Odgovori na vprašanja za teoretični del izpita DS2 IŠRM 2023/24

Anton Luka Šijanec

28. junij 2024

Povzetek

Vprašanja je zbral profesor Sandi Klavžar. Odgovore sem sestavil po svojih zapiskih z njegovih predavanj in drugih virih.

Kazalo

1 Slog

- Z $M_{m,n}\mathbb{F}$ označim množico matrik z m vrsticami in n stolpci nad poljem $\mathbb{F}$.
- Znak za množenje ali dvojiški operator v grupi izpuščam. V bigrupoidih izpuščen operator pomeni množenje (drugo operacijo).

2 Vprašanja in odgovori

2.1 Kaj je stopnja vozlišča grafa in kaj pravi lema o rokovanju? Kako dokažemo to lemo?

Naj bo G graf.

Definicija. Stopnja vozlišča grafa $\deg v$ za $v \in VG$[1] predstavlja število povezav, ki imajo to vozlišče kot krajišče. $\deg v = |\{e \in EG; v \in e\}|$[2][3].

Definicija. Incidenčna matrika BG za $VG = \{v_1, \ldots, v_n\}$, $EG = \{e_1, \ldots, e_n\}$ je široka m in visoka n in velja $BG_{ij} = \begin{cases} 1 & ; v_i \in e_i \\ 0 & ; \text{sicer} \end{cases}$.

Lema. *Lema o rokovanju pravi, da je dvakratnik števila povezav enak vsoti vseh stopenj vozlišč v grafu*[4]*, torej*

$$\sum_{v \in VG} \deg v = 2\,|EG|\,.$$

Pripomba. Posledica leme o rokovanju je, da je v vsakem grafu sodo vozlišč lihe stopnje, saj je vsota soda.

Dokaz. Če po vozliščih preštevamo povezave, ki se stikajo vozlišča, bi vsako povezavo šteli dvakrat; vsakič za eno njeno krajišče. ZDB V vsakem stolpcu incidenčne matrike sta natanko dve enici. Torej je enic $2\,|EG|$. V vsaki vrstici incidenčne matrike je toliko enic, kolikor je stopnja $i-$tega vozlišča, torej je enic $\sum_{v \in VG} \deg v$. □

2.2 Pojasnite sprehod, sklenjen sprehod, pot v grafu, cikel v grafu. Pokažite, da vsak graf, ki vsebuje sklenjen sprehod lihe dolžine, vsebuje tudi cikel lihe dolžine.

Naj bo $G = (VG, EG)$.

Definicija. Sprehod v G je zaporedje vozlišč $v_0, \ldots, v_k$, $k \geq 0$, tako da je $\forall i \in \{1..k\} : v_i v_{i+1} \in EG$[5]. Dolžina

[1] Ko eniški operator zahteva en operand, izpustim oklepaje. Primer: $\sin x$, VG, χG, $M_{2,2}\mathbb{R}$.

[2] Povezava v grafu je množica natanko dveh vozlišč, toda oklepaje in vejico izpuščam. Za $u, v \in VG$ pišem $uv \in EG$. Na $e \in EG$ je torej veljavno gledati kot na množico, zato je $v \in e$ smiseln izraz.

[3] Zapis množic: $\{e \in A; Pe\}$ pomeni vse take elemente A, za katere velja predikat P. Ta predikat je običajno izraz.

[4] Ko je omenjen graf, je običajno mišljen neusmerjen končen graf.

[5] S $\{k..n\}$ označujem množico celih števil od vključno k do vključno n, kot to naredi `bash`. Nekateri bi $\{1..n\}$ označili z $[n]$.

sprehoda je število prehojenih povezav. Sprehod je **sklenjen**, če $v_0 = v_k$. Sprehod je **enostaven**, če so vsa vozlišča medsebojno različna, z izjemo v_0 sme biti v_k.

Trditev. Če v grafu $\exists$ sprehod med dvema vozliščema, med njima obstaja tudi enostaven sprehod.

Dokaz. Naj bo Q sprehod med u in v. Če je enostaven, je najden, sicer se ponovita vsaj dve vozlišči in je Q oblike $u, \ldots, x, \ldots, x, \ldots, v$. Sprehodu priredimo Q', ki odstrani pot od prvega do zadnjega podvojenega vozlišča x, torej je Q' oblike $u, \ldots, x, \ldots, v$ (pravzaprav smo odstranili cikel iz poti). Če je Q' enostaven, je iskani, sicer postopek ponovimo in v končno korakih se postopek ustavi, saj na vsakem koraku za vsaj 2 zmanjšamo dolžino sicer končno dolgega sprehoda. □

Definicija. Pot v grafu je podgraf, ki je enostaven sprehod med dvema vozliščema in je graf Pot (P_n).

Pripomba. Ko govorimo o različnosti/enakosti poti, mislimo različnost/enakost poti kot podgraf. Poti sta torej enaki natanko tedaj, ko sta zaporedji (ne množici) vozlišč poti enaki.

Definicija. Cikel v grafu je podgraf, ki je enostaven sklenjen sprehod dolžine vsaj 3.

Trditev. Če med dvema vozliščema v grafu $\exists$ dve različni poti, potem graf premore cikel.

Dokaz. Naj bosta P in P' dve različni poti od u do v. Naj bo x zadnje (če gledamo usmerjeno $u, v-$pot) vozlišče, ki je skupno P in P'. x je lahko u. Naj bo g prvo naslednje vozlišče za x, ki je na P in P'. Unija podpoti P od x do y in podpoti P' od x do y določa iskani cikel v grafu. □

Trditev. Če graf premore sklenjen sprehod lihe dolžine, potem premore cikel lihe dolžine.

Dokaz. Indukcija po dolžini sprehoda. Naj bo m dolžina sprehoda.

Baza: $m = 3$, najmanjši sklenjen lihi sprehod je cikel dolžine 3, $m = 4$, drugi najmanjši sklenjen lihi sprehod je cikel dolžine 4.

Korak: Naj bo Q poljuben sklenjen sprehod dolžine $m \geq 5$. Če je Q enostaven, je cikel po definiciji, sicer se vsaj eno vozlišče na sprehodu vsaj ponovi: $u, x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, v$ in velja $x_i = x_j$. Poglejmo sprehoda $Q' = x_i, \ldots, x_j = x_i$ in $Q'' = u, x_1, \ldots, x_i, x_{j+1}, \ldots, x_m = u$. Q' in Q'' sta sklenjena sprehoda z dolžinama m' in m'' in velja $m = m' + m''$. Ker je m lih, mora biti lih natanko en izmed m' in m''. BSŠ[6] m' lih in $m' < m$, zato po I. P. m' vsebuje lih cikel. □

2.3 Kaj so dvodelni grafi? Kako jih karakteriziramo? Kako dokažemo to karakterizacijo?

Definicija. G dvodelen[7] $\Leftrightarrow \exists A, B \subseteq VG \ni: A \cup B = VG, A \cap B = \emptyset \ni: \forall uv \in EG : u \in A, v \in B \vee v \in A, u \in B$. ZDB[8] obstaja razdelitev vozlišč na dve množici, da induciran podgraf posamezne množice ne vsebuje povezav. S $K_{m,n}$ označimo poln dvodelni graf $|A| = m$, $|B| = n$. Paru (A, B) pravimo dvodelna razdelitev.

Izrek. *G dvodelen $\Leftrightarrow$ G ne vsebuje lihih ciklov.*

Dokaz. G dvodelen $\Leftrightarrow$ vsaka komponenta G dvodelna, zato BSŠ G povezan. □

($\Rightarrow$) Očitno: Če G vsebuje lih cikel, zagotovo ni dvodelen, saj ne moremo razdeliti niti množice vozlišč cikla. S skico dokažemo, da sodi cikli so dvodelni, lihi pa niso (narišemo cikel kot pot v obliki skeletne formule nenasičenega acikličnega alkana in povežemo prvo in zadnje vozlišče).

($\Leftarrow$) G je po predpostavki brez lihih ciklov ****. Izberimo poljubno $x_0 \in VG$. Naj bo $A = \{u \in VG; d_G(u, x_0) \text{ sod}\}, B = \{u \in VG; d_G(u, x_0) \text{ lih}\}$. x_0 je torej v A, saj je $d_G(x_0, x_0) = 0$. Trdimo, da je (A, B) dvodelna razdelitev G. Razdelitev je, ker je $A \cup B = \emptyset$ in $A \cup B = VG$. Za dvodelnost pa mora veljati $\forall X \in \{A, B\} : \forall u, v \in X : uv \notin EG$. Preverimo za splošen fiksen $X \in \{A, B\}$: Naj bosta $u, v \in X$, BSŠ $d_G(x_0, u) > d_G(x_0, v)$ *. Ločimo dva primera:

[6] Brez Škode za Splošnost trdimo, da

[7] Pomožni glagol biti med osebkom in povedkovnikom izpuščam. „G dvodelen“ namesto „G je dvodelen“.

[8] Z Drugimi Besedami:

$d_G(x_0,u) \neq d_G(x_0,v)$: Vsled iste parnosti velja $|d_G(x_0,u) - d_G(x_0,v)| \geq 2$ ***. PDDRAA[9] $uv \in EG$, tedaj se $d_G(x_0,u)$ in $d_G(x_0,v)$ razlikujeta za največ 1 in velja $d_G(x_0,u) \leq d_G(x_0,v)+1$ **. Iz * in ** sledi $d_G(x_0,u) - d_G(x_0,v) = 1$, kar je v $\rightarrow\!\!\!\prec\!\!\!\leftarrow$ s trditvijo ***.

$d_G(x_0,u) = d_G(x_0,v)$: Naj bo P_x najkrajša $x_0,x-$pot. PDDRAA $uv \in EG$, tedaj $P_u = \{...P_v, v\}$[10], torej $|P_u| = 1 + |P_v|$. Cikel, ki ga tvorijo P_u, P_v in povezava uv, je torej dolžine $2|P_v|+1$, kar je liho število, kar je v $\rightarrow\!\!\!\prec\!\!\!\leftarrow$ s trditvijo ****.

2.4 Kaj je homomorfizem grafov, izomorfizem grafov in avtomorfizem grafa? Kaj je to $\mathrm{Aut}(G)$? Kakšno algebrsko strukturo ima?

Naj bosta G in H grafa.

Definicija. Preslikava $f : VG \to VH$ je hmφ[11] grafov G in $H \Leftrightarrow \forall u,v \in VG : uv \in EG \Rightarrow fufv \in EH$, ZDB če slika povezave v povezave.

Pripomba. Če je f hmφ,porodi preslikavo $f' : EG \to EH$.

Zgled. $f : VK_{n,m} \to VK_2$ s predpisom $fx = \begin{cases} u & ; x \in A \\ v & ; x \in B \end{cases}$ je hmφ. K_2 je homomorfna slika vsakega dvodelnega grafa.

Definicija. Če je hmφ surjektiven po povezavah in vozliščih, je epimorfizem. Če je injektiven na vozliščih (in posledično na povezavah), je monomorfizem ali vložitev. Vložitev je izometrična, če $\forall u,v \in VG : d_G(u,v) = d_H(fu,fv)$ ZDB ohranja razdalje.

Trditev. Če sta $f : VG \to VH$ in $g : VH \to VK$ hmφ, je $g \circ f : VG \to VK$ spet hmφ.

Definicija. Če je $f : VG \to VH$ bijekcija, hmφ in f^{-1} hmφ (ZDB slika nepovezave v nepovezave), je f imφ[12] grafov G in H. ZDB $f : VG \to VH$ im$\varphi \Leftrightarrow f$ bijekcija $\wedge \forall u,v \in VG : uv \in EG \Leftrightarrow fufv \in EH$. Če $\exists$ imφ grafov G in H, pravimo, da sta G in H izomorfna in pišemo $G \cong H$.

Trditev. $\cong$ je na $\mathcal{G}$[13] ekvivalenčna (refleksivna, simetrična, tranzitivna).

Definicija. imφ $G \to G$ je amφ[14]. Vse amφ grafa G združimo v množico in jo opremimo z operacijo komponiranja. Dobimo „grupo avtomorfizmov grafa G“, ki jo označimo z $\mathrm{Aut}\, G$.

Zgled. $\mathrm{Aut}\, C_4 = (\{id, (2,4), (12)(34), (1234), (13), (13)(24), (1423), (4321)\}, \circ)$, $\mathrm{Aut}\, K_n = (S_n, \circ)$ za S_n množica vseh permutacij n elementov,$\mathrm{Aut}\, P_n = (\{id, f(i) = n-i-1\}, \circ)$

Dejstvo. *Za vsako končno grupo X $\exists$ graf $G \ni$: $\mathrm{Aut}\, G = X$. Algebra $\subseteq$ Diskretne strukture. Dokaz na magisteriju.*

2.5 Kaj pomeni, da je graf H minor grafa G? Kdaj sta dva grafa homeomorfna? Pojasni operacijo kartezičnega produkta grafov.

Definicija. Odstranjevanje vozlišč: za neko $S \subseteq VG$ je $G - S$ graf, ki ga dobimo, ko iz G odstranimo vozlišča in vozliščem pripadajoče povezave iz S. Za $S = \{u\}$ pišemo tudi $G - u$. **Odstranjevanje povezav**: za neko $F \subseteq EG$ je $G - F$ graf, ki ga dobimo, ko iz G odstranimo povezave iz F. Za $S = \{e\}$ pišemo tudi $G - e$. **Skrčitev povezave**: za $e = \{u,v\} \in EG$ je G/e graf, ki ga dobimo tako, da identificiramo u in v in odstranimo morebitne vzporedne povezave, s čimer odstranimo tudi zanko $\{u, u = v\}$. $G/e_1/e_2/\ldots/e_n$ označimo z $G/\{e_1, e_2, \ldots, e_n\}$.

Definicija. H minor $G \Leftrightarrow H$ dobimo iz G z nekim zaporedjem operacij, kjer so dovoljene operacije odstranjevanje vozlišča, odstranjevanje povezave in skrčitev povezave. Ekvivalentno je H minor G, če ga lahko dobimo iz nekega podgrafa G, ki mu skrčimo poljubno povezav.

[9] Pa Denimo Da sledeča trditev ne drži (Reductio Ad Absurdum)

[10] Prefiksni razširitveni operator ... razširi množico oziroma v tem primeru zaporedje v seznam elementov. S tem lahko množico uporabimo kot seznam. Povzemam operator ... iz javascripta.

[11] homomorfizem

[12] izomorfizem

[13] množica vseh grafov

[14] avtomorfizem

Definicija. Subdivizija povezav: $G \to G^+e$ za $e \in EG$: $VG^+e = VG \cup \{x_e\}$, $EG^+e = EG \setminus e \cup \{x_eu, x_ev\}$. Graf H je subdivizija $G \Leftrightarrow H$ dobimo iz G z zaporedjem subdivizij povezav G ZDB povezave v G zamenjamo s poljubno dolčimi potmi. Relacija je refleksivna (G subdivizija G).

Definicija. Glajenje vozlišča u stopnje 2: (obratna operacija od subdivizije) $G^-u = (VG \setminus u, (EG \setminus \{e, f\}) \cup \{\{v, w\}\})$, kjer sta e in f povezavi, ki vsebujeta u, v in w pa njuni drugi krajišči (tisti krajišči, ki nista u).

Definicija. Grafa sta homeomorfna, če sta izomorfna po gladitvi vseh vozlišč stopnje 2.

Definicija. Naj bosta G, H grafa. Kartezični produkt grafov G in H označimo z $G\Box H$: $V(G\Box H) = VG \times VH, E(G\Box H) = \{(g,h)(g',h'); g = g' \wedge hh' \in EH \vee h = h' \wedge gg' \in EG\}$.

Pripomba. $(\mathcal{G}, \Box)$ je monoid, kajti K_1 je enota, operacija je komutativna in notranja.

Zgled. $K_2\Box K_2 \cong C_4$

2.6 Kaj so to prerezna vozlišča in prerezne povezave grafa? Kdaj je graf $k-$povezan in kaj je to povezanost grafa?

Naj bo G graf z m vozlišči.

Definicija. $u, v \in VG$ sta v isti povezani komponenti, če v G obstaja sprehod med njima. Število komponent G označimo z ΩG. G povezan $\Leftrightarrow \Omega G = 1$.

Pripomba. Biti v isti komponenti je ekvivalenčna relacija (refleksivna, simetrična in tranzitivna).

Definicija. $x \in VG$ prerezno $\Leftrightarrow \Omega(G - x) > \Omega G$. $e \in EG$ prerezna $\sim e$ most $\Leftrightarrow \Omega(G - e) > \Omega G$. $X \subseteq VG$ je prerezna množica $\Leftrightarrow \Omega(G - X) > \Omega G$. $X \subseteq EG$ je prerezna množica povezav $\Leftrightarrow \Omega(G - X) > \Omega G$.

Definicija. Povezan graf G je $k-$povezan $\Leftrightarrow |VG| \geq k + 1 \wedge \forall X$ prerezna $\subseteq VG : |X| >= k$ prerezna. ZDB ima vsaj $k + 1$ vozlišč in **ne** vsebuje prerezne množice moči manjše od k. Povezanost grafa $G \sim \kappa G$ je največji $k \in \mathbb{N}$, za katerega je G $k-$povezan ZDB najmanjše število vozlišč, ki jih moramo odstraniti iz grafa, da graf ne bo več povezan.

Pripomba. $\kappa G = k \Rightarrow G$ nima prerezne množice moči $< k$.

Zgled. $\kappa K_n = n - 1$, $\kappa P_n = 1$, $\kappa C_n = 2$, $\kappa K_{m,n} = \min\{n, m\}$, $\kappa Q_n = n$, $\kappa G \leq \delta G$[15]

2.7 Pojasnite Whitney-ev izrek, ki katekterizira $2-$povezane grafe. Skicirajte dokaz tega izreka. Zapišite Mengerjev izrek.

Definicija. Poti $[p_1, p_2, \ldots, p_{n-1}, p]$ in $[r_1, r_2, \ldots, r_{m-1}, r_m]$ sta notranje disjunktni, če sta disjunktni množici njunih vozlišč izvzemši prvo in zadnje vozlišče.

Izrek. *Graf G, $|VG| \geq 2$, je $2-$povezan $\Leftrightarrow \forall u, v \in VG \exists$ notranje disjunktni $u, v-$poti.*

Dokaz. Dokazujemo ekvivalenco:

($\Leftarrow$) Po predpostavki za poljubna u, v obstajata dve notranje disjunktni $u, v-$poti. Dokazujemo, da je G $2-$povezan $\Leftrightarrow$ nima prereznega vozlišča $\Leftrightarrow$ ne obstaja prerezna množica, ki je singleton[16]. Dokažimo, da poljubno $x \in VG$ ni prerezno, torej da po odstranitvi tega vozlišča še vedno obstaja povezava med poljubnima $u, v \in V(G - x)$. Ločimo 3 primere: x je na prvi $u, v-$poti, x je na drugi $u, v-$poti, x ni na nobeni izmed $u, v-$poti. V vsakem primeru sta u, v v $G - x$ še vedno v isti povezani komponenti.

($\Rightarrow$) Po predpostavki je G $2-$povezan. Vzemimo poljubna $u, v \in VG$. Indukcija po $d_G(u, v)$:

Baza: $d_G(u, v) = 1$ (sosednji vozlišči) $G - e$ je povezan, sicer je RAAPDD uv most, kar bi bilo v $\rightarrow\!\!\!\!\!\!\leftarrow$ s predpostavko, ker bi bil en izmed u, v prerezno, saj ima G vsaj 3 vozlišča in ima vsaj eden izmed u, v še enega soseda. Sedaj vemo, da $\exists u, v-$pot, ki ni uv. Imamo torej dve notranje disjunktni $u, v-$poti: e in tisto drugo.

Korak: $d_G(u, v) = k \geq 2$. Naj bo P najkrajša $u, v-$pot. Predzadnje vozlišče na njej (tik pred v) naj bo w. $d_G(u, w) = k - 1$ in po I. P. obstajata dve notranje disjunktni $u, w-$poti R in S. Ločimo primera:

[15] δG je minimalna stopnja vozlišča v grafu G

[16] množica moči ena

$v \in VR \cup VS$ Tedaj je v na ciklu, ki ga tvorita poti R in S (je na eni izmed poti). Zato obstajata dve notranje disjunktni $u, v-$poti; ena v eno smer po ciklu, druga v drugo.

$v \notin VR \cup VS$ Tedaj v ni na tem ciklu, vendar je sosed w, ki je na ciklu. $G - w$ mora biti povezan, saj smo odstranili le eno vozlišče, torej $\exists u, v-$pot T. Ločimo primera:

$T \cap (VS \cup VR) = \{u\}$ Našli smo dve notranje disjunktni poti v G: T in $[\ldots R, v]$ (R in wv povezava).

$|T \cap (VS \cup VR)| \geq 2$ Naj bo x zadnje (kjer je v konec poti) vozlišče na T, ki je na $R \cup S$. BSŠ $x \in VS$. $x \neq w$ po konstrukciji T. Dve poti: po S do x in nato po T do v ter $[\ldots R, v]$ (R in wv povezava).

□

Izrek. *Menger (posplošitev Whitneya): naj bo G graf z vsak $k+1$ vozlišči. Tedaj je G $k-$povezan $\Leftrightarrow \forall u, v \in VG \exists k$ paroma notranje disjunktnih $u, v-$poti.*

Definicija. Graf je $k-$ povezan po povezavah, če $\nexists$ prerezna množica povezav moči $< k$. Povezanost grafa G po povezavah ($\kappa' G$) je največji k, da je G $k-$povezan po povezavah.

Izrek. *Menger': G je $k-$povezan po povezavah $\Leftrightarrow \forall u, v \in VG \exists k$ po povezavah notranje disjunktnih $u, v-$poti.*

Izrek. $\forall G \in \mathcal{G} : \kappa G \leq \kappa' G$ *in* $\kappa' G \leq \delta G$.

Dokaze zadnjih treh izrekov najdete na magisteriju.

2.8 Kaj je drevo in kaj je gozd? Katere katekterizacije dreves poznate?

Definicija. Gozd je graf brez ciklov. Drevo je povezan gozd. List je vozlišče stopnje 1.

Lema 1. *Vsako drevo z vsaj dvema vozliščema premore list.*

Dokaz. Naj bo T drevo, $v \in VT$ poljubno. $|VT| \geq 2 \wedge T$ povezan $\Rightarrow v$ ima soseda v_1. Če je v_1 edini sosed v, je v list, sicer je tudi $v_2 \neq v_1$ sosed v. Če je v edini sosed v_2, je v_2 list, sicer je tudi v_3 sosed v. Postopek ponavljamo, dokler ne najdemo lista. V grafu ni ciklov in graf je končen, zato se postopek ustavi. □

Lema 2. T *drevo* $\Rightarrow |ET| = |VT| - 1$

Dokaz. z indukcijo po številu vozlišč:
Baza: $|VT = 1|$, $|EG| = 0$ (izolirano vozlišče je drevo)
Korak: T poljubno drevo $|VG| \geq 2$. $v \in VT$ naj bo list v T po lemi 1. Po I. P. je $|E(T - v)| = |V(T - v)| - 1$, po konstrukciji $T - v$ pa je $|E(T - v)| = |ET| - 1$, $|V(T - v)| = |VT| - 1$, torej $|ET| = |VT| - 1$. □

Lema 3. G *povezan,* $e \in EG$ *leži na ciklu* $\Rightarrow G - e$ *povezan.*

Dokaz. Trdimo, da v $G - e \exists u, v-$pot. Ker je G povezan, $\exists u, v-$pot P v G. Če $e \notin P$, ta pot obstaja tudi v $G - e$. Če $e \in P$, očitno dobimo pot tako, da e v P nadomestimo s preostankom cikla, na katerem leži e v G. □

Lema 4. G *povezan* $\Rightarrow |EG| \geq |VG| - 1$.

Dokaz. Če je G drevo, velja enakost po lemi 2, sicer G premore cikel. Po lemi 3 $\exists e \in EG \ni$: $G - e$ povezan. Odstranjevanje povezav iz ciklov ponavljamo, dokler ne dobimo drevesa T. Velja $VT = VG$ (*) in $|ET| < |EG|$ (**). Torej: $|VG| - 1 \overset{(*)}{=} |VT| - 1 \overset{\text{lema 2}}{=} |ET| \overset{(**)}{<} |EG|$. □

Izrek. *Karakterizacija dreves. NTSE za graf G:*

1. *G drevo*
2. *$\forall u, v \in VG \exists!$ $u, v-$pot ZDB za vsak par vozlišč obstaja enolična pot*
3. *G povezan $\wedge \forall e \in EG : e$ most*
4. *G povezan $\wedge |EG| = |VG| - 1$*

Dokaz. Dokazujemo ekvivalenco:

$(1 \Rightarrow 2)$ PDDRAA $\exists$ dve različni $u, v-$poti za neka $u, v \in VG$. Tedaj graf premore cikel $\Rightarrow$ ni gozd $\Rightarrow$ ni drevo $\rightarrow\!\leftarrow$. PDDRAA $\nexists$ $u, v-$pot za neka $u, v \in VG \Rightarrow \Omega G \neq 1 \Rightarrow$ ni drevo $\rightarrow\!\leftarrow$.

$(2 \Rightarrow 3)$ PDDRAA $\exists uv \in EG \ni$: ni most $\Rightarrow \exists u, v-$pot v $G - e \Rightarrow \exists$ dve različni $u, v-$poti v G (uv in tista v $G - e$) $\rightarrow\!\leftarrow$.

$(3 \Rightarrow 4)$ G povezan $\Rightarrow G$ povezan velja vedno. Dokažimo $|EG| = |VG| - 1$ z indukcijo po številu vozlišč:

Baza: V K_2 je edina povezava most in $|EK_2| = 2 - 1 = 1 = |VK_2|$

Korak: $e \in EG$ poljuben: $\Omega(G - e) = 2$, dve komponenti $G - e$ naj bosta G_1 in G_2. Slednja sta povezana in za njiju velja, da je vsaka povezava most in sta manjša grafa. Po I. P. velja $|EG_1| = |VG_1| - 1$ in $|EG_2| = |VG_2| - 1$. Velja $|EG| = |EG_1| + |EG_2| + 1 = |VG_1| - 1 + |VG_2| - 1 + 1 = |VG_1| + |VG_2| - 1 = |VG| - 1$.

$(4 \Rightarrow 2)$ PDDRAA G premore cikel $\stackrel{\text{lema 3}}{\Rightarrow}$ če mu odstranimo povezavo s cikla, bo ostal povezan. Obenem zaradi velja $|E(G - e)| = |V(G - e)| - 2$, kar je v $\rightarrow\!\leftarrow$ z lemo 4 (G povezan, toda ne velja implikacija).

□

2.9 Kaj je vpeto drevo grafa? Kateri grafi premorejo vpeta drevesa? Kako lahko rekurzivno določimo število vpetih dreves povezanega grafa?

Definicija. Podgraf H grafa G je vpet, če velja $VP = VG$. (Lahko pa ima ima G povezave, ki jih H nima).

Definicija. Vpeto drevo grafa G je vpet podgraf, ki je drevo.

Izrek. *G povezan $\Leftrightarrow$ G premore vpeto drevo.*

Dokaz. ($\Leftarrow$) očitno. ($\Rightarrow$): Če je G drevo, je sam sebi vpeto drevo, sicer vsebuje cikel in iterativno uporabljamo lemo 3, dokler ne konstruiramo vpetega drevesa. □

Definicija. τG naj bo število vpetih dreves grafa G.

Pripomba. T drevo $\Rightarrow \tau T = 1$, $\Omega G > 1 \Rightarrow \tau G = 0$, $\tau C_n = n$

Definicija. Z G/e označimo skrčitev povezave e v multigrafu[17] G. To je enako kot skrčitev povezave v grafu $(G \backslash e)$, le da ne odstranimo večkratnih vzporednih povezav.

Trditev. G povezan, $e \in EG \Rightarrow \tau G = \tau(G - e) + \tau(G/e)$

Dokaz. Naj bo T vpeto drevo v G. Naj bo $e \in EG$ poljuben fiksen. Vpetih dreves, za katere $e \notin T$, je $\tau(G - e)$. Vpetih dreves, za katere $e \in T$, je $\tau(G/e)$. □

Rekurzivno torej določamo število vpetih dreves grafa z zgornjo trditvijo tako, da izbiramo poljubne povezave in jih ožamo ter odstranjujemo in nato seštejemo τ teh dveh operacij.

2.10 Kaj je Laplaceova matrika multigrafa? Kaj pravi Kirchoffov izrek o številu vpetih dreves multigrafa?

Definicija. Laplaceova matrika LG je kvadratna matrika dimenzije n, katere vrstice in stolpci so indeksirani z vozlišči multigrafa G in velja

$$LG_{ij} = \begin{cases} \deg_G v & ; i = j \\ -(\text{število povezav med } v_i \text{ in } v_j) & ; i \neq j \end{cases}$$

Izrek. *Kirchoff: Če je G povezan multigraf, potem je $\tau G = \det(LG$ brez itega stolpca in ite vrstice$)$ za poljuben i. ZDB $\tau G = \det LG_{i,i}$.*

[17] V multigrafu se ista povezava lahko pojavi večkrat.

2.11 Kaj pomeni, da je graf Eulerjev? Kako karakteriziramo Eulerjeve grafe? Skicirajte dokaz slednjega rezultata.

Definicija. Sprehod v multigrafu je Eulerjev, če vsebuje vse povezave in sicer vsako zgolj enkrat. **Sklenjen** Eulerjev sprehod je Eulerjev obhod. Graf je Eulerjev, če premore Eulerjev obhod.

Izrek. *G Eulerjev $\Leftrightarrow \forall v \in VG : \deg_G v$ sod.*

Dokaz. ($\Rightarrow$) očitno. ($\Leftarrow$): $\forall v \in VG : \deg_G v$ sod $\Rightarrow G$ premore cikel. Indukcija po številu povezav:

Baza: Izolirano vozlišče, multigraf $VG = \{u, v\}, EG = \{uv, uv\}$ in C_3 so vsi Eulerjevi.

Korak: Naj bo $|VG| \geq 4$. G gotovo premore cikel C, ker je povezan in nima listov (ni drevo). Naj bo $H \coloneqq G - EC$. $\forall u \in VC : \deg_H u = \deg_G u - 2$, $\forall u \notin VC : \deg_H u = \deg_G u \Rightarrow \forall v \in H : \deg_H v$ sod $\Rightarrow$ vsaka komponenta H je Eulerjev graf po I. P., saj je manjši graf. G je tudi Eulerjev, obhodimo ga lahko po ciklu C; vsakič, ko naletimo na vozlišče, ki je del komponente H, jo obhodimo in nadaljujemo pot po ciklu. □

Fleuryjev algoritem sprejme graf in vrne obhod

1. Začnemo v poljubni povezavi
2. Ko povezavo prehodimo, jo izbrišemo
3. Postopek nadaljujemo in pri tem pazimo le na to, da gremo na most le v primeru, če ni druge možnosti.

Izrek. *Če je G Eulerjev graf, potem Fleuryjev algoritem vrne Eulerjev obhod.*

2.12 Kdaj je graf Hamiltonov? Navedite in pojasnite potrebni pogoj z razpadom grafa za obstoj Hamiltonovega cikla v grafu.

Definicija. Hamiltonov cikel v grafu je cikel, ki vsebuje vsa vozlišča grafa ZDB Hamiltonov cikel je vpet podgraf, ki je cikel. **Graf je Hamiltonov**, če premore Hamiltonov cikel. **Hamiltonova pot** v grafu je pot, ki vsebuje vsa vozlišča grafa ZDB vpet podgraf, ki je pot.

Izrek. *G Hamiltonov, $S \subseteq VG \Rightarrow \Omega(G - S) \leq |S|$. (potreben pogoj za obstoj Hamiltonovega cikla)*

Dokaz. Naj bo $VG = \{v_1, \ldots, v_n\}$ Hamiltonov. BSŠ naj bo $[v_1, \ldots, v_n]$ Hamiltonov cikel. Skica dokaza: Naj bosta $v_i, v_j \in S, i < j$. Tedaj $G - S$ razbije G na dva podgrafa: $K_1 \{v_{i+1}, \ldots, v_{j-1}\}$ in $K_2 = (VG \cap \{v_i, v_j\}) \cap K_1 = \{v_{j+1}, \ldots, v_n, v_1, \ldots, v_{i-1}\}$. Če $i = j - 1$, je ena podgraf prazen, če $n = 3$ prav tako. Podgrafa sta lahko povezana in tvorita skupno komponento, lahko pa nista in tvorita dve komponenti. Toda z odstranjevanjem $|S|$ vozlišč iz cikla lahko napravimo največ $|S|$ komponent. □

Pripomba. Izrek uporabimo v kontrapoziciji: $\exists S \subseteq VG \ni: \Omega(G - S) > |S| \Rightarrow G$ ni Hamiltonov.

Zgled. G vsebuje prerezno vozlišče $\Rightarrow G$ ni Hamiltonov.

Trditev. $K_{m,n}$ Hamiltonov $\Leftrightarrow m = n$.

Dokaz. ($\Rightarrow$) Uporabimo izrek o potrebnem pogoju. RAAPDD BSŠ $m > n$: $\Omega(G - n) = m$, kar vodi v $\rightarrow\!\!\!\!\leftarrow$. ($\Leftarrow$) Očitno lahko skiciramo Hamiltonov cikel. □

Trditev. G dvodelen z razdelitvijo (A, B), $|A| \neq |B| \Rightarrow G$ ni Hamiltonov.

2.13 Navedite Orejev zadostni pogoj za obstoj Hamiltonovega cikla v grafu. Skicirajte dokaz tega izreka.

Izrek. *Ore: G graf, $|VG| \geq 3$, $(\forall u, v \in VG : uv \notin EG \Rightarrow \deg u + \deg v \geq |VG|) \Rightarrow G$ Hamiltonov. ZDB če za vsak par nesosednjih vozlišč v grafu z vsaj tremi vozlišči velja $\deg u + \deg v \geq |VG|$, je graf Hamiltonov.*

Dokaz. Dokaz z metodo najmanjšega protiprimera. RAAPDD izrek ne velja. Tedaj $\exists G$, da predpostavka velja, zaključek pa ne. Med vsemi takimi grafi izberimo tiste z najmanj vozlišči, izmed njih pa enega izmed tistih, ki imajo največ povezav, in ga fiksiramo. Naj bo to graf G. Zanj velja:

- $\forall u, v \in VG : uv \notin EG \Rightarrow \deg u + \deg v \geq |VG|$

- G ni Hamiltonov $\Rightarrow$ G gotovo ni polni graf $\Rightarrow \exists u, v \in VG \ni: uv \notin EG$. Naj bo H graf, da velja $VH \coloneqq VG$ in $EH \coloneqq EG \cup uv$. Zanj še vedno velja prejšnja točka, zaradi izbire G (največ povezav) pa ni več protiprimer za izrek, zato je Hamiltonov. Vsak Hamiltonov cikel v H vsebuje uv, sicer bi obstajal že v G. Vseeno pa G premore Hamiltonovo pot, saj smo do cikla namreč dodali le eno povezavo. Naj bo $[u = v_1, v_2, \ldots, v_{n-1}, v_n = v]$ Hamiltonov cikel v H. Vpeljimo množici $S = \{v_i, uv_{i+1} \in EG\}$ (ZDB predhodniki sosedov u na Hamiltonovi poti v G) in $T = \{v_i, vv_i \in EG\}$ (ZDB sosedje v na Hamiltonovi poti v G). Velja $|S \cup T| = |S| + |T| - |S \cap T|$, torej $|S \cup T| + |S \cup T| = |S| + |T| = \deg_G u + \deg_G v \overset{\text{predpostavka}}{\geq} |VG| = n$. Toda ker je $|S \cup T| = |VG|$, $|S \cap T| \neq \emptyset$, torej ima v soseda iz S (recimo mu v_i), torej lahko konstruiramo Hamiltonov cikel v G: $[u = v_1, v_2, \ldots, v_i, v_n = v, v_{n-1}, \ldots, v_{i+1}, v_1 = u]$ (v_{i+1} je namreč po konstrukciji S sosed u), kar vodi v $\rightarrow\!\!\!\!\!\!\leftarrow$.

□

2.14 Kaj so ravninski grafi? Kaj so lica ravninske vložitve grafa in čemu je enaka vsota dolžin vseh lic ravninske vložitve grafa? Kako lahko omejimo število povezav ravninskega grafa s pomočjo njegove ožine?

Definicija. Graf G ravninski $\Leftrightarrow$ lahko ga narišemo v ravnino tako, da se nobeni povezavi ne križata. Ravninski graf skupaj z ustrezno risbo (vložitvijo) je graf, vložen v ravnino.

Zgled. $K_{2,3}$ je ravninski, $K_{3,3}$ ni ravninski.

Izrek. *Jordan: Sklenjena enostavna krivulja (t. j. taka, ki same sebe ne križa) v ravnini razdeli ravnino v notranjost, zunanjost in krivuljo samo.*

Definicija. Naj bo G ravninski, vložen v ravnino. Sklenjena območja v ravnini, dobljena tako, da iz risbe odstranimo točke, ki ustrezajo vozliščem in povezavam, imenujemo **lica vložitve**. S FG označimo množico lič vložitve. Seveda je tudi zunanje/neomejeno območje lice.

Zgled. $|FQ_3| = 6$

Pripomba. G lahko vložimo v ravnino $\Leftrightarrow$ lahko ga vložimo na sfero.

Definicija. Dolžina lica F (ℓF),je število povezav, ki jih prehodimo, ko obhodimo lice.

Pripomba. Vsako drevo je ravninski graf. Ima eno lice, katerega dolžina je $2\,|ET|$.

Definicija. Ožina grafa G, gG, je dolžina najkrajšega cikla v G. Če je G gozd, je $gG \coloneqq \infty$.

Trditev. Če je G ravninsli graf, vložen v ravnino, velja

$$\sum_{F \in FG} \ell F = 2\,|EG|$$

Naj G premore cikel. Naj bo $F \in FG$. $\ell F \geq gG$. $2\,|EG| = \sum_{F \in FG} \ell F \geq \sum_{F \in FG} gG = gG\,|FG|$
Posledično: Če je G ravninski graf z vsaj enim ciklom in je vložen v ravnino, je $|EG| \geq \frac{gG}{2}\,|FG|(*)$.

2.15 Kaj pravi Eulerjeva formula za ravninske grafe? Skicirajte njen dokaz. Katere posledice Eulerjeve formule poznate?

Izrek. *Eulerjeva formula: Če je G ravninski vložen v ravnino, velja $|VG| - |EG| + |FG| = 1 + \Omega G$.*

Zgled. Graf „tri hiše“: $|VG| = 15$, $|EG| = 18$, $|FG| = 7$, $\Omega G = 3$, $15 + 16 + 7 = 1 + 3$

Dokaz. Dokažimo najprej za povezan multigraf G. Dokazujemo $|VG| - |EG| + |FG| = 2$. Indukcija po številu vozlišč:

Baza: Izolirano vozlišče: $|VG| = 1$, $|EG| = 0 + z$, $|FG| = 1 + z$, kjer je z število zank (za navaden graf $z = 0$). Drži.

Korak: Naj bo $e \in EG$ poljubna. Skrčimo jo (kot v multigrafu). $|V\,(G/e)| = |VG| - 1$, $|E\,(G/e)| = |EG| - 1$, $|F\,(G/e)| = |FE|$. Velja $|VG| - |EG| + |FG| = 2$, saj po I. P. velja$|V\,(G/e)| + 1 - |E\,(G/e)| - 1 + |F\,(G/e)| = 2$.

Sedaj dokažimo še za nepovezan multigraf G z ΩG komponentami. Grafu lahko dodamo $\Omega G - 1$ povezav, da ga povežemo, s čimer ne spremenimo niti $|FG|$ niti $|VG|$. Če je E množica povezav, ki jo moramo dodati, velja $|VG| - |EG \cup E| + |FG| = 2 = |VG| - |EG| - \Omega G + 1 + |FG| \Rightarrow |VG| - |EG| + |FG| = 2 - 1 + \Omega G = 1 + \Omega G$. □

Izrek. *Za ravninski graf z vsaj tremi vozlišči velja* $|EG| \leq 3\,|VG| - 6$*, če je slednji brez trikotnikov, a ima cikel, pa celo* $|EG| \leq 2\,|VG| - 4$*.*

Dokaz. Dokažimo za povezan ravninski graf, sicer mu lahko samo dodamo povezave in ga povežemo. Ločimo primera: □

(G drevo) $|EG| = |VG| - 1$ (karakterizacija dreves) $\overset{?}{\leq} 3\,|VG| - 6$. Drži, kajti $|VG| \geq 3$.

(G premore cikel) Po Eulerjevi formuli velja

$$2 = |VG| - |EG| + |FG| \overset{(*)\text{ iz }2.14}{\leq} |VG| - |EG| + \frac{2\,|EG|}{gG}$$

$$2 \leq |VG| - |EG| + \frac{2\,|EG|}{gG}$$

$$2 - |VG| \leq |EG| \left(\frac{2}{gG} - 1\right) \qquad /^{-1}$$

$$|VG| - 2 \geq |EG| \left(1 - \frac{2}{gG}\right) = |EG| \left(\frac{gG - 2}{gG}\right)$$

$$(|VG| - 2)\,\frac{gG}{gG - 2} \geq |EG|$$

$\frac{gG}{gG-2}$ je največ 3 in to tedaj, ko graf premore trikotnik. Če za vse večje gG bo ta ulomek manjši, torej lahko levo stran omejimo navzdol: $3\,|VG| - 6 \geq (|VG| - 2)\,\frac{gG}{gG-2} \geq |EG|$

Če pa graf ne premore trikotnika, a ima cikel, pa je $\frac{gG}{gG-2} = 2$ in levo stran strožje omejimo navzgor in velja $2\,|VG| - 4 \geq |EG|$.

2.16 Kaj je kromatično število $\chi(G)$ grafa G? Pojasnite požrešni algoritem barvanja grafa. Kako lahko z njegovo pomočjo navzgor omejimo $\chi(G)$?

Definicija. $k-$barvanje grafa G je preslikava $C : VG \to \{1..k\}$, za katero velja $uv \in EG \Rightarrow Cu \neq Cv$. Kromatično število χG je najmanjši k, za katerega najdemo $k-$barvanje G. Za fiksen i je $\{u \in VG; Cu = i\}$ barvni razred, ki je neodvisna množica[18].

Zgled. $\chi K_n = n$, $\chi C_n = \begin{cases} 2 & ; n \text{ sod} \\ 3 & ; n \text{ lih} \end{cases}$, $\chi P_{5,2} = 3$.

Definicija. Klično število grafa G označimo z ωG. Velja $\omega G = |VH|$, kjer je H največji poln podgraf v G.

Pripomba. $\forall G \in \mathcal{G} : \chi G \geq \omega G$.

Definicija. Požrešni algoritem barvanja: V poljubnem vrstnem redu zaporedno barvamo vozlišča. Posameznemu vozlišču priredimo najnižjo barvo, ki še ni uporabljena na njegovih sosedih.

Dejstvo. *Vedno* $\exists$ *vrstni red barvanja, da požrešni algoritem vrne barvanje s* χG *barvami.*

Trditev. $\forall G \in \mathcal{G} : \chi G \leq \Delta G + 1$ ZDB χG je kvečjemu 1 večji od največje stopnje v grafu.

Dokaz. Naj bo $x_1, \ldots, x_n$ poljuben vrstni red vozlišč. Poženemo požrešni algoritem. Na poljubnem $i$tem koraku, ko barvamo x_i, je kvečjemu $\deg_G x_i$ barv, ki niso na razpolago, kar je $\leq \Delta G$. □

Trditev. G ni regularen $\Rightarrow \forall G \in \mathcal{G} : \chi G \leq \Delta G$

Dokaz. Naj bo x tisto vozlišče, ki največje stopnje (*). Vzamemo ga kot koren za BFS in z BFS vozlišča zmečemo v zaporedje a. Nato požrešno barvamo v obratni smeri, kot jo določa a. Na vsakem koraku, razen na korenu, bomo imeli soseda, ki še ni pobarvan, torej je kvečjemu $\deg_G x_i - 1$ barv, ki niso na razpolago, kar je $\leq \Delta G$. Na zadnjem koraku (koren) pa po predpostavki (*) na razpolago ni kvečjemu $\Delta G - 1$ barv. □

[18] Za neodvisno množico $S \subseteq VG$ velja $\forall u, v \in S : uv \notin EG$ ZDB je „brez povezav“. Glej vprašanje 2.18.

Izrek. *Brooks: G povezan, G niti poln niti lihi cikel* $\Rightarrow \chi G \leq \Delta G$.

Izrek. *Naj bo* $d_1 \geq d_2 \geq \cdots \geq d_n$ *zaporedje stopenj grafa G. Tedaj velja* $\chi G \leq 1 + \max_{i=1}^{n} (\min \{d_i, i-1\})$

Dokaz. Poženimo požrešni algoritem barvanja v padajočem zaporedju stopenj. Na $i$tem barvamo vozlišče stopnje d_i, zato imamo gotovo na voljo barvo iz $\{1..d_i+1\}$. Ker smo doslej pobarvali zgolj $i-1$ vozlišč, imamo gotovo na voljo barvo iz $\{1..i\}$. Algoritem pobarva vozlišče z barvo $\leq \min\{i, d_i+1\}$. Največja uporabljena barva k je $\leq \max_{i=1}^{n} \{\min\{d_i+1, i\}\}$. Torej $\chi G \leq 1 + \max_{i=1}^{n} (\min\{d_i, i-1\})$ (izven max smo prišteli 1, znotraj min smo od vseh elementov 1 odšteli). □

2.17 Kaj je kromatični indeks $\chi'(G)$ grafa G? Kaj pravi Vizingov izrek in kako na njegovi osnovi razdelimo vse grafe v dva razreda?

Definicija. $k-$barvanje povezav je preslikava $C : EG \to \{1..k\}$ $\ni$: $uv, uw \in EG \Rightarrow C(uv) \neq C(uw)$. ZDB povezavi s skupnim krajiščem dobita različni barvi. Kromatični indeks grafa G (oznaka $\chi' G$) je najmanjši k, za katerega $\exists k-$barvanje grafa G.

Zgled. $\chi' C_n = \begin{cases} 2 & ; n \text{ sod} \\ 3 & ; n \text{ lih} \end{cases}$

Izrek. *Vizing:* $\forall G \in \mathcal{G} : \Delta G \leq \chi' G \leq \Delta G + 1$.

Dokaz. Prvi neenačaj je očiten, drugega ne bomo dokazali. □

Definicija. Graf G je razreda I, če je $\chi' G = \Delta G$ oziroma razreda II, če je $\chi' G = \Delta G + 1$.

Zgled. C_{2n} so razreda I, C_{2n+1} so razreda II, K_3 je razreda II, K_4 je razreda I

2.18 Kaj je neodvisnostno število grafa? Zanj podajte spodnjo mejo in zgornjo mejo. Opišite algoritem za izračun neodvisnostnega števila drevesa.

Definicija. Če je G graf in $I \subseteq VG$, je I neodvisna $\Leftrightarrow \forall u, v \in I : uv \notin EG$ ZDB če nobeni dve vozlišči v I nista sosednji v G. Moč največje neodvisne množice v G je neodvisnostno število G, označeno z αG.

Zgled. $\alpha K_n = 1$, $\alpha C_n = \lfloor \frac{n}{2} \rfloor$, $\alpha P_{5,2} = 4$

Trditev. $\forall G \in \mathcal{G} : \alpha G \cdot \chi G \geq |VG|$

Dokaz. Naj bo $\chi G = k$ in $V_1, \ldots, V_k$ barvni razredi nekega fiksnega barvanja s k barvami. Slednji so neodvisne množice. $\forall i \in \{1..k\} : |V_i| \leq \alpha G \Rightarrow |VG| = \sum_{i=1}^{k} |V_i| \leq \sum_{i=1}^{k} \alpha G = \alpha G \cdot k = \alpha G \chi G$ □

Posledica. *Spodnja meja za neodvisnostno število* $\alpha G \geq \frac{|VG|}{\chi G}$.

Trditev. Zgornja meja za neodvisnostno število: $\alpha G \leq |VG| - \frac{|EG|}{\Delta G}$.

Dokaz. Naj bo I poljubna največja neodvisna množica v G, torej$|I| = \alpha G$. V $VG \setminus I$ je vozlišč $|VG| - \alpha G$. Ker vozlišča v I medsebojno niso povezana, $|EG| \leq (|VG| - \alpha G) \cdot \Delta G \Rightarrow |EG| \leq |VG|\Delta G - \alpha G \Delta G \Rightarrow \alpha G \Delta G \leq |VG|\Delta G - |EG| \Rightarrow \alpha G \leq |VG| - \frac{|EG|}{\Delta G}$. □

Zgled. $Q_d, d \geq 1$: Zgornja meja: $\alpha Q_d \leq |VQ_d| - \frac{|EQ_d|}{\Delta Q_d} = 2^d - \frac{d2^{d-1}}{d} = 2^d - 2^{d-1} = 2^{d-1}$, Spodnja meja: $\alpha Q_d \geq \frac{|VQ_d|}{\chi Q_d} = \frac{2^d}{2} = 2^{d-1}$, torej $\alpha Q_d = 2^{d-1}$.

Neodvisnostno število dreves Naj bo T drevo s poljubnim korenom $r \in VT$. Odslej na drevo glejmo T kot na drevo s korenom r. Za neodvisno množico S drevesa T in poljubno vozlišče $x \in VT$ velja: $x \in S \Rightarrow$ potomci (otroci) $x \notin S$. Če pa $x \notin S$, pa S sme vsebovati potomce x. Z Iv označimo velikost največje neodvisne množice s korenom v $v \in VT$.

Očitno velja $\alpha T = Ir$. Z rekurzivnim postopkom določimo αT na tak način:

$$\alpha T = Ir = \max\left\{1 + \sum_{v \in \text{vnuki/drugi potomci } r} Iv, \sum_{v \in \text{otroci/potomci } r} Iv\right\}$$

Formula je očitna. Na vsakem rekurzivnem koraku lahko bodisi v množico izberemo v in ne izberemo njegovih potomcev, bodisi izberemo potomce, njega pa ne. Z rekurzivnim algoritmom preverimo vse možnosti.

Zgled. αT_n, kjer je T_n polno dvojiško drevo globine $n \in \mathbb{N}_0$: Vpeljimo zaporedje $a_n = \alpha T_n$ in velja: $(a_n)_{n \in \mathbb{N}_0} = [1, 2, 5, 10, 21, 42, \dots]$.

Izrek. *$a_0 = 1$, $a_1 = 2$, za $n \geq 2$:* $a_n = \begin{cases} 2_{n-1} + 1 & ; n \text{ sod} \\ 2_{n-1} & ; n \text{ lih} \end{cases}$.

Dokaz. Z indukcijo. Baza sta a_0 in a_1. Indukcijska predpostavka je dana v izreku. ITD DOPIŠI DOKAZ. „DS2P FMF 2024-04-18“ stran 5. □

2.19 Kaj je dominacijsko število grafa? Zanj podajte spodnjo mejo in zgornjo mejo. Kakšna je zveza med dominacijskim številom grafa in njegovega vpetega podgrafa?

Naj bo G graf.

Definicija. Neodvisna množica G je maksimalna, če ni prava podmnožica kakšne neodvisne množice v G.

Definicija. $N_G(u) \coloneqq \{v; uv \in EG\}$ je soseščina vozlišča u (sosedje u v G). $N_G[u] \coloneqq N_G(u) \cup \{u\}$ je zaprta soseščina vozlišča u. $N_G[D] = \bigcup_{u \in D} N_G[u]$ je zaprta soseščina množice vozlišč D. $D \subseteq VG$ dominira $X \subseteq VG \Leftrightarrow X \subseteq N_G[D]$. Če D dominira VG, pravimo, da je D dominantna množica grafa G. ZDB D dominantna množica $G \Leftrightarrow \forall u \in VG : u \in D \vee \exists x \in D \ni: xu \in EG$ ZDB vsako vozlišče je v D ali pa ima soseda iz D. Moč najmanjše dominacijske množice za G je dominacijsko število grafa G, označeno z γG.

Pripomba. Vsaka maksimalna neodvisna množica grafa je njegova dominantna množica.

Zgled. $\gamma K_n = 1$, $\gamma C_n = \lceil \frac{n}{3} \rceil$, $\gamma P_{5,2} = 3$.

Izrek. *Za vsak graf brez izoliranih vozlišč velja, da je* $\lceil \frac{|VG|}{\Delta G + 1} \rceil \leq \gamma G \leq \lfloor \frac{|VG|}{2} \rfloor$.

Dokaz. Spodnja meja: Če je G dominantna množica in $u \in D$, potem u dominira $\leq \deg_G u + 1$ vozlišč, torej vsako vozlišče iz D dominira kvečjemu $\Delta G + 1$ vozlišč. Ker $VG \subseteq N_G[D]$ (unija zaprtih okolic vozlišč iz dominantne množice prekrije cel graf), je $|D| \geq \frac{|VG|}{\Delta G + 1}$, kajti $|VG| = |N_G[D]| = \left|\bigcup_{u \in D} N_G[u]\right| \leq \sum_{u \in D} N(u) \leq \sum_{u \in D} (\Delta G + 1) = \gamma G(\Delta G + 1)$.

Zgornja meja: Naj bo I poljubna maksimalna neodvisna množica. Vemo, da je I tedaj dominantna. Če je $|I| \leq \frac{|VG|}{2}$ smo dokazali, sicer vzemimo njen komplement $I' \coloneqq VG \setminus I$. Trdimo, da je I' dominantna. Vzemimo poljubno $u \in G$. Če $u \in I'$, dominira samega sebe, sicer, ker je G brez izoliranih vozlišč, ima u vsaj enega soseda, ker pa je I neodvisna, je ta sosed v I', torej je I' dominantna in ima $\leq \frac{|VG|}{2}$ vozlišč in velja $\gamma G \leq \min\{|I|, |I'|\} \leq \frac{|VG|}{2}$, kajti $I \cup I' = VG$. □

Zgled. Enakost spodnje meje velja v K_n, C_n. Enakost zgornje meje velja pri glavnikih T_n.

Izrek. *Če je H vpet podgraf G, je $\gamma G \leq \gamma H$.*

Dokaz. Naj bo D minimalna dominantna množica za H. $|D| = \gamma H$. Tedaj je D očitno tudi dominantna množica za G. Toda seveda se lahko zgodi, da je v G moč najti manjšo dominantno množico kot v H, ker ima G lahko dodatne povezave. □

2.20 Kaj je dominacijsko število grafa in kaj je celotno dominacijsko število grafa? Kakšna je zveza med njima? Kakšna je povezava med dominacijskim številom grafa in kromatičnim številom komplementa?

Dominacijsko število grafa je definirano v vprašanju 2.19.

Definicija. Dominantna množica D grafa G je povezana, če inducira povezan podgraf, neodvisna, če inducira podgraf brez povezav in **celotna**, če ima vsako vozlišče iz VG soseda v D (tudi vozlišča iz D). Velikost najmanjše povezane dominantne množice označimo z $\gamma_c G$, neodvisne z $\gamma_i G$ in **celotne** z $\gamma_t G$ (connected, independent in total).

Zgled. $\gamma_t K_n = 2$, $\gamma_t P_n = \lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil - \lfloor \frac{n}{4} \rfloor$ (gledamo parčke, ki se dominirajo).

Izrek. *Za vsak graf brez izoliranih vozlišč velja* $\gamma G \leq \gamma_t G \leq 2\gamma G$.

Dokaz. Spodnja meja je očitna, kajti biti celotna dominantna množica je strožji pogoj kot biti dominantna množica. Dokažimo $\gamma_t G \leq 2\gamma G$: Naj bo D poljubna dominantna množica G. Vsakemu $x \in D$ priredimo nekega soseda od x, recimo x' in ga dodajmo v $\hat{D}$, torej $\hat{D} = D \cup \{x'; x \in D\}$, s čimer dominantno množico spremenimo v celotno tako, da ji kvečjemu podvojimo število vozlišč. □

Zgled. Enakost spodnje meje se pojavi pri $\gamma C_4 = \gamma_t C_4 = 2$, neenakost pa pri recimo $\gamma G_3 = 2 \neq 4 = \gamma_t Q_3$.

2.21 Kaj je grupoid, polgrupa, monoid, grupa? Kako v monoidu izračunamo inverz produkta obrnljivih elementov? Kako definiramo potence v monoidu in kateri računski zakoni veljajo zanje?

Definicija. Če uvedemo binarno operacijo f na množici A takole: $f : A \times A \to A, f$ preslikava, je par (A, f) **grupoid**. ZDB zahtevamo, da je operacija preslikava (domena je enaka definicijskemu območju) in s tem zaprtost operacije. Dvojiški operator $f(a, b)$ pišimo kot $a \cdot b$.

Če $\forall a, b, c \in A : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociativnost), pravimo, da je $(A, \cdot)$ **podgrupa** ZDB asocietiven grupoid.
Enota je element $e \in A \ni: \forall a \in A : a \cdot e = e \cdot a = a$. Polgrupi z enoto pravimo **monoid**.
Monoidu, v katerem so vsi elementi obrnljivi, pravimo **grupa** ZDB $\forall a \in A \exists b \in A \ni: a \cdot b = b \cdot a = e$.

Pripomba. Ker so inverzi v monoidu enolični (dokaz pri LA), inverz a označimo z a^{-1}.

Zgled. $(\mathcal{G}, \square)$ monoid, $\left(\mathbb{R}_0^+ = \{x \in \mathbb{R}; x \geq 0\}, \max\right)$ monoid, množica vseh nizov/seznamov s concat operacijo je monoid.

Izrek. *Če sta a in b v monoidu obrnljiva, je obrnljiv tudi njun produkt in velja* $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Dokaz. $(a \cdot b) \cdot \left(b^{-1} \cdot a^{-1}\right) = a \cdot \left(b \cdot b^{-1}\right) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$ in podobno $\left(b^{-1}a^{-1}\right)(ab) = e$, torej $\left(b^{-1}a^{-1}\right)(ab) = (ab)\left(b^{-1}a^{-1}\right) = e \Rightarrow ab = \left(b^{-1}a^{-1}\right)$ po definiciji inverza. □

Posledica. *Če so $a_1, \ldots, a_k$ obrnljivi elementi monoida, je $(a_1 \cdots a_k)$ obrnljiv element monoida in velja* $(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$.

Dokaz. Dokaz z indukcijo: Baza: $k = 2$ velja, Korak: predpostavimo $(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$. Množimo z desne z a_{k+1} in smo dokazali. □

Definicija. Naj bo $(A, \cdot)$ monoid, $n \in \mathbb{N}_0$. $a^0 \coloneqq e$, $a^n = a \cdot a^{n-1}$ za $n \geq 1$.

Posledica. *Velja torej* $a^n a^m = a^{n+m}$, $(a^n)^m = a^{nm}$, $\left(a^{-1}\right)^n = a^{-1} \cdots n - krat \cdots a^{-1} = (a \cdots n - krat \cdots a)^{-1} = (a^n)^{-1}$. *Torej za obrnljiv a velja* $(a^n)^{-1} = \left(a^{-1}\right)^n$.

2.22 Kaj je red elementa v grupi? Kaj je pravilo krajšanja v grupi? Dokažite ga. Kako se pravilo krajšanja odraža v Cayleyevi tabeli grupe?

Definicija. Cayleyeva tabela za grupoid $(A, \cdot)$ je kvadratna tabela širine $|A|$, kjer ima $i, j-$ta celica vrednost $a_i \cdot a_j$, kjer je a_k $k-$ti element množice A. Pač izberemo si neko linearno urejenost A.

Definicija. Naj bo $(G, \cdot)$ končna grupa in $a \in G$. Tedaj je red elementa a najmanjši $n \in \mathbb{N} \ni: a^n = e$.

Izrek. *Dirichletovo načelo:* $\exists n, m \in [k+1], n \neq m : a^n = a^m$

Dokaz. BSŠ $n < m$. $a^n = a^m \Rightarrow a^n (a^m)^{-1} = a^m (a^m)^{-1} \Rightarrow a^{n-m} = e$ □

Izrek. *Pravilo krajšanja: Če je* G[19] *grupa,* $a, b, c \in G$*, velja* $ab = ac \Rightarrow b = c$ *in* $ba = ca \Rightarrow b = c$.

Dokaz. Množimo obe strani z leve ali desne z inverzom a. □

Posledica. *V Cayleyevi tabeli grupe se v vsaki vrstici in v vsakem stolpcu pojavijo vsi elementi grupe.*

2.23 Kaj je permutacijska grupa? Kaj je simetrična grupa S_n in kaj je alternirajoča grupa A_n? Kaj pravi Cayleyev izrek (o univerzalnosti permutacijskih grup) in kakšna je ideja njegovega dokaza?

Definicija. Naj bo A množica. Permutacija A je bijekcija $A \to A$. Permutacijska grupa je množica nekaj permutacij A, ki ga komponiranje tvorijo grupo.

Definicija. Simetrična grupa: $S_n \coloneqq \{\pi; \pi : \{1..n\} \to \{1..n\} \text{ bijekcija}\}$. Alternirajoča grupa: $A_n \coloneqq \{\pi \in S_n; \pi \text{ soda}\}$. Permutacija je soda, če je v zapisu z disjunktnimi cikli vsota dolžin ciklov, ki ji odštejemo število ciklov, soda.

Izrek. $|A_n| = \frac{n!}{2}$.

Definicija. Naj bosta $(G, \circ)$ in $(H, *)$ grupi. $f : G \to H$ je hm$\varphi \Leftrightarrow \forall x, y \in G : f(x \circ y) = fx * fy$. Če je f tudi bijekcija, je $f : G \to H$ izomorfizem. Grupi sta izomorfni, če obstaja izomorfizem med njima. Tedaj pišemo $G \approx H$.

Izrek. *Cayley: Vsaka grupa je izomorfna neki permutacijski grupi.*

Dokaz. (skica dokaza) Naj bo $(G, \cdot)$ grupa. Vsakemu elementu grupe priredimo preslikavo $g \in G \mapsto \alpha_g : G \to G$, ki slika takole: $\forall x \in G : \alpha_k x = g \cdot x$. α_g je permutacija G, saj je bijektivna, ker velja pravilo krajšanja: $x \neq y \Rightarrow \alpha_g x \overset{\text{pravilo krajšanja}}{=} gx \neq gy = \alpha_g y$. $\{\alpha_g; \forall g \in G\}$ tvori permutacijsko grupo, ki je izomorfna izvorni grupi: $(\{\alpha_g; \forall g \in G\}, \circ) \approx (G, \cdot)$. □

2.24 Kaj so odseki grupe G po podgrupi H? Kdaj je $aH = H$ in kdaj je $aH = Ha$? Kaj je vsebina Lagrangeovega izreka o moči podgrup in končnih grup?

Definicija. Naj bo $(G, \cdot)$ grupa in H podgrupa G. Če je $a \in G$, definiramo $aH = \{ah, h \in H\}$ (desni odsek podgrupe H) in $Ha = \{ha, h \in H\}$ (levi odsek podgrupe H).

Izrek. *Naj bo* G *grupa in* $a, b \in G$ *in* H *podgrupa* G*. Tedaj veljajo naslednje lastnosti:*

1. $a \in aH$
2. $aH = H \Leftrightarrow a \in H$
3. $aH = bH \nabla aH \cap bH = \emptyset$
4. $aH = bH \Leftrightarrow a^{-1}b \in H$
5. $|aH| = |bH|$
6. $aH = Ha \Leftrightarrow H = aHa^{-1}$
7. aH *podgrupa* $G \Leftrightarrow a \in H$

Dokaz. Dokažimo trditve:

1. $e \in H \Rightarrow a \cdot e = a \in aH$
2. $(\Rightarrow)$ $a \overset{1}{\in} aH = H \Rightarrow a \in H$, $(\Leftarrow)$ Najprej ena vsebovanost: $\forall x \in aH \exists h \in H \ni : x = ah$, ker $a \in H$, je po zaprtosti podgrupe H $ah = x \in H \Rightarrow aH \subseteq H$. Nato še druga vsebovanost: $\forall x \in H : a^{-1}x \in H \Rightarrow a\left(a^{-1}x\right) = x \in aH \Rightarrow H \subseteq aH$.

[19] Ko omenimo algebrajsko strukturo, občasno omenimo le množico, ko je iz konteksta operacija implicitno znana.

3. Imejmo aH, bH. Če je $aH = bH$, smo dokazali, sicer $\exists x \in aH \cup bH$. Ker $x \in aH \Rightarrow \exists h' \in H \ni: x = ah'$. Ker $x \in bH \exists h'' \in H \ni: x = bh''$. Toree velja $x = ah' = bh''$. Množimo s $h'^{-1} \Rightarrow a = bh''h'^{-1} \Rightarrow aH = bh'' \left(h'^{-1}H\right) \overset{2}{=} bh''H \overset{2}{=} bH$.

4. ...

5. Očitno (pravilo krajšanja)

6. $(\Rightarrow)$ $aH = Ha \Rightarrow aHa^{-1} = Haa^{-1} = H$. $(\Leftarrow)$ $H = aHa^{-1} \overset{\cdot a^{-1}}{\Rightarrow} a^{-1}H = Ha$. Ker je $a \in aH$, je v $a^{-1} \in aH$ (grupa), ker je $a^{-1} \in aH \cap a^{-1}H$, je $aH = a^{-1}H$, torej $a^{-1}H = Ha \Rightarrow aH = Ha$.

□

Izrek. *Lagrange: Če je G končna grupa in H podgrupa G, potem $|H|$ deli $|G|$. Nadalje je število levih/desnih odsekov po H enako $\frac{|G|}{|H|}$.*

Dokaz. Naj bodo $a_1H, a_2H, \ldots, a_nH$ različni odseki. Tedaj $|G| \overset{1}{=} |a_1H \cup \cdots \cup a_nH| \overset{\text{disjunktni odseki}}{=} \sum_{i=1}^{k} |a_iH| = k\,|H| \Rightarrow k = \frac{|G|}{|H|}$. □

Posledica. *Če je G končna grupa in $a \in G$, potem* red a *deli $|G|$.*

Dokaz. $\langle a \rangle = \left\{a^k; k \in \mathbb{Z}\right\} = \left\{e, a, \ldots, a^{n-1}\right\} \overset{\text{Lagrange}}{\Rightarrow} \langle a \rangle$ je gotovo podgrupa $G \Rightarrow n$ deli $|G|$. □

2.25 Kaj je podgrupa edinka? Navedite nekaj primerov podgrup edink. Kaj je faktorska grupa G/H in kaj pomeni, da je operacija v G/H dobro definirana?

Definicija. Naj bo H podgrupa grupe G. Tedaj rečemo, da je H podgrupa edinka, če velja $\forall a \in G : aH = Ha \overset{6}{\Leftrightarrow} \forall a \in G : aHa^{-1} = H$. Oznaka: $H \triangleleft G$. Če sta G in $\{e\}$, kjer je e enota v G, edini edinki G, je G enostavna.

Definicija. Center grupe $G \sim ZG \coloneqq \{a \in G; \forall x \in G : ax = xa\}$ ZDB taki elementi G, ki komutirajo z vsemi.

Zgled. V Abelovi grupi je vsaka podgrupa edinka. $SL_2\mathbb{R} \triangleleft GL_2\mathbb{R}$. $ZG \triangleleft G$.

Definicija. Naj bo $H \triangleleft G$. $G/H \coloneqq \{aH; a \in G\}$. V množico G/H vpeljemo operacijo $(aH)\,(bH) = (ab)\,H$ (*).

Izrek. *Faktorske grupe: Če je $H \triangleleft G$, je G/H grupa za (*).*

Dokaz. Dokazati notranjost, enoto, asociativnost in inverze je trivialno. Treba je še dokazati dobro definiranost, t. j. a, a' iz istega odseka in b, b' iz istega odseka $\Rightarrow (aH)\,(bH) = (ab)\,H = (a'b')\,H = (a'H)\,(b'H)$. Ker $a' \in aH \Rightarrow \exists h' \in H \ni: ah' = a'$. Ker $b' \in bH \Rightarrow \exists h'' \in H \ni: bh'' = b'$. Sedaj $(a'H)\,(b'H) \overset{\text{def.}}{=} (a'b')\,H = (ah'bh'')\,H = ah'b\,(h''H) \overset{2}{=} ah'bH = ah'\,(bH) \overset{H \text{ edinka}}{=} ah'\,(Hb) = a\,(h'H)\,b \overset{2}{=} aHb = (ab)\,H$. □

2.26 Kaj je kolobar, kaj je cel kolobar? Kaj je pravilo krajšanja v kolobarjih in kakšna je povezava tega pravila s celimi kolobarji? Kaj velja za končne cele kolobarje?

Definicija. Bigrupoid $(R, +, \cdot)$ je kolobar, če je $(R, +)$ abelova grupa, $(R, \cdot)$ polgrupa in velja $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c \wedge (a + b) \cdot c = a \cdot c + b \cdot c$ (leva in desna distributivnost). Kolobar je komutativen, če je $(R, \cdot)$ komutativna polgrupa. $(R, +, \cdot)$ je kolobar z enoto, če je $(R, \cdot)$ monoid.

Definicija. Direktna vsota kolobarjev: Naj bosta R in S kolobarja. $R \oplus S = R \times S$ je direktna vsota . Definirajmo operaciji $(r, s) +' (r', s') \coloneqq (r + r', s + s')$, $(r, s) \cdot' (r', s') \coloneqq (r \cdot r', s \cdot s')$.

Definicija. Center kolobarja $\sim ZR \coloneqq \{a \in R; \forall x \in R : ax = xa\}$, ZDB vsi taki elementi R, ki pri množenju s poljubnim elementom kolobarja komutirajo.

Trditev. Če sta R in S kolobarja, je $(R \oplus S, +', \cdot')$ kolobar. Nadalje: Če sta R in S komutativna kolobara, je tudi $(R \oplus S, +', \cdot')$ komutativen kolobar. Če sta z enoto, je tudi $(R \oplus S, +', \cdot')$.

Definicija. Če v kolobarju R velja $a \cdot b = 0$[20] in sta $a \neq 0$ in $b \neq 0$, sta a in b deliteja niča.

Definicija. V kolobarju $(R, +, \cdot)$ velja pravilo krajšanja, če velja $\forall a, b, c \in R, a \neq 0 : ab = ac \Rightarrow b = c$.

Definicija. Komutativen kolobar z enoto $1 \neq 0$ (ZDB multiplikativna enota ni enaka aditivni) brez deliteljev niča je **cel**.

Zgled. $(\mathbb{Z}, +, \cdot)$ je cel, toda $(\mathbb{Z}_6, +_6, \cdot_6)$ ni cel, ker premore delitelje niča.

Izrek. *Naj bo $(R, +, \cdot)$ komutativen kolobar z enoto $1 \neq 0$. Velja R cel $\Leftrightarrow$ v R velja pravilo krajšanja.*

Dokaz. Dokazujemo ekvivalenco:

($\Rightarrow$) Predpostavimo, da je R cel. Predpostavimo $ab = ac$ za poljuben $a \neq 0$ in poljubna b, c. Računamo: $ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0$. Ker je R cel in $a \neq 0$, mora biti $b - c = 0$, sicer bi bila a in $b - c$ delitelja niča, kar bi bilo v $\nrightarrow\nleftarrow$ s predpostavko o celosti R. $b - c = 0 \Rightarrow b = c$, torej $\forall a \neq 0, b, c \in R : ab = ac \Rightarrow b = c \sim$ velja pravilo krajšanja.

($\Leftarrow$) Predpostavimo, da v komutativnem kolobarju z enoto $1 \neq 0$ R velja pravilo krajšanja. Predpostavimo $ab = 0$, $a \neq 0$. Dokazati je treba $b = 0$, sicer bi imeli delitelje niča. Velja $ab = 0 = a \cdot 0$. Uporabimo pravilo krajšanja na $ab = a0$ in dobimo $b = 0$. Kolobar je cel.

□

Definicija. Komutativen kolobar R z enoto $1 \neq 0$ je **obseg**, če je vsak neničeln element obrnljiv v $(R, \cdot)$ ZDB $(R \setminus \{0\}, \cdot)$ je grupa. Obseg R je polje, če je $(R \setminus \{0\}, \cdot)$ abelova grupa ZDB $ZR = R$.

Izrek. *Če je $(R, +, \cdot)$ končen cel kolobar $\Rightarrow$ R polje.*

Dokaz. Dokažimo, da $\forall a \in R, a \neq 0 \exists a^{-1} \ni$: $aa^{-1} = 1$. Naj bo $a \in R$ poljuben, z izjemo $a \neq 0$. Oglejmo si $\{a^k; \forall k \geq 0\}$ ZDB množico vseh potenc a. Ker $|R| < \infty \Rightarrow \exists i, j$,BSŠ $i > j \ni a^i = a^j$ ZDB ker je R končen, se nek element „ponovi“. $a^j \cdot a^{i-j} = a^i = a^j = a^j \cdot 1$ Ker je kolobar cel, $a^j \neq 0$ in ker velja pravilo krajšanja, $a^{i-j} = 1$, pri čemer vemo, da je $i - j > 0$. Ločimo dva primera:

$i - j = 1$ $a = 1 \Rightarrow a$ je kot multiplikativna enota multiplikativni inverz sam sebi

$i - j > 1$ $a = a \cdot a^{i-j-1} = 1$, torej a^{i-j-1} je inverz a.

□

2.27 Kaj je karakteristika kolobarja? Kako lahko določimo karakteristiko kolobarja z enoto? Kaj lahko povemo o karakteristiki celega kolobarja?

Definicija. Karakteristika kolobarja $R \sim \operatorname{char} R$ je najmanjši $n \in \mathbb{N} \ni$: $\forall a \in R : a + \cdots_{n-\text{krat}} \cdots + a = 0$. Če tak n ne obstaja, pravimo $\operatorname{char} R = 0$.

Izrek. *Naj bo $(R, +, \cdot)$ kolobar z enoto.* $\operatorname{char} R = \operatorname{red} 1$ *v grupi $(R, +)$ ZDB red enote v aditivni grupi.*

Dokaz. Po definiciji reda je $1 + \cdots_{\operatorname{red} 1-\text{krat}} \cdots + 1 = 0$ in za nek $m < \operatorname{red} 1$ $1 + \cdots_{m-\text{krat}} \cdots + 1 \neq 0$, torej $\operatorname{char} R \geq \operatorname{red} 1$. Sedaj vzemimo poljuben $a \in R$. Velja $a + \cdots_{\operatorname{red} 1-\text{krat}} \cdots + a = 1 \cdot a + \cdots_{\operatorname{red} 1-\text{krat}} \cdots + 1 \cdot a = a \cdot (1 + \cdots_{\operatorname{red} 1-\text{krat}} \cdots + 1) = a \cdot 0 = 0$, torej $\operatorname{char} R \leq \operatorname{red} 1$, torej $\operatorname{char} R = \operatorname{red} 1$. □

Izrek. *Naj bo $(R, +, \cdot)$ cel kolobar. Tedaj velja bodisi* $\operatorname{char} R = 0$ *bodisi* $\operatorname{char} R = p$*, kjer je p praštevilo.*

Dokaz. Če je $\operatorname{char} R = 0$, smo dokazali, sicer je $\operatorname{char} R = r > 0$. PDDRAA $n = pq$ za $p, q > 1$ in $p, q \in \mathbb{N}$. Po prejšnjem izreku $\operatorname{char} R = \operatorname{red} 1 = n$. Tedaj velja $0 = 1 + \cdots_{n-\text{krat}} \cdots + 1 = 1 + \cdots_{pq-\text{krat}} \cdots + 1 = (1 + \cdots_{p-\text{krat}} \cdots + 1) \cdot (1 + \cdots_{q-\text{krat}} \cdots + 1) = a \cdot b$. Ker smo v celem kolobarju, je bodisi $a = 0$, bodisi $b = 0$, toda to je $\nrightarrow\nleftarrow$, saj bi bil potem $\operatorname{red} 1 = q$ ali $\operatorname{red} 1 = p$, oboje pa je $< pq$. □

[20] 0 je aditivna enota

2.28 Kaj je ideal kolobarja? Kako lahko preverimo, ali je $I \subseteq R$ ideal kolobarja R? Kaj je faktorski kolobar R/I in kako računamo v njem?

Definicija. Če je R kolobar, je njegov podkolobar S ideal, če velja $\forall v \in R, s \in S : rs, sr \in S$ ZDB to je podkolobar, zaprt za zunanje množenje.

Zgled. $n \cdot \mathbb{Z}$ (večkratniki n) za fiksen n so ideal v $\mathbb{Z}$. $\mathbb{Z}$ je podkolobar v $\mathbb{Q}$, toda ni njegov ideal.

Trditev. $I \subseteq R$ je ideal $\Leftrightarrow 0 \in I$ (vsebuje aditivno enoto) $\wedge \forall i, j \in I : i - j \in I$ (zaprt za odštevanje) $\wedge \forall i \in I, r \in R : ir \in I, ri \in I$ (zaprt za zunanje množenje)

Definicija. Naj bo R kolobar in I ideal v R. Faktorski kolobar: $R/I = \{a + I, \forall a \in R\} = \{\{a + i; \forall i \in I\}; \forall a \in R\}$ vsebuje aditivne odseke. V R/I vpeljemo operaciji: $(a + I) +' (b + I) = a + b + I$ in $(a + I) \cdot' (b + I) = a \cdot b + I$.

Izrek. *Če je I ideal v R, je $(R/I, +', \cdot')$ kolobar.*