathcal{R}$-moduly se takto ztotožní s pravými $\mathcal{R}^{op}$-moduly. (Je-li $\mathcal{R}$ komutativní okruh, pak $\mathcal{R} = \mathcal{R}^{op}$, a namísto levých resp. pravých R-modulů mluvíme prostě o R-modulech).

Nechť R je K-algebrou nad komutativním tělesem K. Pak můžeme na M definovat strukturu vektorového prostoru nad K vztahem $mk = m \cdot (1k)$. Z 2.4 ovšem máme $(1k).r = 1.(rk) = (1.r)k = rk = r.(1k)$, a tedy $\varphi(r) = - \cdot r$ je dokonce homomorfismus K-algebry R do K-algebry všech endomorfismů vektorového prostoru M. Proto se někdy v tomto případě místo termínu modul používá termín *lineární reprezentace K-algebry R*.

Příklad 2.43. (1) Nechť K je komutativní těleso. Pak K-moduly jsou právě všechny vektorové prostory nad K (ne nutně konečné dimenze nad K).

(2) $\mathbb{Z}$-moduly jsou právě všechny komutativní grupy. Operace $\cdot z$ v $(M, +, -, 0, \cdot z\ (z \in \mathbb{Z}))$ je totiž v tomto případě odvozena z operací $+$ a $-$, neboť $m \cdot z = \underbrace{m + \cdots + m}_{z\times}$.

(3) Nechť K je komutativní těleso, G je graf s konečnou množinou vrcholů V a množinou (orientovaných, násobných) hran H a $\langle KG\rangle$ je algebra cest grafu G definovaná v 2.7.

Moduly nad $\langle KG\rangle$ lze ztotožnit s K-lineárními reprezentacemi grafu G v následujícím smyslu:

K-lineární reprezentací grafu G rozumíme objekt, vzniklý nahražením všech vrcholů grafu $v_1, \dots$ vektorovými prostory $V_1, \dots$ nad K, a orientovaných hran $h_1, \dots$ K-lineárními zobrazeními $H_1, \dots$, kde $H_k : V_i \to V_j$ pokud orientovaná hrana h_k vede z vrcholu v_i do vrcholu v_j.

Každý pravý $\langle KG\rangle$-modul M určuje K-lineární reprezentaci grafu G následovně: vrchol v je nahražen vektorovým prostorem Mv $(\subseteq M)$; orientovaná hrana h vedoucí z v_i do vrcholu v_j je nahražena K-lineárním zobrazením $H : V_i \to V_j$ definovaným vztahem $m \mapsto m.h$ (to je korektní, neboť $v_i.h = h = h.v_j$). (Poznamenejme ještě, že K-lineární reprezentace grafu G tvoří kategorii ve smyslu následující sekce. Zmíněné ztotožnění lze pak rozšířit do ekvivalence kategorie všech pravých $\langle KG\rangle$-modulů a kategorie všech K-lineárních reprezentací grafu G).

Poznámka 2.44. Moduly se vyskytují v celé řadě dalších, zdánlivě spolu nesouvisejících, kontextů. V Poznámce 1.85 jsme již zmínili jejich roli v teorii reprezentací grup: reprezentace lze ekvivalentně studovat jako moduly nad příslušnou grupovou algebrou. V geometrii a teoretické fyzice hrají důležitou roli Lieovy algebry. Jejich reprezentace lze ekvivalentně zkoumat jako moduly nad tzv. obalujícími algebrami. A v moderní algebraické geometrii hrají moduly klíčovou roli v Grothendieck–Serrově teorii kvazikoherentních svazků na schematech.

Nyní stručně zmíníme některé elementární vlastnosti modulů. Následující tvrzení a jejich důkazy jsou snadnými rozšířeními příslušných vět v sekci 1.2 (pro komutativní grupy): při důkazech se jen navíc ověřuje kompatibilita se všemi unárními operacemi $\cdot r$ $(r \in R)$.

Definice 2.45. Nechť $\mathcal{R}$ je okruh a $\mathcal{M} = (M, +, -, 0, \cdot r\ (r \in R))$ je pravý $\mathcal{R}$-modul. Potom $\mathcal{N} = (N, +', -', 0', \cdot' r\ (r \in R))$ je *podmodul* v $\mathcal{M}$, pokud $N \subseteq M$ a $+', -', 0', \cdot' r$ jsou po řadě restrikce $+, -, 0, \cdot r$. To jest, pokud $(N, +', -', 0')$ je podgrupa v $(M, +, -, 0)$ uzavřená na všechny unární operace $\cdot r$ $(r \in R)$.

Pro každý okruh $\mathcal{R} = (R, +_R, -_R, 0_R, \cdot_R, 1_R)$ je $(R, +_R, -_R, 0_R, \cdot_R r\ (r \in R))$ pravým $\mathcal{R}$-modulem, tzv. *regulárním* pravým $\mathcal{R}$-modulem. Podmoduly regulárního pravého $\mathcal{R}$-modulu (přesněji, jejich nosiče) splývají s pravými ideály okruhu $\mathcal{R}$.

Poznámka 2.46. Nechť $\mathcal{R}$ je okruh. Je-li $\mathcal{M}$ pravý $\mathcal{R}$-modul a $\mathcal{N}$ je podmodul v $\mathcal{M}$, potom na faktorové grupě M/N lze definovat operaci $\bar{\cdot} r$ $(r \in R)$ následovně: $(m+N)\bar{\cdot} r = m \cdot r + N$. Potom $(M/N, \overline{+}, \overline{-}, \overline{0}, \bar{\cdot} r\ (r \in R))$ je pravý $\mathcal{R}$-modul, nazývaný *faktorovým modulem* $\mathcal{M}$ podle $\mathcal{N}$.

Definice 2.47. Nechť $\mathcal{R}$ je okruh a $\mathcal{M} = (M, +, -, 0, \cdot r\ (r \in R))$, $\mathcal{M}' = (M', +', -', 0', \cdot' r\ (r \in R))$ jsou dva pravé $\mathcal{R}$-moduly. Potom zobrazení $\varphi\colon M \to M'$ je *R-homomorfismus*, pokud φ je grupový homomorfismus takový, že $\forall\, m \in M\ \forall\, r \in R\colon \varphi(m \cdot r) = \varphi(m) \cdot' r$.

Poznámka 2.48. Do konce této kapitoly bude $\mathcal{R}$ vždy značit okruh, Mod-$\mathcal{R}$ třídu všech pravých $\mathcal{R}$-modulů a $\mathrm{Hom}_{\mathcal{R}}(M, M')$ množinu všech $\mathcal{R}$-homomorfismů z M do M'.

Věta 2.49 (o homomorfismu pro moduly)**.** *Nechť $\mathcal{M}, \mathcal{M}' \in$ Mod-$\mathcal{R}$, $\varphi \in Hom_{\mathcal{R}}(M, M')$, $\mathcal{N}$ je podmodul v $\mathcal{M}$, pro který platí: $N \subseteq Ker\,\varphi$. Potom existuje právě jeden $\mathcal{R}$-homomorfismus $\psi \in Hom_{\mathcal{R}}(M/N, M')$ takový, že $\psi \odot \pi_N = \varphi$, kde $\pi_N : M \to M/N$ je kanonická projekce definována vztahem $m \mapsto m + N$.*

Důkaz. Definujeme $\psi(m + N) = \varphi(m)$ a zbytek je analogií 1.44. □

Důkaz následujících vět je snadnou modifikací důkazů 1.46, 1.48 a 1.51.

Věta 2.50 (1. věta o izomorfismu pro moduly)**.** *Nechť $\mathcal{M}, \mathcal{M}' \in$ Mod-$\mathcal{R}$, $\varphi \in Hom_{\mathcal{R}}(M, M')$. Pak $Ker\,\varphi$ je podmodul v $\mathcal{M}$, $Im\,\varphi$ je podmodul v $\mathcal{M}'$ a existuje $\mathcal{R}$-izomorfismus: $(M/Ker\,\varphi) \simeq Im\,\varphi$.*

Věta 2.51 (2. věta o izomorfismu pro moduly)**.** *Nechť $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3 \in$ Mod-$\mathcal{R}$, $\mathcal{M}_3$ je podmodul v $\mathcal{M}_2$ a $\mathcal{M}_2$ je podmodul v $\mathcal{M}_1$. Potom existuje $\mathcal{R}$-izomorfismus $(M_1/M_3)/(M_2/M_3) \simeq (M_1/M_2)$.*

Věta 2.52 (3. věta o izomorfismu pro moduly)**.** *Nechť $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3 \in$ Mod-$\mathcal{R}$ a $\mathcal{M}_1, \mathcal{M}_2$ jsou podmoduly v $\mathcal{M}_3$. Potom existuje $\mathcal{R}$-izomorfismus $(M_1 + M_2)/M_1 \simeq M_2/(M_1 \cap M_2)$.*

2.4. **Kategorie modulů.** Velmi účinným nástrojem moderní matematiky je teorie kategorií, jejíž počátky jsou spojeny právě s teorií modulů a homologickou algebrou. Zakladní pojem této teorie, pojem kategorie, je jednoduchý a přirozený:

Definice 2.53. Nechť $\mathcal{K}^o$ je třída a pro každé dva prvky $A, B \in \mathcal{K}^o$ je $\mathcal{K}^m(A, B)$ množina. Prvky množiny $\mathcal{K}^m(A, B)$ budeme zapisovat jako „šipky" $f : A \to B$, přičemž A nazveme *doménou* a B *kodoménou* f. Předpokládejme, že pro každou trojici $A, B, C \in \mathcal{K}^o$ je dáno zobrazení

$$\circ : \mathcal{K}^m(B, C) \times \mathcal{K}^m(A, B) \to \mathcal{K}^m(A, C).$$

Šipky $f : A \to B$ a $g : C \to D$ nazveme *navazujícími* pokud $B = C$; pro ně $g \circ f$ nazveme *složením* g a f v $\mathcal{K}$. Označme $\mathcal{K}^m = \bigcup_{A,B \in \mathcal{K}^o} \mathcal{K}^m(A, B)$.

Trojici $\mathcal{K} = (\mathcal{K}^o, \mathcal{K}^m, \circ)$ nazveme *kategorií*, pokud jsou splněny následující dvě podmínky:

(i) pro každé tři šipky $h : C \to D$, $g : B \to C$, $f : A \to B$, platí

$$h \circ (g \circ f) = (h \circ g) \circ f,$$

(ii) pro každý prvek $A \in \mathcal{K}^o$ existuje právě jedna šipka $\mathrm{id}_A \in \mathcal{K}^m(A, A)$ taková, že pro každé šipky $f : A \to B$ a $g : C \to A$ platí

$$f \circ \mathrm{id}_A = f \quad \text{a} \quad \mathrm{id}_A \circ g = g.$$

Pokud $\mathcal{K}$ je kategorie, pak prvky třídy $\mathcal{K}^o$ nazýváme *objekty* kategorie $\mathcal{K}$, prvky třídy $\mathcal{K}^m$ nazýváme *morfismy* kategorie $\mathcal{K}$, "parciální zobrazení" $\circ$ nazýváme *skládáním morfismů* v $\mathcal{K}$ a id_A *identitou* na objektu A.

Příklad 2.54. Nechť $\mathcal{S}^o$ je třída všech množin, $\mathcal{S}^m(A, B)$ je množina všech zobrazení z množiny A do množiny B a $\circ$ je skládání zobrazení. Pak trojici $(\mathcal{S}^o, \mathcal{S}^m, \circ)$ nazýváme *kategorií množin*.

Příklad 2.55. Nechť $\mathcal{G}^o$ je třída všech grup, $\mathcal{G}^m(G, H)$ je množina všech grupových homomorfismů grupy G do grupy H a $\circ$ je skládání zobrazení. Pak trojici $(\mathcal{G}^o, \mathcal{G}^m, \circ)$ nazýváme *kategorií grup*.

Příklad 2.56. Nechť $\mathcal{R}$ je okruh. Nechť $\mathcal{M}^o_{\mathcal{R}}$ je třída všech pravých $\mathcal{R}$-modulů, $\mathcal{M}^m_{\mathcal{R}}(M,N)$ je množina všech $\mathcal{R}$-homomorfismů z pravého $\mathcal{R}$-modulu M do pravého $\mathcal{R}$-modulu N a $\circ$ nechť je skládání zobrazení. Pak trojici $\mathcal{M}\text{od-}\mathcal{R} = (\mathcal{M}^o_{\mathcal{R}}, \mathcal{M}^m_{\mathcal{R}}, \circ)$ nazýváme *kategorií pravých R-modulů*.

Všechny výše uvedené příklady jsou tzv. *konkrétní kategorie*, tj. objekty těchto kategorií jsou množiny, morfismy jsou zobrazení, $\circ$ je obvyklé skládání zobrazení, a id_A je identické zobrazení objektu A do sebe.

V teorii kategorií nahlížíme objekty dané kategorie jako "body" a morfismy jako "šipky" mezi těmito "body". Části dané kategorie se pak dají nahlížet jako diagramy ve smyslu následující definice:

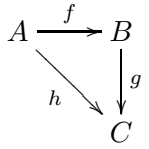
Definice 2.57. Nechť $\mathcal{K} = (\mathcal{K}^o, \mathcal{K}^m, \circ)$ je kategorie. Uspořádanou dvojici $\mathcal{D} = (\mathcal{D}^o, \mathcal{D}^m)$ nazveme *diagramem* v kategorii $\mathcal{K}$, pokud $\mathcal{D}^o$ je neprázdný soubor objektů kategorie $\mathcal{K}$, pro každá $A, B \in \mathcal{D}^o$ je $\mathcal{D}^m(A,B)$ podmnožinou $\mathcal{K}^m(A,B)$ a $\mathcal{D}^m = \bigcup_{A,B\in\mathcal{D}^o} \mathcal{D}^m(A,B)$.

Definice 2.58. (1) Nechť $\mathcal{D} = (\mathcal{D}^o, \mathcal{D}^m)$ je diagram. Pokud $\mathcal{D}^m = \emptyset$, pak se $\mathcal{D}$ nazývá *diskrétní diagram* v $\mathcal{K}$.

(2) Nechť $\mathcal{D} = (\mathcal{D}^o, \mathcal{D}^m)$ je diagram. Pokud pro každou dvojici objektů $A, B \in \mathcal{D}^o$ a každé dvě cesty (= posloupnosti navazujících šipek) z $\mathcal{D}^m$ začínající v A a končící v B jsou morfismy kategorie $\mathcal{K}$ určené složením šipek v těchto posloupnostech totožné, pak se $\mathcal{D}$ nazývá *komutativní diagram*.

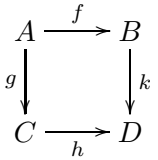
Příklad 2.59. Základními příklady komutativních diagramů jsou komutativní trojúhelník a komutativní čtverec:

Trojúhelník



je komutativní pravě když $g \circ f = h$.

Čtverec



je komutativní pravě když $k \circ f = h \circ g$.

Následující pojem limity diagramu v kategorii koncentruje informaci z daného diagramu do jediného objektu kategorie:

Definice 2.60. Nechť $\mathcal{K} = (\mathcal{K}^o, \mathcal{K}^m, \circ)$ je kategorie a $\mathcal{D} = (\mathcal{D}^o, \mathcal{D}^m)$ je diagram v $\mathcal{K}$.

Limita $\mathcal{D}$ v $\mathcal{K}$ je objekt $L \in \mathcal{K}^o$ a soubor morfismů $(\pi_A \mid A \in \mathcal{D}^o)$ kategorie $\mathcal{K}$ takový, že

(1) $\forall\, A \in \mathcal{D}^o\colon \pi_A \in \mathcal{K}^m(L,A)$

(2) $\forall\, A, B \in \mathcal{D}^o, \forall\, f \in \mathcal{D}^m(A,B)\colon f \circ \pi_A = \pi_B$

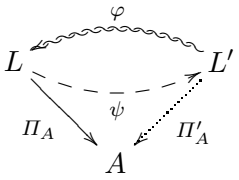
(3) Pro každé $L' \in \mathcal{K}^o$ a každý soubor morfismů $(\pi'_A \mid A \in \mathcal{D}^o)$ kategorie $\mathcal{K}$ splňující podmínky (1) a (2) pro L' a $(\pi'_A \mid A \in \mathcal{D}^o)$ existuje právě jeden morfismus $\varphi \in \mathcal{K}^m(L', L)$ takový, že pro každé $A \in \mathcal{D}^o$ platí $\pi_A \circ \varphi = \pi'_A$.

Definice 2.61. Nechť $\mathcal{K} = (\mathcal{K}^o, \mathcal{K}^m, \circ)$ je kategorie a nechť $\varphi : A \to B$ je morfismus této kategorie. Řekneme, že φ je *izomorfismus* v kategorii $\mathcal{K}$, pokud existuje morfismus $\psi : B \to A$ kategorie $\mathcal{K}$ takový, že $\psi \circ \varphi = \mathrm{id}_A$ a $\varphi \circ \psi = \mathrm{id}_B$. Objekty A a B pak nazýváme *izomorfními* v kategorii $\mathcal{K}$.

Lemma 2.62. *Nechť $\mathcal{K} = (\mathcal{K}^o, \mathcal{K}^m, \circ)$ je kategorie a $\mathcal{D}$ je diagram v $\mathcal{K}$. Potom až na izomorfismus existuje nejvýše jedna limita diagramu $\mathcal{D}$ v kategorii $\mathcal{K}$.*

Přesněji, je-li $L \in \mathcal{K}^o$ se souborem morfismů $(\pi_A \mid A \in \mathcal{D}^o)$ (resp. $L' \in \mathcal{K}^o$ se souborem morfismů $(\pi'_A \mid A \in \mathcal{D}^o)$) limitou diagramu $\mathcal{D}$ v $\mathcal{K}$, potom existují morfismy $\psi : L \to L'$ a $\varphi : L' \to L$ takové, že $\psi \circ \varphi = id_{L'}$ a $\varphi \circ \psi = id_L$, a navíc $\pi'_A = \pi_A \circ \varphi$ a $\pi_A = \pi'_A \circ \psi$ pro každé $A \in \mathcal{D}^o$.

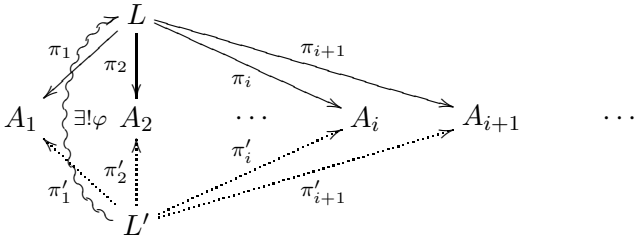
Důkaz.



Protože L' splňuje podmínky (1) a (2) Definice 2.60, existuje morfismus $\varphi \in \mathcal{K}^m(L', L)$, pro který platí $\pi'_A = \pi_A \circ \varphi$. Podobně existuje morfismus $\psi \in \mathcal{K}^m(L, L')$, pro který platí $\pi_A = \pi'_A \circ \psi$. Tedy $\pi_A \circ \varphi \circ \psi = \pi'_A \circ \psi = \pi_A$ a $\pi'_A \circ \psi \circ \varphi = \pi_A \circ \varphi = \pi'_A$. Z jednoznačnosti morfismu v podmínce (3) Definice 2.60 a ze vztahu $\pi_A \circ \mathrm{id}_L = \pi_A$ resp. $\pi'_A \circ \mathrm{id}_{L'} = \pi'_A$ dostáváme $\varphi \circ \psi = \mathrm{id}_L$ resp. $\psi \circ \varphi = \mathrm{id}_{L'}$. Tedy φ a ψ jsou hledanými izomorfismy. □

Limita diskrétního diagramu $\mathcal{D} = (\mathcal{D}^o, \emptyset)$ se nazývá *součinem* souboru objektů $\mathcal{D}^o$ a značí se $\prod_{A \in \mathcal{D}^o} A$. Součiny vždy existují v kategoriích modulů:

Příklad 2.63. Nechť $\mathcal{K} = \mathcal{M}\mathrm{od}\text{-}\mathcal{R}$ a $\mathcal{D} = (\mathcal{D}^o, \emptyset)$ je diskrétní diagram v $\mathcal{K}$.



Nechť $\mathcal{D}^o = (A_i \mid i \in I)$. Položme $L = X_{i \in I} A_i$ (kartézský součin souboru množin A_i, tj. $L = \{f \mid f : I \to \bigcup_{i \in I} A_i,\ \forall i \in I : f(i) \in A_i\}$; tedy L je množinou všech posloupností f délky $|I|$ takových, že pro každé $i \in I$ je i-tá složka f prvkem A_i).

Na L definujeme strukturu pravého R-modulu „po složkách". Pro $f, g \in L$ a $i \in I$ je tedy

$$\begin{aligned}
(f+g)(i) &= f(i) +_{A_i} g(i) \\
(-f)(i) &= -_{A_i}(f(i)) \\
(f \cdot r)(i) &= (f(i)) \cdot_{A_i} r \\
0 \colon I &\to \bigcup_{j \in I} A_j \\
j &\mapsto 0_{A_j}
\end{aligned}$$

Systém morfismů $(\pi_i \mid i \in I)$ definujeme následovně:

$$\begin{aligned} \pi_i \colon L &\to A_i \\ f &\mapsto f(i) \end{aligned}$$

π_i je tedy projekce na i-tou složku. Ukážeme, že L se souborem morfismů $(\pi_i \mid i \in I)$ je součinem souboru $\mathcal{D}^o$ v kategorii $\mathcal{M}$od-$\mathcal{R}$. Podmínky (1) a (2) Definice 2.60 jsou zřejmě splněny.

Nechť (viz. obrázek výše) existuje objekt $L' \in \mathcal{K}^o$ a soubor morfismů $(\pi'_i \mid i \in I)$ splňující podmínky (1) a (2) z Definice 2.60. Pak zobrazení φ definované vztahem

$$\begin{aligned} \varphi \colon L' &\to L \\ x &\mapsto f_x \end{aligned}$$

kde

$$\begin{aligned} f_x \colon I &\to \bigcup_{i \in I} A_i \\ i &\mapsto \pi'_i(x) \end{aligned}$$

je R-homomorfismem, neboť každé π'_i $(i \in I)$ je R-homomorfismus. Navíc platí, že pro každé $i \in I$ a každé $x \in L'$ je $(\pi_i \circ \varphi)(x) = \pi(f_x) = \pi'(x)$, tj. pro každé $i \in I$ platí $\pi_i \circ \varphi = \pi'_i$.

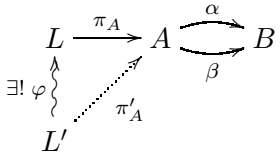
Zbývá dokázat jednoznačnost R-homomorfismu φ. Nechť $\varphi' \colon L' \to L$ je R-homomorfismus, pro který platí, že pro každé $i \in I$ je $\pi_i \circ \varphi' = \pi'_i$. Pak pro každé $x \in L'$ a každé $i \in I$ je $(\pi_i \circ \varphi)(x) = \pi'_i(x) = (\pi_i \circ \varphi')(x)$. Tedy φ i φ' zobrazí prvek x z L' na tutéž posloupnost v L, tj. $\varphi = \varphi'$.

Limita následujícího diagramu v kategorii $\mathcal{K}$

$$A \underset{\beta}{\overset{\alpha}{\rightrightarrows}} B$$

se nazývá *ekvalizátor* morfismů α a β v $\mathcal{K}$. Ekvalizátory vždy existují v kategoriích modulů:

Příklad 2.64. Nechť $\mathcal{K} = \mathcal{M}$od-$\mathcal{R}$.



Položme $L = \{a \in A \mid \alpha(a) = \beta(a)\}$; zřejmě L je podmodulem v A. Označme jako π_A inkluzi $L \hookrightarrow A$. Pak $\alpha \circ \pi_A = \beta \circ \pi_A$, tedy můžeme položit $\pi_B = \alpha \circ \pi_A$.

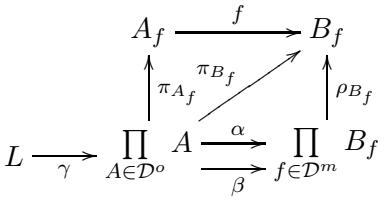
Nechť existuje pravý R-modul L' a R-homomorfismy π'_A, π'_B splňující (1) a (2) z definice 2.60. Pro R-homomorfismus π'_A musí platit $\pi'_B = \alpha \circ \pi'_A = \beta \circ \pi'_A$, tedy Im $\pi'_A \subseteq L$. R-homomorfismus φ v Definici 2.60 tedy můžeme definovat vztahem $\varphi(x) = \pi'_A(x)$ pro každé $z \in L'$. Pokud existuje $\mathcal{R}$-homomorfismus $\varphi' \colon L' \to L$ splňující podmínku (3), pak nutně $\varphi' = \varphi$, neboť π_A je inkluze. Tedy R-modul L spolu s R-homomorfismy π_A a π_B je ekvalizátorem α a β v $\mathcal{K}$.

Definice 2.65. Nechť $\mathcal{K}$ je kategorie. $\mathcal{K}$ se nazývá *úplná* pokud každý diagram $\mathcal{D}$ má v $\mathcal{K}$ limitu.

Následující věta vysvětluje, proč jsme se zatím podrobněji zabývali jen konstrukcí součinů a ekvalizátorů:

Věta 2.66. *Nechť $\mathcal{K}$ je kategorie. Potom $\mathcal{K}$ je úplná právě když v $\mathcal{K}$ existují součiny a ekvalizátory.*

Důkaz. Implikace $\Rightarrow$ je zřejmá. Naopak, sestrojíme limitu obecného diagramu $\mathcal{D}$ v $\mathcal{K}$ za předpokladu, že v $\mathcal{K}$ existují součiny a ekvalizátory. Nechť $\mathcal{D} = (\mathcal{D}^o, \mathcal{D}^m)$ je diagram v $\mathcal{K}$.

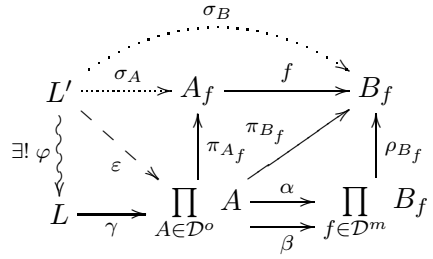


Nechť $\prod_{A\in\mathcal{D}^o} A$ spolu s morfismy $(\pi_A \mid A \in \mathcal{D}^o)$ je součinem souboru všech objektů diagramu $\mathcal{D}$, zatímco $\prod_{f\in\mathcal{D}^m} B_f$ spolu s morfismy $(\rho_{B_f} \mid f \in \mathcal{D}^m)$ je součinem souboru koncových objektů (kodomén) B_f všech morfismů f diagramu $\mathcal{D}$.

Užitím podmínek (1) a (2) z Definice 2.60 pro $L = \prod_{f\in\mathcal{D}^m} B_f$ a $L' = \prod_{A\in\mathcal{D}^o} A$ se souborem morfismů $(\pi_{B_f} \mid f \in \mathcal{D}^m)$ dostáváme existenci morfismu α s vlastností $\forall\, f \in \mathcal{D}^m\colon \rho_{B_f} \circ \alpha = \pi_{B_f}$.

Podobně, užitím podmínek (1) a (2) z Definice 2.60 pro $L = \prod_{f\in\mathcal{D}^m} B_f$ a $L' = \prod_{A\in\mathcal{D}^o} A$ se souborem morfismů $(f \circ \pi_{A_f} \mid f \in \mathcal{D}^m)$ dostáváme existenci morfismu β s vlastností $\forall\, f \in \mathcal{D}^m\colon \rho_{B_f} \circ \alpha = f \circ \pi_{A_f}$.

Nechť nyní L a γ, $\alpha\circ\gamma$ značí ekvalizátor morfismů α a β. Dokážeme, že $(L, \pi_A \circ \gamma\ (A \in \mathcal{D}^o))$ je limitou diagramu $\mathcal{D}$ v $\mathcal{K}$.



Ověříme podmínky Definice 2.60:

(1) Je zřejmé.

(2) Máme dokázat, že pro každý morfismus $f \in \mathcal{D}^m$ platí: $f \circ \pi_{A_f} \circ \gamma = \pi_{B_f} \circ \gamma$. Ale $\beta \circ \gamma = \gamma \circ \alpha$, tedy $f \circ \pi_{A_f} \circ \gamma = \rho_{B_f} \circ \beta \circ \gamma = \rho_{B_f} \circ \alpha \circ \gamma = \pi_{B_f} \circ \gamma$.

(3) Nechť L' a soubor morfismů $(\sigma_A \mid A \in \mathcal{D}^o)$ splňuje podmínky (1) a (2) z Definice 2.60. Protože $\prod_{A\in\mathcal{D}^o} A$ je součinem souboru $\mathcal{D}^o$, existuje morfismus $\varepsilon\colon L' \to \prod_{A\in\mathcal{D}^o} A$ takový, že $\forall\, A \in \mathcal{D}^o\colon \pi_A \circ \varepsilon = \sigma_A$.

Pro každé $f \in \mathcal{D}^m$ máme: $\rho_{B_f} \circ (\alpha \circ \varepsilon) = \pi_{B_f} \circ \varepsilon = \sigma_{B_f} = f \circ \sigma_{A_f} = f \circ \pi_{A_f} \circ \varepsilon = \rho_{B_f} \circ (\beta \circ \varepsilon)$.

Z jednoznačnosti morfismu v podmínce (3) definice součinu $\prod_{f\in\mathcal{D}^m} B_f$ plyne, že $\alpha \circ \epsilon = \beta \circ \epsilon$. Definice ekvalizátoru dává morfismus $\varphi\colon L' \to L$ takový, že $\gamma \circ \varphi = \varepsilon$, a tedy $\forall\, A \in \mathcal{D}^o\colon (\pi_A \circ \gamma) \circ \varphi = \sigma_A$.

Zbývá dokázat jednoznačnost morfismu φ. Nechť $\varphi' \colon L' \to L$ je morfismus pro který platí: $\pi_A \circ \gamma \circ \varphi' = \sigma_A$. Pak $\pi_A \circ (\gamma \circ \varphi) = \sigma_A = \pi_A \circ (\gamma \circ \varphi')$. Jednoznačnost morfismu v podmínce (3) definice součinu $\prod_{A \in \mathcal{D}^o} A$ dává $\gamma \circ \varphi = \gamma \circ \varphi' = \varepsilon$. Z jednoznačnosti morfismu φ v definici ekvalizátoru máme konečně $\varphi = \varphi'$.

□

Z Příkladů 2.63 a 2.64 a Věty 2.66 máme okamžitý

Důsledek 2.67. *Kategorie $\mathcal{M}$od-$\mathcal{R}$ je úplná.*

Velkou výhodou kategoriálního přístupu k algebře je snadná možnost dualizace získaných výsledků pomocí pojmu duální kategorie, která má oproti výchozí kategorii stejné "body", ale obrácené "šipky" a obrácené pořadí skládání morfismů:

Definice 2.68. Nechť $\mathcal{K} = (\mathcal{K}^o, \mathcal{K}^m, \circ)$ je kategorie. Pak uspořádaná trojice $\mathcal{K}^* = (\mathcal{K}^{*o}, \mathcal{K}^{*m}, \circ^*)$ se nazývá *duální kategorií* ke kategorii $\mathcal{K}$, pokud

(1) $\mathcal{K}^{*o} = \mathcal{K}^o$
(2) $\forall A, B \in \mathcal{K}^o \colon \mathcal{K}^{*m}(A, B) = \mathcal{K}^m(B, A)$
(3) $\forall f \in \mathcal{K}^m(A, B), \forall g \in \mathcal{K}^m(B, C) \colon f \circ^* g = g \circ f$.

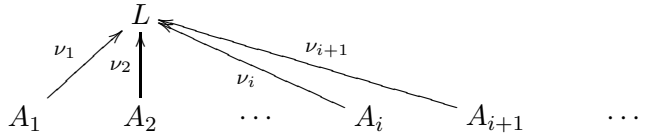
Definice 2.69. Nechť $\mathcal{K}$ je kategorie.

(1) *Kolimita* diagramu $\mathcal{D}$ v $\mathcal{K}$ je definována jako limita diagramu $\mathcal{D}$ v $\mathcal{K}^*$.
(2) *Kosoučin* souboru v $\mathcal{K}$ je definován jako součin téhož souboru v $\mathcal{K}^*$.
(3) *Koekvalizátor* α a β ($\alpha, \beta \in \mathcal{K}^m(A, B)$) v $\mathcal{K}$ je definován jako ekvalizátor α a β v $\mathcal{K}^*$.
(4) Kategorie $\mathcal{K}$ je *koúplná*, pokud každý diagram $\mathcal{D}$ v $\mathcal{K}$ má v $\mathcal{K}$ kolimitu.

Podle Věty 2.66 je kategorie $\mathcal{K}$ koúplná právě když v $\mathcal{K}$ existují kosoučiny a koekvalizátory.

Speciálně, k důkazu koúplnosti kategorií modulů $\mathcal{M}$od-$\mathcal{R}$ stačí pouze sestojit kolimity diskrétních diagramů a koekvalizátory v $\mathcal{M}$od-$\mathcal{R}$. To provedeme v následujících dvou příkladech:

Příklad 2.70. Nechť $\mathcal{K} = \mathcal{M}$od-$\mathcal{R}$. Uvažme diskrétní diagram $\mathcal{D} = (\mathcal{D}^o, \emptyset)$. Sestrojíme kosoučin souboru $\mathcal{D}^o = (M_i \mid i \in I)$.



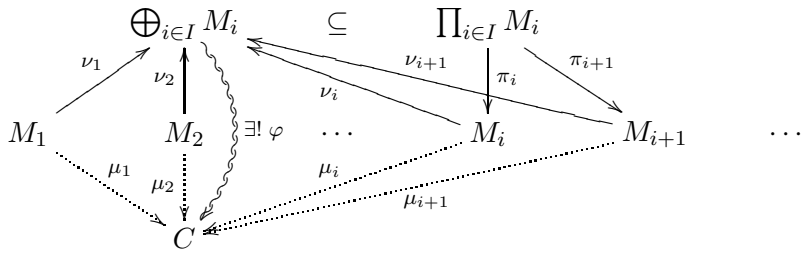
Objekt $L \in$ Mod-$\mathcal{R}$ definuje následovně: $L = \{f \mid f \colon I \to \bigcup_{i \in I} M_i,\ f(i) \in M_i,$ a množina $\{i \in I \mid f(i) \neq 0\}$ je konečná $\}$. L je zřejmě nosičem podmodulu modulu $P = \prod_{i \in I} M_i$ tvořeným všemi skoro všude nulovými posloupnostmi z P. Soubor morfismů $(\nu_i \mid i \in I)$ definujeme následovně:

$$\begin{aligned} \nu_i \colon M_i &\to L \\ m &\mapsto f_{m,i} \end{aligned}$$

kde $f_{m,i}$ je definováno jako

$$\begin{aligned} f_{m,i} \colon I &\to \bigcup_{j \in I} M_j \\ i &\mapsto m \\ j \neq i &\mapsto 0_{M_j} \end{aligned}$$

Nyní dokážeme, že $\bigoplus_{i\in I} M_i$ se souborem $(\nu_i \mid i \in I)$ je kosoučinem souboru $\mathcal{D}^o$ v $\mathcal{M}$od-$\mathcal{R}$.



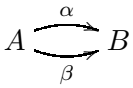
ν_i je zřejmě prvkem $\mathcal{K}^m(M_i, \bigoplus_{i\in I} M_i)$. Nechť C se souborem morfismů $(\mu_i \mid i \in I)$ splňuje podmínky (1) a (2) z definice kosoučinu (= součinu v duální kategorii). Definujme morfismus φ vztahem

$$\begin{aligned} \varphi\colon \bigoplus_{i\in I} M_i &\to C \\ f &\mapsto \sum_{i\in I} \mu_i(\pi_i(f)) \end{aligned}$$

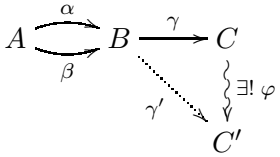
(Výraz $\sum_{i\in I} \mu_i(\pi_i(f))$ má smysl, protože $\pi_i(f) = 0$ pro skoro všechna $i \in I$.) Pro každé $i \in I$ a každé $m \in M_i$ platí $\sum_{j\in I} \mu_j(\pi_j(\nu_i(m))) = \mu_i(\pi_i(\nu_i(m))) = \mu_i(m)$. Tedy $\forall\, i \in I\colon \varphi \circ \nu_i = \mu_i$.

Zbývá ukázat jednoznačnost R-homomorfismu φ. Nechť $\varphi'\colon \bigoplus_{i\in I} M_i \to C$ je takový, že $\forall\, i \in I : \varphi' \circ \nu_i = \mu_i$. Dokážeme, že $\varphi' = \varphi$. Nechť $i \in I$ a $m \in M_i$. Podle předpokladu je $\varphi'(\nu_i(m)) = \mu_i(m)$, tedy φ' a φ se shodují na $\nu_i(M_i)$ pro každé $i \in I$. Protože φ a φ' jsou R-homomorfismy a každé $x \in \bigoplus_{i\in I} M_i$ je konečným součtem prvků z $\bigcup_{i\in I} \nu_i(M_i)$, je nutně $\varphi' = \varphi$.

Příklad 2.71. V tomto příkladě sestrojíme koekvalizátor, tj. kolimitu diagramu



v kategorii $\mathcal{K} = \mathcal{M}$od-$\mathcal{R}$.



Definujme podmodul $B' = \{b \in B \mid \exists\, a \in A\colon b = \alpha(a) - \beta(a)\}$ modulu B, a dále $C = B/B'$, a R-homomorfismus γ:

$$\begin{aligned} \gamma\colon B &\to C \\ b &\mapsto b + B' \end{aligned}$$

Pak $\gamma \circ \beta = \gamma \circ \alpha$. Ukážeme, že C s morfismy $\gamma \circ \alpha$ a γ je koekvalizátor α a β. Podmínky (1) a (2) z Definice 2.60 jsou pro diagram $\mathcal{D}$ v $\mathcal{K}^*$ zřejmé. Nechť C' je pravý $\mathcal{R}$-modul a nechť $\gamma' \in \mathcal{K}^m(B, C')$ je takový $\mathcal{R}$-homomorfismus, že $\gamma' \circ \beta = \gamma' \circ \alpha$. Máme $\gamma' \circ (\alpha - \beta) = 0$, čili $\operatorname{Ker} \gamma' \supseteq \operatorname{Im} (\alpha - \beta) = B' = \operatorname{Ker} \gamma$. Podle Věty 2.49 existuje právě jeden $\mathcal{R}$-homomorfismus $\varphi\colon C \to C'$, pro který platí $\varphi \circ \gamma = \gamma'$ a důkaz je hotov.

Důsledek 2.72. *Kategorie $\mathcal{M}$od-$\mathcal{R}$ je koúplná.*

Poznámka 2.73. Nechť $\mathcal{K} = \mathcal{M}\text{od-}\mathcal{R}$ a $\mathcal{D} = (\mathcal{D}^o, \emptyset)$ je diskrétní diagram, $\mathcal{D}^o = (M_i \mid i \in I)$. Podle Příkladu 2.70 je modul $\bigoplus_{i\in I} M_i$ vždy podmodulem v $\prod_{i\in I} M_i$, a pokud je $\mathcal{D}^o$ konečný, platí dokonce rovnost: $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$.

Teorie kategorií se nezabývá pouze jednotlivými kategoriemi, ale především "morfismy" mezi kategoriemi, tzv. funktory:

Definice 2.74. Nechť $\mathcal{K}$ a $\mathcal{L}$ jsou kategorie. Dvojice $F = (F^o, F^m)$ se nazývá *kovariantní funktor* z $\mathcal{K}$ do $\mathcal{L}$ pokud F^o zobrazuje $\mathcal{K}^o$ do $\mathcal{L}^o$, a F^m zobrazuje $\mathcal{K}^m$ do $\mathcal{L}^m$ tak, že pro každé objekty $A, B, C \in \mathcal{K}^o$ a každé morfismy v $\mathcal{K}^m$, $f : A \to B$ a $g : B \to C$, platí

(1) $F^m(f) \in \mathcal{L}^m(F^o(A), F^o(B))$;
(2) $F^m(g \circ f) = F^m(g) \circ F^m(f)$;
(3) $F^m(\mathrm{id}_A) = \mathrm{id}_{F^o(A)}$.

Pojem *kontravariantního funktoru* je definován analogicky: podmínka (3) je stejná, ale v (1) požadujeme $F^m(f) \in \mathcal{L}^m(F^o(B), F^o(A))$ a (2) je nahražena identitou $F^m(g \circ f) = F^m(f) \circ F^m(g)$. Tedy kontravariantní funktor z $\mathcal{K}$ do $\mathcal{L}$ je totéž, co kovariantní funktor z $\mathcal{K}$ do $\mathcal{L}^*$.

Příklad 2.75. Každý pravý R-modul M indukuje dva *základní* funktory z kategorie $\mathcal{M}\text{od-}\mathcal{R}$ do kategorie všech komutativních grup (= $\mathbb{Z}$-modulů):

(1) kovariantní funktor $\mathrm{Hom}_R(M, -) = (F^o, F^m)$ definovaný vztahy $F^o(N) = Hom_R(M, N)$ a $F^m(f) = Hom_R(M, f)$, kde $Hom_R(M, f) : Hom_R(M, A) \to Hom_R(M, B)$ je pro $f \in Hom_R(A, B)$ určeno vztahem $Hom_R(M, f)(g) = f \circ g$, a

(2) kontravariantní funktor $\mathrm{Hom}_R(-, M) = (G^o, G^m)$ definovaný $G^o(N) = Hom_R(N, M)$ a $G^m(f) = Hom_R(f, M)$, kde $Hom_R(f, M) : Hom_R(B, M) \to Hom_R(A, M)$ je pro $f \in Hom_R(A, B)$ určeno vztahem $Hom_R(f, M)(g) = g \circ f$.

Poznámka 2.76. Studium základních funktorů a jejich derivovaných funktorů je centrálním tématem matematické disciplíny zvané homologická algebra. Ta se používá i v mnohem obecnějších kategoriích, než jsou kategorie modulů, tzv. abelovských kategoriích.

Literatura

1. T. W. Hungerford: *Algebra*, Graduate Texts in Mathematics **73**, Springer Vlg., New York – Berlin 1980.

2. S. Mac Lane, G. Birkhoff: *Algebra*, 3rd ed., Chelsea, New York 1988.

3. C. Menini, F. van Oystaeyen: *Abstract Algebra*, M. Dekker, New York – Basel 2004.

4. S. Lang: *Algebra*, Revised 3rd ed., Graduate Texts in Mathematics **211**, Springer Vlg., New York – Berlin 2002.

5. L. Procházka a kol.: *Algebra*, Academia, Praha 1990.

6. E. B. Vinberg: *A Course in Algebra*, Graduate Studies in Mathematics **56**, Amer. Math. Soc., Providence 2003.

Rejstřík

K-algebra, 20

akce grupy na množině, 11
algebra cest grafu, 21
algebraická množina, 27
  ireducibilní, 28

centrum
  grupy, 12
  okruhu, 19
charakter
  regulární reprezentace, 19
  reprezentace, 17

diagram, 32
  diskrétní, 32
  komutativní, 32
doména morfismu, 31
dělení v grupoidu, 4

ekvalizátor, 34

faktorová grupa, 9
funktor
  kontravariantní, 38
  kovariantní, 38
  základní, 38

grupa, 4
  alternující, 5
  cyklická, 7
  jednoduchá, 16
  komutativní, 4
  nilpotentní, 12
  obecná lineární, 16
  projektivní speciální lineární, 16
  speciální lineární, 16
  symetrická, 4
  zbytkových tříd modulo n, 9
grupoid, 2

homomorfismus
  grupový, 5
  modulový, 30
  monoidový, 3
  okruhový, 22
horní centrální řada, 12

ideál, 21
  extenze do podílového okruhu, 26
  hlavní, 22
  kontrakce, 26
  maximální, 26
izomorfismus
  grupový, 5, 8
  monoidový, 3
  okruhový, 22
  v kategorii, 33

jednotka, 2
jádro homomorfismu, 3

kanonická projekce, 9, 23
kategorie, 31
  duální, 36
  grup, 31
  koúplná, 36
  množin, 31
  modulů, 32
  úplná, 34
kodoména morfismu, 31
koekvalizátor, 36
kolimita, 36
kosoučin v kategorii, 36
krácení v grupoidu, 4
kvazigrupa, 4

lemma
  Burnsideovo, 12
limita diagramu, 32
lokalizace, 27
lupa, 4

modul, 29
  faktorový, 30
  nad algebrou cest grafu, 30
  regulární, 30
monoid, 2
  komutativní, 2
  transformační, 2
morfismus v kategorii, 31
multiplikativní množina, 24

objekt v kategorii, 31
obor integrity, 24

okruh, 19
  celých čísel, 20
  endomorfismů, 29
  faktorový, 23
  hlavních ideálů, 22
  horních trojúhelníkových matic, 20
  jednoduchý, 22
  komutativní, 19
  lokální, 28
  opačný, 29
  podílový, 25
    klasický, 25
  polynomů, 20
  souřadnicový, 28
  zbytkových tříd modulo n, 20
  čtvercových matic, 20
orbita, 11

podalgebra, 21
podgrupa, 5
  generovaná, 7
  normální, 8
podmodul, 30
podmonoid, 3
podokruh, 21
podílové těleso, 26
pologrupa, 2
primární komponenta grupy, 14
prvek
  idempotentní, 24
  invertibilní, 4
  inverzní, 3
  konjugovaný, 8
  nilpotentní, 24
  regulární, 24
prvoideál, 26
prvookruh, 21

reprezentace
  algebry, 29
  ekvivalentní, 17
  grupy, 16
  regulární, 18
  věrná, 16
rozklad grupy podle podgrupy, 6

součin grup, 13
součin v kategorii, 33
stabilizátor, 11
stupeň nilpotence, 12

translace, 3
transverzála, 6
těleso, 20

vnitřní automorfismus, 8
věta
  1. o izomorfismu, 9, 23, 31
  2. o izomorfismu, 10, 23, 31
  3. o izomorfismu, 10, 31
  Cayleyho
    pro grupy, 6
    pro monoidy, 3
  Frobenius-Stickelbergerova, 15
  Lagrangeova, 7
  o homomorfismu, 9, 23, 31
  Poincarého, 7

řád
  grupy, 7
  prvku v grupě, 7

Katedra algebry MFF UK, Sokolovská 83, 186 75 Praha 8
E-mail address: trlifaj@karlin.mff.cuni.cz