Definice, důkazy, abstrakce

Definice se nemusíte učit nazpaměť, můžete používat vlastní slova. Je však třeba pochopit smysl definic a seznámit se s matematickým vyjadřováním. Časem zjistíte, že správné vyjádření vlastními slovy se příliš neliší od definice z té či oné učebnice. Pro zajímavost můžete porovnat definice téhož pojmu z různých učebnic. Zjistíte, že se definice základních matematických pojmů v různých učebnicích od sebe příliš neliší.

Důkazy byste měli hlavně **pochopit**. Matematika se od ostatních věd liší právě tím, že každé tvrzení **dokazuje**. Některé důkazy jsou snadné, některé jsou složitější, některé jsou velmi obtížné. V předmětu Lineární algebra jsou skoro všechny důkazy jednoduché – ovšem **za předpokladu, že dobře rozumíte zavedeným pojmům a zvládáte předchozí látku** – pokud si uvědomíte, co znáte a co chcete dokázat, je důkaz často jednoduchou cestou od předpokladu ke tvrzení (pouze mechanickým odvozováním či prověřením vlastností). V matematické analýze jsou důkazy většinou obtížnější (je třeba přesně znát k daným tvrzením předpoklady).

V lineární algebře činí často problém velká **abstrakce** probírané látky. Proto **je velmi užitečné si při studiu představovat pod obecnými pojmy konkrétní objekty!** Například pod abstraktním pojmem *těleso* si představovat *těleso reálných čísel*.

K důkazu 2.6 (druhá, obtížnější implikace)

Nechť a, b, c jsou prvky Z_p, předpokládejme, že $a \neq 0$, $b > c$. Ukážeme, že v Z_p je

$$ab \neq ac\ .$$

Postupujeme sporem, předpokládáme, že v Z_p se rovnají součiny ab, ac, což znamená, že se při „normálním počítání“ liší o nějaký násobek prvočísla p.

$$\text{Tedy}\quad ab - ac = kp,\quad \text{neboli}\quad a(b-c) = kp.$$

Pravá strana je dělitelná prvočíslem p, tedy musí být prvočíslem p dělitelná i levá strana. Dělí-li prvočíslo součin, musí dělit některého činitele. Proto musí p dělit buď a nebo $b–c$. Protože je a různé od nuly a menší než p, není to možné. A ze stejných důvodů nemůže p dělit $b–c$.

Je-li a nenulový prvek v Z_p, jsou tedy prvky $a\cdot 0$, $a\cdot 1$, $a\cdot 2$, …, $a\cdot(p-1)$ navzájem různé, jsou to tedy právě všechny prvky 0, 1, 2, …, $p–1$ ze Z_p, proto je mezi nimi také číslo 1. Pro nějaké b ze Z_p je tedy $a\cdot b = 1$, tedy b je inverzním prvkem k prvku a.

1. 10. 2020