

Požadavky ke zkoušce z Algebry, 2024/25

David Stanovský

Předmět zkoušky:

Teorie potřebná k úspěšnému vykonání zkoušky se nachází v učebním textu algebra22. Přečíst a pochopit byste měli všechny části, které se objevily na přednášce (viz tabulka na webu), i když na některé níže uvedené drobnosti se ptát nebudu. Čtete nejen holá znění definic, vět a důkazů, ale také ty pasáže mezi nimi, které objasňují kontext, a také všechny poznámky a příklady — často se ptám na příklady algebraických struktur splňujících jisté vlastnosti!

K úspěšnému vykonání zkoušky je dále potřeba jistá *počtářská zručnost*: měli byste znát postupy řešení všech základních úloh ze cvičení a umět je aplikovat i na jiné úlohy podobného typu (tedy nejen na ty, které vznikly triviální záměnou hodnot). V rámci tréninku si spočtete všechny úlohy na pracovních listech ke cvičením (tj. nejen ty, „co by měl každý umět“); pokud tak učiníte, u zkoušky by vás nemělo nic překvapit.

Nebudu zkoušet následující části textu algebra22:

- vícenásobné kořeny (sekce 3.5)
- důkaz spočetnosti množiny algebraických čísel (sekce 3.6)
- řešení diofantických rovnic počítáním v rozšířeních (sekce 6.3 a podobné úlohy)
- důkaz Gaussovy věty (důkazy lemmatu 8.4 a vět 8.5 a 8.6), ale na znění se ptát mohu a měli byste to umět používat
- formulaci obecného algoritmu na čínskou větu o zbytcích (poznámka pod důkazem věty 9.1)
- šifru AES (příklad v sekci 10.1)
- vlastnosti lexikografických uspořádání a Gaussův algoritmus (tj. vše pod zněním věty 11.2 až do konce důkazu této věty), ale na znění věty 11.2 a na znění a důkaz důsledku 11.6 se ptát mohu a určitě se někdy objeví úloha na výpočet pomocí Gaussova algoritmu
- Loydovu patnáctku (sekce 14.3)
- reprezentace grup (sekce 15.5)
- El Gamalův a Schnorrův algoritmus (závěrečná část sekce 16.3)
- grupy autmorfismů (sekce 17.2)
- 2. a 3. větu o izomorfismu pro grupy ani okruhy
- derivovanou podgrupu a tvrzení o vlastnostech řešitelných grup (str. 96-97)
- důkazy lemmat 24.2 a 24.3 o izomorfismech mezi podtělesy kořenových a rozkladových rozšíření (ale znění ano, použije se dále)
- důkaz lemmatu 25.5 a tvrzení 25.6-části(2,3) (ale výpočet $\text{Gal}(x^n - 1/\mathbb{Q})$ ano)
- Cardanovy vzorce (sekce 26.1)
- důkaz Galoisovy věty (žádné důkazy ze sekce 26.2)

Průběh zkoušky:

Organizace:

- *písemný test*
 - 150 minut, 5-6 úloh, max. 78 bodů
 - první část, převážně na znění definic a vět a jednoduchou teorii, odevzdáváte po 75 minutách
- *ústní zkoušení*, zhruba 20 minut na přípravu, 15 minut zkoušení, max. 22 bodů
- v čase ústního zkoušení je možné konzultovat opravený test (úspěšný i neúspěšný)

- hodnocení (*předběžně*): hranice známek 55-67.5-80 bodů
- test 10:00-12:30, ústní zkoušení později odpoledne a druhý den dopoledne v intervalech cca 20 minut; časy upřesním vždy podle počtu účastníků a opravujících; termín 26.5. se koná v 12:15 a ústní zkoušení proběhne až v úterý

Typy otázek v testu:

- definice, příklad, protipříklad („která z následujících grup je řešitelná?“, „uveďte grupu, která je řešitelná stupně přesně 3“)
- znění vět, příklad, protipříklad („napiš polynom stupně tři s pěti kořeny“)
- důkazy typu „rozepiš definice a uvidíš“, včetně takových, které nebyly na přednášce
- kratší důkazy z přednášky
- početní úlohy na grupy (v každém testu!) a ostatní početní úlohy, které nebyly v zápočtovém testu (polynomy více proměnných, symetrické polynomy a Vietovy vztahy, stupeň rozšíření a minimální polynomy, Galoisovy grupy apod.)

Jen zřídka dávám otázky, na něž je možné odpovědět citací rozsáhlé pasáže ze skript. Připravte se na otázky, které vytrhují nějaký argument z kontextu (odpovědí je část jistého důkazu ze skript), které jsou speciálním případem obecné věty ze skript („dokažte, že v žádné stoprvkové grupě neexistuje prvek řádu 101; můžete použít Lagrangeovu větu a základní fakta ze sekce 13, všechna ostatní tvrzení, která chcete použít, musíte dokázat“), drobné parafráze, atd. To vše s cílem, abych otestoval, zda tomu opravdu rozumíte.

Typy otázek na ústním:

- delší důkazy z přednášky: vysvětlit hlavní myšlenky důkazu a být schopen na požádání doplnit jakýkoliv detail, včetně důkazu lemmatu („dokaž zobecněnou základní větu aritmetiky“)
- vysvětlit ucelené téma („vysvětli neřešitelnost úloh pravítkem a kružítkem, ilustruj na úloze třetění úhlu“)

Typicky lze odpovědět citací rozsáhlé pasáže ze skript. Připravte se na zvědavé otázky, abych zjistil, jestli tomu rozumíte (“kde jste použili tenhle předpoklad a co kdyby tam místo něj bylo něco jiného”).

Ukázka šest let starých testů:

- ZS: https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/1819/algebra_zkzs1.pdf
- LS: https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/1819/algebra_zkls1.pdf

Formát bude trochu jiný, tenkrát byl předmět dvousemestrální, zápočet byl organizován jinak atd., ale můžete vyzorovat styl otázek.

Máte-li jakékoliv otázky nebo nápady, jak něco dělat lépe, neváhejte se (včas) ozvat.