Otázky testu:

Odpovědi nejsou nijak ověřené.

---

1. Booleovy okruhy

1.1 Definujte Booleův okruh.

O okruhu R(+; *; -; 0; 1) řekneme, že je Booleùv, je-li to komutativní okruh a pro každé r ∈ R platí, že r*r = r a r + r = 0.

1.2 Kdy je Booleův okruh oborem integrity?

K ověření:
Obor integrity - komutativní okruh, kde navíc a!=0 & b!=0 => a*b!=0
buď BO booleúv okruh, ten odpovídá booleově algebře (podle 1.2(2)), tak je izomorfní s potenční algebrou nad atomy A. Pak podmínka je "a průnik b != 0", což funguje jen, pokud |A|=<1. Tedy pokud |P(A)|=|BA|=|BO|<=2^1, tedy jen případ kdy obsahuje právě 1 a 0 a pokud vyhovuje definicím, tak i případ jediný prvek je 1=0.
Lépe: a*a=a -> (1-a)*a=0 -> více než dva prvky má netriviální dělitele nuly

1.3 Uveďte příklad Booleova okruhu.

Viz příklad 1.1 P(X)(sym dif, průnik, id, 0, X)

1.4 Popište konstrukci Booleova okruhu na Booleově algebře.

V1.2: Nechť SA = S(v;^; 0; 1; 0) je Booleova algebra. Denujeme-li na S binární operaci + předpisem a + b = (a ^ b 0) v (a 0 ^ b), pak S0 = S(+;^;IdS; 0; 1) je Booleův okruh. Navíc P je podalgebra resp. kongruence SA, právě když je P podalgebra resp. ró kongruence SO.

1.5 Popište konstrukci Booleovy algebry na Booleově okruhu.

V1.2: (2) Nechť S0 = S(+;* ;- ; 0; 1) je Booleův okruh. Denujeme-li na S binární operaci s předpisem a v b = a+b+(a*b) a unární operaci ' předpisem a a' = 1+a, pak SA = S(v;*; 0; 1;') je Booleova algebra. Navíc P je podokruh resp. kongruence SO, právě když je P podalgebra resp. kongruence SA.

1.6 Jak souvisí kongruence a podalgebry Booleovy algebry a Booleova okruhu?

Věta 1.2

1.7 Kolik kongruencí existuje na Booleově algebře o 2^n prvků?

1.8 Kolik kongruencí existuje na Booleově okruhu o 2^n prvků?

odpovědi:

1. V x : x^2 = x
2. pokud obsahuje 2 prvky - {0,1} jinak a průnik a^c = 0 dává spor
3. P(X)(%, prunik, Id, \emptyset, X)
4. S_o=S(+,.,=,0,1) —> S_a(or,.,0,1,'), a or b := a+b+a.b
5. S_a=S(or, and, 0, 1, ') —> S_o=S(+, and, Id, 0, 1), a+b:= (a & b') | (a' & b)
6. P je podalg. / ró kongr. na S_a <=> P je podalg. / kongr. S_o
7. Svaz všech kongruencí je izom. svazu všech podmonžin atomů konečné BA
8. 2^n
9. —||—

---

2. Dělitelnost

2.1 Zaveďte relace dělení a asociovanosti na komutativním monoidu s krácením.
2.2 Zaveďte relace dělení a asociovanosti na oboru integrity.
2.3 Popište relaci dělení a asociovanosti na oboru integrity pomocí ideálů.
2.4 Kdy tvoří relace dělení na komutativním monoidu s krácením uspořádání?
2.5 Definujte v komutativním monoidu s krácením největší společný dělitel.
2.6 Definujte v komutativním monoidu s krácením ireducibilní prvek.
2.7 Definujte v komutativním monoidu s krácením prvočinitel.
2.8 Je v oboru integrity každý prvočinitel ireducibilním prvkem? Pokud ne, uveďte příklad.
2.9 Je v oboru integrity každý ireducibilní prvek prvočinitelem? Pokud ne, uveďte příklad.
2.10 Vyslovte tvrzení o jednoznačnosti ireducibilního rozkladu v komutativním monoidu s krácením. // žemlička slibuje, že tam nebude, protože ho nebral
2.11 Vyslovte tvrzení o existenci a jednoznačnosti ireducibilního rozkladu v oborech integrity hlavních ideálů.
PID(obor hlavnich idealu) je UFD (veta 3.3) ktery ma z definice jednoznacny rozklad az na asociovanost.

1. a|b iff ex. k: ak = b; a||b iff a/b & b/a
2. —||—
3. R, a|b iff bR \subset aR && a||b iff aR = bR
4. pokud S(.) = S(.)/|| - poznámka 2.3.(4)(neboli neexistují dva různé asociované prvky)
5. c je GCD(a_1,..,a_n), c|a_i. && V d, d|a_i => d|c
6. TODO: Ired
7. TODO: Prvoc
8. Ano. V2.6
9. Ne. příklad 3.2 + norma(v Z[sqrt(5) prvky 2 a sqrt(5)+1)
10.

---

3. Obory hlavních ideálů

3.1 Co je obor integrity hlavních ideálů?
kazdy ideal je hlavni
3.2 Definujte obor UFD.
3.3 Uveďte příklad oboru integrity, který není oborem integrity hlavních ideálů.
pr 3.7.1
3.4 Uveďte příklad oboru integrity, který není eukleidovský.
to samy
3.5 Definujte eukleidovský obor integrity.
3.6 Uveďte nějakou eukleidovskou funkci na podokruhu Z[i] okruhu komplexních čísel.
norma: a ^2 + b^2
3.7 Uveďte nějakou eukleidovskou funkci na oboru polynomů R[x] s reálnými koeficienty.
stupen polynomu

3.8 Rozhodněte, zda je obor Z[i] eukleidovský. Stručně vysvětlete.
Ano - aa+bb je norma - viz priklad 3.4
3.9 Rozhodněte, zda je obor Z[√5] eukleidovský. Stručně vysvětlete.
Neni obor hlavnich idealu - nemuze byt euklidovsky - priklad 3.2
3.10 Rozhodněte, zda je obor Z[x] eukleidovský. Stručně vysvětlete.
Neni obor hlavnich idealu - nemuze byt euklidovsky - priklad 3.7
3.11 Rozhodněte, zda je obor Z2[x] eukleidovský. Stručně vysvětlete.
Ano - normou je stupen polynomu - priklad 3.4.2
3.12 Rozhodněte, zda je obor Q[x] eukleidovský. Stručně vysvětlete.
Ano - normou je stupen polynomu - priklad 3.4.2
3.13 Rozhodněte, zda je obor Z7[x] eukleidovský. Stručně vysvětlete.
-//-
3.14 Je v eukleidovském oboru každý prvočinitel ireducibilním prvkem?
je to obor hlavnich idealu, tam to plati, takze tady taky (3.3)

---

4. Polynomy

4.1 Definujte násobení v monoidovém okruhu.
4.2 Definujte sčítání v monoidovém okruhu.
4.3 Definujte stupeň polynomu.
4.4 Uveďte příklad polynomů, pro něž deg p · q < deg p + deg q.
p = 2 q = 2 nad Z4[x]
4.5 Pro které okruhy R platí, že deg(p + q) ≤ max(deg p, deg q) ∀p, q ∈ R[x]?
Pro vsechny - V4.3
4.6 Pro které okruhy R je R[x] je obor integrity?
pro obory - V4.3
4.9 Lze polynom X^17 + X^4 + 2 vydělit se zbytkem polynomem 2X^2 + 1 v oboru Z[x]?
Ne, protoze neexistuje takové k, že x^17 = k*2X^2
4.10 Lze polynom X^17 + X^4 + 2 vydělit se zbytkem polynomem 2X^2 + 1 v oboru Q[x]?
Ano, jde o těleso a tedy funguje EA.
4.11 Lze polynom X^17 + X^4 + 2 vydělit se zbytkem polynomem 2X^2 + 1 v oboru Z3[x]?
Ano, jde o těleso a tedy funguje EA.
4.12 Definujte dosazovací homomorfismus na komutativním okruhu polynomů.
pozn 4.4
4.13 Definujte kořen a vícenásobný kořen polynomu.
za pozn 4.4
4.14 Co znamená, že se polynom rozkládá na kořenové činitele?
stejna def
4.15 Jak souvisí stupeň polynomu nad oborem a počet jeho kořenů?
Poznamka 4.5.3 - je-li polynom nenulový, pak má nejvýše tolik kořenů jako je stupeň.
4.16 Definujte derivaci polynomu.
4.17 Popište vícenásobný kořen polynomu pomocí derivace.
je to vícenásobní koren ⇔ je to koren derivace a zaroven koren puvdoniho polynomu
4.7

4.18 Má polynom X^12 – x vícenásobný kořen v oboru Z3[x]? Stručně zdůvodněte.
derivace je -1, ta nemá kořen, takže nemá vícenásobný ten původní
4.19 Má polynom X^12 – 1 vícenásobný kořen v oboru Z3[x]? Stručně zdůvodněte.
Ano, má 1 a 2 jako vícenásobné, protože derivace je nula -> všechny kořeny původního polynomu (což jsou 1 a 2 podle dosazení) jsou kořeny i zderivovaného.
4.20 Má polynom X^11 – 1 vícenásobný kořen v oboru Z3[x]? Stručně zdůvodněte.
Ne - původní má kořen jen číslo 1, derivace jen 0
4.21 Má polynom X^22 – x vícenásobný kořen v oboru Z11[x]? Stručně zdůvodněte.
Ne, derivace nemá kořen.
4.22 Má polynom X^22 – 1 vícenásobný kořen v oboru Z11[x]? Stručně zdůvodněte.
Ano - derivace je nula -> má všdechny kořeny, víme, že původní má kořen třeba 1, ten vyhovuje
//4.23 Má polynom X^22 – x vícenásobný kořen v oboru Z11[x]? Stručně zdůvodněte.
4.24 Má polynom X^22 – 1 vícenásobný kořen v oboru C[x]? Stručně zdůvodněte.
víme, jak kořeny vypadají (jsou různé a na jednotkové kružnici) a nejsou vícenásobné

---

5. Kořenová a rozkladová nadtělesa

5.1 Uveďte definici kořenového a rozkladového nadtělesa polynomu.
5.2 Definujte stupeň rozšíření těles.
5.3 Vyslovte tvrzení o existenci kořenového nadtělesa polynomu.
V5.6
5.4 Vyslovte tvrzení o existenci a jednoznačnosti rozkladového nadtělesa polynomu.
existence veta 5.6 jednoznacnot dusledek 7.4.
5.5 Je stupeň kořenového nadtělesa polynomu jednoznačně určen polynomem? Stručně vysvětlete.
Ne, protipříklad: x^4-1, R je kořenové nadtěleso, ale C taky a mají různé stupně rozšíření
5.6 Je stupeň kořenového nadtělesa ireducibilního polynomu jednoznačně určen polynomem? Stručně vysvětlete.
podle D7.2 - ano
5.7 Je stupeň rozkladového nadtělesa polynomu jednoznačně určen polynomem? Stručně vysvětlete.
Ano - //dáno z definice a tím i jeho stupeň
(asi spis dano z jednoznacnosti podle dusledku 7.4)
5.8 Určete stupeň rozšíření kořenového nadtělesa polynomu x^2 + 1 nad tělesem Q. Stručně zdůvodněte.
Má kořeny i a -i a tedy kořenové nadtěleso je tak jako tak Q[i]. To má stupeň **2.**
5.9 Určete stupeň rozšíření kořenového nadtělesa polynomu x^2 + 1 nad tělesem R. Stručně zdůvodněte.
Má kořeny i a -i a tedy kořenové nadtěleso je tak jako tak C - má stupeň dva.
5.10 Určete stupeň rozšíření kořenového nadtělesa polynomu x^2 + 1 nad tělesem Z3. Stručně zdůvodněte.
Je ireducibilní, podle 6.3.1, kde deg m = deg tohohle polynomu, stupeň je 2
5.11 Existuje prvek řádu 5 v multiplikativní grupě tělesa Z67? Stručně zdůvodněte.
Ne, protože nedělí velikost multiplikaticní grupy z67, která má velikost 66.

5.12 Existuje prvek řádu 66 v multiplikativní grupě tělesa Z67? Stručně zdůvodněte.
Ano, protože dělí velikost multiplikaticní grupy z67, která má velikost 66.
5.13 Existuje prvek řádu 6 v multiplikativní grupě tělesa Z67? Stručně zdůvodněte.
Ano, protože dělí velikost multiplikaticní grupy z67, která má velikost 66.
5.14 Existuje prvek řádu 11 v multiplikativní grupě tělesa Z67? Stručně zdůvodněte.
Ano, protože dělí velikost multiplikaticní grupy z67, která má velikost 66.
5.15 Existuje prvek řádu 12 v multiplikativní grupě tělesa Z67? Stručně zdůvodněte.
Ne, protože nedělí velikost multiplikaticní grupy z67, která má velikost 66.

---

6. Minimální polynomy a algebraické prvky

6.1 Definujte algebraický prvek a algebraické rozšíření těles.
6.2 Co je minimální polynom algebraického prvku nad tělesem?
6.3 Je-li T ⊆ U rozšíření těles a α ∈ U, popište kdy T[α] != T(α).
6.4 Je-li T ⊆ U rozšíření těles a α ∈ U, popište kdy T[α] = T(α).
V6.3.3, když je alfa algebraická
6.5 Je-li T ⊆ U rozšíření těles a α ∈ U, popište kdy je [T(α) : T] konečné.
6.6 Jak souvisí stupeň minimálního polynomu algebraického prvku se stupněm rozšíření?
Rovnají se, 6.3.1
6.7 Rozhodněte, zda je prvek √5 + (jedenáctá odmocnina ze 13) ∈ R algebraický nad tělesem Q. Stručně zdůvodněte.
Ano. x-√5 = (jedenáctá odmocnina ze 13), umocním na jedenáctou, doupravím
6.8 Rozhodněte, zda je prvek 2^(-3/7) +3 ∈ R algebraický nad tělesem Q. Stručně zdůvodněte.
Ano.
6.9 Určete stupeň minimálního polynomu prvku i ∈ C nad tělesem Q. Stručně zdůvodněte.
x^2 +1 . Stupen aspon dva, kvuli tomuhle polynomu je to 2.
6.10 Určete stupeň minimálního polynomu prvku i ∈ C nad tělesem R. Stručně zdůvodněte.
x^2 +1 . Stupen aspon dva, kvuli tomuhle polynomu je to 2.
6.11 Určete stupeň minimálního polynomu prvku i - √15 ∈ C nad tělesem R. Stručně zdůvodněte.
2
6.12 Určete stupeň minimálního polynomu prvku 1/(sqrt15 - 11) ∈ R nad tělesem Q. Stručně zdůvodněte.
Po rozšíření je vidět, že stačí přidat sqrt 15.

---

7. Rozkladová nadtělesa a Galoisova teorie

7.1 Definujte pojem rozkladového nadtělesa polynomu.

7.2 Vyslovte tvrzení o existenci a jednoznačnosti rozkladového nadtělesa polynomu.

V7.4 + V5.6

7.3 Je pro prvočíslo p každé kořenové nadtěleso polynomu X^p − 1 nad Q Galoisovým rozšířením? Vysvětlete.

Kořenové nadtěleso kořene 1 je triviální (Q) - je galoisovo. Jinak je (x^p-1)/(x-1) je ireducibilní, takže kořenové nadtěleso se rovná rozkladovému(to neplati ne? :D). A vím, že nemá násobné kořeny, protože vím, jak vypadají.

Nebo se da rict, ze kdyz tam bude jeden koren, tak ten vygeneruje vsechny ostatni, protoze p je prvocislo a koreny jsou klasicky na jednotkove kruznici.

7.4 Jak vypadá rozkladové nadtěleso polynomu X^2 + 1 nad tělesem R?

C

7.5 Jak vypadá rozkladové nadtěleso polynomu X^2 + 1 nad tělesem Q?

Q[i]

7.6 Jak vypadá rozkladové nadtěleso polynomu X^3 − 2 nad tělesem R?

C

7.7 Jak vypadá rozkladové nadtěleso polynomu X^3 − 2 nad tělesem Q?

Q[3odmocnina ze 2 , e^(i*⅔*pí)]

7.8 Definujte Galoisovo rozšíření.

7.9 Je rozšíření Q ⊆ Q[√5] Galoisovo?

Ano, x^2 - 5

7.10 Je rozšíření Q ⊆ Q[třetí odmocnina z pěti] Galoisovo?

Polynom x^3-2 je ireducibilní nad Q a zaroven je to minimalni polynom daneho prvku. A tedy každé rozkladové nadtěleso, které obsahuje tento prvek nutně obsahuje i komplexní část, tedy kořenové nadtěleso daného prvku se nerovná rozkladovému.

7.11 Najděte aspoň dva různé prvky Galoisovy grupy rozšíření Z5 ⊆ F, kde F je konečné těleso o 125 prvcích.

- zde je trochu záludně skryt odkaz na 10.1(c), totiž na pozorování,
že zobrazení f_{p^n} je pro homomorfismus konečného tělesa F do sebe,
což musí být Z_p-izomorfismus (tedy prvek Galoisovy grupy).
Protože Věta 9.5 říká, že v daném případě má Galoisova grupa
právě [F:Z_p]=3 prvky, není už těžké nahlédnout, že ji tvoří vedle
identity homomorfismus f_5 a f_{25}.

---

8. Abelova-Ruffiniho věta a Galoisovy grupy

8.1 Definujte Galoisovu grupu rozšíření těles.

8.2 Existuje nějaká nekonečná Galoisovu grupa Galoisova rozšíření? Stručně vysvětlete.

Je to galoisovo rozšíření a tedy jde o rozkladové nadtěleso polynomu stupne n a tím pádem je konečného stupně. Podle D8.2 existuje prostý grupový homomorfismus do Sn.

8.3 Jak vypadá Galoisova grupa rozšíření Q ⊆ Q[√3]?

={id,proužkovana identita(= a+ b√3 -> a -b√3)}

8.4 Jak vypadá Galoisova grupa rozšíření Q ⊆ Q[třetí odmocnina ze dvou]?

id. Pouze jeden koren minimalniho polynomu je obsazen v telese. (pr 8.3.3)

8.5 Jak vypadá Galoisova grupa rozšíření R ⊆ C?

id, prouzkovana identita

8.6 Pro T ⊆ U ⊆ V Galoisova rozšíření komutativních těles vyslovte tvrzení o vztahu Galoisových grup pak Gal(V /U), Gal(V /T) a Gal(U/T).

v 8.6

8.7 Co znamená, že je polynom řešitelný v radikálech?

8.8 Vyslovte tvrzení o vztahu řešitelnosti polynomu v radikálech a řešitelností vhodné grupy.

V9.5

8.9 Vyslovte nějakou verzi Abelovy-Ruffiniho věty o řešitelnosti polynomů.

V9.8

---

9. Konečná tělesa

9.1 Vyslovte tvrzení o existenci a jednoznačnosti konečných komutativních těles dané velikosti.

V 10.2

9.2 Kolik existuje neizomorfních těles o 50 prvcích? Stručně zdůvodněte.

0

9.3 Kolik existuje neizomorfních těles o 49 prvcích? Stručně zdůvodněte.

1

9.4 Kolik existuje neizomorfních těles o 47 prvcích? Stručně zdůvodněte.

1

9.5 Vyslovte tvrzení o existenci ireducibilních polynomů nad konečnými komutativními tělesy.

V10.5

9.6 Existuje ireducibilní polynom stupně 2 nad tělesem o 4 prvcích?

jo, V10.5

9.7 Vyslovte tvrzení o existenci podtěles konečných komutativních těles.

P10.4

9.8 Kolik podtěles obsahuje 64-prvkové těleso? Stručně zdůvodněte.

4

Tělesa o velikost 2 ^ {1,2,4,8}

PODLE p10.4

9.9 Existuje podtěleso o čtyřech prvcích 32-prvkového tělesa? Stručně zdůvodněte.

NE

2 nedeli 5

Podle p10.4

9.10 Existuje podtěleso o čtyřech prvcích 16-prvkového tělesa? Stručně zdůvodněte.

Jo. 2|4

Podle p10.4

9.11 Co je bezčtvercový rozklad a je k dispozici pro každý nekonstantní polynom?

Viz skripta.

A existuje.

P 11.2

---

10. Volné algebry a variety

10.1 Zkonstruujte volnou algebrou termů.

10.2 Vyslovte tvrzení o tom, jak dostat libovolnou algebru z algebry termů.

10.3 Kdy jsou dvě algebry termů izomorfní?

10.4 Definujte součin algeber.

10.5 Definujte pojem varieta algeber.

10.6 Uveďte příklad nějaké variety algeber.

10.7 Co znamená, že algebra splňuje nějakou identitu?