Úvod do algebry v obrázcích

Aleš Drápal

29. dubna 2002

Obsah

Seznam obrázků

1 Uzávěrové systémy, relace a ekvivalence

Množinu všech podmnožin množiny A budeme značit $\mathcal{P}(A)$ a nazývat *potencí* nebo *potenční množinou* A. Je tedy

$$\mathcal{P}(A) = \{B;\ \ B \subseteq A\}.$$

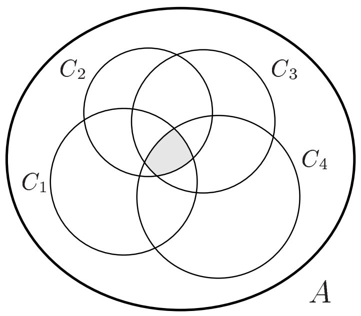
Speciálně, $A \in \mathcal{P}(A)$ a $\emptyset \in \mathcal{P}(A)$.

Je-li A množina a $\mathcal{C} \subseteq \mathcal{P}(A)$, nazveme $\mathcal{C}$ *uzávěrovým systémem nad* A, jsou-li splněny tyto podmínky:

(i) $A \in \mathcal{C}$,

(ii) Jsou-li $B_i \in \mathcal{C}$, $i \in I \neq \emptyset$, je $\bigcap(B_i;\, i \in I) \in \mathcal{C}$.

Vyjádřeno slovně, systém podmnožin $\mathcal{C}$ množiny A je uzávěrovým systémem nad A, jestliže obsahuje A a je uzavřen na průniky.



Do uzávěrového systému $\mathcal{C}$ nad A mohou patřit nejrůznější množiny. Vždy je tam však množina A. Jsou-li v $\mathcal{C}$ nějaké další množiny (třeba C_1, C_2, C_3 a C_4), je v $\mathcal{C}$ i jejich průnik.

Obrázek 1.1: Množiny v uzávěrovém systému

Je-li B podmnožina množiny A a $\mathcal{C}$ je uzávěrový systém nad A, tak mezi množinami z $\mathcal{C}$, které obsahují B, je podle (i) jistě množina A. Soustava $\{C \in \mathcal{C};\ B \subseteq C\}$ je proto vždy neprázdná. Označme E průnik $\cap\{C \in \mathcal{C};\, B \subseteq C\}$. Množina E obsahuje množinu B a podle (ii) patří do uzávěrového systému $\mathcal{C}$. Množina E byla přitom definována tak, aby ležela v každé množině z $\mathcal{C}$, jež obsahuje B. Proto je E nejmenší množinou z $\mathcal{C}$, jež obsahuje B. Budeme ji značit $\mathrm{cl}_{\mathcal{C}}(B)$ a nazývat *uzávěrem* B v $\mathcal{C}$ nebo *množinou generovanou v* $\mathcal{C}$ *množinou* B. Všimněte si, že $\mathrm{cl}_{\mathcal{C}}(C) = C$ platí právě když C patří do $\mathcal{C}$.

Zobrazení $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ nazýváme *uzávěrový operátor na množině* A, jestliže má tyto vlastnosti:

(i) $B \subseteq \alpha(B)$ pro všechna $B \subseteq A$ (extenzita),

(ii) $\alpha(\alpha(B)) = \alpha(B)$ pro všechna $B \subseteq A$ (idempotence),

(iii) kdykoliv $B \subseteq C \subseteq A$, tak $\alpha(B) \subseteq \alpha(C)$ (monotónnost).

1.1 Tvrzení.

(i) Je-li $\mathcal{C}$ *uzávěrový systém nad* A*, je* $\mathrm{cl}_{\mathcal{C}}$ *uzávěrový operátor na* A*.*

(ii) Je-li α *uzávěrový operátor na* A*, tvoří* $\mathcal{C} = \{C \subseteq A;\ \alpha(C) = C\}$ *uzávěrový systém nad* A *a* $\alpha = \mathrm{cl}_{\mathcal{C}}$*.*

Důkaz. Část (i) plyne přímo z definice uzávěrového systému. Budeme proto dokazovat jen část (ii). Buď α uzávěrový operátor a ať C_i, $i \in I$, je neprázdná soustava podmnožin množiny A takových, že $\alpha(C_i) = C_i$ pro každé $i \in I$. Podle (i) je $\bigcap C_i \subseteq \alpha(\bigcap C_i)$. Podle (iii) je $\alpha(\bigcap C_i) \subseteq \alpha(C_i) = C_i$ pro každé $i \in I$, takže $\alpha(\bigcap C_i) = \bigcap C_i$. Dokázali jsme, že $\mathcal{C}$ je uzávěrový systém. Je-li $B \subseteq A$, je $\alpha(B) \in \mathcal{C}$ podle (ii). Tudíž $\mathrm{cl}_{\mathcal{C}}(B) \subseteq \alpha(B)$. Naopak, z $B \subseteq \mathrm{cl}_{\mathcal{C}}(B)$ dostáváme podle (iii) $\alpha(B) \subseteq \alpha(\mathrm{cl}_{\mathcal{C}}(B)) = \mathrm{cl}_{\mathcal{C}}(B)$. □

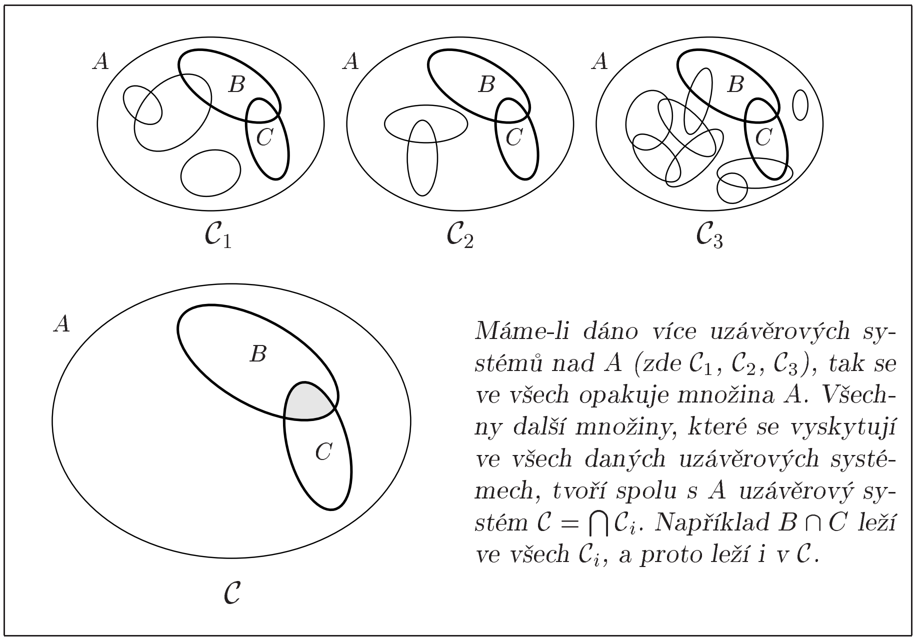
Uzávěrové operátory a uzávěrové systémy jsou tudíž ve vzájemně jednoznačném vztahu.

1.2 Tvrzení. *Všechny uzávěrové systémy nad* A *tvoří uzávěrový systém nad* $\mathcal{P}(A)$*.*

Důkaz. $\mathcal{P}(A)$ je uzávěrový systém nad A. Jsou-li $\mathcal{C}_i$, $i \in I \neq \emptyset$, uzávěrové systémy nad A a pro $j \in J \neq \emptyset$ je $B_j \in \mathcal{C}_i$ pro všechna $i \in I$, je i $\bigcap(B_j;\ j \in J) \in \bigcap(\mathcal{C}_i;\ i \in I)$. □

1.3 Lemma. *Buď* $\mathcal{A}$ *a* $\mathcal{B}$ *uzávěrové systémy nad* A*. Je-li* $\mathcal{A} \subseteq \mathcal{B}$*, tak* $\mathrm{cl}_{\mathcal{B}}(C) \subseteq \mathrm{cl}_{\mathcal{A}}(D)$ *kdykoliv* $C \subseteq D \subseteq A$*.*

Důkaz. $\mathrm{cl}_{\mathcal{B}}(C) \subseteq \mathrm{cl}_{\mathcal{B}}(D) \subseteq \mathrm{cl}_{\mathcal{A}}(D)$. □



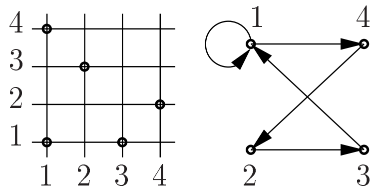
Obrázek 1.2: Průniky uzávěrových systémů

Relací z A do B rozumíme každou podmnožinu $A \times B$. *Relací na A* rozumíme relaci z A do A. Místo $(a, b) \in \rho$, kde ρ je relace, píšeme často $a \rho b$. Relaci $\{(a, a);\ a \in A\}$ značíme id_A (čteme *identita na A*). Je-li $\rho \subseteq A \times B$, značí ρ^{-1} *opačnou relaci*, $\rho^{-1} = \{(b, a);\ (a, b) \in \rho\}$.

Je-li ρ relace na A, označuje ρ^+ tu relaci na A, kde $(a, b) \in \rho^+$ právě když existuje posloupnost $c_0, c_1, \ldots, c_k \in A$ taková, že $a = c_0$, $b = c_k$, $k \geq 1$ a $c_{i-1} \rho c_i$ pro všechna $1 \leq i \leq k$.

Buď ρ relace na A. Tato relace se nazývá

– *reflexivní,* jestliže $\mathrm{id}_A \subseteq \rho$;
– *antireflexivní,* jestliže $\mathrm{id}_A \cap \rho = \emptyset$;
– *symetrická,* jestliže $\rho = \rho^{-1}$;
– *antisymetrická,* jestliže $\rho \cap \rho^{-1} = \emptyset$;



Relaci ρ na A mohu znázornit jako podmnožinu $A \times A$ nebo orientovaným grafem. Zde volíme $A = \{1, 2, 3, 4\}$ a $\rho = \{(1,1), (1,4), (2,3), (3,1), (4,2)\}$.

Obrázek 1.3: Zobrazování relací

– *tranzitivní,* jestliže z $a\rho b$, $b\rho c$ plyne $a\rho c$ pro všechna $a, b, c \in A$.

Poznamenejme, že terminologie v případě antisymetrických relací není zcela jednotná. Mnozí autoři nazývají relaci ρ antisymetrickou právě když z $a\rho b$ a $b\rho a$ vždy plyne $a = b$. Takovýto přístup usnadňuje definici (částečného) uspořádání jakožo reflexivní, antisymetrické a tranzitivní relace (viz kapitola 4), není však zcela v souladu s intuitivním významem slova 'antisymetrický'.

1.4 Tvrzení. *Reflexivní (resp. symetrické, resp. tranzitivní) relace na množině A tvoří uzávěrový systém nad $A \times A$. Označíme-li tento systém $\mathcal{C}$, je $\mathrm{cl}_{\mathcal{C}}(\rho)$ pro $\rho \subseteq A \times A$ rovno $\rho \cup \mathrm{id}_A$ (resp. $\rho \cup \rho^{-1}$, resp. ρ^+).*

Důkaz. $\rho \cup \mathrm{id}_A$ (resp. $\rho \cup \rho^{-1}$, resp. ρ^+) musí být obsaženo v každé reflexivní (resp. symetrické, resp. tranzitivní) relaci, která obsahuje ρ. Současně ale $\rho \cup \mathrm{id}_A$ (resp. $\rho \cup \rho^{-1}$, resp. ρ^+) je samo reflexivní (resp. symetrické, resp. tranzitivní). $\square$

Relace ρ nad A, která je současně reflexivní, symetrická a tranzitivní, se nazývá *ekvivalence* na A. Z 1.2 a 1.4 vyplývá, že všechny ekvivalence na A tvoří uzávěrový systém nad $A \times A$.

1.5 Lemma. *Buď ρ relace na A.*

(i) Je-li ρ reflexivní, jsou ρ^+ i $\rho \cup \rho^{-1}$ reflexivní.
(ii) Je-li ρ symetrická, je ρ^+ symetrická.

Důkaz. Snadný. $\square$

Pro ρ relaci na A pišme na chvíli $ref(\rho)$ místo $\rho \cup \mathrm{id}_A$, $sym(\rho)$ místo $\rho \cup \rho^{-1}$ a $tra(\rho)$ místo ρ^+. Podle 1.4 je na místě o ref, sym a tra hovořit jako o reflexivním, symetrickém a tranzitivním uzávěru. Ukážeme, že jejich kombinací lze vždy popsat nejmenší ekvivalenci obsahující danou relaci.

1.6 Tvrzení. *Buď ρ relace na množině A. Potom*

$$tra(sym(ref(\rho))) = ((\rho \cup \mathrm{id}_A) \cup (\rho \cup \mathrm{id}_A)^{-1})^+ = (\rho \cup \rho^{-1} \cup \mathrm{id}_A)^+$$

je nejmenší ekvivalence na A, která obsahuje relaci ρ.

Důkaz. Označme equ uzávěrový operátor příslušející uzávěrovému systému všech ekvivalencí na množině A. Potom z 1.3 dostáváme inkluzi $tra(sym(ref(\rho))) \subseteq equ(equ(equ(\rho))) = equ(\rho)$. Z 1.5 vyplývá, že $tra(sym(ref(\rho)))$ je ekvivalence. □

Je-li ρ ekvivalence na A a $a \in A$, tak $[a]_\rho = \{b;\ a\rho b\}$ budeme nazývat *blokem ekvivalence* ρ nebo *ekvivalenční třídou* ρ, případně též ekvivalenční třídou *modulo* ρ. Klademe $A/\rho = \{[a]_\rho;\ a \in A\}$. Množina A/ρ se nazývá *kvocient* A *modulo* ρ.

Je-li A množina, tak $\mathcal{B} \subseteq \mathcal{P}(A)$ nazveme *rozkladem* A, jestliže

(i) $A = \bigcup(B;\ B \in \mathcal{B})$,
(ii) $B \cap C = \emptyset$, jestliže $B, C \in \mathcal{B}$ a $B \neq C$, a
(iii) $\emptyset \notin \mathcal{B}$.

1.7 Tvrzení. *Je-li ρ ekvivalence na A, je $\{[a]_\rho;\ a \in A\}$ rozklad množiny A.*

Důkaz. Pro všechna $a \in A$ je $a \in [a]_\rho$, takže podmínky (i) a (iii) jsou jistě splněny. Jestliže $b, c \in A$ a $d \in [b]_\rho \cap [c]_\rho$, tak pro každé $a \in [b]_\rho$ máme $a\rho b\rho d\rho c$, čili $a \in [c]_\rho$, a tedy $[b]_\rho \subseteq [c]_\rho$. Opačnou inkluzi dostaneme stejným postupem, a proto platí $[b]_\rho = [c]_\rho$. □

Každý rozklad množiny A naopak určuje ekvivalenci na A, jejíž bloky (tj. ekvivalenční třídy) jsou právě množiny tohoto rozkladu.

Je-li ρ ekvivalence na A, tak platí $\mathrm{id}_A \subseteq \rho \subseteq A \times A$. Ekvivalenci id_A odpovídá rozklad na jednobodové množiny, a obvykle se jí říká *triviální* ekvivalence.

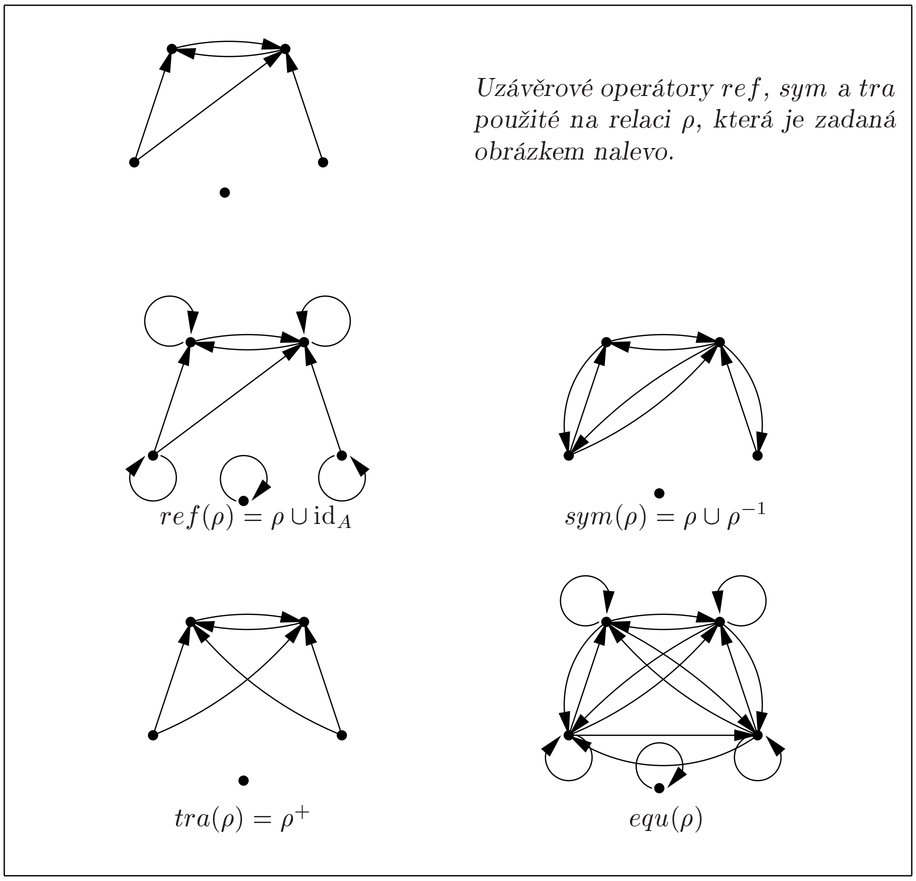
Ekvivalence $A \times A$ odpovídá rozkladu, který obsahuje jedině množinu A. Tato ekvivalence se nejčastěji označuje jako *universální* ekvivalence.

Ekvivalenci ρ nazýváme *vlastní*, jestliže neplatí ani $\rho = \mathrm{id}_A$ ani $\rho = A \times A$.

V algebře, ale i jinde v matematice, se často pracuje s ekvivalencemi kvocientu A/ρ. Předpokládejme, že σ je nějaká další ekvivalence na A, a ať σ obsahuje ρ. Na A/ρ definujeme relaci σ/ρ tak, že pro ekvivalenční třídy $B, C \in A/\rho$ je

$$(B, C) \in \sigma/\rho \iff (b, c) \in \sigma \text{ platí pro všechna } b \in B \text{ a } c \in C.$$

1.8 Lemma. *(i) Pro $b, c \in A$ platí $([b]_\rho, [c]_\rho) \in \sigma/\rho$ právě když je $(b, c) \in \sigma$.*



Obrázek 1.4: Uzávěry relací

(ii) Relace σ/ρ je ekvivalence na A/ρ.

Důkaz. (i) Ať je $(b, c) \in \sigma$ a ať $b' \in A$ patří do $[b]_\rho$ a $c' \in A$ do $[c]_\rho$. Je třeba dokázat $(b', c') \in \sigma$. Ovšem $(b', b) \in \rho$ a $(c', c) \in \rho$ implikují $(b', b) \in \sigma$ a $(c', c) \in \sigma$, neboť platí $\rho \subseteq \sigma$. Stačí tedy použít tranzitivitu ekvivalence σ.
(ii) Ať $B, C, D \in A/\rho$ jsou rozkladové třídy ekvivalence ρ. Vyberme prvky $b \in B$, $c \in C$ a $d \in D$. Je tedy $B = [b]_\rho$, $C = [c]_\rho$ a $D = [d]_\rho$. Předpokládejme, že platí

$(B, C) \in \sigma/\rho$ a $(C, D) \in \sigma/\rho$. Podle definice musí být $(b, c) \in \sigma$ a $(c, d) \in \sigma$, takže je rovněž $(b, d) \in \sigma$. Ovšem to podle (i) implikuje $(B, D) \in \sigma/\rho$. Relace σ/ρ je tedy tranzitivní. Symetrie a reflexivita se dokáží podobně. □

1.9 Tvrzení. *Ať ρ je ekvivalence na množině A a ať η je ekvivalence na A/ρ. Pak existuje právě jedna ekvivalence $\sigma \supseteq \rho$ na A, pro kterou platí $\eta = \sigma/\rho$.*

Důkaz. Má-li být $\eta = \sigma/\rho$, tak podle 1.8(i) musí být $(b, c) \in \sigma$ právě když je $([b]_\rho, [c]_\rho) \in \eta$. Tento vztah σ jednoznačně určuje, takže ho lze použít jako definici. Je třeba ukázat, že takto definovaná relace σ je ekvivalence, obsahuje ρ a splňuje $\eta = \sigma/\rho$.

To, že σ je ekvivalence, se okamžitě odvodí z toho, že η je ekvivalence.

Uvažme prvky b, c množiny A. Je-li $(b, c) \in \rho$, je $[b]_\rho$ rovno $[c]_\rho$, takže jistě platí $([b]_\rho, [c]_\rho) \in \eta$, a tedy i $(b, c) \in \sigma$.

Vztah $([b]_\rho, [c]_\rho) \in \eta$ lze podle definice σ vyjádřit jako $(b, c) \in \sigma$, což podle 1.8(i) nastane právě když platí $([b]_\rho, [c]_\rho) \in \sigma/\rho$. Tím je dokázáno, že ekvivalence η a σ/ρ se shodují. □

Zobrazením $f : A \to B$ rozumíme, jak je obvyklé, takovou relaci z A do B, že pro každé $a \in A$ existuje právě jedno $b \in B$ takové, že $(a, b) \in f$. Přitom píšeme $b = f(a)$.

Zobrazení f se nazývá *injektivní* (*prosté*), jestliže $f(a_1) = f(a_2)$ implikuje $a_1 = a_2$ pro všechna $a_1, a_2 \in A$. Zobrazení f je *surjektivní* (zobrazení *na*), jestliže pro každé $b \in B$ existuje takové $a \in A$, že $b = f(a)$.

Zobrazení f nazveme *bijektivní,* jestliže je současně injektivní a surjektivní. Připomeňme zde také, že o množinách A a B říkáme, že jsou stejně mohutné (nebo že mají stejnou mohutnost), jestliže existuje (alespoň jedna) bijekce $f : A \to B$.

Je-li dáno zobrazení $f : A \to B$, tak obor hodnot $\{f(a); a \in A\}$ označujeme $\operatorname{Im} f$. Zobrazení $f : A \to B$ je tedy surjektivní právě když $\operatorname{Im} f = B$. Množinu $\operatorname{Im} f$ nezýváme *obrazem* f.

Je-li $f : A \to B$ zobrazení, tak *jádrem* tohoto zobrazení nazýváme ekvivalenci $\ker f$ na množině A, která je dána vztahem: $(a, b) \in \ker f$ právě když $f(a) = f(b)$.

Zobrazení z A do A/ρ, $a \mapsto [a]_\rho$ se nazývá *přirozené* (naturální) zobrazení *podle* ρ a budeme ho značit nat_ρ. (Někdy se tomuto zobrazení také říká *přirozená projekce* a značívá se π_ρ.) Zřejmě platí $\rho = \ker \mathrm{nat}_\rho$.

Jsou-li $f : A \to B$ a $g : B \to C$ dvě zobrazení, tak jejich složení $g \circ f : A \to C$ je pro každé $a \in A$ dána vztahem $(g \circ f)(a) = g(f(a))$.

Je-li $f : A \to B$ zobrazení, tak (relace) f^{-1} je zobrazení právě když f je bijekce. V takovém případě se f^{-1} nazývá *inverzní zobrazení* a platí $f \circ f^{-1} = \mathrm{id}_B$ a $f^{-1} \circ f = \mathrm{id}_A$. Naopak, jestliže k danému zobrazení $f : A \to B$ lze nalézt takové zobrazení $g : B \to A$, že platí $f \circ g = \mathrm{id}_B$ a $g \circ f = \mathrm{id}_A$, musí být f bijekcí a g rovno f^{-1}.

1.10 Tvrzení. *Buďte $f : A \to B$ zobrazení a ρ ekvivalence na A. Zobrazení $g : A/\rho \to B$, které splňuje $g \circ \mathrm{nat}_\rho = f$, existuje právě když platí $\rho \subseteq \ker f$. Je-li $\rho \subseteq \ker f$, je g určeno jednoznačně, $\ker g = (\ker f)/\rho$ a $g([a]_\rho) = f(a)$ pro každé $a \in A$.*

Zobrazení g je bijektivní právě když f je surjektivní a platí $\rho = \ker f$.

Důkaz. Pro každé $a \in A$ má platit $g([a]_\rho) = (g \circ \mathrm{nat}_\rho)(a) = f(a)$. Zobrazení g proto nemůže být definováno žádným jiným způsobem. Pro $(a, b) \in \rho$ máme $f(a) = g([a]_\rho) = g([b]_\rho) = f(b)$, takže vskutku musí platit $\rho \subseteq \ker f$. Ať tomu tak opravdu je. Potom z $[a]_\rho = [b]_\rho$ plyne $f(a) = f(b)$, takže g lze skutečně vztahem $g([a]_\rho) = f(a)$ definovat.

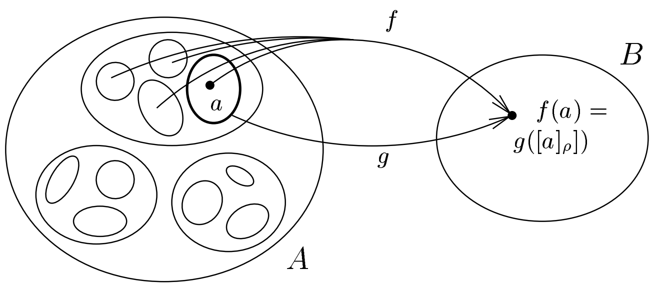
Pro $a, b \in A$ máme $g([a]_\rho) = g([b]_\rho)$ právě když platí $(a, b) \in \ker f$. To podle 1.8(i) znamená, že $\ker g$ je rovno $(\ker f)/\rho$.

Jelikož $\mathrm{Im}\, g$ se shoduje s $\mathrm{Im}\, f$, je f surjektivní právě když je g surjektivní. Podle 1.9 lze každou ekvivalenci v A/ρ jednoznačně vyjádřit jako σ/ρ, kde $\sigma \supseteq \rho$. Triviální ekvivalenci $\mathrm{id}_{A/\rho}$ vyjadřuje ρ/ρ, takže g je injektivní právě když $\ker g = (\ker f)/\rho$ se rovná ρ/ρ, čili právě když $\rho = \ker f$. □

V prvním odstavci předchozího důkazu jsme museli dokázat, že z $[a]_\rho = [b]_\rho$ plyne $f(a) = f(b)$, neboť jinak by definice $g([a]_\rho) = f(a)$ nebyla možná. Je-li totiž obraz bloku ekvivalence v definovaném zobrazení odvozen od prvku příslušného bloku , je definice v pořádku jedině tehdy, nezávisí-li hodnota obrazu na výběru tohoto prvku, ale pouze na jeho příslušnosti do daného bloku.

Běžně se postupuje tak, že se nové zobrazení definuje způsobem, který by vlastně mohl být nesprávný, a v prvém kroku důkazu se ověřuje korektnost takové definice.

1.11 Lemma. *Ať $f : A \to B$ je bijekce dvou množin a ať ρ a η jsou (po řadě) ekvivalence na A a B, přičemž pro všechna $a, b \in A$ platí $(a, b) \in \rho$ právě když je $(f(a), f(b)) \in \eta$. Potom $[a]_\rho \mapsto [f(a)]_\eta$ je korektně definovaná bijekce A/ρ a B/η.*



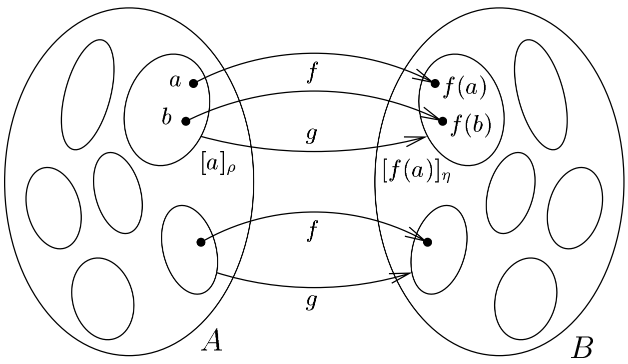
Bloky jádra ker f *zobrazení* $f : A \to B$ *jsou znázorněny většími ovály a bloky ekvivalence* ρ *menšími ovály. Ze vztahu* $\rho \subseteq \ker f$ *plyne, že každý blok* ρ *je podmnožinou nějakého bloku* ker f*, což znamená, že všechny body daného bloku* ρ *se pomocí* f *zobrazí stejně. Proto lze definovat* $g : A/\rho \to B$ *tak, že obraz daného bloku se shoduje s obrazem (určeným* f*) každého z jeho bodů.*

Obrázek 1.5: Ilustrace Tvrzení 1.10

Důkaz. Pro $(a, b) \in \rho$ je $(f(a), f(b)) \in \eta$, takže $g([a]_\rho) = [f(a)]_\eta$ je korektní definice zobrazení $g : A/\rho \to B/\eta$. Pro všechna $c, d \in B$ lze nalézt (jednoznačně určená) $a, b \in A$ tak, aby bylo $c = f(a)$ a $d = f(b)$, a proto z $(c, d) \in \eta$ plyne $(f^{-1}(c), f^{-1}(d)) \in \rho$, a $h([c]_\rho) = [f^{-1}(c)]_\eta$ je tím pádem korektní definice zobrazení $h : B/\eta \to A/\rho$. Pro všechna $a \in A$ máme $hg([a]_\rho) = h[f(a)]_\eta = [f^{-1}f(a)]_\rho = [a]_\rho$, takže je $hg = \mathrm{id}_{A/\rho}$. Podobně dostáváme $gh = \mathrm{id}_{B/\eta}$. Zobrazení g a h jsou tudíž vzájemně inverzní, a tedy bijektivní. $\square$

2 Operace, algebry, homomorfismy a kongruence

Je-li A množina, tak A^n, $n \geq 1$, bude značit, jak je obvyklé, kartézský součin $A \times \cdots \times A$ o n činitelích. Prvky A^n jsou všechny n–tice $(a_1, \ldots, a_n)$, kde $a_1, \ldots, a_n$ jsou prvky A. Všimněte si, že bychom také mohli A^n definovat jako množinu všech zobrazení z $\{1, \ldots, n\}$ do A. Při takové definici je pak přirozené A^0 definovat jako



Jestliže pro $a, b \in A$ je $a \,\rho\, b$ právě když $f(a) \,\eta\, f(b)$, přičemž $f : A \to B$ je bijekce, tak je zřejmé, že f převádí bloky ekvivalence ρ na bloky η. Každému bloku $[a]_\rho$ lze proto přiřadit jako obraz blok $[f(a)]_\eta$, a tím je definována bijekce $g : A/\rho \to B/\eta$.

Obrázek 1.6: Ilustrace k Lemmatu 1.11

množinu všech zobrazení z $\emptyset$ do A. Ovšem $\emptyset \times A = \emptyset$, takže takové zobrazení existuje právě jedno, a je to opět $\emptyset$. Je tedy $A^0 = \{\emptyset\}$.

Operací četnosti $n \geq 0$ na množině A rozumíme každé zobrazení A^n do A. Operace četnosti 0 je tudíž zobrazení $\{\emptyset\}$ do A, čili pro každé $a \in A$ existuje právě jedna operace f_a četnosti 0 taková, že $f_a(\emptyset) = a$. Operaci f_a a prvek a můžeme ztotožnit, neboť se liší jen formálně. Operací četnosti 0 proto prostě pro nás bude vybrání nějakého prvku množiny A.

Operace četnosti nula se nazývá nulární operace, operace četnosti jedna unární operace, četnosti dva binární operace a četnosti tři ternární operace. Mluvíme také o n–ární operaci f, přičemž n se nazývá *aritou* f.

Lze se setkat s prefixovým, infixovým a sufixovým zápisem operace — v případě binární operace je $f(a, b)$ prefixový, afb infixový a $(a, b)f$ či $(a, b)^f$ sufixový zápis.

Často bude pro nás výhodné, abychom operace na dvou různých množinách (například A a B) značili stejně (například $+$). Pokud budeme v takovém případě potřebovat v zápise rozlišit mezi oběma operacemi, připojíme k označení operace vhodný index (například označení množiny, píšeme pak $+_A$ a $+_B$).

Buď na množině A dána operace α četnosti n. O podmnožině $C \subseteq A$ řekneme, že je *uzavřená na* α právě když $\alpha(c_1, \ldots, c_n) \in C$ pro všechna $c_1, \ldots, c_n \in C$. Všimněte si, že pokud je α nulární operace, tak $C \subseteq A$ je uzavřená na α právě když $\alpha_A \in C$.

$\circ$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

$\bullet$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Ať $A = \{1, 2, 3, 4\}$ a na A ať jsou binární operace $\circ$ a $\bullet$ dány tabulkami vlevo. Množiny uzavřené na $\circ$ jsou $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$ a A, zatímco množiny uzavřené na $\bullet$ jsou $\emptyset$, $\{1\}$, $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$ a A. Algebra $A(\circ, \bullet)$ má tedy podalgebry $\emptyset$, $\{1\}$ a A.

Obrázek 2.1: Uzavřenost na binární operace

2.1 Tvrzení. *Ať je na množině A dána operace α. Potom soustava všech podmnožin A, které jsou uzavřené na α, tvoří uzávěrový systém nad A.*

Důkaz. Buďte C_j, $j \in J \neq \emptyset$, množiny uzavřené na $\alpha : A^n \to A$. Jestliže $c_1, \ldots, c_n \in C_j$ pro všechna $j \in J$, je i $\alpha(c_1, \ldots, c_n) \in C_j$ pro všechna $j \in J$. □

Ať na množinách A a B je dána operace α (stejné) četnosti $n \geq 0$. O *zobrazení* $f : A \to B$ řekneme, že je *slučitelné* s operací α, jestliže pro libovolné $a_1, \ldots, a_n \in A$ platí

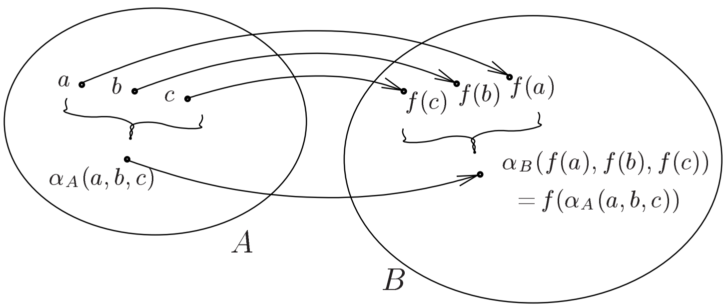
$$f\alpha_A(a_1, \ldots, a_n) = \alpha_B(f(a_1), \ldots, f(a_n)).$$

Všimněte si, že v případě $n = 0$ je f slučitelná s α právě když $f(\alpha_A) = \alpha_B$.

2.2 Tvrzení. *Ať je na množinách A, B a C dána operace α četnosti $n \geq 0$. Buďte $f : A \to B$ a $g : B \to C$ zobrazení slučitelná s α. Potom je i $g \circ f : A \to C$ zobrazení slučitelné s operací α.*

Je-li $f : A \to B$ bijektivní zobrazení slučitelné s α, je $f^{-1} : B \to A$ také zobrazení slučitelné s α.

Důkaz. Buďte $a_1, \ldots, a_n \in A$. Potom $(g \circ f)(\alpha_A(a_1, \ldots, a_n))$ je rovno $g(\alpha_B(f(a_1), \ldots, f(a_n))) = \alpha_C(g(f(a_1)), \ldots, g(f(a_n)))$. Ať je $f : A \to B$ bijektivní a ať b_1,



Grafické vyjádření vztahu $f(\alpha_A(a,b,c)) = \alpha_B(f(a),f(b),f(c))$, který musí platit pro všechna $a,b,c \in A$, má-li být zobrazení $f : A \to B$ slučitelné s ternární operací α.

Obrázek 2.2: Slučitelnost zobrazení s operací

$\dots$, $b_n \in B$. Potom existují $a_i \in A$, že $b_i = f(a_i)$, $1 \le i \le n$, takže z $f(\alpha_A(a_1, \dots, a_n)) = \alpha_B(b_1, \dots, b_n)$ plyne $f^{-1}(\alpha_B(b_1, \dots, b_n)) = \alpha_A(f^{-1}(b_1), \dots, f^{-1}(b_n))$. $\square$

2.3 Tvrzení. *Předpokládejme, že na A i na B je dána operace α četnosti n, a ať $f : A \to B$ je zobrazení slučitelné s α. Je-li $C \subseteq A$ množina uzavřená na α, je $f(C)$ rovněž uzavřená na α. Speciálně je tedy* $\operatorname{Im} f$ *uzavřené na α. Naopak, je-li $D \subseteq B$ uzavřené na α, je $f^{-1}(D)$ také uzavřené na α.*

Důkaz. Buď $b_1, \dots, b_n \in f(C)$. Pak existují $a_1, \dots, a_n \in C$, že $b_1 = f(a_1)$, $\dots$, $b_n = f(a_n)$. Tudíž $\alpha(b_1, \dots, b_n) = \alpha(f(a_1), \dots, f(a_n)) = f(\alpha(a_1, \dots, a_n)) \in f(C)$.

Buď nyní $D \subseteq B$ uzavřená na α a ať $a_1, \dots, a_n \in f^{-1}(D)$. Prvky $f(a_1), \dots, f(a_n)$ jsou z D, takže $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) \in D$, a tedy $\alpha(a_1, \dots, a_n) \in f^{-1}(D)$. $\square$

Buď α operace četnosti n na A. O *relaci* ρ na A řekneme, že je *slučitelná* s α, jestliže pro libovolná $a_1, \dots, a_n \in A$ a $b_1, \dots, b_n \in A$ taková, že $a_1 \rho b_1, \dots, a_n \rho b_n$, platí $\alpha(a_1, \dots, a_n)\ \rho\ \alpha(b_1, \dots, b_n)$. Všimněte si, že s nulární operací je slučitelná každá reflexivní relace. Všimněte si také, že triviální ekvivalence id_A i universální ekvivalence $A \times A$ jsou slučitelné s libovolnou operací α.

2.4 Tvrzení. *Buď α operace četnosti n na A. Potom všechny relace (resp. ekvivalence) na A slučitelné s α tvoří uzávěrový systém nad $A \times A$.*

Důkaz. Buďte $a_1, \dots, a_n \in A$ a $b_1, \dots, b_n \in A$ takové, že $a_1 \rho_j b_1, \dots, a_n \rho_j b_n$ pro všechna $j \in J \neq \emptyset$, kde ρ_j jsou relace na A slučitelné s α. Potom pro každé $j \in J$ platí $\alpha(a_1, \dots, a_n)\ \rho_j\ \alpha(b_1, \dots, b_n)$. □

2.5 Tvrzení. *Ať na množinách A a B je dána operace α téže četnosti n. Je-li $f : A \to B$ zobrazení slučitelné s α, tak $\ker f$ je ekvivalence slučitelná s α.*

Důkaz. Ať $a_1, \dots, a_n \in A$ a $b_1, \dots, b_n \in A$ jsou taková, že $f(a_1) = f(b_1)$, $\dots$, $f(a_n) = f(b_n)$. Potom $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) = \alpha(f(b_1), \dots, f(b_n)) = f(\alpha(b_1, \dots, b_n))$. □

Buď ρ ekvivalence na A slučitelná s operací $\alpha : A^n \to A$. Na A/ρ definujeme operaci α tak, že jsou-li $B_1, \dots, B_n$ bloky ekvivalence ρ, přičemž $a_1 \in B_1, \dots, a_n \in B_n$, položíme $\alpha(B_1, \dots, B_n) = [\alpha(a_1, \dots, a_n)]_\rho$. Jinak vyjádřeno, $\alpha([a_1]_\rho, \dots, [a_n]_\rho) = [\alpha(a_1, \dots, a_n)]_\rho$ pro libovolná $a_1, \dots, a_n \in A$.

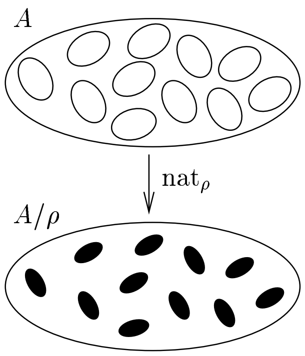
Je ovšem třeba dokázat, že takto lze operaci α na A/ρ skutečně definovat, tj. že takováto definice je korektní. Pro $b_1 \in B_1, \dots, b_n \in B_n$ platí $a_1 \rho b_1$, $\dots$, $a_n \rho b_n$, takže podle definice slučitelnosti je $\alpha(a_1, \dots, a_n)\ \rho\ \alpha(b_1, \dots, b_n)$, a tedy $[\alpha(a_1, \dots, a_n)]_\rho = [\alpha(b_1, \dots, b_n)]_\rho$. Hodnota $\alpha(B_1, \dots, B_n)$ je tedy nezávislá na tom, které prvky $a_i \in B_i$, $1 \leq i \leq n$, jsme vybrali.

2.6 Tvrzení. *Buď α operace četnosti n na A a ρ ekvivalence na A slučitelná s α. Potom přirozené zobrazení $\mathrm{nat}_\rho : A \to A/\rho$ je slučitelné s α.*

Důkaz. Buď $a_1, \dots, a_n \in A$. Potom $\mathrm{nat}_\rho(\alpha_A(a_1, \dots, a_n)) = [\alpha_A(a_1, \dots, a_n)]_\rho = \alpha_{A/\rho}([a_1]_\rho, \dots, [a_n]_\rho) = \alpha_{A/\rho}(\mathrm{nat}_\rho(a_1), \dots, \mathrm{nat}_\rho(a_n))$. □

Množinu A spolu s operacemi $\alpha_1, \dots, \alpha_k$ na A nazýváme *algebrou* na A. Někdy tuto algebru označujeme samostatným symbolem, pak například píšeme $B = A(\alpha_1, \dots, \alpha_k)$ a říkáme, že A je *nosičem* algebry B. Častěji algebru i její nosič označujeme stejným symbolem. Pak píšeme například $A = A(\alpha_1, \dots, \alpha_n)$ (tento zápis je sice trochu nelogický, leč zcela běžný).

V dalším textu budou $+$, $\cdot$, $\circ$, $\wedge$, $\vee$ (a případné od nich odvozené varianty) označovat vždy binární operace. Naopak $^{-1}$, $-$ a $'$ značí unární operace a $\mathbf{0}$, $\mathbf{1}$ nulární operace.



Faktorizaci podle kongruence si lze představit tak, že každý z bloků kongruence ρ (což jsou původně množiny) začnu chápat jako nedělitelnou jednotku (jako bod kvocientní algebry). Tento proces formálně vyjadřuje přirozené zobrazení nat_ρ. *Obrázek ho pak znázorňuje jako stažení množin (tříd) do (trochu tučnějších) bodů.*

Obrázek 2.3: Přirozená projekce

Algebra $S = S(\cdot)$ se nazývá *pologrupa,* jestliže $\cdot$ splňuje asociativní zákon (tj. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro libovolná $a, b, c \in S$). Prvek $e \in S$ se nazývá *neutrální,* jestliže $a \cdot e = e \cdot a = a$ pro libovolné $a \in S$.

2.7 Tvrzení. *Pologrupa $S(\cdot)$ obsahuje nanejvýš jeden neutrální prvek.*

Důkaz. Buď $e, f \in S$ neutrální prvky. Pak $e = e \cdot f = f$. $\square$

Algebra $S = S(\cdot, \mathbf{1})$ se nazývá *monoid,* jestliže $S(\cdot)$ je pologrupa a $\mathbf{1}$ je její neutrální prvek.

Příklady pologrup a monoidů:

A. Buď $\mathbb{N}$ množina všech přirozených čísel $\{1, 2, \ldots\}$, $\mathbb{N}_0$ množina všech nezáporných celých čísel $\{0, 1, 2, \ldots\}$ a $\mathbb{Z}$ množina všech celých čísel $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Potom $\mathbb{N}(\cdot, 1)$, $\mathbb{N}_0(\cdot, 1)$, $\mathbb{Z}(\cdot, 1)$ jsou monoidy, $\mathbb{N}_0(+, 0)$ a $\mathbb{Z}(+, 0)$ jsou rovněž monoidy, ale $\mathbb{N}(+)$ je pologrupa bez neutrálního prvku.

B. Položme $Bool = \{\mathrm{T}, \mathrm{F}\}$ a definujme na $Bool$ binární operaci $\cdot$ odpovídající logickému 'AND' (tj. $\mathrm{T} \cdot \mathrm{F} = \mathrm{F} \cdot \mathrm{T} = \mathrm{F} \cdot \mathrm{F} = \mathrm{F}$ a $\mathrm{T} \cdot \mathrm{T} = \mathrm{T}$). Potom $Bool(\cdot, \mathrm{T})$ je monoid.

C. Buď $\mathbb{A}$ nějaká abeceda. Potom množina $\mathbb{A}^+$ všech neprázdných slov nad $\mathbb{A}$ je pologrupa vzhledem k operaci konkatenace (tj. $a_1 \ldots a_n \cdot b_1 \ldots b_m$ je rovno slovu $a_1 \ldots a_n b_1 \ldots b_m$). Přidáme-li k $\mathbb{A}^+$ prázdné slovo λ, dostaneme množinu, jež se obvykle značí $\mathbb{A}^*$. Je zřejmé, že $\mathbb{A}^*(\cdot, \lambda)$ je monoid.

D. Je-li Ω libovolná množina, tak množina T_Ω všech zobrazení z Ω do Ω je monoid vzhledem k operaci skládání zobrazení $\circ$ a neutrálnímu prvku id_Ω. $T_\Omega(\circ, \mathrm{id}_\Omega)$ se nazývá *transformační monoid* množiny Ω.

Pologrupa (monoid) se nazývá *komutativní,* jestliže $a \cdot b = b \cdot a$ pro všechny prvky a, b této pologrupy (monoidu). V příkladech A a B jsou uvedeny komutativní monoidy, monoidy z příkladů C a D jsou (obecně vzato) nekomutativní.

Buď dána algebra $A = A(\alpha_1, \ldots, \alpha_n)$. Řekneme, že množina $C \subseteq A$ je *podalgebra* A, jestliže C je uzavřená na všechny operace $\alpha_1, \ldots, \alpha_n$. Z 1.2 a 2.1 okamžitě dostáváme:

2.8 Tvrzení. *Všechny podalgebry algebry $A = A(\alpha_1, \ldots, \alpha_n)$ tvoří uzávěrový systém nad A.* □

Podalgebru C algebry $A(\alpha_1, \ldots, \alpha_n)$ chápeme skutečně jako algebru, tj. předpokládáme, že je vybavena operacemi $\alpha_1, \ldots, \alpha_n$, jež jsou zúžením původních operací na A.

Podalgebře monoidu se říká *podmonoid,* podalgebře pologrupy *podpologrupa,* a podobně i u dalších typů algeber.

Je-li A algebra a $\mathcal{C}$ uzávěrový systém jejích podalgeber, tak $\mathrm{cl}_{\mathcal{C}}(B)$ se pro $B \subseteq A$ obvykle nazývá podalgebra *generovaná množinou B*

Buďte $A = A(\alpha_1, \ldots, \alpha_n)$ a $B = B(\alpha_1, \ldots, \alpha_n)$ dvě algebry, a ať $f : A \to B$ je zobrazení. Toto zobrazení nazveme *homomorfismem,* jestliže f je slučitelné s každou operací α_i, $1 \le i \le n$. Z 2.2 plyne

2.9 Tvrzení. *Buďte dány algebry $A = A(\alpha_1, \ldots, \alpha_n)$, $B = B(\alpha_1, \ldots, \alpha_n)$, $C = C(\alpha_1, \ldots, \alpha_n)$ a homomorfismy $f : A \to B$, $g : B \to C$. Potom $g \circ f : A \to C$ je také homomorfismus. Je-li $f : A \to B$ bijektivní, je $f^{-1} : B \to A$ rovněž homomorfismus.* □

2.10 Tvrzení. *Buď $f : A \to B$ homomorfismus algeber $A = A(\alpha_1, \ldots, \alpha_n)$ a $B = B(\alpha_1, \ldots, \alpha_n)$. Je-li C podalgebra A, je $f(C)$ podalgebra B. Speciálně je* $\mathrm{Im}\, f$ *podalgebrou B. Naopak, je-li D podalgebra B, je $f^{-1}(D)$ podalgebra A.* □

Homomorfismus $f : A \to B$ se nazývá *izomorfismus,* je-li f bijektivní. Izomorfní algebry mají stejnou strukturu a liší se jen označením svých prvků.

Homomorfismus $f : A \to A$ se nazývá *endomorfismus,* bijektivní endomorfismus se nazývá *automorfismus.* Množina všech endomorfismů se značí $\mathrm{End}(A)$. Množina všech automorfismů se značí $\mathrm{Aut}(A)$.

2.11 Tvrzení. *Buď dána algebra $A = \Omega(\alpha_1, \ldots, \alpha_n)$. Potom* $\mathrm{End}(A)$ *je podmonoid monoidu T_Ω.*

Důkaz. $\mathrm{id}_A \in \mathrm{Aut}(A) \subseteq \mathrm{End}(A)$ a z $f, g \in \mathrm{End}(A)$ plyne podle 2.9 $g \circ f \in \mathrm{End}(A)$. □

Ať $f : A \to B$ je homomorfismus algeber. Pak

- *obrazem podalgebry A je podalgebra B,*
- *vzorem podalgebry B je podalgebra A,*
- *jádro* $\ker f$ *homomorfismu je kongruence A,*
- *je-li f bijekcí, je $f^{-1} : B \to A$ rovněž homomorfismus*

O homomorfismech platí, že jsou uzavřené na skládání.

Obrázek 2.4: Vlastnosti homomorfismů

Příklady podalgeber a homomorfismů:

A. Je-li $S(\cdot, \mathbf{1})$ monoid, je $\{\mathbf{1}\}$ podmonoid S. Například $\{0\}$ je podmonoid $\mathbb{Z}(+, 0)$. Buď $n \in \mathbb{Z}$. Pak $n\mathbb{Z} = \{na;\, a \in \mathbb{Z}\}$ je podmonoid $\mathbb{Z}(+, 0)$ a podpologrupa $\mathbb{Z}(\cdot)$. Pro $-1 \neq n \neq 1$ ovšem $n\mathbb{Z}$ není podmonoid $\mathbb{Z}(\cdot, 1)$. Zobrazení $\varphi : \mathbb{Z}(+, 0) \to n\mathbb{Z}(+, 0)$, $\varphi(a) = na$ pro každé $a \in \mathbb{Z}$, je izomorfismus, jestliže $n \neq 0$.

B. Zobrazení $\theta : \mathbb{Z}(\cdot, 1) \to \mathit{Bool}(\cdot, \mathrm{T})$ takové, že $\theta(a) = \mathrm{T}$ pro $a \neq 0$ a $\theta(0) = \mathrm{F}$, je surjektivní homomorfismus. Naopak, $\beta : \mathit{Bool}(\cdot, \mathrm{T}) \to \mathbb{Z}(\cdot, 1)$, $\beta(\mathrm{T}) = 1$, $\beta(\mathrm{F}) = 0$ je injektivní homomorfismus. Z 2.10 plyne, že $\mathrm{Im}(\beta) = \{0, 1\}$ je podmonoid $\mathbb{Z}(\cdot, 1)$ (to lze samozřejmě nahlédnout také přímo).

Poznámka. Při definici homomorfismu z algebry $A = A(\alpha_1, \ldots, \alpha_n)$ do algebry $B = B(\alpha_1, \ldots, \alpha_n)$ jsme předpokládali, že operace jsou v oboru algebrách označeny stejně. V předchozím příkladu ovšem neutrální prvek v $\mathbb{Z}$ je 1 a v *Bool* je T. Přesto i zde hovoříme o homomorfismu. Důležité totiž je, aby bylo jasné, která operace v B odpovídá které operaci v A, nikoliv zcela shodné formální označení. V tomto duchu budeme s homomorfismy zacházet i jinde – je to tak pružnější než pracovat s korektnější, ale těžkopádnou definicí, ve které by se formálně specifikovalo, která operace bude odpovídat které.

C. Definujme $\sigma : \mathbb{A}^* \to \mathbb{N}_0$ tak, že pro $a_1, \dots, a_n \in \mathbb{A}$ je $\sigma(a_1 \dots a_n) = n$ (σ udává tedy délku slova). Zobrazení σ je homomorfismus $\mathbb{A}^*$ na $\mathbb{N}_0$.

D. Ať $\Omega \neq \emptyset$. Zobrazení $\omega \in T_\Omega$ nazveme *konstantním,* jestliže existuje $a \in \Omega$ takové, že $\omega(b) = a$ pro každé $b \in \Omega$. Potom množina všech konstantních zobrazení C_Ω tvoří podpologrupu T_Ω. Množina $C_\Omega \cup \{\mathrm{id}_\Omega\}$ je podmonoidem T_Ω.

   Zobrazení $\omega : \Omega \to \Omega$ se nazývá *permutace,* je-li bijektivní. Složení dvou permutací je opět permutace, takže množina S_Ω všech permutací tvoří podmonoid T_Ω. Tomuto podmonoidu se říká *symetrická grupa.* Symetrickou grupu na množině $\{1, 2, \dots, n\}$ značíme S_n.

   Definujme zobrazení $\tau : T_\Omega \to \mathit{Bool}$ tak, že pro $\omega \in T_\Omega$ je $\tau(\omega) = \mathrm{T}$, je-li ω permutace a $\tau(\omega) = \mathrm{F}$, není-li ω permutace. Zobrazení τ je homomorfismus právě když Ω je konečná množina.

Je-li B podalgebra algebry A, tak zobrazení *inkluze* $i_B : B \to A$, $i_B(b) = b$ pro každé $b \in B$, je zjevně injektivní homomorfismus.

Buď dána algebra $A = A(\alpha_1, \dots, \alpha_n)$. Ekvivalenci ρ na A nazveme *kongruencí algebry A,* jestliže je slučitelná s každou operací α_i, $1 \le i \le n$. Z 2.4, 2.5 a 1.2 dostáváme

2.12 Tvrzení. *Buď $A = A(\alpha_1, \dots, \alpha_n)$ algebra. Všechny její kongruence tvoří uzávěrový systém nad $A \times A$.* □

2.13 Tvrzení. *Buď $f : A \to B$ homomorfismus algeber. Potom je* $\ker f$ *kongruence algebry A.* □

Konečně z 2.6 okamžitě odvodíme

2.14 Tvrzení. *Buď ρ kongruence algebry A. Potom přirozené zobrazení* $\mathrm{nat}_\rho :$ $A \to A/\rho$ *je homomorfismus a* $\rho = \ker \mathrm{nat}_\rho$. □

Příklady kongruencí:

A. Pro $a, b \in \mathbb{Z}$ a $n \in N$ pišme $a \equiv b \bmod n$ (a je kongruentní s b modulo n) právě když n dělí $a - b$. Je zřejmé, že $\bmod n$ je kongruence jak $\mathbb{Z}(+, 0)$, tak $\mathbb{Z}(\cdot, 1)$.

B. $\ker \theta$ je kongruence $\mathbb{Z}(\cdot, 1)$, která má dvě ekvivalenční třídy – v jedné leží nula a v druhé všechna ostatní přirozená čísla.

Slovníček morfismů

Ať A a B jsou jsou algebry, jejichž operace si včetně násobnosti jednoznačně odpovídají (a tedy je lze shodně označit). Zobrazení $f : A \to B$ je homomorfismus, *je-li slučitelné se všemi operacemi. Přitom homomorfismus f se nazývá*

$$\left.\begin{array}{l}\textit{endo}\\ \textit{izo}\\ \textit{auto}\end{array}\right\}\textit{morfismus, je-li}\left\{\begin{array}{l}A = B\\ f\ \textit{bijektivní}\\ A = B\ \textit{a}\ f\ \textit{bijektivní}\end{array}\right.$$

Někdy se též mluví o monomorfismech a epimorfismech. Přesné definice záleží na širším kontextu a k jejich porozumění je dobré znát základy teorie kategorií. V mnoha případech však platí, že homomorfismus f je

$$\left.\begin{array}{l}\textit{mono}\\ \textit{epi}\end{array}\right\}\textit{morfismus, je-li } f \textit{ zobrazení}\left\{\begin{array}{l}\textit{injektivní (prosté)}\\ \textit{surjektivní (na)}\end{array}\right.$$

Injektivní homomorfismus se někdy též nazývá vložení, vnoření *nebo* imerse. *Toto označení se používá i pro inkluzi, tedy pro případ, kdy je A podalgebra B a $f(a) = a$ pro všechna $a \in A$.*

Obrázek 2.5: Morfismy

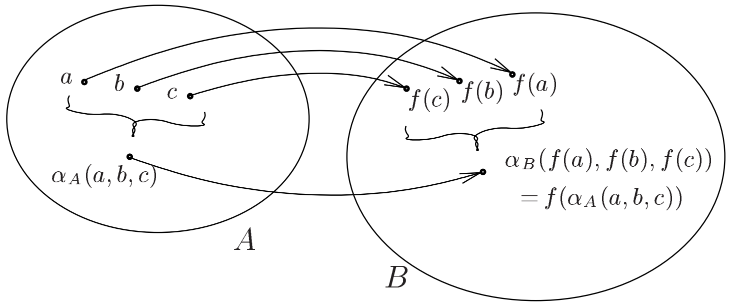
C. $\ker\sigma$ je kongruence $\mathbb{A}^*$, kde ve stejné ekvivalenční třídě leží slova stejné délky.

D. $\ker\tau$ má ekvivalenční třídy S_Ω a $T_\Omega \backslash S_\Omega$. Ekvivalence $\ker\tau$ je kongruence právě když množina $\Omega \neq \emptyset$ je konečná.

Buďte A a B dvě množiny, a ať $f : A \to B$ je bijektivní zobrazení. Předpokládejme, že na A je definována operace četnosti $n \geq 0$. Pak můžeme na B definovat jediným způsobem operaci α tak, aby zobrazení f bylo s α slučitelné — pro $b_1, \ldots, b_n \in B$ takové, že $b_1 = f(a_1), \ldots, b_n = f(a_n)$, je totiž vztah $\alpha_B(b_1, \ldots, b_n) = \alpha_B(f(a_1), \ldots, f(a_n)) = f(\alpha_A(a_1, \ldots, a_n))$ jednoznačnou definicí hodnoty $\alpha_B(b_1, \ldots, b_n)$. Takto definovanou operaci α_B nazýváme operací *indukovanou* bijektivním *zobrazením* f.

Buď nyní dána algebra $A = A(\alpha_1, \ldots, \alpha_k)$ a bijektivní zobrazení $f : A \to$

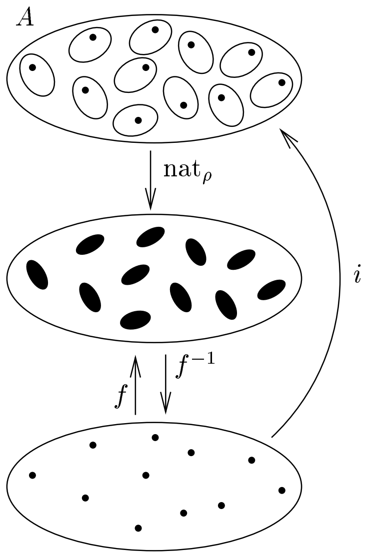
B. Definujme algebru $B = B(\alpha_1, \ldots, \alpha_k)$ tak, že operace $\alpha_1, \ldots, \alpha_k$ na B jsou indukovány zobrazením f. Pak $f : A \to B$ je izomorfismus a o $B = B(\alpha_1, \ldots, \alpha_k)$ mluvíme jako o *algebře indukované* f.



Ať A, B jsou množiny a α ternární operace na A. Ať ještě f je bijekce A a B. Pak na B definujem operaci α tak, aby $\alpha_B(f(a), f(b), f(c))$ se rovnalo $f(\alpha_A(a, b, c))$, a to pro libovolná $a, b, c \in A$. Všimněte si, že použitý obrázek se shoduje s obrázkem ilustrujícím slučitelnost zobrazení f. To je způsobeno tím, že výsledné vztahy jsou stejné. V prvém případě byly dány operace α_A a α_B, a zjišťovali jsme, zda $f : A \to B$ je slučitelné. Nyní je dáno $f : A \to B$ a definujeme α_B tak, aby $f : A \to B$ bylo slučitelné s α. Pro jednoznačnost definice α_B ovšem potřebujeme, aby f bylo bijektivní (tj. vzájemně jednoznačné).

Obrázek 2.6: Operace indukované bijekcí

Je-li ρ ekvivalence na A, tak podmnožinu T množiny A nazýváme *transversálou* ρ, jestliže pro každé $a \in A$ existuje právě jedno $b \in T$ takové, že platí $a\rho b$. Jinými slovy, T je transversála právě když každá ekvivalenční třída ρ obsahuje přesně jeden prvek T. Z definice je tedy zřejmé, že zobrazení $b \mapsto [b]_\rho$ je bijekcí mezi T a A/ρ. V případě, že $A = A(\alpha_1, \ldots, \alpha_k)$ je algebra a ρ je kongruence A, tak zobrazení inverzní k $b \mapsto [b]_\rho$ bijektivně zobrazuje A/ρ na T, a indukuje tak na T operace $\alpha_1, \ldots, \alpha_k$. Je-li například $\alpha = \alpha_1$ četnosti n a $b_1, \ldots, b_n$ jsou prvky T, tak $\alpha_T(b_1, \ldots, b_n)$ je definováno jako ten (jednoznačně určený) prvek $b \in T$, pro který platí $(b, \alpha_A(b_1, \ldots, b_n)) \in \rho$. Algebru $T = T(\alpha_1, \ldots, \alpha_n)$ nazveme algebrou *indukovanou transversálou* T kongruence ρ.



$T \subseteq A$ je tranversálou kongruence ρ algebry A, jestliže v každém bloku ρ je právě jeden bod T (na obrázku jsou body T znázorněny tečkami). Vložení $i : T \to A$, $t \mapsto t$ je jistě injektivní. Pokud T chápeme jako algebru indukovanou transversálou, definujeme na T operace tak, aby $f = \mathrm{nat}_\rho \circ i : T \to A/\rho$ byl izomorfismus. Zatímco nat_ρ i f homomorfismy jsou (a f je dokonce izomorfismus), i je homomorfismus tehdy a jen tehdy, je-li T podalgebra A. V takovém případě se ovšem operace definované na T pomocí f shodují s operacemi na T jako podalgebře. Konstrukce tedy přináší něco nového jen tehdy, jestliže v A nastane situace, kdy operandy leží v T, ale výsledek operace je mimo T.

Obrázek 2.7: Algebra indukovaná tranversálou kongruence

Na závěr této kapitoly zmíníme ještě několik jednoduchých vlastností monoidů.

Prvek a monoidu $S = S(\cdot, \mathbf{1})$ se nazývá *zprava invertibilní,* jestliže existuje takové $b \in S$, že platí $a \cdot b = \mathbf{1}$. Podobně definujeme prvek *zleva invertibilní.*

2.15 Lemma. *Ať pro prvky a, b, c monoidu $S(\cdot, \mathbf{1})$ platí $a \cdot b = \mathbf{1} = c \cdot a$. Potom je b rovno c.*

Důkaz. $b = \mathbf{1} \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot \mathbf{1} = c$. □

Invertibilním nazveme každý prvek, který je současně invertibilní zleva i zprava. Podle 2.15 pro každý invertibilní prvek $a \in S$ existuje jednoznačně určené $b \in S$, jež splňuje $a \cdot b = \mathbf{1} = b \cdot a$. Prvku b se říká prvek *inverzní* (vzhledem k a).

2.16 Lemma. *Uvažme monoid $S = S(\cdot, \mathbf{1})$.*

(i) Ať $b \in S$ je inverzní prvek invertibilního prvku $a \in S$. Potom b je rovněž invertibilní a a je jeho inverzní prvek.
(ii) Ať $a \in S$ je inverzní vzhledem k $b \in S$ a $c \in S$ je inverzní vzhledem k $d \in S$. Potom $a \cdot c$ je inverzní prvek prvku $d \cdot b$.

Důkaz. (i) je zřejmé a (ii) plyne z $(ac) \cdot (db) = a \cdot (cd) \cdot b = a \cdot b = \mathbf{1} = d \cdot c = d \cdot (ba) \cdot c = (db) \cdot (ac)$. □

2.17 Důsledek. *Invertibilní prvky monoidu $S(\cdot, \mathbf{1})$ tvoří podmonoid.* □

3 Věty o homomorfismech a kongruencích

3.1 Lemma. *Ať na množině A i na množině B je dána operace α četnosti n. Jsou-li $f : A \to B$ a $g : A \to B$ zobrazení slučitelná s α, tak $\{a \in A;\ f(a) = g(a)\}$ je uzavřená na α.*

Důkaz. Ať $a_i \in A$ a $f(a_i) = g(a_i)$ pro $1 \leq i \leq n$. Pak $f(\alpha_A(a_1, \ldots, a_n)) = \alpha_B(f(a_1), \ldots, f(a_n)) = \alpha_B(g(a_1), \ldots, g(a_n)) = g(\alpha_A(a_1, \ldots, a_n))$. □

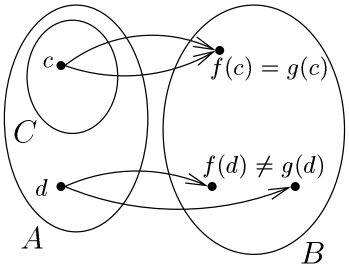
3.2 Tvrzení. *Ať $f : A \to B$, $g : A \to B$ jsou homomorfismy algeber $A = A(\alpha_1, \ldots, \alpha_k)$ a $B = B(\alpha_1, \ldots, \alpha_k)$. Potom $\{a \in A;\ f(a) = g(a)\}$ je podalgebra algebry A.*

Důkaz. $\{a \in A;\ f(a) = g(a)\}$ je podle 3.1 uzavřená na všechny operace α_i, $1 \leq i \leq k$. Je to tedy podalgebra A. □

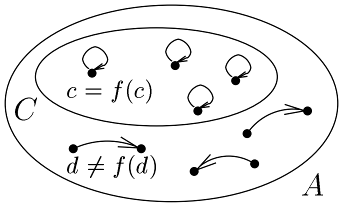
3.3 Důsledek. *Ať $f : A \to B$, $g : A \to B$ jsou homomorfismy algeber $A = A(\alpha_1, \ldots, \alpha_k)$ a $B = B(\alpha_1, \ldots, \alpha_k)$. Jestliže X generuje A a $f(a) = g(a)$ pro každé $a \in X$, tak $f = g$.*

Důkaz. $\{a \in A;\ f(a) = g(a)\}$ je podalgebra A, která obsahuje X. Ovšem jediná podalgebra A, jež obsahuje X, je přímo A. □

Buď ρ ekvivalence na množině A. Každou ekvivalenci na A/ρ lze podle 1.9 jednoznačně vyjádřit jako σ/ρ, kde σ obsahuje ρ. Je-li $A = A(\alpha_1, \ldots, \alpha_n)$ algebra a ρ kongruence, je přirozené se tázat, kdy bude σ/ρ kongruence algebry A/ρ. Ukážeme, že σ/ρ je kongruence A/ρ právě když je σ kongruence A.



Množina bodů C, na které se shodují dané homomorfismy $f : A \to B$ a $g : A \to B$, je podalgebrou A.



Proto platí, že je-li $f \in \mathrm{End}(A)$, je $C = \{c \in A; f(c) = c\}$ také podalgebrou A (lze totiž položit $B = A$ a $g = \mathrm{id}_A$).

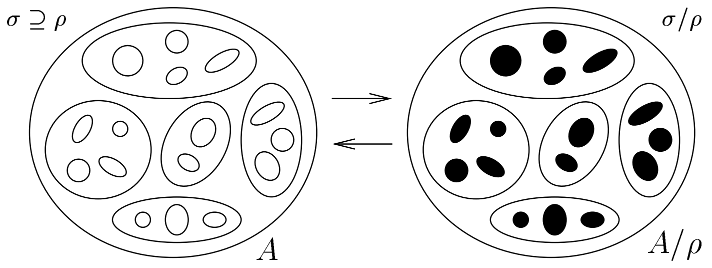
Obrázek 3.1: Podalgebry určené shodou homomorfismů

3.4 Lemma. *Buď ρ ekvivalence na množině A, jež je slučitelná s operací $\alpha = \alpha_A$ na A. Buď $\sigma \supseteq \rho$ další ekvivalence na A. Pak σ je slučitelné s α_A právě když σ/ρ je slučitelné s $\alpha_{A/\rho}$.*

Důkaz. Označme n četnost operace α a ať $a_1, \ldots, a_n$ a $b_1, \ldots, b_n$ jsou prvky A. Podle 1.8 je $(a_i, b_i) \in \sigma$ právě když $([a_i]_\rho, [b_i]_\rho) \in \sigma/\rho$. Předpokládejme, že $(a_i, b_i) \in \sigma$ platí pro všechna i, $1 \le i \le n$. Pak ekvivalence σ je slučitelná s α_A právě když pro libovolnou takovou volbu prvků a_i a b_i platí $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \sigma$, zatímco ekvivalence σ/ρ je slučitelná s $\alpha_{A/\rho}$ právě když pro libovolné takové a_i a b_i platí $([\alpha(a_1, \ldots, a_n)]_\rho, [\alpha(b_1, \ldots, b_n)]_\rho) \in \sigma/\rho$. Poslední podmínka je ovšem, opět podle 1.8, shodná s podmínkou $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \sigma$. □

Z dokázaného lemmatu okamžitě plyne:

3.5 Tvrzení. *Buď ρ kongruence algebry $A = A(\alpha_1, \ldots, \alpha_k)$ a ať $\sigma \supseteq \rho$ je ekvivalence na A. Potom σ/ρ je kongruence algebry A/ρ právě když σ je kongruence algebry A.*



Mezi kongruencemi σ algebry A, které obsahují pevně danou kongruenci ρ algebry A, a všemi kongruencemi algebry A/ρ je vzájemně jednoznačný vztah. Každá kongruence A/ρ je tvaru σ/ρ, $\sigma \supseteq \rho$. Konguence σ/ρ je vlastně konguence σ, ve které se bloky ρ považují za (nové) body.

Obrázek 3.2: Kongruence kvocientní algebry

Buď dána $A = A(\alpha_1, \dots, \alpha_k)$. Triviální ekvivalence id_A i universální ekvivalence $A \times A$ jsou slučitelné s každou operací α_i, $1 \leq i \leq k$, takže obě tyto ekvivalence patří mezi kongruence algebry A. Těmto kongruencím se říká *nevlastní,* zatímco ostatní kongruence algebry A jsou *vlastní.* Nemá-li algebra A vlastní kongruence a má-li přitom alespoň dva prvky, nazýváme ji *jednoduchou.*

Kongruenci ρ algebry $A = A(\alpha_1, \dots, \alpha_k)$ nazveme *maximální,* jestliže

(i) $\rho \neq A \times A$ a

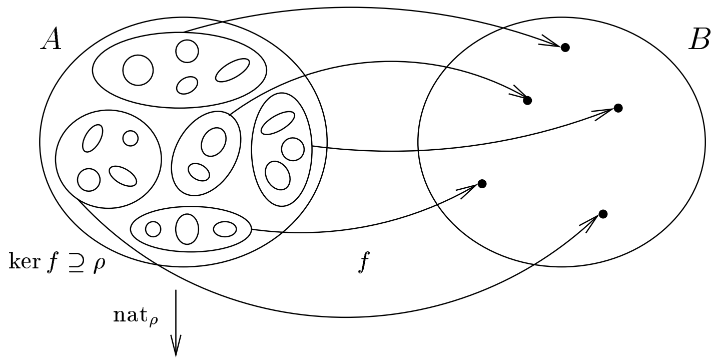
(ii) pro každou kongruenci σ algebry A ze $\sigma \supseteq \rho$ plyne $\sigma = \rho$ nebo $\sigma = A \times A$.

Algebra $A = A(\alpha_1, \dots, \alpha_k)$ je tedy jednoduchá právě tehdy, když id_A je maximální kongruence A.

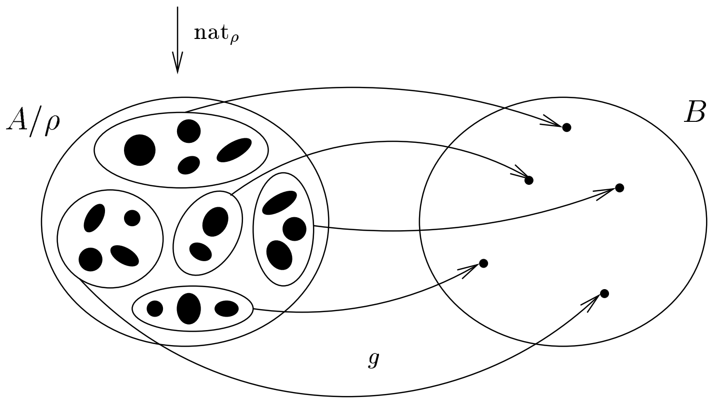
3.6 Tvrzení. *Buď ρ kongruence algebry $A = A(\alpha_1, \dots, \alpha_k)$. Potom A/ρ je jednoduchá algebra právě když ρ je maximální kongruence algebry A.*

Důkaz. Všechny kongruence A/ρ mají podle 3.5 tvar σ/ρ, kde σ obsahuje ρ. Mezi $A \times A$ a ρ proto neleží žádná další kongruence právě tehdy, když neleží žádná kongruence mezi $(A \times A)/\rho = (A/\rho) \times (A/\rho)$ a $\rho/\rho = \mathrm{id}_{A/\rho}$. $\square$

Ať je dán homomorfismus $f : A \to B$ algeber A a B a ať je dána kongruence ρ algebry A, která je obsažena v jádru f. Jde tedy o následující situaci (menší ovály jsou bloky ρ, větší ovály jsou bloky $\ker f$):



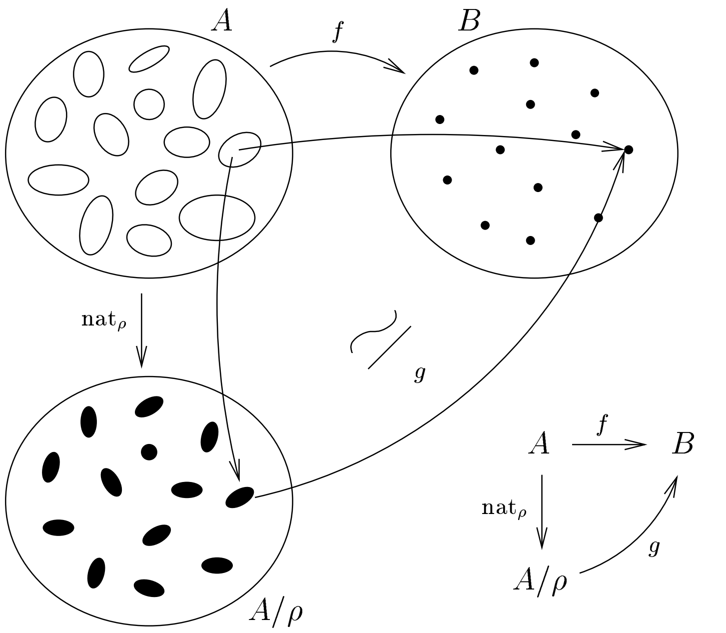
Věta o homomorfismu říká, že v této situaci existuje jediné $g : A/\rho \to B$ tak, aby $f = g \circ \operatorname{nat} \rho$.



Je zřejmé, že $\ker g = (\ker f)/\rho$.

Obrázek 3.3: Věta o homomorfismu

V případě, kdy $f : A \to B$ je surjektivní homomorfismus algeber a $\rho = \ker f$, dostaneme z Věty o homomorfismu První větu o izomorfismu.

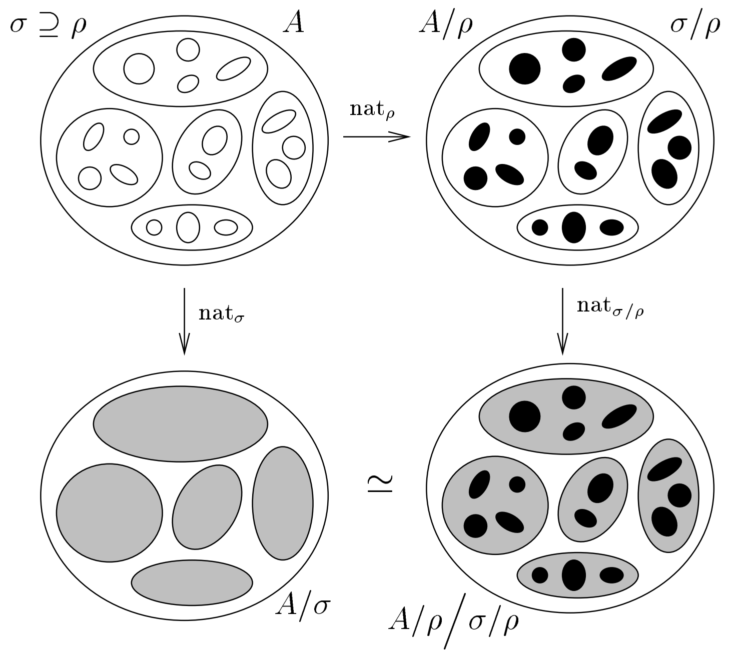


Obrázek 3.4: První věta o izomorfismu

Nyní obrátíme svou pozornost na Tvrzení 1.10 a ukážeme, jak ho vztáhnout na algebry. Následující věty patří v algebře k těm nejužívanějším.

3.7 Lemma. *Ať je na množině A i na množině B dána operace α četnosti n a ať $f : A \to B$ je zobrazení slučitelné s α. Ať dále ρ je ekvivalence A slučitelná s α. Zobrazení $g : A/\rho \to B$ slučitelné s α a takové, že $f = g \circ \mathrm{nat}_\rho$, existuje právě když $\rho \subseteq \ker f$. Je-li $\rho \subseteq \ker f$, je g určeno jednoznačně, $g([a]_\rho) = f(a)$ pro každé $a \in A$ a $\ker g = (\ker f)/\rho$.*

Důkaz. Vzhledem k 1.10 je třeba pouze dokázat, že v případě $\rho \subseteq \ker f$ je zob-



Ačkoliv Druhá věta o izomorfismu může na prvý pohled vyvolávat dojem něčeho velmi složitého, obrázek jasně ukazuje, že izomorfismus A/σ *a* $A/\rho\Big/\sigma/\rho$ *není nic jiného, nežli způsob pohledu na bloky kongruence* σ*, které se v* $A/\rho\Big/\sigma/\rho$ *projeví jako množiny složené z těch bloků* ρ*, jež jsou v daném bloku* σ *obsaženy.*

Obrázek 3.5: Druhá věta o izomorfismu

razení g dané vztahem $g([a]_\rho) = f(a)$ slučitelné s α. Ať $a_1, \ldots, a_n \in A$. Pak $g(\alpha_{A/\rho}([a_1]_\rho, \ldots, [a_n]_\rho)) = g([\alpha_A(a_1, \ldots, a_n)]_\rho) = f(\alpha_A(a_1, \ldots, a_n))$, což je rovno $\alpha_B(f(a_1), \ldots, f(a_n)) = \alpha_B(g([a_1]_\rho), \ldots, g([a_n])_\rho))$. $\square$

Ze 3.7 bezprostředně dostáváme:

3.8 Tvrzení. (Věta o homomorfismu.) *Buď dán homomorfismus* $f : A \to B$ *algeber* $A = A(\alpha_1, \ldots, \alpha_k)$ *a* $B = B(\alpha_1, \ldots, \alpha_k)$, *a ať* ρ *je kongruence* A. *Homomorfismus* $g : A/\rho \to B$ *takový, že* $f = g \circ \mathrm{nat}_\rho$, *existuje právě když* $\rho \subseteq \ker f$. *Je-li* $\rho \subseteq \ker f$, *pak je* g *určeno jednoznačně,* $g([a]_\rho) = f(a)$ *pro každé* $a \in A$ *a* $\ker g = (\ker f)/\rho$. *Přitom* g *je izomorfismus právě když je* f *surjektivní a platí* $\ker f = \rho$.

3.9 Důsledek. (První věta o izomorfismu.) *Ať* $f : A \to B$ *je surjektivní homomorfismus algeber* $A = A(\alpha_1, \ldots, \alpha_k)$ *a* $B = B(\alpha_1, \ldots, \alpha_k)$. *Pak* $[a]_{\ker f} \mapsto f(a)$ *je izomorfismus algeber* $A/\ker f$ *a* B.

3.10 Důsledek. (Druhá věta o izomorfismu.) *Ať* $A = A(\alpha_1, \ldots, \alpha_k)$ *je algebra a* $\rho \subseteq \sigma$ *jsou její kongruence. Pak* $[[a]_\rho]_{\sigma/\rho} \mapsto [a]_\sigma$ *je izomorfismus* $A/\rho \Big/ \sigma/\rho \simeq A/\sigma$.

Důkaz. Podle 3.8 lze $\mathrm{nat}_\sigma : a \mapsto [a]_\sigma$ faktorizovat přes ρ, takže $[a]_\rho \mapsto [a]_\sigma$ je homomorfismus $A/\rho \to A/\sigma$. Jeho jádrem je podle 3.8 kongruence σ/ρ a zbytek plyne z 3.9. □

4 Uspořádané množiny, svazy a Galoisova korespondence

Relaci $\leq$ na množině M nazveme *uspořádáním* M, jestliže $\leq$ je reflexivní, tranzitivní a jestliže pro libovolná $a, b \in M$ z $a \leq b$ a $b \leq a$ plyne $a = b$.

Uspořádání, kde pro libovolné $a, b \in M$ platí $a \leq b$ nebo $b \leq a$, se nazývá *lineární.*

Poznámka. Často se používá jiné terminologie: relace uvedených vlastností se nazývá *částečné uspořádání,* přičemž uspořádáním se míní lineární uspořádání. Částečně uspořádané množiny se pak leckdy označují akronymem *poset* — z anglického 'partially ordered set'.

Dva prvky a, b uspořádané množiny $(M, \leq)$ se nazývají *porovnatelné,* je-li $a \leq b$ nebo $b \leq a$. V opačném případě jsou tyto prvky *neporovnatelné.* Prvek $a \in A \subseteq M$ je *nejmenší* prvek A, pokud $a \leq b$ pro každé $b \in A$. Dále $a \in A \subseteq M$ je *největší* prvek A, je-li $b \leq a$ pro všechna $b \in A$. Každá množina $A \subseteq M$ má zjevně nanejvýš jeden největší a nanejvýš jeden nejmenší prvek.

Prvek $a \in M$ je *dolní závorou* množiny $A \subseteq M$, jestliže $a \leq b$ pro každé $b \in A$. Prvek $a \in M$ je *horní závorou* množiny $A \subseteq M$, jestliže $b \leq a$ pro každé $b \in A$. Všimněte si, že každý prvek $a \in M$ je dolní i horní závorou prázdné množiny.

Buď $A \subseteq M$. Označme na chvíli B množinu horních závor A a C množinu jeho dolních závor. Nejmenší prvek B (pokud existuje) se nazývá *supremum* A (značíme $\sup_{\leq} A$). Podobně největší dolní závoru (pokud existuje) nazýváme *infimum* A ($\inf_{\leq} A$).

Řekneme, že $b \in M$ *pokrývá* $a \in M$, jestliže $a \leq b$, $a \neq b$ a pro $a \leq c \leq b$ je buď $a = c$, nebo $b = c$. Někdy se pak píše $a \lessdot b$.

Jestliže M obsahuje nejmenší prvek, řekněme e, tak $a \in M$ se nazývá *atomem* právě když a pokrývá e. Jestliže M obsahuje největší prvek, řekněme f, tak $a \in M$ se nazývá *koatomem* právě když f pokrývá a.

V $(\mathbb{Z}, \leq)$ je každé číslo k pokryté číslem $k+1$. Naopak, v $(\mathbb{Q}, \leq)$ žádný prvek pokrytí nemá.

Je-li $(M, \leq)$ konečná uspořádaná množina, má v ní každý prvek pokrytí. Grafické zachycení relace pokrytí (a a b spojíme úsečkou právě když $a \lessdot b$, přičemž b umístíme výše než a) se nazývá *Hasseův diagram.*

Definujeme-li na M relaci $\preccurlyeq$ tak, že $a \preccurlyeq b$ právě když $b \leq a$, dostaneme opět uspořádání. Tomuto uspořádání se říká *opačné.* Při přechodu od $\leq$ k $\preccurlyeq$ se z koatomů stanou atomy, z horních závor dolní závory, ze suprem infima, a naopak.

4.1 Lemma. *Buď M_i, $i \in I$ podmnožiny uspořádané množiny $(M, \leq)$. Ať pro každé $i \in I$ je $b_i \in M$ supremem množiny M_i. Potom $\sup_{\leq}\{b_i; i \in I\}$ existuje právě když existuje $\sup_{\leq}(\bigcup(M_i;\ i \in I))$. Přitom obě suprema, pokud existují, si jsou rovna.*

Důkaz. Ať $b = \sup_{\leq}\{b_i; i \in I\}$. Je-li $a \in \bigcup(M_i;\ i \in I)$, je $a \in M_i$ pro nějaké $i \in I$, a tedy $a \leq b_i \leq b$. Je-li c takové, že $a \leq c$ pro všechna $a \in \bigcup(M_i;\ i \in I)$, je též $b_i \leq c$ pro všechna $i \in I$, takže $b \leq c$. Naopak, ať $m = \sup(\bigcup(M_i;\ i \in I))$. Pak $m \geq b_i$ pro každé $i \in I$. Je-li $d \geq b_i$ pro všechna $i \in I$, je i $d \geq a$ pro všechna $a \in \bigcup(M_i;\ i \in I)$, takže $d \geq m$. $\square$

Podobné lemma lze vyslovit a dokázat též pro infima. Ovšem infima jsou suprema v opačném uspořádání, takže takovéto duální lemma je zřejmé a není nutné ho výslovně uvádět.

Předpokládejme nyní, že $(M, \leq)$ je taková uspořádaná množina, že každé dva prvky z M mají supremum i infimum. Pak z 4.1 indukcí okamžitě vyplývá, že každá konečná neprázdná množina má supremum i infimum. Označíme-li $a \vee b =$

$\sup_{\leq}\{a,b\}$ a $a \wedge b = \inf_{\leq}\{a,b\}$ pro každé $a, b \in M$, dostáváme dvě binární operace na M (nazývají se *spojení* a *průsek*). Pro tyto operace platí

(komutativita)
$$a \wedge b = b \wedge a \quad \text{a} \quad a \vee b = b \vee a$$
(idempotence)
$$a \wedge a = a = a \vee a$$
(asociativita)
$$(a \wedge b) \wedge c = a \wedge (b \wedge c) \quad \text{a} \quad (a \vee b) \vee c = a \vee (b \vee c)$$
(absorpce)
$$a \wedge (b \vee a) = a = a \vee (b \wedge a)$$

Ověřit uvedené identity je snadné – přitom asociativita vyplývá z 4.1, neboť $(a \vee b) \vee c = \sup_{\leq}\{a,b,c\} = a \vee (b \vee c)$.

Algebra $M = M(\wedge, \vee)$, ve které jsou definovány binární operace $\wedge$ a $\vee$, jež splňují komutativní, idempotentní, asociativní a absorpční zákon, se nazývá *svaz.*

Ve svazu $M = M(\wedge, \vee)$ zaveďme relaci $\leq$ tak, že $a \leq b$ právě když $b = a \vee b$. Potom $a \leq a$ podle idempotentního zákona, $a \leq b$ a $b \leq c$ implikuje $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$ a z $a \leq b$, $b \leq a$ máme $b = a \vee b = b \vee a = a$. $(M, \leq)$ je tedy uspořádaná množina. Přitom pro každé $a, b \in M$ je $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$, takže $a \leq a \vee b$ a $b \leq a \vee b$. Je-li $c \geq a$ a $c \geq b$, je $c \vee (a \vee b) = (c \vee a) \vee b = c \vee b = c$, takže $a \vee b$ je supremum množiny $\{a, b\}$. Je-li $b = a \vee b$, je $a \wedge b = a \wedge (a \vee b) = a$. Naopak, je-li $a \wedge b = a$, je $a \vee b = a \vee (a \wedge b) = a$. To znamená, že $a \leq b$ platí právě když $a \wedge b = a$. Z této ekvivalentní definice uspořádání se analogicky dokáže, že $\inf\{a, b\} = a \wedge b$.

Z předchozího plyne, že svaz můžeme definovat ekvivalentně jako uspořádanou množinu, kde každé dva prvky mají supremum a infimum. Je zbytečné rozhodovat, zda prvotní by měla být tato definice, nebo definice vycházející z identit. V dalším budeme prostě předpokládat, že ve svazu máme definovány jak operace průseku a spojení, tak uspořádání.

Ve svazu může a nemusí existovat nejmenší a největší prvek. Pokud chceme existenci nejmenšího a největšího prvku algebraicky zachytit, definujeme 'svaz s nulou a jedničkou' $M = M(\wedge, \vee, \mathbf{0}, \mathbf{1})$, kde navíc platí identity
$$a \wedge \mathbf{1} = a = a \vee \mathbf{0}.$$
(Důsledkem absorpčního zákona pak je, že $a \vee \mathbf{1} = \mathbf{1}$ a $a \wedge \mathbf{0} = \mathbf{0}$.)

Svaz nazveme *úplný,* jestliže každá množina má supremum a infimum. V úplném svazu tedy existuje největší a nejmenší prvek (uvědomte si, že největší prvek je infimem prázdné množiny).

Množina všech podmnožin dané množiny s uspořádáním inkluzí a operacemi průniku a sjednocení je úplný svaz. Jeho podsvazem je svaz konečných množin. Sjednocení konečných množin nemusí být konečná množina, proto na nekonečné množině není podsvaz konečných množin úplný. Soustavu $\mathcal{P}(M)$ všech podmnožin dané množiny M bychom však mohli také chápat jako $\mathbf{0},\mathbf{1}$–svaz, ve kterém $\mathbf{0} = \emptyset$ a $\mathbf{1} = M$. Je-li M nekonečná množina, tak ovšem množina všech konečných podmnožin není podalgebra algebry $\mathcal{P}(M)(\cap, \cup, \mathbf{0}, \mathbf{1})$, třebaže je podalgebrou algebry $\mathcal{P}(M)(\cap, \cup)$.

4.2 Tvrzení. *Buď $\mathcal{C}$ uzávěrový systém nad množinou A. Potom $(\mathcal{C}, \subseteq)$ je úplný svaz, ve kterém pro $\mathcal{B} \subseteq \mathcal{C}$ platí* $\inf \mathcal{B} = \bigcap(C;\ C \in \mathcal{B})$ *a* $\sup \mathcal{B} = \mathrm{cl}_{\mathcal{C}}(\bigcup(C;\ C \in \mathcal{B}))$.

Důkaz. To, že $\inf \mathcal{B} = \bigcap(C;\ C \in \mathcal{B})$, plyne z toho, že $\bigcap(C;\ C \in \mathcal{B})$ je infimum v $\mathcal{P}(A)$. Položme $D = \bigcup(C;\ C \in \mathcal{B})$. Pak $C \subseteq \mathrm{cl}_{\mathcal{C}}\, D$ pro každé $C \in \mathcal{B}$, takže $\mathrm{cl}_{\mathcal{C}}\, D$ je horní závora. Je-li $E \in \mathcal{C}$ takové, že $C \subseteq E$ pro každé $C \in \mathcal{B}$, je $D \subseteq E$, a tedy $\mathrm{cl}_{\mathcal{C}}\, D \subseteq \mathrm{cl}_{\mathcal{C}}\, E = E$. $\square$

Všechny ekvivalence na množině A tvoří uzávěrový systém nad $A \times A$, takže podle 4.2 můžeme množinu všech ekvivalencí pokládat za svaz. Ze 4.2 a z 1.6 plyne, že spojení $\vee(\rho_i;\ i \in I)$, kde ρ_i jsou ekvivalence na A, je rovno $(\cup(\rho_i;\ i \in I))^+$.

Je-li $A = A(\alpha_1, \ldots, \alpha_k)$ algebra, tak podle 2.8 a 2.12 lze za svaz považovat jak množinu všech podalgeber A (značívá se $\mathrm{Sub}(A)$), tak množinu všech kongruencí algebry A (značívá se $\mathrm{Con}(A)$). Sjednocení dvou podalgeber nemusí být podalgebrou, takže $\mathrm{Sub}(A)$ obvykle není podsvazem svazu $\mathcal{P}(A)$. Lze však dokázat (a není to obtížné), že $\mathrm{Con}(A)$ je vždy podsvazem svazu všech ekvivalencí na A.

Uvažme nějaký uzávěrový systém $\mathcal{C}$ nad množinou A a připomeňme, že $(\mathcal{C}, \subseteq)$ je podle 4.2 úplný svaz. Atomy v takovém svazu je zvykem spojovat se slovem *minimální* a koatomy se slovem *maximální,* takže mluvíme například o maximální podalgebře nebo kongruenci. Všimněte si, že maximální kongruence byly v kapitole 3 skutečně takto definovány.

Slova minimální a maximální budeme v tomto textu používat pouze právě uvedeným způsobem. Budiž však poznamenáno, že často se minimálním prvkem množiny $A \subseteq M$, kde $\leq$ je uspořádání M, míní každý takový prvek $a \in A$, pro který platí $a \leq b$, kdykoliv $b \in A$ je porovnatelné s a. Podobně lze samozřejmě definovat i maximální prvky. Takovéto chápání slov maximální a minimální se však v dalším textu neuplatní.

Podobnou konvenci jako pro slova maximální a minimální zavedeme i pro slova *vlastní* a *nevlastní*, kde vlastní jsou ty množiny uzávěrového systému, které jsou různé od jeho nejmenší a největší množiny. Hovoříme tedy o vlastních či nevlastních podalgebrách, nebo vlastních či nevlastních kongruencích. V tomto smyslu byl ostatně pojem vlastní kongruence definován již v předchozí kapitole.

Jestliže v axiomech svazu zaměníme $\wedge$ a $\vee$, axiomy se nezmění. Proto, když ke svazu $L = L(\wedge, \vee)$ definujeme algebru $L^{op} = L(\wedge_{op}, \vee_{op})$ tak, že $a \wedge_{op} b = a \vee b$ a $a \vee_{op} b = a \wedge b$, dostaneme opět svaz, tento svaz se nazývá svazem *opačnými.* Označíme-li uspořádání v L symbolem $\leq$ a uspořádání v L^{op} symbolem $\leq_{op}$, vidíme, že $a \leq_{op} b$ právě když $a = a \wedge_{op} b = a \vee b$, což platí právě když $a \leq b$. Uspořádání v opačném svazu je tedy opačné uspořádání.

Jsou-li $(A, \leq)$ a $(B, \leq)$ dvě uspořádané množiny, tak zobrazení $f : A \to B$ se nazývá *monotonní,* jestliže pro všechna $a, b \in A$ z $a \leq b$ plyne $f(a) \leq f(b)$.

4.3 Lemma. *Buďte $L = L(\wedge, \vee)$ a $M = M(\wedge, \vee)$ dva svazy. Je-li $f : L \to M$ homomorfismus svazů, je f monotonní zobrazení.*

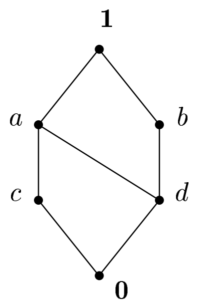
Důkaz. Ať $a, b \in L$ a $a \leq b$. Pak $f(a) \wedge f(b) = f(a \wedge b) = f(a)$, takže je $f(a) \leq f(b)$. □

4.4 Tvrzení. *Buďte $L = L(\wedge, \vee)$ a $M = M(\wedge, \vee)$ dva svazy. Bijektivní zobrazení $f : L \to M$ je izomorfismus těchto svazů právě když f i f^{-1} jsou monotonní.*

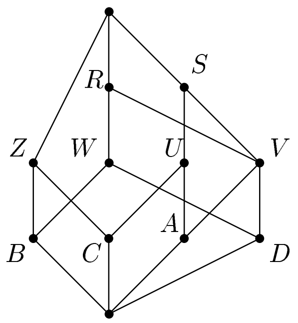
Důkaz. Je-li f izomorfismus, jsou f a f^{-1} monotonní dle 4.3. Naopak, buďte f a f^{-1} monotonní a ať $a, b \in L$. Potom $f(a \wedge b) \leq f(a)$, $f(a \wedge b) \leq f(b)$ a pro $d \in M$ takové, že $d \leq f(a)$ a $d \leq f(b)$, existuje $c \in L$, že $f(c) = d$. Tudíž $c = f^{-1}(d) \leq f^{-1}(f(a)) = a$, a stejně tak $c \leq b$. Proto $c \leq a \wedge b$ a $f(c) = d \leq f(a \wedge b)$. Dokázali jsme $f(a \wedge b) = \inf\{f(a), f(b)\}$, takže nutně $f(a \wedge b) = f(a) \wedge f(b)$. Obdobně se ukáže $f(a \vee b) = f(a) \vee f(b)$. □

4.5 Lemma. *Buďte $(A, \leq)$ a $(B, \leq)$ uspořádané množiny a ať $f : A \to B$ je prosté monotonní zobrazení. Je-li $a \in C \subseteq A$ nejmenší (největší) prvek C, je $f(a)$ nejmenší (největší) prvek $f(C) \subseteq B$.*

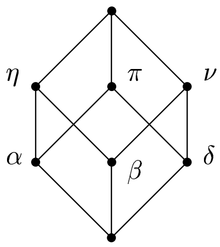
Důkaz. Buď $d = f(c)$ pro $c \in C$. Pak $a \leq c$, a proto $f(a) \leq f(c) = d$. □



Ať L značí $\mathbf{0},\mathbf{1}$–svaz s uvedeným Hasseovým diagramem. Není obtížné ověřit, že všechny vlastní podalgebry svazu $L(\wedge,\vee,\mathbf{0},\mathbf{1})$ (tedy všechny vlastní $\mathbf{0},\mathbf{1}$–podsvazy) jsou tyto: $A=\{\mathbf{0},\mathbf{1},a\}$, $B=\{\mathbf{0},\mathbf{1},b\}$, $C=\{\mathbf{0},\mathbf{1},c\}$, $D=\{\mathbf{0},\mathbf{1},d\}$, $U=\{\mathbf{0},\mathbf{1},a,c\}$, $V=\{\mathbf{0},\mathbf{1},a,d\}$, $W=\{\mathbf{0},\mathbf{1},b,d\}$, $Z=\{\mathbf{0},\mathbf{1},b,c\}$, $R=\{\mathbf{0},\mathbf{1},a,b,d\}$ a $S=\{\mathbf{0},\mathbf{1},a,c,d\}$.



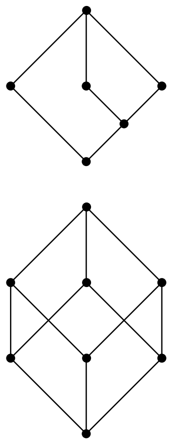
Všechny $\mathbf{0},\mathbf{1}$–podsvazy L tvoří uzávěrový systém $\mathrm{Sub}(L)$, který je svazem vzhledem k uspořádání inkluzí. Vlevo je uveden Hasseův diagram tohoto svazu. Podalgebry Z, R, S jsou maximální a podalgebry B, C, A, D jsou minimální.



Svaz L má 6 vlastních kongruencí. Při jejich výčtu píšeme místo $M\times M$, kde M je množina, pouze M^2. Běží o ekvivalence $\alpha=\{\mathbf{1},a\}^2\cup\{b,d\}^2\cup\{c\}^2\cup\{\mathbf{0}\}^2$; $\beta=\{\mathbf{1},b\}^2\cup\{a,d\}^2\cup\{\mathbf{0},c\}^2$; $\delta=\{\mathbf{1}\}^2\cup\{b\}^2\cup\{a,c\}^2\cup\{\mathbf{0},d\}^2$; $\eta=\{\mathbf{1},a,b,d\}^2\cup\{\mathbf{0},c\}^2$; $\nu=\{\mathbf{1},b\}^2\cup\{\mathbf{0},a,c,d\}^2$ a $\pi=\{\mathbf{1},a,c\}^2\cup\{\mathbf{0},b,d\}^2$.

Obrázek 4.1: Podsvazy a kongruence $\mathbf{0},\mathbf{1}$–svazů

Ať L je svaz stejný jako na obr. 4.1. Všimněte si, že svaz kongruencí $\mathrm{Con}(L)$ je izomorfní svazu $\mathcal{P}(M)$, kde M je libovolná tříprvková množina. Kongruence η, π, ν jsou maximální a kongruence α, β, δ jsou minimální.



Položme $\mathcal{C} = \mathrm{Con}(L)$ a hleďme na $\mathcal{C}$ především jako na uzávěrový systém. Pak $\mathcal{C}_b = \big\{L, \{b\}, \{b,d\}, \{\mathbf{1},b\}, \{a,b,d\}, \{\mathbf{0},b,d\}\big\}$ je uzávěrový systém, který indukuje svaz s Hasseovým diagramem na horním obrázku, zatímco $\mathcal{C}_d = \big\{L, \{d\}, \{b,d\}, \{a,d\}, \{\mathbf{0},d\}, \{\mathbf{1},a,b,d\}, \{\mathbf{0},a,c,d\}, \{\mathbf{0},b,d\}\big\}$ je uzávěrový systém, který poskytuje svaz s Hasseovým diagramem na dolním obrázku. Zobrazení $\mathcal{C} \mapsto \mathcal{C}_d$, které $\sigma \in \mathcal{C}$ přiřazuje $[d]_\sigma$, je izomorfismus příslušných svazů.

Obrázek 4.2: Uzávěrové systémy vzniklé volbou pevného bodu

4.6 Lemma. *Buď $\mathcal{C}$ takový uzávěrový systém nad množinou $A \times A$, že každý prvek $\rho \in \mathcal{C}$ je ekvivalencí nad A. Pak pro každé $a \in A$ je $\mathcal{C}_a = \{[a]_\rho;\ \rho \in \mathcal{C}\}$ uzávěrový systém nad A.*

Důkaz. Ať $\rho = \cap(\rho_i;\ i \in I)$, kde I je neprázdná množina a $\rho_i \in \mathcal{C}$ pro všechna $i \in I$. Protože $[a]_\rho$ je rovno $\cap([a]_{\rho_i}; i \in I)$ a $\mathcal{C}_a$ obsahuje $A = [a]_{A\times A}$, je $\mathcal{C}_a$ vskutku uzávěrový systém nad A. □

4.7 Lemma. *Buď $\mathcal{C}$ takový uzávěrový systém nad množinou $A \times A$, že každý prvek $\rho \in \mathcal{C}$ je ekvivalence na A. Ať $\mathcal{N}$ je nějaký systém podmnožin množiny A a ať e je prvek A. Předpokládejme, že platí:*

(1) Pro každé $\rho \in \mathcal{C}$ je $[e]_\rho \in \mathcal{N}$,
(2) jsou-li $\rho, \eta \in \mathcal{C}$, tak z $[e]_\rho \subseteq [e]_\eta$ plyne $\rho \subseteq \eta$, a
(3) pro každé $N \in \mathcal{N}$ lze nalézt takové $\rho \in \mathcal{C}$, že je $N = [e]_\rho$.

Potom je $\mathcal{N}$ uzávěrový systém nad A a zobrazení $\rho \mapsto [e]_\rho$ je izomorfismem svazů $(\mathcal{C}, \subseteq)$ a $(\mathcal{N}, \subseteq)$.

Důkaz. Podle (1) a (3) je $\mathcal{N}$ rovno $\mathcal{C}_e$ ve smyslu 4.6. Je-li $[e]_\rho$ rovno $[e]_\eta$, kde ρ a η patří do $\mathcal{C}$, je podle (2) $\rho \subseteq \eta$ a $\eta \subseteq \rho$, takže platí $\rho = \eta$. Podle (2) a (3) je proto zobrazení $\rho \mapsto [e]_\rho$ bijekcí. Jelikož z $\eta \subseteq \rho$ jistě plyne $[e]_\eta \subseteq [e]_\rho$, tak je podle (2) a 4.4 toto zobrazení izomorfismem svazů $(\mathcal{C}, \subseteq)$ a $(\mathcal{N}, \subseteq)$. □

Buďte A a B dvě množiny. Dvojici zobrazení $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ nazveme *Galoisovou korespondencí,* jestliže platí

(i) Z $A_1 \subseteq A_2 \subseteq A$ plyne $\alpha(A_2) \subseteq \alpha(A_1)$ a z $B_1 \subseteq B_2 \subseteq B$ plyne $\beta(B_2) \subseteq \beta(B_1)$, a to pro všechna $A_1 \subseteq A_2 \subseteq A$ a $B_1 \subseteq B_2 \subseteq B$.

(ii) Pro všechna $A_1 \subseteq A$ a $B_1 \subseteq B$ platí $\beta(\alpha(A_1)) \supseteq A_1$ a $\alpha(\beta(B_1)) \supseteq B_1$.

4.8 Lemma. *Buď $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$, $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ Galoisova korespondence. Potom $\alpha\beta\alpha(A_1) = \alpha(A_1)$ pro každé $A_1 \in \mathcal{P}(A)$ a $\beta\alpha\beta(B_1) = \beta(B_1)$ pro všechna $B_1 \in \mathcal{P}(B)$.*

Důkaz. Z (ii) dostáváme $\alpha\beta(\alpha(A_1)) \supseteq \alpha(A_1)$ a $\beta\alpha(\beta(B_1)) \supseteq \beta(B_1)$. Naopak z $\beta\alpha(A_1) \supseteq A_1$ a $\alpha\beta(B_1) \supseteq B_1$ podle (i) plyne $\alpha\beta\alpha(A_1) \subseteq \alpha(A_1)$ a $\beta\alpha\beta(B_1) \subseteq \beta(B_1)$. □

4.9 Tvrzení. *Buď $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$, $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ Galoisova korespondence. Potom $\beta\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ a $\alpha\beta : \mathcal{P}(B) \to \mathcal{P}(B)$ jsou uzávěrové operátory. Označme $\mathcal{A} \subseteq \mathcal{P}(A)$ a $\mathcal{B} \subseteq \mathcal{P}(B)$ příslušné uzávěrové systémy. Pak $\alpha(A_1) \in \mathcal{B}$ a $\beta(B_1) \in \mathcal{A}$ pro všechna $A_1 \subseteq A$, $B_1 \subseteq B$. Označme $\alpha' : \mathcal{A} \to \mathcal{B}$ a $\beta' : \mathcal{B} \to \mathcal{A}$ odpovídající zúžení α a β. Zobrazení α' a β' jsou bijektivní a $\alpha' = (\beta')^{-1}$. Pro $A_1, A_2 \in \mathcal{A}$ je $A_1 \subseteq A_2$ právě když $\alpha(A_1) \supseteq \alpha(A_2)$.*

Důkaz. Z $A_1 \subseteq A_2 \subseteq A$ podle (i) dostáváme $\alpha(A_1) \supseteq \alpha(A_2)$, a opět podle (i) $\beta\alpha(A_1) \subseteq \beta\alpha(A_2)$. Podle 4.6 je $\beta\alpha\beta\alpha(A_1) = \beta\alpha(A_1)$. Dokázali jsme, že $\beta\alpha$ je uzávěrový operátor. Podobně je i $\alpha\beta$ uzávěrový operátor. Je-li $A_1 \subseteq A$, je $\alpha\beta\alpha(A_1) = \alpha(A_1)$, a tudíž $\alpha(A_1) \in \mathcal{B}$. Podobně $\beta(B_1) \in \mathcal{A}$ pro $B_1 \subseteq B$. Pro $A_1 \in \mathcal{A}$ je $\beta\alpha(A_1) = A_1$ a pro $B_1 \in \mathcal{B}$ je $\alpha\beta(B_1) = B_1$, takže α' a β' jsou vzájemně inverzní. Jsou-li $A_1, A_2 \in \mathcal{A}$, tak z $A_1 \subseteq A_2$ plyne $\alpha(A_1) \supseteq \alpha(A_2)$ podle (i). Platí-li $\alpha(A_1) \supseteq \alpha(A_2)$, tak $A_1 = \beta\alpha(A_1) \subseteq \beta\alpha(A_2) = A_2$. □

Poznámka. Díváme-li se na $\mathcal{A}$ a na $\mathcal{B}$ jako na svazy (viz 4.2), tak podle 4.4 je α' izomorfismus svazů $\mathcal{A}$ a $\mathcal{B}^{op}$. Izomorfismu svazu a opačného svazu se říká *antiizomorfismus.* (Je-li $f : L \to M$ antiizomorfismus svazů, je $f(a \wedge b) = f(a) \vee f(b)$ a $f(a \vee b) = f(a) \wedge f(b)$ pro libovolná $a, b \in L$.)

Tuto kapitolu zakončíme následujícím příkladem.

Buď $\rho \subseteq A \times B$. Definujme zobrazení $\alpha_\rho : \mathcal{P}(A) \to \mathcal{P}(B)$ tak, že pro $A_1 \subseteq A$ je $\alpha_\rho(A_1) = \{b \in B;\, a\rho b$ pro každé $a \in A_1\}$, a zobrazení $\beta_\rho : \mathcal{P}(B) \to \mathcal{P}(A)$ tak, že pro $B_1 \subseteq B$ je $\beta_\rho(B_1) = \{a \in A;\, a\rho b$ pro každé $b \in B_1\}$.

4.10 Tvrzení. *Buď dána relace $\rho \subseteq A \times B$. Potom $\alpha_\rho : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta_\rho : \mathcal{P}(B) \to \mathcal{P}(A)$ tvoří Galoisovu korespondenci.*

Důkaz. Buď $A_1 \subseteq A$. Potom $\beta_\rho\alpha_\rho(A_1) = \{a' \in A;\, a'\rho b$ pro všechna $b \in \alpha_\rho(A_1)\}$. Je-li $a \in A_1$, je $a\rho b$ pro každé $b \in \alpha_\rho(A_1)$, takže $A_1 \subseteq \beta_\rho\alpha_\rho(A_1)$. Podobně $B_1 \subseteq \alpha_\rho\beta_\rho(B_1)$ pro libovolné $B_1 \subseteq B$. Pro $A_1 \subseteq A_2 \subseteq A$ je zjevně $\{b \in B;\, a\rho b$ pro všechna $a \in A_1\} \supseteq \{b \in B;\, a\rho b$ pro všechna $a \in A_2\}$, takže $\alpha_\rho(A_1) \supseteq \alpha_\rho(A_2)$, a obdobně $\beta_\rho(B_1) \supseteq \beta_\rho(B_2)$ pro $B_1 \subseteq B_2 \subseteq B$. $\square$

Představme si nyní, že množina A je množina nějakých objektů, že množina B je množina vlastností (atributů) a že relace ρ značí, že objekt $a \in A$ má vlastnost $b \in B$. Buď $\mathcal{A} \subseteq \mathcal{P}(A)$ a $\mathcal{B} \subseteq \mathcal{P}(B)$ uzávěrové systémy dané Galoisovou korespondencí α_ρ, β_ρ. Dvojici (C, D), kde $C \in \mathcal{A}$, $D \in \mathcal{B}$ a $D = \alpha_\rho(C)$, budeme říkat *koncept.* Koncept je tedy každá dvojice (C, D), kde $C \subseteq A$, $D \subseteq B$, $D = \alpha_\rho(C)$ a $C = \beta_\rho(D)$. Lze také říci, že koncept je dvojice množin objektů C a množin vlastností D, kde:

1. každý objekt z C má všechny vlastnosti D,
2. objekty z C nemají žádnou společnou vlastnost z $B \backslash D$,
3. všechny objekty A, které mají všechny vlastnosti D, patří do C.

Přiřazení $C \mapsto (C, D)$ je bijekce $\mathcal{A}$ na množinu všech konceptů $\mathcal{K}$. Protože $\mathcal{A}$ je svaz, indukuje tato bijekce svazové operace na $\mathcal{K}$. Můžeme proto mluvit o *svazu konceptů.* Uspořádání ve svazu konceptů je tedy zvoleno tak, že jeden koncept je 'větší' než druhý, jestliže se týká většího množství objektů, tj. jestliže je obecnější.

Vytváření svazů konceptů je jedním z nástrojů *pojmové analýzy.*

5 Kvaziuspořádání a dělitelnost v komutativních monoidech

Buď $S = S(\cdot, \mathbf{1})$ monoid a ať $a \in S$. Definujeme $a^0 = \mathbf{1}$ a $a^n = a^{n-1}a$, je-li $n \in \mathbb{N}$.

5.1 Lemma. *Budiž $S = S(\cdot, \mathbf{1})$ monoid, $a \in S$ a $n, m \in \mathbb{N}_0$. Potom*

(i) $a^n a^m = a^{n+m}$,
(ii) $(a^n)^m = a^{nm}$.

Důkaz. Indukcí dle m. Dokažme nejprve (i), a pak (ii). Pro $m = 0$ oba vztahy zjevně platí. Ať $m > 0$:

(i) $a^n a^m = a^n a^{m-1} a = a^{n+m-1} a = a^{n+m}$,
(ii) $(a^n)^m = (a^n)^{m-1} a^n = a^{n(m-1)} a^n = a^{nm}$.

□

Reflexivní a tranzitivní relace na množině A se nazývá *kvaziuspořádání* A.

Buď $\leq$ kvaziuspořádání množiny A. Pro $a, b \in A$ pišme $a \sim b$, jestliže současně platí $a \leq b$ a $b \leq a$.

5.2 Lemma. *Relace $\sim$ je ekvivalence.*

Důkaz. $\sim$ je zjevně reflexivní a symetrická. Je-li $a \sim b$ a $b \sim c$, je $a \leq b \leq c$ a $c \leq b \leq a$, takže $a \sim c$. □

Relaci $\sim$ nazýváme *jádrem* kvaziuspořádání $\leq$.

5.3 Lemma. *Buď $\sim$ jádro kvaziuspořádání $\leq$ množiny A a ať $\beta, \gamma \in A/\sim$. Jestliže $b_0 \in \beta$, $c_0 \in \gamma$ jsou takové, že $b_0 \leq c_0$, tak $b \leq c$ pro libovolná $b \in \beta$, $c \in \gamma$.*

Důkaz. Je $b \leq b_0 \leq c_0 \leq c$. □

Na $A/\sim$ definujeme relaci $\preccurlyeq$ tak, že $\beta \preccurlyeq \gamma$ platí právě když existují $b \in \beta$ a $c \in \gamma$ taková, že je $b \leq c$. Z 5.3 vyplývá, že v takovém případě je $b \leq c$ pro všechna $b \in \beta$ a $c \in \gamma$. Můžeme tedy vyslovit následující lemma.

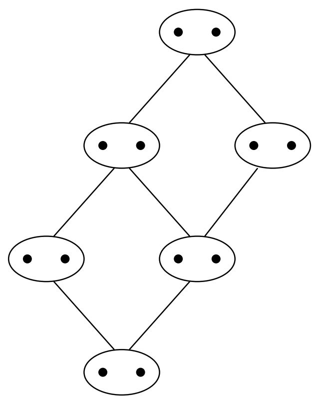
5.4 Lemma. *Buď $b, c \in A$. Pak $[b]_\sim \preccurlyeq [c]_\sim$ právě když $b \leq c$.* □

5.5 Tvrzení. *Relace $\preccurlyeq$ je na $A/\sim$ uspořádáním.*

Důkaz. Důkaz reflexivity a tranzitivity je okamžitý. Ať $\beta, \gamma \in A/\sim$ a $\beta \preccurlyeq \gamma$, $\gamma \preccurlyeq \beta$. Potom pro $b \in \beta$, $c \in \gamma$ máme $b \leq c$, $c \leq b$, takže $b \sim c$ a $\beta = \gamma$. □

Buď $\leq$ kvaziuspořádání A, $\sim$ jeho jádro a $\preccurlyeq$ uspořádání $A/\sim$. Kvaziuspořádání $\leq$ si můžeme představit tak, jakoby vzniklo z uspořádání $\preccurlyeq$ rozpadem jeho prvků do více exemplářů (prvek $\beta \in A/\sim$ se tedy jakoby rozpadá na všechna b obsažená v β, přičemž vztahy dané uspořádáním nijak narušeny nejsou). Pojmy definované pro uspořádání budeme používat i pro kvaziuspořádání, a to tímto způsobem:

Je-li $\mathcal{V}$ nějaká vlastnost prvků svazu, tak řekneme, že prvky a_1, a_2, … z A mají vlastnost $\mathcal{V}$ právě když ji mají prvky $[a_1]_\sim$, $[a_2]_\sim$, … svazu $(A/\sim, \preccurlyeq)$.



Na kvaziuspořádání lze hledět jako na uspořádání, ve kterém se každý bod může rozpadnout na libovolný počet bodů, jež jsou ekvivalentní (tvoří jádro kvaziuspořádání). Vlevo na obrázku má každý blok jádra právě dva body. Obrázek je možné interpretovat například jako diagram vztahů dělitelnosti mezi celočíselnými děliteli čísla 12 (místo 12 lze uvažovat třeba 75, či jiné vhodné číslo tvaru p^2q nebo $-p^2q$, kde p a q jsou různá prvočísla).

Obrázek 5.1: Uspořádání, kvaziuspořádání a dělitelnost

Tak například $a, b \in A$ jsou porovnatelné v $(A, \leq)$, jsou-li $[a]_\sim$ a $[b]_\sim$ porovnatelné v $(A/\sim, \preccurlyeq)$. Podobně definujeme v $(A, \leq)$ dolní a horní závory, infima a suprema, atomy a koatomy. Zápis $b = \inf_\leq B$ ovšem v kvaziuspořádání prvek b neurčuje jednoznačně, jednoznačně je určena pouze třída $[b]_\sim$ (je totiž $[b]_\sim = \inf_\preccurlyeq \{[c]_\sim;\ c \in B\}$).

Protože atomy kvaziuspořádání mají v dalším textu značný význam, uvedeme nyní výslovně podmínky, kdy $a \in A$ je atomem:

(i) A má (alespoň jeden) nejmenší prvek,

(ii) a není nejmenší prvek A,

(iii) je-li $c \in A$ a $c \leq a$, tak buď $c \sim a$, nebo je c nejmenší prvek A.

Kvaziuspořádání $\leq$ množiny A nazveme *noetherovské,* jestliže neexistuje nekonečná posloupnost $a_1, a_2, a_3, \ldots$ prvků z A taková, že pro každé $i \in \mathbb{N}$ je $a_i \geq a_{i+1}$, a současně neplatí $a_i \sim a_{i+1}$.

5.6 Tvrzení. *Buď $\leq$ noetherovské kvaziuspořádání množiny A a ať a je nejmenší prvek A. Potom pro každé $c \in A$ platí, že je buď $c \sim a$, nebo existuje atom $b \in A$ takový, že $b \leq c$.*

Důkaz. Předpokládejme, že není $c \sim a$. Položme $c_1 = c$ a ať $c_1, \ldots, c_n$ jsou takové prvky A, že pro $1 \leq i \leq n$ není $c_i \sim a$, a že pro $1 \leq i \leq n-1$ je $c_i \geq c_{i+1}$ a neplatí $c_i \sim c_{i+1}$. Jestliže c_n není atomem, existuje $c_{n+1} \in A$ takové, že $c_n \geq c_{n+1} \geq a$ a není ani $c_{n+1} \sim c_n$, ani $c_{n+1} \sim a$. Protože $\leq$ je noetherovské, lze takto zkonstruovat jen konečně mnoho členů posloupnosti $c_1, c_2, c_3, \ldots$. Proto musí existovat $n \in \mathbb{N}$, že c_n je atomem. □

Buď nyní $S = S(\cdot, \mathbf{1})$ monoid. Řekneme, že $a \in S$ *dělí* (zleva) $b \in S$, jestliže existuje $c \in S$ takové, že $b = a \cdot c$. Symbolicky píšeme $a|b$ a a nazýváme *dělitelem* b.

5.7 Tvrzení. *Relace dělitelnosti $|$ v monoidu $S = S(\cdot, \mathbf{1})$ je kvaziuspořádáním, přičemž $\mathbf{1}$ je jeho nejmenší prvek.*

Důkaz. Buď $a, b \in S$. Pak $\mathbf{1}|a$, $a|a$, a z $a|b$ a $b|c$ plyne $a|c$. □

Jádro kvaziuspořádání $|$ budeme, jak je obvyklé, značit $||$. Je-li $a||b$, říkáme, že a a b jsou *asociovány.*

Uvědomte si, že z pouhého faktu, že $|$ je kvaziuspořádání, plyne podle 5.3 několik důsledků. Jsou-li $a, b \in S$ asociovány, tak pro každé $c \in S$ například dostáváme $a|c \Leftrightarrow b|c$ a $c|a \Leftrightarrow c|b$.

Buď $B = \{b_1, \ldots, b_k\} \subseteq A$, $k \geq 1$. Místo $b = \inf_| B$ píšeme $b = NSD(b_1, \ldots, b_k)$ a místo $b = \sup_| B$ píšeme $b = NSN(b_1, \ldots, b_k)$. Přitom NSD znamená *největší společný dělitel* a NSN *nejmenší společný násobek.*

V každém kvaziuspořádání je $b \leq c$ právě když $b = \inf_{\leq}\{b, c\}$. Proto platí:

5.8 Lemma. *Buď $b, c \in S$. Pak $b = NSD(b, c)$ právě když $b|c$.*

Z 4.1, 5.4 a 5.5 okamžitě dostáváme:

5.9 Lemma. *Ať $b_1, \ldots, b_{n+1}$, kde $n \in \mathbb{N}$, jsou prvky monoidu S, a ať $c \in S$ je takové, že $c = NSD(b_1, \ldots, b_n)$. Potom $NSD(b_1, \ldots, b_{n+1})$ existuje právě když existuje $NSD(c, b_{n+1})$. Pokud tyto největší společní dělitelé existují, jsou asociovány.*

V S tedy existují největší společní dělitelé, existuje-li $NSD(b, c)$ pro libovolná $b, c \in S$. Totéž lze říci o největších společných násobcích. Z 5.5 plyne, že v S existují největší společní dělitelé a nejmenší společné násobky právě když uspořádaná množina $(S/||, |)$ je svaz.

Prvky $a, b \in S$ se nazývají *nesoudělné,* jestliže $\mathbf{1} = NSD(a, b)$. Dělitel a prvku b se nazývá *vlastní,* jestliže neplatí ani $a||\mathbf{1}$ ani $a||b$.

Budeme se zabývat především komutativními monoidy s krácením. Monoid S je *komutativní,* jestliže $b \cdot c = c \cdot b$ pro libovolná $b, c \in S$. Monoid S je *s krácením,* jestliže pro libovolná $a, b, c \in S$ z $a \cdot b = a \cdot c$ plyne $b = c$ a z $b \cdot a = c \cdot a$ rovněž plyne $b = c$.

Všimněte si, že prvek $a \in S$ je asociován s $\mathbf{1}$ (tedy je v kvaziuspořádání dělením nejmenší) právě když existuje $b \in S$ splňující $ab = \mathbf{1}$ (tedy právě když je a zprava invertibilní). V komutativním případě proto platí, že prvek je asociován s $\mathbf{1}$ právě tehdy, když je invertibilní, a že prvky asociované s $\mathbf{1}$ tvoří podmonoid monoidu $S(\cdot, \mathbf{1})$ (viz 2.17).

5.10 Lemma. *Buď S komutativní monoid s krácením, a ať $a, b \in S$. Potom $a||b$ platí právě když existuje $u \in S$ invertibilní takové, že $b = a \cdot u$.*

Jestliže $a = bc$ pro nějaké $c \in S$, tak nastane jedna z následujících možností:

(i) b i c jsou vlastní dělitelé a,
(ii) b je invertibilní a $a||c$,
(iii) c je invertibilní a $a||b$.

Důkaz. Je-li $a||b$, existují $u, v \in S$ takové, že $a = bu$ a $b = av$. Tudíž $a = avu$, takže $vu = \mathbf{1}$. Jestliže $a = bu$ a u je invertibilní, lze nalézt $v \in S$ takové, že $uv = \mathbf{1}$, takže $b = buv = av$.

Je-li b (nebo c) invertibilní, tak $a||c$ (nebo $a||b$) platí podle prvé části lemmatu. Je-li $a||c$, tak existuje $u \in S$ takové, že $c = au$. Tudíž $a = bc = bau = abu$, a krácením dostáváme $\mathbf{1} = bu$, takže b je invertibilní. Podobně z $a||b$ plyne invertibilita prvku c. □

Ve zbytku této kapitoly bude $S = S(\cdot, \mathbf{1})$ vždy značit komutativní monoid s krácením, $|$ kvaziuspořádání S dělitelností, a $||$ jádro $|$.

Atomy kvaziuspořádání $|$ budeme nazývat *ireducibilními* prvky.

5.11 Tvrzení. *Ať kvaziuspořádání $|$ je noetherovské. Potom každý prvek S, který není invertibilní, lze vyjádřit jako součin ireducibilních prvků.*

Důkaz. Podle 5.6 má každý prvek S, který není invertibilní, ireducibilního dělitele. Ať $a = a_0$ není invertibilní. Budeme konstruovat posloupnost neinvertibilních prvků $a_0, a_1, \dots$ a posloupnost ireducibilních prvků $p_1, p_2, \dots$. Pokud a_i není ireducibilní, položíme $a_i = p_{i+1}a_{i+1}$ tak, aby p_{i+1} byl ireducibilní dělitel a_i. Potom je p_{i+1} vlastní dělitel a_i, takže podle 5.10 je i a_{i+1} vlastní dělitel a_i. Kdyby a_i nebyl ireducibilní pro žádné $i \in \mathbb{N}$, vznikla by nekonečná posloupnost $a_0, a_1, \dots,$ ve které by pro každé $i \in \mathbb{N}$ byl a_i vlastní dělitel a_{i-1}. Protože předpokládáme, že $|$ je noetherovské, existuje $n \in \mathbb{N}$ takové, že a_n je ireducibilní, takže $a = p_1 \cdots p_{n-1}a_n$. □

5.12 Lemma. *Buď $a, b, c \in S$ a ať $d = NSD(a, b)$ a $e = NSD(ac, bc)$. Potom $e||dc$.*

Důkaz. $dc|ac$ a $dc|bc$, takže $dc|e$ a $e = dcu$ pro nějaké $u \in S$. Ať $x, y \in S$ jsou takové, že $ac = ex$ a $bc = ey$. Pak $a = dux$, $b = duy$, a vidíme, že du je společný dělitel a a b. Proto $du|d$, takže $du||d$ a u je invertibilní podle 5.10. Proto $e||dc$. □

5.13 Lemma. *Buď $a, b, c \in S$ a ať a a b jsou nesoudělné. Jestliže $NSD(ac, bc)$ existuje, tak z $a|bc$ plyne $a|c$.*

Důkaz. Podle 5.12 je $c = NSD(a, b)c = NSD(ac, bc)$. Odsud dostáváme $NSD(a, c) = NSD(a, ac, bc) = NSD(a, bc) = a$, takže $a|c$. □

Prvek $p \in S$ se nazývá *prvočinitel,* jestliže není invertibilní, a pro každé $a, b \in S$ z $p|ab$ plyne, že $p|a$ nebo $p|b$.

5.14 Tvrzení. *Každý prvočinitel S je ireducibilní. Jestliže v S existují největší společní dělitelé, tak je každý ireducibilní prvek prvočinitel.*

Důkaz. Buď p prvočinitel, a ať $p = ab$. Z faktu, že p je prvočinitel, plyne $p|a$ (a pak $p||a$) nebo $p|b$ (a pak $p||b$). Ať naopak $p \in S$ je ireducibilní, $p|ab$, p nedělí a a $d = NSD(p, a)$. Protože p nedělí a, není $d||p$. Protože p je ireducibilní a $d|p$, je $d||\mathbf{1}$. Prvky p a a jsou tedy nesoudělné, a podle 5.13 z existence $NSD(pb, ab)$ plyne $p|b$. □

5.15 Lemma. *Ať p je prvočinitel v S. Potom z $p|a_1 \dots a_n$, kde $a_i \in S$, $1 \le i \le n$, plyne, že $p|a_j$ pro některé $1 \le j \le n$.*

Důkaz. Postupujme indukcí dle n. Pro $n = 2$ tvrzení vyplývá z definice prvočinitele. Položme $b = a_2 \dots a_n$. Pak p dělí $a_1 b$, čili p dělí a_1 nebo p dělí $a_2 \dots a_n$. V druhém případě podle indukčního předpokladu existuje $2 \le j \le n$ takové, že $p|a_j$. □

Řekneme, že prvek $a \in S$ má *jednoznačný ireducibilní rozklad*, jestliže:

(i) existují $p_1, \dots, p_r \in S$ ireducibilní a takové, že $a = p_1 \dots p_r$,

(ii) kdykoliv $a = q_1 \dots q_s \in S$, kdy $q_1, \dots, q_s \in S$ jsou ireducibilní, tak $r = s$ a existuje permutace $\sigma \in S_r$, že $p_i || q_{\sigma(i)}$ pro $1 \le i \le r$.

(Jinými slovy ireducibilní rozklad je jednoznačný až na pořadí a $||$ ekvivalenci).

5.16 Tvrzení. *Jestliže v S je každý ireducibilní prvek prvočinitelem, tak jsou ireducibilní rozklady v S jednoznačné.*

Důkaz. Ať $p_1 \dots p_n = q_1 \dots q_m$, kde p_i, $1 \le i \le n$ a q_j, $1 \le j \le m$ jsou ireducibilní, a ať $n \le m$. Z $q_1 | p_1 \dots p_n$ plyne podle 5.15, že můžeme předpokládat, že $q_1 = p_1 u$ pro u invertibilní. Je-li $n = 1$, dostáváme krácením $\mathbf{1} = u q_2 \dots q_m$. Ovšem ireducibilní prvky nedělí $\mathbf{1}$, takže v tomto případě $m = 1$ a $p_1 = q_1$. Postupujme dále indukcí dle $n \ge 2$. Položme $q'_i = q_i$ pro $1 \le i \le n$, $i \ne 2$ a $q'_2 = u p_2$. Pak $p_2 \dots p_n = q'_2 \dots q'_m$, a podle indukčního předpokladu $n = m$ a existuje $\sigma \in S_n$ takové, že $\sigma(1) = 1$ a $p_i || q'_{\sigma(i)}$. □

5.17 Tvrzení. *Ať každý neinvertibilní prvek má v S jednoznačný ireducibilní rozklad. Potom je každý ireducibilní prvek prvočinitel.*

Důkaz. Buď p ireducibilní prvek a ať $p|ab$. Buď $ab = pc$ a ať $c = c_1 \dots c_t$ je ireducibilní rozklad c (je-li c invertibilní, položme $c_1 = c$). Ať $a = a_1 \dots a_r$ a $b = b_1 \dots b_s$ jsou ireducibilní rozklady a a b. Potom $p c_1 \dots c_t = a_1 \dots a_r b_1 \dots b_s$ a z jednoznačnosti ireducibilních rozkladů plyne, že $p || a_i$ pro některé $1 \le i \le r$ (pak $p|a$) nebo $p || b_j$ pro některé $1 \le j \le s$ (pak $p|b$). □

5.18 Věta. *Buď $S = S(\cdot, \mathbf{1})$ komutativní monoid s krácením, ve kterém každý neinvertibilní prvek má jednoznačný ireducibilní rozklad. Ať $P \subseteq S$ je taková množina ireducibilních prvků, že*

(a) kdykoliv $r \in S$ je ireducibilní, tak existuje $p \in P$, že $p || r$,

(b) jsou-li $p_1, p_2 \in P$, tak $p_1 || p_2$ právě pro $p_1 = p_2$.

Označme ještě I množinu všech invertibilních prvků. Potom platí:

(i) *Každý prvek $a \in S$ lze (až na pořadí) jednoznačně vyjádřit ve tvaru $a = up_1^{k_1} \dots p_r^{k_r}$, kde $p_i \in P$, $k_i \in \mathbb{N}$ a $u \in I$ (přitom předpokládáme, že $p_i \neq p_j$ pro $1 \leq i < j \leq r$).*

(ii) *Je-li $a = up_1^{k_1} \dots p_r^{k_r}$ a $b = vp_1^{h_1} \dots p_r^{h_r}$, kde pro $1 \leq i \leq r$ je $p_i \in P$, $k_i \in \mathbb{N}_0$ a $h_i \in \mathbb{N}_0$, přičemž $u, v \in I$ a $p_i \neq p_j$ pro $1 \leq i < j \leq r$, tak $p_1^{\min(k_1,h_1)} \dots p_r^{\min(k_r,h_r)} = NSD(a,b)$. Dále platí, že b dělí a právě když $h_i \leq k_i$ pro $1 \leq i \leq r$, přičemž b je vlastním dělitelem a, jestliže navíc existují $1 \leq s, t \leq r$ taková, že $h_s < k_s$ a $1 \leq h_t$.*

Důkaz. (i) Jestliže a je invertibilní, tak nutně $u = a$, $r = 0$. Pokud a není invertibilní, existuje vyjádření $a = q_1 \dots q_2$, kde q_i, $1 \leq i \leq s$ jsou ireducibilní. Ovšem $q_i = u_i p_i$, kde $p_i \in P$ a $u_i \in I$, takže každý prvek lze jistě zapsat v požadovaném tvaru. Ať $a = up_1^{k_1} \dots p_r^{k_r} = vp_1^{h_1} \dots p_r^{h_r}$, kde $u, v \in I$, $p_i \in P$ a $k_i, h_i \in \mathbb{N}_0$. Ať přitom $p_i \neq p_j$ pro $1 \leq i < j \leq r$. Kdyby bylo například $k_1 < h_1$, tak $up_2^{k_2} \dots p_r^{k_r} = vp_1^{h_1-k_1} p_2^{h_2} \dots p_r^{h_r}$, takže podle 5.7 a 5.15 $p_1 || p_j$ pro některé $2 \leq j \leq r$. To však odporuje předpokládaným vlastnostem množiny P, a proto $k_i = h_i$ pro $1 \leq i \leq r$. Krácením dostáváme $u = v$, čímž je důkaz jednoznačnosti vyjádření uzavřen.
(ii) Ať $vp_1^{h_1} \dots p_r^{h_r} = b$ dělí $a = up_1^{k_1} \dots p_r^{k_r}$ a ať je například $h_1 \geq k_1$. Potom $vp_1^{h_1-k_1} p_2^{h_2} \dots p_r^{h_r}$ dělí $up_2^{k_2} \dots p_r^{k_r}$ a z 5.7 a 5.15 plyne, že $h_1 - k_1 = 0$, čili $h_1 = k_1$. Proto $h_i \leq k_i$ pro $1 \leq i \leq r$. Hledejme nyní $NSD(a,b)$, kde $a = up_1^{k_1} \dots p_r^{k_r}$ a $b = vp_1^{h_1} \dots p_r^{h_r}$. Buď $m_i = \min(k_i, h_i)$ pro $1 \leq i \leq r$. Z předchozího plyne, že $d = p_1^{m_1} \dots p_r^{m_r}$ dělí a i b. Ať c dělí rovněž a i b. Pak $c = wp_1^{c_1} \dots p_r^{c_r}$, kde $w \in I$ a $c_i \leq k_i$ a $c_i \leq h_i$ pro $1 \leq i \leq r$. Proto c dělí d, takže $d = NSD(a,b)$.

Zkoumejme ještě, kdy $b = vp_1^{h_1} \dots p_r^{h_r}$ je vlastní dělitel $a = up_1^{k_1} \dots p_r^{k_r}$. Víme, že pak $h_i \leq k_i$ pro $1 \leq i \leq r$. Je-li $h_i = k_i$ pro všechna $1 \leq i \leq r$, je $a = uv^{-1}b$, takže $a||b$. Naopak, z $a||b$ plyne $h_i = k_i$ pro $1 \leq i \leq r$. Dále platí, že b je invertibilní právě když $h_1 = \cdots = h_r = 0$. Proto je b vlastní dělitel a jedině tehdy, jestliže existují $1 \leq s, t \leq r$ taková, že $h_s < k_s$ a $1 \leq h_t$. □

5.19 Věta. *Buď $S = S(\cdot, \mathbf{1})$ komutativní monoid s krácením. Pak následující podmínky jsou ekvivalentní.*

(i) *V S má každý neinvertibilní prvek jednoznačný ireducibilní rozklad.*

(ii) *V S existují největší společní dělitelé a současně platí, že kvaziuspořádání dělitelností je noetherovské.*

(iii) *Každý ireducibilní prvek S je prvočinitelem a současně platí, že kvaziuspořádání dělitelností je noetherovské.*

Důkaz. (ii) plyne z (i) podle 5.18.
(iii) plyne z (ii) podle 5.14.
(i) plyne z (iii) podle 5.11 a 5.16. □

5.20 Tvrzení. *Ať $S = S(\cdot, \mathbf{1})$ je komutativní monoid s krácením, ve kterém existují největší společné dělitele. Potom existují i nejmenší společné násobky, přičemž jsou-li $b, c, e, f \in S$ takové, že $e = NSD(b, c)$ a $ef = bc$, je $f = NSN(b, c)$. Uspořádání $S/||$ indukované dělitelností je v takovém případě svaz.*

Důkaz. Je-li $e = NSD(b, c)$, tak $e|bc$, takže jistě existuje f takové, že $bc = ef$. Buď nejprve $e = \mathbf{1}$. Pak je třeba ukázat, že $bc = NSN(b, c)$. Ať $b|h$, $c|h$ a $h = bg$. Potom $c|bg$, a podle 5.13 c dělí g. Tudíž $g = cx$, $h = bcx$, $bc|h$. Ať nyní $e \neq \mathbf{1}$, $b = eu$, $c = ev$. Pak $f = euv$ a pro $d = NSD(u, v)$ platí, že $ed|e$. Proto $ed||e$ a $\mathbf{1} = NSD(u, v)$. Ať $b|h$ a $c|h$. Pak $e|h$, a $h = ey$ pro nějaké $y \in S$. Krácením e dostáváme $u|y$, $v|y$, a podle prvé části důkazu platí $uv|y$. Tudíž $f = euv$ dělí $ey = h$. □

6 Grupy a jejich podgrupy

Grupa $G = G(\cdot, {}^{-1}, \mathbf{1})$ je algebra taková, že $\cdot$ je asociativní binární operace, $\mathbf{1}$ je neutrální prvek a pro každý prvek $a \in G$ je a^{-1} prvek inverzní.

Z 2.16 plyne, že v každé grupě G jsou pro všechna $a, b \in G$ splněny identity $(a^{-1})^{-1} = a$ a $(ab)^{-1} = b^{-1}a^{-1}$.

Jestliže v monoidu $S(\cdot, \mathbf{1})$ jsou všechny prvky invertibilní, tak lze definovat na S unární operaci ${}^{-1}$ tak, že pro $a \in S$ je a^{-1} jeho (jednoznačně určený) inverzní prvek. Algebra $S(\cdot, {}^{-1}, \mathbf{1})$ je pak grupa. Rozdíl mezi grupami a monoidy, které jsou tvořeny výhradně invertibilními prvky, je tedy pouze formální, a spočívá v tom, zda přiřazení inverzního prvku je nebo není výslovně uvedeno v seznamu operací příslušné algebry.

Důsledek 2.17 může proto být formulován také tak, že invertibilní prvky libovolného monoidu tvoří grupu. Například invertibilní prvky monoidu $\mathbb{Z}(\cdot, 1)$ jsou 1 a -1, zatímco invertibilní prvky monoidů $\mathbb{Q}(\cdot, 1)$, $\mathbb{R}(\cdot, 1)$ a $\mathbb{C}(\cdot, 1)$ jsou všechna nenulová čísla příslušného číselného oboru. Tyto grupy jsou komutativní, příkladem nekomutativní grupy pro nás bude symetrická grupa S_Ω (binární operací je skládání permutací, unární operací inverzní permutace a nulární operací identická permutace).

Všimněte si, že existenci inverzních prvků v monoidu $S(\cdot, 1)$ lze také formulovat tak, že rovnice $a \cdot x = 1$ a $y \cdot a = 1$ jsou řešitelné pro každé $a \in S$ (viz 2.15). Ovšem pak jsou řešitelné i všechny rovnice tvaru $a \cdot x = b$ a $y \cdot a = b$, neboť lze položit $x = a^{-1}b$ a $y = ba^{-1}$.

Jestliže $G = G(\cdot, {}^{-1}, \mathbf{1})$ je grupa, tak z $ac = bc$ plyne $a = acc^{-1} = bcc^{-1} = b$ a z $ca = cb$ podobně plyne $a = b$. Znamená to, že $G(\cdot, \mathbf{1})$ je monoid s krácením. Rovnice $ax = b$ a $ya = b$ proto mají v grupách vždy právě jedno řešení.

6.1 Lemma. *Buď $G = G(\cdot, {}^{-1}, \mathbf{1})$ a $H = H(\cdot, {}^{-1}, \mathbf{1})$ dvě grupy a $f : G \to H$ zobrazení slučitelné s $\cdot$. Potom je f homomorfismus grup.*

Důkaz. Z $\mathbf{1}_G \cdot \mathbf{1}_G = \mathbf{1}_G$ plyne $f(\mathbf{1}_G) \cdot f(\mathbf{1}_G) = f(\mathbf{1}_G) = f(\mathbf{1}_G) \cdot \mathbf{1}_H$, takže $f(\mathbf{1}_G) = \mathbf{1}_H$. Z $aa^{-1} = \mathbf{1}_G$ plyne $f(a)f(a^{-1}) = f(\mathbf{1}_G) = \mathbf{1}_H$, takže $f(a^{-1}) = (f(a))^{-1}$. □

V grupě $G = G(\cdot, {}^{-1}, \mathbf{1})$ definujeme i záporné mocniny. Je-li $a \in G$, $n \in \mathbb{N}$, tak $a^{-n} = (a^{-1})^n$. Podle 2.16 je zobrazení $a \mapsto a^{-1}$ bijekcí G.

6.2 Lemma. *Pro $a \in G$, $n \in \mathbb{Z}$ je $a^{-n} = (a^n)^{-1}$.*

Důkaz. Pro $n = 0$ zřejmé. Je-li $n = -m < 0$, je třeba ukázat $a^m = (a^{-m})^{-1}$, čemuž je ekvivalentní $(a^m)^{-1} = a^{-m}$. Stačí tedy ověřit, že $a^{-n} = (a^n)^{-1}$ platí pro $n > 0$. Postupujme indukcí, pro $n = 1$ je to zřejmé. Máme $a^{-n-1} = (a^{-1})^{n+1} = (a^{-1})^n \cdot a^{-1} = a^{-n} \cdot a^{-1} = (a^n)^{-1}a^{-1} = (aa^n)^{-1} = (a^{n+1})^{-1}$. □

6.3 Lemma. *Pro $a \in G$, $n, m \in \mathbb{Z}$ je $a^n a^m = a^{n+m}$.*

Důkaz. Je-li $n = 0$ nebo $m = 0$, je vztah zřejmý. Je-li $n > 0$, $m > 0$, použij 5.1. Je-li $n < 0$, $m < 0$, je $a^n a^m = (a^{-n})^{-1}(a^{-m})^{-1} = ((a^{-m})(a^{-n}))^{-1} = (a^{-m-n})^{-1} = a^{n+m}$. Je-li $n > 0 > m$ a $n \geq -m$, tak $a^n a^m = a^{n+m}a^{-m}a^m = a^{n+m}$. Je-li $n > 0 > m$ a $-m > n$, tak $a^n a^m = a^n a^{-n} a^{m+n} = a^{m+n}$. Konečně, je-li $n < 0 < m$, je $a^n a^m = a^n a^{-n} a^{m+n} = a^{n+m}$. □

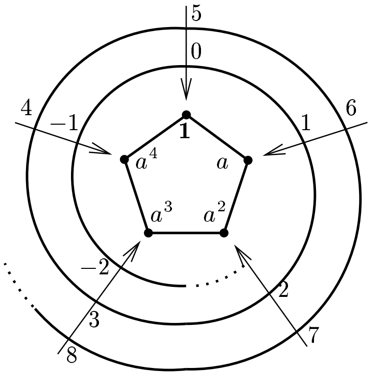
6.4 Lemma. *Pro $a \in G$, $n, m \in \mathbb{Z}$ je $(a^n)^m = a^{nm}$.*

Důkaz. Je-li $n = 0$ nebo $m = 0$, je vztah zřejmý. Pro $n > 0$, $m > 0$ lze použít 5.1. Je-li $m > 0 > n$, je $(a^n)^m = ((a^{-n})^{-1})^m = ((a^{-n})^m)^{-1} = (a^{-nm})^{-1} = a^{nm}$. Je-li $m < 0$, je $(a^n)^m = ((a^n)^{-m})^{-1} = (a^{-nm})^{-1} = a^{nm}$. □

Každá podgrupa generovaná jednoprvkovou množinou se nazývá *cyklická*.

6.5 Tvrzení. *Ať G je grupa a ať $a \in G$ je její prvek. Zobrazení $i \mapsto a^i$ je homomorfismus grup $\mathbb{Z}(+, -, \mathbf{0}) \to G(\cdot, {}^{-1}, \mathbf{1})$. Cyklická podgrupa G, která je generována prvkem a, se shoduje s obrazem tohoto homomorfismu a je rovna $\{a^i; i \in \mathbb{Z}\}$.*

Důkaz. Podle 6.3 a 6.1 je $i \mapsto a^i$ vskutku homomorfismus grup. Jeho obrazem je podle 2.10 nějaká podgrupa G, a ta se rovná $\{a^i; i \in \mathbb{Z}\}$. Protože každá podgrupa G, která obsahuje prvek a, musí obsahovat pro každé $i \in \mathbb{Z}$ prvek a^i, je $\{a^i; i \in \mathbb{Z}\}$ nejmenší podgrupa G, ve které leží prvek a. □



Zobrazení $i \mapsto a^i$ je homomorfismus $\mathbb{Z}(+,-,\mathbf{0})$ na cyklickou grupu generovanou prvkem a. Je-li tato grupa konečného řádu n, má zobrazení charakter namotávání nekonečného provázku na n-úhelník. V našem případě je $n = 5$.

Obrázek 6.1: Obrazy aditivní grupy celých čísel

Řádem podgrupy grupy G se míní její mohutnost. Řád G se obvykle značí $|G|$, zatímco pro vyjádření mohutnosti (obecné) množiny A použijeme značení $\mathrm{card}(A)$. *Řád prvku* $a \in G$ je řád cyklické podgrupy generované a.

Buď H podgrupa grupy G. Definujme relaci $\mathrm{rmod}\, H$ tak, že prvky a, b jsou v této relaci (což zapisujeme $a \equiv b \,\mathrm{rmod}\, H$) právě když $ab^{-1} \in H$.

Podobně pišme $a \equiv b \,\mathrm{lmod}\, H$ právě když $a^{-1}b \in H$.

6.6 Lemma. *Relace* $\mathrm{rmod}\, H$ *a* $\mathrm{lmod}\, H$ *jsou ekvivalence, a pro všechna* $(a,b) \in G$ *platí* $a \equiv b \,\mathrm{rmod}\, H$ *právě když je* $(a^{-1}, b^{-1}) \in \mathrm{lmod}\, H$.

Důkaz. $a \equiv a \,\mathrm{rmod}\, H$, neboť $aa^{-1} = \mathbf{1} \in H$. Je-li $ab^{-1} \in H$, je $(ab^{-1})^{-1} = ba^{-1} \in H$, takže relace $\mathrm{rmod}\, H$ je symetrická. Ať $a \equiv b \,\mathrm{rmod}\, H$ a $b \equiv c \,\mathrm{rmod}\, H$. Pak $ac^{-1} = ab^{-1}bc^{-1} \in H$. Dokázali jsme, že $\mathrm{rmod}\, H$ je ekvivalence. Případ $\mathrm{lmod}\, H$ je podobný. Přitom $ab^{-1} \in H$ lze zapsat, také jako $(a^{-1})^{-1}b^{-1} \in H$, tedy jako $(a^{-1}, b^{-1}) \in \mathrm{lmod}\, H$. □

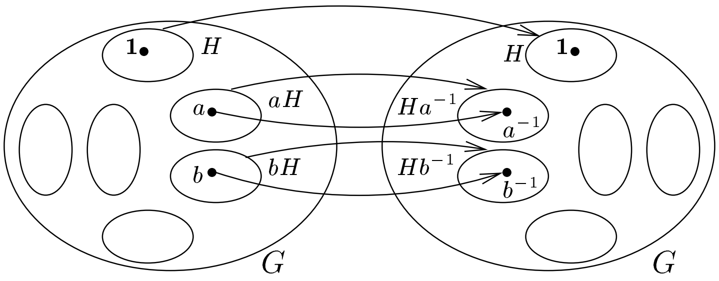
Jsou-li A, B dvě podmnožiny G, tak $A \cdot B = AB$ označuje množinu $\{cd;\ c \in A, d \in B\}$. Pro $a, b \in G$ místo $\{a\}B$, $A\{b\}$ píšeme prostě aB, Ab.

6.7 Lemma. *Buď $a \in G$. Pak $[a]_{\mathrm{rmod}\, H} = Ha$ a $[a]_{\mathrm{lmod}\, H} = aH$. Přitom platí, že* $\mathrm{card}[a]_{\mathrm{rmod}\, H} = |H| = \mathrm{card}[a]_{\mathrm{lmod}\, H}$.

Důkaz. Ať $b \equiv a \,\mathrm{rmod}\, H$. Pak $b = ba^{-1}a \in Ha$. Naopak $ha \equiv a \,\mathrm{rmod}\, H$ pro každé $h \in H$, neboť $haa^{-1} = h \in H$. Je tedy $[a]_{\mathrm{rmod}\, H} = Ha$. Zobrazení $h \mapsto ha$ je bijekce H na Ha, takže $\mathrm{card}(Ha) = \mathrm{card}(H) = |H|$. $\square$

Zobrazení $a \mapsto a^{-1}$ je permutace G, neboť $(a^{-1})^{-1}$ je rovno a. Z 1.11 a 6.6 proto plyne, že zobrazení $[a]_{\mathrm{rmod}\, H} \mapsto [a]_{\mathrm{lmod}\, H}$ je bijekcí $G/\mathrm{rmod}\, H$ a $G/\mathrm{lmod}\, H$. Podle 6.7 lze tuto bijekci vyjádřit ve tvaru $Ha \mapsto a^{-1}H$. Společná mohutnost množin $G/\mathrm{rmod}\, H$ a $G/\mathrm{lmod}\, H$ se nazývá *index* podgrupy H v grupě G a označuje se $|G : H|$.

Množiny Ha se nazývají *pravé rozkladové třídy* H v G. Množiny aH se nazývají *levé rozkladové třídy* H v G. O podgrupě N grupy G řekneme, že je *normální,* jestliže $a^{-1}ha \in N$ pro každé $h \in N$ a $a \in G$.



Zobrazení $a \mapsto a^{-1}$ převádí levé rozkladové třídy H v G na pravé rozkladové třídy H v G. Proto je levých i pravých rozkladových tříd stejně. Jejich počet se nazývá index H v G a značí se $|G : H|$. Všechny rozkladové třídy mají stejnou mohutnost jako H.

Obrázek 6.2: Vztahy levých a pravých rozkladových tříd

6.8 Věta. (Lagrangeova) *Buď G grupa a H její podgrupa. Pak $|G| = |H| \cdot |G : H|$.*

Důkaz. Rozkladových tříd (například levých) je $|G : H|$, a podle 6.7 mají všechny stejnou mohutnost, která je rovna $|H|$. $\square$

6.9 Důsledek. *Buď G konečná grupa a H její podgrupa. Pak $|H|$ dělí $|G|$.*

6.10 Tvrzení. *Buď G grupa a N její podgrupa. Následující podmínky jsou ekvivalentní.*

(i) *N je normální podgrupa G,*
(ii) *$aN = Na$ pro každé $a \in G$,*
(iii) $\operatorname{rmod} N$ *je kongruence G.*

Všechny normální podgrupy grupy G tvoří uzávěrový systém a zobrazení $\rho \mapsto [\mathbf{1}]_\rho$ je izomorfismem svazu kongruencí grupy G a svazu normálních podgrup G.

Dříve než přistoupíme k důkazu 6.10, zmíníme, že podle 6.7 lze 6.10(ii) vyjádřit také jako rovnost ekvivalencí $\operatorname{rmod} N$ a $\operatorname{lmod} N$. V takovém případě je zvykem psát pouze $\operatorname{mod} N$ – přitom vztah $a \equiv b \operatorname{mod} N$ se čte 'a je kongruentní s b modulo N'.

Důkaz. Buď N podgrupa G. (i) $\Rightarrow$ (ii) Buď $a \in G$ a $h \in N$. Pak $ah = aha^{-1}a \in Na$, a naopak $ha = aa^{-1}ha \in aN$.
(ii) $\Rightarrow$ (iii) Buď $a, b, c, d \in G$ a ať $a \equiv c \operatorname{rmod} N$ a $b \equiv d \operatorname{rmod} N$. Pak $ac^{-1} \in N$, $bd^{-1} \in N$, takže $(ab)(cd)^{-1} = abd^{-1}c^{-1} = hac^{-1}$, kde $h \in N$ je dáno vztahem $a(bd^{-1}) = ha$. Tudíž $(ab)(cd)^{-1} \in N$ a $\operatorname{rmod} N$ je slučitelná s binární operací $\cdot$. Protože platí $a \equiv c \operatorname{lmod} N$, je $a^{-1}c = a^{-1}(c^{-1})^{-1} \in N$, takže $a^{-1} \equiv c^{-1} \operatorname{rmod} N$ a $\operatorname{rmod} N$ je slučitelné také s unární operací ${}^{-1}$.
(iii) $\Rightarrow$ (i) Buď $h \in N$, $a \in G$ a ať $\operatorname{rmod} N$ je kongruence. Pak $ha \equiv a \operatorname{rmod} H$, takže $a^{-1}ha \equiv a^{-1}a \operatorname{rmod} H$. Protože $a^{-1}a = \mathbf{1}_G$, tak nutně $a^{-1}ha \in H$.

Nyní vyjasníme vztah normálních podgrup G a kongruencí G. Ať ρ je nějaká kongruence grupy G. Položme $H = [\mathbf{1}]_\rho$. Pak pro $a, b \in H$ z $a \,\rho\, \mathbf{1}$ a $b \,\rho\, \mathbf{1}$ plyne $(a \cdot b) \,\rho\, (\mathbf{1} \cdot \mathbf{1})$ a $a^{-1} \,\rho\, \mathbf{1}^{-1}$. Ovšem $\mathbf{1} = \mathbf{1} \cdot \mathbf{1} = \mathbf{1}^{-1}$, takže je $a \cdot b \in H$ a $a^{-1} \in H$. Pro libovolné $g \in G$ je též $(gag^{-1}) \,\rho\, (g \cdot \mathbf{1} \cdot g^{-1})$, a z $g \cdot \mathbf{1} \cdot g^{-1} = \mathbf{1}$ tedy máme $gag^{-1} \in H$. Dokázali jsme, že H je normální podgrupa G.

Ať η je další kongruence G. Položme $K = [\mathbf{1}]_\eta$ a předpokládejme $H \subseteq K$. Jsou-li $s, t \in G$ takové, že je $s \,\rho\, t$, tak z $t^{-1} \,\rho\, t^{-1}$ máme $st^{-1} \,\rho\, tt^{-1}$, a tedy $st^{-1} \,\rho\, \mathbf{1}$, čili $st^{-1} \in H$. Odsud $st^{-1} \in K$, takže je $st^{-1} \,\eta\, \mathbf{1}$, a to spolu s $t \,\eta\, t$ dává $(st^{-1}t) \,\eta\, (\mathbf{1} \cdot t)$. Protože $st^{-1}t = s$ a $\mathbf{1} \cdot t = t$, vidíme, že $s \,\rho\, t$ implikuje $s \,\eta\, t$, a tedy platí $\rho \subseteq \eta$.

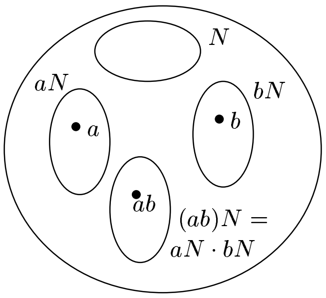
Označme $\mathcal{N}$ systém všech normálních podgrup G a označme $\mathcal{C}$ systém všech kongruencí G. Dokázali jsme, že (1) pro každé $\rho \in \mathcal{C}$ je $[\mathbf{1}]_\rho \in \mathcal{N}$, že (2) pro

$\rho, \eta \in \mathcal{C}$ z $[\mathbf{1}]_\rho \subseteq [\mathbf{1}]_\eta$ plyne $\rho \subseteq \eta$ a že (3) pro každé $N \in \mathcal{N}$ existuje $\rho \in \mathcal{C}$ takové, že $N = [\mathbf{1}]_\rho$ (podle (iii) lze totiž položit $\rho = \operatorname{rmod} N$).

Podle 4.7 je tedy $\mathcal{N}$ uzávěrový systém a $\rho \mapsto [\mathbf{1}]_\rho$ je izomorfismus svazu $\mathcal{C}$ a svazu $\mathcal{N}$. □

6.11 Důsledek. *Každá podgrupa indexu* 2 *je normální.*

Důkaz. Z $|G : H| = 2$ plyne, že G má dvě pravé a dvě levé rozkladové třídy. Protože H je jak levá, tak pravá rozkladová třída, musí být druhá rozkladová třída v obou případech rovna $G \backslash H$. Z 6.10(ii) tudíž dostáváme, že H je normální podgrupa G. □



Každá kongruence ρ grupy G odpovídá nějaké normální podgrupě N. Bloky ρ jsou rovny rozkladovým třídám N v G. Součin dvou tříd je součin prvků „viděných z dálky“ (vidíme pouze třídy, jejich prvky nám splývají).

Obrázek 6.3: Normální podgrupy a kongruence grupy

Je-li $f : G \to H$ homomorfismus grup, tak jádro zobrazení f je kongruence grupy G. To znamená, že existuje právě jedna normální podgrupa N grupy G, pro kterou je $\ker f$ rovno $\bmod N$. Podgrupa N se shoduje s tou rozkladovou třídou ekvivalence $\ker f$, která obsahuje neutrální prvek $\mathbf{1}_G$, takže $N = \{a \in G;\ f(a) = \mathbf{1}_H\}$. Podgrupě N se říká *jádro homomorfismu* f a značí se $\operatorname{Ker} f$.

6.12 Tvrzení. *Buď $f : G \to H$ homomorfismus grup. Pak* $\operatorname{Ker} f$ *je normální podgrupa G, $|G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$ a $|\operatorname{Im} f| = |G : \operatorname{Ker} f|$.*

Důkaz. Protože řád podgrupy $\operatorname{Im} f$ grupy H je roven počtu tříd ekvivalence $\ker f$, a protože $\ker f$ má $|G : \operatorname{Ker} f|$ tříd, dostáváme uvedené vztahy přímo z Lagrangeovy věty. □

Je-li N normální podgrupa grupy G, tak můžeme zkonstruovat kvocientní grupu $G/\bmod N$. Jejími prvky jsou všechny rozkladové třídy N v G. Místo $G/\bmod N$ se většinou píše pouze G/N.

Ve zbytku této kapitoly se budeme především věnovat symetrickým grupám. Tomu, kdo absolvoval standardní kurs lineární algebry, bude značná část uvedené látky pravděpodobně známa.

Je-li f permutace množiny Ω, tak definujeme relaci ρ_f na Ω tak, že $(a,b) \in \rho_f$ právě když $f^m(a) = b$ pro nějaké $m \in \mathbb{Z}$. Relace ρ_f je zjevně reflexivní, symetrická a tranzitivní, takže to je ekvivalence na Ω. Rozkladovým třídám ρ_f říkáme *orbity tranzitivity.* (Uvážíme-li na Ω graf s hranami $\{a, f(a)\}$, tak orbity tranzitivity se shodují s tranzitivními komponentami tohoto grafu.)

Je-li $\Gamma \subseteq \Omega$ orbita tranzitivity permutace f a a je prvek Γ, tak každý prvek Γ musí být možné vyjádřit jako $f^m(a)$, takže Γ je rovno $\{f^m(a);\ m \in \mathbb{Z}\}$.

Ať pro nějaká celá čísla $s > r$ platí $f^s(a) = f^r(a)$. Pak je $f^{s-r}(a) = a$ a $s - r > 0$. Ať $k > 0$ je nejmenší takové, že $f^k(a) = a$. Potom pro $0 \le i < j < k$ je $f^i(a) \ne f^j(a)$ a Γ obsahuje právě prvky $\{a, f(a), \dots, f^{k-1}(a)\}$.

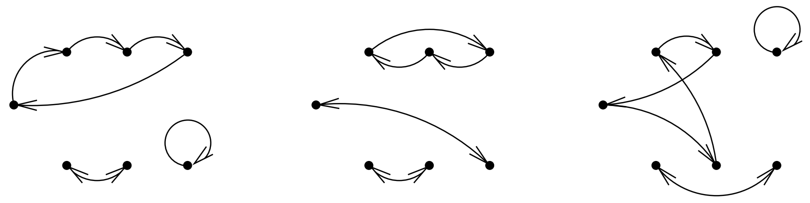
Uvedených vlastností lze použít v případě, kdy množina Ω je konečná, k *cyklickému zápisu* permutace f:

Ať $\Gamma_1, \dots, \Gamma_r$ jsou orbity tranzitivity permutace f, ať $\{a_1, \dots, a_r\}$ je nějaká transversála tohoto rozkladu a ať k_i, $1 \le i \le r$, udává počet prvků orbity Γ_i. Pro $1 \le i \le r$ a $1 \le j \le k_i$ položme $a_{ij} = f^j(a_i)$. Pak permutaci f zapisujeme ve tvaru

$$(a_{11}\ \dots\ a_{1k_1})(a_{21}\ \dots\ a_{2k_2})\ \dots\ (a_{r1}\ \dots a_{rk_r}).$$

Přitom prvek a_i se zřejmě shoduje s a_{ik_i}. Platí $\Gamma_i = \{a_{ij};\ 1 \le j \le k_i\}$, takže každý prvek Ω se v cyklickém zápisu vyskytuje právě jednou. Zápisu lze rozumět tak, že každý prvek, za kterým nenásleduje pravá závorka, se zobrazí do prvku od něj vpravo, a prvek, za kterým následuje pravá závorka, se zobrazí za nejbližší předcházející levou závorku.

Uvažme například permutaci h množiny $\{1,2,3,4,5,6\}$, která je zadaná vztahy $h(1) = 2$, $h(2) = 5$, $h(3) = 6$, $h(4) = 4$, $h(5) = 1$ a $h(6) = 3$. Její cyklický zápis bude $(1\,2\,5)(3\,6)(4)$. Přesný tvar zápisu ovšem záleží na volbě pořadí orbit a na výběru transversály. Při jiném pořadí orbit bude i jiné pořadí částí v závorkách, a při jiné volbě reprezentanta orbity budou prvky uvnitř odpovídajících závorek cyklicky posunuty. Výše uvedenou permutaci je tudíž možno zapsat například také $(2\,5\,1)(4)(6\,3)$. Jednobodové orbity se často ze zápisu vynechávají, a pak se hovoří o *zkráceném cyklickém zápisu.* Jedním z možných zkrácených zápisů permutace h je $(3\,6)(2\,5\,1)$.



2 3 4 1 5 7 6	5 4 2 3 1 7 6	6 3 1 4 7 2 5
(1 2 3 4)(5)(6 7)	(1 5)(2 4 3)(6 7)	(1 6 2 3)(4)(5 7)
(1 2 3 4)(6 7)	(2 4 3)(1 5)(6 7)	(2 3 1 6)(7 5)

V prvém řádku je uvedena permutace $\{1, \ldots, 7\}$ jako posloupnost (i se zobrazí do prvku na i-tém místě posloupnosti). Pak následuje cyklický a zkrácený cyklický zápis téže permutace (danou permutaci lze každým z nich ovšem zapsat více způsoby). Z cyklického zápisu je okamžitě vidět, že prvá a třetí permutace mají stejný typ. Cyklický zápis také více zdůrazňuje, že permutace je zobrazení. Pokud permutace kreslíme (tak jako zde v horní části obrázku), je zvykem šipkou znázornit, jak se daný bod zobrazí. Najděte, jak mají být body v obrázku označeny číslicemi.

Obrázek 6.4: Různé zápisy permutací

Pro každou orbitu tranzitivity Γ_i permutace f definujeme permutaci $f_i \in S_\Omega$ tak, že $f_i(a) = f(a)$ pro $a \in \Gamma_i$ a $f_i(a) = a$ pro $a \notin \Gamma_i$. Je zřejmé, že f je rovno $f_1 \circ f_2 \circ \cdots \circ f_r$ a že permutace f_i vzájemně komutují (tj. pro $1 \leq i \leq j \leq r$ je $f_i \circ f_j = f_j \circ f_i$). Všimněte si, že f_i je identita právě když má orbita Γ_i jediný bod. Zápisu $f = f_1 \circ \cdots \circ f_r$ se říká *úplná dekompozice* permutace f. Protože orbity f jsou jednoznačně určeny, je úplná dekompozice definována až na pořadí také jednoznačně.

Zkrácený cyklický zápis permutace f_i je $(a_{i1} \ldots a_{ik})$. Například výše definovaná permutace $h \in S_6$ má úplnou dekompozici $h_1 \circ h_2 \circ h_3$, kde h_1 má zkrácený cyklický zápis $(1\,2\,5)$, h_2 má zkrácený cyklický zápis $(3\,6)$ a h_3 je identita.

Permutace $f \in S_\Omega$ se zkráceným cyklickým zápisem $(a\,b)$ se nazývají *transpozice.*

6.13 Lemma. *Ať $f \in S_\Omega$ má zkrácený cyklický zápis $(c_1 \dots c_k)$, kde $k \geq 2$. Transpozici $(c_i\,c_{i+1})$, $1 \leq i < k$, označme t_i. Potom platí $f = t_1 \circ \cdots \circ t_{k-1}$.*

Důkaz. Pro $1 \leq i < k$ je, jak lze snadno ověřit indukcí, $t_i \circ t_{k-1}(c_k)$ rovno c_i. Proto $t_1 \circ \cdots \circ t_{k-1}$ zobrazí c_k na c_1.

Transpozice $t_{i+1}, \dots, t_{k-1}$ prvkem c_i nepohnou, takže $t_i \circ \cdots \circ t_{k-1}(c_i)$ je rovno c_{i+1}. Protože transpozice $t_1, \dots, t_{i-1}$ prvkem c_{i+1} nehýbají, tak vskutku platí $t_1 \circ \cdots \circ t_{k_1}(c_i) = c_{i+1}$. □

Každou složku cyklické dekompozice permutace $f \in S_\Omega$ lze tedy vyjádřit jako složení transpozic. Proto platí:

6.14 Důsledek. *Buď Ω konečná množina. Transpozice na množině Ω generují S_Ω.*

V následujícím lemmatu jsou permutace reprezentovány svými zkrácenými cyklickými zápisy. Obě rovnosti lze bezprostředně ověřit.

6.15 Lemma. *Buď $r \geq 0$ a $s \geq 0$ celá čísla. Pak*

$$(a\,b) \circ (a\,c_1 \dots c_r\,b\,d_1 \dots d_s) = (a\,c_1 \dots c_r)(b\,d_1 \dots d_s) \tag{$*$}$$

a

$$(a\,b) \circ (a\,c_1 \dots c_r)(b\,d_1 \dots d_s) = (a\,c_1 \dots c_r\,b\,d_1 \dots d_s) \tag{$**$}$$

Je-li Ω konečná množina o n prvcích, tak S_Ω je izomorfní symetrické grupě S_n. Proto se při vyšetřování permutací konečných množin lze omezit na permutace z S_n.

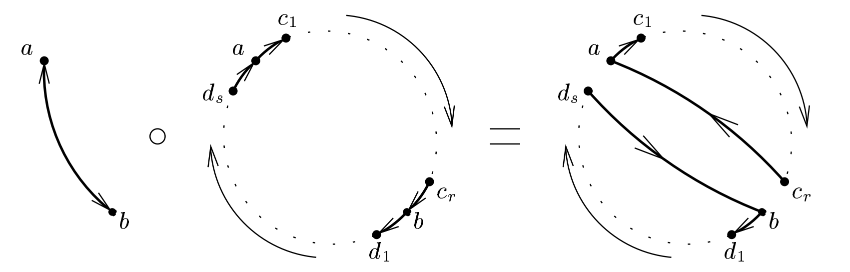
Znaménko $\operatorname{sgn}(f)$ permutace $f \in S_n$ definujeme jako $(-1)^{n-k}$, kde k je počet orbit tranzitivity permutace f. Permutacím se znaménkem 1 se říká *sudé,* ostatním permutacím se říká *liché.* Protože identická permutace má n orbit a transpozice $n-1$ orbit, vidíme, že identita je permutace sudá a transpozice jsou permutace liché.

6.16 Lemma. *Buď $t \in S_n$ transpozice. Pak pro každou permutaci $f \in S_n$ platí*

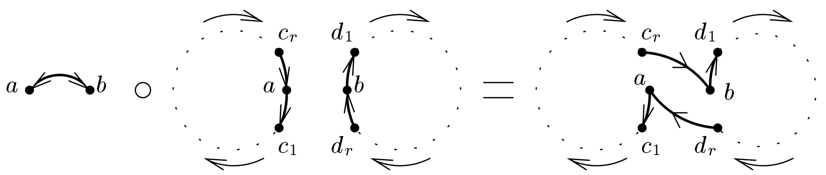
$$\operatorname{sgn}(t \circ f) = -\operatorname{sgn}(f).$$

Důkaz. Ať $(a\,b)$ je zkrácený cyklický zápis transpozice t. Jsou-li a a b v téže orbitě tranzitivity permutace f, tak $t \circ f$ má podle $(*)$ o jednu orbitu více než f. Naopak, leží-li a a b v různých orbitách f, počet orbit podle $(**)$ o jednu klesne. □

6.17 Důsledek. *Buď* $t_1, \ldots, t_k \in S_n$ *transpozice. Pak* $\operatorname{sgn}(t_1 \circ \cdots \circ t_k) = (-1)^k$.



Skládání permutace s transpozicí vždy mění počet cyklů o jeden, a proto má složená permutace opačné znaménko. Na horním obrázku je složení transpozice $t = (a\,b)$ s permutací f v případě, že prvky a a b leží uvnitř jednoho z cyklů f. V dolní části obrázku je naopak znázorněn případ, kdy prvky a a b leží v různých cyklech permutace f. (Permutace f samozřejmě může mít i další cykly, které zde uvedeny nejsou, neboť jejich struktura se složením s t nezmění.)

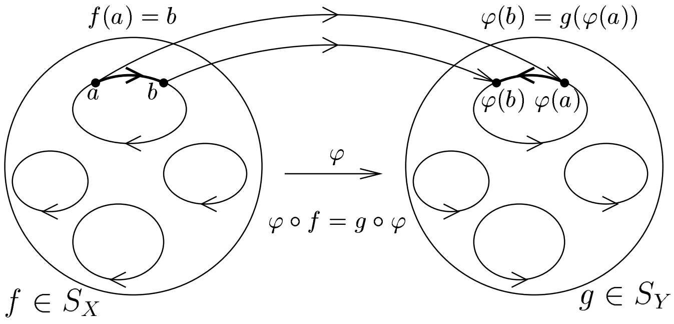


Obrázek 6.5: Skládání transpozice s cykly

6.18 Důsledek. sgn *je homomorfismus* S_n *na* $\{-1, 1\}$.

Důkaz. Buď f a g dvě permutace z S_n. Podle 6.14 lze každou z nich zapsat jako součin transpozic, například ať $f = t_1 \circ \cdots \circ t_r$ a $g = t'_1 \circ \cdots \circ t'_s$. Podle 6.17 je $\operatorname{sgn}(g \circ f) = (-1)^{s+r} = (-1)^s(-1)^r = \operatorname{sgn}(g) \cdot \operatorname{sgn}(f)$. □

Jádro homomorfismu sgn jsou právě všechny sudé permutace. Podgrupě sudých permutací se říká *alternující grupa* a značívá se A_n. Je to normální podgrupa S_n, což plyne například z toho, že je jádrem homomorfismu. Podle 6.12 má A_n v S_n index 2, takže 6.11 nám nabízí jiný důkaz normality A_n v S_n. Grupa S_n má řád $n!$ a grupa A_n má řád $\frac{n!}{2}$.



Ať $\varphi : X \to Y$ je bijekce a $f \in S_X$ permutace X. Definujme $g \in S_Y$ tak, že $g(\varphi(a)) = \varphi(f(a))$. Pak $g = \varphi f \varphi^{-1}$ a vidíme, že g kopíruje strukturu f pomocí φ. Je-li $X = Y$, je f konjugováno s g. Vyjdeme-li naopak od f a g, které mají stejnou strukturu (stejný typ), lze jistě definovat φ tak, aby bylo $g = \varphi f \varphi^{-1}$.

Obrázek 6.6: Konjugovanost permutací stejného typu

O dvou prvcích a, b grupy G řekneme, že jsou *konjugovány* v grupě G, jestliže existuje $g \in G$ takové, že $g^{-1}ag = b$. Protože $g^{-1}ag = b$ je ekvivalentní $gbg^{-1} = a$, je relace 'být konjugován' symetrická. Každý prvek je konjugován sám se sebou, neboť $a^{-1}aa = a$. S $\mathbf{1}$ není konjugován žádný jiný prvek, jelikož $g^{-1}\mathbf{1}g = \mathbf{1}$ pro každé $g \in G$. Z $g^{-1}ag = b$ a $h^{-1}bh = c$ plyne $(gh)^{-1}a(gh) = c$, čímž je ověřena tranzitivita, a vidíme, že relace 'být konjugován' je ekvivalencí.

V obecném případě může být odpověď na otázku, zda dva prvky grupy jsou konjugovány, velmi obtížná. Lineární algebra má tolik významných aplikací právě proto, že tento problém je v grupě regulárních matic nad komplexními čísly dobře algoritmicky zpracován. (Součin dvou regulárních matic je opět regulární matice, jednotková matice je regulární a matice inverzní je rovněž regulární. Proto regulární matice tvoří vzhledem k běžnému násobení matic grupu, a to nad libovolným tělesem, nejen nad komplexními nebo reálnými čísly.) V lineární algebře se ovšem spíše než o konjugaci matic hovoří o jejich podobnosti. To je ovšem jen jiný název pro tentýž pojem, neboť o maticích A a B říkáme, že jsou podobné, jestliže existuje regulární matice C taková, že $A = CBC^{-1}$.

Ukážeme, že v případě symetrických grup lze konjugaci dvou permutací snadno poznat. Ať permutace $f \in S_n$ má orbity r orbit o $k_1, k_2 \dots, k_r$ prvích. Můžeme předpokládat, že platí $k_1 \geq k_2 \geq \dots k_r$. Posloupnosti $(k_1, k_2, \dots, k_r)$ se říká *typ* permutace.

6.19 Tvrzení. *Dvě permutace $f, g \in S_n$ jsou konjugovány právě když mají stejný typ.*

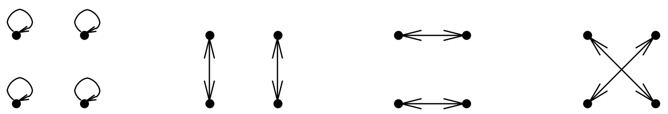
Důkaz. Má-li permutace f cyklický zápis $(a_{11} \ \dots \ a_{1k_1}) \dots (a_{r1} \ \dots \ a_{rk_r})$, tak permutace hfh^{-1} má cyklický rozklad $(h(a_{11}) \ \dots \ h(a_{1k_1})) \dots (h(a_{r1}) \ \dots \ h(a_{rk_r}))$, takže permutace vzájemně konjugované vskutku mají tentýž typ. Naopak, jestliže f a g mají stejný typ $(k_1, \dots, k_r)$, tak pro vhodná a_{ij} a b_{ij} lze f zapsat ve tvaru $(a_{11} \ \dots \ a_{1k_1}) \dots (a_{r1} \ \dots \ a_{rk_r})$ a g lze zapsat ve tvaru $(b_{11} \ \dots \ b_{1k_1}) \dots (b_{r1} \ \dots \ b_{rk_r})$. Označme h zobrazení $a_{ij} \mapsto b_{ij}$. Pak h je permutace z S_n a platí $g = hfh^{-1}$. □

Všimněte si, že podgrupa N grupy G je normální právě tehdy, když s každým prvkem $a \in N$ jsou v N obsaženy i všechny prvky s ním konjugované. Pokud najdeme takovou podgrupu S_n, která obsahuje kromě identické permutace pouze všechny prvky nějakého typu, bude to jistě normální podgrupa grupy S_n.

6.20 Tvrzení. $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1)(2)(3)(4)\}$ *je normální podgrupa* S_4.

Důkaz. Uvedený seznam permutací obsahuje všechny permutace z S_4, které jsou typu $(2, 2)$. Podle předchozího tedy stačí ukázat, že tyto permutace skutečně tvoří podgrupu S_4. Položme $\Omega = \{1, 2, 3, 4\}$ a ať $(a\ b)(c\ d)$ a $(i\ j)(k\ l)$ jsou permutace Ω. Jsou-li shodné, vznikne jejich složením id_Ω. Jsou-li různé, lze předpokládat $a = i$, $c = k$. Pak nutně $b = l$ a $d = j$, přičemž $(a\ d)(c\ b) \circ (a\ b)(c\ d) = (a\ c)(b\ d)$. □

Grupě permutací $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1)(2)(3)(4)\}$ se říká *Kleinova grupa.* Tato grupa je z hlediska grup permutací dosti výjimečná, neboť lze ukázat, že pro $n \neq 4$ a $n \geq 3$ nemá S_n kromě A_n žádnou jinou vlastní normální podgrupu. (Podgrupa H grupy G se nazývá *vlastní,* je-li různá od G a od $\{\mathbf{1}_G\}$.)



Čtyři uvedené permutace tvoří Kleinovu grupu, která je normální podgrupa grupy S_4 a je obsažena v A_4.

Obrázek 6.7: Kleinova grupa

Jsou-li f a g dva automorfismy nějaké algebry $A = \Omega(\alpha_1, \ldots, \alpha_k)$, tak $f \circ g$ i f^{-1} jsou podle 2.9 rovněž automorfismy této algebry. Množina $\mathrm{Aut}(A)$ všech automorfismů algebry A je tudíž podmonoid monoidu $\mathrm{End}(A)$ a současně podgrupa grupy S_Ω. Leží-li dva prvky $a, b \in A$ v téže orbitě nějakého automorfismu $f \in \mathrm{Aut}(A)$, tak jsou ze strukturálního hlediska ekvivalentní. Z tohoto prostého faktu vychází řada úvah jak v matematice samotné, tak i v jejích aplikacích. Přitom grupu automorfismů má smysl vyšetřovat i u jiných objektů než u algeber — například má smysl mluvit o grupě automorfismů nějakého grafu, automatu nebo formálního jazyka.

7 Abelovy grupy, okruhy a tělesa

Grupa $G = G(\cdot, ^{-1}, \mathbf{1})$ se nazývá *komutativní,* jestliže $ab = ba$ pro každé $a, b \in G$. Pro komutativní grupy se často používá aditivní notace – binární operace se značí $+$, unární $-$ a nulární $\mathbf{0}$. Komutativní grupě v aditivní notaci se zpravidla říká grupa *Abelova* (též abelovská).

Abelova grupa $A = A(+, -, \mathbf{0})$ je tedy algebra s jednou binární, jednou unární a jednou nulární operací, která splňuje pro všechna $a, b, c \in A$ tyto identity:

$$a + (b + c) = (a + b) + c, \quad a + b = b + a, \quad a + (-a) = \mathbf{0} \quad \text{a} \quad a + \mathbf{0} = a.$$

Místo $a + (-b)$ píšeme, jak je obvyklé, pouze $a - b$. V aditivní notaci se prvek $-a$ nenazývá prvek inverzní, ale *prvek opačný* (vzhledem k a).

Číselné obory $\mathbb{Z}(+, -, 0)$, $\mathbb{Q}(+, -, 0)$, $\mathbb{R}(+, -, 0)$, $\mathbb{C}(+, -, 0)$ jsou Abelovy grupy. Přitom logaritmus $\lg : \mathbb{R}^+(\cdot, ^{-1}, 1) \to \mathbb{R}(+, -, 0)$ je izomorfismus multiplikativní grupy všech kladných reálných čísel a aditivní grupy všech reálných čísel.

Existují mnohé jiné příklady komutativních grup, zde jmenujme alespoň Kleinovu grupu.

V aditivním zápisu místo a^n píšeme na. Pro Abelovy grupy podle 6.2 – 6.4 tedy platí:

7.1 Lemma. *Buď $A = A(+, -, 0)$ Abelova grupa, $a \in A$ a $n, m \in \mathbb{Z}$. Potom $n(-a) = -(na)$, $(n + m)a = na + ma$ a $(nm)a = n(ma)$.*

Všimněte si, že každá podgrupa Abelovy grupy je normální.

Algebra $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ se nazývá *okruh,* jestliže $R(+, -, \mathbf{0})$ je Abelova grupa, $R(\cdot, \mathbf{1})$ je monoid a pro všechna $a, b, c \in R$ platí

$$a(b + c) = ab + ac \qquad \text{a} \qquad (b + c)a = ba + ca.$$

Tyto identity jsou známy jako (levý a pravý) *distributivní zákon.*

7.2 Lemma. *Buď $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ okruh. Pak pro libovolná $a, b \in R$ je splněno $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$, $(-a)b = -(ab) = a(-b)$ a $(-a)(-b) = ab$.*

Důkaz. $a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0}$, čili $a \cdot \mathbf{0} = \mathbf{0}$. Podobně $\mathbf{0} \cdot a = (\mathbf{0} + \mathbf{0}) \cdot a = \mathbf{0} \cdot a + \mathbf{0} \cdot a$, a tedy $\mathbf{0} \cdot a = \mathbf{0}$. Tudíž $\mathbf{0} = \mathbf{0} \cdot b = (a + (-a)) \cdot b = ab + (-a)b$. Odsud $(-a)b = -(ab)$, a podobně $-(ab) = a(-b)$, takže $ab = -((-a)b) = (-a)(-b)$. $\square$

7.3 Lemma. *Buď $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ okruh. Je-li $\operatorname{card}(R) \geq 2$, tak $\mathbf{0} \neq \mathbf{1}$.*

Důkaz. Ať $a \neq \mathbf{0}$. Pak $a \cdot \mathbf{1} = a \neq \mathbf{0} = a \cdot \mathbf{0}$, takže $\mathbf{1} \neq \mathbf{0}$. $\square$

Okruh se nazývá *triviální,* jestliže má právě jeden prvek. Podle 7.3 jsou v každém netriviálním okruhu $\mathbf{1}$ a $\mathbf{0}$ různé.

Relace dělitelnosti a pojmy invertibilního a inverzního prvku se vztahují, jedná-li se o okruh $R(+, \cdot, -, \mathbf{0}, \mathbf{1})$, k monoidu $R(\cdot, \mathbf{1})$.

Podmnožina I okruhu R se nazývá *ideál* okruhu R, je-li I podgrupa $R(+, -, \mathbf{0})$ a ra i ar patří do I pro každé $r \in R$ a $a \in I$.

7.4 Tvrzení. *Ať R je okruh. Všechny ideály okruhu R tvoří uzávěrový systém a zobrazení $\rho \mapsto [\mathbf{0}]_\rho$ je izomorfismem svazu všech kongruencí okruhu R a svazu všech jeho ideálů. Každá kongruence okruhu R je tedy tvaru $\operatorname{mod} I$, kde I je jednoznačně určený ideál okruhu R a pro $a, b \in R$ platí $a \equiv b \operatorname{mod} I$ právě když $a - b \in I$!*

Důkaz. Je-li ρ kongruence okruhu R, tak ρ je i kongruencí Abelovy grupy, takže podle 6.10 musí platit $\rho = \operatorname{mod} I$, kde $I = [\mathbf{0}]_\rho$. Pro každé $a \in I$ a $r \in R$ pak z $(a, \mathbf{0}) \in \rho$ a $r \cdot \mathbf{0} = \mathbf{0} = \mathbf{0} \cdot r$ plyne $(ra, \mathbf{0}) \in \rho$ a $(ar, \mathbf{0}) \in \rho$, což znamená, že platí $ra \in I$ a $ar \in I$, takže I je opravdu ideál.

Jsou-li ρ a η dvě kongruence R, tak z $I = [\mathbf{0}]_\rho \subseteq [\mathbf{0}]_\eta = J$ samozřejmě plyne $\operatorname{mod} I = \rho \subseteq \eta = \operatorname{mod} J$.

Ke splnění předpokladů lemmatu 4.7 je ještě třeba ukázat, že pro každý ideál I je $\operatorname{mod} I$ skutečně kongruencí R. Podle 6.10 je $\operatorname{mod} I$ slučitelné s operacemi grupy $R(+, -, \mathbf{0})$, takže stačí ověřit slučitelnost s operací $\cdot$. Ať $a \equiv b \operatorname{mod} I$ a $c \equiv d \operatorname{mod} I$ pro nějaká $a, b, c, d \in R$. Potom $b - a \in I$, $d - b \in I$, a proto $cd - ab = c(d - b) + (c - a)b \in I$, takže $ab \equiv cd \operatorname{mod} I$.

Dokončení tvrzení nyní plyne z 4.7. □

Je-li $A \subseteq R$ a $\mathcal{J}$ je uzávěrový systém všech ideálů v R, tak $\operatorname{cl}_{\mathcal{J}}(A)$ nazýváme *ideálem generovaným* množinou A.

Součet $a_1 + a_2 + \cdots + a_n$ prvků okruhu R píšeme též $\sum_{1 \le i \le n} a_i$. Je-li $n = 0$, tak $\sum_{1 \le i \le n} a_i$ klademe rovné $\mathbf{0}$.

7.5 Lemma. *Buď R okruh a $A \subseteq R$. Potom množina $I = \{\sum_{1 \le i \le n} r_i a_i s_i;\ r_i, s_i \in R,\ a_i \in A$ a $n \in \mathbb{N}_0\}$ je rovna ideálu generovanému množinou A.*

Důkaz. I je zjevně uzavřeno na součty, obsahuje $\mathbf{0}$ a podle 7.2 i opačné prvky. Dále $A \subseteq I$ a I musí ležet v každém ideálu, který obsahuje A. Je-li $r \in R$, tak podle distributivních zákonů je $r(\sum r_i a s_i) = \sum r r_i a_i s_i$ a $(\sum r_i a s_i) r = \sum r_i a s_i r$, takže I je vskutku ideál. □

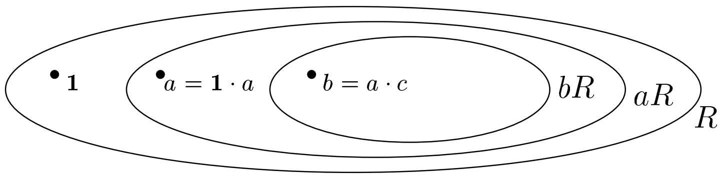
Budeme se zabývat takřka výhradně *komutativními okruhy,* to jest okruhy R, ve kterých $ab = ba$ pro všechna $a, b \in R$. V komutativním okruhu lze ideál I generovaný množinou A vyjádřit jako $\{\sum_{1 \le i \le n} r_i a_i;\ r_i \in R,\ a_i \in A,\ n \in \mathbb{N}_0\}$. Je-li $A = \{a\}$ jednoprvková množina, tak $I = Ra$. Ideál komutativního okruhu R se nazývá *hlavní,* jestliže existuje $a \in R$, že $I = Ra$.

7.6 Lemma. *Buď R komutativní okruh a $a, b \in R$. Pak:*

(i) a je invertibilní právě když $Ra = R$.
(ii) $a|b$ právě když $Ra \supseteq Rb$.
(iii) $a||b$ právě když $Ra = Rb$.

Důkaz. (i) Je-li $Ra = R$, existuje $c \in R$, že $ca = \mathbf{1}$. Je-li c inverzní prvek a, je $r = rca \in Ra$ pro každé $r \in R$.

(ii) Ať $b = ca$ a $r \in R$. Pak $rb = (rc)a$, takže $Rb \subseteq Ra$. Je-li $Ra \supseteq Rb$, je $b \in Ra$, takže $b = ca$ pro nějaké $c \in R$.
(iii) $a||b$ právě když $a|b$ a $b|a$, tedy právě když $Ra \supseteq Rb$ a $Rb \supseteq Ra$, tedy právě když $Ra = Rb$. □



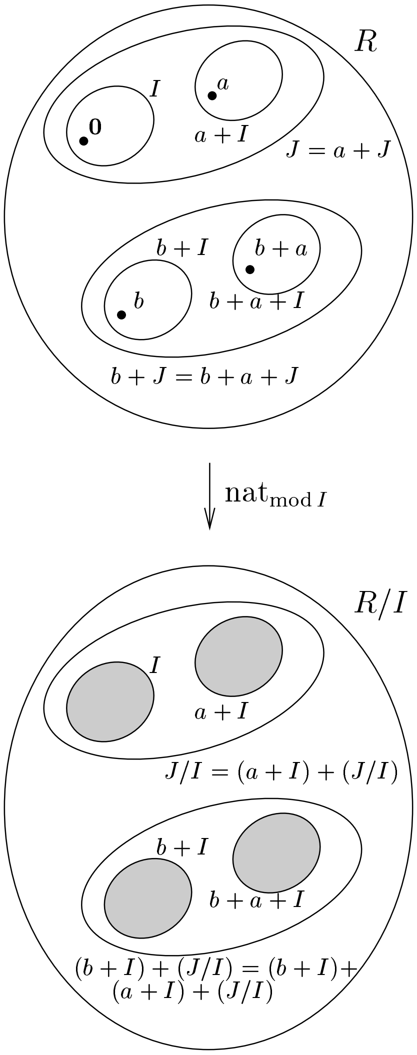
V komutativním okruhu R lze dělitelnost vyjadřovat inkluzemi hlavních ideálů. Vidíme, že $bR \subseteq aR$ právě když a dělí b. Čím je hlavní ideál menší, tím má jeho generátor více dělitelů. Největším hlavním ideálem je celý okruh R. Přitom R je jako hlavní ideál generován právě každým invertibilním prvkem. Invertibilní prvky mají nejméně dělitelů — dělitelem invertibilního prvku je zase jenom invertibilní prvek. Maximální hlavní ideály jsou na tom o něco lépe — jejich generátorem je nějaký ireducibilní prvek, a děliteli jsou kromě prvků invertibilních i prvky s tímto ireducibilním prvkem asociované. Žádný z dělitelů ireducibilního prvku ovšem není jeho vlastní dělitel — však také mezi maximálním hlavním ideálem a celým okruhem R žádný jiný hlavní ideál neleží.

Obrázek 7.1: Dělitelnost a inkluze hlavních ideálů

7.7 Lemma. *Jediné ideály okruhu $\mathbb{Z}(+,\cdot,-,0,1)$ jsou hlavní ideály $m\mathbb{Z}$, $m \in \mathbb{N}_0$.*

Důkaz. Buď I ideál $\mathbb{Z}$ a ať $a \in I$ je nenulové. Protože $-a$ patří také do I, lze předpokládat $a > 0$. Buď m nejmenší možné takové a. Pak $m\mathbb{Z} \subseteq I$, a je-li naopak $n \in I$, lze nalézt $p \in \mathbb{Z}, q \in \mathbb{N}_0$, že $n = mp+q$, $0 \leq q < m$. Protože $q = n - mp \in I$, musí být $q = 0$, a tedy $n \in m\mathbb{Z}$. □

Je-li I ideál okruhu R, tak kvocientní okruh $R/\bmod I$ se, podobně jako v případu grup, označuje R/I. Jeho prvky jsou množiny $r + I$, kde r probíhá R. Označení A/I ve významu $\{a + I;\ a \in A\}$ používáme i pro všechna $A \subseteq R$, kde $a + I \subseteq A$ platí pro všechna $a \in A$.



Jsou-li $I \subseteq J$ ideály okruhu R, tak J se rozkládá na bloky $a+I$ modulo J, kde $a \in J$. Pro každé $b \in R$ je $b+J$ blokem modulo J (čili $b+J \in R/J$), přičemž $b+J$ se – podobně jako J – rozkládá na bloky modulo I. Tyto bloky lze zapisovat $(b+a)+I$, kde $a \in J$.

Při projekci modulo I se z bloků modulo I stávají prvky okruhu R/I. Tyto prvky určují bloky kongruence $\mathrm{mod}\, J/I$ podle své příslušnosti do bloků modulo J v R. Ideál J/I se tedy skládá z těch $a+I \in R/I$, pro která platí $a \in J$, a blok $(b+I)+(J/I)$ modulo J/I se skládá z těch prvků R/I, které lze vyjádřit jako $b+a+I$, $a \in J$.

Obrázek 7.2: Ideály v kvocientním okruhu

7.8 Lemma. *Buď R okruh a ať I je jeho ideál. Pak každý ideál okruhu R/I lze jediným způsobem vyjádřit jako J/I, kde J je ideál R, který obsahuje I.*

Důkaz. Ať ρ označuje kongruenci mod I okruhu R. Podle 3.5 lze každou kongruenci okruhu R/I jednoznačně vyjádřit jako σ/ρ, kde σ je kongruence R, která obsahuje ρ. Podle 7.4 je σ tvaru mod J pro nějaký ideál J okruhu R, přičemž $\sigma \supseteq \rho$ znamená $J \supseteq I$. Množina $[\mathbf{0}_{R/I}]_{\sigma/\rho}$ je, jak lze například nahlédnout z 1.8(i), rovna $\{j + I;\, j \in J\} = J/I$. Ze 7.4 tudíž plyne $\sigma/\rho =$mod J/I. □

Je-li $f : R \to S$ homomorfismus okruhů, tak $\ker f$ je kongruence R a $\operatorname{Ker} f = [0]_{\ker f} = f^{-1}(\mathbf{0}_S)$. Proto platí:

7.9 Lemma. *Buď $f : R \to S$ homomorfismus okruhů. Pak* $\operatorname{Ker} f$ *je ideál R.*

Protože v dalších kapitolách budeme na několika místech používat První větu o izomorfismu (viz kapitola 3) pro okruhy, uvedeme ji zde jako samostatné tvrzení.

7.10 Tvrzení. (První věta o izomorfismu pro okruhy) *Ať $f : R \to S$ je surjektivní homomorfismus okruhů a ať I je jeho jádro. Potom zobrazení $a + I \mapsto f(a)$ je izomorfismus okruhů R/I a S.*

Připomeňme, že okruh R je jednoduchý (ve smyslu definice jednoduché algebry v kapitole 3), jestliže má alespoň dva prvky a nemá vlastní ideály.

Okruh T se nazývá *těleso,* jestliže je každý jeho nenulový prvek invertibilní a jestliže T obsahuje alespoň dva prvky. Množina $T\backslash\{\mathbf{0}\}$ se značívá T^*. Protože T^* je monoid, který obsahuje pouze invertibilní prvky, lze T^* považovat za grupu (hovoříme o *multiplikativní grupě* tělesa T). Inverzní prvky v T^* značíme a^{-1}.

7.11 Lemma. *Těleso neobsahuje vlastní ideály.*

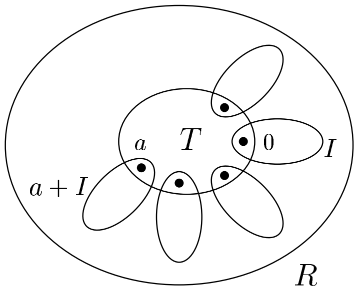
Důkaz. Ať I je ideál tělesa T a ať $a \in I$, $a \neq \mathbf{0}$. Pak $aa^{-1} = \mathbf{1} \in I$, takže $I = T$. □

7.12 Důsledek. *Buďte T těleso a R netriviální okruh. Pak každý homomorfismus $f : T \to R$ je injektivní.*

Důkaz. $f(\mathbf{1}_T) = \mathbf{1}_R \neq \mathbf{0}_R$. Proto je $\operatorname{Ker} f \neq T$, takže podle 7.11 je $\operatorname{Ker} f = \{\mathbf{0}_T\}$. Tudíž $\ker f = \mathrm{id}_T$ a tedy f je injektivní. □

V případě komutativních okruhů platí k 7.11 i opačné tvrzení:

7.13 Tvrzení. *Buď R netriviální komutativní okruh. Pak R je těleso právě když R neobsahuje vlastní ideály.*



V okruhu R je T transversálou kongruence modulo I právě když $T + I = R$ a dále pro všechna $a, b \in T$ z $a - b \in I$ plyne $a = b$.
Na T je indukována struktura okruhu izomorfního s R/I (viz obr. 2.7). Je-li R komutativní a I maximální, dostaneme tak strukturu komutativního tělesa.

Obrázek 7.3: Okruh indukovaný transversálou

Důkaz. Ať R obsahuje pouze nevlastní ideály a $a \in R$ je nenulové. Podle 7.6(i) je a invertibilní. □

Podle 7.13 je komutativní okruh těleso právě když je to okruh jednoduchý. Aplikací 3.6 tudíž dostáváme

7.14 Tvrzení. *Buď I ideál komutativního okruhu R. Pak R/I je těleso právě když I je maximální ideál R.*

Podokruh tělesa T, který je sám tělesem, se nazývá *podtěleso*.

7.15 Tvrzení. *Množina všech podtěles tělesa T tvoří uzávěrový systém.*

Důkaz. Ať $\mathcal{R}$ označuje uzávěrový systém podokruhů T, $\mathcal{G}$ uzávěrový systém podgrup T^* a ať $\mathcal{G}' = \{G \cup \{\mathbf{0}\};\ G \in \mathcal{G}\}$. K je podtěleso T právě když $K \in \mathcal{G}' \cap \mathcal{R}$, takže lze použít 1.2. □

Je-li T těleso, $\mathcal{T}$ uzávěrový systém jeho podtěles a $A \subseteq T$, tak $\mathrm{cl}_{\mathcal{T}}(A)$ se nazývá *podtěleso generované* množinou A. Nejmenší podtěleso (je generované prázdnou množinou) se nazývá *prvotěleso*. Podobně v okruhu R existuje nejmenší podokruh, který je generován prázdnou množinou v uzávěrovém systému všech podokruhů okruhu R. Je zřejmé, že tento nejmenší podokruh vždy obsahuje $\mathbf{0}_R$ a $\mathbf{1}_R$. Přitom prvotěleso tělesa T samozřejmě vždy tento nejmenší podokruh musí obsahovat.

Buď $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ okruh, $a \in R$ a $n \in \mathbb{Z}$. Protože $R(+, -, \mathbf{0})$ je Abelova grupa, lze použít zápisu $n{\cdot}a$. Vyjasníme nyní vztah tohoto multiplikativního zápisu a multiplikativního zápisu daného okruhovou operací $\cdot$. Abychom oba zápisy od sebe výrazněji oddělili, budeme někdy místo $n \cdot a$ psát $n \times a$. Je tedy například $3 \times a = a + a + a$ a $(-2) \times a = (-a) + (-a)$.

Následující lemma je speciální příklad tvrzení 6.5. Lze ho také ověřit přímo pomocí 7.1.

7.16 Lemma. *Buď R okruh a $a \in R$. Zobrazení $n \mapsto n \times a$ je pro každé $a \in R$ homomorfismus $\mathbb{Z}(+,-,0)$ do $R(+,-,\mathbf{0})$.*

7.17 Lemma. *Buď R okruh, $a \in R$ a $n \in \mathbb{Z}$. Pak $n \times a = (n \times \mathbf{1}_R) \cdot a$.*

Důkaz. Podle 7.16 platí $-(n \times a) = (-n) \times a$, takže $((-n) \times \mathbf{1})a = (-(n \times \mathbf{1}))a = -((n \times \mathbf{1})a)$, a proto stačí podat důkaz pro $n \geq 0$. Pro $n \leq 1$ vztah zjevně platí, postupujme tedy indukcí a ať $n > 1$. Pak $n \times a = ((n-1) \times a) + a = ((n-1) \times \mathbf{1}) \cdot a + (1 \times \mathbf{1}) \cdot a = (((n-1) \times \mathbf{1}) + (1 \times \mathbf{1})) \cdot a = (n \times \mathbf{1}) \cdot a$. □

7.18 Tvrzení. *Ať R je okruh a $\varphi : \mathbb{Z} \to R$, $\varphi(n) = n \times \mathbf{1}$ pro každé $n \in \mathbb{Z}$. Potom φ je homomorfismus okruhů a $\operatorname{Im} \varphi$ je nejmenší podokruh okruhu R.*

Důkaz. Buď $n, m \in \mathbb{Z}$. Podle 7.16 je $\varphi(n+m) = \varphi(n) + \varphi(m)$ a podle 7.1 a 7.17 je $\varphi(nm) = (nm) \times \mathbf{1} = n \times (m \times \mathbf{1}) = (n \times \mathbf{1}) \cdot (m \times \mathbf{1}) = \varphi(n)\varphi(m)$. $\operatorname{Im} \varphi$ musí obsahovat provookruh P. Protože $\mathbf{1} \in P$ a $-\mathbf{1} \in P$, je $n \times \mathbf{1} \in P$ pro každé $n \in \mathbb{Z}$, takže také $\operatorname{Im} \varphi \subseteq P$. □

Jádro $\operatorname{Ker} \varphi$ zobrazení $\varphi : \mathbb{Z} \to R$ je podle 7.7 hlavní ideál $m\mathbb{Z}$ pro nějaké $m \in \mathbb{N}_0$, přičemž podle 7.6(iii) je m určeno jednoznačně. Číslo m nazýváme *charakteristikou* okruhu R. Z definice zobrazení φ okamžitě plyne:

7.19 Tvrzení. *Buď R okruh charakteristiky p a ať $n \in \mathbb{Z}$. Potom $n \times \mathbf{1}_R = \mathbf{0}_R$ právě když p dělí n.*

Je-li R okruh charakteristiky p a $p > 0$, tak p je nejmenší kladné číslo takové, že $p \times \mathbf{1}_R = \mathbf{0}$. (Z této vlastnosti se často vychází při definici charakteristiky okruhu.)

Důkaz následujícího tvrzení lze vynechat, neboť je zcela stejný jako důkaz běžné binomické věty.

7.20 Lemma. *Buď R komutativní okruh $a, b \in R$ a $n \in \mathbb{N}$. Pak*

$$(a+b)^n = \sum_{0 \leq i \leq n} \binom{n}{i} \times a^i b^{n-i}.$$

Je-li $G(\cdot, ^{-1}, \mathbf{1})$ *grupa a* a *její prvek, je podle 6.5 zobrazení*

$$\mathbb{Z} \to G, \quad n \mapsto a^n$$

homomorfismem $\mathbb{Z}(+, -, \mathbf{0})$ *na cyklickou pogrupu* G *generovanou* a. *V případě Abelovy grupy* $A(+, -, \mathbf{0})$ *má tento homomorfismus tvar*

$$\mathbb{Z} \to A, \quad n \mapsto n \cdot a.$$

Stejný homomorfismus konstruujeme i pro okruh $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$. *Zde iterované sčítání* $n \cdot a$ *píšeme také jako* $n \times a$. *Díky distributivitě lze iteraci omezit na jednotkový prvek okruhu* R. *Zobrazení*

$$\mathbb{Z} \to R, \quad n \mapsto n \times a = (n \times \mathbf{1}_R) \cdot a$$

je homomorfismus grup $\mathbb{Z}(+, -, \mathbf{0}) \to R(+, -, \mathbf{0})$. *Položíme-li* $a = \mathbf{1}$, *dostaneme homomorfismus okruhů*

$$\mathbb{Z} \to R, \quad n \mapsto n \times \mathbf{1}_R.$$

Obrázek 7.4: Iterované sčítání a násobení

7.21 Důsledek. *Buď* R *komutativní okruh charakteristiky* $p > 0$ *a ať* p *je prvočíslo. Potom zobrazení* $a \mapsto a^p$ *je endomorfismus okruhu* R.

Důkaz. Buď $a, b \in R$. Jistě $(ab)^p = a^p b^p$. Dále platí $(a + b)^p = a^p + b^p + \sum_{1 \le i < p} \binom{p}{i} \times a^i b^{p-i}$, přičemž p dělí $\binom{p}{i}$ pro každé $1 \le i < p$, takže podle 7.19 je $\sum_{1 \le i < p} \binom{p}{i} \times a^i b^{p-i} = \mathbf{0}$. □

Endomorfismu $a \mapsto a^p$ říkáme *Frobeniův endomorfismus*. Označíme-li ho φ, tak $\varphi^k(a) = a^{p^k}$ pro každé $a \in R$ a $k \ge 0$. Pro popis konečných těles má velký význam následující tvrzení.

7.22 Tvrzení. *Nechť* T *je komutativní těleso prvočíselné charakteristiky* p. *Pak* $\{a \in T;\, a^{p^k} = a\}$ *je pro každé* $k \ge 0$ *podtělesem* T.

Ať $R = R(+, -, \cdot, \mathbf{0}, \mathbf{1})$ je okruh. Pokud při opakovaném sčítání

$$\mathbf{1}, \mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}, \ldots$$

nikdy v okruhu R neobdržíme nulu, tedy pokud $n \times \mathbf{1} \neq \mathbf{0}$ pro všechna $n \in \mathbb{N}$, tak bude mít R charakteristiku nula. Pokud $n \times \mathbf{1} = \mathbf{0}$ pro nějaké $n \in \mathbb{N}$, tak R má charakteristiku n, jestliže n je nejmenší přirozené číslo, pro které je $n \times \mathbf{1} = \mathbf{0}$.
Předpokládejme, že R má charakteristiku $n > 0$. Pak je víceméně zřejmé, že $m \times \mathbf{1} = 0$ právě když n dělí m a že pro $m = a \cdot n + b$, kde $a, m, b \in \mathbb{Z}$, platí $m \times \mathbf{1} = b \times \mathbf{1}$. Tuto skutečnost lze vyjádřit také tak, že $n\mathbb{Z}$ je jádrem okruhového homomorfismu

$$\mathbb{Z} \to R, \quad a \mapsto a \times \mathbf{1}.$$

Obrázek 7.5: Charakteristika okruhu

Důkaz. Ať φ značí Frobeniův endomorfismus. Položme $f = \varphi^k$ a $g = \mathrm{id}_T$. Z 3.2 plyne, že $\{a \in T; a^{p^k} = a\}$ je podokruh tělesa T. Je-li $a^{p^k} = a$, tak platí $(a^{-1})^{p^k} = (a^{p^k})^{-1} = a^{-1}$, takže tento podokruh je uzavřený na inverzní prvky, a je tedy podtělesem tělesa T. $\square$

Na závěr této kapitoly uvedeme několik často používaných pojmů. Podmnožina I okruhu $R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ se nazývá *levý ideál,* je-li I podgrupa $R(+, -, \mathbf{0})$ a $ra \in I$ pro každé $a \in I$, $r \in R$. Podobně se definuje *pravý ideál.*

Abelova grupa $M(+, -, \mathbf{0})$ se nazývá *modul* nad okruhem R, jestliže pro každé $r \in R$, $a \in M$ je definován skalární násobek $r \cdot a$ tak, že

$$r(a+b) = ra + rb, \quad (r+s)a = ra + sa, \quad r(sa) = (rs)a \quad \text{a} \quad \mathbf{1} \cdot a = a$$

pro všechna $a, b \in M$ a $r, s \in R$. Modulům nad tělesem se říká vektorové prostory.

Polookruh je algebra $R(+, \cdot, \mathbf{0}, \mathbf{1})$ taková, že $R(+, \mathbf{0})$ je komutativní monoid, $R(\cdot, \mathbf{1})$ monoid a platí distributivní zákony $a(b+c) = ab + ac$ a $(b+c)a = ba + ca$.

V reálných číslech je $(a+b)^2 \neq a^2+b^2$ kdekoliv je $2ab \neq 0$, tedy kdykoliv je a či b nenulové. Podobně v každém komutativním okruhu $R = R(+,\cdot,-,\mathbf{0},\mathbf{1})$ je $(a+b)^2 = a^2+b^2+2\times ab$ různé do a^2+b^2, pokud $2\times ab = (\mathbf{1}+\mathbf{1})ab \neq 0$, což pro a,b nenulová v případě, že jejich součin je rovněž nenulový, nastane právě když R je charakteristiky různé od dvou. Je-li R netriviální a char $R \neq 2$, *tak taková a a b lze vždy nalézt, a proto v takovém případě není zobrazení $a \mapsto a^2$ slučitelné se sčítáním. Naopak, je-li R komutativní okruh charakteristiky dvě, je $(a+b)^2 = a^2+b^2$ splněno vždy. Protože vztahy $(ab)^2 = a^2b^2$, $(-a)^2 = -a^2$, $1^2 = 1$ a $0^2 = 0$ jsou pak rovněž splněny, vidíme, v takovém případě je $a \mapsto a^2$ endomorfismem okruhu R. Tomuto endomorfismu se říká Frobeniův. Podobným postupem se ukazuje, že $a \mapsto a^p$ je endomorfismus i v případě, kdy R má charakteristiku p, přičemž p je liché prvočíslo (viz 7.21). I zde mluvíme Frobeniově endomorfismu.*

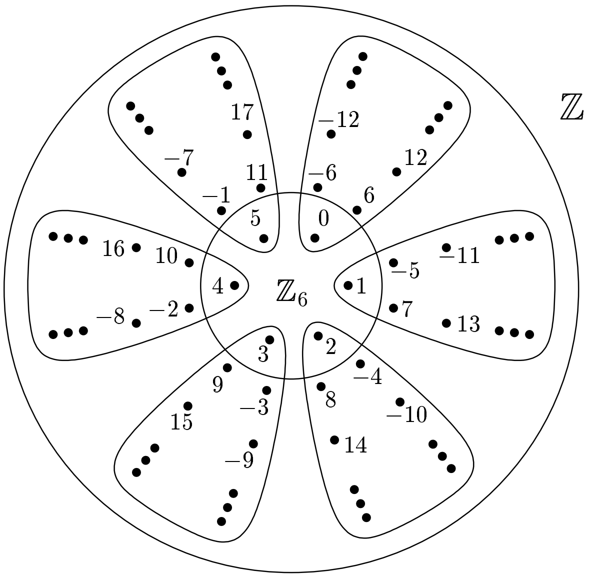
Obrázek 7.6: Frobeniův endomorfismus

8 Cyklické grupy

Podle 7.7 jsou jedinými ideály okruhu $\mathbb{Z}$ ideály $n\mathbb{Z}$, kde $n \in \mathbb{N}_0$. Je-li $n = 0$, běží o triviální (nulový) ideál. Předpokládejme dále, že n je kladné celé číslo. Pro $a, b \in \mathbb{Z}$ budeme místo $a \equiv b \bmod n\mathbb{Z}$ psát, jak je obvyklé, pouze $a \equiv b \bmod n$. Rovněž označení $[a]_{\mathrm{mod}\, n}$ bloku ekvivalence $\bmod n$ budeme zkracovat, a to na $[a]_n$. Ze 7.4 plyne, že $\bmod n$ je kongruence okruhu $\mathbb{Z}$ a že $a \equiv b \bmod n$ platí právě když n dělí $a-b$.

Ke každému $a \in \mathbb{Z}$ existují jediná $q, r \in \mathbb{Z}$ taková, že $a = qn + r$ a $0 \leq r < n$. Přitom $a \equiv r \bmod n$. Pro zápis celočíselného podílu q a zbytku r si lze vypůjčit označení používané v některých programovacích jazycích, a psát q jako $a \operatorname{div} n$ a r jako $a \bmod n$.

Je-li $0 \leq r_1 < r_2 < n$, tak nikdy není $r_1 \equiv r_2 \bmod n$. Pro $a, b \in \mathbb{Z}$ je $a \equiv b \bmod n$ splněno právě když $a \bmod n$ je rovno $b \bmod n$. Z toho vyplývá, že množina $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ je transversálou kongruence $\bmod n$, a můžeme ji tedy považovat za okruh touto transversálou indukovaný (ve smyslu definice uvedené v kapitole 2). Struktura okruhu $\mathbb{Z}_n$ je tedy určena tak, aby zobrazení $i \mapsto [i]_n$ bylo izomorfismem okruhů $\mathbb{Z}_n$ a $\mathbb{Z}/n\mathbb{Z}$. To znamená, že jsou-li a, b prvky $\mathbb{Z}_n$, tak jejich součet je roven $(a+b) \bmod n$ a jejich součin je roven $(a \cdot b) \bmod n$.



Okruh $\mathbb{Z}_6$ je okruh určený transversálou $\{0,1,2,3,4,5\}$ kongruence mod 6 *okruhu $\mathbb{Z}$ (viz obr. 7.3). Podobně je definován okruh $\mathbb{Z}_n$ pro každé $n \geq 2$.*

Obrázek 8.1: Definice okruhu $\mathbb{Z}_6$

Tradičně se transversála ekvivalence mod n nazývá *úplná soustava zbytků modulo n*. Množina $\{0,1,\ldots,n-1\}$ samozřejmě není jediná úplná soustava zbytků – často se například pracuje s množinou $\{i \in \mathbb{Z};\, -\frac{n}{2} \leq i < \frac{n}{2}\}$.

Pišme na chvíli opět $m \times a$ ve významu $a + \cdots + a$, resp. $(-a) + \cdots + (-a)$. Je-li prvek a obsažen v nějaké podgrupě, je jistě i $m \times a$ obsaženo v téže podgrupě, a to pro každé $m \in \mathbb{Z}$.

V okruhu $\mathbb{Z}(+,\cdot,-,0,1)$ je $a \times b$ rovno $a \cdot b$ pro všechna $a, b \in \mathbb{Z}$. Proto je každá podgrupa $\mathbb{Z}(+,-,0)$ ideálem okruhu $\mathbb{Z}(+,\cdot,-,0,1)$, takže podle 7.7 jsou všechny podgrupy $\mathbb{Z}(+,-,0)$ tvaru $k\mathbb{Z}$, $k \geq 0$.

Podobnou úvahu lze provést i pro okruhy $\mathbb{Z}_n(+,\cdot,-,0,1)$, $n \geq 1$. Podle 7.17 pro $a, b \in \mathbb{Z}_n$ máme $a \cdot b = (a \times 1) \cdot b = a \times b$, takže i zde je každá podgrupa $\mathbb{Z}_n(+,-,0)$ ideálem $\mathbb{Z}_n(+,\cdot,-,0,1)$. (Je-li totiž A podgrupa, a prvek A a b libovolný prvek $\mathbb{Z}_n$, tak $b \cdot a = b \times a$ patří do A, takže A je vskutku ideál.)

Z předchozí kapitoly (Lemma 7.8) víme, že ideály $\mathbb{Z}/n\mathbb{Z}$ jsou tvaru $I/n\mathbb{Z}$, kde $I \supseteq n\mathbb{Z}$ je ideál $\mathbb{Z}$. Ze 7.7 a 7.6 plyne, že I musí být rovno $k\mathbb{Z}$, kde k dělí n. Rozkladová třída $[a]_n$ patří do $k\mathbb{Z}/n\mathbb{Z}$ právě když a patří do $k\mathbb{Z}$, tedy právě když k dělí a.

Každý kladný dělitel k čísla n tedy určuje ideál $k\mathbb{Z}/n\mathbb{Z}$ okruhu $\mathbb{Z}/n\mathbb{Z}$, přičemž tento ideál je tvořen všemi bloky $[a]_n$, kde k dělí $a \in \mathbb{Z}$. Kvocientní algebra $\mathbb{Z}/n\mathbb{Z}$ má právě n prvků, a to $[0]_n$, $[1]_n, \ldots$ $[n-1]_n$, neboť množina $\{0, 1, \ldots, n-1\}$ je transversálou kongruence $\bmod n$. Položme $r = \frac{n}{k}$. Pak $k\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [k]_n, [2k]_n, \ldots, [(r-1)k]_n\}$, takže z izomorfismu $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$, $i \mapsto [i]_n$, dostáváme, že každý ideál $\mathbb{Z}_n$ je určen nějakým kladným dělitelem k čísla n a je roven $k\mathbb{Z}_n = \{0, k, 2k, \ldots, (r-1)k\}$, kde $r = \frac{n}{k}$.

Provedené úvahy shrneme do následujícího tvrzení (prvá část tvrzení se týká $\mathbb{Z}$, druhá $\mathbb{Z}_n$).

8.1 Tvrzení. *Pro $A \subseteq \mathbb{Z}$ je ekvivalentní:*

(i) *A je podgrupa $\mathbb{Z}(+,-,0)$,*

(ii) *A je ideál $\mathbb{Z}(+,\cdot,-,0,1)$,*

(iii) *$A = k\mathbb{Z}$ pro nějaké $k \geq 0$.*

Přitom číslo $k \geq 0$ je určeno jednoznačně a pro $k > 0$ je zobrazení $i \mapsto ki$ izomorfismus Abelových grup $\mathbb{Z}$ a $k\mathbb{Z}$.

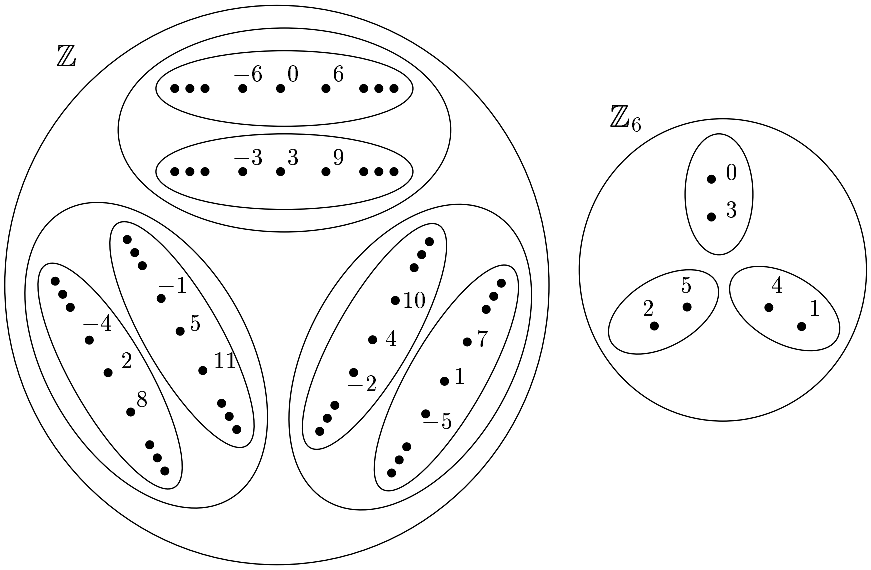
Pro $A \subseteq \mathbb{Z}_n$, $n \geq 1$, je ekvivalentní:

(i) *A je podgrupa $\mathbb{Z}_n(+,-,0)$,*

(ii) *A je ideál $\mathbb{Z}_n(+,\cdot,-,0,1)$,*

(iii) *$A = k\mathbb{Z}_n$, kde $k \in \mathbb{Z}_n$ dělí n nebo je rovno 0.*

Přitom číslo k je určeno jednoznačně a pro $k > 0$, $n = kr$, je zobrazení $i \mapsto ki$ izomorfismus Abelových grup $\mathbb{Z}_r$ a $k\mathbb{Z}_n$.



V okruhu $\mathbb{Z}$ je šest zbytkových tříd (bloků) modulo 6 a tři zbytkové třídy modulo 3. Protože je $6\mathbb{Z} \subseteq 3\mathbb{Z}$, musí se zbytkové třídy modulo 3 skládat ze zbytkových tříd modulo 6. To je na obrázku vyznačeno. Ideál $3\mathbb{Z}$ okruhu $\mathbb{Z}$ určuje ideál $3\mathbb{Z}/6\mathbb{Z}$ okruhu $\mathbb{Z}/6\mathbb{Z}$. (Viz též obr. 7.2, kde $J = 3\mathbb{Z}$ a $I = 6\mathbb{Z}$). Z izomorfismu $\mathbb{Z}_6$ a $\mathbb{Z}/6\mathbb{Z}$ tedy plyne, že $\{0, 3\}$ je ideál $\mathbb{Z}_6$ a že $\{1, 4\}$ a $\{2, 5\}$ jsou rozkladové třídy určené tímto ideálem.
Podobně lze určit ideály v $\mathbb{Z}_n$ pro každé $n \geq 2$. Ve všech případech je samozřejmě lze snadno určit i přímo. Námi zvolený postup je však založen na skutečnosti, že při faktorizaci se určité strukturní vlastnosti přenášejí na kvocient, takže je možné výpočty provádět pouze v původní nefaktorizované struktuře. Tento princip nalézá uplatnění v mnoha jiných situacích, často daleko složitějších než právě popsaná.

Obrázek 8.2: Ideály v okruhu $\mathbb{Z}_6$

Důkaz. Ekvivalence podmínek (i-iii) byla vyložena výše. Zobrazení $\mathbb{Z} \to k\mathbb{Z}$, $i \mapsto ki$, je zjevně homomorfismus grup (je to zvláštní případ 7.16), který je pro $k > 0$ injektivní a surjektivní, takže to je izomorfismus.

Ideál $A = k\mathbb{Z}_n$, kde $k > 0$ dělí n, je tvořen prvky 0, k, $2k$, $\dots$, $(r-1)k$. Přitom číslo k je nejmenší nenulové číslo v A, a proto je určeno jednoznačně. Zobrazení $i \mapsto ki$ je bijekce $\mathbb{Z}_r$ na $k\mathbb{Z}_n$, takže stačí ukázat, že jde o homomorfismus. Zvolme $i, j \in \mathbb{Z}_r$ a položme $a = (i + j) \bmod r$. (Prvek $a \in \mathbb{Z}_r$ je tedy výsledek operace $+$ v $\mathbb{Z}_r$ a platí $a \equiv i + j \bmod r$.) Podle 6.1 je třeba ověřit, že $ka \equiv ki + kj \bmod n$. Ze vztahu $a \equiv i + j \bmod r$ však plyne $ka \equiv k(i + j) \bmod kr$ a kr je rovno n. $\square$

Každá z podgrup $k\mathbb{Z}_n$ Abelovy grupy $\mathbb{Z}_n(+, -, 0)$, kde $k \geq 1$ dělí $n \in \mathbb{N}$ a $k < n$, je cyklická, neboť každý její prvek lze získat iterovaným sčítáním prvku $k \in \mathbb{Z}_n$. (Cyklická je samozřejmě i triviální podgrupa $0\mathbb{Z}_n$.) Prvek k je tedy generátorem cyklické grupy $k\mathbb{Z}_n$. Speciálně je 1 generátor cyklické grupy $\mathbb{Z}_n$.

Z následujícího vyplyne, že každá nekonečná cyklická grupa je izomorfní Abelově grupě $\mathbb{Z}(+, -0)$ a každá konečná cyklická grupa je izomorfní Abelově grupě $\mathbb{Z}_n(+, -, 0)$, kde n je rovné řádu dané cyklické grupy. Porozumět struktuře cyklických grup tedy znamená porozumět struktuře grup $\mathbb{Z}(+, -, 0)$ a $\mathbb{Z}_n(+, -, 0)$.

8.2 Tvrzení. *Buď $G = G(\cdot, {}^{-1}, \mathbf{1})$ grupa a ať H je podgrupa G generovaná prvkem $a \in G$. Je-li H nekonečná, je $i \mapsto a^i$ izomorfismus $\mathbb{Z}(+, -, 0)$ a $H(\cdot, {}^{-1}, \mathbf{1})$. Je-li a konečného řádu n, je $i \mapsto a^i$ izomorfismus $\mathbb{Z}_n(+, -, 0)$ a $H(\cdot, {}^{-1}, \mathbf{1})$.*

Důkaz. Označme f zobrazení $\mathbb{Z} \to H$, $i \mapsto a^i$. Podle 6.5 je toto zobrazení homomorfismus grupy $\mathbb{Z}(+, -, 0)$ na grupu $H(\cdot, {}^{-1}, \mathbf{1})$. Jádro tohoto homomorfismu je nějaká podgrupa $\mathbb{Z}$, takže podle prvé části Tvrzení 8.1 máme $\operatorname{Ker} f = m\mathbb{Z}$ pro nějaké $m \in \mathbb{N}_0$. Homomorfismus f je surjektivní, a proto f bude izomorfismus tehdy a jen tehdy, když bude injektivní, tedy když bude $\operatorname{Ker} f = 0$, což znamená $m = 0$. Podle Prvé věty o izomorfismu 3.9 je zobrazení $g : \mathbb{Z}/m\mathbb{Z} \to H$, $[i]_m \mapsto a^i$, izomorfismem grup. Grupa $\mathbb{Z}/m\mathbb{Z}$ je konečná právě když $m > 0$, a pak je řádu m. Protože izomorfní grupy jsou stejného řádu, vidíme, že $m = 0$ právě tehdy, když grupa H je nekonečná. Předpokládejme $m > 0$. Pak $n = m$ a $(g \circ h)(i) = a^i$ pro každé $i \in \mathbb{Z}_n$, kde h označuje izomorfismus $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$, $i \mapsto [i]_n$. $\square$

Z 8.1 a 8.2 okamžitě obdržíme:

8.3 Důsledek. *Každá podgrupa cyklické grupy je cyklická.*

8.4 Důsledek. *Je-li G cyklická podgrupa konečného řádu n, tak pro každé $m|n$ obsahuje G právě jednu podgrupu řádu m.*

Všimněte si, že je-li a prvek grupy G konečného řádu, je jeho řád roven nejmenšímu $i \in \mathbb{N}$ takovému, že $a^i = 1$.

8.5 Tvrzení. *Buď $n \in \mathbb{N}$. Pak $i \mapsto ai$, kde a probíhá $\mathbb{Z}_n$, jsou právě všechny endomorfismy cyklické grupy $\mathbb{Z}_n(+,-,0)$. Je-li ψ některý z těchto endomorfismů, pak jeho obraz $\operatorname{Im}\psi = a\mathbb{Z}_n$ je roven té podgrupě $\mathbb{Z}_n(+,-,0)$, která je generována prvkem a.*

Důkaz. Skutečnost, že zobrazení $i \mapsto ai$ je endormorfismus grupy $\mathbb{Z}_n(+,-,0)$, vyplývá z toho, že $\mathbb{Z}_n$ je okruh (distributivní zákon není nic jiného než vyjádření slučitelnosti násobení daným prvkem – zde prvkem a – s binární operací sčítání). Je-li $\psi \in \operatorname{End}(\mathbb{Z}_n(+,-,0))$ a $\psi(1) = a$, tak se ψ shoduje s endomorfismem $i \mapsto ai$ na generátoru 1 Abelovy grupy $\mathbb{Z}_n(+,-,0)$. Podle 3.3 se však pak oba endomorfismy musí rovnat.

Obrazem endomorfismu ψ je hlavní ideál okruhu $\mathbb{Z}_n$ generovaný prvkem a. Protože $\operatorname{Im}\psi$ je podgrupa grupy $\mathbb{Z}_n(+,-,0)$, která obsahuje prvek a, zbývá dokázat, že každý prvek $\operatorname{Im}\psi$ leží v cyklické grupě generované prvkem a. To ovšem plyne (stejně jako v úvahách před 8.1) z toho, že podle 7.17 pro každé $i \in \mathbb{Z}_n$ platí $ia = (i \times 1)a = i \times a$. □

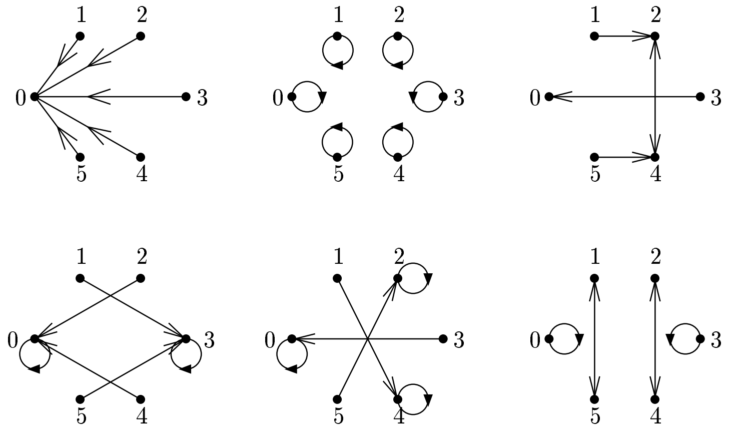
8.6 Tvrzení. *Buď $n \in \mathbb{N}$, $a \in \mathbb{Z}_n$, $a \neq 0$ a $k = NSD(a,n)$. Ať A je podgrupa $\mathbb{Z}_n(+,-,0)$ generovaná a. Pak $A = k\mathbb{Z}_n$.*

Důkaz. Číslo k dělí n a generuje cyklickou podgrupu $k\mathbb{Z}_n$ grupy $\mathbb{Z}_n(+,-,0)$. Protože $a \in \mathbb{Z}_n$ je nenulový násobek k, musí být jednak $k < n$, jednak $a \in k\mathbb{Z}_n$. Protože $k\mathbb{Z}_n$ je podgrupa, která obsahuje prvek a, musí obsahovat i cyklickou podgrupu generovanou tímto prvkem, takže platí $k\mathbb{Z}_n \supseteq A$.

Podgrupa A grupy $\mathbb{Z}_n(+,-,0)$ musí být jednou z podgrup této grupy, jež jsou popsány v 8.1. Protože a je nenulové, je A netriviální, a proto existuje dělitel d čísla n takový, že $A = d\mathbb{Z}_n$ a $0 < d < n$. Protože a je prvek A, musí d dělit a, takže d dělí i $k = NSD(a,n)$. Tudíž $A = d\mathbb{Z}_n \supseteq k\mathbb{Z}_n$, a tedy $A = k\mathbb{Z}_n$. □

8.7 Důsledek. *Buď $n > 1$. Pro $a \in \mathbb{Z}_n$ jsou následující podmínky ekvivalentní:*

(i) *a generuje $\mathbb{Z}_n(+,-,0)$,*
(ii) *a je invertibilní prvek okruhu $\mathbb{Z}_n$,*
(iii) *$NSD(a,n) = 1$,*
(iv) *endomorfismus $i \mapsto ai$ Abelovy grupy $\mathbb{Z}_n(+,-,0)$ je její automorfismus.*



Na obrázku je všech šest endomorfismů Abelovy grupy $\mathbb{Z}_6(+,-,0)$. Každý z nich je jednoznačně určen obrazem některého generátoru grupy $\mathbb{Z}_6(+,-,0)$. Protože jediné prvky, které lze zvolit za generátor, jsou prvky 1 *a* 5*, má tato grupa přesně dva automorfismy. Prvky* 1 *a* 5 *lze také charakterizovat jako invertibilní prvky okruhu $\mathbb{Z}_6$, anebo jako ty prvky $\mathbb{Z}_6$, které jsou nesoudělné s číslem* 6*.*

Obrázek 8.3: Endomorfismy Abelovy grupy $\mathbb{Z}_6$

Důkaz. Podle 7.6(i) je a invertibilní v $\mathbb{Z}_n$ právě když $a\mathbb{Z}_n = \mathbb{Z}_n$, což podle 8.5 lze vyjádřit tak, že endomorfismu $\psi : i \mapsto ai$ je surjektivní, nebo tak, že podgrupa $\mathbb{Z}_n(+,-,0)$ generovaná prvkem a je rovna $\mathbb{Z}_n$. Podle 8.6 prvek a generuje $\mathbb{Z}_n$ právě když je a s n nesoudělné. Zbývá si uvědomit, že $\mathbb{Z}_n$ je konečná množina, takže $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ je surjektivní právě když je bijektivní. $\square$

8.8 Důsledek. *Buď $n \in \mathbb{N}$. Okruh $\mathbb{Z}_n$ je těleso právě když je n prvočíslo.*

Buď $n > 1$. Počet invertibilních prvků okruhu $\mathbb{Z}_n$ je podle 8.7 roven počtu přirozených čísel k, $0 < k < n$, jež jsou nesoudělná s n. Tento počet se označuje $\varphi(n)$, přičemž φ se nazývá *Eulerova funkce.* Pro p prvočíslo je zjevně $\varphi(p) = p-1$. Hodnotu $\varphi(1)$ definujeme jako 1.

Buď $n, m \in \mathbb{N}$ nesoudělná. Pak pro každé $a \in \mathbb{N}_0$ platí, že

(1) $NSD(a, n) = NSD(a \bmod n, n)$,
(2) $NSD(a, nm) = 1$ právě když $NSD(a, n) = 1$ a $NSD(a, m) = 1$.

8.9 Lemma. *Ať $n, m \in \mathbb{N}$ jsou nesoudělná čísla. Pak $\varphi(nm) = \varphi(n)\varphi(m)$.*

Důkaz. Uvažme zobrazení $a \mapsto (a \bmod n, a \bmod m)$ ze $\mathbb{Z}_{nm}$ do $\mathbb{Z}_n \times \mathbb{Z}_m$. Ať $a, b \in \mathbb{Z}_{nm}$ se zobrazí stejně a $b \geq a$. Pak $(b - a) \bmod n = 0 = (b - a) \bmod m$, takže nm dělí $b - a$, a tudíž $a = b$. Zobrazení je injektivní, a proto i bijektivní.

Prvek a okruhu $\mathbb{Z}_{nm}$ je v tomto okruhu invertibilní právě když $NSD(a, nm) = 1$, což podle (2) nastane právě když $NSD(a, n) = 1$ a $NSD(a, m) = 1$. Tyto podmínky jsou ovšem podle (1) ekvivalentní požadavkům $NSD(a \bmod n, n) = 1$ a $NSD(a \bmod m, m) = 1$. Vidíme, že a je v okruhu $\mathbb{Z}_{nm}$ invertibilní tehdy a jen tehdy, je-li současně $a \bmod n$ invertibilní prvek okruhu $\mathbb{Z}_n$ a $a \bmod m$ invertibilní prvek okruhu $\mathbb{Z}_m$.

Protože zobrazení $a \mapsto (a \bmod n, a \bmod m)$ je bijekcí množin $\mathbb{Z}_{nm}$ a $\mathbb{Z}_n \times \mathbb{Z}_m$, je počet invertibilních prvků okruhu $\mathbb{Z}_{nm}$ nutně roven počtu dvojic $(u, v) \in \mathbb{Z}_n \times \mathbb{Z}_m$ takových, že u je invertibilní v $\mathbb{Z}_n$ a v je invertibilní v $\mathbb{Z}_m$. Takových dvojic je ovšem právě $\varphi(n)\varphi(m)$. $\square$

8.10 Lemma. *$\varphi(p^r) = (p - 1)p^{r-1}$ pro každé prvočíslo p a každé $r \in \mathbb{N}$.*

Důkaz. Prvek $a \in \mathbb{Z}_{p^r}$ není invertibilní právě když $p|a$. V okruhu $\mathbb{Z}_{p^r}$ je právě p^{r-1} násobků p. $\square$

Z 8.9 a 8.10 okamžitě plyne:

8.11 Tvrzení. *Ať $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} \in \mathbb{N}$, kde $p_1 < p_2 < \dots < p_k$ jsou prvočísla a $r_i > 0$, $1 \leq i \leq k$. Pak $\varphi(n) = p_1^{r_1-1} p_2^{r_2-1} \dots p_k^{r_k-1}(p_1 - 1)(p_2 - 1) \dots (p_k - 1)$.*

Invertibilní prvky $\mathbb{Z}_n$, $n > 1$, tvoří multiplikativní grupu. Tato grupa má řád $\varphi(n)$. Řád každého jejího prvku proto musí dělit $\varphi(n)$ a $a^{\varphi(n)} = 1$ pro každé a z této grupy. Dokázali jsme:

8.12 Tvrzení. *Ať $a, n \in \mathbb{N}$ jsou nesoudělná čísla. Pak $a^{\varphi(n)} \equiv 1 \bmod n$.*

(Pro n prvočíslo je vztah 8.12 známý jako Malá Fermatova věta.)

8.13 Tvrzení. *Buď $n \in \mathbb{N}$. Jestliže $k|n$, tak $\mathbb{Z}_n(+, -, 0)$ obsahuje právě $\varphi(k)$ prvků řádu k.*

Důkaz. Ať $r = \frac{n}{k}$. Podle 8.1 a 8.6 má $a \in \mathbb{Z}_n$ řád k právě když a generuje $r\mathbb{Z}_n \simeq \mathbb{Z}_k$. Ovšem $\mathbb{Z}_k$ má právě $\varphi(k)$ generátorů. $\square$

8.14 Důsledek. *Buď $n \in \mathbb{N}$. Pak $n = \sum_{k|n} \varphi(k)$.*

9 Podílová tělesa

O prvku a komutativního okruhu $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ řekneme, že je *dělitel nuly,* jestliže $a \neq \mathbf{0}$ a existuje $b \in R$, $b \neq \mathbf{0}$ takové, že $ab = \mathbf{0}$. Okruh $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$, který je komutativní, není triviální a je bez dělitelů nuly, se nazývá *obor integrity.* Všimněte si, že netriviální komutativní okruh R je oborem integrity právě když $R^{\#} = R \setminus \{\mathbf{0}\}$ je podmonoid $R(\cdot, \mathbf{1})$.

Je-li R obor integrity a $a, b, c \in R^{\#}$, tak z $ab = ac$ plyne $a(b - c) = 0$, odkud $b - c = 0$, a tedy $b = c$. To znamená, že $R^{\#}(\cdot, \mathbf{1})$ je komutativní monoid s krácením.

9.1 Lemma. *Konečný obor integrity je komutativní těleso.*

Důkaz. Ať R je konečný obor integrity a $a \in R$, $a \neq \mathbf{0}$. Zobrazení $x \mapsto ax$ je injektivní, a protože R je konečné, je to permutace R. Proto existuje $b \in R$, že $ab = \mathbf{1}$. $\square$

Buď nyní $R = R(+, \cdot, -, 0, 1)$ obor integrity. Na množině $F = R \times R^{\#}$ budeme definovat algebru $F = F(+, \cdot, -, \mathbf{0}, \mathbf{1})$. Pro přehlednost budeme uspořádané dvojice $(a, b) \in R \times R^{\#} = F$ zapisovat $\frac{a}{b}$. Buď $a, c \in R$ a $b, d \in R^{\#}$. Definujeme

$$
\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \qquad & \mathbf{0} &= \frac{0}{1}, \qquad & -\frac{a}{b} &= \frac{-a}{b}, \\
\frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd} \qquad \text{a} & \mathbf{1} &= \frac{1}{1}.
\end{aligned}
$$

9.2 Lemma. *$F(+, \mathbf{0})$ a $F(\cdot, \mathbf{1})$ jsou komutativní monidy.*

Důkaz. Komutativita je zřejmá přímo z definice. Buď $a \in R$ a $b \in R^{\#}$. Pak $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}$ a $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$, takže $\mathbf{0}$ a $\mathbf{1}$ jsou neutrálními prvky. Pro násobení asociativita plyne rovněž okamžitě z definice. Ověřme asociativitu sčítání. Buď $a, c, e \in R$ a $b, d, f \in R^{\#}$. Pak $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf} = \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$. $\square$

Na F definujeme ekvivalenci $\sim$ tak, že $\frac{a}{b} \sim \frac{c}{d}$ právě když $ad = bc$.

9.3 Lemma. $\sim$ *je kongruence* F.

Důkaz. Nejprve je třeba ověřit, že $\sim$ je vskutku ekvivalence. Reflexivita a symetrie je jasná. Ať $\frac{a}{b} \sim \frac{c}{d}$ a $\frac{c}{d} \sim \frac{e}{f}$. Pak $acf = ade = bce$, čili $af = be$. Nyní je třeba ověřit, že $\sim$ je kongruence. Buď $\frac{a}{b} \sim \frac{c}{d}$. Pak jistě $-\frac{a}{b} \sim -\frac{c}{d}$. Buď ještě $\frac{e}{f} \sim \frac{g}{h}$. Pak $\frac{a}{b} + \frac{e}{f} = \frac{af+be}{bf}$ a $\frac{c}{d} + \frac{g}{h} = \frac{ch+dg}{dh}$. Ovšem $afdh + bedh = adfh + bdeh = bcfh + bdfg = bfch + bfdg$, takže $\frac{a}{b} + \frac{e}{f} \sim \frac{c}{d} + \frac{g}{h}$. Podobně z $adeh = bcfg$ plyne $\frac{a}{b} \cdot \frac{e}{f} \sim \frac{c}{d} \cdot \frac{g}{h}$. □

Očividně platí

9.4 Lemma. *Buď* $a \in R^{\#}$. *Potom* $\frac{0}{a} \sim \mathbf{0}$ *a* $\frac{a}{a} \sim \mathbf{1}$.

9.5 Lemma. $F/\sim$ *je komutativní okruh.*

Důkaz. Podle 9.2 stačí ověřit, že unární minus poskytuje opačné prvky, a ověřit distributivní zákon. Buď $a \in R$ a $b \in R^{\#}$. Pak $\frac{a}{b} + (-\frac{a}{b}) = \frac{ab-ab}{bb} \sim \mathbf{0}$. Buď ještě $c, e \in R$ a $d, f \in R^{\#}$. Pak $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} \sim \frac{abcf+abde}{bbdf} = \frac{ac}{bd} + \frac{ae}{bf}$. □

Z 9.4 dostáváme:

9.6 Lemma. *Buď* $a, b \in R^{\#}$. *Pak* $\frac{a}{b} \cdot \frac{b}{a} \sim \mathbf{1}$.

Formálně správnější (ale méně přehledné) by bylo v předchozím textu místo $\frac{a}{b}$ psát (a, b). Představme si, že jsme zvolili tento formálně korektnější postup a nyní definujeme $\frac{a}{b} = [(a, b)]_{\sim}$. Čili od této chvíle zlomkem $\frac{a}{b}$ označujeme celou ekvivalenční třídu $\sim$. (Koneckonců v tomto významu zlomky používáme běžně – to, že $\frac{2}{6} = \frac{1}{3}$ překvapí jen málokoho.)

Z 9.5 a 9.6 plyne, že $T = F/\sim$ je komutativní těleso. Toto těleso se nazývá *podílovým tělesem* oboru integrity R. Je tvořeno všemi zlomky $\frac{a}{b}$, kde $a \in R$ a $b \in R^{\#}$.

9.7 Tvrzení. *Buď* R *obor integrity a* T *jeho podílové těleso. Definujme zobrazení* $\sigma : R \to T$ *tak, že* $\sigma(r) = \frac{r}{1}$. *Platí, že* σ *je injektivní homomorfismus okruhů.*

Důkaz. Zjevně $\frac{r}{1} + \frac{s}{1} = \frac{r+s}{1}$, $\frac{r}{1} \cdot \frac{s}{1} = \frac{rs}{1}$ atd., takže σ je homomorfismus. Přitom $\frac{r}{1} = \frac{s}{1}$ právě když $r = s$, a proto je σ prosté. □

Ztotožníme-li, jak je obvyklé, každý prvek $r \in R$ s $\frac{r}{1} \in T$, plyne z 9.7, že můžeme R považovat za podmnožinu (a tedy podokruh) T.

9.8 Tvrzení. *Ať je R obor integrity, U těleso a $\sigma : R \to U$ injektivní homomorfismus okruhů. Potom existuje jediný homomorfismus $\psi : T \to U$, kde T je podílové těleso R, takový, že $\psi(a) = \sigma(a)$ pro každé $a \in R$. Přitom $\psi(\frac{a}{b}) = \sigma(a)(\sigma(b))^{-1}$ pro všechna $\frac{a}{b} \in T$.*

Důkaz. Protože $\mathbf{1} = \psi(\mathbf{1}) = \psi(\frac{b}{b}) = \psi(b \cdot \frac{1}{b}) = \sigma(b) \cdot \psi(\frac{1}{b})$, musí být $\psi(\frac{1}{b}) = (\sigma(b))^{-1}$ pro každé $b \in R^{\#}$, a tedy $\psi(\frac{a}{b}) = \psi(a \cdot \frac{1}{b}) = \sigma(a)(\sigma(b)^{-1})$ pro každé $\frac{a}{b} \in T$. Pro libovolná $a, b \in R^{\#}$ je $\sigma(a)\sigma(b) = \sigma(ab) = \sigma(ba) = \sigma(b)\sigma(a)$, a proto i $\sigma(b)\sigma(a)^{-1} = \sigma(a)^{-1}\sigma(b)$. Tudíž pro $\frac{a}{b} = \frac{c}{d}$ (a tedy $ad = bc$), dostáváme $\sigma(a)\sigma(b)^{-1} = \sigma(b)^{-1}\sigma(a) = \sigma(c)\sigma(d)^{-1}$. Tím je dokázána korektnost a jednoznačnost definice ψ. Zbývá ověřit, že ψ je homomorfismus. Zjevně $\psi(\mathbf{0}) = \mathbf{0}$, $\psi(\mathbf{1}) = \mathbf{1}$, $\psi(-\frac{a}{b}) = -\psi(\frac{a}{b})$, $\psi(\frac{a}{b} \cdot \frac{c}{d}) = \psi(\frac{a}{b})\psi(\frac{c}{d})$, a konečně $\psi(\frac{a}{b} + \frac{c}{d}) = \psi(\frac{ad+bc}{bd}) = \sigma(ad + bc)\sigma(bd)^{-1} = \sigma(a)\sigma(b)^{-1} + \sigma(c)\sigma(d)^{-1} = \psi(\frac{a}{b}) + \psi(\frac{c}{d})$. □

9.9 Tvrzení. *Buď $\sigma : R \simeq S$ izomorfismus oborů integrity. Buď T podílové těleso R a U podílové těleso S. Potom $\psi : T \to U$, $\psi(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)}$ pro každé $\frac{a}{b} \in T$ je také izomorfismus.*

Důkaz. Protože $S \subseteq U$, je ψ podle 9.8 korektně definováno. Současně k $\sigma^{-1} : S \simeq R$ existuje homorfismus $\kappa : U \to T$ takový, že $\kappa(\frac{c}{d}) = \frac{\sigma^{-1}(c)}{\sigma^{-1}(d)}$ pro všechna $\frac{c}{d} \in U$. Ovšem $\kappa\psi(\frac{a}{b}) = \frac{a}{b}$ a $\psi\kappa(\frac{c}{d}) = \frac{c}{d}$, takže ψ je bijektivní. □

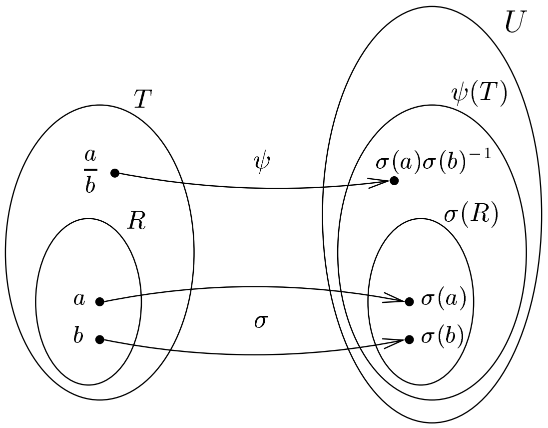
9.10 Tvrzení. *Buď U těleso, $R \subseteq U$ obor integrity a T podílové těleso R. Buď V podtěleso U generované R. Potom $\sigma : T \to V$, kde $\sigma(\frac{a}{b}) = ab^{-1}$ pro každé $\frac{a}{b} \in T$, je izomorfismus.*

Důkaz. To, že $\sigma : T \to V$ je injektivní homomorfismus, plyne z 9.8 a 7.12. Přitom $\sigma(T) \subseteq V$ je těleso, takže musí být i $V \subseteq \sigma(T)$. □

9.11 Důsledek. *Buď T podílové těleso $\mathbb{Z}$ a $\sigma : T \to \mathbb{Q}$ homomorfismus, kde $\sigma(\frac{a}{b}) = ab^{-1}$ pro každé $\frac{a}{b} \in T$. Pak σ je izomorfismus.*

Poznámka. V teoretické aritmetice se postupně logicky budují jednotlivé číselné obory. Racionální čísla se odvozují z celých čísel konstrukcí, jež není ničím jiným leč definicí podílového tělesa. Z tohoto hlediska je Důsledek 9.11 vlastně definicí racionálních čísel.

9.12 Důsledek. *Buď U komutativní těleso a T jeho podílové těleso. Pak $U = T$.*



Jestliže v tělese U naleznu kopii $\sigma(R)$ oboru integrity R, naleznu v U i kopii podílového tělesa T oboru integrity R. Přitom injektivní homomorfismus $\sigma : R \to U$ lze rozšířit jediným způsobem na injektivní homomorfismus $\psi : T \to U$. Těleso $\psi(T)$ je podtělesem U, které je generováno $\sigma(R)$.

Obrázek 9.1: Ilustrace Tvrzení 9.8

Důkaz. Podle 9.7 je $\sigma : U \to T$, $\sigma(a) = \frac{a}{1}$ injektivní homomorfismus. Pro každé $\frac{a}{b} \in T$ je $\frac{a}{b} = \frac{ab^{-1}}{1} = \sigma(ab^{-1})$, takže σ je dokonce izomorfismus. Přitom ztožňujeme a a $\frac{a}{1}$. □

9.13 Tvrzení. *Buď R netriviální okruh a ať je P jeho nejmenší pokokruh. Položme $n = \operatorname{char} R$. Je-li $n = 0$, je $P \cong \mathbb{Z}$. Je-li $n > 0$, je $P \cong \mathbb{Z}_n$. Je-li $n > 0$ a R je obor integrity, je n prvočíslo.*

Důkaz. Podle 7.18 je P obrazem homomorfismu $\mathbb{Z} \to R$, $i \mapsto i \times 1$, kde $\times$ označuje iterované sčítání. Podle definice $n = \operatorname{char} R$ je jádro tohoto homomorfismu rovno $n\mathbb{Z}$. Pro $n = 0$ je jádro triviální, takže $P \cong \mathbb{Z}$. Pro $n > 0$ je $P \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Zbývá použít 9.1 a 8.8. □

9.14 Tvrzení. *Buďte T těleso a P jeho prvotěleso. Je-li $p = \operatorname{char} T > 0$, tak P je rovno nejmenšímu podokruhu R a $P \cong \mathbb{Z}_p$. Je-li T charakteristiky nula, tak $\frac{a}{b} \mapsto (a\mathbf{1}_T) \cdot (b\mathbf{1}_T)^{-1}$ je izomorfismus $\mathbb{Q}$ a P.*

Důkaz. Pro nenulovou charakteristiku tvrzení plyne z 8.8 a 9.13. Je-li $\operatorname{char} T = 0$, je $a \mapsto a\mathbf{1}_T$ izomorfismus $\mathbb{Z}$ a nejmenšího podokruhu S okruhu R. Prvotěleso P je podokruhem R, takže S obsahuje. Můžeme proto naň nahlížet jako na těleso okruhem S generované. Podle 9.10 je P izomorfní podílovému okruhu S, a ten je podle 9.9 izomorfní podílovému okruhu $\mathbb{Z}$. Ovšem podle 9.11 je podílový okruh $\mathbb{Z}$ izomorfní okruhu racionálních čísel $\mathbb{Q}$. □

10 Okruhy polynomů

Buď R okruh a ať x je nějaký symbol mimo R. Množinu všech (formálních) mocninných řad $\sum_{i=0}^{\infty} a_i x^i$ značíme $R[[x]]$.

V $R[[x]]$ definujeme součet a součin:
$(\sum a_i x^i) + (\sum b_i x^i) = \sum (a_i + b_i) x^i$,
$(\sum a_i x^i) \cdot (\sum b_j x^j) = \sum c_k x^k$, kde $c_k = \sum_{i+j=k} a_i b_j$.

$R[[x]]$ je vzhledem k těmto binárním operacím, vzhledem k unární operaci $-(\sum a_i x^i) = \sum (-a_i) x^i$ a vzhledem k nulárním operacím $\mathbf{0} = 0 \cdot x^0$ a $\mathbf{1} = 1 \cdot x^0$ okruh.

Ověřme například asociativitu násobení (ostatní axiomy se ověří ještě snadněji): $((\sum a_i x^i) \cdot (\sum b_j x^j)) \cdot (\sum c_k x^k) = (\sum_r (\sum_{i+j=r} a_i b_j) x^r) \cdot (\sum c_k x^k) =$
$\sum_t (\sum_{r+k=t} (\sum_{i+j=r} a_i b_j) c_k) x^t = \sum_t (\sum_{i+j+k=t} a_i b_j c_k) x^t =$
$\sum_t (\sum_{i+s=t} a_i (\sum_{j+k=s} b_j c_k)) x^t = (\sum a_i x^i) \cdot (\sum_s (\sum_{j+k=s} b_j c_k) x^s) =$
$(\sum a_i x^i) \cdot ((\sum b_j x^j) \cdot (\sum c_k x^k))$.

Ztotožníme-li každý prvek a okruhu R s odpovídajícím prvkem ax^0 okruhu $R[[x]]$, stane se okruh R podokruhem okruhu $R[[x]]$. Z definice je zřejmé, že $R[[x]]$ je komutativní okruh právě když R je komutativní okruh.

10.1 Lemma. *$R[[x]]$ je obor integrity právě když R je obor integrity.*

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_j x^j$ jsou takové mocninné řady, že $a \neq \mathbf{0} \neq b$. Položme $r = \min\{i; a_i \neq 0\}$ a $s = \min\{j; b_j \neq 0\}$. Ať $a \cdot b = \sum c_k x^k$. Pak $c_{r+s} = \sum_{i+j=r+s} a_i b_j = \sum_{i<r} a_i b_{r+s-i} + a_r b_s + \sum_{s>j} a_{r+s-j} b_j = a_r b_s \neq 0$, takže $a \cdot b \neq 0$. □

Pro $a = \sum a_i x^i$ definujeme (formální) derivaci a' tak, že a' je mocninná řada $\sum (i+1)a_{i+1}x^i$. Všimněte si, že rovněž platí $a' = \sum_{i\geq 1} ia_{i-1}x^i$.

10.2 Tvrzení. *Buď $a, b \in R[[x]]$ a $r \in R$. Pak $(a+b)' = a' + b'$, $(ab)' = a'b + ab'$ a $(ra)' = ra'$.*

Důkaz. Ať $a = \sum a_i x^i$, $b = \sum b_i x^i$. Pak $(a+b)' = \sum (i+1)(a_{i+1}+b_{i+1})x^i = \sum (i+1)a_{i+1}x^i + \sum (i+1)b_{i+1}x^i = a' + b'$. Dále $(ab)' = \sum_k \big((k+1)(\sum_{i+j=k+1} a_i b_j)\big)x^k = \sum_k \big(\sum_{i+j=k+1}(i+j)a_i b_j\big)x^k = \sum \big(\sum_{i+j=k+1}(ia_i)b_j\big)x^k + \sum \big(\sum_{i+j=k+1} a_i(jb_j)\big)x^k = \sum_k \big(\sum_{i+j=k}(i+1)a_{i+1}b_j\big)x^k + \sum_k \big(\sum_{i+j=k} a_i(j+1)b_{j+1}\big)x^k = a'b + ab'$. Konečně $(ra') = r'a + ra' = ra'$, neboť $r' = 0$. □

Mocninné řady $\sum a_i x^i$, pro které lze najít takové $k \geq 0$, že $a_i = 0$ pro každé $i \geq k$, se nazývají *polynomy*. Je-li $a = \sum a_i x^i$ polynom, definujeme jeho *stupeň* $\operatorname{st} a$ tak, že $\operatorname{st} \mathbf{0} = -1$ a pro $\mathbf{0} \neq a$ je $\operatorname{st} a = \max\{i; a_i \neq 0\}$.

10.3 Lemma. *Buď $a, b \in R[[x]]$ dva polynomy. Pak, $-a$, $a+b$ a $a \cdot b$ jsou polynomy a platí:*

(i) $\operatorname{st}(-a) = \operatorname{st} a$ *a* $\operatorname{st}(a+b) \leq \max\{\operatorname{st} a, \operatorname{st} b\}$.

(ii) Pro $a \neq \mathbf{0} \neq b$ je $\operatorname{st}(a \cdot b) \leq \operatorname{st} a + \operatorname{st} b$. Je-li R obor integrity, tak pro $a \neq \mathbf{0} \neq b$ je $\operatorname{st}(ab) = \operatorname{st} a + \operatorname{st} b$.

Důkaz. (i) je zřejmé, dokažme (ii). Ať $a = \sum a_i x^i$, $b = \sum b_j x^j$ a $a \cdot b = \sum c_k x^k$. Ať $n = \operatorname{st} a$ a $m = \operatorname{st} b$. Je-li $i+j > n+m$, je $i > n$ nebo $j > m$, takže $\operatorname{st}(a \cdot b) \leq n+m$. Protože $c_{n+m} = a_n b_m$, pro obory integrity platí $\operatorname{st}(a \cdot b) = \operatorname{st} a + \operatorname{st} b$. □

Množina všech polynomů okruhu R se značí $R[x]$.

10.4 Důsledek. *$R[x]$ je podokruh okruhu $R[[x]]$.*

Je-li R obor integrity, je i $R[x]$ obor integrity.

I nadále budeme ztožňovat prvky R a polynomy nultého stupně.

10.5 Tvrzení. *Buď R obor integrity. Polynom $a \in R[x]$ je invertibilní právě když $\operatorname{st} a = 0$ a a je invertibilní v R.*

Důkaz. Ať $a \cdot b = \mathbf{1}$. Pak $\operatorname{st} a + \operatorname{st} b = \operatorname{st} \mathbf{1} = 0$, takže $\operatorname{st} a = \operatorname{st} b = 0$. Zbytek je jasný. □

10.6 Věta. *Buď R obor integrity a $a = \sum a_i x^i$ a $b = \sum b_i x^i$ dva polynomy nad R. Ať $m = \operatorname{st} b \geq 0$ a b_m je invertibilní v R. Pak existují jednoznačně určené polynomy $q, r \in R[x]$ takové, že $a = bq + r$, kde $\operatorname{st} r < m$.*

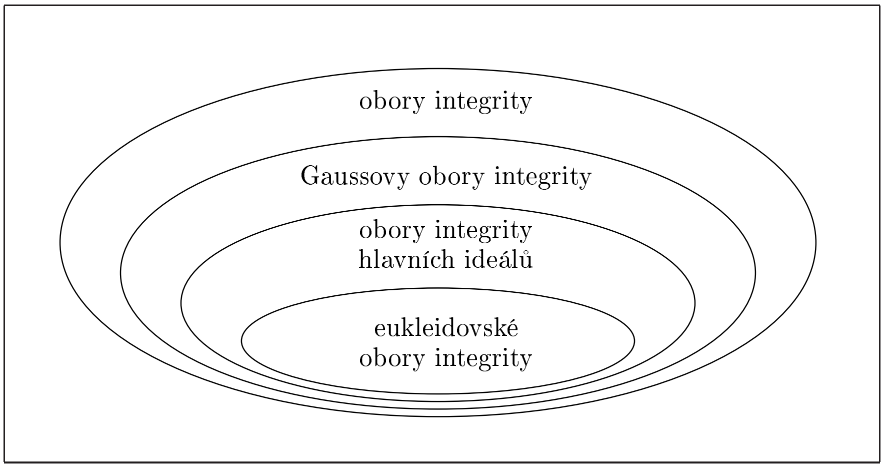
Důkaz. Dokažme nejprve, že uvedené polynomy skutečně existují. Položme $n = \operatorname{st} a$. Je-li $m > n$, tak stačí položit $q = 0$ a $r = a$. Pro $n \geq m$ budeme postupovat indukcí dle $\delta = n - m$. Je-li $\delta = 0$, položíme $q = a_n b_n^{-1}$ a $r = a - qb$. Ať je $\delta > 0$. Položme $s = a_n b_m^{-1} x^\delta$ a $c = a - sb$. Pak $\operatorname{st} c \leq \operatorname{st} a = n$ a současně koeficient u x^n v c je roven $a_n - a_n b_m^{-1} b_m = 0$, takže $\operatorname{st} c \leq n - 1$. Podle indukčního předpokladu existují polynomy t a r takové, že $c = bt + r$, $\operatorname{st} r < \operatorname{st} b$. Potom $a = c + sb = bt + r + bp = b(t + p) + r$, a stačí položit $q = t + p$.

Ať $a = bq_1 + r_1 = bq_2 + r_2$ a ať platí $\operatorname{st} r_1 < m$ a $\operatorname{st} r_2 < m$. Potom b dělí $r_1 - r_2$ a z $r_1 - r_2 \neq 0$ by podle 10.3(ii) plynulo $\operatorname{st} b \leq \operatorname{st}(r_1 - r_2) < m$. To je spor, takže musí platit $r_1 = r_2$, a tím i $q_1 = q_2$. □

Buď R obor integrity. Zobrazení $\nu : R^\# \to \mathbb{N}_0$ (kde $R^\# = R \setminus \{\mathbf{0}\}$) se nazývá *eukleidovskou funkcí,* jestliže pro libovolné $a, b \in R$ platí:

- pokud $a|b$ a $b \neq \mathbf{0}$, tak $\nu(a) \leq \nu(b)$,
- pokud $a \neq \mathbf{0} \neq b$, tak existují $q, r \in R$ takové, že $a = bq + r$, kde $r = 0$ nebo $\nu(r) < \nu(b)$.

Obor integrity R, pro který lze definovat alespoň jednu eukleidovskou funkci, se nazývá *eukleidovským oborem integrity.*



Obrázek 10.1: Vztahy mezi různými obory integrity

10.7 Věta. *Jestliže R je komutativní těleso, tak $R[x]$ je eukleidovský obor integrity, přičemž stupeň polynomu je eukleidovskou funkcí.*

Důkaz. Použij 10.3(ii) a 10.6. □

Obor integrity R se nazývá *oborem integrity hlavních ideálů,* jestliže každý ideál R je hlavní ideál.

10.8 Tvrzení. *Každý eukleidovský obor integrity je oborem integrity hlavních ideálů.*

Důkaz. Buď $\nu : R^{\#} \to \mathbb{N}_0$ eukleidovská funkce a ať I je nenulový ideál v R. Položme $t = \min\{\nu(b);\ \mathbf{0} \neq b \in I\}$ a zvolme $a \in I$ tak, aby $\nu(a) = t$. Pak $aR \subseteq I$. Naopak, je-li $b \in I$, tak $b = aq + r$, kde $r = \mathbf{0}$ nebo $\nu(r) < \nu(a) = t$. Protože $r \in I$, tak z minimality t dostáváme $r = \mathbf{0}$, takže $b \in aR = I$. □

Obor integrity R se nazývá *Gaussův,* jestliže v $R^{\#}(\cdot, \mathbf{1})$ má každý neinvertibilní prvek jednoznačný ireducibilní rozklad. (Připomeňme, že ve Větě 5.19 jsou formulovány další podmínky této podmínce ekvivalentní.)

10.9 Tvrzení. *Buď R obor integrity hlavních ideálů a $a_1, \dots, a_n \in R$. Pak existují $u_1, \dots, u_n \in R$ takové, že $\sum u_i a_i = NSD(a_1, \dots, a_n)$.*

Důkaz. Ať I je ideál generovaný prvky $a_1, \dots, a_n$. Pak existuje $d \in R$, že $I = dR$, takže $d = \sum a_i u_i$ dle 7.5. Současně $d|a_i$ pro $1 \leq i \leq n$. Jestliže $t|a_i$ pro $1 \leq i \leq n$, tak také $t| \sum a_i u_i = d$. □

10.10 Lemma. *Buď R obor integrity hlavních ideálů. Pak kvaziuspořádání R dělitelností je noetherovské.*

Důkaz. Ať $a_0, a_1, \dots$ je nekonečná posloupnost vlastních dělitelů. Potom pro $i \in \mathbb{N}_0$ je $a_i R \subsetneqq a_{i+1} R$. Snadno ověříme, že $I = \bigcup_i a_i R$ je ideál, a tedy existuje $d \in R$, pro které je $I = dR$. To ovšem znamená, že $d \in a_j R$ pro některé $j \in \mathbb{N}_0$, takže $a_j R = dR = a_{j+1} R$, spor. □

10.11 Důsledek. *Obory integrity hlavních ideálů jsou Gaussovy.*

Důkaz. Použij 5.19, 10.9 a 10.10. □

10.12 Tvrzení. *Buď R obor integrity hlavních ideálů. Potom $a \in R$ je prvočinitel právě když aR je maximální ideál v R.*

Důkaz. Prvek a je prvočinitel právě když je ireducibilní, tj. právě když není invertibilní a nemá vlastní dělitele. Buď I ideál, $R \supsetneqq I \supseteq aR$. Pak existuje $b \in R$, že $I = bR$. Ovšem $bR \supsetneqq aR$ jedině tehdy, jestliže b je vlastní dělitel a. □

Víme, že v eukleidovských oborech integrity existují největší společní dělitelé. Tyto obory integrity dostali svůj název podle prastarého algoritmu, který umožňuje největší společné dělitele účinně nacházet.

10.13 Tvrzení. (Eukleidův algoritmus.) *Buď R obor integrity a $\nu : R^{\#} \to \mathbb{N}_0$ eukleidovská funkce a ať a_0, a_1 jsou prvky $R^{\#}$. Budeme definovat posloupnost $a_0, a_1, \ldots$ takovýmto způsobem:*

(i) Je-li $i \geq 1$ a a_i nedělí a_{i-1}, tak zvolíme a_{i+1} tak, že pro nějaké $q_i \in R$ je $a_{i-1} = a_i q_i + a_{i+1}$ a $\nu(a_{i+1}) < \nu(a_i)$.

(ii) Je-li $i \geq 1$ a a_i dělí a_{i-1}, tak položíme $n = i$ a posloupnost ukončíme.

Takto vytvořená posloupnost je vždy konečná a $a_n = NSD(a_0, a_1)$.

Důkaz. Konečnost posloupnosti plyne z toho, že $\nu(a_i) > \nu(a_{i+1})$. $NSD(a_n, a_{n-1}) = a_n$ dle 4.8, takže stačí ukázat, že pro každé $1 \leq i \leq n-1$ je $d||t$, kde $d = NSD(a_{i-1}, a_i)$ a $t = NSD(a_i, a_{i+1})$. Vidíme, že d dělí $a_{i+1} = a_{i-1} - a_i q$, takže $d|t$. Naopak, t dělí $a_{i-1} = a_i q + a_{i+1}$, takže $t|d$. □

Aplikujme nyní dosažené výsledky na eukleidovský obor integrity $T[x]$, kde T je komutativní těleso. Přitom na T hledíme jako na podokruh $T[x]$. Multiplikativní grupu tělesa T budeme označovat T^*. (Pro těleso T je tedy T^* rovno $T^{\#}$; obecně pro okruhy tato rovnost však neplatí, neboť R^* označuje množinu (grupu) invertibilních prvků okruhu R.)

Invertibilní prvky $T[x]$ jsou nenulové prvky tělesa T (viz 10.5). Obor integrity $T[x]$ je eukleidovský (10.7), tedy obor integrity hlavních ideálů (10.8), tedy Gaussův (10.11).

Polynom $a = \sum a_i x^i \in T[x]$ nazvu *monický,* jestliže $a_{\mathrm{st}\, a} = 1$ a $a \neq \mathbf{0}$. Každý nenulový polynom je zjevně asociován právě s jedním monickým polynomem. Z 5.18 plyne, že každý polynom $a \in T[x]$ stupně alespoň 1 lze napsat až na pořadí jediným způsobem jako $cp_1^{k_1} \ldots p_r^{k_r}$, kde $p_1, \ldots, p_r$ jsou navzájem různé monické ireducibilní polynomy, $k_1, \ldots, k_r$ jsou přirozená čísla a $c \in T^*$ (přitom $c = a_{\mathrm{st}\, a}$ a $\mathrm{st}\, a = \sum k_i (\mathrm{st}\, p_i)$).

Pro $a, b \in T[x]$ platí $aT[x] = bT[x]$ právě když jsou polynomy a, b v $T[x]$ asociovány (viz 7.6). Protože invertibilní prvky okruhu $T[x]$ se shodují s nenulovými prvky tělesa T (viz 10.5) a protože prvky jsou asociovány tehdy, liší-li se o invertibilní prvek (viz 5.10), vidíme, že $aT[x] = bT[x]$ platí právě když polynom a je roven tb pro nějaké $t \in T$. To znamená, že hlavní ideál $aT[x]$, $a \neq 0$, lze jediným způsobem vyjádřit jako $mT[x]$ tak, aby m byl polynom monický. Tudíž každý monický polynom obsažený v $aT[x]$ je buď roven m, nebo má stupeň vyšší než $\operatorname{st} a = \operatorname{st} m$. V okruhu $T[x]$ jsou všechny ideály hlavní, takže jsme dokázali, že každý nenulový ideál je jednoznačně charakterizován monickým polynomem, který ho generuje.

Prvek $\alpha \in T$ nazveme *kořenem* polynomu $a \in T[x]$, jestliže polynom $x - \alpha$ dělí a. Přitom $x - \alpha$ je podle 10.3(ii) a 10.5 ireducibilní prvek $T[x]$ pro každé $\alpha \in T$. Je-li $a = cp_1^{k_1} \dots p_r^{k_r}$ rozklad nenulového polynomu a na ireducibilní polynomy, tak ty z nich, které jsou tvaru $x - \alpha$, nazýváme *kořenovými* činiteli a. Jsou-li všechna $p_1, \dots, p_r$ stupně 1, říkáme, že a se *rozkládá na kořenové činitele.* Je-li p_i, $1 \leq i \leq r$, kořenový činitel, $p_i = x - \alpha$, tak číslo k_i nazýváme *násobností* kořenu α. Jestliže se a rozkládá na kořenové činitele, tak $\operatorname{st} a = \sum k_i$. Počet kořenů, počítáme-li každý tolikrát, kolik činí jeho násobnost, je tedy menší nebo roven stupni polynomu, přičemž rovnost nastává právě když se polynom rozkládá na kořenové činitele. (Je třeba si uvědomit, že tyto výroky se týkají pouze nenulového polynomu.)

Komutativní těleso T, ve kterém se každý polynom $a \in T[x]$, $\operatorname{st} a \geq 1$, rozkládá na kořenové činitele, se nazývá *algebraicky uzavřené.* Příkladem algebraicky uzavřeného tělesa je těleso komplexních čísel $\mathbb{C}$.

10.14 Tvrzení. *Buď T těleso, $0 \neq a \in T[x]$ a ať α je kořen a. Potom α je násobnosti alespoň 2 právě když je také kořenem a'.*

Důkaz. Ať je $a = (x - \alpha)b$ pro vhodné $b \in T[x]$. Máme $a' = b + (x - \alpha)b'$, takže $x - \alpha$ dělí a' právě když $x - \alpha$ dělí b. □

10.15 Důsledek. *Buď T těleso, $a \in T[x]$ a ať $NSD(a, a') = \mathbf{1}$. Potom a nemá vícenásobné kořeny.*

10.16 Tvrzení. *Buď $n \in \mathbb{N}$, T těleso a ať $\operatorname{char} T$ nedělí n. Pak polynomy $x^n - \mathbf{1}$ a $x^{n+1} - x$ nemají vícenásobné kořeny.*

Důkaz. Polynom $(x^n - \mathbf{1})' = nx^{n-1} = (n \cdot \mathbf{1})x^{n-1}$ je asociován s polynomem x^{n-1}, neboť z toho, že $\operatorname{char} T$ nedělí n, plyne $n \cdot \mathbf{1} \neq 0$. Je $x^n - \mathbf{1} = x \cdot x^{n-1} - \mathbf{1}$, a proto $NSD(x^n - \mathbf{1}, x^{n-1}) = \mathbf{1}$.

Polynom $x^{n+1} - x = x \cdot (x^n - \mathbf{1})$ má za kořeny nulu a všechny kořeny polynomu $x^n - \mathbf{1}$. Protože nula není kořenem polynomu $x^n - \mathbf{1}$, nemůže mít ani polynom $x^{n+1} - x$ jakýkoliv vícenásobný kořen. □

Jsou-li $S \supseteq R$ do sebe vřazené komutativní okruhy a α je prvek S, definujeme *dosazovací homomorfismus* $j_\alpha : R[x] \to S$ tak, že $j_\alpha(\sum a_i x^i) = \sum a_i \alpha^i$ pro každé $a = \sum a_i x^i \in R[x]$.

10.17 Lemma. *$j_\alpha : R[x] \to S$ je homomorfismus okruhů.*

Důkaz. Pro polynomy $a = \sum a_i x^i$ a $b = \sum b_j x^j$ jistě platí $j_\alpha(a+b) = j_\alpha(a)+j_\alpha(b)$. Podobně pro $a \cdot b = c = \sum c_k x^k$ dostáváme $j_\alpha(c) = \sum_k (\sum_{i+j=k} a_i b_j)\alpha^k = (\sum a_i \alpha^i)(\sum b_j \alpha^j) = j_\alpha(a) j_\alpha(b)$. □

Místo $j_\alpha(a)$ se většinou píše $a(\alpha)$. Ale označení j_α budeme pro dosazovací homomorfismus dále používat také.

10.18 Tvrzení. *Buď T komutativní těleso, $a \in T[x]$ a $\alpha \in T$. Pak α je kořen polynomu a právě když $a(\alpha) = 0$.*

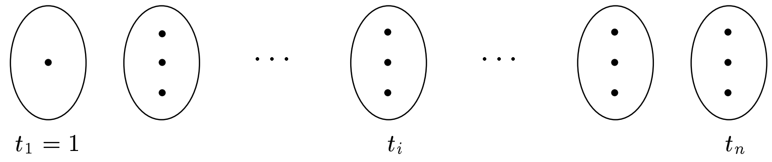
Důkaz. Ať $a = (x-\alpha)b$ pro $b \in T[x]$. Podle 10.17 je $f_\alpha(a) = a(\alpha) = (\alpha-\alpha)b(\alpha) = 0$. Naopak, ať $a(\alpha) = 0$ a $a = (x-\alpha)q + r$, kde $\operatorname{st} r \leq 0$ (čili $r \in T$). Potom $0 = a(\alpha) = (\alpha-\alpha)q(\alpha) + r(\alpha) = r$. □

10.19 Tvrzení. *Buď T komutativní těleso a $G \subseteq T^*$ nějaká podgrupa (tj. G je množina uzavřená na násobení a inverzní prvky). Je-li G konečná, tak je cyklická.*

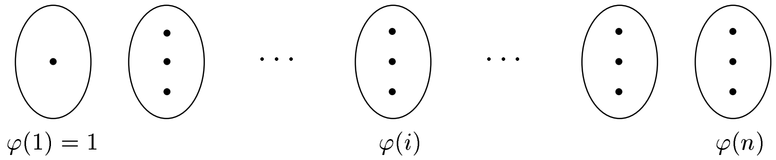
Důkaz. Položme $n = |G|$ a připomeňme, že řád každého prvku G dělí n (Lagrangeova věta). Pro dělitel k čísla n označme t_k počet prvků řádu k. Protože každý prvek má nějaký řád, musí platit $n = \sum t_k$. Grupa G bude cyklická, je-li $t_n \geq 1$ (a pak je $t_n = \varphi(n)$, kde φ označuje Eulerovu funkci). Podle 8.14 máme $n = \sum \varphi(k)$. Není-li G cyklická, je $0 = t_n < \varphi(n)$, takže pro nějaký vlastní dělitel k čísla n musí platit $t_k > \varphi(k)$. Předpokládejme, že tomu tak je, zvolme prvek $a \in G$ řádu k, a označme A podgrupu tímto prvkem generovanou. Ta má k prvků, z nichž $\varphi(k)$ má řád k. Z $t_k > \varphi(k)$ plyne, že musí existovat alespoň jeden prvek $b \in G$, jenž je řádu k, ale neleží v A. Každý prvek A je kořenem polynomu $x^k - 1$. Ale i prvek b je kořenem tohoto polynomu. To znamená, že polynom $x^k - 1$ má přinejmenším $|A| + 1 = k + 1$ různých kořenů. To je ovšem spor, takže grupa G skutečně musí být cyklická. □

Je-li R nějaký okruh, S jeho podokruh a $M \subseteq R$, budeme podokruh R generovaný množinou $S \cup M$ značit $S[M]$. Je-li $M = \{a_1, \ldots, a_n\}$, tak místo $S[M]$ píšeme též $S[a_1, \ldots, a_n]$. (Protože okruh polynomů $R[x]$ je generovaný $R \cup \{x\}$, není zde žádný konflikt s již zavedeným značením.)

Prvky grupy G řádu n rozdělíme do bloků tak, aby v jednom bloku byly prvky stejného řádu. Počet prvků řádu i označím t_i



Platí $\sum_{i|n} t_i = n$, a $t_n > 0$ právě když G je cyklická.
Je-li $a \in G$ řádu k, tak každá mocnina a^j je kořenem polynomu $x^k - \mathbf{1}$. (Máme $(a^j)^k = (a^k)^j = \mathbf{1}^j = \mathbf{1}$.) V grupě $A = \{a^j;\ j \in \mathbb{Z}\}$ generované prvkem a je jednak k kořenů polynomu $x^k - \mathbf{1}$, jednak $\varphi(k)$ prvků řádu k. To znamená, že když je $t_k > \varphi(k)$, tak musí v G být i prvek řádu k, který neleží v A. Pak bychom ale měli příliš mnoho kořenů polynomu $x^k - \mathbf{1}$, a proto je $t_k \le \varphi(k)$.
Víme, že $n = \sum_{i|n} \varphi(i)$. Když $\mathbb{Z}_n$ rozdělíme do bloků tak, aby v jednom bloku byly prvky stejného řádu, máme



Protože je vždy $t_i \le \varphi(i)$ a současně $\sum \varphi(i) = \sum t_i$, musí být $t_i = \varphi(i)$ pro každé i dělící n, a tedy i $t_n = \varphi(n) > 0$.

Obrázek 10.2: Důkaz Tvrzení 10.19

11 Existence kořenových a rozkladových nadtěles

Je-li $f : R \to S$ homomorfismus okruhů, definujeme $f_x : R[x] \to S[x]$ tak, že pro $a = \sum a_i x^i \in R[x]$ je $f_x(a) = \sum f(a_i) x^i$. Protože R a S chápeme po řadě jako podokruhy $R[x]$ a $S[x]$, je zobrazení f_x rozšířením homomorfismu f.

11.1 Lemma. *$f_x : R[x] \to S[x]$ je okruhový homomorfismus.*

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_i x^i$ jsou polynomy z $R[x]$. Pak $f_x(a+b) = \sum f(a_i + b_i)x^i = \sum (f(a_i) + f(b_i))x^i = f_x(a) + f_x(b)$ a $f_x(a \cdot b)$ lze vyjádřit jako $\sum_k f(\sum_{i+j=k} a_i b_j)x^k = \sum_k (\sum_{i+j=k} f(a_i)f(b_j))x^k = f_x(a)f_x(b)$. Zbytek je zřejmý. □

Každý homomorfismus je dle 3.3 určen hodnotami na množině generátorů. Okruh $R[x]$ je generován množinou $R \cup \{x\}$. Odsud plyne, že pro okruh A a homomorfismy h_1, h_2 z $R[x]$ do A platí $h_1 = h_2$ právě když $h_1(x) = h_2(x)$ a pro každé $r \in R$ je $h_1(r) = h_2(r)$. Tohoto pozorování níže vícekrát využijeme.

11.2 Lemma. *Buďte $f : R \to S$ a $g : S \to T$ homomorfismy okruhů. Pak $(gf)_x = g_x f_x$.*

Důkaz. Platí $(gf)_x(x) = g_x(f_x(x))$, a pro $r \in R$ je $g_x f_x(r) = gf(r) = (gf)_x(r)$. □

11.3 Důsledek. *Buď $f : R \simeq S$ izomorfismus okruhů. Pak $f_x : R[x] \to S[x]$ je rovněž izomorfismus.*

Důkaz. Podle 11.2 je $f_x(f^{-1})_x = (\mathrm{id}_S)_x = \mathrm{id}_{S[x]}$ a $(f^{-1})_x f_x = (\mathrm{id}_R)_x = \mathrm{id}_{R[x]}$. □

11.4 Lemma. *Buď $f : R \to S$ homomorfismus komutativních okruhů a ať $\alpha \in R$. Pak $fj_\alpha = j_{f(\alpha)} f_x$.*

$$\begin{tikzcd} R[x] \arrow[r, "f_x"] \arrow[d, "j_\alpha"'] & S[x] \arrow[d, "j_{f(\alpha)}"] \\ R \arrow[r, "f"] & S \end{tikzcd}$$

Důkaz. Máme $fj_\alpha(x) = f(\alpha) = j_{f(\alpha)}(x) = j_{f(\alpha)} f_x(x)$, a pro $r \in R$ je $fj_\alpha(r) = f(r) = j_{f(\alpha)}(f(r)) = j_{f(\alpha)}(f_x(r))$. Využili jsme toho, že při dosazování absolutní členy nemění svou hodnotu a že f_x se na nich shoduje s f. □

11.5 Tvrzení. *Buď T komutativní těleso a ať $u \in T[x]$ je polynom stupně $n \geq 1$. Položme $I = uT[x]$. Množina $\{a \in T[x];\ \mathrm{st}\, a < n\}$ je transversálou kongruence* mod I.

Zobrazení $f_x : R \to S$ lze slovně popsat tak, že v polynomech nad R se koeficienty modifikují pomocí f, čímž vznikají polynomy nad S.
Jednou z možných aplikací je situace, kdy R i S jsou rovny nějakému komutativnímu tělesu T a f je automorfismus T. Například ať $T = \mathbb{C}$ a ať f zobrazí každé komplexní číslo na číslo komplexně sdružené, tedy $f(a+bi) = \overline{a+bi} = a - bi$ pro všechna $a, b \in \mathbb{R}$. Pak f_x je podle 11.3 automorfismus $\mathbb{C}[x]$. Ilustrujme to na příkladu, kdy $u, v \in \mathbb{C}[x]$ mají hodnoty

$$u = (2+i)x^2 + (1-i) \quad \text{a} \quad v = (1-2i)x + (2+3i).$$

Potom $uv = (4-3i)x^3 + (1+8i)x^2 + (-1-3i)x + (5+i)$, takže $f_x(uv) = (4+3i)x^3 + (1-8i)x^2 + (-1+3i)x + (5-i)$. Ověřme, že vskutku $f_x(uv) = f_x(u) \cdot f_x(v)$. Máme

$$f_x(u) = (2-i)x^2 + (1+i) \quad \text{a} \quad f_x(v) = (1+2i)x + (2-3i),$$

což po vynásobení skutečne dává

$$(4+3i)x^3 + (1-8i)x^2 + (-1+3i)x + (5-i).$$

Obrázek 11.1: Slučitelnost modifikace koeficientů s násobením

Důkaz. Pro $b, c \in T[x]$ je $b \equiv c \bmod I$ právě když u dělí $b - c$. Je-li $b = uq + r$, kde $b, q, r \in T[x]$ jsou polynomy, platí $b \equiv r \bmod I$. Proto je každý polynom $b \in T[x]$ modulo I kongruentní s nějakým polynomem $r \in T[x]$, $\operatorname{st} r < n = \operatorname{st} u$.

Jsou-li a, b dva polynomy stupně menšího než n, tak je i $\operatorname{st}(a-b) < n$. Proto v takovém případě z $a \equiv b \bmod I$ plyne $a - b = 0$, a tedy $a = b$. $\square$

V kapitole 2 jsme vyložili konstrukci algebry indukované transversálou T kongruence ρ, kde ρ je kongruence algebry $A = A(\alpha_1, \dots, \alpha_k)$. Konstrukci lze popsat tak, že je-li $\alpha = \alpha_i$, $1 \leq i \leq k$, operace četnosti n, tak $\alpha_T(b_1, \dots, b_k) = \pi(\alpha_A(b_1, \dots, b_k))$, kde $b_1, \dots, b_k$ jsou prvky transversály T a $\pi(a)$ pro každé $a \in A$ udává ten jediný prvek c transversály T, jenž splňuje $c \equiv a \bmod \rho$. Při takové definici algebry T se π stává surjektivním homomorfismem $A \to T$ s jádrem ρ.

V kapitole 8 jsme uvedený postup použili pro definici okruhů $\mathbb{Z}_n$. V tomto

Vztah $fj_\alpha = j_{f(\alpha)}f_x$ lze slovně vyjádřit tak, že modifikace dosazené hodnoty se rovná dosazení modifikované hodnoty do polynomu s modifikovanými koeficienty.
Zkoumejme situaci, kdy $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $n > 1$, a f je redukce modulo n (tedy $f(a)$ je rovno zbytku po dělení a číslem n). Je-li $u \in \mathbb{Z}[x]$ a $\alpha \in \mathbb{Z}$, tak $fj_\alpha(u) = f(u(\alpha))$ udává redukci $u(\alpha)$ modulo n. Naopak $j_{f(\alpha)}f_x(u) = f_x(u)(f(\alpha))$ označuje výpočet v $\mathbb{Z}_n$, kde do polynomu s koeficienty redukovanými modulo n se dosazuje hodnota α redukovaná modulo n. Lemma 11.4 říká, že výsledek je v obou případech stejný.
Ať je například $n = 3$, $u = x^4 - 3x^3 + 5x^2 + x + 8$ a $\alpha = 4$. Pak $u(\alpha) = 156$ a $f(u(\alpha)) = 0$. Současně $f_x(u) = x^4 + 2x^2 + x + 2$, $f(\alpha) = 1$ a $j_1 f_x(u) = 1^4 + 2 \cdot 1^2 + 1 + 2$ je modulo 3 skutečně rovno nule, tak jak z rovnosti $j_{f(\alpha)}f_x(u) = f_x(u)(f(\alpha))$ vyplývá.

Obrázek 11.2: Modifikace polynomů a dosazování

okruhu je tedy například součet prvků $a, b \in \mathbb{Z}_n$ roven $\pi_n(a + b)$, kde $\pi(n)$ udává zbytek při dělení modulo n.

Ať T je opět komutativní těleso a ať $a, u \in T[x]$ jsou polynomy, $\operatorname{st} u \geq 1$. Označme $\pi_u(a)$ ten jediný polynom $c \in T[x]$, pro který současně platí $a \equiv c \bmod I$, $I = uT[x]$, a $\operatorname{st} c < n$, $n = \operatorname{st} u$. Z Tvrzení 11.5 vyplývá, že taková definice π_u je možná. Současně vidíme, že $\pi_u(a)$ je rovno zbytku po dělení polynomu a polynomem u.

Okruh indukovaný transversálou $\{a \in T[x];\ \operatorname{st} a < n\}$ označíme $(T[x])_u$. Skládá se ze všech polynomů nad T, které mají stupeň menší než $n = \operatorname{st} u$. Součet polynomů $a, b \in (T[x])_u$ je podle definice roven $\pi_u(a+b)$. Ovšem $\operatorname{st}(a+b) < n$ (viz 10.3(i)), takže sčítání v $(T[x])_u$ je shodné se sčítáním v $T[x]$. Tím se konstrukce $(T[x])_u$ odlišuje od konstrukce $\mathbb{Z}_n$, jinak je jí však velmi podobná. Násobek polynomů a a b je v $(T[x])_u$ roven $\pi_u(a + b)$. Zde se dělení se zbytkem vyhnout nelze, neboť součin $a \cdot b$ může mít v $T[x]$ stupeň až $2n - 2$.

11.6 Tvrzení. *Buď T komutativní těleso a ať $u \in T[x]$ je polynomem stupně alespoň 1. Okruh $(T[x])_u$ je tělesem právě když u je ireducibilní polynom.*

Důkaz. Položme $n = \operatorname{st} u$ a předpokládejme nejprve, že polynom u není ireducibilní. Pak $u = ab$, kde $\operatorname{st} a < n$ a $\operatorname{st} b < n$. Součin a a b v $(T[x])_u$ je tedy roven

0, byť a i b jsou nenulové prvky $(T[x])_u$. To znamená, že $(T[x])_u$ není ani obor integrity, natož těleso.

Předpokládejme nyní, že u je ireducibilní a že $a \in (T[x])_u$ je nenulový polynom. Polynomy a a u jsou nesoudělné, a proto podle 10.9 existují polynomy $v, w \in T[x]$ takové, že $va + wu = 1$. To ale znamená $\pi_u(va) = 1$, takže $\pi_u(v)$ je v $(T[x])_u$ vůči a prvek inverzní. $\square$

Předchozí důkaz je zde uveden kvůli jeho přímočarosti a konstruktivnosti. Je však dobré si uvědomit, že tvrzení 11.6 je obsaženo v již dříve dokázaných vztazích. Víme totiž, že obor integrity hlavních ideálů $T[x]$ je Gaussův (viz 10.11), takže ireducibilní prvky se shodují s prvočiniteli (viz 5.19), a tedy $uT[x]$ je maximální ideál právě když u je ireducibilní (viz 10.12). Podle 7.14 je proto $(T[x])_u \cong T[x]/uT[x]$ těleso právě když u je ireducibilní.

Je-li p prvočíslo a je-li $u \in \mathbb{Z}_p[x]$ ireducibilní polynom stupně $n \geq 1$, je $(\mathbb{Z}_p[x])_u$ komutativní těleso, které má p^n prvků (neboť právě tolik je polynomů stupně menšího než n). Pro každé prvočíslo p a každé prvočíslo p a každé $n \geq 1$ existuje alespoň jeden ireducibilní polynom $u \in \mathbb{Z}_p[x]$ stupně n, takže konečné komutativní těleso lze sestrojit pro každý řád p^n. Důkaz existence ireducibilních polynomů však není zcela přímočarý a provedeme ho až v následujících kapitolách.

Polynom $u = y^3 + y + 1 \in \mathbb{Z}_2[y]$ nemá za kořen ani prvek 0 ani prvek 1. Polynomy stupně 3, které nejsou ireducibilní, musí mít alespoň jeden kořen. Proto je $y^3 + y + 1$ v $\mathbb{Z}_2[y]$ ireducibilní a $(\mathbb{Z}_2[y])_{y^3+y+1}$ je těleso řádu 8.
Sčítání se v tomto tělese shoduje s běžným sčítáním polynomů a násobení polynomů a a b je rovno $\pi_u(a \cdot b)$, což poskytuje následující tabulku:

Obrázek 11.3: Těleso řádu 8

$\cdot$	0	1	y	$y{+}1$	y^2	$y^2{+}1$	$y^2{+}y$	$y^2{+}y{+}1$
0	0	0	0	0	0	0	0	0
1	0	1	y	$y{+}1$	y^2	$y^2{+}1$	$y^2{+}y$	$y^2{+}y{+}1$
y	0	y	y^2	$y^2{+}y$	$y{+}1$	1	$y^2{+}y{+}1$	$y^2{+}1$
$y{+}1$	0	$y{+}1$	$y^2{+}y$	$y^2{+}1$	$y^2{+}y{+}1$	y^2	1	y
y^2	0	y^2	$y{+}1$	$y^2{+}y{+}1$	$y^2{+}y$	y	$y^2{+}1$	1
$y^2{+}1$	0	$y^2{+}1$	1	y^2	y	$y^2{+}y{+}1$	$y{+}1$	$y^2{+}y$
$y^2{+}y$	0	$y^2{+}y$	$y^2{+}y{+}1$	1	$y^2{+}1$	$y{+}1$	y	y^2
$y^2{+}y{+}1$	0	$y^2{+}y{+}1$	$y^2{+}1$	y	1	$y^2{+}y$	y^2	$y{+}1$

Nyní budeme uvažovat ireducibilní polynom $u \in T[y]$ stupně $n \geq 2$. Okruh $(T[x])_u$ je podle 11.6 tělesem a v dalším se budeme zabývat polynomy nad tímto tělesem, což jsou prvky okruhu $(T[y])_u[x]$. Polynomy z $(T[y])_u[x]$ mají koeficienty, jež jsou polynomy v y stupně menšího než n. Proměnnou y používáme proto, abychom u takových polynomů rozlišili koeficienty od polynomiální proměnné.

Položme $f = \pi_u$. Zobrazení $f : T[y] \to (T[y])_u$ je homomorfismus okruhů. Podle 11.1 z něj lze odvodit homomorfismus $f_x : T[y][x] \to (T[y])_u[x]$. Máme $T \subseteq T[y]$, takže $T[x] \subseteq T[y][x]$. Přitom pro $a \in T[x]$ je $f_x(a) = a$, neboť všechny koeficienty a leží v $T \subseteq T[y]$, takže se při redukci modulo $uT[y]$ nemění. Podle 11.4 pro každé $a \in T[y][x]$ a každé $\alpha \in T[y]$ platí

$$f(a(\alpha)) = fj_\alpha(a) = j_{f(\alpha)}f_x(a) = f_x(a)(f(\alpha)).$$

Pokud zvolíme $a \in T[x]$ a $\alpha \in T[y]$ tak, že bude $f(a(\alpha)) = 0$, tak podle této rovnosti bude $f(\alpha)$ kořenem polynomu $f_x(a) = a$. Taková volba je snadno uskutečnitelná — za α zvolíme y (z $n \geq 2$ plyne, že je $f(y) = y$) a polynom a zvolíme jako $\sum u_i x^i$, kde $u = \sum u_i y^i$. Pak je $a(\alpha) = \sum u_i y^i$ rovno u, a z $f(u) = 0$ plyne, že y je kořenem polynomu $a = \sum u_i x^i \in T[x] \subseteq (T[y])_u[x]$. V následujícím tvrzení můžeme proto tento fakt zaznamenat jako dokázaný.

11.7 Tvrzení. *Buď T komutativní těleso a ať $u = \sum u_i y^i$ je v $T[y]$ ireducibilní polynom stupně alespoň 2. Potom je $(T[y])_u$ komutativní těleso, které obsahuje těleso T, a polynom y (chápaný jako prvek tělesa $(T[y])_u$) je kořenem polynomu $\sum u_i x^i \in T[x]$.*

Každý polynom stupně alespoň 1 je součinem ireducibilních polynomů, a proto tvrzení 11.7 okamžitě implikuje

Použijeme-li tabulku násobení v tělese $(\mathbb{Z}_2[y])_{y^3+y+1}$ pro výpočet y^3+y+1, dostaneme nulu, neboť y^3 je roven součinu y^2 a y, což je $y+1$. Dosažený výsledek je samozřejmě v souladu s obsahem tvrzení 11.7. Důkaz tohoto tvrzení se opírá o vztah

$$f(a(\alpha)) = fj_\alpha(a) = j_{f(\alpha)}f_x(a) = f_x(a)(f(\alpha))$$

z lemmatu 11.4, který je použit pro $f = \pi_u$.
V našem příkladu je $T = \mathbb{Z}_2$ a $u = y^3+y+1$. Bude-li a rovno x^3+x+1, tak je $f_x(a) = a$, a pro každé $\alpha \in T[y]$ platí rovnost π_u-projekce polynomu $\alpha^3+\alpha+1$ (tuto projekci obdržíme jako zbytek při dělení polynomem u) a hodnoty $\pi_u(\alpha)^3+\pi_u(\alpha)+1$ počítané v $(T[y])_u$. Bude-li α polynom stupně menšího než $3 = \operatorname{st} u$, tak se $\pi_u(\alpha)$ shoduje s α. Výše jsme ověřili, že v případě $\alpha = y$ dává výpočet v $(T[y])_u$ nulu, což se rovná $\pi_u(y^3+y+1)$. Pokud bude například $\alpha = y^2$, dostaneme výpočtem v $(T[y])_u$ součet šesté, druhé a nulté mocniny y, což je součet y^2+1 s y^2 a 1, a to je také nula. Proto nulu obdržíme i jako projekci $\pi_u(y^6+y^2+1)$, což lze z odvodit z rovnosti $y^6+y^2+1 = (y^3+y+1)^2$, která v $\mathbb{Z}_2[x]$ platí díky Frobeniovu endomorfismu. Vidíme, že polynom x^3+x+1 má v našem osmiprvkovém tělese kořeny y a y^2, takže se rozkládá na kořenové činitele. Není obtížné ověřit, že posledním z kořenů je y^2+y, což je čtvrtá mocnina prvku y.
Ilustrujme vztah $f(a(\alpha)) = f_x(a)(f(a))$ ještě na příkladu, kde nedostáváme jako výsledek nulovou hodnotu. Zvolíme $\alpha = y+1$ a $a = (y^2+1)x^6+yx^5+x^2+(y^2+y+1)$. Pak je $f(a(\alpha))$ rovno $\pi_u((y^2+1)(y+1)^6+y(y+1)^5+(y+1)^2+(y^2+y+1)) = \pi(y^8+y^6+y^5-y^2+1) = \pi_u((y^3+y+1)y^5+(y^2+1)) = y^2+1$, zatímco $f_x(a)(f(\alpha))$ se spočítá dosazením $f(\alpha) = \alpha = y+1$ do $f_x(a) = a = (y^2+1)x^6+yx^5+x^2+(y^2+y+1)$ v $(\mathbb{Z}_2[y])_{y^2+y+1}$. Z tabulky násobení dostáváme $\alpha^4 = y^2+y+1$, $\alpha^5 = y$ a $\alpha^6 = y^2+y$, takže výsledná hodnota je rovna $(y^2+1)(y^2+y)+y\cdot y+(y^2+1)+(y^2+y+1) = (y+1)+y^2+(y^2+1)+(y^2+y+1) = y^2+1$, v souladu s očekáváním.

Obrázek 11.4: Dosazování v tělese řádu 8

11.8 Důsledek. *Buď T komutativní těleso a ať $u \in T[x]$ je polynom stupně* *alespoň* 1. *Potom existuje komutativní těleso* $U \supseteq T$ *takové, že* u *má v* U *alespoň jeden kořen.*

Nemalá péče věnovaná předchozím tvrzením byla vedena snahou souběžně ilustrovat, že počítání v $(T[y])_u$ je velmi podobné počítání dle číselných modulů. Pokud bychom však chtěli důsledek 11.8 dokázat co nejúsporněji, mohli bychom postupovat následovně.

Důkaz. Protože polynom u je součinem polynomů ireducibilních v $T[x]$, lze předpokládat, že je ireducibilní. Pak $I = uT[x]$ je maximální ideál a $U = T[x]/I$ je těleso. Zobrazení $t \mapsto t + I$ je homomorfismus těles $T \to U$, takže při ztotožnění t a $t + I$ můžeme T chápat jako podtěleso U. Máme tedy $T[x] \subseteq U[x]$, a dosazením $x + I$ do $u \in U[x]$ dostaneme $u + I$. Ovšem z $u \in I$ plyne $u + I = I = \mathbf{0}_U$, a proto $u(x + I) = \mathbf{0}_U$. □

Buď U komutativní těleso a T jeho podtěleso. Pro $S \supseteq U$ se podtěleso generované $T \cup S$ značí $T(S)$. Je-li $S = \{\alpha_1, \dots, \alpha_k\}$, tak vedle $T(S)$ píšeme též $T(\alpha_1, \dots, \alpha_k)$. O tělesu $T(S)$ říkáme, že vzniklo *adjunkcí* množiny S k tělesu T.

Nechť opět jsou $T \subseteq U$ do sebe vřazená komutativní tělesa, a ať $a \in T[x]$ je polynom. Těleso U se nazývá *kořenové nadtěleso* polynomu a právě když $U = T(\alpha)$ pro nějaký kořen α tohoto polynomu. Těleso U je *rozkladovým nadtělesem* polynomu a právě když a se v U rozkládá na kořenové činitele a platí $U = T(\alpha_1, \dots, \alpha_k)$, kde $\alpha_1, \dots, \alpha_k$ jsou kořeny polynomu a.

Existence kořenových nadtěles plyne z 11.8, indukcí snadno dokážeme existenci rozkladových nadtěles:

11.9 Tvrzení. *Buď* T *komutativní těleso a* $a \in T[x]$ *ať je polynom stupně alespoň* 1. *Pak existuje komutativní těleso* $U \supseteq T$ *takové, že* a *se v* $U[x]$ *rozkládá na kořenové činitele.*

Důkaz. Postupujme indukcí podle $n = \operatorname{st} a$. Je-li $n = 1$, stačí položit $U = T$. Ať je $n > 1$ a ať $V \supseteq T$ je kořenové nadtěleso polynomu a, přičemž $\alpha \in V$ je kořen a. Pak a je rovno $(x - \alpha)b$, kde $b \in V[x]$ je stupně $n - 1$. Podle indukčního předpokladu existuje komutativní těleso $U \supseteq V$, ve kterém se b (a tím pádem i a), rozkládá na kořenové činitele. □

12 Algebraické prvky a minimální polynomy

V celé této kapitole 'těleso' znamená 'komutativní těleso'.

Jestliže $U \supseteq T$ jsou komutativní tělesa, tak U můžeme chápat jako vektorový prostor nad T (sčítání je v tomto vektorovém prostoru shodné se sčítáním v U a skalární násobení $t \cdot u$, kde $t \in T$ a $u \in U$, definujeme jako součin $t \cdot u$ v tělese U).

Dimenze $\dim_T U$ vektorového prostoru U se značí $[U : T]$ a nazývá se *stupeň* tělesa U (nad T). Je-li $[U : T] < \infty$, hovoříme o *rozšíření konečného stupně.*

Zápis komplexních čísel ve tvaru $a + bi$ vyjadřuje skutečnost, že dvojice $(1, i)$ poskytuje bázi $\mathbb{C}$ nad $\mathbb{R}$, pokud $\mathbb{C}$ chápeme jako reálný vektorový prostor. Je tedy $[\mathbb{C} : \mathbb{R}] = 2$.

Obrázek 12.1: Tělesa reálných a komplexních čísel

12.1 Lemma. *Buď $T \subseteq U \subseteq V$ do sebe vřazená tělesa. Potom $[V : T] = [V : U] \cdot [U : T]$.*

Důkaz. Ať A je báze U nad T a B je báze V nad U. Stačí ukázat, že $C = \{ab;\ a \in A,\ b \in B\}$ je báze V nad T. Je-li $v \in V$, existují $u_b \in U$, že $v = \sum_{b \in B} u_b b$, a protože každé u_b lze zapsat jako $\sum_{a \in A} t_{a,b} a$, kde $t_{a,b} \in T$, tak $v = \sum t_{a,b} ab$. Naopak, ať $\sum t_{a,b} ab = 0$, kde $a \in A$, $b \in B$ a $t_{a,b} \in T$. Pak $\sum_{b \in B} (\sum_{a \in A} t_{a,b} a) b = 0$, takže pro každé $b \in B$ je $\sum_{a \in A} t_{a,b} a = 0$, a tedy $t_{a,b} = 0$ pro všechna $a \in A$, $b \in B$. □

12.2 Lemma. *Ať $S \supseteq R$ jsou komutativní okruhy a α ať je prvek S. Pak okruh $R[\alpha]$ je roven okruhu $\operatorname{Im} j_\alpha = \{a(\alpha);\ a \in R[x]\}$.*

Důkaz. $\{a(\alpha);\ a \in R[x]\} = \operatorname{Im} j_\alpha$ je podokruh S, a proto $R[\alpha] \subseteq S$. Pro $a = \sum a_i x^i \in R[x]$ je $a(\alpha) = \sum a_i \alpha^i$ jistě prvek $R[\alpha]$. □

Prvek $\alpha \in U$ se nazývá *algebraický* (nad T), jestliže $a(\alpha) = 0$ pro nějaké $a \in T[x]$, $a \neq 0$. Pokud takový polynom a neexistuje, nazýváme α *transcendentní* (nad T).

12.3 Tvrzení. *Nechť $T \subseteq U$ jsou tělesa a ať $\alpha \in U$ je prvek algebraický nad T. Pak existuje jediný monický polynom $m \in T[x]$ takový, že pro všechna $a \in T[x]$ je $a(\alpha) = 0$ právě když m dělí a. Polynom m je ireducibilní a hlavní ideál $mT[x]$ je jádrem dosazovacího homomorfismu $j_\alpha : T[x] \to U$. Zobrazení $a + mT[x] \mapsto a(\alpha)$ je izomorfismus okruhů $T[x]/mT[x]$ a $T[\alpha]$. Oba tyto okruhy jsou tělesa a platí $T[\alpha] = T(\alpha)$.*

Zkonstruujme příklad tělesa $U \supseteq \mathbb{Q}$, pro které platí $[U:\mathbb{Q}] = 3$. Ať $U = \{a+b\sqrt[3]{2}+c\sqrt[3]{4};\, a,b,c \in \mathbb{Q}\}$. Máme $(a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4})(a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4}) = (a_1a_2+2b_1c_2+2c_1b_2)+(a_1b_2+b_1a_2+2c_1c_2)\sqrt[3]{2}+(a_1c_2+c_1a_2+b_1b_2)\sqrt[3]{4}$, takže U je podmnožina $\mathbb{R}$, jež je uzavřena na součiny. Protože je zjevně uzavřena i na součty, je to podokruh $\mathbb{C}$. Abychom si mohli být jisti, že U je těleso, potřebujeme ještě ověřit, že pro každé nenulové $u \in U$ padne do U i u^{-1}.

Nejprve však nahlédneme, že pokud je $u = a+b\sqrt[3]{2}+c\sqrt[3]{4}$, kde a, b a c jsou racionální čísla, tak je a, b i c určeno jednoznačně. Pokud by tomu tak nebylo, tak by existovala $a,b,c \in \mathbb{Q}$ taková, že alespoň jedno je nenulové a že $c\cdot(\sqrt[3]{2})^2 + b\cdot(\sqrt[3]{2}) + a = 0$. Hodnota $\sqrt[3]{2}$ je kořenem polynomu $x^3-2 \in \mathbb{Q}[x]$. Polynom x^3-2 má v $\mathbb{C}$ tři vesměs různé kořeny, z nichž jenom jeden je reálný. Proto musí být největší společný dělitel polynomů x^3-2 a cx^2+bx+a roven $x-\sqrt[3]{2}$. Protože ale tento největší společný dělitel je možno spočítat v $\mathbb{Q}[x]$, musí být $\sqrt[3]{2}$ číslo racionální. To je spor, a tím je jednoznačnost vyjádření $u \in U$ dokázána. Předpokládejme, že $u = a+b\sqrt[3]{2}+c\sqrt[3]{4} \neq 0$, kde $a,b,c \in \mathbb{Q}$. Víme, že je $(a,b,c) \neq (0,0,0)$, a snadno ověříme, že pak je i $(a^2-2bc, 2c^2-ab, b^2-ac) \neq (0,0,0)$. Položme $v = (a^2-2bc)+(2c^2-ab)\sqrt[3]{2}+(b^2-ac)\sqrt[3]{4}$. Protože $u \neq 0$ i $v \neq 0$, stačí ukázat, že uv je racionální číslo, neboť pak máme $u^{-1} = v\cdot(uv)^{-1} \in U$. Jelikož $uv = a^3+2b^3+4c^3-6abc$ opravdu racionální je, můžeme vskutku tvrdit, že U je těleso.

Z jednoznačnosti volby (a,b,c) vyplývá, že $(1, \sqrt[3]{2}, \sqrt[3]{4})$ je bází U nad $\mathbb{Q}$, takže $[U:\mathbb{Q}] = 3$. Těleso U je zjevně rovno nejmenšímu podtělesu $\mathbb{C}$, které současně obsahuje $\mathbb{Q}$ i $\sqrt[3]{2}$, a proto ho můžeme identifikovat jako $\mathbb{Q}(\sqrt[3]{2})$.

Zde provedené výpočty odpovídají situaci, ve které není k dispozici prakticky žádná teorie algebraických rozšíření. V této kapitole jsou učiněny prvé kroky k vybudování takové teorie. Uvidíme, že většinu dokázaných faktů je možno odvodit okamžitě z toho, že U je kořenovým nadtělesem polynomu x^3-2.

Obrázek 12.2: Rozšíření racionálních čísel stupně tři

> *Předpokládejme, že je dáno nějaké těleso U, jež splňuje $\mathbb{Q} \subseteq U \subseteq \mathbb{R}$. Položme $V = \{s + it;\ s,t \in U\}$. Pak $(s+it)(s-it) = s^2 + t^2 \in U$ pro všechna $s,t \in U$, z čehož vidíme, že v okruhu V leží i inverzní prvky, takže jde o podtěleso $\mathbb{C}$. Máme $[V : U] = 2$ a podle lemmatu 12.1 je $[V : \mathbb{Q}] = 2[U : \mathbb{Q}]$. Je-li U konečného stupně, je konečného stupně i V. Ať je $U = \mathbb{Q}(\sqrt[3]{2})$, jako výše. Pak $[U : \mathbb{Q}] = 3$ a $[V : \mathbb{Q}] = 6$. Jednou z možných bází U nad $\mathbb{Q}$ je $(1, \sqrt[3]{2}, \sqrt[3]{4})$, zatímco za bázi V nad U lze zvolit $(1, i)$. Z důkazu 12.1 plyne, že $(1, \sqrt[3]{2}, \sqrt[3]{4}, i, i\sqrt[3]{2}, i\sqrt[3]{4})$ je bází V nad $\mathbb{Q}$. Nyní je snadné dokázat, že $V = \mathbb{Q}(i\sqrt[3]{2})$.*

Obrázek 12.3: Vnořená tělesa malých stupňů

Důkaz. Pro $a \in T[x]$ platí $a(\alpha) = 0$ právě když je $j_\alpha(a) = 0$. Jádro homomorfismu j_α je vlastní ideál, a z kapitoly 10 víme, že každý vlastní ideál lze jednoznačným způsobem vyjádřit jako hlavní ideál generovaný monickým polynomem.

Ať m dělí pq, kde $p, q \in T[x]$ jsou polynomy. Pak $0 = m(\alpha) = p(\alpha)q(\alpha)$, takže je $p(\alpha) = 0$ nebo $q(\alpha) = 0$. Čili m dělí p nebo q, takže vidíme, že m je prvočinitel, a tedy ireducibilní polynom.

Podle 12.2 je $\operatorname{Im} j_\alpha$ rovno $T[\alpha]$, takže j_α je surjektivní homomorfismus $T[x]$ na $T[\alpha]$. Podle první věty o izomorfismu 7.10 je zobrazení $a + mT[x] \mapsto a(\alpha)$ izomorfismem okruhů $T[x]/mT[x]$ a $T[\alpha]$. Protože $mT[x]$ je maximální ideál (viz 10.12), tak je okruh $T[x]/mT[x]$ tělesem (viz 7.14), a proto je i okruh $T[\alpha]$ těleso. Protože $T(\alpha)$ je nejmenší podtěleso U, které obsahuje $T[\alpha]$, musí být $T(\alpha) = T[\alpha]$. □

Polynom m z Tvrzení 12.3 se nazývá *minimální polynom* prvku α (nad T) a značí se m_α.

12.4 Tvrzení. *Buď $\alpha \in U \supseteq T$. Pak α je algebraický nad T právě když $[T(\alpha) : T] < \infty$. Je-li α algebraický nad T, tak $T(\alpha) = T[\alpha]$ a $[T[\alpha] : T] = \operatorname{st} m_\alpha$.*

Důkaz. Ať $[T(\alpha) : T] = n$. Je-li $n < \infty$, jsou $1, \alpha, \dots, \alpha^n$ prvky nad T lineárně závislé, takže existují $c_0, c_1, \dots, c_n$ prvky T takové, že $\sum c_i \alpha^i = 0$ a $c_j \neq 0$ pro alespoň jedno $0 \leq j \leq n$. Tudíž $c(\alpha) = 0$ pro $0 \neq c = \sum c_i x^i$, takže α je algebraický nad T.

Naopak, ať $\alpha \in U$ je algebraický nad T a $s = \operatorname{st} m_\alpha$. Ukážeme, že $1, \alpha, \dots, \alpha^{s-1}$ tvoří bázi $T[\alpha] = T(\alpha)$. Je-li $c \in T[x]$, $\operatorname{st} c \leq s - 1$, tak $c(\alpha) = 0$ jedině pro $c = 0$.

Budeme počítat minimální polynomy některých komplexních a reálných čísel nad tělesem racionálních čísel.
Protože i je kořenem polynomu x^2+1 a tento polynom je v $\mathbb{R}[x]$ (a tím spíše v $\mathbb{Q}[x]$) ireducibilní, je $m_i = x^2+1$. Podobně $m_{-i} = x^2+1$.
Je-li $\alpha = \sqrt[3]{2}$, tak je $m_\alpha = x^3 - 2$, neboť $\sqrt[3]{2}$ je kořenem polynomu $x^3 - 2 \in \mathbb{Q}[x]$, a tento polynom je v $\mathbb{Q}[x]$ ireducibilní, neboť je stupně 3 a nemá racionální kořeny.
Položme ještě $\theta_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$, kde $n \geq 2$. Pak $(\theta_n)^n = 1$, takže θ_n je kořenem polynomu $x^n - 1$. Nikdy ovšem neplatí $m_{\theta_n} = x^n - 1$, neboť $x^n - 1 = (x-1)(x^{n-1} + \cdots + 1)$ není ireducibilní. Polynom m_{θ_n} se značívá t_n a nazývá se n-tý cyklotomický (kruhový) polynom. Lze dokázat, že $t_n = (x^n - 1)/\prod_m (x^m - 1)$, kde součin probíhá přes všechna m, jež dělí n. Také platí $t_n = \prod_i (x - \theta_n^i)$, kde i nabývá všech kladných hodnot nesoudělných s n a menších než n. Je tedy $\operatorname{st} t_n = \varphi(n)$. Cyklotomické polynomy a jejich kořenová nadtělesa mají velký význam v teorii čísel.

Obrázek 12.4: Příklady minimálních polynomů

Proto jsou $1, \alpha, \ldots, \alpha^{s-1}$ lineárně nezávislé. Je-li $\beta \in T[\alpha]$, tak existuje $b \in T[x]$, že $\beta = b(\alpha)$. Ovšem $b = m_\alpha q + r$, kde $q, r \in T[x]$, $r = \sum r_i x^i$ a $\operatorname{st} r < \operatorname{st} m_\alpha = s$, takže $\beta = b(\alpha) = r(\alpha) = \sum_{1 \leq i \leq s-1} r_i \alpha^i$. $\square$

Ať $T \subseteq U$ jsou tělesa. U nazveme *algebraickým rozšířením* T, jestliže každý prvek $\beta \in U$ je algebraický nad T.

12.5 Důsledek. *Každé rozšíření konečného stupně U tělesa T je algebraické rozšíření.*

Důkaz. Buď $\beta \in U$. Podle 12.1 je $[U : T] = [U : T(\beta)] \cdot [T(\beta) : T]$, takže $[T(\beta) : T]$ je konečné číslo. Podle 12.4 je β algebraický prvek. $\square$

12.6 Tvrzení. *Ať $T \subseteq U$ jsou tělesa a $\alpha_1, \ldots, \alpha_n \in U$ jsou algebraické nad T. Potom $V = T(\alpha_1, \ldots, \alpha_n)$ je konečné algebraické rozšíření T a $V = T[\alpha_1, \ldots, \alpha_n]$.*

Důkaz. Položme $T_0 = T$ a $T_i = T[\alpha_1, \ldots, \alpha_i]$, $1 \leq i \leq n$. Indukcí ukážeme, že T_i je těleso a že pro $i \geq 1$ je $[T_i : T_{i-1}]$ konečné. Pro $i = 0$ není co dokazovat,

> *Rozšíření $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ je algebraické. Proto je každý prvek $\beta \in \mathbb{Q}(\sqrt[3]{2})$ kořenem nějakého polynomu $b \in \mathbb{Q}[x]$. Ukažme existenci takového polynomu například pro $\beta = 1+\sqrt[3]{2}$. Pak lze zvolit $b = x^3-3x^2+3x-9 = (x-1)^3-8$. Lze formulovat obecnou metodu, jak takový polynom nalézt; zde to však dělat nebudeme.*

Obrázek 12.5: Polynom algebraického prvku

ať $0 \leq i \leq n-1$. Pak $T_{i+1} = T_i[\alpha_{i+1}]$, přičemž α_{i+1} je algebraický nad $T_i \supseteq T$. Podle 12.3 je T_{i+1} těleso a podle 12.4 je $[T_{i+1} : T_i]$ konečné.

Tudíž $V = T_n$, V je rozšíření konečného stupně, a to je podle 12.5 algebraické. $\square$

12.7 Důsledek. *Ať $U \supseteq T$ je rozkladové nadtěleso polynom $a \in T[x]$ a ať $\alpha_1, \ldots, \alpha_n \in U$ jsou všechny kořeny a. Pak $U = T[\alpha_1, \ldots, \alpha_n]$.*

Následující tvrzení je z předchozího již víceméně samozřejmé. Přesto ho raději uvedem výslovně.

12.8 Tvrzení. *Stupeň $[U : T]$ kořenového nadtělesa U ireducibilního polynomu $a \in T[x]$ je roven $\operatorname{st} a$. Pokud je $\alpha \in U$ kořenem a, přičemž polynom a je monický, tak je a rovno minimálnímu polynomu α nad T a platí $U = T(\alpha)$.*

Důkaz. Bez újmy na obecnosti lze předpokládat, že polynom a je monický. Ať je $\alpha \in U$ nějaký kořen polynomu a. Pak musí být $a = m_\alpha$, neboť m_α dělí polynom a, a tento je ireducibilní a monický. Z tvrzení 12.4 plyne $[T(\alpha) : T] = \operatorname{st} a$. Máme $U \supseteq T(\alpha) \supseteq T$. Podle předpokladu lze zvolit takový kořen β polynomu a, že $U = T(\beta)$. Proto $[U : T] = \operatorname{st} a$ a $U = T(\alpha)$. $\square$

13 Jednoznačnost kořenových a rozkladových nadtěles

13.1 Lemma. *Ať $f : R \simeq S$ je izomorfismus okruhů a ať $I \subseteq R$ a $J \subseteq S$ jsou ideály takové, že $f(I) = J$. Potom zobrazení $a + I \mapsto f(a) + J$ je korektně definované a je to izomorfismus $R/I \simeq S/J$.*

Důkaz. $\mathrm{nat}_J f : R \to S/J$ je surjektivní homomorfismus, který zobrazuje prvek $a \in R$ na $f(a) + J$. Jeho jádrem je ideál I, a proto podle 1. věty o izomorfismu (7.10) je $a + I \mapsto f(a) + J$ izomorfismus R/I a S/J. □

13.2 Lemma. *Buď $f : T \simeq S$ izomorfismus komutativních těles a ať $I \subseteq T[x]$ a $J \subseteq S[x]$ jsou nenulové ideály, pro které platí $f_x(I) = J$. Jsou-li $a \in T[x]$ a $b \in S[x]$ ty (jednoznačně určené) monické polynomy, které splňují $I = aT[x]$ a $J = bS[x]$, tak platí $f_x(a) = b$.*

Důkaz. $bS[x] = J = f_x(I) = f_x(aT[x]) = f_x(a)f_x(T[x]) = f_x(a)S[x]$ a $f_x(a)$ je monický polynom. Víme (viz kapitola 10), že ideál J je generován právě jedním monickým polynomem. Proto se $f_x(a)$ musí rovnat b. □

13.3 Tvrzení. *Buďte $T \subseteq U$ a $S \subseteq V$ komutativní tělesa, $f : T \simeq S$ izomorfismus a ať $\alpha \in U$ je prvek algebraický nad T a $\beta \in V$ prvek algebraický nad S. Izomorfismus $g : T[\alpha] \simeq S[\beta]$ splňující $g(\alpha) = \beta$ a $g(t) = f(t)$ pro všechna $t \in T$ existuje právě když $f_x(m_\alpha) = m_\beta$.*

Důkaz. Předpokládejme nejprve, že platí $f_x(m_\alpha) = m_\beta$. S využitím 12.3 a 13.1 sestrojíme řadu izomorfismů

$$T[\alpha] \simeq T[x]/m_\alpha T[x] \simeq S[x]/m_\beta S[x] \simeq S[\beta].$$

Oba krajní izomorfismy vyjadřují skutečnost, že každé kořenové nadtěleso algebraického prvku je strukturálně shodné s kvocientem podle hlavního ideálu příslušného minimálního polynomu (toto pozorování je obsahem Tvrzení 12.3). Prostřední izomorfismus je pak přímou aplikací 13.1, kde se říká, že izomorfismus okruhů (zde je to izomorfismus f_x) lze přenést na izomorfismus kvocientních okruhů, jestliže faktorizujeme přes ideály, které si v daném izomorfismu jednoznačně odpovídají (zde to jsou hlavní ideály generované polynomy m_α a m_β).

Proveďme nyní naznačený postup podrobně. Podle Tvrzení 12.3 jsou zobrazení $u : T[x]/m_\alpha T[x] \to T[\alpha]$ a $v : S[x]/m_\beta S[x] \to S[\beta]$, jež jsou definována vztahy $u(a + m_\alpha T[x]) = a(\alpha)$ a $v(b + m_\beta S[x]) = b(\beta)$, izomorfismy. Protože f_x je podle 11.3 izomorfismus $T[x]$ a $S[x]$ a protože podle předpokladu je $f_x(m_\alpha T[x]) = m_\beta S[x]$, dostáváme z 13.1 izomorfismus $w : T[x]/m_\alpha T[x] \simeq S[x]/m_\beta S[x]$, $w(a + m_\alpha T[x]) = f_x(a) + m_\beta S[x]$.

Jako vhodný kandidát se na místo hledaného izomorfismu g nabízí vwu^{-1}. Stačí ověřit, že je $vwu^{-1}(\alpha) = \beta$ a že $vwu^{-1}(t) = f(t)$ pro každé $t \in T$. Z definic izomorfismů v, w a u ale skutečně dostáváme $vwu^{-1}(t) = vw(t + m_\alpha T[x]) =$

$v(f(t) + m_\beta S[x]) = f(t)$. Protože $x(\alpha) = \alpha$ a $x(\beta) = \beta$, tak $vwu^{-1}(\alpha) = vw(x + m_\alpha T[x]) = v(x + m_\beta S[x]) = \beta$, a lze tedy položit $g = vwu^{-1}$. Nyní naopak předpokládejme, že existuje izomorfismus $g : T[\alpha] \simeq S[\beta]$, který je rozšířením $f : T \simeq S$, a splňuje $g(\alpha) = \beta$. Uvažme dosazovací homomorfismy $j_\alpha : T[\alpha][x] \to T[\alpha]$ a $j_\beta : S[\beta][x] \to S[\beta]$. Podle 11.4 je $j_\beta g_x = g j_\alpha$:

$$\begin{array}{ccc} T[x] \subseteq T[\alpha][x] & \xrightarrow{g_x} & S[\beta][x] \supseteq S[x] \\ {\scriptstyle j_\alpha}\big\downarrow & & \big\downarrow{\scriptstyle j_\beta} \\ T \subseteq T[\alpha] & \xrightarrow{g} & S[\beta] \supseteq S \end{array}$$

Pro $a \in T[x]$ je jistě $f_x(a) = g_x(a)$, neboť g je rozšířením f. Pro $a \in T[x]$ tedy platí $a \in m_\alpha T[x] \Leftrightarrow a(\alpha) = 0 \Leftrightarrow j_\alpha(a) = 0 \Leftrightarrow g j_\alpha(a) = 0 \Leftrightarrow j_\beta g_x(a) = 0 \Leftrightarrow (g_x(a))(\beta) = 0 \Leftrightarrow (f_x(a))(\beta) = 0 \Leftrightarrow f_x(a) \in m_\beta S[x]$. Polynom a tedy patří do ideálu $m_\alpha T[x]$ právě když $f_x(a)$ patří do ideálu $m_\beta S[x]$, takže $f_x(m_\alpha T[x]) = m_\beta S[x]$. Podle 13.2 je $f_x(m_\alpha)$ rovno m_β. □

13.4 Věta. *Buď $f : T \simeq S$ izomorfismus komutativních těles, $a \in T[x]$,* st $a \geq 1$, *a ať $U \supseteq T$ je rozkladové nadtěleso polynomu $a \in T[x]$, zatímco $V \supseteq S$ je rozkladové nadtěleso polynomu $b = f_x(a)$. Ať $\alpha_1, \dots, \alpha_m$ jsou kořeny a v U a $\beta_1, \dots, \beta_n$ kořeny b ve V. Pak $m = n$ a existuje permutace $\sigma \in S_n$ a izomorfismus $g : U \simeq V$ tak, že $g(t) = f(t)$ pro všechna $t \in T$ a $g(\alpha_i) = \beta_{\sigma(i)}$ pro $1 \leq i \leq n$.*

Důkaz. Ať $a = p_1^{k_1} \dots p_r^{k_r}$ je rozklad polynomu a na ireducibilní činitele v $T[x]$. Položme $q_i = f_x(p_i)$, $1 \leq i \leq k$. Pak $b = q_1^{k_1} \dots q_r^{k_r}$ je podle 11.3 rozklad na ireducibilní činitele v $S[x]$. Důkaz provedem indukcí podle $[U : T]$. Je-li $U = T$, lze kořeny uspořádat tak, že $p_i = x - \alpha_i$ a $q_i = x - \beta_i$, $1 \leq i \leq r$, takže stačí položit $g = f$. Ať je $[U : T] = j > 0$ a ať věta platí pro každý stupeň menší než j. Kořeny a polynomy jistě můžeme uspořádat tak, aby α_1 byl kořen p_1 a β_1 kořen q_1, a aby $\operatorname{st} p_1 = \operatorname{st} q_1 > 1$. Podle 13.3 existuje izomorfismus $h : T(\alpha_1) \to S(\beta_1)$ takový, že $h(\alpha_1) = \beta_1$ a $h(t) = f(t)$ pro každé $t \in T$. Protože $[U : T] = [U : T(\alpha_1)] \cdot [T(\alpha_1) : T] = [U : T(\alpha_1)] \cdot \operatorname{st} p_1$ (viz 12.1 a 12.3), je $[U : T(\alpha_1)] < j$. U je rozkladové nadtěleso polynomu $a \in T(\alpha_1)[x]$ a V je rozkladové nadtěleso polynomu $b \in S(\beta_1)[x]$. Podle indukčního předpokladu existuje izomorfismus $g : U \to V$, který má požadované vlastnosti a rozšiřuje h, a tím i f. □

13.5 Věta. *Nechť q je přirozené číslo. Konečné komutativní těleso řádu q existuje právě když q je rovno p^n pro některé prvočíslo p a nějaké přirozené n. V takovém* *případě jsou všechna komutativní tělesa řádu q izomorfní rozkladovému nadtělesu polynomu $x^{q-1} - 1 \in \mathbb{Z}_p[x]$, takže až na izomorfismus existuje jediné komutativní těleso řádu q.*

Důkaz. Ať T je těleso řádu q a ať P je jeho prvotěleso. Podle tvrzení 9.14 je $P \cong \mathbb{Z}_p$ pro vhodné prvočíslo p. Položme $n = [T : P]$. Pak T lze chápat jako n-rozměrný vektorový prostor nad p-prvkovým tělesem P, takže $q = |T| = p^n$. Podle 10.19 je grupa T^* cyklická. Její řád je roven $q-1$, takže pro každé $\alpha \in T^*$ platí $\alpha^{q-1} - 1 \in P[x]$. Těleso T je tudíž rozkladovým nadtělesem tohoto polynomu a z $P \cong \mathbb{Z}_p$ podle věty 13.4 vyplývá, že libovolná dvě komutativní konečná tělesa řádu q jsou izomorfní.

Ještě jsme však neukázali, že těleso řádu p^n existuje. Z 11.9 dostáváme existenci rozkladového nadtělesa U polynomu $x^{p^n} - x \in \mathbb{Z}_p[x]$. Množina $M = \{a \in U;\ a^{p^n} = a\}$ je rovna množině všech kořenů tohoto polynomu, a podle 10.16 má p^n prvků. Podle 7.22 je M podtěleso U (takže platí $M = U$). □

13.6 Důsledek. *Pro každé prvočíslo p a každé přirozené $n \geq 1$ existuje ireducibilní polynom $a \in \mathbb{Z}_p[x]$, který je stupně n.*

Důkaz. Uvažme těleso T řádu p^n a ať ξ je nějaký generátor cyklické grupy T^*. Můžeme předpokládat, že prvotěleso T je rovno $\mathbb{Z}_p$. Máme $T = \mathbb{Z}_p[\xi]$ a $[T : \mathbb{Z}_p] = n$. Podle 12.4 je $n = \operatorname{st} m_\xi$. □

Generátor ξ cyklické grupy T^* je zvykem nazývat *primitivní prvek*. Podle 8.7 je počet primitivních prvků tělesa T roven $\varphi(p^n - 1)$ (kde φ je Eulerova funkce).

Komutativní těleso T řádu p^n se často značí $\mathbb{F}_q$ nebo $GF(p^n)$, kde GF je zkratka z 'Galois field'. Lze se dohodnout, že $GF(p)$ je rovno $\mathbb{Z}_p$. Ovšem pro $n > 1$ se už žádný kanonický tvar $GF(p^n)$ nezavádí.

14 Modulární, distributivní a komplementární svazy

14.1 Lemma. *Buď $L = L(\wedge, \vee)$ svaz a ať jsou $a, b, c \in L$. Je-li $a \leq c$, je $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.*

Důkaz. $a \leq a \vee b$ a $a \leq c$, proto $a \leq (a \vee b) \wedge c$. Současně $b \wedge c \leq a \vee b$, $b \wedge c \leq c$, takže $b \wedge c \leq (a \vee b) \wedge c$. □

Vraťme se k tělesu $(\mathbb{Z}_2[y])_{y^3+y+1})$, kterým jsme se zabývali v kapitole 11. Jako mocniny prvku y postupně dostáváme y, y^2, $y+1$, y^2+y, y^2+y+1, y^2+1, 1. Vidíme, že y je primitivní prvek tohoto tělesa. Primitivních prvků je $\varphi(8-1)=6$ a jsou jimi všechny prvky různé od 0 a 1 (tak je tomu vždy, když je p^n-1 prvočíslo.)
Dané těleso je podle 13.5 rozkladovým nadtělesem polynomu x^8-x. Ten se v $\mathbb{Z}_2[x]$ rozkládá na $x(x-1)(x^3+x+1)(x^3+x^2+1)$, přičemž činitelé tohoto rozkladu jsou všechny ireducibilní polynomy ze $\mathbb{Z}_2[x]$, které jsou stupně ≤ 3. (Obecně se $x^{p^n}-x$ rozkládá na součin všech ireducibilních polynomů ze $\mathbb{Z}_p[x]$, které jsou stupně $\leq n$.)
Polynom x^3+x+1 je minimální polynom primitivních prvků y, y^2 a y^2+y, zatímco x^3+x^2+1 je minimálním polynomem primitivních prvků $y+1$, y^2+y+1 a y^2+1.

Obrázek 13.1: Primitivní prvky osmiprvkového tělesa

Poznámka. Zkusme získat duální nerovnost k nerovnosti $a\vee(b\wedge c)\leq(a\vee b)\wedge c$ ($\vee$ a $\wedge$ prohodíme a $\leq$ zaměníme za $\geq$). Ta bude znít, že z $a\geq c$ plyne $a\wedge(b\vee c)\geq(a\wedge b)\vee c$. Vyměníme-li a a c, dostaneme, že z $a\leq c$ plyne $c\wedge(b\vee a)\geq(c\wedge b)\vee a$. To ovšem je naše původní nerovnost, čili jsme neobdrželi žádný nový vztah. Uvedená nerovnost je samoduální.

14.2 Tvrzení. *Buď $L=L(\wedge,\vee)$ svaz. Potom jsou následující podmínky ekvivalentní.*

(i) $a\vee(b\wedge c)=(a\vee b)\wedge c$, *kdykoliv* $a,b,c\in L$ *a* $a\leq c$.
(ii) $(a\wedge c)\vee(b\wedge c)=((a\wedge c)\vee b)\wedge c$ *pro všechna* $a,b,c\in L$.
(iii) $(a\vee c)\wedge(b\vee c)=((a\vee c)\wedge b)\vee c$ *pro všechna* $a,b,c\in L$.

Důkaz. (i) $\Longleftrightarrow$ (ii): Položíme-li $a'=a\wedge c\leq c$, bude mít identita (ii) tvar $a'\vee(b\wedge c)=(a'\vee b)\wedge c$.

(i) $\Longleftrightarrow$ (iii): Položíme-li $c'=a\vee c\geq c=a'$, získá identita (iii) tvar $c'\wedge(b\vee a')=(c'\wedge b)\vee a'$. □

Svaz, který vyhovuje ekvivalentním podmínkám tvrzení 14.2, se nazývá *modulární.*

14.3 Lemma. *Buď a, b, c prvky svazu L, $a \leq c$. Je-li $a \leq b$ nebo $b \leq c$, platí $a \vee (b \wedge c) = (a \vee b) \wedge c$.*

Důkaz. Stačí ukázat $a \vee (b \wedge c) \geq (a \vee b) \wedge c$. Ať nejprve $b \geq a$. Pak $a \vee (b \wedge c) \geq b \wedge c = (a \vee b) \wedge c$. Pokud $b \leq c$, tak dostáváme $a \vee (b \wedge c) = a \vee b \geq (a \vee b) \wedge c$. □

Na množině $\{0, 1, u, v, w\}$ definujeme uspořádání tak, že u a v pokrývají 0, w pokrývá v a 1 pokrývá w a u. Takto definované uspořádání dává svaz, a ten se obvykle značí N_5. (Nakreslete si Hasseův diagram!).

14.4 Tvrzení. *Svaz L je modulární právě když neobsahuje podsvaz izomorfní svazu N_5.*

Důkaz. Svaz N_5 modulární není, neboť $v \vee (u \wedge w) = v$, zatímco $(v \vee u) \wedge w = w$. Proto L, je-li modulární, nemůže obsahovat podsvaz izomorfní s N_5.

Není-li L modulární, lze najít $a, b, c \in L$, že $a \leq c$ a $a \vee (b \wedge c) < (a \vee b) \wedge c$. Ukážeme, že $\{b \wedge c, a \vee (b \wedge c), (a \vee b) \wedge c, a \vee b, b\}$ tvoří podsvaz izomorfní s N_5. Z $b \wedge c = a \vee (b \wedge c)$ plyne $a \leq b \wedge c$, odkud $a \leq b$. Z $a \vee b = (a \vee b) \wedge c$ dostáváme $a \vee b \leq c$, takže $b \leq c$. Ovšem podle 14.3 neplatí ani $a \leq b$ ani $b \leq c$. Proto $b \wedge c < a \vee (b \wedge c) \leq (a \vee b) \wedge c < a \vee b$ a $b \wedge c < b < a \vee b$. Tím jsou dány operace $\wedge$ a $\vee$ na uvedených řetězcích. Zbývá určit $b \wedge x$ a $b \vee x$, kde $x \in \{a \vee (b \wedge c), (a \vee b) \wedge c\}$. Platí $b \wedge c \leq b \wedge (a \vee (b \wedge c)) \leq b \wedge ((a \vee b) \wedge c) = (b \wedge c) \wedge (a \vee b) \leq b \wedge c$, takže $b \wedge c = b \wedge (a \vee (b \wedge c)) = b \wedge ((a \vee b) \wedge c)$. Obdobně $b \vee a \geq b \vee ((a \vee b) \wedge c) \geq b \vee a \vee (b \wedge c) = b \vee a$. □

Modulární svazy jsou v matematice velmi důležité. Bez důkazu uvedeme jednu jejich typickou vlastnost: Jestliže $a = a_0 < \cdots < a_k = b$ a $c = c_0 < \cdots < c_r = d$ jsou dvě posloupnosti prvků modulárního svazu, kde každý člen posloupnosti pokrývá člen předchozí, tak z $a = c$ a $b = d$ plyne $r = k$. (V konečném modulárním svazu tedy platí, že každé dvě cesty v Hasseově diagramu mezi dvěma prvky jsou stejně dlouhé – pokud se ovšem pohybujeme pouze zdola nahoru nebo pouze zeshora dolů.)

14.5 Tvrzení. *Buď G grupa a A a B její podgrupy. Je-li A normální v G, tak podgrupa generovaná $A \cup B$ je rovna $AB = BA$. Svaz normálních podgrup G je modulární.*

Důkaz. Podgrupu generovanou $A \cup B$ označíme $A \vee B$. Uvažme množinu AB. Jsou-li $a_i \in A$, $b_i \in B$, $i = 1, 2$, tak $a_1 b_1 a_2 b_2 = a_1 b_1 a_2 b_1^{-1} b_1 b_2$, přičemž $b_1 a_2 b_1^{-1} \in A$. Proto je množina AB uzavřená na binární operaci $\cdot$. Dále $(a_1 b_1)^{-1} = b_1^{-1} a_1^{-1} = b_1^{-1} a_1^{-1} b_1 b_1^{-1} \in AB$.

Buď nyní A, B, C normální podgrupy G, $A \subseteq C$. Je třeba ukázat $A \vee (B \cap C) \supseteq (A \vee B) \cap C$, čili $A(B \cap C) \supseteq (AB) \cap C$. Je-li $a \in A$, $b \in B$ a $ab \in C$, je $b = a^{-1}(ab) \in C$, takže $b \in B \cap C$. □

14.6 Tvrzení. *Buď L svaz. Potom jsou následující podmínky ekvivalentní.*

(i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ *pro všechna* $a, b, c \in L$.
(ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *pro všechna* $a, b, c \in L$.
(iii) $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$ *pro všechna* $a, b, c \in L$.

Přitom svaz splňující tyto podmínky je modulární.

Důkaz. (i) $\Longrightarrow$ (ii) : $(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge ((a \wedge b) \vee c) = a \wedge ((a \vee c) \wedge (b \vee c)) = (a \wedge (a \vee c)) \wedge (b \vee c) = a \wedge (b \vee c)$.

(ii) $\Longrightarrow$ (i) : Identity (i) a (ii) jsou duální. V předchozím důkazu tedy stačí zaměnit $\wedge$ a $\vee$.

(i+ii) $\Longrightarrow$ (iii) : $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \wedge (b \vee c)) \vee (b \wedge c) = ((a \wedge (b \vee c)) \vee b) \wedge ((a \wedge (b \vee c)) \vee c) = ((a \vee b) \wedge (b \vee c)) \wedge ((a \vee c) \wedge (b \vee c)) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$.

(iii) $\Longrightarrow$ (i) : Nejprve ukážeme modularitu. Je-li $a \leq c$, dostáváme $a \vee (b \wedge c) = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c) = (a \vee b) \wedge c$. Buď nyní $a, b, c \in L$ libovolná. Položme $u = (a \wedge b) \vee (b \wedge c) \vee (a \wedge c)$. Pak $a \wedge (b \vee c) = a \wedge u = (((a \wedge b) \vee (a \wedge c)) \vee (b \wedge c)) \wedge a = ((a \wedge b) \vee (a \wedge c)) \vee (b \wedge c \wedge a) = (a \wedge b) \vee (a \wedge c)$. □

Svazy, které splňují ekvivalentní podmínky tvrzení 14.6 se nazývají *distributivní* a vztahy (i) a (ii) se nazývají distributivními zákony.

Na množině $\{0, u, v, w, 1\}$ definujme svaz tak, že 0 je nejmenší prvek, 1 největší prvek, $u \wedge v = u \wedge w = v \wedge w = 0$ a $1 = u \vee v = u \vee w = v \vee w$. Tento svaz se obvykle značí M_5. Často se mu říká 'diamant'.

M_5 zjevně není distributivní. Proto žádný distributivní svaz neobsahuje podsvaz izomorfní N_5 nebo M_5. Platí i obrácené tvrzení.

14.7 Tvrzení. *Svaz L je distributivní právě když neobsahuje podsvaz izomorfní N_5 nebo M_5.*

Nástin důkazu. Potřebujeme ukázat, že pokud modulární svaz není distributivní, lze v něm nalézt M_5. Není-li L distributivní, lze najít $x, y, z \in L$ takové, že $r = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z) \wedge (y \vee z) = s$. Pak $r < s$ a pro $a = (x \wedge s) \vee r$, $b = (y \wedge s) \vee r$, $c = (z \wedge s) \vee r$ lze s trochou počítání pomocí modulárního zákona ukázat, že $a \wedge b = r$ a $a \vee b = s$. Ze symetrie pak vyplyne, že $a \wedge c = r = b \wedge c$ a $a \vee c = s = b \vee c$. Zbytek je již snadný. □

Buď $L = L(\wedge, \vee, \mathbf{0}, \mathbf{1})$ 0,1–svaz, a ať $a \in L$. Potom $b \in L$ nazveme *komplementem* (doplňkem), jestliže $a \wedge b = 0$ a $a \vee b = 1$. Z definice plyne, že je-li b komplementem a, je a komplement b.

14.8 Tvrzení. *Buď L distributivní 0,1–svaz. Potom má každý prvek nejvýše jeden komplement.*

Důkaz. Buď b a c komplementy a. Pak $b = b \wedge \mathbf{1} = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = b \wedge c$. Tudíž $b \geq c$. Obdobně dostaneme $b \leq c$, a tedy $b = c$. □

V N_5 má každý prvek komplement, ale tento komplement nemusí být jednoznačný. Totéž platí o M_5. Představme si, že v distributivním 0,1–svazu L má každý prvek komplement. Pak je jednoznačně určena unární operace $'$ taková, že pro všechna $a \in L$ je $a \wedge a' = \mathbf{0}$ a $a \vee a' = \mathbf{1}$.

Algebra $L = L(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$, kde $L(\vee, \wedge, \mathbf{0}, \mathbf{1})$ je distributivní 0,1–svaz a $'$ je unární operace, která vyhovuje identitám $a \wedge a' = \mathbf{0}$ a $a \vee a' = \mathbf{1}$, se nazývá *Booleova algebra.*

14.9 Lemma. *Ať $L = L(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ je Booleova algebra. Potom*

(i) $(a')' = a$ *pro všechna* $a \in L$.

(ii) $\mathbf{0}' = \mathbf{1}$ *a* $\mathbf{1}' = \mathbf{0}$.

(iii) $(a \wedge b)' = a' \vee b'$ *a* $(a \vee b)' = a' \wedge b'$ *pro všechna* $a, b \in A$. *(De Morganovy zákony.)*

Důkaz. (i) a je komplement a'. Podle 14.8 je komplement jednoznačně určen. Proto $a = (a')'$.
(ii) Toto jistě každý zvládne.
(iii) $(a \wedge b) \vee (a' \vee b') = (a \vee a' \vee b') \wedge (b \vee a' \vee b') = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. $(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$. Druhý zákon je k prvému duální. □

15 Booleovy algebry

Je-li $L = L(\wedge, \vee, \mathbf{0}, \mathbf{1})$ 0,1–svaz, nazývá se $a \in L$ *atomem,* jestliže $a \neq \mathbf{0}$ a z $\mathbf{0} \leq b \leq a$ plyne $b = a$ pro každé $b \in L$. Je-li L konečný svaz a $\mathbf{0} \neq b$, tak jistě existuje alespoň jeden atom $a \in L$ takový, že $\mathbf{0} < a \leq b$.

15.1 Lemma. *Buď $S = S(\wedge, \vee, \mathbf{0}, \mathbf{1}, ')$ a $T = T(\wedge, \vee, \mathbf{0}, \mathbf{1}, ')$ dvě Booleovy algebry. Bijektivní zobrazení $\varphi : S \to T$ je izomorfismem právě když pro všechna $a, b \in S$ platí, že $a \leq_S b$ tehdy a jen tehdy, je-li $\varphi(a) \leq_T \varphi(b)$.*

Důkaz. Připomeňme, že podle 4.4 je $\varphi : S(\wedge,\vee) \to T(\wedge,\vee)$ izomorfismus, pokud $a \leq_S b$ je ekvivalentní $\varphi(a) \leq_T \varphi(b)$ pro $a, b \in S$. Je proto třeba ukázat, že pro izomorfismus $\varphi : S(\wedge,\vee) \to T(\wedge,\vee)$ platí $\varphi(\mathbf{0}) = \mathbf{0}$, $\varphi(\mathbf{1}) = \mathbf{1}$ a $\varphi(a') = (\varphi(a))'$ pro všechna $a \in S$. Pro každé $b \in T$ existuje $c \in S$, že $\varphi(c) = b$. Protože $\varphi(\mathbf{0}) \wedge b = \varphi(\mathbf{0} \wedge c) = \varphi(\mathbf{0})$, je $\varphi(\mathbf{0})$ nejmenší prvek $T(\wedge,\vee)$. Ovšem $T(\wedge,\vee)$ může mít jen jeden nejmenší prvek, takže $\varphi(\mathbf{0}) = \mathbf{0}$. Podobně $\varphi(\mathbf{1}) = \mathbf{1}$. Zbývá ukázat, že $\varphi(a')$ je komplement $\varphi(a)$. Ovšem $\varphi(a') \wedge \varphi(a) = \varphi(a' \wedge a) = \varphi(\mathbf{0}) = \mathbf{0}$ a $\varphi(a') \vee \varphi(a) = \varphi(a' \vee a) = \varphi(\mathbf{1}) = \mathbf{1}$. □

Typickým příkladem Booleových algeber je množina $\mathcal{P}(X)$ všech podmnožin množiny X s operacemi průniku, sjednocení a množinovým doplňkem. Konečné Booleovy algebry jsou dokonce vždy takové algebře izomorfní.

Je-li $M = \{u_1, \dots, u_k\}$ nějaká neprázdná konečná podmnožina Booleovy algebry S, klademe $\bigwedge_M = m_1 \wedge \dots \wedge m_k$ a $\bigvee_M = m_1 \vee \dots \vee m_k$. Definitoricky $\bigwedge_\emptyset = \mathbf{1}$ a $\bigvee_\emptyset = \mathbf{0}$.

15.2 Věta. *Buď $S = S(\wedge,\vee,\mathbf{0},\mathbf{1},')$ konečná Booleova algebra a A ať je množina jejích atomů. Definujme zobrazení $\varphi : \mathcal{P}(A) \to S$ tak, že $\varphi(B) = \bigvee_B$ pro všechna $B \subseteq A$. Potom φ je izomorfismus Booleových algeber.*

Důkaz. Definujme $\psi : S \to \mathcal{P}(A)$ tak, že $\psi(s) = \{a \in A;\, a \leq s\}$. Nejprve ukážeme, že $\varphi\psi(s) = s$. Položme $\psi(s) = T$ a $\varphi\psi(s) = \bigvee_T = t$. Pak $t \leq s$. Předpokládejme, že $t < s$. Pak $s = s \wedge \mathbf{1} = s \wedge (t \vee t') = (s \wedge t) \vee (s \wedge t') = t \vee (s \wedge t')$. Z $s \neq t$ plyne $s \wedge t' \neq \mathbf{0}$. Tudíž existuje $a \in A$ takový, že $a \leq s \wedge t'$. Z $a \leq s$ plyne $a \in T$, takže $a \leq t$. Současně ale $a \leq t'$, takže dostáváme $a \leq t \wedge t' = \mathbf{0}$, a to je spor. Je tedy $s = t$ a $\varphi\psi(s) = s$ pro každé $s \in S$.

Nyní dokážeme, že $\psi\varphi(B) = B$ pro všechna $B \subseteq A$. Položme $b = \bigvee_B$ a $T = \psi(b) = \{a \in A;\, a \leq b\}$. Zjevně $T \supseteq B$. Ať $a \in T \setminus B$. Pak $a = a \wedge b = \bigvee_{c \in B}(a \wedge c)$. Ovšem $a \wedge c \leq c$, takže z $a \neq c$ plyne $a \wedge c = \mathbf{0}$, a tedy $a = \mathbf{0}$. Proto $T = B$.

Pro $B \subseteq C \subseteq A$ jistě $\varphi(B) \leq \varphi(C)$ a pro $s \leq t$ jistě $\psi(s) \subseteq \psi(t)$. Podle 15.1 je ψ izomorfismus Booleových algeber. □

Okruh R se nazývá *idempotentní*, jestliže $a^2 = a$ pro každé $a \in R$.

15.3 Tvrzení. *Buď $B(\wedge,\vee,\mathbf{0},\mathbf{1},')$ Booleova algebra. Definujeme na B operace $+, \cdot$ tak, že $a + b = (a \wedge b') \vee (a' \wedge b)$ a $a \cdot b = a \wedge b$. Položíme dále $-a = a$ pro každé $a \in B$. Potom je $B(+,\cdot,-,\mathbf{0},\mathbf{1})$ komutativní idempotentní okruh charakteristiky 2. Naopak, je-li $B(+,\cdot,-,\mathbf{0},\mathbf{1})$ komutativní idempotentní okruh charakteristiky 2, tak $B(\wedge,\vee,\mathbf{0},\mathbf{1},')$, kde $a \wedge b = a \cdot b$, $a \vee b = a + b + a \cdot b$, $a' = 1 + a$, je Booleova algebra.*

Důkaz. Buď nejprve $B(\wedge, \vee, \mathbf{0}, \mathbf{1}, ')$ Booleova algebra. Pak zjevně $a + b = b + a$, $a + a = \mathbf{0}$, $a + \mathbf{0} = a$. Zbývá ověřit $a + (b + c) = (a + b) + c$ a $a \cdot (b + c) = a \cdot b + a \cdot c$ pro $a, b, c \in B$. Je $a + (b + c) = a + ((b' \wedge c) \vee (c' \wedge b)) = (a \wedge ((b' \wedge c) \vee (c' \wedge b))') \vee (a' \wedge ((b' \wedge c) \vee (c' \wedge b)) = (a \wedge (b \vee c') \wedge (c \vee b')) \vee (a' \wedge b' \wedge c) \vee (a' \wedge c' \wedge b)$. Ovšem $a \wedge (b \vee c') \wedge (c \vee b') = ((a \wedge b) \vee (a \wedge c')) \wedge (c \vee b') = (a \wedge b \wedge c) \vee (a \wedge b' \wedge c')$. Je tedy $a + (b + c) = (a \wedge b \wedge c) \vee (a \wedge b \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c)$. V tomto výraze lze a, b i c vzájemně zaměnit, aniž by se změnila hodnota tohoto výrazu. Vyměníme-li a a c, dostaneme opačnými úpravami, že $a + (b + c)$ je rovno $c + (a + b) = (a + b) + c$. Dále $a \cdot (b + c) = a \wedge ((b \wedge c') \vee (b' \wedge c)) = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$. Ovšem $(a \wedge b) \wedge (a \wedge c)' = a \wedge b \wedge c'$ a $(a \wedge b)' \wedge (a \wedge c) = a \wedge b' \wedge c$.

Na druhou stranu, ať $B(+, \cdot, -, \mathbf{0}, \mathbf{1})$ je komutativní idempotentní okruh charakteristiky 2. Pak $a \vee a = a + a + a^2 = a$, $(a \vee b) \vee c = a + b + ab + c + ac + bc + abc = a + b + c + bc + ab + ac + abc = a \vee (b \vee c)$, $a \vee \mathbf{1} = a + \mathbf{1} + a = \mathbf{1}$, $a \vee 0 = a$, $a \wedge (b \vee a) = a + ab + ab = a$, $a \vee (b \wedge a) = a + ba + ba = a$, $a \wedge (b \vee c) = a \cdot (b + c + bc) = ab + ac + a^2bc = (a \wedge b) \vee (a \wedge c)$. Konečně $(a')' = \mathbf{1} + \mathbf{1} + a = a$, $a \vee a' = a + \mathbf{1} + a + a + a^2 = \mathbf{1}$ a $a \wedge a' = a(\mathbf{1} + a) = a + a = \mathbf{0}$. □

Index