3. Algebraické systémy

Na rozdíl od klasické algebry, jejíž ústředním tématem jsou rovnice a potřebný aparát pro jejich řešení /matice, polynomy,.../, moderní /abstraktní/ algebra se zabývá obecnými algebraickými strukturami /grupy, svazy, okruhy,.../.

Algebraická struktura je systém množin spolu se systémem operací definovaných na těchto množinách. Pojmy operace, algebraická struktura /algebraický systém, algebra/ a její typ byly podrobně pojednány v kapitole 1 a to v souvislosti s relačními strukturami.

Až na vyjímky, se v této kapitole omezíme jen na homogenní algebraické struktury s jediným nosičem a to s jedinou nebo jen několika málo operacemi /většinou binárními/.

Definice 3.1:

Nechť $*$ označuje binární operaci na množině A. Nejčastějšími vlastnostmi binárních operací jsou zejména následující vlastnosti:

- ***Universalita a jednoznačnost***: $(\forall a,b)(\exists_1 c)[a*b=c]$ UN
- ***Komutativita***: $(\forall a,b)[a*b=b*a]$ KO
- ***Asociativita***: $(\forall a,b,c)[(a*b)*c=a*(b*c)]$ AS
- ***Existence nulového prvku*** z: $(\exists z)(\forall a)[a*z=z*a=z]$ NU
- ***Existence jednotkového prvku*** e: $(\exists e)(\forall a)[a*e=e*a=a]$ JE
- ***Existence inverzního prvku***: $(\forall a)(\exists b)[a*b=b*a=e]$ IN

/Prvek b inverzní k prvku a označujeme $b=a^{-1}$./

Věta 3.1:

Existuje nejvýše jeden nulový a nejvýše jeden jednotkový prvek vzhledem k libovolné binární operaci $*$ na množině A.

Důkaz:

Sporem. Nechť z_1,z_2 jsou dva různé nulové prvky vzhledem k operaci $*$. Podle NU tedy platí:

$$a*z_1=z_1*a=z_1, \quad a*z_2=z_2*a=z_2.$$

Uvedené rovnosti jsou platné pro všechna a, a tedy také pro $a=z_2$ a $a=z_1$. Dostáváme tak

$$z_2*z_1=z_1*z_2=z_1, \quad z_1*z_2=z_2*z_1=z_2,$$

odkud plyne $z_1=z_2$.

Existenci nejvýše jednoho jednotkového prvku dokážeme obdobným způsobem.

Věta 3.2:

Nechť binární operace $*$ na množině A je asociativní a má jednotkový prvek /tj. platí AS,JE/. Pak každý prvek $a\in A$ má vzhledem k operaci $*$ v A nejvýše jeden inverzní prvek.

Důkaz:

Sporem. Nechť b_1,b_2 jsou dva různé inverzní prvky prvku $a\in A$ vzhledem k operaci $*$. Podle IN tedy platí:

$$a*b_1=b_1*a=e, \quad a*b_2=b_2*a=e.$$

Z JE,AS a právě uvedených rovností vyplývá platnost následujího řetězce rovností:

$$b_1=b_1*e=b_1*(a*b_2)=(b_1*a)*b_2=e*b_2=b_2.$$

Prvky b1,b2 nejsou tedy různé.

Poznámky 3.1:

1. Je-li operace * asociativní, pak ve výraze
$$(...((a_1*a_2)*a_3)*...)*a_n$$
nezáleží na rozmístění závorek a závorky netřeba psát vůbec. Jsou-li navíc všechny operandy totožné, pak je možné používat tzv. ***mocninový zápis*** definovaný rekurentně takto:
$$a^1=a,\ a^{i+1}=a^i*a \quad \text{pro } i=1,2,...$$

2. Má-li operace * na množině A jednotkový prvek e, pak klademe
$$a^0=e.$$

3. Jsou-li prvky množiny A vzhledem k operaci * invertovatelné, pak klademe
$$a^{-n}=(a^{-1})^n.$$

4. Pro počítání s mocninami zavedenými v předchozích bodech platí pravidla:
$$a^r*a^s=a^{r+s},\ (a^r)^s=a^{r.s}.$$
/Symboly +,. jsou operátory číselného sčítání a násobení, kdežto symbol * je symbol obecné binární operace, algebraického "násobení"./

Definice 3.2:

Nechť *,∘ jsou dvě binární operace na množině A. Říkáme, že operace * je distributivní /má vlastnost ***distributivity***/ vzhledem k operaci ∘, jestliže platí:

$(\forall a,b,c)[(a\circ b)*c=(a*c)\circ(b*c)]$ .. pravý distributivní zákon DIp

$(\forall a,b,c)[a*(b\circ c)=(a*b)\circ(a*c)]$ ... levý distributivní zákon DIl

3.1. Morfismy a kongruence

Pojmy morfismu a kongruence budou zavedeny pro homogenní algebraické systémy s jediným nosičem. Zobecnění pro případ nehomogenních algebraických systémů s více nosiči je nasnadě.

Definice 3.1.1:

Nechť ω je n-ární operace na množině A a nechť $A'\subseteq A$. Podmnožina A' se nazývá ***uzavřenou vzhledem k operaci*** ω jestliže platí:

$$a_1,a_2,...,a_n \in A' \Rightarrow \omega(a_1,a_2,...,a_n) \in A'.$$

Definice 3.1.2:

Algebra $\langle A';\omega,...\rangle$ je ***podalgebrou*** algebry $\langle A;\omega,...\rangle$, jestliže:

- $\emptyset\neq A'\subseteq A$,
- A' je uzavřená vzhledem ke všem operacím algebry.

Příklady 3.1.1:

Nechť N,I,Q,R označují po řadě množinu všech přirozených, celých, racionálních a reálných čísel. Potom $\langle N;+,.\rangle$ je podalgebrou algebry $\langle I;+,.\rangle$, $\langle I;+,.\rangle$ je podalgebrou algebry $\langle Q;+,.\rangle$ a $\langle Q;+,.\rangle$ je podalgebrou algebry $\langle R;+,.\rangle$.

Věta 3.1.1:

Relace "být podalgebrou" je uspořádáním na množině všech algeber téhož typu.

Důkaz:

Snadno ověříme, že relace má vlastnosti RE, AN, TR.

Definice 3.1.3:

Nechť $\langle A;\omega,...\rangle$ a $\langle A';\omega',...\rangle$ jsou dvě algebry se stejnou signaturou /tj. algebry mají stejný počet operací a navzájem si odpovídající operace mají stejnou aritu/. ***Morfismus*** /nazývaný také ***homomorfismus***/ algebry $\langle A;\omega,...\rangle$ do algebry $\langle A';\omega',...\rangle$ je zobrazení $h: A \rightarrow A'$ s následující vlastností /platnou pro všechny dvojice ω,ω' vzájemně si odpovídajících operací a pro všechny prvky nosiče A/:

$$h(\omega(a_1,a_2,...,a_n) = \omega'(h(a_1),h(a_2),...,h(a_n)).$$

/Slovy: obraz výsledku operace je roven výsledku operace provedené s obrazy argumentů./

Speciální případy morfismu jsou:

- ***epimorfismus***: zobrazení h je surjektivní,
- ***monomorfismus***: zobrazení h je injektivní,
- ***isomorfismus***: zobrazení h je bijektivní,
- ***endomorfismus***: h je zobrazení z A do A /$h(A)\subseteq A$/,
- ***automorfismus***: h je zobrazení z A na A /$h(A)=A$/.

Algebry $\langle A;\omega,...\rangle$ a $\langle A';\omega',...\rangle$ se nazývají ***isomorfní***, jestliže existuje isomorfismus z algebry $\langle A;\omega,...\rangle$ do algebry $\langle A';\omega',...\rangle$.

Příklady 3.1.2:

1. $h(x)=\log(x)$ je isomorfismus z $\langle R_+;.\rangle$ do $\langle R;+\rangle$ /symbolem R_+ je označena množina kladných reálných čísel/, neboť:
   - $\log(x)$ je bijekce z R_+ do R,
   - $\log(x.y)=\log(x)+\log(x)$.

2. $h(X)=\det(X)$ je epimorfismus z $\langle R_{nn};*\rangle$ do $\langle R;.\rangle$, neboť:
   - $\det(X)$ je surjekce z R_{nn} /množiny všech čtvercových matic n-tého řádu/ do R,
   - $\det(X*Y)=\det(X).\det(Y)$.

3. $h(x)=abs(x)$ je endomorfismus z $\langle R;.\rangle$ do $\langle R;.\rangle$, neboť:
   - $abs(x)$ je zobrazení z R do R,
   - $abs(x.y)=abs(x).abs(x)$.

4. $h(x)=k.x$ /$k\neq 0$/ je automorfismus (a současně isomorfismus) z $\langle R;+\rangle$ do $\langle R;+\rangle$, neboť:
   - $k.x$ je zobrazení R na R,
   - $h(x+y)=k.(x+y)=k.x+k.y=h(x)+h(y)$.

5. $h(x)=\exp(x)$ je endomorfismus z $\langle R;+\rangle$ do $\langle R;.\rangle$, neboť:
   - $\exp(x)$ je zobrazení z R do R,
   - $\exp(x+y)=\exp(x).\exp(x)$.

   $h(x)=\exp(x)$ je současně isomorfismus z $\langle R;+\rangle$ na $\langle R_+;.\rangle$.

Věta 3.1.2:

Relace "být isomorfní" je ekvivalencí na množině všech algeber téhož typu.

Důkaz:

Označme symbolem ~ isomorfismus mezi algebrami. Třeba dokázat, že relace ~ je RE(flexivní), SY(metrická) a TR(anzitivní).

- RE: $\langle A;\omega,...\rangle \sim \langle A;\omega,...\rangle$
  Isomorfismus je realizován identickým zobrazením h(a)=a pro všechna $a\in A$.

- SY: $\langle A;\omega,...\rangle \sim \langle A';\omega',...\rangle \Rightarrow \langle A';\omega',...\rangle \sim \langle A;\omega,...\rangle$
  Je-li h bijekce realizující isomorfismus z A do A', pak zobrazení h^{-1} je bijekce realizující isomorfismus z A' do A.

- TR: $\langle A;\omega,...\rangle \sim \langle A';\omega',...\rangle \wedge \langle A';\omega',...\rangle \sim \langle A'';\omega'',...\rangle \Rightarrow$
  $\Rightarrow \langle A;\omega,...\rangle \sim \langle A'';\omega'',...\rangle$
  Jsou-li h,h' bijekce představující isomorfismy z A do A' a z A' do A'', pak kompozice těchto bijekcí h''= h o h' představuje isomorfismus z A do A''.

Věta 3.1.3:

Existuje-li epimorfismus /nebo dokonce isomorfismus/ algebry $\langle A;\omega,...\rangle$ do algebry $\langle A';\omega',...\rangle$, pak všechny vlastnosti operací algebry $\langle A;\omega,...\rangle$ se přenášejí na jím odpovídající operace algebry $\langle A';\omega',...\rangle$.

Důkaz:

Na ukázku dokážeme, že z komutativnosti operace ω vyplývá komutativnost operace ω'. Důkazem je následující řetěz rovností:

1. $\omega'(a',b')=$
2. $=\omega'(h(a),h(b))=$ neboť h je surjekce /tj. $(\forall a')(\exists a)[h(a)=a']$/
3. $=h(\omega(a,b))=$ neboť h je morfismus
4. $=h(\omega(b,a))=$ neboť ω je komutativní
5. $=\omega'(h(b),h(a))=$ neboť h je morfismus
6. $=\omega'(b',a')$ Q.E.D.

Pro jiné vlastnosti operací /AS,JE,NU,IN,DI,.../ se platnost tvrzení dokáže obdobně.

Věta 3.1.4:

Je-li h morfismus algebry $\langle A;\omega,...\rangle$ do algebry $\langle A';\omega',...\rangle$, pak $\langle h(A);\omega',...\rangle$ je podalgebrou algebry $\langle A';\omega',...\rangle$.

/Připomeňme, že $h(A)=\{b\in A': (\exists a\in A)[h(a)=b]\}$ je množina obrazů všech prvků z A./

Důkaz:

Předně je zřejmé, že $\emptyset\neq h(A)\subseteq A'$. Zbývá dokázat, že množina h(A) je uzavřená vzhledem k operacím ω'. Důkazem je následující implikační řetězec:

$a_1',a_2',...,a_n'\in h(A) \Rightarrow a_1,a_2,...,a_n\in A \Rightarrow \omega(a_1,a_2,...,a_n)\in A \Rightarrow$
$\Rightarrow h(\omega(a_1,a_2,...,a_n))\in h(A) \Rightarrow \omega'(h(a_1),h(a_2),...,h(a_n))\in h(A) \Rightarrow$
$\Rightarrow \omega'(a_1',a_2',...,a_n')\in h(A)$.

Definice 3.1.4:

Relace ρ na množině A se nazývá ***kongruencí na algebře*** $\langle A;\omega,...\rangle$ jestliže platí:

- relace ρ je ekvivalencí na nosiči A algebry,

- relace ρ splňuje pro všechny operace ω algebry $\langle A;\omega,...\rangle$ podmínku:
  $(a_1\rho b_1)\wedge(a_2\rho b_2)\wedge...\wedge(a_n\rho b_n) \Rightarrow \omega(a_1,a_2,...,a_n)\ \rho\ \omega(b_1,b_2,...,b_n)$.

Definice 3.1.5:

Faktorová algebra algebry $\langle A;\omega,...\rangle$ podle kongruence ρ /na této algebře/ je algebra $\langle \underline{\mathbf{A}};\underline{\boldsymbol{\omega}},...\rangle$, kde

- $\underline{A}=A/\rho$ je faktorová množina množiny A podle ekvivalence ρ,
- operace $\underline{\omega}$ je definována vztahem

$$\underline{\boldsymbol{\omega}}(\underline{\mathbf{a}}_1,\underline{\mathbf{a}}_2,...,\underline{\mathbf{a}}_n)=\underline{\mathbf{b}} \Leftrightarrow_{def} \omega(a_1,a_2,...,a_n)=b,$$

kde

$$a_1,a_2,...,a_n,b\in A,$$
$$\underline{\mathbf{a}}_1,\underline{\mathbf{a}}_2,...,\underline{\mathbf{a}}_n,\underline{\mathbf{b}}\in\underline{\mathbf{A}},$$
$$a_1\in\underline{\mathbf{a}}_1,a_2\in\underline{\mathbf{a}}_2,...,a_n\in\underline{\mathbf{a}}_n,b\in\underline{\mathbf{b}}.$$

Příklady 3.1.3:

1. Ekvivalence $\equiv(\mathrm{mod}\ m)$ na množině celých čísel I /tzv. kongruence modulo m - viz příklad 2.3.1 / je kongruencí na algebře $\langle I;+\rangle$. K tomu stačí dokázat:
   $$x\equiv x' \wedge y\equiv y' \Rightarrow x+y\equiv x'+y'.$$
   Důkazem je následující implikační posloupnost:
   1. $x\equiv x' \wedge y\equiv y'$ předpoklad
   2. $x-x'=j.m \wedge y-y'=k.m$ podle definice $\equiv(\mathrm{mod}\ m)$ z 1.
   3. $(x+y)-(x'+y')=(j+k).m$ sečtením rovností z 2.
   4. $x+y\equiv x'+y'$ podle definice $\equiv(\mathrm{mod}\ m)$ z 3., Q.E.D.
2. Ekvivalence $\equiv(\mathrm{mod}\ m)$ na množině celých čísel I je kongruencí na algebře $\langle I;.\rangle$. K tomu stačí dokázat:
   $$x\equiv x' \wedge y\equiv y' \Rightarrow x.y\equiv x'.y'.$$
   Důkazem je následující implikační posloupnost:
   1. $x\equiv x' \wedge y\equiv y'$ předpoklad
   2. $x-x'=j.m \wedge y-y'=k.m$ podle definice $\equiv(\mathrm{mod}\ m)$ z 1.
   3. $x.y-x'.y = y.j.m \wedge x'.y-x'.y'=x'.k.m$ úpravou 2.
   4. $x.y-x'.y' = (y.j+x'.k).m$ sečtením rovností z 2.
   5. $x.y\equiv x'.y'$ podle definice $\equiv(\mathrm{mod}\ m)$ z 4., Q.E.D.
3. Ekvivalence $\equiv(\mathrm{mod}\ m)$ na množině celých čísel I je kongruencí na algebře $\langle I;+,.\rangle$. Vyplývá to ihned z odstavce 1.a 2.
4. $\langle \underline{I};\underline{+}\rangle=\langle Z_m;\underline{+}\rangle$, $\langle \underline{I};\underline{.}\rangle=\langle Z_m;\underline{.}\rangle$, $\langle \underline{\mathbf{I}};\underline{+},\underline{.}\rangle=\langle Z_m;\underline{+},\underline{.}\rangle$ jsou faktorové algebry algeber $\langle I;+\rangle$, $\langle I;.\rangle$, $\langle I;+,.\rangle$. Operace $\underline{+},\underline{.}$ jsou definovány takto:
   $$\underline{\mathbf{x}}\ \underline{+}\ \underline{\mathbf{y}} =_{def} \underline{x+y}, \quad \underline{\mathbf{x}}\ \underline{.}\ \underline{\mathbf{y}} =_{def} \underline{x.y}$$
5. $h(x)=\underline{x}$, kde $\underline{x}=\{y: y\equiv x\ (\mathrm{mod}\ m)\}$, je epimorfismus z algebry $\langle I;+,.\rangle$ do algebry $\langle \underline{\mathbf{I}};\underline{+},\underline{.}\rangle=\langle Z_m;\underline{+},\underline{.}\rangle$.