Požadavky ke zkoušce z Teorie čísel, 2020/21

David Stanovský

Předmět zkoušky:

Vše potřebné k úspěšnému vykonání zkoušky se nachází v učebním textu Víti Kaly a zápiscích ze cvičení. Měli byste si to kompletně přečíst a pochopit, měli byste znát postupy řešení úloh ze cvičení. Mohu se zeptat na libovolný důkaz, který je v textu označen jako cvičení.

Ke zkoušce se nemusíte učit následující části:

- důkazy ze sekcí 1.6 a 1.7 (ale definice a tvrzení byste znát měli, mimo jiné kvůli jejich použití v sekci 1.8)
- kryptosystém RSA (sekce 3.6)
- důkazy z poslední přednášky, které nejsou sepsány ve skriptech Víti Kaly.

Průběh zkoušky:

- zkouška bude písemná (dopoledne) a ústní (odpoledne)
- každý si může volně vybrat, zda se zapíše na prezenční nebo distanční termín
- test se píše na papír, společný pro obě varianty, 4 úlohy (z každé kapitoly jedna)
- prezenční: 90 minut; distanční: 2x 50 minut (včetně odeslání řešení), na každou etapu dostanete pouze 2 úlohy
- testové otázky se budou pídit po znění definic a vět (málo), příkladech ilustrujících definice a věty, početní úlohy ve stylu cvičení, jednoduché důkazy (ze skript či jejich parafráze)
- ústní zkouška bude spočívat ve vysvětlení jednoho delšího důkazu nebo jedné kratší sekce, cca 20 minut na přípravu a 15 minut rozhovor
- hodnocení: test 72 bodů, ústní 20 bodů, kvízy max. 8 bodů, hranice známek 55-67.5-80
- přesné pokyny pro on-line zkoušení viz str. 3

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

Vzorový test z předmětu Komutativní okruhy

(jenom abyste viděli strukturu testu a typy otázek)

1. (17 bodů)

a) Napište dvě různé definice noetherovského okruhu a dokažte, že jsou ekvivalentní.

b) Které z následujících okruhů jsou noetherovské? $\mathbb{Z}[x], \mathbb{Z}[\sqrt{103}]$. Pokud používáte nějakou větu, formulujte ji.

c) Dokažte: je-li R noetherovský a I jeho ideál, pak je R/I noetherovský.

2. (20 bodů)

a) Definujte stupeň separability a dokažte, že je shora omezen stupněm ve smyslu druhácké algebry. Pokud používáte nějaké tvrzení, formulujte jej.

b) Popište Galoisovu grupu $Gal(U/\mathbb{Q})$, kde U je rozkladové nadtěleso polynomu x^4-8x^2+15. Kolik má prvků, s jakou známou grupou je izomorfní? Kolik má těleso U podtěles?

3. (20 bodů)

a) Napište co nejvíce ekvivalentních podmínek definujících celistvý prvek.

b) Uvažujte okruhová rozšíření $R \subset S \subset T$. Je-li S konečně generovaný nad R jako okruh a je-li T konečně generovaný nad S jako modul, je T nad R konečně generovaný jako okruh? jako modul? Pokud ano, dokažte. Pokud ne, napište protipříklad.

c) Změnila by se odpověď, pokud by R, S, T byla tělesa? Z jaké věty to plyne?

4. (17 bodů)

a) Definujte normu ideálu v oboru O_K, $K = \mathbb{Q}(\sqrt{D})$. Spočtěte podle definice normu ideálu $(5, 2i)$ v $\mathbb{Z}[i]$.

b) Dokažte, že $N(IJ) = NI \cdot NJ$.

c) Jak se bezprostředně použije norma v důkazu věty o jednoznačných rozkladech ideálů na prvoideály? Tuto část věty formulujte a důkaz napište.

Pokyny pro distanční zkoušku

Co potřebujete:

- tužka, papír
- nějaké zařízení s kamerou a mikrofonem, aplikace zoom
- nějaké zařízení, které umí skenovat, například mobil s aplikací AdobeScan
- průkazka studenta

Přihlašovací údaje pošlu emailem.

Průběh testu:

- v daný čas se přihlásíte pod svým jménem, budu pouštět přes waiting room
- ukážete mi na kameru studentskou průkazku
- ukážete mi na kameru, že jste v místnosti sami a nikde neleží studijní materiály
- po dobu testu musíte mít zapnutou kameru a mikrofon (aby bylo slyšet, že se s nikým nedomlouváte)
- po dobu testu se nesmíte vzdálit z místa, odskočit si můžete mezi odevzdáním části testu a novým zadáním
- test má dvě části po 50 minutách (včetně odeslání řešení)
- zadání testu nasdílím přes zooom
- na email stanovsk@karlin.mff.cuni.cz mi pošlete naskenované řešení testu v daném časovém limitu **ve formátu PDF s názvem, který začíná vaším příjmením**
- po dobu testu nesmíte manipulovat s žádným elektronickým zařízením z jiného důvodu, než sken řešení – po jakékoliv manipulaci s mobilem/tiskárnou očekavám v krátkém okamžiku email s řešením
- po skončení poslední části testu zůstáváte přihlášeni, v breakout místnostech rychle projdeme (já nebo jiný zkoušející) kritické části testu s jednotlivými studenty
- v případě výpadku techniky či spojení na delší než krátkou chvíli:
  - v jiné než poslední části: zkouška se anuluje, termín vám nepropadá
  - v poslední nebo ústní části:
    - pokud předchozí části nasvědčují, že zkoušku nemáte šanci složit, jste hodnoceni nedostatečně
    - pokud předchozí části nasvědčují, že výsledek bude nevalný (3–4), zkouška se anuluje a termín vám nepropadá
    - pokud předchozí části nasvědčují, že výsledek bude pěkný (1–2), dohodneme se na náhradním dozkoušení
  - buďte připraveni na emailové instrukce ke znovunavázaní spojení (pokud bude chyba na mé straně)

Ústní část:

- čas si domluvíme na konci písemného testu
- v daný čas se přihlásíte a ukážete mi na kameru, že jste v místnosti sami a nikde neleží studijní materiály
- po dobu přípravy i zkoušení musíte mít zapnutou kameru a mikrofon a nesmíte se vzdálit z místa
- vysvětlím zadání, budete mít cca 20 minut na přípravu, poté mi pošlete naskenovanou přípravu a budeme si o ní povídat
- typicky budete přihlášení dva nebo tři, pokud vás bude zvuk rušit, tak si jej vypněte (ale ne mikrofon)

Podmínky jsou adaptací obecných instrukcí UK, viz https://karlovkaonline.cz/