Algebraici nejsou hustodémoni

Alexandr Kazda

Cílem tohoto krátkého textu je vám pomoci úspěšně přežít první kontakt s teorií grup, okruhů a modulů. Nechci vás tu učit matematiku, ale spíš naznačit, jaký druh myšlení je v algebře potřeba.

Abstraktní algebra je oproti třeba analýze méně intuitivní; sice tu nemáme epsilony a delty, ale zato se bavíme o objektech, které jako by spadly z Měsíce. Grupy? Okruhy? Tělesa? Moduly? Kam na ty názvy ti matematici chodí?

Odpověď na poslední otázku je, že názvy matematických pojmů vyplývají z historického vývoje – algebra z Měsíce nespadla, je to lidské dílo. V dnešní podobě se algebra zformovala relativně nedávno, během 19. a první poloviny 20. století. (Věřte nevěřte, na začátku byla geometrie a otázka řešitelnosti rovnic.) Pokud vám bude algebra připadat jako náhodný shluk tvrzení, sáhněte po nějaké knížce o vývoji moderní matematiky – v historickém kontextu by vám mohly všechny ty faktorgrupy začít dávat smysl. Dobré (byť ne vždy zcela přesné) čtení je třeba knížka Simona Singha „Velká Fermatova věta“ nebo webový článeček "The Origins of Abstract Algebra".
`http://www.math.hawaii.edu/ lee/algebra/history.html`

Tak řekněme, že uznáváme právo algebry na existenci a víme, že se algebraické objekty hodí pro mnoho ryze praktických aplikací (například tři věci na k: kryptografie, krystalografie a krutá částicová fyzika). Jak si na algebru zvyknout? Existuje několik triků, které vám putování po grupách a okruzích ulehčí.

1 Tipy a triky

- Pamatujte, že ekvivalence se typicky dokazuje jako dvě implikace.
- Podobně rovnost množin se nejsnáze ověří jako dvě inkluze.
- Obecně: Velký problém se nejlépe vyřeší tak, že si ho rozložíte na několik lehčích problémů (hledám místa, kudy lze na problém zaútočit).
- Je problém příliš těžký? Zkuste zformulovat a vyřešit jeho lehčí variantu (třeba pro komutativní grupy místo obecných grup).
- Nezapomňte, že pokud máme $\forall g, h \phi(g, h)$, kde $\phi(g, h)$ je nějaká podmínka (třeba rovnice), tak může být g=h.

- Když na vás vybafne rovnice, můžete ji zleva i zprava násobit písmenky a dostanete důsledky rovnice (často dokonce dostanete rovnici ekvivalentní s tou původní). Jaká písmenka volit? To je občas oříšek, ale na druhou stranu někdy ja to očividné: Rovnici $xy^{-1} = zy^{-1}$ třeba skoro určitě chci vynásobit y zprava, abych dostal $x = z$.
- Z dobrých důvodů je v případě grup oblíbená posloupnost písmenek ghg^{-1} (konjugace). Pokud nevíte, co dál, zkuste najít/vyrobit podobný výraz.
- Tajmený výraz homomorfismus znamená „chová se dobře na operace“. Pokud se v zadání problému vyskytuje homomorfismus, nejspíš v nějaký okamžik budete potřebovat použít vztah typu $f(xy) = f(x)f(y)$.
- A konečně: Spousta věcí ze skript se dá dokázat z definice: Prostě dosaďte do definice pojmu X vlastnosti pojmu Y a použijte selský rozum. Když budete mít štěstí (jakože asi v deseti procentech případů ho mít nebudete, protože to jsou těžké věty), tak dokážete, že každé Y je X.

1.1 Intuice

Algebra bez intuice je na houby. Abyste měli šanci tenhle kurs se ctí absolvovat, potřebujete si při slově „grupa“ představit něco jiného než „to je ta divná věc ze skript“. Proto silně doporučuji vybudovat si zoo z grup a okruhů. Na poměrně konkrétních obyvatelích tohoto zoo pak můžete testovat hypotézy a zkoušet dokazovat věty.

1.1.1 Pavilon grup

(neděste se, detaily budou na cvičeních):

- $(\mathbb{Z}_n, +)$ (komutativní, konečná, snadno se v ní počítá)
- $\mathbb{Z}_p^*$ (pořád komutativní a konečná, ale už dá práci spočítat inverzy)
- $(\mathbb{Z}, +)$ (komutativní, nekonečná, pěkná)
- Grupa D_n symetrií n-úhelníka s operací skládání symetrií
- S_n (nejobecnější konečné grupy)

1.1.2 Pavilon okruhů

- Stará dobrá tělesa: $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$.
- $\mathbb{Z}_n$
- $\mathbb{Z}$
- $M(n, \mathbb{R})$ (matice)
- $M(n, \mathbb{Z}_k)$
- Polynomy v jedné neurčité nad $\mathbb{R}$, $\mathbb{Z}$

1.1.3 Kabinet modulů

- $\mathbb{R}^n$ (jako vektorový prostor) nad $\mathbb{R}$
- $\mathbb{R}^n$ jako modul nad $M(n, \mathbb{R})$
- $\mathbb{Z}$ nad $\mathbb{Z}$ (násobení je násobení v $\mathbb{Z}$)
- $(\mathbb{Z}_n, +)$ nad $\mathbb{Z}$ (násobení jako v $\mathbb{Z}_n$)