

Tělesa

Martin “Lishaak” Podloucký

11. července 2007

1 Úvodem

Jemným a nenásilným úvodem do algebraických těles bych rád započal sérii článků popisující naprosté základy lineární algebry, kterou spousta lidí musí na vysoké škole překousnout, přestože je matematika třeba vůbec nebaví. Dopředu nemám naplánováno, kolik článků a na jaká témata napíšu. Všechno záleží na tom, jak se vám moje práce bude líbit a po jakých tématech budete toužit. Pokud se vám tedy můj článek líbí (nebo k němu máte jakoukoliv připomínku či výhradu), dejte mi o tom prosím vědět na můj e-mail [lishaak\[zavinac\]matfyz.cz](mailto:lishaak[zavinac]matfyz.cz).

K pochopení následujícího výkladu nepotřebujete žádné speciální matematické dovednosti ani vědomosti. Stačí rozumět naprostým základům středoškolské matematiky a mít chuť se něco nového dozvědět či přiučit.

2 Bubák jménem algebraické těleso

Pokud vám již samotný název *algebraické těleso* nahání hrůzu, vezte, že opravdu není čeho se bát. Takové těleso je ve skutečnosti velmi jednoduchá věc, podíváme-li se na něj z toho správného úhlu.

Algebraické těleso je jakákoliv **libovolná množina** plus dvě **binární operace**, splňující určité podmínky. Toť vše. Nic víc ani míň. Jak vidíte, rozhodně nic nebezpečného nebo hrůzostrašného. A jakmile toto víme, můžeme se už beze strachu jít podívat trošičku blíž.

2.1 Množina prvků tělesa

Naši libovolnou množinu si označíme T a jejím prvkům budeme říkat **prvky tělesa**. Věřte, přátelé, že množina prvků tělesa může být naprosto libovolná.

Může to být množina všech sudých čísel, množina všech ponožek, ke kterým nemáte druhou do páru nebo třeba vaše sbírka plyšových slonů. Snad jediná podmínka je, že množina T nesmí být prázdná. To bychom si totiž mnoho legrace neužili.

2.2 Binární operace

Pokud vám není ihned zřejmé, cože to vlastně je ta *binární operace*, můžete si ji představit jako takový **malý mlýnek**. Vložíte do něj dva (odtud to *binární* v názvu) prvky nějaké množiny, zatočíte lehce klikou a on vám vypadne nějaký další prvek z vaší množiny. Taková hezká binární operace je například dělení. Zajímá vás, kolik je $10 / 5$? Vezměte si binární operaci dělení (mlýnek), kde vaše množina bude množina reálných čísel. Do mlýnku nasype nejprve desítku a potom pětku, zatočte klikou a, světe div se, vypadne dvojka.

My si naše dvě operace pojmenujeme **sčítání** a **násobení** a budeme je značit \oplus a \otimes . Nenechte se zmást jejich názvem. Se sčítáním a násobením, které používáme normálně, nemusí mít tyto operace mnoho společného. Je to právě kvůli tomu, že prvky tělesa můžou být jakékoliv objekty. A právě na plyšové slony nebo ponožky se “naše” sčítání a násobení použít nedá.

3 Operace nad tělesem

Operace \oplus a \otimes musí splňovat určité podmínky. Nemůžeme si je zavést úplně libovolně. Smyslem zavádění těchto operací je totiž zobecnění obyčejného sčítání a násobení, které používáme na čísla. Chceme, aby se tyto operace daly zavést tak, abychom je mohli použít na prvky tělesa, které, jak už víme, mohou být naprosoto libovolné objekty, tedy ne jenom čísla. Přesto ale chceme, aby si operace \oplus a \otimes zachovaly jakýsi základní smysl sčítání a násobení. To zajistíme tak, že zavedeme desatero podmínek, které musí tyto operace splňovat aby naše struktura byla tělesem. Těmto podmínkám budeme říkat **axiomy tělesa**. Zde jsou:

1. **Komutativita sčítání.**

Pro libovolné dva prvky a, b z tělesa T musí platit $a \oplus b = b \oplus a$.

2. **Asociativita sčítání.**

Pro libovolné tři prvky a, b, c z tělesa T musí platit $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

3. **Existence nulového prvku.**

Musí existovat prvek z tělesa T , označíme ho 0 (pozor, neplést s číslem 0), který musí mít tu vlastnost, že pro libovolný prvek a z tělesa T platí $a \oplus 0 = a$.

4. **Existence opačného prvku.**

Musí existovat prvek z tělesa T , označíme ho $-a$, který musí mít tu vlastnost, že pro libovolný prvek a z tělesa T platí $a \oplus -a = 0$.

5. **Komutativita násobení.**

Pro libovolné dva prvky a, b z tělesa T musí platit $a \otimes b = b \otimes a$.

6. **Asociativita násobení.**

Pro libovolné tři prvky a, b, c z tělesa T musí platit $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

7. **Existence jednotkového prvku.**

Musí existovat prvek z tělesa T , označíme ho 1 (pozor, neplést s číslem 1), který musí mít tu vlastnost, že pro libovolný prvek a z tělesa T platí $a \otimes 1 = a$.

8. **Existence inverzního prvku.**

Musí existovat prvek z tělesa T , označíme ho a^{-1} , který musí mít tu vlastnost, že pro libovolný prvek a různý od 0 z tělesa T platí $a \otimes a^{-1} = 1$.

9. **Distributivita.**

Pro libovolné tři prvky a, b, c z tělesa T musí platit $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

10. **Netrivialita.**

Nulový a jednotkový prvek nesmí být jeden a ten samý. Tedy $0 \neq 1$

Pro toho, kdy by se chtěl pocvičit v matematickém formalizmu, jsem zde napsal axiomy tělesa tak, jak se v matematické hantýrce zapisují.

1. $\forall a, b \in T \quad a \oplus b = b \oplus a$

2. $\forall a, b, c \in T \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$

3. $\exists 0 \in T \forall a \in T \quad a \oplus 0 = a$

4. $\exists -a \in T \forall a \in T \quad a \oplus -a = 0$

5. $\forall a, b \in T \quad a \otimes b = b \otimes a$

6. $\forall a, b, c \in T \quad (a \otimes b) \otimes c = a \otimes (b \otimes c)$
7. $\exists 1 \in T \forall a \in T \quad a \otimes 1 = a$
8. $\exists a^{-1} \in T \forall a \in T, a \neq 0 \quad a \otimes a^{-1} = 1$
9. $\forall a, b, c \in T \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
10. $0 \neq 1$

Ted' si možná říkáte, že těch axiomů je strašlivě moc. Všechny jsou ale snadno pochopitelné, když si uvědomíme, co znamenají. První čtyři popisují obvyklé vlastnosti sčítání a další čtyři obvyklé vlastnosti násobení, které jsou navíc těm prvním čtyřem velmi podobné. Devátý axiom říká, v jakém vztahu jsou spolu sčítání a násobení. Jenom desátý je taková spíše technická záležitost, která zajišťuje, aby to těleso nemohlo mít nějaké podivné vlastnosti.

Všimněte si, jak hezky jsme se vyhnuli zavádění odčítání a dělení. Tyto operace jsou zavedeny pomocí přičítání opačného prvku a násobení inverzním prvkem. Tedy například $4 - 2$ je pouze zkratka za $4 + (-2)$ a $4 / 2$ je pouze zkratka za 4×2^{-1} .

4 Přehledka těles

Nyní již máme formálně zaveden pojem algebraické těleso. Pokud bychom chtěli nějak intuitivně vyjádřit, cože to vlastně to těleso je, můžeme říct, že je to jakási struktura, která nám umožňuje sčítat, odčítat, násobit a dělit libovolné objekty, na kterých dokážeme tyto operace zadefinovat, a to způsobem, podobným tomu, jak tyto operace provádíme v elementární aritmetice.

4.1 Naše první těleso

Když už jsme si tak hezky vymysleli a popsali tělesa, pojďme si nějaké skutečné těleso sestrojít. Nejdříve si zvolíme množinu prvků tělesa. Zatím nebudeme příliš experimentovat s plyšovými slony nebo ponožkami a jako prvky tělesa si zvolíme přirozená čísla. Aby to všechno bylo opravdu jednoduché, vezmeme pouze čísla 0, 1, 2, 3, 4. Tedy naše množina T bude vypadat takto:

$$T = \{0, 1, 2, 3, 4\}$$

Ted' už zbývá pouze nějak šikovně nadefinovat operace \oplus a \otimes . Tady si vypomůžeme operacemi sčítání a násobení, které již známe z aritmetiky. Trošku je ale upravíme, aby fungovaly i na našem tělese.

- **Operace \oplus**

Součet dvou prvků $a \oplus b$ provedeme tak, že vypočteme zbytek po dělení pěti ze součtu $a + b$. Sčítání v našem tělese tedy budou vypadat takto:

$$1 \oplus 1 = 2 \quad 1 \oplus 3 = 4 \quad 2 \oplus 3 = 0 \quad 4 \oplus 2 = 1 \quad \text{apod.}$$

- **Operace \otimes**

Součin dvou prvků $a \otimes b$ provedeme tak, že vypočteme zbytek po dělení pěti ze součinu ab . Násobení v našem tělese tedy budou vypadat takto:

$$1 \otimes 1 = 1 \quad 2 \otimes 2 = 4 \quad 2 \otimes 3 = 1 \quad 4 \otimes 2 = 3 \quad \text{apod.}$$

A je to. Nyní už máme vyrobené plnohodnotné těleso. Ještě by to chtělo ověřit platnost všech axiomů abychom si byli jisti, že jsme vyrobili skutečně těleso a ne nějaký paskvil.

- **Komutativitu** a **asociativitu** sčítání a násobení jste jistě schopni ověřit sami, stejně tak **distributivitu**.
- Z toho, jak jsme zadefinovali sčítání a násobení taky plyne, že existuje nulový prvek (v našem případě je to náhodou zrovna číslo 0) a jednotkový prvek (v našem případě 1), které jsou navzájem různé.
- Teď už nám tedy zbývá ověřit pouze existenci opačného a inverzního prvku. Určitě všichni vidíme, že ke každému číslu z množiny $\{0, 1, 2, 3, 4\}$ existuje nějaké číslo z té samé množiny tak, že výsledek jejich součtu je pět (tedy v našem tělese 0). Obdobně to platí také pro násobení a výsledek 6 (v našem tělese 1). Zkuste si to!

4.2 Příklady dalších těles

Před chvílí jsme vyrobili těleso, které má pět prvků. Ukazuje se, že stejným způsobem se dají vyrobit i další tělesa, kde počet jejich prvků je prvočíslo. Takovým tělesům se říká **tělesa zbytkových tříd** a označují se \mathbb{Z}_p , kde p je počet prvků tělesa, a jsou hodně často používána jak v matematice nebo informatice tak samozřejmě i v různých písemkových příkladech.

Jdou vyrobit i tělesa s jiným než s prvočíselným počtem prvků? Ano jdou, ale už to nejde takovým způsobem, jak jsem to předvedl před chvílí. Proč? Představte si těleso vyrobené výše popsáním postupem, které má pouze čtyři prvky. V takovém tělese platí $2 \otimes 2 = 0$. Tedy součin dvou nenulových čísel

je nula. To se v tělese nesmí stát. Není to sice přímo zakázáno v axiomech tělesa, ale dá se to z nich celkem snadno odvodit. Ukazuje se ovšem, že pokud se místo čísel jako prvků tělesa použijou polynomy, dají se vyrobit i tělesa, jejichž počet prvků je mocninou prvočísla. Tedy čtyřprvkové těleso existuje, neboť čtyřka je mocninou dvojky.

Samozřejmě jsou možná i tělesa s nekonečným počtem prvků. Tak například množina reálných čísel plus naše obvyklé operace sčítání a násobení také tvoří těleso. To samozřejmě neplatí jen pro čísla reálná, ale také pro přirozená, celá, racionální i komplexní.

A to nejlepší nakonec. Nikdo nám samozřejmě nepředepisuje, že tělesa musí být tvořena čísla, polynomy nebo vůbec nějakými matematickými objekty. Jak už jsem říkal, můžete si vyrobit těleso ponožek, plyšových slonů atd. Jediný problém asi bude, jak zadefinovat sčítání a násobení na slonech. Tady je zajímavá ta věc, že se vám nikdy nemůže podařit vyrobit těleso, které obsahuje šest ponožek. Protože šestka není ani prvočíslo ani mocnina prvočísla. Ale můžete klidně vyrobit těleso, které čítá sedmnáct ponožek, každou z nich si očíslovat (bílá ponožka bude 0, černá 1, zelená 2 atd.) a sčítat je potom stejně, jako jsme my sčítali ve tělese zbytkových tříd.

5 A k čemu to všechno je?

Pokud jste dočetli až sem, možná si říkáte, na co probůh potřebujem takovou šílenou strukturu jako je algebraické těleso? Inu, tělesa jsou velice důležitá, jak z teoretického hlediska, neboť popisují a hlavně zobecňují to, čemu by se dalo říkat počítání, tedy aritmetiku, tak z praktického hlediska, neboť spousta matematických nebo informatických problémů se snadněji vyřeší, představíme-li si je jako počítání v tělesech. Konečná tělesa mají například velký význam pro kódy na CD nebo DVD discích. Jinak, co se týče samotné lineární algebry, jsou tělesa základním kamenem pro další, složitější a tím také daleko užitečnější a zajímavější struktury, jako jsou například vektorové prostory. Ty totiž tvoří jakýsi základ celé lineární algebry.