TEORIE

Uvodni kapitoly

def. az k homomorfismu (1.2, 1.3) +dk

1. Algebra, Podalgebry a Homomorfismy.

Definicie, pak se zameril na (1.3)

2. Vlastnosti homomorfismu (slouceni, inverz, a obraz a vzor podalgeber) tedy poznamky 1.2 a 1.3 s dukazem

def. od homomorfismu do konce 1 (1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11) +dk

3. vztahy mezi kongruencemi a homomorfizmy na algebrach (neboli priroz projekce kongurence je homo, jadro homorfizmu je kongurence **(1.6 , 1.7)**)

4. Kongruence, faktoralgebry, prirozena projekce, jadro zobrazeni. Pridokazat - faktoralgebra je algebra (neboli dokazat korektnost definice operace alfa na A/ro), a pak prirozena projekce je homomorfismus**(1.7)**. kongruence, faktoralgebry (definice); jádro homomorfismu a přirozená projekce (jakě je mezi nimi vztah **1.6** dokazat).

5. Kongruence na faktorovych algebrach, 2. veta o isomorfismu
Napisal som definiciu relacie sigma/ro na A/ro, znenie pozn **1.5**, pozn **1.8** a dokazal som 2. vetu o izomorfizme **(1.11)**

6. Vztah jadra a obrazu zobrazeni (veta o homomorfismu, 1. + chtel 2. veta o isomorfismu)(1.9, 1.10 a 1.11)

U vety o homomorfismu se staci odvolat na vetu **1.4.**

def. z 2 (2.1, 2.3, 2.4, 3.2, 3.3, 4.3) +dk

7. Monoid, jak vypadaji vsechny invertibilni prvky (2.3 2.4), konstrukce grupy. Jednoznačnost neutrálního prvku. (neutralni prvky e,f z G(*), e=e*f=f) (2.1)

8. Uzaverove systemy, uzaver, operator, 2 vety s dukazy ktere mluvi o jejich zakladnim vztahu. Vztah uplnych svazu a uzaverovych systemu (3.2, 3.3, 4.3)

Svazy

def. z 4 do bool (4.1, 4.2, 4.4, 4.5, 4.11) +dk

9. Svaz ako usporiadanie mnoziny a algebra(poznamky 4.1, 4.2 - dukaz)

Usporiadanie sa da nahradit spojenim a prusekom a naopak. Teda Poznamku 4.1 a potom aj lahsiu cast Poznamky 4.2. Nemusel som dokazat tu cast Poznamky 4.2, ze m v n sa rovna presne infimu a spojenie supremu.

Opacny svaz(S(A,V) svaz, pak taky S(V,A) je svaz, 4.4 s dukazem). dukaz z 4.1 a 4.2

10.Modularita a distributivita svazu(definice a poznamka tesne predtim s "polomodularitou" (4.5) s dukazem) a priklady modularnich (tri vrcholy nad sebou spojene hranami) **a distr. Svazu** (<|> není distr. ale je modularni)

11. Distributivni svazy a Booleovy algebry. Charakteristika konecnych B. Algeber. (def BA a 4.11)

def. monotonie (4.12, 4.13, 4.14, 4.15) +dk

12. Svazy, monotonni zobr(4.13), isomorfismus svazu. Dukaz vetu o isomorfismu svazu.

Definici uspořádání, infima, suprema, monotonie, homomorfismu a izomorfie.

věty (4.12 a 4.13) – vety dokazat

-Věta o bijekci na svazech, že je izomorfismus právě když je monotónní z obou stran (4.13).

13. Vztah medzi jej normalnymi podgrupami a svazom vsetkych kongruencii? Měl jsem to definovat a dokázat izomorfizmus (4.14, 4.15)

Ide o to sialene tvrdenie 4.14 z ktoreho vyplyva potom 4.15 (ze tie normalne podgrupy a kongruencie su izomorfne)

def. GK (4.16) +dk

14. Gailosova korespondence-definice a veta (4.16).

U vety mi na zacatku rekl, ze je to jedna z tech co si clovek nemusi drzet v hlave tak kdyz nebudu vedet - klidne mi ji rekne. Hlavni je dukaz. V nem jsem dal jen ty trivialni

Grupy

def. 5 do řád (5.2, 5.3) +dk

15. Lagrangeova veta (5.3)-dukaz, poznamka 5.2 -dukaz. Grupa definice. resp. souvislost velikosti podgrupy a grupy,

coz je uplna pohodka, a pak mi dal samozrejme dokazat veci z poznamky 5.2.

def. od řád do cykl. (5.7, 5.8, 5.9, 5.10) +dk

16. Cyklicke grupy a jejich popis. K teorii jsem napsal definici, dokazal veticku, ze cyklicka grupa je isomorfni se Z resp. Zn pro kardinalitu grupy nekonecnou resp. konecnou**(5.7)**. Co jsem tam zapomnel napsat bylo v te konecne variante ze zobrazeni psi dane predpisem k |-> k mod n je homomorfismus, abych mohl pouzit vetu o isomorfismu. On me upozornil, pak jsme to nejak dali dohromady a dobry. A jeste jsem dokazal asi poznamku $g^{|G|}=1$ pro grupu G a $g \in G$.**(5.9)**

17. Cyklicke grupy, jejich charakterizace. Vlastnosti podgrup a faktoru. Chcel co je to cyklicka grupa, ze kazda (ne)konecna je izomorfna Z(n) (a ako) **(5.7)**, potom vety, ze podgrupa aj faktorgrupa je tiez cyklicka...

18. Vztah cyklickych grup, jejich podgrup a faktorgrup = Dokazte (**5.8)**

19. existence a jednoznacnost podgrup v cyklickych grupach (dokazat vetu "G je cyklicka grupa. Pro kazde prirozene k delici rad existuje prave jedna podgrupa radu k." - **5.10 + dk.**)

- existence se dokaze tak, ze zkonstruhujete obecne podgrupu a ukazete, ze ma k prvku
- jednoznacnost se dokaze nejak trivialne, ale presne jak to nevim

def. euler. (5.12, 5.13, 5.16, 5.17) +dk

20. Eulerova funkce + jeji vztah ke grupam a monoidum. K teorii jsem musel napsat zneni vety f(nm)=f(n)*f(m), pro nesoudelna a pak to s tim p^r. K obojimu chtel dukaz. (5.12, 5.16, 5.17.)

K tomu vztahu ke grupam a monoidum chtel vety o tom, ze f(n) je pocet prvku, ktery generujou grupu Z_n(+,-,0) a taky pocet invertibilnich v Z_n(*,1).

21. Eulerova funkce, mala fermatova veta. Definice, dukaz (5.13)

def. součinu algeber (5.15) +dk

22. Součin algeber (def. před ČV) a Cinska veta o zbytcich (5.15) (vztah algeber $Z_{n1..nk}(+,.,-)$ a $\Pi Z_{n1..nk}(+,.,-)$)

Okruhy

def. komut.okruh az max.ideál (6.2, 6.4, 6.5) +dk

23. Okruhy, ideály, vztah kongruencí a ideálů na okruhu (dokazat vety 6.2 a pro důkaz znát 4.14,4.15)

24. Chtěl definice okruhu a ideálu, větu o vztahu kongruencí a ideálů (6.2), ty dvě tvrzení o vztahu mezi okruhy a tělesy (6.4), (6.5).

Popis tělesa pomocí ideálů (6.4)**:** R je těleso <=> má pouze nevlastní pravé ideály <=> má pouze nevlastní levé ideály. Hlavní ideály chtěl i dokázat že to jsou ideály a pak se zeptal na důkaz (6.1(2)): -(a.b)=a.(-b) dukaz: 0=0.b=(a+(-a)).b=a.b+(-a).b

25. Komutativní okruh a maximální ideál (napsat definice + formulovat a dokázat větu 6.5 -> mohl jsem se v důkazu odvolávat na nějaké předchozí věty)

def. obor integrity, pod.teleso (6.9) +dk

26. Podilove teleso oboru integrity (okolo 6.9)

Q(Z)=Q, Q(R[x]) jsou racionální funkce, Q(Z[i])=Q[i], Q(Z[V5])=Q[V5]

Chtel ho sestrojit a dokazat, ze splnuje zakladni podminky. Neco mu stacilo popsat slovne, neco si vyzadal pisemne (treba dokazat, ze pouzita relace ~ je kongruence, ze vznikle F/~ ma korektne definovane operace, a na zaver, ze je + asociativni).

PRAKTICKE

1.Homomorfizmy, grupy...

Tady asi nemame otazku :)

Invertibilní prvky v takove grupe jsou vsechna cisla, co jsou nesoudelna s radem grupy (NSD(cislo, rad grupy) = 1)

1. Jak vypada mnozina vsech invertibilnich prvku mnoziny vsech linearnich zobrazeni V->V.

Je to grupa permutaci (grupa ma inverzní prvek ke kazdému svému prvku)

9. G(*,$^{-1}$,1) je grupa, mame-li f: G -> G, f(h)= ghg^{-1} (to g^{-1} je inverzni prvek k g), g z G. (a) Je to homomorfismus? (b) Jaky je ker f, pokud nasobeni je komutativni?

(a) f(a^{-1}) ?= f(a)$^{-1}$: f(a)= gag^{-1} (nasobenim inv.prvky) **=>** f(a)$^{-1}$=ga^{-1}g^{-1}=f(a^{-1})

f(a*b) ?= f(a)*f(b) : f(a*b)= ga*bg^{-1}=gag^{-1} gbg^{-1} =f(a)*f(b) **=>** ANO je-to homomorfismus

(b) f(h)= ghg^{-1} = gg^{-1}h=h **=>** ker f=id

36. G(*,$^{-1}$,1) je grupa, Z(G) = { a z G | ah=ha pro vsechny h z G }. (a) Je Z(G) normalni podgrupa? (b) Jak bude vypadat Z(G), kdyz bude nasobeni v G komutativni?

(a) stacilo overit **uzavrenost**:

takze: mejme a, b ze Z; tedka sa ptame, jestli a.b nalezi Z = tedy jestli je to uzavrene na nasobeni

1. vime ze ah=ha

2. vime ze bh=hb

chceme dokazat, ze abh=hab kde h nalezi G

takze: abh=ahb=hab

na prvnim „=“ pouziju druhy predpoklad a na druhem „=“ pouziju prvni predpoklad

a podminku **normality**, pomoci ah=ha jde snadno:

ahh^{-1}=hah^{-1}

a=hah^{-1} pro kazde a z Z(G) a h z G

(b) bude to cela G (komutativni => ah=ha je to same)

vsechno se dokazalo snadnym poprehazovanim pismenek, neni tam zadny chytak

2.Uzaverove vlastnosti

37. najst inverzny prvok k 26 v monoide Z_{157}(.,1)

pomocou Eu.alg.:

1=26*a+157*b

157=6*26+1
26=26*1+0

=> 1=157-6*26

26^{-1}= -6 mod 157= 151

96. Dokazat, ze existuje a najit inverzni prvek k cislu 35 v Z_{121}.
Reseni je uplne trivialni - pouzije se eukleiduv algoritmus a zpetnym chodem se najdou takove x a y, ze

1=35.x + 121.y

121=3*35+16
35=2*16+3

16=5*3+1

=> 1=121-3*35-5*(35-2*(121-3*35))=11*121-38*35

35^{-1}= -38 mod 121= 83

Dukazem, ze takovy prvek existuje je to, ze ho najdete. Pokud byste ho nenasli, pak to nutne neznamena, ze neexistuje!

98. Najděte inverzní prvek k prvku 71 v tělese Z_{103}

Najprv si rozlozis cisla nasledovne, az kym nebude zvysok po deleni jedna (ten algoritmus tam snad uvidis):

103 = 71*1 + 32
71 = 32*2 + 7
32 = 7*4 + 4
7 = 4*1 + 3
4 = 3*1 + 1

Teraz si spatne musis vyjadrovat zvysky ako linearne kombinacie pomocou substitucii predchadzujich vyjadreni:

32 = 103 - 71*1
7 = 71 - 32*2 = 71 - (103 - 71*1)*2 = 3*71 - 2*103
4 = 32 - 7*4 = (103 - 71*1) - (3*71 - 2*103)*4 = 9*103 - 13*71
3 = 7 - 4*1 = (3*71 - 2*103) - (9*103 - 13*71)*1 = 16*71 - 11*103
1 = 4 - 3*1 = (9*103 - 13*71) - (16*71 - 11*103)*1 = 20*103 - 29*71

Z toho vyplyva, inverzom v Z_{103} je -29, teda 74...

24. Je dan monoid slov M({x,y})(*,e) a vztah (x*y,e). To definuje minimalni kongruenci eta. Jak vypada M/eta?

Vezmes nejmensi ekvivalenci obs. vztah (xy,e). To je zrejme ekvivalencni trida [e] = { xy, e } a same singletony [x] ={x}, [y]={y},[xx]={xx}... . A ted musis udelat uzaver vzhledem k operaci *(=zretezeni 2 slov). Takze vyjde spousta ekvivalencnich trid, nejak takhle:
[e] = { e, $(xy)^i$ }
[x] = { x, $(xy)^i$ x, x$(xy)^i$ }
[y] = { y, $(xy)^i$ y, y$(xy)^i$ }
[xx] = { xx, xx$(xy)^i$, x$(xy)^i$ x, $(xy)^i$ xx }
- na kazdou pozici v rade xxxx... muzes dat $(xy)^i$ a bude to ve stejny tride
- pro radek yyy... uplne stejne
[yx] = { yx, yx$(xy)^i$, y$(xy)^i$ x, $(xy)^i$ yx }
stejne mas pro yyyyyy.... xxxxx..., ale uz ne xxxxx... yyyy...., to je ekvivalentni e.

-no a takhle vypadaj vsechny tridy v M/eta

(nekdy se vyskytuje varianta zadani s min.kongruenci {(x*y,e)(y*x,e)} ta vyjde analogicky ještě hezci :))

3.Isomorfizmus

30. Dokazat nebo vyvratit izomorfismus monoidu Z(+,0) a Z(*,1)

Jsem nejak vyvratil pres invertibilni prvky (izom=bijekt. homomorf.):

Z(+,0): inverzni k prvku a je -a (každý prvek je invertibilní)

Z(*,1): jediný invertibilní jsou 1 a -1

34. Existuje isomorfismus mezi N_0(+,0) a N(*,1)? Pokud ano najdete ho...

-ne

-Neexistuje - v N_0(+,0) totiz neexistuje (nekonecne velka) analogie prvocisel, tedy je zde jen konecne mnoho cisel nezapsatelnych jako soucet dvou (nenulovych) prvku (konkretne jen jednicka)... Nakonec se to uhraje pres vlastnosti homomorfismu jakozto slucitelneho zobrazeni (f(a+b)=f(a)*f(b)) a bijekce jakozto zobrazeni prosteho a na

-Izomorfne nie su, ale nic rozumne ako to dokazat ma nenapadlo, tak Zemlicka mi poradil nech to skusim cez prvocisla, tie nemaju v monoide N_0 analogiu protoze v N(*,1) prvocisla proste mas ... ale v N_0(+,0) nic jim podobneho ... nic co by se nedalo rozlozit na soucet vice prvku jinak nez jako (0+p)

-N_0(+,0) ma dva generatory <{1,0}>, N(*,1) není konečně generovaná algebra (napr. pro prvocisla) => nejsou

izomorfni

(korb. 11/1.Př.)

47. rozhodnut. ci je Z_4(+,-,0) izomorfne Z_8*(. , $^{-1}$, 1).

-není

-pretoze Z_4 je cyklicka zatialco Z_8* (mnozina všech invertib.prvku ze Z_8) nie je (pre kazdy prvok a ∈ Z_8* : <a> = {1, a} ... to si clovek moze vsimnut napr pri samotnom hladani prvkov Z_8*) φ(8)=1*2^(3-1)=4 ; Z_8*={1,3,5,7}

97. Je grupa S_3(o, -1, Id) izomorfni s grupou Z_2xZ_3(+,-,(0,0)) ?
-není

-Pri zadavani mi mezi reci rekl, ze mam dokazat, ze ta *cyklicka* Z_2xZ_3 je izomorfni s tou druhou. Coz me trochu nakoplo. Nejdriv me napadaly myslenky, ze takovy homomorfismus v nejhorsim najdu rucne, ale nastesti me osvitilo a zkousil jsem zjistit, jestli ta druha grupa je taky cyklicka.

- Z_2xZ_3 jde vygenerovat pomoci (1,1), (a (1,2)).
- U tech permutaci v S_3 jdou 4 vyloucit hnedka na prvni pohled, ze nebudou generatory (a to ty, ktere zobrazi aspon jeden prvek sam na sebe = Id, (12), (13), (23)).
- Zbyle 2 jsou navzajem inverzni ((123), (132)), staci to zkusit pro jeden a tam [kdyz si to clovek napise a udela poradne - muj problem], zjisti, ze pomoci neho vygeneruje jenom 3 prvky (skladanim permutaci).
- Takze S3 cyklicka neni, takze to nemuze byt izomorfni. Kdyz se na to prisel podivat, tak rekl, ze mam pravdu, ze jsem na to sel mozna zbytecne slozite, ale ze je to spravne a ze mam za 1 [po 1.5 hod boji] :]

-Udajne to bylo jednodussi utlouct s tim, ze Z2xZ3 je komutativni [je to cyklicke] a S3 komutativni neni.

33. Grupa (o,$^{-1}$,Id) izomorfismů tvaru G -> G , kde G je standartní grupa (x,$^{-1}$,1), a ty izomorfismy ve tvaru f(h)=ghg^{-1}, kde g je z G, že ta celá grupa izomorfismů je normální podgrupou všech izomorfismů z G do G (Aut(G)(o,$^{-1}$,Id)).

Měl jsem jen dokázat, že je to podgrupa (uzavřenost na operace) a že je normální.

Uplne nechapu otazku :)

2. Dokázat uzavřenost na operace a normalitu grupy In(G) v Aut(G), bylo to více rozepsáno...

nekompletni otazka, pravdepodobne jde ale o **33.**

4.Svazy

10. Mam N a usporadani "deli" tedy N(/), je to svaz?*(a)* mam Z a to same usporadani, je to svaz?*(b)* Je tento svaz modularni?*(c)* [btw: opravdu v zadani bylo jednotne cislo... buhvi jestli nahodou nebo jako nenapadna napoveda]

(a) takze, N(/) ano, dukaz: inf{a,b} = gcd(a,b), sup{a,b} = lcm(a,b) *(lcm=nejmensi spol. nasobek)*

(b) Z(/) ne, protoze / neni na Z usporadani, dukaz:
a/b <=> existuje c: ac=b
usporadani - reflexivni, tranzitivni, **a/b & b/a => a=b (slabě antisymetricka)**
-1/1, -1*-1=1
1/-1, 1*-1=-1
ale 1 != -1, takze **Z(/) nemuze byt svaz pac to neni usporadana mnozina (relace neni slabě antisymetricka)**

(c) modularni ano, dukaz:
pokud a<=c [tohle jsem tam zapomnel dat, vymyslel protipriklad a on mi taktne naznacil ze to tam neni a nedelal s tim problemy]
tzn dokazat a ∨ (b ∧ c) = (a ∨ b) ∧ *c* (∧ – prusek,prunik,infimum)
ja to umlatil pres prvociselnej rozklad (**∧ je totiz gcd, ∨ lcm viz vyse**)
tzn:
$a=p_1^{k1} * p_2^{k2} * ... * p_n^{kn}$
$b=p_1^{l1} * p_2^{l2} * ... * p_n^{ln}$
$c=p_1^{m1} * p_2^{m2} * ... * p_n^{mn}$

(nektery exponenty prvocisel mohly bejt 0, jako ze v rozkladu to prvocislo neni).

uvedomime si, ze **lcm(a,b) = p1^max{k1,l1}*..*pn^max{kn,ln}**
gcd obdobne s minimem
takze ve vysledku:
pokud a<=c $a \vee (b \wedge c) = (a \vee b) \wedge c$ pak:
lcm(a,gcd(b,c)) ?= gcd(lcm(a,b),c)

kdyz preskocim par kroku pak pro kazde prvocislo plati:
p_i^max{k_i,min{l_i,m_i}} ?=p_i^min{max{k_i,l_i},m_i} **(*)**
a vim ze $k_i \leq m_i$ (protoze a deli c)
mno a zbyva nekam zaradit b (testujeme v **(*)**):
$k_i \leq m_i \leq l_i$: p_i^m_i =p_i^m_i ano
$k_i \leq l_i \leq m_i$: p_i^l_i =p_i^l_i ano
$l_i \leq k_i \leq m_i$: p_i^k_i =p_i^k_i ano
takze vskutku rovnost plati...

[uvedomme si, ze jsme netrivialni ulohu modularity svazu N(/) prevedli na trivialni modularitu na N(<=) ktera je trivialni... kdyz mi tohle zemlicka rekl, modlil jsem se aby nezeptal, co jsem si dale uvedomil, pac samostatne jsem si uvedomoval jenom ze jsem v Katedre Algebry]

další reseni:

V praxi se muselo dokazat, ze relace je usporadani a potom ze pro kazdy dva a,b prvky je infimum = NSD(a,b) a sup = nsn(a,b). Pro N to svaz byl,

pro Z stacilo najit ze -1|1, 1|-1 a pritom 1 se nerovna -1 (relace neni antisymetricka).

Modularita: k overeni bylo treba se nejak vyporadat s tim, ze tam vychazelo pro a<=c musi nsn(a,NSD(b,c)) = NSD(nsn(a,b),c). Trik byl v tom si cisla zapsat jako prvociselnej rozklad
a = p_1^a_1 * ... * p_n^a_n
b = p_1^b_1 * ... * p_n^b_n
c = p_1^c_1 * ... * p_n^c_n
(nektery exponenty prvocisel mohly bejt 0, jako ze v rozkladu to prvocislo neni).

4. Napsat vsechny atomy a koatomy svazu podgrup grupy Z_{30}.

-rozlozit 30 na prvocisla (2*3*5), nahazet vsechny podgrupy do Hasseova diagramu tj. “krychle“ (pozn.$15Z_{30}$ ={0,15})

koatomy: $2Z_{30}$; $3Z_{30}$; $5Z_{30}$

atomy: $6Z_{30}$; $10Z_{30}$; $15Z_{30}$

(zeml.2004-5 3/15 nebo zeml.2007-8 4.12)

22. atomy a koatomy svazu vsetkych kongruencii na Z_{100} (Z_{500}).

To je izomorfni podle nejaky vety svazu norm. podgrup a pak je to taky snadne **(4.15)**

100=2^2*5^2, nahazet vsechny podgrupy do Hasseova diagramu tj. “2x2 diagram“

koatomy: $2Z_{100}$; $5Z_{100}$

atomy: $20Z_{100}$; $50Z_{100}$

Z_{500}:

500=2^2*5^3, nahazet vsechny podgrupy do Hasseova diagramu tj. “2x3 diagram“

koatomy: $2Z_{500}$; $5Z_{500}$

atomy: $100Z_{500}$; $250Z_{500}$

13. svaz vsech podgrup Z(+,-,0) a najit vsechny koatomy a atomy.

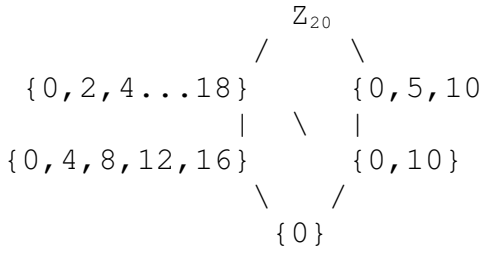
Atomy nema a koatomy jsou pZ - p prvocisla Ten svaz by mel vypadat tak, ze nahore je to cele Z, a pod nim jsou vsechny podgrupy pZ, kde p je prvocislo => vsechny pZ jsou koatomy. Atomy tento svaz NEMA, protoze je nekonecny... v dalsich urovnich svazu se dostavame svazy jako p*qZ ..., kde p a q jsou opet prvočísla **Poznámku 5.6** chtel jeste dokazat, ze to co rikam je pravda, tzn. obe se dokazalo sporem a bylo.

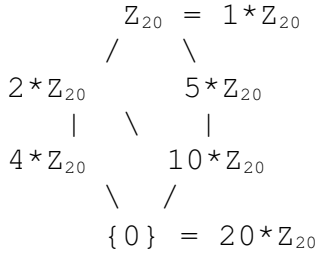
23. svaz vsetkych podgrup cyklickej grupy s 20 prvkami...

20-prvkova cyklicka grupa je izomorfna Z_{20}, **(5.7(2))**

20=2^2*5, tzn soucin lineálních svazů L_{2^2} a L_5, nahazet vsechny podgrupy do Hasseova diagramu tj. "2x1 diagram"

-k nej podgrupy dostanem ako k*Z_{20}, kde k deli n=20, cize
k = 2,4,5,10





(zeml.2004-5 3/15 nebo zeml.2007-8 4.12 nebo zeml.2007-8 4.7)

43. Nakreslete Hasseův diagram třicetiprvkové cyklické grupy

30-prvkova cyklicka grupa je izomorfna Z_{30}, **(5.7(2))**

-rozlozit 30 na prvocisla (2*3*5), nahazet vsechny podgrupy do Hasseova diagramu tj. "krychle" (pozn.$15Z_{30}$ ={0,15})

koatomy: $2Z_{30}$; $3Z_{30}$; $5Z_{30}$

atomy: $6Z_{30}$; $10Z_{30}$; $15Z_{30}$

(zeml.2004-5 3/15 nebo zeml.2007-8 4.12)

27. Popište (nakreslete) svaz všech kongruencí v grupě S_3(o,-1,Id)...

- Chtel dukaz, ze jsem zadnou normalni nevynechal (podle L. Vety - H/G: musi mit podgrupa rad 6,3,2 nebo 1) – tak se proberou vsechny takove podgrupy):
Zřejmě množina {Id} tvoří nejmenší podgrupu grupy S3 a množina S3 je největší podgrupou grupy S3. Poznamenejme, že každá podgrupa musí být uzavřena na nulární operaci, tj. musí obsahovat neutrální prvek Id. Dale snadno nahledneme, že množiny {Id, (12)}, {Id, (23)} a {Id, (13)} jsou

podgrupy, protože (ab) ◦ (ab) = Id pro každou dvojici různych čisel a, b ∈ {1, 2, 3}, z čehož plyne, že {Id, (ab)} je uzavřena na binarni i unarni operaci. Tim jsme probrali grupy generovane transpozicemi (12), (13) a (23).

Snadno rovněž nahledneme, že množina {Id, (123), (132)} je podgrupou generovanou prvkem (123) nebo (132), čimž mame probrany všechny jednogenerovane podgrupy.

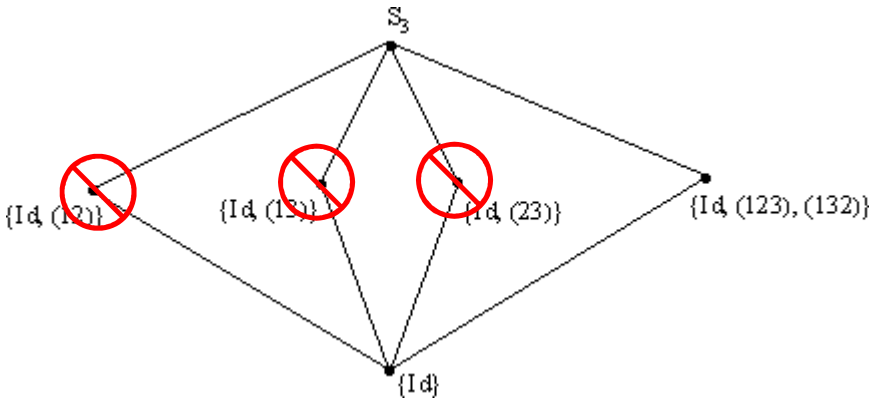
Uvažujme podgrupu H obsahujici dvě různe transpozice (ab) a (ac). Potom H obsahuje take součin (bc) = (ab) ◦ (ac) ◦ (ab), tedy v H už nutně leži všechny transpozice grupy S3. Věta z přednašky linearni algebry, ktera řika, že každou

permutaci dostaneme jako součin transpozic, nam zaručuje, že H obsahuje všechny permutace (protože H je uzavřene na skladani), tedy H = S3. Uvažme konečně podgrupu H obsahujici jednu transpozici (ab) a jeden trojcyklus např. (abc). Potom H obsahuje i transpozici (ac) = (abc)(ab). Obsahuje-li podgrupa H dvě různe transpozice, leži v ni podle předchozi uvahy všechny permutace, proto opět dostavame H = S3.

Podgrupou obsahujici dva různe trojcykly je, jak už vime, množina {Id, (123), (132)}, mame tedy probrane všechny podgrupy grupy S3.

Podle vety o isomorfismu svazu (**4.15**) je isomorfni svazu vsech normalnich podgrup. Na každe nenulove grupě najdeme dvě trivialni normalni podgrupy, v tomto připadě grupy {Id} a S3 a jim přisluši trivialni kongruence id a S3 × S3.

Na přednašce linearni algebry bylo dokazano, že množina všech sudych permutaci (značme ji A3) je uzavřena na skladani, inverzni permutace a obsahuje neutralni prvek. Navic pro každou permutaci p ∈ S3 a σ ∈ A3 plati, že $\mathrm{sgn}(p \circ \sigma \circ p^{-1}) = \mathrm{sgn}(p) \cdot \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(p)^{-1} = \mathrm{sgn}(\sigma)$ tedy $p \circ \sigma \circ p^{-1} \in A3$. Proto je množina všech sudych permutaci A3 = {Id, (123), (132)} normalni podgrupou S3. Kongruence ~ odpovidajici teto podgrupě je určena pravě vztahem $p \sim q \leftrightarrow p^{-1}q \in A3$, což nastava pravě tehdy, když jsou maji obě permutace p i q stejne znamenko.
Protože s prvkem tvaru (ab) musi normalni podgrupa obsahovat i všechny prvky tvaru (s(a)s(b)), kde s ∈ S3, žadna další normalni podgrupa, a tudiž ani žadna další kongruence na S3 neexistuje. $(ac)(ab)(ac)^{-1}=(ac)(ab)(ac)=(bc)$
Jedine normalni podgrupy jsou: A_3 = {Id,(123),(132)} (sude permutace) a trivialni (tedy S_3 a Id). V Hasseove diagramu S_3 -> A_3 -> Id.



(zeml.2004-5 2/10, zeml.2004-5 2/11)

38. Je (Q,<=(klasicke na racionalnych cislach)) svaz? Ak je, tak ci je modularny a ci je uplny.

...

|

0

|

-...

je svaz: inf = minimum a sup = maximum

je modulární: pze je lineární (∀abc, a,<=c: a ∨ (b ∧ c) = (a ∨ b) ∧ c)

není úplný: napr. pokud si vezmeme jako podmnozinu cele Q tak nemá sup

5.Grupy

5. Kolik prvku ma mnozina vsech invertibilnich prvku monoidu grupy Z_{50}(. , 1)(Z_{50} = mod 50).

- V zasade to nebolo fakt nic tazke, staci si zobrat eulerovu fnkciu do nej postupne nasypat vsetky hodnoty a je to, avsak ma upozornil ze prave kvoil takymto pripadom chcel dat Z500 tam by sa to proste riesilo obdobne, ja som to tiez takto robil, ze si nadjete co deli 500(2,5) no a tie prvky vyhadzete a vyhadzete aj sude a je to zostane mnozina invertibilnych prvku, dufam ze som to nepoplietol, inac vysledok mal byt 20 prvkova mnozina {1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49}. Tu som este potom mal dokazat ci dane riesenie je fakt uplne a ci plati pre nejaky obecny pripad

- měla se použít Eulerova funkce a její vlastnosti **(5.12)**:

φ(mn) = φ(m)φ(n) pro *n, m* **nesoudělné** a φ(p^r) = (p-1)p^(r-1) pro *p* prvočíslo **(5.16)**

tedy "počet invertibilních prvků Z_{50} " = φ(50) = φ(5^2)φ(2^1) = 4 * 5^1 * 1 = 20

66. Kolik prvku ma mnozina vsech invertibilnich prvku monoidu grupy Z_{500}(. , 1).

- "počet invertibilních prvků Z_{500} " = φ(500) = φ(5^3)φ(2^2) = 4 * 5^2 * 1 * 2^1 = 200 **(5.12,5.16)**

7. Kolik prvku ma mnozina vsech invertibilnich prvku monoidu grupy Z_{990}(. , 1)?

- "počet invertibilních prvků Z_{990} " = φ(990) = φ(2*3^2*5*11) = (2^0*1) * (3^1*2) * (5^0*4) * (11^0*10) = 1 * 6 * 4 * 10 = 240 **(5.12,5.16)**

8. Kolik generatoru ma Z_{270} :

- smyslem bylo napsat definici fce (+ ty dve dalsi doplnujici - tim bylo myslim splneno i to vztah ke grupam a monoidum) + vzorec pro n (jak si to rozlozim na mocniny prvocisel - 5.16) + dukaz toho vzorecku -> takze dokazat 5.16 ... tam jsem se trosicku zamotal v miste, kde se vyuziva 5.15 (Cinska o zbytcich) - respektive ja blbec jsem se mu priznal, ze si v tom, ze Zn.m* je isomorfni s Zn* x Zm* nejsem uplne jisty - i kdyz jsem to tam mel napsane ---> on na to: "Ale vzdyt to tu mate napsane, to je cinska veta o zbytcich... No, tak si teda dokazte, ze tam nejaky isomorfismu je, zkuste tam nejaky najit" ... takze sranda, vlastne jsem (mozna zbytecne) musel delat neco na zpusob dukazu CVoZb

- φ(270) = φ(2*3^3 *5) = (1*2^0) * (2*3^2) * (4*5^0) = 1 * 18 * 4 = 72 **(5.12,5.16)**

25. Dokazat, ze mnozina vsetkych regularnych matic radu n tvori grupu (GL_n(T)(*, -1, I_n)) a pre par

vybranych podmnozin urcit ci su to podgrupy.

Stacilo vediet z linagebry, ze regularne matice maju vzdy inverz (=ex.inverz.prvku), nasobeni 2 reg.matic je regulární matice(=uzavrenost na nas.), nasobenie je asociativne (=asociativita nas.) a ze det(AB)=det(A)det(B) (na co nam to je det? Na ty podrupy?).

48. Kolik prvku radu 20 (tj. takovych, ze generuji podgrupu radu 20) obsahuje cyklicka grupa radu 1000 ?

-Je nutne vyuzit Lagrangeovu vetu k overeni toho, ze CG_{1000} vubec obsahuje nejakou podgrupu radu 20 (**Dusledek 5.4**: 20 / 1000), potom se ukaze ze ji obsahuje, a ze takova podgrupa je tam jen jedna (udelame hassenuv diagram podrup a z nej vidime ze $|50*CG_{1000}|=20$ a je jenom 1) a protoze podgrupa cyklicke je opet cyklicka, tak pocet jejich generatoru je φ(20) (eulerova funkce). φ(20)=8 a to je vysledek.

Je dobry vedet jak je definovana Eulerova funkce (φ(n)=|{k|0<k<n,NSD(k,n)=1}|).

6.Okruhy

49. Popiste vsechny kongruence na okruhu celych cisel Z(+,*,-,0,1)

-Pouzit vetu **(6.2)**. Nez jsem se do toho pustil, tak mi stihl behem zadavani rict, ze mam pouzit vetu, ktera dava do vztahu kongruence a idealy okruhu. Dokonce mi rekl, ze je to ta posledni veta z toho, co se zatim probralo. Dale mi k tomu rekl, ze idealem Z je podgrupa Z a at si uvedomim, co jsou podgrupy Z. Po tomto to bylo zase na jeden radek. Stacilo napsat zneni vety, kterou jsem si nepamatoval. Nastesti je to analogie s 1.13, tak jsem zkusil:
ρ je kongruence na Z ⇔ $[0]_\rho$ je ideal Z a (a,b)∈ ρ ⇔$^{def.}$ b-a ∈ $[0]_\rho$.
Kdyz mi navic rekl, ze ideal je podgrupa (podgrupy Z jsou normalni) tak je to v podstate 1.13 (trefa! to je veta **6.2**)

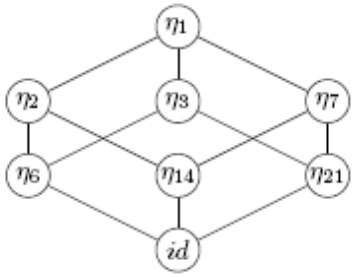
Reseni ulohy je: kZ jsou vsechny podgrupy Z (5.6) => kZ jsou vsechny idealy Z (**6.2**) => kongruence ρ na Z jsou prave: (a,b)∈ ρ ⇔ b-a ∈ kZ neboli k|(b-a)

- Napsal jsem jen, ze podle vety 6.2 je izomorfni svazu vsech idealu a podle 5.6 ma Z idealy prave tvaru kZ pro k nezaporne cele cislo.Pak jsem nakreslil jak ten svaz idealu vypada.

- takze treba (6.2) (aspon myslim) a vzpomenout si na idealy nad Z

17. Nakreslit svaz všech kongruencí na okruhu Z_{42}(+,*,-,0,1)

Podle Věty **(6.2)** z přednášky nám stačí najít izomorfní svaz všech ideálů. Podle zjištění předchozí úlohy se jedná právě o Hasseův diagram svazu všech podgrup grupy Z_{42}(+,−, 0). Označíme-li opět ný kongruenci odpovídající ideálu kZ_{42}, tj. kongruenci pro niž platí, že (a, b) ∈ nýk ⇔ k/a − b, dostáváme obvyklým způsobem:



(zeml.2007-8 5.4)

41. Nakreslit svaz všech kongruencí na okruhu Z_{27}(+,*,-,0,1)

lineární svaz Z_{27}->$3Z_{27}$->$9Z_{27}$->{0}

21. Popiste svaz kongruenci na okruzich realnych cisel R(+,*,-,0,1) a racionalnich cisel Q(+,*,-,0,1).

Staci si uvedomit, ze kazda kongruence na okruhu je izomorfni nejakemu idealu **(6.2)**, a protoze realna i racionalni cisla jsou telesa, maji jenom dva idealy {0} a R **(6.4)**, ktere odpovidaji Id a RxR (QxQ). Pak chtel k tomu jeste napsat vety, z kterych to plyne, bez dukazu

RxR->id

14. Popsat svaz vsech kongruenci okruhu komplexnich cisel C(+,.,-,0,1).

Pouzilo se, ze kongruence a idealy na okruhu si vzajemne odpovidaji **(6.2)**. Ale protoze jsem nevedela, jak najit vsechny idealy, Zemlicka mi poradil, ze mam nejak vyuzit, ze C je teleso. Teleso obsahuje pouze 2 idealy **(6.4)**, v nasem pripade C a {0}, takze svaz kongruenci je tvoren kongruencemi CxC a Id.

CxC->id

39. Popsat maximalni idealy okruhu Z(+, -, ., 0, 1)

pZ, kde je p prvocislo **(5.6)** (max.ideal – koatom svazu všech ideálů)

3. Dokažte, že I je ideál okruhu Zn(+, ·,–, 0, 1), právě když je tvaru I = kZ pro k = 0 nebo k/n.

Stačí si rozmyslet, že ideály okruhu Zn(+, ·,–, 0, 1) právě splývají s podgrupami grupy Zn(+,–, 0). Podle **Věty 5.6** právě tvaru kZ_n pro vlastní dělitele čísla n nebo k = 0

44. Rozhodnete, zda struktura P(X)(sym. diference, prunik, Id, prazdna mnozi., X) je okruhem. Pokud ano, naleznete nejaky netrivialni ideal a jemu prislusnou kongruenci.

Je to easy, jen se chce trosku zamyslet. Clovek si napise odpovidajici definici okruhu a zkouma, zda se chovaji operace pruniku a symetricke diference jako krat a plus. Inverzni prvek k A je A (potom sym. dif. je prazdna mnozina). Jeste overit asoc. zprava a zleva. Po dalsi trosce premysleni by cloveka mohlo napadnout, ze pokud C nalezi do P(X), tak potom P(C) je ideal. Pres vetu, ktera dava do vztahu idealy a kongruence se mechanicky dostane prislusna kongruence

50. existuje nejaky izomorfizmus mezi libovolnymi dvema nasledujicimi okruhy - Z(+,-,×,1,0) ; R(+,-,×,1,0) ; C(+,-,×,1,0).

-mezi Z a cimkoli se dal pouzit argument |Z| < |R| resp.|C| (stacilo rict, netreba diagonalizovat ci jinak dokazovat mohutnost |R|). Btw da se na to jit i vylozene pres homomorfizmy, a sice ze 1 musi jit na 1, 0 na 0 => vsechny zbyle prvky Z uz nutne musi jit na sve "ekvivalenty" v R resp. C ... proto to rozhodne neni zobrazeni na (epimorfizmus).

-Mezi R a C si staci vsimnout, ze v C je prvek a, pro ktery plati, ze a×a je opacny prvek k 1 (ktera musi jit na 1, protoze homomorfizmus), ale takovy prvek v R fakt není

20. Jsou nektere z okruhu Z(+,.,-,0,1), Q(+,.,-,0,1) a R(+,.,-,0,1) izomorfni?

stacilo sa opriet o to, ze v Z nie su inverzne prvky oproti Q a R a v Q zas odmocniny oproti R, nejak to formalne zapisat a bolo.

15. Dana mnozina R={ $\frac{a}{b}$: a,b∈ Z, NSD(b,7) = 1 }. Popisat svaz vsetkych idealov R.

R ma okrem trivialnych idealov aj vlastne idealy a tie maju tvar (7*k).R , pze pro r ∈ R a i ∈ (7*k).R: r i ∈ (7*k).R a ir ∈ (7*k).R

Popisat svaz vsetkych kongruencii na R. Lineární svaz R->7*R->14*R->.....->{0}

45. Mejme prvocislo p a mnozinu R={ $\frac{a}{b}$: a,b∈ Z, NSD(b,p)=1}. Dokazte, ze R je podokruh racionalnich cisel

R(+,-,*,0,1) je okruh

skoro stejna definice jako Q => podokruh

42. Najdi nejmensi kladny prvek k idealu $245Z_{320}$, pak najdi x takové že x.245=k v Z_{320}

proste zpetny chod eukleidova alg:

320 = 1*245+75

245 = 3*75+20

75=3*20+5

k=NSD(245,320)=5

5=320 - 1*245-3*(245 - 3*(320 - 1*245))= 10*320-13*245

x=-13 mod 320=307

46. Najdi nejmensi kladny prvek k idealu $248Z_{320}$, pak najdi x takové že x.248=k v Z_{320}

320 = 1*248+72

248 = 3*72+32

72=2*32+8

k=NSD(248,320)=8

8=320 - 1*248-2*(248-3*(320 - 1*248))=7*320-9*248

x=-9 mod 320=311

11. Jak vypadá podílové těleso okruhu všech realných polynomů jedné neurčité R[x] (resp. dvou neurčitých R[x,y]).

- Tohle je taky jednoduchý, jak se nad tím zamyslíte. Já tam furt hledal nějaký chytáky a na tom zkejsl sakra dlouho. F/~ je těleso izomorfní tělesu Q = {p/q; p je polynom, q je nenulový polynom}. To po mně taky chtěl dokázat a nakonec na boj o jedničku jsem mu dokázal, že ~ je ekvivalence. Mezi racionálními čísly a F/~ nějaká bijekce bude. Což o to Ale nenajdeš tam žádnej izomorfismus. Já jen chtěl naznačit, že s racionálními čísly se tam vůbec neoperuje a vysvětlit nedorozumění, ke kterému došlo pravděpodobně, když jsem si těleso lomených polynomů označil jako Q. Jinak ta bijekce může vypadat jakkoliv se ti zlíbí, já použil "nejintuitivnější" f: p/q -> [(p,q)]~

- To je gASK-ova otazka z lonska z z fearu a je tam i plus minus vysvetlena ... R[x] je obor integrity takze muzu definovat algebru F, ekvivalenci ~ a F/~ jako podilove teleso a dostanu to co potrebuju -- plyne to z vet 6.9 a 6.10 v tom sylabu

95. Uvažujem okruh polynomů R[x](+,.,-,0,1) rozhodnete zda je fakt.okruh R[x]/(x^2+1)R[x] tělesem

podle ty vety 6.5: R/I je teleso kdyz I je maximalni ideál
maximalni ideal je koatom ve svazu podrup, koatomy jsou v Z prvocisla krat Z (pZ), no a tady mame polymomy kde ekvivalent prvocisel jsou ireducibilni polynomy (nejde uz nicim vydelit, jenom sam sebou)
(x^2+1) je maximalni bo je v R ireducibilni
takze je to teleso