Algebra I - poznámky

Libor Polák

1 Vlastnosti operací, označení

Pro číselné množiny používáme následující (standardní) značení:
$\mathbb{N} = \{1, 2, \ldots\}$ množina všech přirozených čísel,
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ množina všech nezáporných celých čísel,
$\mathbb{Z}$ množina všech celých čísel,
$\mathbb{Q}$ množina všech racionálních čísel,
$\mathbb{R}$ množina všech reálných čísel,
$\mathbb{C}$ množina všech komplexních čísel,
X^* značí množinu všech nenulových prvků z $X \subseteq \mathbb{C}$ a
X^+ značí množinu všech kladných prvků z $X \subseteq \mathbb{R}$.

Nechť $n \in \mathbb{N}_0$ a A je množina. Zobrazení $f : A^n \to A$ nazýváme ***n-ární operace na množině*** A. Poněvadž A^0 je jednoprvková množina, lze nulární operace ztotožnit s výběry prvků z množiny A. Pro binární operace obvykle používáme symboly $\cdot, +$, atd. a píšeme $a \cdot b$ místo $\cdot(a, b)$, atd. Často píšeme dokonce jen ab místo $a \cdot b$.

Binární operace $\cdot$ na množině A se nazývá
– ***asociativní***, je-li $\forall\, a, b, c \in A \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
– ***komutativní***, je-li $\forall\, a, b \in A \quad a \cdot b = b \cdot a$,
– ***idempotentní***, je-li $\forall\, a \in A \quad a \cdot a = a$.

Prvek $e \in A$ nazýváme
– ***levým neutrálním***, je-li $\forall\, a \in A \quad e \cdot a = a$,
– ***pravým neutrálním***, je-li $\forall\, a \in A \quad a \cdot e = a$,
– ***neutrálním***, je-li jak levý neutrální tak i pravý neutrální;
– ***levým nulovým***, je-li $\forall\, a \in A \quad e \cdot a = e$,
– ***pravým nulovým***, je-li $\forall\, a \in A \quad a \cdot e = e$,
– ***nulovým***, je-li jak levý nulový tak i pravý nulový;
– ***idempotentem***, je-li $e \cdot e = e$.

V případě existence neutrálního prvku e se $b \in A$ nazývá
– ***levou inverzí*** prvku $a \in A$, je-li $b \cdot a = e$,
– ***pravou inverzí*** prvku $a \in A$, je-li $a \cdot b = e$,
– ***inverzí*** prvku $a \in A$, je-li jeho levou i pravou inverzí.

Uspořádaná dvojice $\mathcal{A} = (A, \cdot)$ se nazývá ***grupoid***. Je-li operace $\cdot$ asociativní, hovoříme o ***pologrupě***. Pologrupa s neutrálním prvkem se nazývá ***monoid***; píšeme též $(A, \cdot, e)$, kde e je neutrální prvek. Konečně ***grupa*** je monoid, v němž má libovolný prvek inverzi.

Cvičení 1.1 *Zjistěte, zda* $+, \cdot, -, :$ *jsou operacemi na výše uvedených číselných množinách*

a v kladném případě vyšetřete jejich vlastnosti.

Nechť A je množina. Klademe
$T(A)$ – množina všech zobrazení množiny A do sebe (mluvíme též o ***transformacích***; jiné označení je A^A) ,
$PT(A) = \{\ \rho \subseteq A \times A \mid\ (\forall\, a, b, c \in A)(\ a\rho b,\ a\rho c$ implikuje $b = c\ )\ \}$ – množina všech ***parciálních transformací*** množiny A,
$S(A)$ – množina všech bijekcí množiny A na sebe (hovoříme též o ***permutacích***),
$S_n = S(\{1, ..., n\}),\ n \in \mathbb{N}$,
$PB(A) = \{\ f : B \to A \mid\ B \subseteq A,\ f$ prosté $\}$ – množina všech parciálních bijekcí množiny A do sebe.

Cvičení 1.2 *Ukažte, že uvedené množiny jsou vzhledem k operaci skládání zobrazení monoidy (tuto operaci značíme* $\circ$ *a* $g \circ f$ *čteme* g *po* f*). Najděte v nich všechny levé/pravé nulové/neutrální prvky a všechny idempotenty.*

Další označení:
$M_{mn}(\mathbb{R})$ – množina všech matic typu m/n nad $\mathbb{R}$,
$GL_n(\mathbb{R})$ – množina všech regulárních matic řádu n nad $\mathbb{R}$,
$SL_n(\mathbb{R})$ – množina všech matic řádu n nad $\mathbb{R}$ s determinantem rovným 1.

Cvičení 1.3 *Zjistěte, zda obvyklé "operace"* $+,\ \cdot$ *jsou na těchto množinách skutečně operacemi a v kladném případě vyšetřete jejich vlastnosti.*

Cvičení 1.4 *Na množině* 2^A *všech podmnožin množiny* A *(někdy používáme označení* $B(A)$*) uvažujme "operace"* $\cup,\ \cap,\ \setminus$ *(množinový rozdíl) ,* $'$ *(komplement) ,* $\div$ *(symetrická diference) . Jsou to operace ? V kladném případě vyšetřete jejich vlastnosti.*

Cvičení 1.5 *Uvažujte "operace" nsd (největší společný dělitel) a nsn (nejmenší společný násobek) na množinách* $\mathbb{N},\ \mathbb{N}_0,\ \mathbb{Z}$.

2 Grupy permutací

Věnujme se grupám $(S_n, \circ),\ n \in \mathbb{N}$.

Nechť $k \in \mathbb{N},\ k \geq 2$, nechť $i_1, ..., i_k \in \{1, ..., n\}$ jsou po dvou různá. Permutace f definovaná vztahem

$$f(i_j) = i_{j+1} \text{ pro } j = 1, ..., k-1,\ f(i_k) = i_1,\ f(i) = i \text{ jinak}$$

se nazývá ***cyklus*** délky k. Píšeme $f = (i_1, ..., i_k)$. Cykly $(i_1, ..., i_k)$ a $(j_1, ..., j_l)$ jsou ***nezávislé***, je-li $\{i_1, ..., i_k\} \cap \{j_1, ..., j_l\} = \emptyset$. ***Transpozice*** je cyklus délky 2.

Věta 2.1 *Libovolná permutace* $f \in S_n$ *je součinem nezávislých cyklů. Přitom tento rozklad je určen jednoznačně až na pořadí činitelů. (Součin nula činitelů považujeme za identickou permutaci.)*

Věta 2.2 *Libovolná permutace* $f \in S_n$ *je součinem transpozic. Počet činitelů ve všech takových rozkladech dané* f *je buď sudý (pak hovoříme o sudé permutaci) nebo lichý (lichá permutace).*

Klademe $A_n = \{f \in S_n \mid f \text{ sudá }\}$.

3 Pologrupy

Cvičení 3.1 *Vyšetřete vlastnosti prvků pologrupy $(B(A \times A), \circ)$ všech relací na množině A.*

Nechť $\mathcal{S} = (S, \cdot)$ je pologrupa. Prvek $a \in S$ se nazývá ***regulární***, existuje-li $b \in S$ tak, že $aba = a$. Prvky $a, b \in S$ jsou (vzájemně) ***inverzní***, platí-li $aba = a,\ bab = b$. Pologrupa $\mathcal{S}$ je ***regulární***, je-li každý její prvek regulární.

Cvičení 3.2 *1. Ukažte, že každý regulární prvek má inverzi.*
2. Dokažte, že pologrupa $(T(A), \circ)$ je regulární.
3. Ukažte, že pologrupa $(B(A \times A), \circ)$ obecně není regulární.

Nechť Λ, M jsou neprázdné množiny, nechť $\mathcal{G} = (G, \cdot)$ je grupa, Nechť P je matice nad G typu M/Λ. Na množině $\Lambda \times G \times M$ definujme (zřejmě asociativní) násobení vztahem

$$(\lambda, g, \mu) \cdot (\nu, h, o) = (\lambda, g \cdot p_{\mu\nu} \cdot h, o)\ .$$

Označení: $\mathcal{M}(\Lambda, G, M; P)$. Hovoříme o ***maticové pologrupě nad grupou*** $\mathcal{G}$.

Cvičení 3.3 *Najděte všechny idempotenty v $\mathcal{M}(\Lambda, G, M; P)$.*

Má-li pologrupa $(S, \cdot)$ neutrální prvek, klademe $S^1 = S$. V opačném případě vyberme $e \notin S$, položíme $S^1 = S \cup \{e\}$ a dodefinujme $e \cdot a = a \cdot e = a$ pro $a \in S$ a $e \cdot e = e$. Zřejmě je $(S^1, \cdot)$ opět pologrupa.

Nechť $\mathcal{S} = (S, \cdot)$ je pologrupa, nechť $a, b \in S$. Klademe
$a\mathcal{L}b \iff$ existují $p, q \in S^1$ tak, že $pa = b,\ qb = a$,
$a\mathcal{R}b \iff$ existují $u, v \in S^1$ tak, že $au = b,\ bv = a$,
$a\mathcal{J}b \iff$ existují $p, q, u, v \in S^1$ tak, že $pau = b,\ qbv = a$.
Položme $\mathcal{H} = \mathcal{R} \cap \mathcal{L},\ \mathcal{D} = \mathcal{R} \vee \mathcal{L}$ (ve svazu všech ekvivalencí na množině S). Hovoříme o tzv. ***Greenových*** relacích na pologrupě $\mathcal{S}$.

Cvičení 3.4 *Charakterizujte Greenovy relace na pologrupách $(T(A), \circ)$ a $\mathcal{M}(\Lambda, G, M; P)$.*

Poznámka 3.1 *Neutrální prvek podgrupy G dané pologrupy $\mathcal{S} = (S, \cdot)$ je idempotentem v $\mathcal{S}$. Naopak, například $\{e\}$ je podgrupa v $\mathcal{S}$ mající idempotent e za neutrální prvek.*

Cvičení 3.5 *1. Dokažte, že*

$$G_e = \{\ a \in S \mid ae = ea = a,\ \textit{existuje } b \in S \textit{ tak, že } be = eb = b,\ ab = ba = e\ \}$$

je největší podgrupou pologrupy $\mathcal{S} = (S, \cdot)$ mající idempotenta $e \in S$ za neutrální prvek.
2. Nechť G je podgrupa pologrupy $\mathcal{S} = (S, \cdot)$ s neutrálním prvkem e a nechť H je podgrupa v $\mathcal{S}$ s neutrálním prvkem f. Nechť $e \neq f$. Ukažte, že $G \cap H = \emptyset$.

Pologrupa se nazývá
– ***inverzní***, má-li každý její prvek právě jednu inverzi;
– ***úplně regulární***, má-li každý její prvek a takovou inverzi b, že $ab = ba$.

Cvičení 3.6 *1. Ukažte, že pologrupa $(PB(A), \circ)$ je inverzní a není úplně regulární.*
2. Ukažte, že pologrupa $\mathcal{M}(\Lambda, G, M; P)$ je úplně regulární a není inverzní.
3. Ukažte, že pologrupa $(T(A), \circ)$ není ani inverzní ani úplně regulární.

4 Ještě grupy

Problém rozšíření: pro dané grupy $\mathcal{G}$ a $\mathcal{K}$ hledáme všechny dvojice $\mathcal{K},\ L$, kde $\mathcal{K} = (K, \cdot)$ je grupa, L její normální podgrupa, takové, že platí: $(L, \cdot) \cong \mathcal{G}$ a $\mathcal{K}/L \cong \mathcal{H}$.
Grupu $\mathcal{K}$ nazýváme ***rozšířením*** grupy $\mathcal{G}$ pomocí grupy $\mathcal{H}$.

Cvičení 4.1 *Tento problém neřešte v plné obecnosti - nicméně jedno rozšíření byste mohli najít.*

Nechť $\mathcal{G} = (G, \cdot)$ a $\mathcal{H} = (H, \cdot)$ jsou grupy. Nechť $\varphi : \mathcal{H} \to (\mathrm{Aut}\mathcal{G}, \circ)$ je homomorfismus (druhá z grup je grupa všech automorfismů grupy $\mathcal{G}$ s operací skládání).
Na množině $G \times H$ definujeme operaci vztahem

$$(a, p) \cdot (b, q) = (a \cdot \varphi(p)(b),\ p \cdot q)\ ,\ a, b \in G,\ p, q \in H\ .$$

Vzniklý grupoid značíme $\mathcal{G} \times_\varphi \mathcal{H}$ a nazýváme ho ***polopřímým součinem*** grupy $\mathcal{G}$ s grupou $\mathcal{H}$ pomocí akce φ.

Cvičení 4.2 *1. Ukažte, že $\mathcal{G} \times_\varphi \mathcal{H}$ je opět grupa a že součin je speciálním případem této konstrukce.*
2. Ukažte, že tato grupa je rozšířením grupy $\mathcal{G}$ pomocí grupy $\mathcal{H}$.

Prezentací rozumíme zápis

$$\mathrm{Gp} <\ a, b\ ;\ a^r = 1,\ b^s = 1,\ ab = ba^t\ >\ ,$$

kde $r, s, t \in \mathbb{N}$. Prvky a, b nazýváme ***generátory*** a rovnosti za středníkem ***relace***. Poněvadž nám dosud chybí základy univerzální algebry, nezabýváme se problematikou v plné obecnosti.
Pravíme, že grupa $\mathcal{G} = (G, \cdot)$ je ***zadána*** výše uvedenou prezentací, ***vzhledem k zobrazení*** ι, platí-li:
(i) $\iota : \{a, b\} \to G$,
(ii) množina $\{\iota(a), \iota(b)\}$ generuje grupu $\mathcal{G}$,
(iii) v grupě $\mathcal{G}$ platí $(\iota(a))^r = 1,\ (\iota(b))^s = 1,\ \iota(a)\iota(b) = \iota(b)(\iota(a))^t$,
(iv) pro libovolnou grupu $\mathcal{H} = (H, \cdot)$ a libovolné zobrazení $\alpha : \{a, b\} \to H,\ a \mapsto A,\ b \mapsto B$ splňující $A^r = 1,\ B^s = 1,\ AB = BA^t$ existuje homomorfismus $\beta : \mathcal{G} \to \mathcal{H}$ vlastnosti $\beta \circ \iota = \alpha$.
Jednoduší verze naší definice následuje.
Grupa $\mathcal{G} = (G, \cdot)$ je ***zadána*** výše uvedenou prezentací, platí-li:
(i) $a, b \in G$,
(ii) množina $\{a, b\}$ generuje grupu $\mathcal{G}$,
(iii) v grupě $\mathcal{G}$ platí $a^r = 1,\ b^s = 1,\ ab = ba^t$,
(iv) pro libovolnou grupu $\mathcal{H} = (H, \cdot)$ a libovolná $A, B \in H$ splňující $A^r = 1,\ B^s = 1,\ AB = BA^t$ lze zobrazení $a \mapsto A,\ b \mapsto B$ rozšířit do homomorfismu grupy $\mathcal{G}$ do grupy $\mathcal{H}$.
První verze má tu výhodu, že grupa $\mathcal{G}$ vždy existuje, druhá verze je v pořádku, pokud si relace nevynutí ztotožnění generátorů.

Cvičení 4.3 *Určete grupu $\mathcal{G}$ - není to jednoduché, ale pokud o tom budete přemýšlet, nic se vám nestane.*

5 Syntaktický monoid

Kongruencí pologrupy $(S,\cdot)$ (resp. monoidu $(S,\cdot,e)$) nazýváme relaci ekvivalence $\sim$ na množině S, která splňuje

$$(\forall\ a,b,c,d \in S\ )\ (\ a \sim b,\ c \sim d\ \Rightarrow\ ac \sim bd\ )\ .$$

Poznamenejme, že místo této podmínky stačí uvažovat

$$(\forall\ a,b,c \in S\ )\ (\ a \sim b\ \Rightarrow\ ac \sim bc,\ ca \sim cb\ )\ .$$

Nechť $a\sim\, = \{\ b \in S \mid b \sim a\ \}$ pro $a \in S$ a nechť $S/\!\sim\, = \{\ a\sim \mid a \in S\ \}$ je rozklad na množině S příslušný této relaci ekvivalence. Na množině $S/\!\sim$ definujeme operaci $\cdot$ vztahem $a\!\sim \cdot\, b\!\sim\, = (a \cdot b)\!\sim$. Tato operace je zřejmě asociativní a hovoříme o ***faktorové*** pologrupě (resp. monoidu — v tomto případě je $e\sim$ neutrálním prvkem); označení $(S,\cdot)/\sim$ (resp. $(S,\cdot,e)/\sim$).

Nechť A je neprázdná konečná množina (tzv. ***abeceda***). Označme

$$A^* = \{\ (a_1,\dots,a_n) \mid n \in \mathbb{N}_0,\ a_1,\dots,a_n \in A\ \}\ .$$

Prvky množiny A^* nazýváme ***slovy*** nad A. Píšeme stručněji $a_1\dots a_n$ místo $(a_1,\dots,a_n)$ a slovo pro $n=0$ označujeme λ a říkáme mu ***prázdné***.

Na A^* definujeme operaci $\cdot$ vztahem

$$a_1\dots a_m \cdot b_1\dots b_n = a_1\dots a_m b_1\dots b_n \text{ pro } a_1,\dots,a_m,b_1,\dots,b_n \in A\ .$$

Tato operace je zřejmě asociativní a λ je pro ni neutrálním prvkem. Pravíme, že monoid $(A^*,\cdot,\lambda)$ je ***volný*** nad množinou A.

Libovolnou podmnožinu množiny A^* nazýváme ***jazykem*** nad A. Pro jazyky U,V definujeme jejich ***součin*** $U\cdot V = \{\ uv \mid u \in U,\ v \in V\ \}$ a ***iteraci*** $U^* = \{\ u_1\dots u_n \mid n \in \mathbb{N}_0,\ u_1,\dots,u_n \in U\ \}$ (i zde máme λ pro $n=0$, ale pozor: je to něco jiného než A^* výše). Jazyk $L \subseteq A^*$ se nazývá ***regulární*** vznikl-li z $\emptyset$ a prvků množiny A použitím konečně mnoha aplikací operací $\cdot$, * a (binárního) sjednocení. Poznamenejme, že $\emptyset^* = \{\lambda\}$.

(Konečný deterministický úplný) ***automat*** je uspořádaná pětice $\mathcal{A} = (Q,A,\cdot,i,T)$, kde A je jako výše neprázdná konečná abeceda, Q neprázdná konečná množina ***stavů***,

$$\cdot : Q \times A \to Q,\ (q,a) \mapsto q \cdot a$$

je zobrazení, $i \in Q$ je ***počáteční*** stav a $T \subseteq Q$ je množina ***koncových*** stavů.

Libovolné $u \in A^*$ definuje transformaci

$$[u] : Q \to Q,\ q \mapsto q \cdot u$$

takto : zobrazení $[a]$ pro $a \in A$ je již definováno a $q\cdot(ua) = (q\cdot u)\cdot a$ pro $q \in Q,\ u \in A^*,\ a \in A$. Monoid

$$(\ \{\ [u] \mid u \in A^*\ \},\cdot\ ),\ \text{kde}\ \ [u]\cdot[v] = [uv]\ ,$$

se nazývá ***transformační monoid*** automatu $\mathcal{A}$. Klademe $\mathcal{L}(\mathcal{A}) = \{\ u \in A^* \mid i \cdot u \in T\ \}$ — tzv. ***jazyk přijímaný*** automatem $\mathcal{A}$.

Automat $\mathcal{A}$ je ***minimální***, jestliže
(i) $\{\ i \cdot u \mid u \in A^*\ \} = Q$,
(ii) $(\ \forall\ p,q \in Q\ )\ (\ (\ \forall\ u \in A^*\ )\ (\ p \cdot u \in T\ \Leftrightarrow\ q \cdot u \in T)\ \Rightarrow\ p = q\ )$.

Jazyk $L \subseteq A^*$ definuje na množině A^* relaci $\sim_L$ vztahem

$$u \sim_L v \text{ právě když } (\ \forall\ s,t \in A^*)\ (\ sut \in L\ \Leftrightarrow\ svt \in L\ )\ .$$

Lze ukázat, že $\sim_L$ je kongruence monoidu $(A^*,\cdot)$. Příslušný faktorový monoid nazýváme ***syntaktickým monoidem*** jazyka L ; označení $(\mathsf{O}(L),\cdot)$.

Následující relace je uspořádáním na množině $\mathsf{O}(L)$:

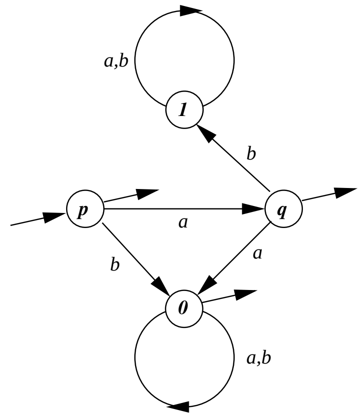
$$u\sim_L\ \leq_L\ \ v\sim_L \text{ právě když } (\ \forall\ s,t \in A^*\ )\ (\ svt \in L\ \Rightarrow\ sut \in L\ )\ .$$

Věta 5.1 *Nechť minimální automat $\mathcal{A} = (Q,A,\cdot,i,T)$ přijímá jazyk $L = \mathcal{L}(\mathcal{A})$. Pak syntaktický monoid jazyka L je izomorfní s transformačním monoidem automatu $\mathcal{A}$.*

Věta 5.2 *Pro jazyk $L \subseteq A^*$ je ekvivalentní*
(i) L je regulární,
(ii) L je přijímaný automatem,
(iii) $\mathsf{O}(L)$ je konečná množina.

Pro regulární jazyky nad množinou A nám Věta 5.1. dává algoritmus pro výpočet syntaktických monoidů: uvažujeme postupně transformace množiny Q dané slovy v pořadí jejich délek přičemž slova stejné délky probíráme v tzv. lexikografickém uspořádání (pro $A = \{a,b\}$ je to $\lambda, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa, aaab, \dots$). Dostáváme tak dokonce tzv. prezentaci syntaktického monoidu.

Příklad 5.1 *Transformační monoid minimálního automatu*



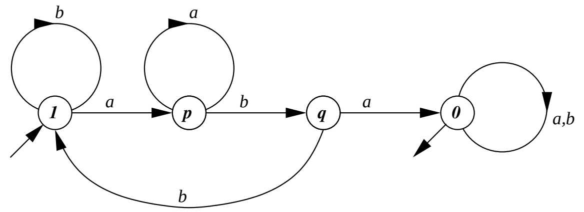
má prvky

u	***p q 0 1***
1	***p q 0 1***
a	***q 0 0 1***
b	***0 1 0 1***
a^2	***0 0 0 1***
ab	***1 0 0 1***

a syntaktický monoid jazyka přijímaného tímto automatem má prezentaci

$$< \ a, b \ \mid ba = b, \ b^2 = b, \ a^3 = a^2, \ a^2 b = a^2 \ > \ .$$

Cvičení 5.1 *Určete syntaktický monoid jazyka přijímaného následujícím automatem.*



V řadě případů lze z vlastností (konečného!) uspořádaného syntaktického monoidu daného regulárního jazyka usoudit na některé vlastnosti tohoto jazyka; např.

Věta 5.3 *Jazyk $L \subseteq A^*$ je konečným sjednocením konečných průniků jazyků tvaru $A^* a_1 A^* \dots A^* a_k A^*$ právě když je neutrální prvek jeho syntaktického monoidu největším prvkem v uspořádané množině $(\mathsf{O}(L), \leq)$.*

Věta 5.4 (Simon) *Jazyk $L \subseteq A^*$ je konečným sjednocením konečných průniků jazyků tvaru $A^* a_1 A^* \dots A^* a_k A^*$ a jejich komplementů právě když je jeho syntaktický monoid $\mathcal{J}$-triviální.*

Věta 5.5 (Schützenberger) *Jazyk $L \subseteq A^*$ lze zadat zobecněným regulárním výrazem bez použití iterace (tj. je "star-free") právě když jeho syntaktický monoid obsahuje jen triviální podgrupy.*

Cvičení 5.2 *Ukažte, že jazyk zadaný regulárním výrazem $(ab + ba)^*$ nad $A = \{a, b\}$ je star-free.*

6 Primální algebry

Na množině $\{0, 1\}$ pravdivostních hodnot je 16 binárních operací (logických spojek). Libovolnou z nich lze "vygenerovat" pomocí unární negace a binární konjunkce. Dokonce binární spojka "ani ... ani ..." na to stačí sama.

Zobecníme tyto poznatky na libovolnou konečnou množinu.

Algebra je uspořádaná dvojice $\mathcal{A} = (A, F)$, kde A je množina a F je množina operací na A.

Nechť $m, n \in \mathbb{N}, \ f : A^n \to A, \ \tau : \{1, ..., n\} \to \{1, ..., m\}$. Klademe

$$f_\tau(a_1, \dots, a_m) = f(a_{\tau(1)}, ..., a_{\tau(n)}), \ a_1, \dots, a_m \in A.$$

Pak $f_\tau : A^m \to A$ a pravíme, že f_τ vznikla z f ***transformací argumentů***.

Nechť $f : A^n \to A, \ g : A^m \to A, \ m, n \in \mathbb{N}$. Klademe

$$(f(g))(a_1, \dots, a_{m+n-1}) = f(g(a_1, \dots, a_m), a_{m+1}, \dots, a_{m+n-1}), \ a_1, \dots, a_{m+n-1} \in A.$$

Pak $f(g) : A^{m+n-1} \to A$ a pravíme, že $f(g)$ vznikla ***kompozicí*** f a g.

Nechť $\mathcal{A} = (A, F)$ je algebra. Množina všech jejích ***algebraických operací*** $T(\mathcal{A})$ je nejmenší množina splňující:
(i) $F \subseteq T(\mathcal{A})$,
(ii) identické zobrazení množiny A na sebe patří do $T(\mathcal{A})$,
(iii) $T(\mathcal{A})$ je uzavřená na transformace argumentů,
(iv) $T(\mathcal{A})$ je uzavřená na kompozice.

Algebra $\mathcal{A}$ je ***primální***, je-li libovolná operace na množině A nenulové arity algebraickou operací algebry $\mathcal{A}$.

Následující tvrzení jsou pozoruhodná:

Věta 6.1 (Sierpiński) *Libovolná operace nenulové arity vznikne z binárních operací transformacemi argumentů a kompozicemi.*

Věta 6.2 (Post) *Algebra $\mathcal{A} = (\{0, 1, ..., n-1\}, \ \wedge, \ g)$, kde $i \wedge j = min\{i, j\}, \ g(i) = i+1$ pro $i = 0, ..., n-2, \ g(n-1) = 0$, je primální.*

Nejprve dokážeme:

Lemma 6.1 (Post) *Nechť A je alespoň dvouprvková konečná množina, nechť $0, 1 \in A$, nechť $\wedge, \vee$ jsou binární operace na A splňující*

$$(\forall \ a \in A) \ (a \wedge 0 = 0, \ a \wedge 1 = a, \ a \vee 0 = a = 0 \vee a).$$

Nechť c_a je unární konstanta na prvek $a, \ a \in A$,
nechť $\chi_a(b) = 0$ pro $a \neq b, \ \chi_a(a) = 1$ pro $a, b \in A$ je rovněž unární.
Pak je algebra $\mathcal{A} = (A, 0, 1, \wedge, \vee, \ (c_a)_{a \in A}, \ (\chi_a)_{a \in A})$ primální.

Důkaz lemmatu.
Nechť f je n-ární operace na množině A.
Položme

$$\chi_{(a_1, \dots, a_n)}(b_1, \dots, b_n) = (...(\chi_{a_1}(b_1) \wedge \chi_{a_2}(b_2)) \wedge ...) \wedge \chi_{a_n}(b_n) \ .$$

Pak $\chi_{(a_1, \dots, a_n)}(b_1, \dots, b_n) = 0$ pro $(a_1, \dots, a_n) \neq (b_1, \dots, b_n), \ \chi_{(a_1, \dots, a_n)}(a_1, \dots, a_n) = 1.$

Položme

$$f_{(a_1, \dots, a_n)}(b_1, \dots, b_n) = c_{f(a_1, \dots, a_n)}(b_1) \wedge \chi_{(a_1, \dots, a_n)}(b_1, \dots, b_n) \ .$$

Pak $f_{(a_1, \dots, a_n)}(b_1, \dots, b_n) = 0$ pro $(a_1, \dots, a_n) \neq (b_1, \dots, b_n)$,
$f_{(a_1, \dots, a_n)}(a_1, \dots, a_n) = f(a_1, \dots, a_n)$.

Nechť $A^n = \{(a_{11}, ..., a_{1n}), ..., (a_{s1}, ..., a_{sn})\}$, $s = |A|^n$. Máme

$$f(b_1, \ldots, b_n) = (...(f_{(a_{11},...,a_{1n})}(b_1, \ldots, b_n) \vee f_{(a_{21},...,a_{2n})}(b_1, \ldots, b_n)) \vee ...) \vee f_{(a_{11},...,a_{sn})}(b_1, \ldots, b_n) \,.$$

Důkaz Postovy věty.
Prvky $0, 1$ z lemmatu značme $\underline{0}, \underline{1}$. Položme

$$\underline{0} = 0,\ \underline{1} = n-1,\ c_0(a) = a \wedge g(a) \wedge ... \wedge g^{n-1}(a),\ c_i(a) = g^i(c_0(a)) \text{ pro } i \geq 1 \,,$$

$$\chi_i(a) = g^{n-1}(\underline{1} \wedge g^{n-i}(a)),\ a \vee b = g(g^{n-1}(a) \wedge g^{n-1}(b)) \,.$$

Důkaz Sierpińského věty.
Pro konečnou množinu A to plyne z Postovy věty, pro nekonečnou množinu to zatím dokazovat nebudeme.

Věta 6.3 (Webb) *Algebra* $(\{0, 1, ..., n-1\}, |)$, *kde* $i \mid j = ...$ *je primální.*

Důkaz. Položme $a \wedge b = ...,\ g(i) = ...$

To byla ukázka, jak dokazovat primalitu. Dokázat, že daná algebra není primální vyžaduje nové metody. Snad později.