

2. izpit iz DISKRETNIH STRUKTUR 2 (IŠRM)

30. junij 2017

REŠITVE

Priimek in ime: _____

Vpisna št.: _____ Vrsta: _____ Kolona: _____

1. (16 točk) Naj bo končni obseg $GF(2^5)$ generiran z nerazcepnim polinomom $f(x) = x^5 + x^2 + 1$. Preverite, da je polinom f res nerazcepen nad $\mathbb{Z}_2$. Izračunajte inverz elementa $x^2 + 1$. Rezultat zapišite v obliki polinoma stopnje največ 4.

a) Ali lahko f razcepimo?- ime linearni faktor $\Leftrightarrow$ ima ničlo

$$f(0) = 1, f(1) = 1 \quad \Rightarrow f \text{ nima lin. faktorja}$$

- kvadratni + kubni faktor: v obeh sta vredni in prosti člen enako 0

$$\begin{aligned} f(x) &= (x^2 + ax + 1)(x^3 + bx^2 + cx + 1) \\ &= x^5 + x^4(a+b) + x^3(1+ab+c) + x^2(1+b+ac) \\ &\quad + (a+c)x + 1 \end{aligned}$$

$$x^4: a+b=0 \rightarrow a=b$$

$$x^3: 1+ab+c=0 \rightarrow a=c$$

$$x^2: 1+b+ac=1$$

$$x: a+c=0$$

 $\Rightarrow f$ je nerazcepen!

$$\begin{aligned} 1+0^2+a &= 0 \\ 1+a+0^2 &= 1 \end{aligned} \rightarrow \text{konflikt}$$

b) Inverze izračunamo s pomočjo R.E.A.

x^3+x+1	x^5+x^2+1	$\cancel{x}$	0
	x^2+1	$\cancel{0}$	1
x	x	x^3+x+1	
x	1	<u>x^4+x^2+x+1</u>	
	0		

$$(x^2+1)^{-1} = \underline{\underline{x^4+x^2+x+1}}$$

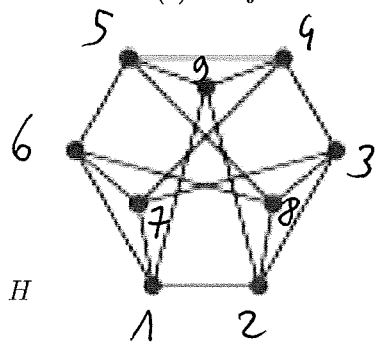
Vse naloge je treba ustrezno utemeljiti!

2. (9+7+9=25 točk) Za graf $G = C_3 \square C_3$ določite naslednje lastnosti:

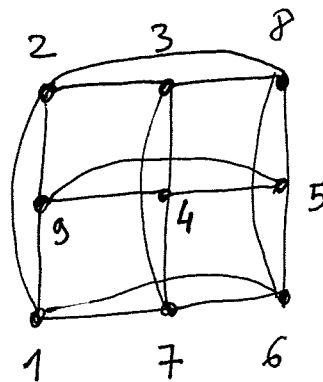
(a) Ali je ravninski?

(b) Kromatično število.

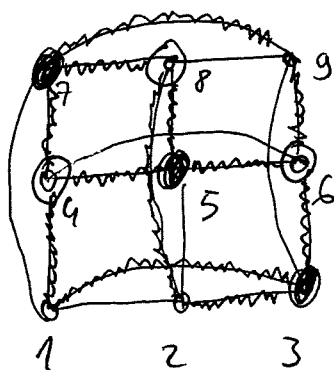
(c) Ali je izomorfen grafu H iz spodnje slike?



H ni ravninski
drugače:
(v vsaki vrstici
po en Δ ,
preverimo, da
so vsi tri pravi)



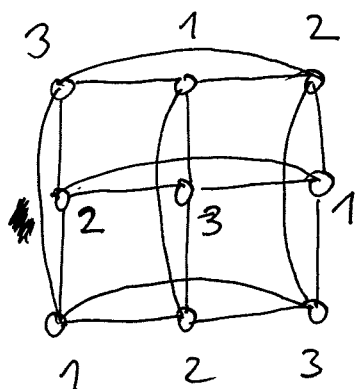
a)



Graf $C_3 \square C_3$ ni ravninski;
v njem smo našli subd. $K_{3,3}$;
nosilci je označenih 6 ~~točk~~ vršic
(3 belo, 3 črne) in prezoze / poti
med njimi.

b) Graf vsebuje cikel lihe dolžine (npr. 123),
zato je $\chi(C_3 \square C_3) \geq 3$

Ker se lahko pobarvamo s tremi barvami
(označeno na sliki spodaj), $\chi(C_3 \square C_3) \leq 3$
Torej je $\chi(C_3 \square C_3) = 3$



c) Grafo sta izomorfna,
Eden od izomorfizmov je

$$f: \begin{array}{c|ccccccccc} V(H) & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline V(G) & 1 & 7 & 8 & 5 & 6 & 3 & 2 & 9 & 4 \end{array}$$

Očitno je bijekcija.

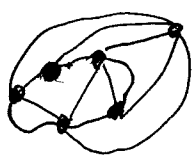
Ker sta grafo enako narisana
in slikamo vršiča v istakene vršiče,
se ohranjajo tudi prezoze. Torej je f izomorfizem.

3. (9+9+7=25 točk) Graf je *zunanje ravninski*, če ga v ravnino lahko narišemo tako, da se nobeni dve povezavi ne sekata (je ravninski) in so pri tem vsa vozlišča na robu zunanjega lica.

- (a) Pokažite, da je graf G zunanje ravninski natanko tedaj, ko je ravninski graf G' , ki ga dobimo tako, da grafu G dodamo eno vozlišče in ga povežemo s povezavami z vsemi vozlišči grafa G .
- (b) Naj bo G povezan zunanje ravninski graf z n vozlišči in m povezavami. Pokažite, da potem velja $m \leq 2n - 3$.
- (c) Pokažite, da noben 4-regularen graf ni zunanje ravninski.

(a) ($\Rightarrow$) Naj bo G zunanje ravninski $\Rightarrow$ v ravnino ga narišemo tako, da so vse vozlišča na robu zunanjega lica. Potem ~~pozicija lica~~ po želji novo vozlišče narišemo v notranjosti zunanjega lica in ga povežemo z vsemi drugimi vozlišči tako, da se preseki ne sekajo. $\Rightarrow G'$ je ravninski

($\Leftarrow$) Naj bo G' ravninski. Narišemo ga v ravnino tako, da je novo vozlišče v' na robu zunanjega lica.



V grafu $G = G' - v'$ so vse vozlišča na robu zunanjega lica $\Rightarrow G$ je zunanje ravninski.

(b) Naj bo $G' = G * v'$ (dodamo eno vozlišče v' in ga povežemo z vsemi vozlišči v G)

po točki (a) je G' ravninski.

$$\text{Zato velja } \underbrace{|E(G')|}_{m+n} \leq 3 \underbrace{|V(G')|}_{n+1} - 6$$

$$\text{Torej: } m+n \leq 3(n+1) - 6 = 3n - 3$$

$$\Rightarrow \underline{m \leq 2n - 3}$$

(c) G 4-regularen graf z n vozlišči in m povezavami.

Iz leme o robovanju sledi: $2m = 4n$

$$\text{Oziroma } m = 2n$$

Če bi bil G zunanje ravninski: $\underbrace{m}_{2n} \leq 2n - 3 \rightarrow \text{kontr.}$

4. (10+12+12=34 točk) Dana je grupa D_{12} .

(a) Za vsakega od možnih redov poiščite po en element grupe D_{12} tega reda.

(b) Za vsak izomorfnostni razred podgrup grupe D_{12} do reda 6 poiščite po enega predstavnika.

(c) Ali je grupa D_{12} izomorfna grupi $D_4 \times C_3$?

a) $|D_{12}| = 24$ $D_{12} = \langle \rho, \tau; \rho^{12} = \tau^2 = id, \rho\tau = \tau\rho^{-1} \rangle$
 $= \langle \rho, \rho^2, \dots, \rho^{12} = id, \tau\rho, \tau\rho^2, \dots, \tau\rho^{11}, \tau \rangle$

Vemo: $a \in D_{12}$: $red(a) \mid |D_{12}| = 24$

red	1	2	3	4	6	8	12	24
element	id	ρ^6	ρ^4	ρ^3	ρ^2	//	ρ	//

τ
 $\tau\rho^i$

↑ element reda 24
 bi obstajal, če
 bi bila D_{12} ciklična,
 po mi

$red(\rho) = 12$

$red(\rho^i) = \frac{12}{gcd(12, i)}$

Elemento reda ρ mi, saj
 imo $\tau\rho^i$ red 2,

ρ^i po red $\frac{12}{gcd(12, i)} \neq \rho$

b) moč 1: $\{id\}$

moč 2: $\{id, \tau\}$ (generirano s katerikoli elementom reda 2)

moč 3: $\{id, \rho^4, \rho^8\}$ (generirano z el. reda 3)

moč 4: — ciklično — generirano z el. reda 4

↑
 2 neizomorfni $\{id, \rho^3, \rho^6, \rho^9\}$

— izomorfne $\mathbb{Z}_2 \times \mathbb{Z}_2$: vsebuje 3 el. reda 2, npr.

$\{id, \rho^6, \tau, \tau\rho^6\}$:

do je vsa podgrupe,
 vidimo iz Cayleyjeve
 tabele

	id	ρ^6	τ	$\tau\rho^6$
id	id	ρ^6	τ	$\tau\rho^6$
ρ^6	ρ^6	id	$\tau\rho^6$	τ
τ	τ	$\tau\rho^6$	id	ρ^6
$\tau\rho^6$	$\tau\rho^6$	τ	ρ^6	id

moč 6: — ciklično — generirano z el. reda 6

↑
 2 neizomorfni $\{id, \rho^2, \rho^4, \rho^6, \rho^8, \rho^{10}\}$

- dieklske

$$\{id, f^4, f^8, \tau, \tau f^4, \tau f^8\}$$

→ ni izomorfne
presjarki, saj ni
ciklične - ne
vključuje elementov
reda 6

do je res podgrupa (opravičeno)

Je notranja - zadošča za klenične punde)

preverimo s Cayleyjevom tabelo

	id	f^4	f^8	τ	τf^4	τf^8
id	id	f^4	f^8	τ	τf^4	τf^8
f^4	f^4	f^8	id	τf^8	τ	τf^4
f^8	f^8	id	f^4	τf^4	τ^8	τ
τ	τ	τf^4	τf^8	id	f^4	f^8
τf^4	τf^4	τf^8	τ	f^8	id	f^4
τf^8	τf^8	τ	τf^4	f^4	f^8	id

$$c) D_4 = \{id, f^1, f^{12}, f^{13}, \tau, \tau f^1, \tau f^{12}, \tau f^{13}\}$$

$$C_3 = \{1, a, a^2\}$$

$$D_4 \times C_3 = \{(\tau^k f^{1i}, a^j) \mid i \in \{0, 1, 2\}, k \in \{0, 1\}, j \in \{0, 1, 2\}\}$$

Grupi $D_4 \times C_3$ in D_{12} nista izomorfni.

Grupi D_{12} ima 13 elementov reda 2. To so:

$$\tau, \tau f^1, \dots, \tau f^{11}, f^6$$

Grupi $D_4 \times C_3$ ima 5 elementov reda 2:

$$D_4 \text{ ima 5 el. reda 2: } \tau, \tau f^1, \tau f^{12}, \tau f^{13}, f^{12}$$

$$C_3 \text{ nima el. reda 2}$$

→ $D_4 \times C_3$ ima 5 el. reda 2. To so $(\tau, 1), (\tau f^1, 1), (\tau f^{12}, 1), (\tau f^{13}, 1)$
in $(f^{12}, 1)$. Redi se ne ujamejo ⇒ grupi nista izom.