

1. Nechápu, jak může mít nějaké těleso jinou charakteristiku než 0. Prosím o vysvětlení a ukázání na příkladu. Příkladem je těleso Z_2 . Platí v něm $1+1=0$ a tedy char $Z_2=2$. Nebo těleso Z_3 . Platí v něm $1+1+1=0$ a neplatí $1+1=0$, takže char $Z_3=3$.

2. Prosím o spočítání matice z příkladu 3.14. v tělese Z_{11} , nejsem si jist, že jsem pochopil jednotlivé úpravy. Myslíte spočítání SLR dané maticí z příkladu 3.14. Pokusíme se.

3.3.3 Existence inverzních prvků

(citace) "Zjistili jsme, že v Z_3 je 2 inverzní prvek k 2. A protože v Z_3 platí také $1 \cdot 1 = 1$ (což platí v každém Z_n), našli jsme inverzní prvek ke každému nenulovému prvku $a \in Z_3$. To znamená, že počítání v Z_3 splňuje i axiom (N3) a Z_3 je těleso."

Proč platí, že když najdeme inverzní prvek ke 2 a zároveň víme, že $1 \cdot 1 = 1$, existuje inverzní prvek ke každému nenulovému prvku v Z_3 ?

Protože Z_3 má jen dva nenulové prvky, 1 a 2.

Aké těleso si mám představit pod pojmem kvaterniony?

Kvaterniony zobecňují komplexní čísla přidáním dalších dvou komplexních jednotek, viz 3.5.5

Ako presne funguje charakteristika telies, teda ako je možné, že po sčítaní n počtu jednotiek dostaneme 0 ?

Viz výše příklad se Z_2 . Pokud je těleso konečné a má k prvků, pak jednotlivé součty jednotek 1, $1+1$, $1+1+1$, atd. nemohou nabývat všechny navzájem různých hodnot. Pokud dva nabývají stejné hodnoty, pak jejich rozdíl, který je také součtem jednotek, je roven nule.

Ako sa zistí, či je prvok teleso ?

Těleso je množina s danou algebraickou strukturou, ne prvek.

Aký je rozdiel medzi označením vektorov "b s vlnkou T" a "b"?

" b_i s vlnkou T" označuje i-tý řádek matice B, viz oddíl 4.2, b_i by označovalo i-tý sloupec matice A.

Aký je rozdiel medzi klasickým $+$ a $\cdot$ oproti $+$ a $\cdot$ v kroužku ?

Označení $+$ a $\cdot$ v kroužku používáme ze začátku pro odlišení sčítání a násobení modulo n a běžného sčítání a násobení. Rozdíl je např. při počítání modulo 10, kde $5 + 7 = 12$, kdežto 5 $+$ v kroužku $7 = 2$.

Budeme počítat matice i metodou, kdy se po gaussově eliminaci ještě "zbavíme" přebytečných nenulových prvků (tedy ponecháme nenulové pouze pivoty)?

Ano, viz definice 5.90.

Byl bych rad kdybyste vysvetlil pouzivani modulu v telesech

Na přednášce i cvičení se budeme tělesům Z_p věnovat.

Co je tedy např. Z_4 , když to není těleso (kvůli neexistenci inverzního prvku k 2)? Je to "nic" nebo pro to existuje odborné označení?

Je to tzv. komutativní okruh.

Co je to lemma?

Pomocná věta, typicky taková, jejíž znění je třeba pro důkaz nějaké podstatné věty.

Rozdíl mezi lemma/věta/tvrzení/pozorování je jenom v důrazu, které na dané tvrzení klademe.

Co je to přesně těleso?

Těleso je algebraická struktura, která abstrahuje a zobecňuje vlastnosti racionálních, reálných a komplexních čísel. Přesně viz def. 3.2.

Co představuje symbol alfa v sekci 3.5.1? Píše se tam polynom. Mám si to tedy přestavit jako libovolný polynom s reálnými koeficienty, který pro účely počítání v čtyřprvkovém tělese považujeme za "číslo"?

Víceméně ano. Polynomy se dají mezi sebou sčítat a násobit, výsledkem je vždy polynom. Je tedy možné na ně nahlížet jako na svého druhu zobecněná čísla. Na hodnotě proměnné alfa algebraické operace mezi polynomy nezávisí, dají se popsat jako operace na koeficientech polynomu. Tyto koeficienty se berou z jiného tělesa, v nejjednodušším případě $\mathbb{R}$, v našem případě Z_2 .

Co to je inverzní prvek a jak zjistím, zda k danému číslu existuje, nebo ne, případně jakou má hodnotu?
Inverzní prvek k a je takový prvek b , že $a \cdot b = 1$. V reálných číslech je to převrácená hodnota, v konečných tělesech ho lze najít například zkouškou, postupně zkoušíme všechna b a díváme se, zda $a \cdot b = 1$. V tělesech $\mathbb{Z}_p$ lze použít Euklidův algoritmus, ale to je nad rámec kurzu.

Také prosím o vysvětlení důkazu tvrzení 4.29.

Pokusíme se na přednášce. Jde o aplikaci definice násobení matic a porovnávání jednotlivých elementů matice na levé a na pravé straně.

Co to znamená „netrivialita“ v kapitole u definice tělesa?

Že má těleso alespoň dva prvky. Podle tvrzení 3.3 (10) z toho pak plyne, že 0 se nerovná 1 .

Dá sa zostaviť matica aj z prvkov, ktoré nie sú z telesa?

Dá, běžně se třeba uvažují matice, jejichž prvky jsou polynomy, a ty těleso netvoří. Takovým maticím se ale v kurzu nebudeme věnovat.

Definícia 3.15 hovorí koľkokrát najmenej treba sčítat' jednotkový prvok, aby sme dostali 0 . Nerozumiem, ako sčítaním jednotiek dostaneme nulu?

Viz výše.

Dobrý deň,

ja by som sa chcela spýtať, či pri dôkaze Lemma 3.6. namiesto $s = c \bmod n$ by nemalo byť $s = b \bmod n$?

Ano, je to překlep.

V 3.5.1. (4-prvkové těleso) je značení GF, čo to znamená ?

Galois Field, neboli Galoisovo těleso.

V 4.2.6. (blokové násobení matic) je súčin $C = AB$, nemalo by byť v príslušnom obrázku C_{r1} , $C_{r2}, \dots$, C_{rt} ?

Ano, také překlep.

Za odpoveď ďakujem. :)

My děkujeme za upozornění.

Dobrý den,

co přesně znamená pojem modulo? V textu nemohu nikde najít přesnou definici.

Zbytek po celočíselném dělení. V textu je to v oddílu 3.3.1

Děkuji

Dobrý den, budeme ke zkoušce potřebovat umět formálně dokázat všechny vlastnosti těles z každého tvrzení, nebo stačí znát, kterými vlastnostmi se tělesa vyznačují?

Nevím jestli rozumím. Vlastnosti tělesa jsou součástí definice 3.2. Tam není co dokazovat, umět to přesně zformulovat ale musíte. Vlastnosti v tvrzení 3.3. je potřeba umět dokázat, pokud soubor s požadavky ke zkoušce neřekne jinak (u konkrétně tohoto tvrzení se ještě domluvíme). Dokazovat se také dá, zda daná množina s danými operacemi (třeba $\mathbb{Z}_2$ se sčítáním a násobením modulo n) tyto vlastnosti má. I to byste měli umět. Ne pro množinu $\mathbb{R}$, protože její konstrukcí se tu nezabýváme, ale pro $\mathbb{C}$, $\mathbb{Z}_p$ za pomoci vlastností $\mathbb{R}$ ano (opět pokud nebude řečeno jinak).

Dobry den, chcem sa opytat ci je potrebný ten prvý dokaz z telies o jednoznacnosti nuloveho prvku.. Mne pride ze to plynie z toho ze $a+x=b$ má jednoznačne riešenie a viac ze z toho tvrdenia NEvyplýva ze pre každé ' a ' existuje len jedine $b=0$ take ze $a+b=a$, čo mi pride užitočnejšie.. Analogicky to iste pre jednotkový

Asi máte pravdu. V důkazu jednoznačnosti řešení $a+x=b$ se s nulovým prvkem operuje, takže bychom pak museli říkat, že je to jen nějaký nulový prvek. Trochu by se to tím zamotalo.

Dobrý den, chtěla bych se zeptat, jak přesně se řeší lineární rovnice s maticí v tělese $\mathbb{Z}_n$. Nedokáží to ze skript pochopit. Děkuji

Řeší se úplně stejně jako s reálnými/komplexními čísly, akorát se jinak počítá. Zkusíte si na cvičení a uvidíte, že to není těžší než v reálných číslech.

Dobrý deň, mňa by zaujímalo ako sa definuje nekomutatívny prvek ?

Byla to sice v kvízu jedna z mnohých odpovědí, ale nic takového neexistuje ani to nedává smysl - komutativita je logicky vlastnost dvojice prvků a operace mezi nimi.

Dobrý deň, pri sčítaní matíc sčítavame navzájom si zodpovedajúce prvky. Má v lineárnej algebre zmysel taký typ súčinu matíc (rovnakého rozmeru), kde by sme násobili navzájom si zodpovedajúce prvky ako pri sčítaní ?

I takový součin se někdy používá, my o něm mluvit nebudeme.

Dobrý deň, tak ako je teleso komplexných čísel rozšírením telesa reálnych čísel a teleso kvaterniónov rozšírením telesa komplexných čísel, existuje aj "typické" rozšírenie telesa kvaterniónov a ak áno, aké to je?

Ano, říká se tomu oktoniony, ale už to není ani asociativní.

Dobrý večer,

zo skript mi nebolo veľmi jasné ako vypočítam v Z_n nejaké číslo, ktoré je umocnené na -1 , Mohli by ste mi to vysvetliť? Ďakujem.

Mocnina na -1 je označení inverzního prvku. V Z_n počítejte zkusmo (viz výše).

Existuje geometrická interpretace matice?

Například: Lze na matici A typu 3×2 nahlížet jako na třísloužkový vektor, jehož každé složce přisuzujeme nějaké dvě vlastnosti?

To by byla spíš interpretace matice jako datové struktury. Geometrická interpretace je jakožto zobrazení.

Existuje možnost, jak jednodušeji (rychleji) počítat zobrazení?

Děkuji za odpověď.

Co znamená počítat zobrazení?

Celá kapitola 6 je o lineárních zobrazeních. Jakmile vybudujeme aparát maticového počtu a vektorových prostorů, bude počítání s některými zobrazeními mnohem systematičtější.

Existuje nějaká rada popřípadě nějaký "algoritmus" jak nejlépe postupovat při elementárních řádkových operacích u Gauss-Jordanovy eliminační metody, abych se co nejjednodušší cestou dostal k správnému konci?

Typicky stačí jen dávat na pivota co nejjednodušší číslo, nejlépe 1.

Existuje teda teleso Z_4 , keďže 4 je 2^2 a 2 je prvočíslo?

Z_4 těleso není, ale čtyřprvkové těleso existuje.

Existuje těleso, ve kterém se nulový prvek $\neq 0$, ale jinému číslu?

V tělese žádný prvek označený 0 vůbec nemusí být, množina T je libovolná. I když tam je, tak nemusí být nulovým prvkem: např. na R můžete zavést pro libovolné nenulové číslo r operace $a +' b := a + b + 1/r$, $a .' b := a + b + a . b . r$. Bude to těleso s nulovým prvkem $-1/r$.

Chcel by som sa opýtať, čo presne znamená charakteristika telesa, keďže som ju zo skript nie príliš pochopil, je to najmenší možný súčet jednotkových prvkov, ktorý dáva nulu? Vede by ste mi to vysvetliť na konkrétnom príklade prosím Vas? Ďakujem

Viz výše.

Chci se zeptat, proč vlastně poté, co matici dostaneme do odstupňovaného tvaru, provádíme raději zpětné dosazení, než další úpravu matice. Vlastně pokud budu postupovat obdobně, tak mi zbydou koeficienty v pivottech a výsledné neznámé jenom přečtu. Je to velmi jednoduché a v případě počítání s nějakým středním počtem (třeba 4 až 1000) pravděpodobně i rychlejší než zpětné dosazování. Ptám se proto, protože mi to na střední škole taky zakazovali, ale bez důvodu. Tak jestli to má nějaký hlubší důvod, proč raději zpětné dosazovat.

My vám nic nezakazujeme :-)) Ale

- (1) Výsledné neznámé si přečtete jen v případě, že v soustavě nejsou volné proměnné
- (2) Není to rychlejší (když si spočítáte počet operací). Možná to bude někdy výhodnější při počítání na papíře, ale rozdíl nebude podstatný

Doplnění: Teď mi Dalibor vysvětlil, že řešení si snadno přečtete i když volné proměnné jsou. Takže (1) беру zpět. Za (2) si zatím stojím, ale můžu se mýlit :)

Další doplnění: znovu jsem si spočítal počet operací a teď mi to (alespoň pro soustavy bez volných proměnných) vychází úplně stejně. Takže si nestojím ani za (2)

Chtěl bych se zeptat, zda-li 10 vlastností tělesa i s důkazem (skoro 2 stránky ve skriptech) může být 1 otázka u zkoušky? Pokud ano, přihlíží se u zkoušky i k rozsahu věty, kterou máme dokázat? Děkuji

Vlastnosti tělesa jsou axiomy, není na nich nic k dokazování. Definice tělesa může být otázka u zkoušky.

Jakýkoliv důkaz (kromě výjimek, které si přečtete v požadavcích) může být u zkoušky. Spíše ale budou otázky testovat vaše porozumění a schopnost definice a věty aktivně používat. Struktura zkoušky už je zveřejněna na webu.

Chtěla bych se zeptat, za jakých situací lze použít Frobeniovu větu.

Frobeniova věta je ve skutečnosti drobné pozorování vyjadřující podmínku řešitelnosti rovnic pomocí maticového aparátu.

Jak poznám, které důkazy jsou podstatné a mohou být předmětem zkoušky a které ne?

Viz též výše. Na webu je struktura zkoušky, v ní je jako jedna z částí "důkaz těžšího tvrzení". Tato tvrzení budou na webu vyjmenována. U ostatních vět a lemmat se hlavně čekává, že jste pochopili jeho myšlenku a stala se součástí vašeho porozumění lineární algebry jako celku. Učení nazpaměť nemá smysl, budeme se také ptát na důkazy tvrzení, které přímo nejsou ve skriptech.

Jak poznáme, jestli je těleso konečné nebo nekonečné?

Těleso je množina s danými operacemi, konečnost nebo nekonečnost množiny bývá zřejmá z její definice.

Jak se hledají inverzní prvky v Z_n ?

Zkusmo (viz výše).

Jak si mám představit těleso kvaternionů? Bylo by možno problematiku kvaternionů více rozvést?

Jako zobecnění komplexních čísel. Nebudeme na kvaterniony mít čas, ale možná stojí za zmínku, že měly nedávno narozeniny:

http://www.slate.com/articles/health_and_science/science/2016/10/we_should_celebrate_hamilton_day_a_mathematical_holiday_on_oct_16.html

Jak vznikla jednotková matice? Začala se používat kvůli binárním kódům?

Nebo kvůli čemu?

Jednotková matice se chová jako jednotkový prvek vůči násobení matic, popisuje zobrazení identity, je tudíž základním a přirozeným pojmem maticového počtu.

Jaká je formální definice netriviality? Jsem trochu zmatený z těch uvozovek a zápisu $|T| > 1$...

Viz výše.

Jaká jsou konkrétnější praktická využití počítání s modulem?

Nejpoužívanější metody šifrování jsou realizovány pomocí operací s modulem, viz např.

<https://cs.wikipedia.org/wiki/RSA>

Dále například návrh kódů pro přenos signálů s šumem, počítání s velkými celými čísly a polynomy.

Jako příklad těles s nenulovou charakteristikou jsme si uvedli tělesa typu Z_p , kde jsou zavedeny operace modulo p . Existují nějaké jiné typy konečných těles, kde se nepoužívá modulární aritmetika?

Všechna konečná tělesa jsou tvaru $GF(p^k)$ až na přeznační prvky, tedy se dají realizovat pomocí polynomů nad Z_p

Jaký je přesně rozdíl mezi číselným tělesem a tělesem obecně? Chápu správně, že číselná tělesa jsou podmnožinou těles?

Ano, číselným tělesem se většinou rozumí podtěleso komplexních čísel s nějakými dalšími vlastnostmi.

Jaký je rozdíl mezi kvaterniony a komplexními čísly?

Viz výše.

Jaký je univerzální postup pro výpočet inverzních prvků v tělese Z_n ?

Viz výše.

Jaký smysl má modulo n, lze tím něco vypočítat, kromě tedy těles Z_p? Viz výše.
Jakým způsobem jste získali tabulku inverzních prvků v tělese Z_{11}? (strana 67) Viz výše.
Je součástí pozdější látky zobecnění kvaternionů na libovolný počet rozměrů a mají kromě popisů rotace další využití? Kvaterniony již nelze zobecnit, ne tak, aby to bylo těleso. Existuje matematická škola, která tvrdí, že pomocí kvaternionů by měla být zformulována celá fyzika https://en.wikipedia.org/wiki/Geometric_algebra V reálu je jejich použití geometrie ve třech a čtyřech rozměrech.
Je vďakaa součinu matice A s vektorem b možné počítat s libovolným množstvím rovnic v soustavě rovnic? Ano.
Je-li libovolný sloupec v matici nulový lze ho vyškrtnout? Podle toho, na co matici používáte. Pokud na řešení SLR, pak je odpověď ne. Změnil by se počet neznámých. Nulový sloupec znamená, že příslušná neznámá může nabývat libovolné hodnoty.
Jen pro ověření - pokud jsem skriptu pochopila správně, u pojmu "tělesa" se zabýváme s něčím abstraktním? (nejsou to tělesa typu krychle, kvádr, apod.) Ano.
Jsou i jiná konečná tělesa než Z_n pro prvočísla? Viz výše.
K čemu je dobré počítat např. rovnice v daném tělese? (jako ve skriptech v Z_{11}) Z početního hlediska je to obvykle i jednodušší než v R, protože se nemohou vyskytnout zlomky. Z koncepčního je užitečné si uvědomit, které vlastnosti čísel jsou pro co důležité. Některé aplikace viz výše. Chápu dobře, že charakteristika tělesa $Z_{10} = 10$? Z_{10} není těleso. Z_{11} ano, $\text{char } Z_{11} = 11$.
K čemu je charakteristika tělesa? Je to užitečný pojem. Některé věty o maticích mají v předpokladech, že platí pouze pokud charakteristika příslušného tělesa není 2.
K čemu se vlastně obvykle takové matice využívají v praxi? Mnoho numerických výpočtů jsou výpočty s maticemi. Od předpovídání počasí přes výpočet, jestli most nespadne až po Google PageRank.
K čemu slouží jednotková matice? Viz výše.
K čemu všemu se využívá sčítání a násobení modulu n? Co mi to všechno říká? K čemu jsou vůbec dobrá tahle tělesa? Viz výše. Není I_n matice přímo jednotková tzv. má všude nulu až na 1 na diagonále? Ano.
K důkazu tvrzení 3.3 (10): Pokud bychom měly prvky $a, b, c, \dots$, které všechny budou rovny jednomu jedinému číslu, pak v mohutnosti množiny budou brány jako jeden? Tedy např. pro množinu $M = \{7, 7, 7, 7, 7\}$ platí $M = 1$? Ano, $M = \{7, 7, 7, 7, 7\} = \{7\}$ (je to ta samá množina!), $M = 1$. Liší se v něčem smysl zápisu kongruence pomocí symbolu $\equiv$ (který jsme používali na SS) od $=$, jež je používáno ve skriptech? Je to jen konvence, tři čárky se používají jako vztah mezi celými čísly, $=$ je prostě rovnost (např. v tělese Z_p). Tedy např. v celých číslech platí $6 + 5 \equiv 4 \pmod{7}$, v tělese Z_7 platí $6 + 5 = 4$
Kde lze toto počítání s maticemi využít v praxi? Viz výše.
Kedy sa pri maticiach využívajú determinanty?

Determinant bude obsahem posledních dvou přednášek.

Kvaterniony a jejich rotace a otáčení kolem osy, je jen pro zajímavost?

Ano. Na webu je seznam požadavků ke zkoušce, v němž je uvedeno, které pasáže skript jsou informativní.

Lemma 3.6: není zde chyba označení ('c')?

Ano, viz výše.

Len si niesom celkom istý, či v prípade, keď je napísané Matice I_n Ide o Zapis velké i (I_n) alebo o zápis malé I (I_n) inými slovami je prvé písmeno pri zápise malé alebo veľké?

Bylo tím myšleno velké I.

Lze inverzní prvek a^{-1} zapsat i jako zlomek $1/a$, nebo je striktně dáno, že se musí zapisovat tímto způsobem?

Zapisuje se tímto způsobem, pro inverzní prvek používat $1/a$ není příliš zvykem. Ale výraz $1/a$ dává pro nenulové a smysl (protože jsme obecně definovali $a/b = a \cdot b^{-1}$) a je roven inverznímu prvku.

Ma pri grafickem nacrte kvaternion čtyři dimenze?

Víceméně ano, ale samotný kvaternion žádnou dimenzi nemá.

Kvaternion je možné chápat jako vektor v R^4 se speciálně zavedeným násobením.

Mají nějaké využití derivace v maticích? Či by je možné je zde nějak užít, pro zjednodušení exponenciálních rovnic v nich?

Pokud matice závisí na proměnné, pak ji lze podle této proměnné derivovat, resp. zobecňovat všechny pojmy z matematické analýzy na matice. Je to ale nad rámec našeho kurzu.

Mají symboly $+$ a $*$ nějaký jiný význam pokud jsou v kroužku?

Ve skriptech mají význam sčítání a násobení modulo n , je to ale jenom pomocné značení pro účely výkladu.

Mají-li kvaterniony své využití v zápisu třídimensionálních rotací, mají rovněž oktoniony a sedeniony svá využití v zápisu čtyřdimensionálních a pětidimensionálních, respektive?

Nevím o tom. Rotace ve 4D se popisují pomocí kvaternionů a oktoniony či sedeniony praktické aplikace zatím nemají.

mám dotaz ohledně řešení rovnic v maticovém zápisu. Když jsme na střední počítali například soustavu dvou rovnic o dvou neznámých a chtěli se jedné neznámé v jedné rovnici zbavit, Tak jsem klasicky první vynásobili něčím a přičetli k druhé, jako to děláme teď, jen s tím rozdílem, že jsme museli mít to vynásobení první rovnice napsané :

$$x+3y=4$$

$$2x+2y=5$$

$$-2x-6y=-8$$

$$2x+2y=5$$

$$-4y=-3$$

Trochu mě mate proč ten první řádek necháváme v tom základním tvaru a nenapišeme ho v tom vynásobeném?

Vynásobení řádku a přičtení násobku řádku do jiného řádku jsou dvě různé úpravy. Můžete dělat jednu z nich nebo obě, podle toho, co se vám zdá z hlediska výpočtu perspektivní.

Bývá výhodnější přičítat násobek řádku k jinému, například máte-li soustavu

$$x+..... =...$$

$$2x+... = ...$$

$$3x + ... = ...$$

Mám otázku čo sa týka značenia, či mám správnu predstavu. Platí, že vektor a_i s vlnovkou je vlastne klasický stĺpcový vektor matice A^T ? V tom prípade, keď ho transponujeme dostávame riadkový vektor matice A ? Vyjadrenie prvku matice v mieste (i,k) v súčine AB (tvrdenie 4.21) je teda v podstate súčin matice $1 \times n$ a $n \times 1$, ktorého výsledok je matica 1×1 a teda jej jediný prvok je umiestnený na pozícii (i,k) ? Táto hodnota je vlastne potom štandardný skalárny súčin daného riadkového a stĺpcového vektora?

Ano, s tím, že pojem "standardní skalární součin" se používá jen pro reálné aritmetické vektory.

Matice I_n je vyjadřuje diagonální relace nějaké množiny?

Nevím, co je diagonální relace. Jednotková matice popisuje zobrazení identity.

Moc nerozumím zápisu, co je tady v kvízech používán, např. dnes konkrétně Z_n nebo I_n . Co jsem ještě rozluštil, tak byly mocniny a^n . Mohli bychom si to na přednášce nebo na cvičení projít? Díky.

Podtržítko $_$ značí dolní index, $^$ značí horní index. Nic složitějšího nepoužíváme.

Mohl byste prosím na přednášce věnovat pozornost oddílům 3.5.2 a 3.5.3? Chtěla bych slyšet váš komentář k charakteristice tělesa apod - moc tomu nerozumím. Např., že těleso s n prvky existuje právě když n je mocnina prvočísla, to platí pro všechna tělesa? Děkuji.

Ano, platí.

Možná jsem to ve skriptech přehlédla, ale co by byla množina Z_p , kde p není prvočíslo, když ne těleso?

Viz výše.

Můžou se tělesa Z_n navzájem sčítat, násobit, nebo provádět jakékoli operace? Co by bylo případným výsledkem?

Mezi tělesy o tom nevím. Pokud se Z_n považuje pouze za grupu vůči sčítání, pak by příkladem takové "operace" mohla být tzv. Čínská věta o zbytcích.

https://cs.wikipedia.org/wiki/%C4%8C%C3%ADnsk%C3%A1_v%C4%9Bta_o_zbytc%C3%ADch

Nedovedu si příliš představit lineární rovnici v tělese Z_{11} , už vůbec ne soustavy těchto rovnic. Existuje pro ně nějaké přibližování (jako když jsme si u soustav lineárních rovnic nad R řekli, že řešení je průnik nadrovin)?

Je to pořád průnik nadrovin, jen jsou to nadroviny v prostoru $(Z_{11})^n$. Vizualní představa také možná je, ale bylo by to složitější.

Nechápu moc zisťování inverzního prvku. Jak se určuje?

Viz výše.

Nechápu přímo pojem "těleso", co si pod tím mám kromě definicí představit?

Viz výše.

Nejsem si jistá, co myslíte maticí „ I_n “

$n \times n$ jednotkovou matici, Definice 4.7

Nejsem si úplně jistý, jestli jsem pochopil vysvětlení, že neexistuje nulový prvek pro sčítání modulo n .

Je to kvůli tomu, že rovnost $a = a \bmod n$ platí jenom tehdy, když $a \in Z_n$ a tato množina Z_n není shodná se Z ? (tudíž platí tato rovnost pouze pro některé $a \in Z$ a ne pro všechna?)

Ano.

Nejsem si zcela jistý, zda chápu binární operaci. Resp. moc tomu nerozumím, bude to se vysvětlovat na hodině?

Zatím chápu, že pokud máme nějakou množinu, třeba A , tak udělám kartézský součin $A \times A$, ale jak potom každé dvojici čísel (a,b) přiřadím číslo z původní množiny A ? Nebo musíme nejdřív definovat nějaké pravidlo, kterým budeme tato čísla přiřazovat jednotlivým dvojicím (a,b) ? Jako například modulo n ?

Přesně tak, binární operace je jakékoli "pravidlo" (lépe zobrazení), které dvojici (a,b) prvků z A přiřadí prvek z A . Třeba obyčejné sčítání je binární operace na R (ale i na N , na Z nebo na Q).

Nemělo by na stránce 63 u lemma 3.6 v důkazu být místo $s = c \bmod n$ toto $s = b \bmod n$? Pokud je to jen překlep tak chápu. Pokud je to tak ale správně, tak bych poprosil o vysvětlení, kde se c vzalo.

Mělo, je to překlep.

Nemělo by ve skriptech na straně 63, v důkazu, 2. řádek místo $(s = c \bmod n)$ být $s = b \bmod n$

Ano.

Kde se můžeme setkat s Kvaterniony?

Viz výše.

Není mi úplně jasné, jak získáme inverzní prvek v tělese Z_n .

Viz výše.

Není ve skriptech u důkazu asociativity modulárního sčítání překlep v " $s = c \bmod n$ " - místo " c " " b "?

Ano.

Nepochopila jsem co znamená takové to plus/násobení v kroužku (popřípadě jak se to čte), jestli jsem to dobře pochopila tak to nenahrazuje klasické sčítání a násobení.

Je to násobení a sčítání modulo n , viz výše.

Nerozumím v příklade 3.8 jednému kroku: Ako sa z čísla -223 dostane číslo 5? - Rozumiem, že z 321 je 3 (pretože $321 \bmod 6 = 3$), ale $-223:6 = -37, 166..$ a keď spätne vynásobím $-37 \cdot 6 = -222$ - $-223 - (-222) = -1$, v záporných číslach to funguje inak? Do zvyšku nula mi chýba 1, čiže vzdialenosť zvyšku 5 do nuly je 1 alebo ako to funguje?

$-223 : 6$ je -38, zvyšok 1, pretože $-223 = (-38) \cdot 6 + 1$

na zvyšok po dělení 6 se můžete dívat tak, že k danému číslu tak dlouho odečítáte (když je kladné) nebo přičítáte 6 (když je záporné), až Vám vyjde číslo mezi 0,1,...,5. A to výsledné číslo je zbytek.

Nie som si úplne istý ale pre telesá Z_n pre n väčšie nanajvýš rovné 2 sme v tvrzení 3.9 povedali, že spĺňajú všetky axiomy okrem $N3$. Pričom na predchádzajúcej strane sme zase povedali, že pre operáciu modulo nulový prvok neexistuje. Nevylúčili sme teda platnosť axiómu $S2$?

Ne, pretože výrok "nulový prvok neexistuje" se týkal operace sčítání modulo n zavedené na celém Z . V tvrzení 3.9 už se omezujeme jen na Z_n .

Omlouvám se za hloupý dotaz, ale nepochopil jsem, jak se z lemmatu 3.6 na stránce 63 odvodily jeho 2 použití, které ve skriptech následují po jeho důkazu?

Každé číslo nahrazujeme jeho zbytkem po dělení n a z lemmatu víme, že se výsledek násobení ani sčítání nezmění.

Pokud je nějaká množina s našimi dvěma binárními operacemi těleso, jsou potom i její podmnožiny tělesy?

Některé. Třeba R je podtěleso C , ale iR (imaginární osa) není, nebo $\{2,3,4\}$ také ne.

Pořádně nerozumím otázce číslo 2. Byla by možnost vysvětlení?

Tvrzení 3.10 a Věta 3.11.

Potřeboval bych vysvětlit transponovanou matici. Nevím, jak si mám zápis vyložit, když se zapíše v tomto tvaru.

Je to matice, jejíž i -tý řádek je roven i -tému sloupci matice původní (pro všechna i).

Používajú sa v telesach kde sa neda použiť aritmetický priemer ine priemery? Alebo nestaci aritmetický priemer rozložit na niekoľko priemerov a tie spriemerovať vazeným aritmetickým priemerom?

O některých jiných průměrech budeme mluvit v druhém semestru (v kapitole afinní prostory). Pokud je $\text{char } T = 2$, pak aritmetický průměr žádným trikem rozumně nenadefinujeme.

Prečo nulová matica je v odstupňovanom tvaru keď podľa definície 2.12 pre odstupňovaný tvar majú byť riadky $1, \dots, r$ nenulové?

V definici se připouští i $r=0$. Výrok "řádky $1, \dots, r$ jsou nenulové" se běžně v matematice chápe tak, že "pro každé celé číslo i takové, že $1 \leq i \leq r$ je i -tý řádek nenulový". Tento výrok je triviálně splněný pro $r=0$, protože žádné takové i neexistuje.

Prečo sa to nazýva teleso? je to matice oproti telesu čo je 3D objekt...

Je to z němčiny, původní termín byl Zahlkörper, tedy "číselná těla", používána v podobném smyslu jako například v kriminalistice "body of evidence", propojená sada důkazů, tedy zde (algebraickými operacemi) propojená množina čísel. Český překlad "tělesa" není úplně šťastný, ale kdyby se to vzalo z angličtiny, kde se používá termín "field", nebylo by to lepší.

ale jinak, píšete že hlavní diagonála sú prvky a_{ii} . čo ak máme maticu a pridáme tam nulový vektor na začiatok? potom matica sa nezmení, keď len pridáme 0, no zmení sa diagonála.

Pokud přidáme k matici řádek, pak dostaneme matici jiného typu (takže se rozhodně změní), je pak logické, že má i jiné diagonály.

Prečo v príklade 3.12/13 pracujeme so zápornými prvkami, keď v telese sú podľa tvrdenia 3.9 prvky od 0 po $n-1$?

Nepracujeme se zápornými prvky, ale s prvky opačnými k danému prvku. Tj. -3 neznamená "prvek -3" ale "opačný prvek k prvku 3". Například v Z_7 je $-3=4$.

Pro tělesa $\mathbb{Z}_p$ je jednodušší počítat tak že výpočty děláme nad $\mathbb{R}$ a pak výsledek zmodulujeme podle p .

Moje otázka je že mezi kterými tělesy lze takhle přecházet, jestli je to nějak formálně definované?

Stačí když máme dvě tělesa se stejnými binárními operacemi, nebo je třeba mít nějakou další podmínku?

Zde to máme podloženo lemmatem 3.6, v jiných případech bychom si museli dokázat něco podobného. To se bez specifikace, co jsou to "stejně" binární operace nedá říct.

Děkuji

Proč násobení matic není komutativní a proč po vynásobení matice vektorem vyjde vektor?

Zkuste si vzít dvě náhodné 2×2 matice a vynásobit si je z jedné a druhé strany. Druhé otázce nerozumím, vyjde to, protože je to tak definované. Vysvětlení, proč je to tak definované, zabírá ve skriptech značnou část kapitoly.

Proč používáme "mod" a ne "%"? Zatím všude jinde jsem viděl psát modulo pouze pomocí "%".

Mod je běžnější v matematice, % v programování.

Proč se prvky jednotkové matice zapisují jako Kroneckerova delta? Co Kroneckerova delta znamená?

Je to užitečné a běžně používané označení.

Proč se zabýváme kvaterniony? Jak je můžeme využít?

Viz výše.

Proč se začíná výkladem těles dříve než výkladem grup. Nebylo by pak jednodušší tělesa pochopit? Všiml jsem si, že v učebnici od doktora Bečváře jsou všechny podobné objekty popsány hned na začátku.

Grupy a další pojmy umožňují skutečně definici tělesa strukturovat a tím pro někoho i lépe pochopit (ale pochobuji o tom). V našem kurzu se jimi ale dále nebudeme zabývat, proto jsme je nezaváděli. Pořádně se s nimi seznámíte ve druhém ročníku, ale určitě nezaškodí, když si o nich něco přečtete i samostatně.

Spíše než dotaz mám menší žádost. Nejsem si jist zda úplně rozumím násobení matic, takže bych rád, kdyby se tomuto tématu na přednášce věnovala pozornost.

Určitě bude.

Takto definovaná tělesa asi nijak nesouvisí s tělesy, které jsme znali do teď, jako například krychle, válec, koule atd., proč se tedy nazývají zrovna tělesa?

Nesouvisí.

Tvrzení 4.23 a následný příklad 4.24, proč se tento jednodušší způsob neučí jako hlavní postup pro řešení násobení matic (Tady ho vidím poprvé a připadá mi stejně srozumitelný jako ten základní). Je to způsobeno tím, že má určité výjimky nebo je to jen proto, že vyžaduje znalost LinKomb, která nemusí být hned zřejmá při prvním násobení matic.

Vždycky je dobré vidět stejnou věc z více pohledů. Dohromady máme tři základní pohledy, každý z nich je v některé situaci užitečný (i početně). Nejužitečnější pro účely výkladu je ten první způsob (sloupcový), kvůli důležité interpretaci matice jako zobrazení.

U čtyřprvkového tělesa (str. 69) se při sčítání sčítají $\alpha + (\alpha+1)$, ale u násobení se násobí $(\alpha+1)(\alpha+1)$. Zajímalo by mne, proč se u násobení nenásobí α a $(\alpha+1)$ jako při sčítání.

To je jenom příklad, součin je prostě ilustrován na jiné dvojici prvků než součet.

U čtyřprvkového tělesa ukázaného ve skriptech: $\{0, 1, a, a+1\}$ si pod 'a' mám tedy představit jakýkoliv polynom, například že $\{0, 1, x^2, x^2 + 1\}$ bude těleso?

Ne, a je proměnná, nikoli polynom. Polynomem v proměnné a jsou $a+1, a, 1$ i 0 , stejně tak jejich součty a součiny. Počítání modulo polynom a^2+a+1 zaručí, že výsledek bude zase v množině $\{0,1,a,a+1\}$ a že dostaneme těleso.

U definice tělesa si nejsem jistý, zda jsem porozuměl poslednímu bodu, a sice: " $(\neg T)$ („netrivialita") $|T| > 1$ ". Znamená to, že množina T má více prvků než 1?

Ano.

Už vím, jak najít čtyřprvkové těleso, ale zajímalo by mě zda existuje i 6,8,10,...-prvkové těleso a popřípadě jak ho najít?

Těleso s n prvky existuje právě když n je mocnina prvočísla. Tedy 8-prvkové těleso existuje (není to $\mathbb{Z}_8$), 6 a 10-prvková tělesa neexistují. Jak 8-prvkové těleso zkonstruovat je nad rámec kurzu, stručně je to popsáno v 3.5.2

V kapitole 3.5.1 (Čtyřprvkové těleso) nerozumím, proč nahrazujeme α^2 součtem $\alpha + 1$. Proč to v tom hraje roli modulo zrovna polynomu $\alpha^2 + \alpha + 1$?

Protože $a^2 = (a+1) + (a^2+a+1)$, počítáme-li s koeficienty v $\mathbb{Z}_2$.

V kapitole 3.5.4 (Podtělesa komplexních čísel) píšete, že: "... neexistuje vzoreček (využívající operace $+$, $\cdot$, $-$, $:$, n) pro kořeny polynomu většího

než čtvrtého stupně..." Znamená to, že nějaký vzoreček se "speciálními" operacemi přece jenom existuje?

Rovnice 5. stupně lze řešit pomocí hypergeometrických funkcí, dál nevím.

<http://mathworld.wolfram.com/QuinticEquation.html>

V podkapitole 3.3 (konkrtně strana 64) je nejprve napsáno, že nulový prvek pro sčítání modulo n neexistuje a hned o pár řádků níže je uvedeno, že jsme dokázali, že pro sčítání a násobení modulo n na množině $\mathbb{Z}_n$ nulový a jednotkový prvek existují. Chápu to tedy správně tak, že ta první věta se vztahovala na všechny množiny čísel a pak se dokázalo, že pro množinu $\mathbb{Z}_n$ prvek existuje?

Víceméně ano. První věta se vztahovala na množinu všech celých čísel, pro $\mathbb{Z}_n$ je nulovým prvkem 0.

V příklade 3.12. sa píše: "Tedy v $\mathbb{Z}_p$ je $(p-1)^{-1} = (p-1)$ ". Z čoho to vyplýva? Ako sa k tomu dospelo?

$(p-1)(p-1) = p^2 - 2p + 1 = p(p-2) + 1$, takže zbytek po dělení čísla $(p-1)(p-1)$ číslem p je 1.

Jiný způsob je ve cvičení 3.12. V každém tělese platí $(-1)^{-1} = -1$ (čtete: inverzní prvek k opačnému prvku k je opačný prvek k). Protože v $\mathbb{Z}_p$ je $-1 = p-1$ (čtete: opačný prvek k je $p-k$), platí $(p-1)^{-1} = p-1$

V příklade 3.14 sme počítali s telesom $\mathbb{Z}_{11}$ a predtým sme si urobili tabuľku inverzných prvkov, ktorá nám uľahčila počítanie. Keď budeme počítat s telesom $\mathbb{Z}_s$ nejakým veľkým prvočísлом tak urobiť takú tabuľku bude trvať večnosť, existuje nejaký trik?

Pro velká p se inverzní prvky počítají pomocí Euklidova algoritmu. Jiný trik: z Malé Fermatovy věty

https://en.wikipedia.org/wiki/Fermat%27s_little_theorem plyne, že $a^{p-1} = a^{p-2} \bmod p$.

A myslím, že som našla chybu na str. 63, v lemma 3.6, v dôkaze, je tam označené $s = c \bmod n$, nemalo by to byť $s = b \bmod n$?

Ano.

V prípade hľadání řešení soustavy rovnic tužkou a papírem, stačí použít Gaussovu eliminační metodu, nebo preferují matematici spíše zápis v Jordanově tvaru? Nebo je to pro řešení specifických problémů zcela osobní volba? (pro budoucí referenci při zkouškách a podobně)

Na metodě nezáleží, spíš jde o správný obsah a formu výsledku.

V zhrnutí je napísané, že každé konečné těleso má nenulovou charakteristiku. Prečo je to tak, z čoho vieme, že pri konečnom telese vždy vieme vyskladať daný súčet?

Viz výše.

Keďže elementárna matica je tá, ktorú dostávame z matice I_m , platí, že elementárne matice sú teda vždy štvorcové matice? A obsahujú vždy maximálne jeden prvok iný ako 0 alebo 1?

Ano.

Ve ktorých prípadoch matic platí, že součin $AB = BA$? Myslím si, že to platí pro $A = B = I_n$, ale jsou ještě nějaké další případy?

Mnoho dalších, třeba $B = A^k$.

Ve skriptech je, že množina celých čísel netvoří těleso, protože nespĺňuje požadavek na existenci inverzního prvku. Ale dále je množina $\mathbb{Z}(p)$ označená za těleso, přestože nespĺňuje stejnou podmínku a ještě, myslím, výsledek sčítání a násobení jejích členů neleží vždy v té množině.

To je ale vůči jiným operacím, sčítání a násobení modulo p .

A mohl byste na přednášce trochu víc vysvětlit pojem axiom (znamená něco podobného jako pravidlo)?

Znamená to výchozí předpoklad, který se nedokazuje.

Ve skriptech nechápu kdy značkou $\mathbb{Z}_x$ označujete množinu a kdy těleso na této množině.

Ano, formálně by se to mělo rozlišovat, ale obvykle se to nedělá.

Dále, domníval jsem se, že zbytek a modulo jsou ekvivalentní pouze pro kladná čísla, tj. ve Vašem příkladu $-32 \bmod 7$ je 3, ale $-32 / 7$ dává 4, zbytek -4. Je toto také jedna z věcí, na které se matematici neshodnou?

V našem pojetí je zbytek vždy nezáporné číslo.

Zajímá mě podrobněji součin matic.

Zkuste být příště konkrétnější.

Zajímalo by mě, jak se dá odvodit nebo přijít na to, že pro lib. čtvercovou matici A je symetrická matice $2AA^T + A^TA$. Důkaz je mi jasný, jen bych rád věděl, kde se to vzalo.

Protože $A^T B^T = (BA)^T$, víme, že A^TA i AA^T jsou symetrické matice. Tedy i jejich součet.

Další otázky

A ještě jeden dotaz, který mě zajímá už od první hodiny. Má to značení číselných oborů na MFF nějaký hlubší význam nebo to je jen aby se odlišili proměnné a číselné obory.

Je to standardní matematické značení.

Bude někde k dispozici správné řešení domácích úkolů?

Zatím s tím nepočítáme.

Bylo by možné přidat obsah do skript? Občas je velice náročné najít něco konkrétního.

Obsah je, špatně jsem přeložil poslední verzi. V pdf je dobré zapnout záložky, také funguje textové vyhledávání.

Co mám dělat, když si s nějakým domácím úkolem vůbec nebudu vědět rady? Můžu se zeptat narovinu na některém ze cvičení, jak se obecně řeší daný úkol?

Zkuste se poradit se spolužáky, případně si domluvit konzultaci se cvičícím nebo přednášejícím.

Co se týká kvadrionů, patří do rámce poznatků, které máme nadobudnut už v prvním semestru nebo je to rozšiřující učivo?

Ne, je to prostě jen pěkná věc, o které je dobré vědět.

Hledám příklady z lineární algebry i s celým postupem řešení, můžete mi prosím doporučit nějaké zdroje?

Na webu kurzu jsou odkazy.

Bude na webu zveřejněno vzorové řešení domácího úkolu?

Spíše ne.

Na přednáškách z matematické analýzy nám byla nabídnuta možnost konzultací s tutorem, existuje tutor i pro lineární algebru?

Tutor pro lineární algebru není, ale můžete se během cvičení s čímkoli obracet na cvičící, případně si domluvit konzultaci.

Chtěla bych se zeptat, jaké bude rozdělení bodů u zkoušky kolik procent cca připadne na jednotlivé typy látek (definice, věty, důkazy, ano/ne, jednoduché početní úlohy, úlohy k zamyšlení)

Už je to na webu.

Jak lze procvičit a zafixovat látku, kterou čteme ve skriptech. Obávám se, že brzy po přečtení skript se nové poznatky ztratí v kvantech dalších a dalších informací.

Těžká otázka.

Přemýšlet o tom, přemýšlet o příkladech na cvičení, přemýšlet o tom, co zatím víme, přemýšlet o tom, co říkáme na přednášce.

Jaký je rozdíl mezi Lemou a Tvzením?

viz výše - žádný podstatný. Lemma je pomocné tvrzení.

Je ještě jiná možnost odevzdání DÚ, než do schránky v Karlíně?

Na přednášce (před termínem). Ve velmi (!) výjimečném případě emailem (např. jste nemocní a v Tanzanii).

Kde najdem v skriptách oddiely, ktoré si máme prečítať na budúci kvíz, 4.5.1 a 4.5.2? Nemajú to byť oddiely 4.6.1 a 4.6.2?

Asi máte starou verzi skript. Kapitola 4 se dost menila.

Kde se da najít tabulka s aktualnim počtem bodu?

Bude na stránce

Kdo konkrétně opravuje naše domácí úkoly?

To vám neřekneme :)

Lemma 3.6. (str. 64) - v důkazu má být podle mě $s = b \bmod n$, a ne $s = c \bmod n$

Máte pravdu, díky za upozornění

Má zmysel chodiť na prednášky, keď sa to aj tak všetko naučíme predtým zo skript ?

Pokud máte pocit, že všemu dostatečně rozumíte ze skript, tak ne. To se ale týká jen velmi malého počtu studentů (jednotky). Na přednášce se máte šanci ptát, vysvětlujeme vám většinu ještě jednou a nejspíše aspoň trochu jinak, ptáme se (a tak si můžete ověřit, zda opravdu tak dobře rozumíte), zdůrazníme nejdůležitější věci, řekneme nějaké zajímavosti, apod. Proto má snad přednáška pro drtivou většinu studentů smysl. Nemá smysl chodit opisovat tabuli.

Minule mi nefungoval kvíz, byť bylo 19.00. Co mám dělat?

Pošlete Daliborovi Šmídovi email s detailnějším popisem problému.

Můžou se objevit na zkoušce příklady které se týkají i částečně fyziky (jako ve skriptech)?

Ne, fyzikální znalosti se nepředpokládají

Na cvičeních bych preferoval společnou práci celé třídy, např. vždy po jednotlivcích u tabule se společným řešením příkladů. Když máme příklady řešit individuálně a nikdo ze třídy nemá ani páru o čem daný příklad je nebo jak se má řešit a cvičící se tváří, že to je všechno úplně jasné a předpokládá, že to všichni zvládnou, pak takové cvičení ztrácí smysl...

Díky za názor.

Společné řešení příkladů má obrovskou nevýhodu v tom, že řada lidí bude pouze kopírovat tabuli.

Když nemáte páru, o čem to je, tak nerozumíte látce z přednášky. Zpracujte na tom, dořeňte to. Cvičící je od toho, aby vám s tím pomohl.

Na stránce 65 v odstavci nad tvrzením 3.10 je překlep "součinn".

máte asi starší verzi skript

Našla som preklep v lemme 3.6 - prvý odstavec dôkazu spomína premennú c so zvyškom s mod n, zvyšok pracuje s b.

máte pravdu, díky

Pokud jsem si všimla správně, na přednáškách se v zápisu někdy používá $:=$ (např. $x := (x_1, x_2, x_3)^T$) a jindy jen $=$. Nikdy dříve jsem se s tím nesetkala. Jaký je v tom rozdíl a jak důležité je používat správnou variantu?

$A := B$ je trochu programátorská hantýrka, znamená to, že A je definované jako B (tj ve Vašem případě, že vektor x je definován jako vektor $(x_1, x_2, x_3)^T$). V matematice se většinou nepoužívá a opíše se slovně: vektor x je definovaný vztahem ...

Pokud přednáška odpadne (například 25.10. kvůli imatrikulaci), bude se nějak nahrazovat?

nebude

Proc je prohozeni radku elementarni uprava, kdyz se ji da docilit pomoi zbylych dvou uprav?

proč ne?

Ve skriptech pred tvrzenim 2.20 se scita pocet nasobeni/deleni pri zpetne substituci. Proc se do tohoto poctu nepocita nasobeni ktore probehne uvnitr zavorek (napr. $c[1,n]*x[n]$) ?

počítá, kdyby se nepočítalo, bylo by jich n

Při cvičeních by mi více vyhovovalo častější předvádění a hromadné počítání spojené s vysvětlováním daného problému.

Pokud si nevím rady, mám možnost se cvičícího individuálně zeptat, jenže obvykle si s problémem nevím rady více lidí, tudíž by se vysvětlování dalo zefektivnit.

Viz též výše. K vysvětlování nejasností je přednáška, ptejte se! Cvičení je od toho, abyste si to sami zkusili.

rad bych na cviceni probрал ulohu 2.6 z cviceni minuleho tejdne

Poproste cvičícího

Stihl jsem to?

Uvidíte ve výsledcích

Škoda že zobrazenia niesu nikde v skriptach, prednášku sme mali iba jednu a na cvičení sa toho nestihlo veľa. Tá úloha je vzhľadom na tieto skutočnosti celkom náročná.

Máte pravdu, až bude nějaký čas, zkusíme něco napsat.

Tyto dotazy jsou také bodované?

ne

U Gaussově eliminaci se mi zdálo nejasně vysvětlené, že $k_1 < k_2 < k_3$, myslím, že by tam mělo být dopsáno, že se jedná o indexy a ne o hodnotu čísla

Nerozumím, co je nejasného na $k_1 < k_2 < k_3$. Znamená to prostě, že k_1 je menší než k_2 a to je menší než k_3 .

Význam k_i jako indexů je vysvětlen přímo v definici 2.12. Co je "hodnota čísla" nevím.

V zhrnutí tretej kapitoly v bode (5), malo byť asi, že zbytek bereme vždy z množiny Z_n a nie Z_p .

Je tam víc takových překlepů, díky.

Ve skriptech občas místo čárky píšete tečku (ve větách nebo i mezi čísly), tak by mě zajímalo jestli to je pouze překlep nebo to u čísel má nějaký jiný význam?

Nevím, co myslíte. Dejte konkrétní příklad.

Zatím pořád moc pěkné a pěkně vysvětlené přednášky. :)

Díky!