Algebra 1 – přednáška 6 – struktury se dvěma operacemi

V prvních pěti přednáškách předmětu jsme se věnovali studiu některých základních vlastností operace, vzniklých z vlastností operací +, · jako axiomy, které platí.

Viděli jsme, že operace podobných vlastností se objevují v mnohých dalších oblastech matematiky. Definice izomorfismu a homomorfismu mezi algebraickými strukturami s jednou operací nám pomáhají popsat (či zjistit), zda jsou dané dvě algebraické struktury naprosto totožné (nejen co do počtu prvků, ale i co se týká algebraických vlastností, jako je inverze prvku, řád prvku, počet prvků podgrupy, atd.), nebo zda known zachování výsledku operace mají aspoň nějakou společnou vlastnost algebraickou (viz homomorfismus).

Ve druhé polovině semestru – přednáškách 6 až 10 – se budeme věnovat algebraickým strukturám, na kterých jsou definovány dvě operace. Dnešní přednáška 6 prezentuje úvody důležité pojmy a jen mírně doplňuje či parafrázuje skripta, str. 68–72.

Studovat zákonitosti, které přinášejí dvě operace na jedné množině M, je přirozeným rozšířením úvah tohoto předmětu, protože v „matematické realitě" vlastně téměř vždy pracujeme s množinami, na kterých jsou definovány operace dvě (N, Z, Q, R, C), a sice sčítání a násobení – co se týká operací odčítání a dělení, zde je možné říci, že se nejedná o dvě další operace, ale že operace odčítání představuje přičtení inverzního prvku vzhledem ke sčítání, operace dělení představuje přinásobení inverzního prvku vzhledem k operaci násobení. Operace odčítání a dělení lze tedy vyjádřit pomocí operací +, · a pojmu inverzního prvku.

Podívejme se nejprve na struktura (Z, +, ·)… proč ne (N, +, ·)? Asi tušíte, že inverzními prvky vzhledem k operaci sčítání k číslům přirozeným budou celá čísla záporná, a že neutrálním prvkem vzhledem ke sčítání je 0 – tedy struktura (Z, +, ·) je z algebraického hlediska ucelenější, kompaktnější než (N, +, ·). Hlavní definici přednášky bychom ovšem měli vyslovit obecně, tedy pro obecné operace ∇, ∗ na množině M:

Def. 6.1. Algebraická struktura (M, ∇, ∗) se nazývá <u>okruh</u> (anglicky: ring), jestliže

a) operace ∇ splňuje na M vlastnosti ①, ②, ③, ④, ⑤, tj. (M, ∇) je komutativní grupa;

b) operace ∗ splňuje na M vlastnosti ①, ②, ③, tj. (M, ∗) je monoid;

c) sama operací ∇, ∗ splňuje tzv. distributivní zákony na M, tj.

(6a) $\forall x, y, z \in M: \quad x * (y \nabla z) = (x * y) \nabla (x * z)$

(6b) $\forall x, y, z \in M: \quad (y \nabla z) * x = (y * x) \nabla (z * x)$

} distributivní zákony jsou dva, protože obecně není zaručena komutativita (5) operace ∗

<u>Pozn.</u>: V definici okruhu tedy celkem platí 10 vlastností; z toho nové jsou pouze vlastnosti 6a, 6b, které sledují/popisují souhru obou operací společně – ostatních 8 jsou pouze vlastnosti vždy jedné ze dvou daných operací, které jsme už sledovali v prvních 5 přednáškách.

Příklad: Podívejme se na množinu Z_6 zbytkových tříd, kde jsou celá čísla rozdělena do šesti podmnožin podle toho, jaký zbytek dávají po dělení šesti. Pouze z pohodlnosti tyto zbytkové třídy označujeme stejně jako čísla 0, 1, 2, 3, 4, 5.

Na takto definových prvcích lze zavést operace sčítání a násobení s následujícími tabulkami:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Když prozkoumáme vlastnosti těchto operací, tak zjistíme, že

a) + splňuje vlastnosti 1, 2, (3), 4, 5 → 0 je neutrální

b) · splňuje vlastnosti 1, 2, (3), 5 ... nesplňuje 4, protože neexistují inverze vzhledem k násobení pro prvky 0, 2, 3, 4 → 1 je neutrální

c) +, · splňují oba distributivní zákony 6a, 6b

---

tedy celkem $(Z_6, +, \cdot)$ je komutativní okruh

↑ slovo „komutativní" je doplněno pro operaci ·, která v okruhu obecně není definována

Pozn.: Vlastnost asociativity (3) pro operace +, · bychom mohli ověřit z tabulky, ale ta tabulka bychom museli udělat prostorovou, měla by rozměr $6\times6\times6$, a vyrobením dvou těchto prostorových tabulek o 216 prvcích (každou s jiným uzávorkováním) bychom pak mohli potvrdit, že prvky na příslušných pozicích obou těchto prostorových tabulek jsou stejné.

Podobně náročné by bylo ověření distributivních zákonů 6a, 6b: díky komutativitě násobení „6a = 6b", tj. stačí ověřovat jen jeden z těchto vztahů, ale opět bychom museli porovnávat výsledek operace $x*(y\nabla z)$ v tabulce $6\times6\times6$, a výsledek operace $(x*y)\nabla(x*z)$ v tabulce 36×36, tj. to je taky spousta práce. Obyčejně se při důkazu (3), (6a), (6b) odkazujeme, že tyto vlastnosti platí pro běžné operace +, · na množině reálných čísel, a tam se tyto vlastnosti považují za axiomy, a nebo bychom je mohli dokázat důkazem matematickou indukcí, protože prvky těchto množin lze uspořádat.

Vraťme se ještě k našemu příkladu struktury $(Z_6, +, \cdot)$, která je komutativním okruhem. Už jsem upozorňoval na jednu „patologickou" = nenormální vlastnost v tom smyslu, že se s ní u běžných čísel nesetkáme:

$2\cdot3=0$ v Z_6

↑ součin dvou prvků nenulových je roven „nule" = neutrálnímu prvku vzhledem ke sčítání.

Tuto vlastnost jsme schopni matematicky popsat až při uvažování obou operací SOUČASNĚ:

Def. 6.2 Struktura $(M, \nabla, *)$ obsahuje nenulové dělitele nuly, když $\exists\, a, b \in M$:

NDN: $a \neq 0,\ b \neq 0 \ \wedge\ a * b = 0$

kde 0 je neutrální prvek vzhledem k ∇

Všimněte si, že ve vymezení pojmu se objevují obě operace, ikdyž ∇ je trochu skrytá: 0 je neutrální prvek vzhledem k ∇

Určitě tuto zvláštní vlastnost, která u celých čísel nenastává, chceme nějak zachytit (či spíše vyloučit) v definici algebraické struktury — touto strukturou je tzv. obor integrity

Def. 6.3 Algebraická struktura $(M, \nabla, *)$ se nazývá obor integrity (anglicky: integral domain), jestliže současně platí

a) operace ∇ splňuje na M vlastnosti 1, 2, 3, 4, 5, 7; (M, ∇) je komutativní grupa

b) operace $*$ splňuje na M vlastnosti 1, 2, 3, NNDN, 5, 7;
$(M, *)$ je komutativní monoid, který neobsahuje NDN vzhledem k ∇

c) platí distributivní zákon, který je díky komutativitě operace $*$ v předchozím tvaru už jen jeden (6) $\forall x, y, z \in M: x * (y \nabla z) = (x * y) \nabla (x * z)$

Pozn.: 1) V definici oboru integrity tedy platí současně 11 vlastností — dvě z nich už jsou komutativity obou operací.

2) Integrita tedy nyní v algebraickém smyslu znamená, že daná struktura je zcela čistá od té „bizarní" vlastnosti, nenulových dělitelů nuly; podobně v Bibli integrita = bezúhonnost v očích Boha, integrita lingvisticky = celistvost, zachování svých složek (... is an integral part of ... je nedílnou součástí něčeho).

Příklad: $(\mathbb{Z}, +, \cdot)$ je tedy algebraický obor integrity!

No a při náhradě vlastnosti NNDN v definici 6.3 vlastností $I = (4)$ dostaneme třetí důležitou definici algebraické struktury, a to definici tělesa. Musíme být opatrní i u vlastnosti inverze s inverzním prvkem 0 vzhledem k násobení — ten u běžných množin $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ neexistuje, tedy hledat ho by byla marná snaha i v velmi hezkých množinách; z toho důvodu zavádíme označení

$\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Z}_6^*, \mathbb{Z}_5^* \ldots$ množiny, ze kterých byla vyloučena 0

obecně $M^* \ldots$ množina, ze které byl vyloučen neutrální prvek 0 vzhledem k 1. operaci ∇

Def. 6.4. Algebraická struktura $(M, \nabla, *)$ se nazývá těleso (anglicky: field), jestliže

a) operace ∇ splňuje na M vlastnosti 1, 2, 3, 4, 5, 7; (M, ∇) je komutativní grupa

b) operace $*$ splňuje na M^* vlastnosti 1, 2, 3, 4, 5, 7; $(M^*, *)$ je komut. grupa

c) platí distributivní zákon na M: $\forall x, y, z \in M: x * (y \nabla z) = (x * y) \nabla (x * z)$

Pozn.: V definici tělesa je tedy 11 vlastností, vzhledem k oboru integrity byla NNDN vyměněna za $(4) = I$

Příklad a) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ → jsou tělesa, protože množiny $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ obsahují všechny inverzní prvky vzhledem k násobení.

b) i $(\mathbb{Z}_5,+,\cdot)$, $(\mathbb{Z}_7,+,\cdot)$, $(\mathbb{Z}_{13},+,\cdot)$ → jsou tělesa, protože množiny $\mathbb{Z}_5^*, \mathbb{Z}_7^*, \mathbb{Z}_{13}^*$ obsahují všechny inverzní prvky vzhledem k násobení

(problémem s NDN a neexistencí inverzních prvků se objevuje pouze u $\mathbb{Z}_n$, kde n není prvočíslo; blíže viz str. 54–55 ve skriptech)

Aby algebra získala hezké tvary, tj. řekla v jedné větě významné slovo pro více různých množin a operací, podívejme se ještě na operace $\cup, \cap, \div$, zda se v těchto končinách vyskytují ti bizarní NDN:

Příklad. Zjistěte, co jsou z algebraického hlediska struktury a) $(2^A, \cup, \cap)$ b) $(2^A, \cap, \cup)$ c) $(2^A, \div, \cap)$

(2^A ... množina všech podmnožin množiny A pro $A = \{1,2,3,4,5\}$)

---

ad a) $(2^A, \cup, \cap)$ ... vypišme si vlastnosti operací $\cup$ ... 1, 2, 3 (... „nula" je $\emptyset$), 5

(4 neplatí, protože $\{1\} \cup X \neq \emptyset$ pro žádnou podmnožinu X)

$\cap$ ... 1, 2, 3 (... „jednotka" je A), 5

(4 neplatí, protože $\{1\} \cap X \neq \{1,2,3,4,5\}$ pro žádnou podmnožinu X)

$\{1\} \cap \{2,3\} = \emptyset$ ... existují zde NDN!!!

distributivní zákon (6): $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ ... lze dokázat Vennovými diagramy

tuto strukturu bychom snad mohli nazvat polookruhem, který obsahuje NDN
protože množina podmnožin není grupou vzhledem k žádné z operací $\cup, \cap$

ad b) $(2^A, \cap, \cup)$ ... vlastně tytéž operace, pouze vlastnost (6) je NAOPAK – sjednocení ve významu „násobení" – průnik ve významu „sčítání"

$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ ... lze dokázat Vennovými diagramy!!

$\{1,2\} \cup \{3,4,5\} = A$ existují zde NDN!!!

↓ „nula" je zde něco jiného než v příkladu (a) ... nulu vždy určujeme jako nulový prvek 1. zadané operace, v rovnosti samotné pak vystupuje 2. operace

opět $(2^A, \cap, \cup)$ je polookruh, který obsahuje NDN

Co je na příkladech a), b) zajímavé, je to, že distributivní zákon zde platí, i když zaměníme pořadí obou operací!

$$X\cap(Y\cup Z)=(X\cap Y)\cup(X\cap Z)$$
$$X\cup(Y\cap Z)=(X\cup Y)\cap(X\cup Z)$$

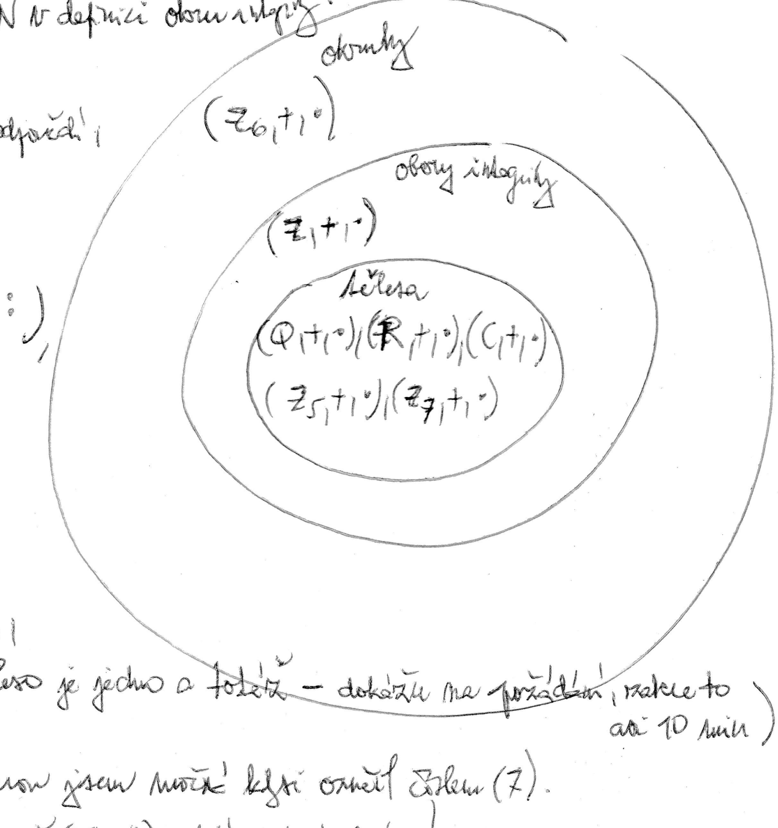
Třeba u čísel distributivní zákon platí jen v jednom směru:

$$3\cdot(4+5)=3\cdot 4+3\cdot 5$$
$$23=3+(4\cdot 5)\neq(3+4)\cdot(3+5)=180$$

To je z algebraického hlediska hodně zajímavé a vedlo to ke studiu množiny všech podmnožin (ještě podrobněji), zavedení pojmu distributivní uspořádané množiny, atd. Tím se zde nebudeme už zabývat – jen si můžete pamatovat, že struktura $(2^A,\cup,\cap)$ se z hlediska této další teorie nazývá Booleho algebra. Smysluplné studium by zde zabralo minimálně polovinu semestru. Celá teorie Booleho algeber má i aplikační využití v souvislosti s konstrukcemi logických obvodů pro počítače. Celá teorie je náročná, ovšem řadu věcí lze kreslit v Hasseových diagramech, takže by to šlo pěkné téma pro bakalářskou práci – spíše jen pro někoho, kdo měl A nebo B ze základů matematiky a souhlasil by s výukou ještě 2 hod/14 dní, aby nemusel dané věci studovat úplně sám.

Ondřeje Bočka a Vítězslava Křížka bude určitě zajímat, proč nadřazuji vlastnost (4) v definici tělesa nad vlastnost NNDN v definici oboru integrity. To jsem ještě dosud nevysvětlil.

Pokusím se jim odpovědět. Jednou z odpovědí, proč těleso je „více než" obor integrity (v tom smyslu, že splňuje přísnější podmínky, tj. těles je vlastně méně než oborů integrity – viz obr.:) je existence $(\mathbb{Z},+,\cdot)$... to je obor integrity, který není tělesem.



Platí to však vždy, že obor integrity je „méně než" těleso? Druhou možnou odpovědí je věta, že každý konečný obor integrity je tělesem (jinými slovy, pokud M je konečná, tak pojem obor integrity a těleso je jedno a totéž – dokážu na požádání, zabere to asi 10 min)

Třetí odpověď na to jde přes vlastnost krácení, kterou jsem možná kdysi označil číslem (7). Pokud si dobře vzpomínám, říkal jsem vám, že v grupě $(M,*)$ platí vlastnost krácení

$$(7)\quad \forall x,y,z\in M:\quad x*y=x*z \Rightarrow y=z$$

(Dokážeme jednoduše: v grupě platí (4), tj. $\exists x^{-1}$: vynásobme předpoklad inverzí zleva: $x*y=x*z \,/\, x^{-1}*$ zleva

$$y \overset{(3)}{=} 1*y \overset{(4)}{=} x^{-1}*x*y = x^{-1}*x*z \overset{(4)}{=} 1*z \overset{(3)}{=} z$$
$$y=z$$

důkaz je hotov)

| věta matematická: ①, ②, ③, ④ ⇒ ⑦ |

Otázku si rozumíme položit, která souvisí se zákonem krácení:
lze krátit ve strukturách, ve kterých neexistuje inverze x^{-1} ke každému prvku – lze například krátit v okruhu nebo v oboru integrity?

$(\mathbb{Z}_6, +, \cdot)$ je okruh, víme, že zde krátit nelze $2 \cdot 2 = 2 \cdot 5 \not\Rightarrow 2 = 5$

$(\mathbb{Z}, +, \cdot)$ je obor integrity a víme (ze zkušeností?), že v celých číslech krátit lze, platí to však vždy? Co kdyby je to jen náhoda? Ukážeme se, že to platí vždy:

Věta z matematiky: V každém okruhu $(M, +, \cdot)$ (0, 1) platí: je splněna vlastnost $(7)^*$ $\iff$ NNDN

$$\left((7)^* \text{ pro } a,b,c \in M \,(a \neq 0 : a \cdot b = a \cdot c \Rightarrow b = c) \right)$$

toto je normální požadavek, na který jsme zvyklí ze celých čísel

její důkaz: "$\Rightarrow$" předpokládejme, že $(M, +, \cdot)$ je okruh splňující $(7)^*$, chceme dokázat, že NNDN

$\forall a,b \in M$, pro které $a \cdot b = 0$

1) pokud $a = 0$, jsme hotovi, protože a, b nejsou NDN
2) pokud $a \neq 0$, můžeme psát

$$a \cdot b = 0 = a \cdot 0$$

$$a \cdot b = a \cdot 0 \xrightarrow{\text{platí } (7)^*} b = 0, \text{ tedy opět } a, b \text{ nejsou NDN}$$

$$\| \; c$$

celkem aspoň 1 ze čísel a, b je nula $\Rightarrow$ nejedná se o NDN, to jsme chtěli dokázat

"$\Leftarrow$" předpokládejme, že $(M, +, \cdot)$ je okruh NNDN, ukážeme, že splňuje $(7)^*$

$\Downarrow$

pokud $a \neq 0$, $a \cdot b = a \cdot c$ .... a^{-1} NEMUSÍ EXISTOVAT, ALE NYNÍ VYUŽIJEME TÉ DRUHÉ OPERACE, TJ. EXISTENCE prvku $(-a \cdot c)$

$a \cdot b - a \cdot c = 0$ ... využijeme distributivní zákon (6a)

$a \cdot (b - c) = 0$

víme, že okruh neobsahuje NDN $\Rightarrow$ musí nastat $b - c = 0$

$b = c$, dokázali jsme $(7)^*$

Teď už víme, že vlastnost $(7)^*$ je ekvivalentní s vlastností NNDN. Ale vlastnost $(7)^*$ se v každém tělese snadno dokáže vynásobením inverzí a^{-1}, která nám vždy existuje pro $a \neq 0$. Tedy ekvivalentně: každé těleso NNDN

(tedy $(M, +, \cdot)$ je těleso $\Rightarrow (M, +, \cdot)$ je obor integrity. Naopak to neplatí, protipříkladem je $(\mathbb{Z}, +, \cdot)$)

Tím pádem je odpovědět obrázek na předchozí straně.