Diskretne strukture II

zapiski predavanj - prezentacija

doc. dr. R. Škrekovski

Osnovno o grafih

Če odnose med določenimi objekti opišemo z dvomestno relacijo, lahko to relacijo tudi "narišemo" (oz. grafično upodobimo). Recimo, da je relacija simetrična in irefleksivna. Na primer:

Takemu objektu pravimo **graf**. Pri tem sama slika ni pomembna, isti graf bi lahko narisali tudi takole:

Pomembno je le to, kakšna je osnovna relacija, tj. med katerimi pari imamo povezave in med katerimi povezav ni.

Grafi se kot model pojavljajo v različnih vedah:

kemija: molekularni grafi, grafi kemijskih reakcij;

elektrotehnika: električna vezja;

operacijske raziskave: omrežja - transportna, komunikacijska;

ekonomija: odnosi med ekonomskimi subjekti;

genetika: struktura genov;

sociologija, psihologija: odnosi med socialnimi skupinami ali posamezniki;

teoretično računalništvo: algoritmi, baze podatkov, komunikacijska omrežja;

matematika: kombinatorika, topologija.

Definicija

V – končna neprazna množica;

E – poljubna družina dvoelementnih podmnožic množice V.

Paru $G = (V, E)$ pravimo **graf**

- na **množici točk** $V = V(G)$; in
- z **množico povezav** $E = E(G)$.

Element $\{u, v\}$ množice E pišemo krajše kot uv.

Kadar je par točk uv element množice E pravimo, da sta točki u in v **sosednji** v grafu G in pišemo $u \sim_G v$ (ali samo $u \sim v$).

Za povezavi pravimo, da sta **sosednji**, če imata kako skupno krajišče.

Včasih obravnavamo tudi grafe, ki imajo

- **vzporedne povezave** – več povezav nad istim parom točk;
- **zanke** – povezave, ki imajo obe krajišči enaki.

Takim grafom bomo rekli **multigrafi**.

Kadar želimo poudariti, da govorimo o grafih brez zank in vzporednih povezav, takim grafom rečemo **enostavni grafi**.

Stopnja

Stopnja točke u v grafu G, označimo jo z $\deg_G(u)$ ali $d_G(u)$, je število povezav grafa G, ki imajo točko u za svoje krajišče.

Točkam stopnje 0 pravimo **izolirane točke**, točkam stopnje 1 pa **listi**.

Najmanjšo stopnjo točke grafa G označimo z $\delta(G)$, največjo pa z $\Delta(G)$.

Graf G je **regularen**, če velja $\delta(G) = \Delta(G)$, in d**-regularen**, če velja $d = \delta(G) = \Delta(G)$.

Grafom, ki so 3-regularni, pravimo tudi **kubični** grafi.

Naloga 1 *Dokaži, da v skupini dveh ali več ljudi lahko vedno najdemo dva, ki imata v tej skupini enako število prijateljev!*

Dokaz.

Matrike grafov

G graf

$V(G) = \{v_1, v_2, \ldots, v_n\}$

$E(G) = \{e_1, e_2, \ldots, e_m\}$

Matrike sosednosti $A(G)$

$$A(G) = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \qquad a_{ij} = \begin{cases} 1, & \text{če } v_i \sim v_j \\ 0, & \text{sicer.} \end{cases}$$

Incidenčna matrika $B(G)$

$$B(G) = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} & \ldots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{nm} \end{bmatrix} \qquad b_{ij} = \begin{cases} 1, & \text{če } v_i \in e_j \\ 0, & \text{sicer.} \end{cases}$$

Stopnje točk in število povezav grafa so povezane z naslednjo enakostjo:

Lema 1 (O rokovanju). *Za vsak graf G velja*

$$\sum_{v \in V(G)} \deg_G(v) = 2 \cdot |E(G)| .$$

Posledica 2 *Za r-regularni graf G velja zveza*

$$r \cdot |V(G)| = 2 \cdot |E(G)|.$$

Posledica 3 *Vsak graf ima sodo mnogo točk lihe stopnje.*

Podgrafi

Graf H je **podgraf** grafa G, oznaka $H \subseteq G$, če velja

$$V(H) \subseteq V(G) \quad \text{in} \quad E(H) \subseteq E(G).$$

Podgraf H je **vpet**, če velja $V(H) = V(G)$.

Podgraf H je **induciran (z množico točk)** $U \subseteq V(G)$, če velja

$$V(H) = U \quad \text{in} \quad E(H) = \{uv \in E(G) \mid u, v \in V(H)\}.$$

Pišemo tudi $H = G[U]$.

Podobno definiramo tudi podgraf grafa G, **induciran z množico povezav** $F \subseteq E(G)$, kot podgraf H, za katerega velja

$$E(H) = F \quad \text{in} \quad V(H) = \{u \in V(G) \mid \exists e \in F : u \text{ je krajišče } e\}.$$

Tak podgraf označimo z $G[F]$.

Naloga 2 *Za dani graf preštej število podgrafov.*

Naloga 3 *Za graf iz prejšne naloge preštej število induciranih podgrafov.*

Naloga 4 *Naj bo G graf z n točkami in m povezavami. Ugotovi, koliko vpetih in koliko induciranih podgrafov ima graf G!*

Nekatere družine grafov

Polni grafi K_n: $V(K_n) = \mathbb{Z}_n$, $E(K_n) = \{uv \mid u, v \in \mathbb{Z}_n, u \neq v\}$.

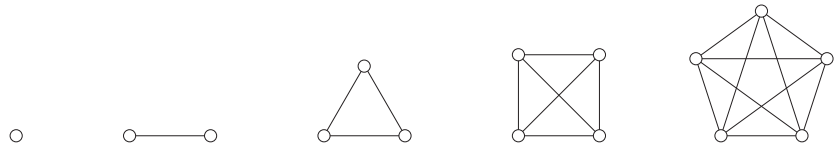


Figure 1: Polni grafi K_1, K_2, K_3, K_4 in K_5.

Polni graf K_n ima n točk in $\binom{n}{2} = \frac{n(n-1)}{2}$ povezav in je $(n-1)$-regularen.

Poti P_n: $V(P_n) = \mathbb{Z}_n$, $E(P_n) = \{u(u+1) \mid u = 0, 1, \ldots, n-2\}$.

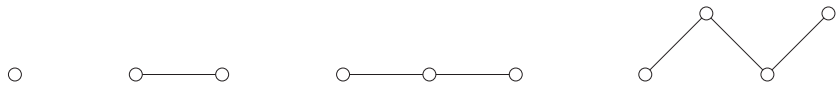


Figure 2: Poti P_1, P_2, P_3 in P_4.

Pot P_n ima n točk in $n-1$ povezav (njena **dolžina** je $n-1$). Za $n = 1$ in $n = 2$ je enaka grafu K_n.

Cikli C_n $(n \geq 3)$: $V(C_n) = \mathbb{Z}_n$, $E(C_n) = \{u(u+1) \mid u \in \mathbb{Z}_n\}$.

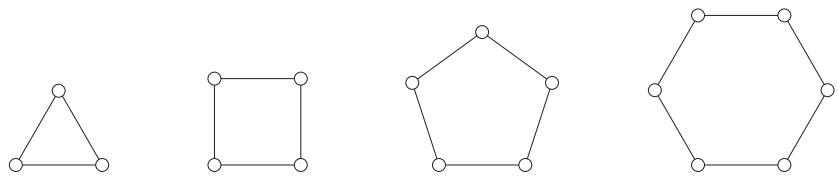


Figure 3: Cikli C_3, C_4, C_5 in C_6.

Kadar dopuščamo tudi multigrafe, sta definirana še cikla C_1 (zanka) in C_2 (par vzporednih povezav). Cikel C_n ima n točk in n povezav. Je 2-regularen graf. Cikel C_3 imenujemo tudi **trikotnik**.

Graf G je **dvodelen**, če lahko množico točk $V(G)$ zapišemo kot disjunktno unijo dveh podmnožic $A, B \subseteq V(G)$ tako, da je za vsako povezavo $uv \in E(G)$ ena od točk u, v vsebovana v množici A, druga pa v množici B.

A in B imenujemo **množici dvodelnega razbitja** grafa G.

Trditev 4 *Naslednje trditve so ekvivalentne:*

(a) Graf je dvodelen;

(b) Graf je 2-obarljiv (pobarvamo točke z dvema barvama tako, da nista dve sosednji točki enako obarvani);

(c) Graf ne vsebuje lihega cikla.

Dokaz.

Polni dvodelni grafi $K_{m,n}$: $V(K_{m,n}) = A \cup B$, kjer velja $|A| = m$, $|B| = n$ in $A \cap B = \emptyset$, $E(K_{m,n}) = \{uv \mid u \in A, v \in B\}$.

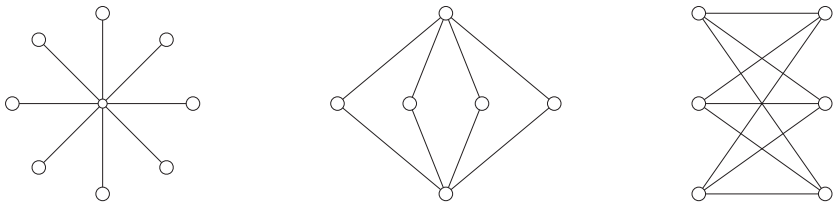


Figure 4: Polni dvodelni grafi $K_{1,8}$, $K_{2,4}$ in $K_{3,3}$.

Polni dvodelni graf $K_{m,n}$ ima $m+n$ točk in mn povezav. Grafom $K_{1,n}$ pravimo tudi **zvezde**.

Kolesa W_n $(n \geq 3)$: $V(W_n) = \mathbb{Z}_n \cup \{\infty\}$, $E(W_n) = \{u(u+1), u\infty \mid u \in \mathbb{Z}_n\}$.

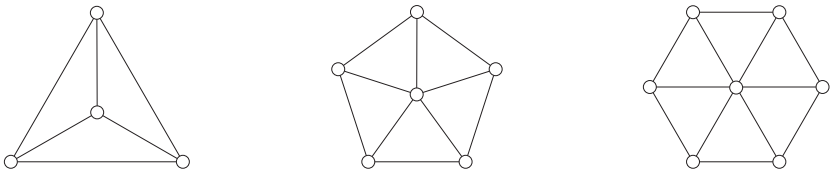


Figure 5: Kolesa W_3, W_5 in W_6.

Graf W_n ima $n+1$ točk in $2n$ povezav.

Hiperkocke Q_d: $V(Q_d) = \{(u_1, u_2, \ldots, u_d) \mid u_i \in \{0, 1\}\}$, $E(Q_n) = \{uv \mid u, v \in V(Q_d) : \sum_{i=1}^{d} |u_i - v_i| = 1\}$.

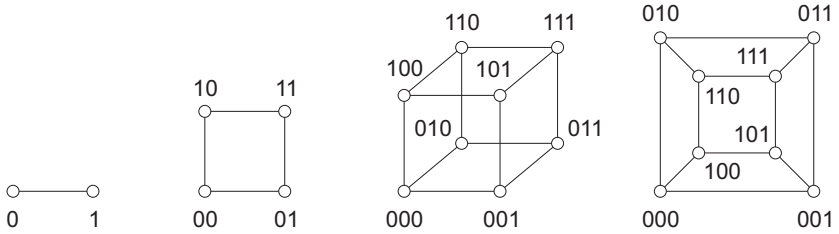


Figure 6: Hiperkocki Q_1 in Q_2 ter dve sliki hiperkocke Q_3.

Običajno med hiperkocke štejemo tudi 0-razsežno kocko $Q_0 = K_1$.

Hiperkocka Q_d (skelet d-razsežne kocke) ima 2^d točk ter $d \cdot 2^{d-1}$ povezav in je d-regularen graf.

Trditev 5 *Hiperkocke so dvodelni grafi.*

(**Namig:** za množici dvodelnega razbitja vzamemo množico točk, ki imajo sodo mnogo komponent enakih 0, in množico točk, ki imajo liho mnogo komponent enakih 0.)

Posplošeni Petersenovi grafi $P_{n,k}$ ($n \geq 3$ in $0 < k < n$): $V(P_{n,k}) = \{u_i, v_i \mid i \in \mathbb{Z}_n\}$, $E(P_{n,k}) = \{u_i u_{i+1}, u_i v_i, v_i v_{i+k} \mid i \in \mathbb{Z}_n\}$.

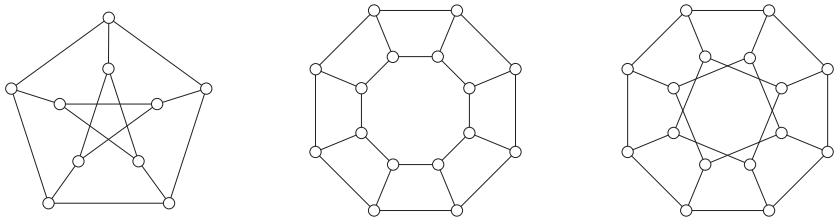


Figure 7: Petersenov graf in posplošena Petersenova grafa $P_{8,1}$ in $P_{8,2}$.

Posplošeni Petersenov graf $P_{n,k}$ ima $2n$ točk. Če je $n \neq 2k$, ima $3n$ povezav in je kubičen graf, za $n = 2k$ pa ima $\frac{5n}{2}$ povezav in velja $\delta(P_{n,k}) = 2$, $\Delta(P_{n,k}) = 3$.

Družina ima ime po **Petersenovem grafu** $P_{5,2}$.

Krožni grafi $\mathrm{Cir}(n; S)$: Naj bo S poljubna podmnožica množice $\mathbb{Z}_n$, ki ne vsebuje elementa 0 in ki z vsakim elementom $s \in S$ vsebuje tudi nasprotni element $n - s$. **Krožni graf** $G = \mathrm{Cir}(n; S)$ na n točkah in s **simbolom** S je določen takole:

$$V(G) = \mathbb{Z}_n \qquad \text{in} \qquad E(G) = \{uv \mid u - v \in S\}\,.$$

Med krožne grafe spadajo polni grafi in cikli:

- $K_n = \mathrm{Cir}(n; \{1, 2, \ldots, n-1\})$; in
- $C_n = \mathrm{Cir}(n; \{1, n-1\})$.

Krožni graf $\mathrm{Cir}(n; S)$ ima n točk in $\frac{n|S|}{2}$ povezav in je $|S|$-regularen graf.

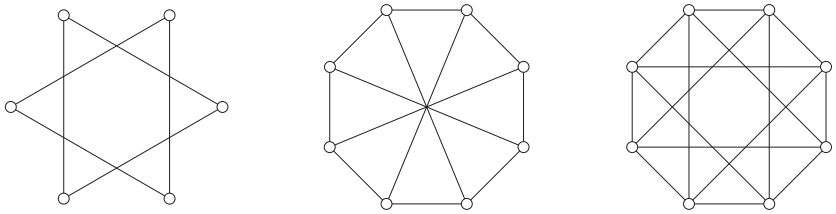


Figure 8: Krožni grafi $\mathrm{Cir}(6; \{2, 4\})$, $\mathrm{Cir}(8; \{1, 4, 7\})$ in $\mathrm{Cir}(8; \{1, 3, 5, 7\})$.

Operacije z grafi

Odstranjevanje točk: Naj bo G graf in $u \in V(G)$. Z $G - u$ označimo graf, ki ga dobimo tako da

- iz $V(G)$ odstranimo točko u;
- iz $E(G)$ odstranimo vse povezave, ki imajo za krajišče u.

Odstranjevanje povezav: Naj bo G graf in $e \in E(G)$. Z $G - e$ označimo graf, ki ga dobimo tako da

- iz $E(G)$ odstranimo povezavo e.

Komplementarni graf: Naj bo G graf. Grafu $\overline{G}$ z isto množico točk kot graf G, v katerem sta dve točki sosednji natanko tedaj, ko nista sosednji v grafu G, pravimo **komplementarni graf** (tudi **komplement**) grafa G.

Unija grafov: Unija grafov G_1 in G_2 je graf $G = G_1 \cup G_2$ z

- množico točk $V(G) = V(G_1) \cup V(G_2)$; in
- množico povezav $E(G) = E(G_1) \cup E(G_2)$.

Če je $V(G_1) \cap V(G_2) = \emptyset$, govorimo o **disjunktni uniji** grafov.

Skrčitev povezave: Naj bo $e \in E(G)$. Z G/e označimo graf, ki ga dobimo iz grafa G tako, da identificiramo krajišči povezave e in odstranimo zanko (ta nastane iz povezave e) ter morebitne vzporedne povezave (te nastanejo, če je povezava e vsebovana v trikotnikih grafa G). Če delamo z multigrafi, potem nastalih vzporednih povezav ne odstranjujemo.

Naloga 5 *Skrči pet povezav v Petersenovem grafu, da dobiš* K_5.

Spoj grafov: Spoj grafov G_1 in G_2, kjer je $V(G_1) \cap V(G_2) = \emptyset$, je graf $G = G_1 * G_2$, ki je določen takole:

$$\begin{aligned} V(G) &= V(G_1) \cup V(G_2)\,, \\ E(G) &= E(G_1) \cup E(G_2) \cup \{uv \mid u \in V(G_1), v \in V(G_2)\}\,. \end{aligned}$$

Spoj ima $|V(G_1)|+|V(G_2)|$ točk in $|E(G_1)|+|E(G_2)|+|V(G_1)| \cdot |V(G_2)|$ povezav.

Primer spoja grafov so kolesa in polni dvodelni grafi:

$$W_n \simeq K_1 * C_n \quad \text{in} \quad K_{m,n} \simeq \overline{K_m} * \overline{K_n}.$$

Kartezični produkt: Kartezični produkt grafov $G_1 = (V_1, E_1)$ in $G_2 = (V_2, E_2)$ je graf $G = G_1 \Box G_2$, ki ima množico točk

$$V(G) = V_1 \times V_2 \,,$$

sosednost pa je določena s predpisom

$$(u_1, v_1) \sim_G (u_2, v_2) \iff$$
$$(u_1 \sim_{G_1} u_2 \ \wedge \ v_1 = v_2) \vee (u_1 = u_2 \ \wedge \ v_1 \sim_{G_2} v_2) \,.$$

Kartezični produkt ima $|V_1| \cdot |V_2|$ točk in $|V_1| \cdot |E_2| + |V_2| \cdot |E_1|$ povezav.

Primer standardne družine, konstruirane s pomočjo kartezičnega produkta, so hiperkocke:

$$Q_d = \underbrace{K_2 \Box \cdots \Box K_2}_{d \text{ faktorjev}} \,.$$

Graf povezav: Naj bo G graf z vsaj eno povezavo. Graf povezav $L(G)$ grafa G je določen takole:

$$V(L(G)) = E(G) \quad \text{in} \quad E(L(G)) = \{ef \mid e, f \in E(G), e \cap f \neq \emptyset\}.$$

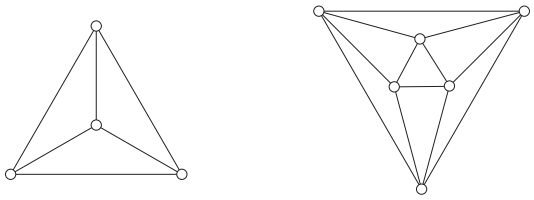


Figure 9: Graf K_4 (tetraeder) in njegov graf povezav $L(K_4)$ (oktaeder).

Graf povezav ima $|E(G)|$ točk in $\frac{1}{2}\sum_v (\deg_G(v))^2 - |E(G)|$ povezav.

Izomorfizem grafov

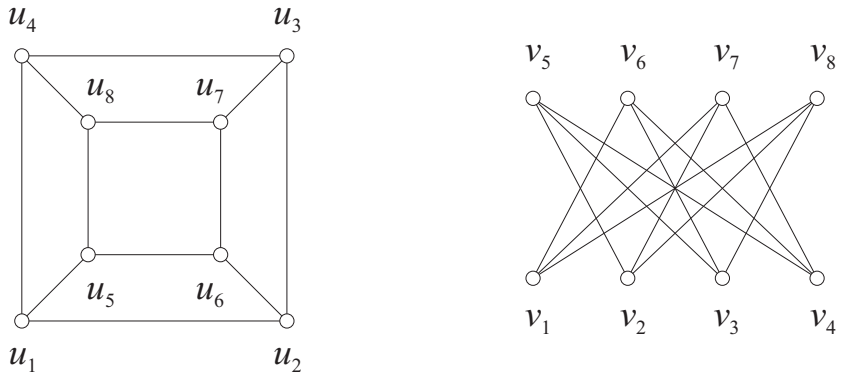
Vzemimo grafa G_1 in G_2. Preslikava $h : V(G_1) \to V(G_2)$ je **izomorfizem**, če velja:

- h je bijekcija;
- $uv \in E(G_1)$ natanko tedaj, ko je $h(u)h(v) \in E(G_2)$.

V tem primeru, grafa G_1 in G_2 sta **izomorfna**, označimo $G_1 \simeq G_2$.

V primeru, ko je graf G_1 kar enak grafu G_2, izomorfizmu grafov pravimo **avtomorfizem**.

Naloga 6 *Pokaži, da sta grafa izomorfna.*



Trditev 6 *Izomorfnost* ($\simeq$) *je ekvivalenčna relacija.*

Grafovske invariante

Lastnosti grafa, ki jo imajo poleg grafa samega tudi vsi z njim izomorfni grafi, pravimo **invarianta** grafa.

Grafovske invariante so na primer:

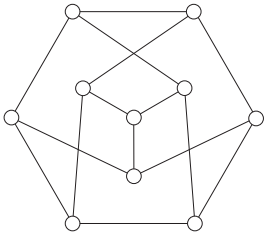
- število točk
- število povezav
- število komponent
- število točk stopnje 4
- število trikotnikov
- dvodelnost
- število mostov
- ....
- ....

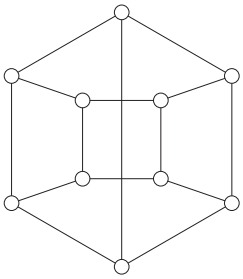
Osnovni način, s katerim dokažemo, da grafa nista izomorfna, je, da poiščemo grafovsko invarianto, v kateri se obravnavana grafa ločita.

Pozor: Matrika sosednosti $A(G)$ ni grafovska invarianta, ker je odvisna od vrstnega reda oz. oštevilčenja vozlišč. Tudi incidenčna matrika $B(G)$ ni invarianta.

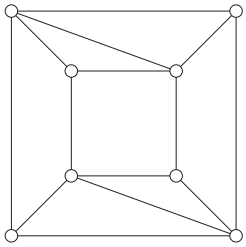
Dolžini najkrajšega cikla v grafu pravimo **notranji obseg** oz. **ožina** grafa.

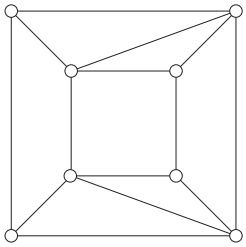
Spodnja grafa nista izomorfna, ker imata različno ožino.

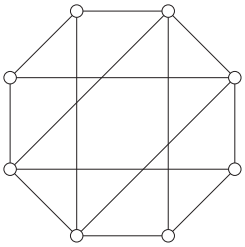




Naloga 7 *Pokaži, da so grafi paroma neizomorfni.*







Sprehodi

Zaporedje točk in povezav

$$S = v_0 e_1 v_1 e_2 v_2 \cdots v_{k-1} e_k v_k, \qquad \text{kjer je } e_i = v_{i-1} v_i$$

imenujemo **sprehod** v grafu.

Velikokrat zapišemo samo zaporedje točk

$$S = v_0 v_1 v_2 \cdots v_k$$

Dolžina sprehoda $S = v_0 v_1 v_2 \cdots v_k$ je enaka številu povezav k.

Obhod je sklenjen sprehod t.j. $v_0 = v_k$.

Sprehod je **enostaven**, kadar so vse povezave $e_1, e_2, \ldots, e_k$ med seboj različne.

Enostavni sprehod je **pot**, kadar so vse točke $v_0, v_1, \ldots, v_k$ med seboj različne.

Enostavni sprehod je **cikel**, kadar so vse točke $v_0, v_1, \ldots, v_{k-1}$ med seboj različne in $v_0 = v_k$.

Trditev 7 *Če v grafu obstaja sprehod od u do v, potem obstaja pot od u do v.*

Komponente in razdalja

Točki grafa sta v isti **povezani komponenti** tedaj, ko v grafu med njima obstaja pot.

Število povezanih komponent grafa G bomo označili z $\Omega(G)$.

Graf je **povezan**, če ima eno samo povezano komponento, tj. $\Omega(G) = 1$.

Razdaljo $d_G(u, v)$ med točkama $u, v \in V(G)$ v grafu G definiramo kot dolžino najkrajše poti od u do v v G. Če taka pot ne obstaja, za razdaljo vzamemo vrednost ∞.

S tako definirano razdaljo postane povezan graf G **metrični prostor** oz. veljajo naslednje lastnosti:

1. $\forall v \in V(G) : \; d(v, v) = 0$;
2. $\forall u, v \in V(G) : \; d(u, v) = d(v, u)$;
3. $\forall u, v, w \in V(G) : \; d(u, v) + d(v, w) \geq d(u, w)$.

Največji razdalji med parom točk grafa pravimo **diameter** oz. **premer** grafa,

$$\operatorname{diam}(G) = \max\{d_G(u, v) \mid u, v \in V(G)\}\,.$$

Naloga 8 *Izračunaj diameter grafov* $K_n, P_n, C_n, K_{n,n}, Q_n$*!*

Izometrični podgrafi

Podgraf H grafa G je **izometrični podgraf**, če se razdalje med točkami ohranjajo, tj.

$$\forall u, v \in V(H) : d_H(u, v) = d_G(u, v).$$

Naloga 9 *Poišči izometrični 6-cikel v Q_3. Pošči še 6-cikel v Q_3, ki ni izometrični.*

Trditev 8 *Vsak izometrični podgraf je induciran.*

Trditev 9 *Naj bo C najkrajši cikel v nekem grafu G s končno ožino. Tedaj je C izometrični podgraf.*

Intervalni in konveksni podgrafi

Naj bosta $u, v \in V(G)$. **Intervalni graf** $I_G(u, v)$ je podgraf grafa G induciran z vseh vozlišč, ki pripadajo kakšni najkrajši poti med u in v.

Graf H je **konveksni podgraf** grafa G, če je za vsak par točk u, v, $I_G(u, v)$ podgraf grafa H.

Naloga 10 *Kakšne konveksne podgrafe ima Q_3?*

Naloga 11 *Kakšne konveksne podgrafe ima mreža $n \times m$?*

Naloga 12 *Ali je vsak intervalni podgraf $I_G(u, v)$ konveksni?*

Naloga 13 *Pokaži, da je vsak konveksni podgraf tudi izometrični podgraf.*

Prirejanja in faktorji

M množica povezav grafa G je **prirejanje**, če nobeni dve povezavi iz M nimata skupnega krajišča.

k-faktor je vpet k-regularen podgraf.

1-faktorju rečemo tudi **popolno prirejanje**.

Zgledi:

Naloga 14 *Izračunaj*

- *Koliko popolnih prirejanj ima graf $K_{n,n}$?*
- *Koliko različnih (ne-izomorfnih) 1-faktorjev ima Q_3? Kaj pa 2-faktorjev?*

Problem 1 *Dokaži, da Q_d vsebuje k-faktor za vsak $k \in \{0, \ldots, d\}$!*

Drevesa

Grafu, ki ne vsebuje nobenega cikla, pravimo **gozd**.

Če je gozd tudi povezan, mu pravimo **drevo**.

Trditev 10 *Naj bo T drevo z n točkami in m povezavami. Velja:*

1. *Če $T \neq K_1$, potem ima T vsaj dva lista;*
2. *$m = n - 1$;*
3. *Za poljubna $u, v \in V(T)$ obstaja natanko ena pot med u in v;*
4. *Če drevesu T dodamo novo povezavo, potem dobljeni graf vsebuje natanko en cikel;*
5. *T je dvodelni graf.*

Trditev 11 *Vsako drevo T ima vsaj $\Delta(T)$ listov.*

Povezava e v povezanem grafu G je **most**, če $G - e$ razpade na dva dela.

Trditev 12 *V drevesu je vsaka povezava most.*

Naloga 15 *Naj bo T drevo na 14 točkah, v katerem so samo točke stopenj 1 in 4. Koliko točk stopnje 4 ima drevo T?*

Rešitev:

Izrek 13 *Za graf G so ekvivalentne naslednje trditve:*

(a) *G je drevo.*

(b) *G je povezan graf, za katerega velja $|E(G)| = |V(G)| - 1$.*

(c) *G je graf brez ciklov, za katerega velja $|E(G)| = |V(G)| - 1$.*

(d) *G je povezan in vsaka povezava grafa G je most.*

(e) *Za vsak par točk $u, v \in V(G)$ v grafu G obstaja natanko ena pot med u in v.*

(f) *G ne vsebuje cikla, če pa mu dodamo katerokoli povezavo, dobimo cikel.*

Vpeta drevesa

Naj bo G poljuben multigraf. **Vpeto drevo** v G je vsak vpet podgraf, ki je drevo.

Trditev 14 *Vsak povezan graf vsebuje vpeto drevo.*

Število vpetih dreves multigrafa G označimo s $\tau(G)$.

Velja, če je G drevo, potem $\tau(G) = 1$.

Naloga 16 *Izračunaj* $\tau(C_n)$.

Naloga 17 *Izračunaj* $\tau(K_1)$, $\tau(K_2)$, $\tau(K_3)$, $\tau(K_4)$.

Računanje $\tau(G)$

Zanke ne vplivajo na število vpetih dreves, zato jih pred štetjem vedno odstranimo.

Trditev 15 *Število $\tau(G)$ lahko izračunamo s pomočjo* ***rekurzivne formule:***

$$\tau(G) = \tau(G - e) + \tau(G/e)\,,$$

kjer je e poljubna povezava multigrafa G, ki ni zanka.

(Prvi člen $\tau(G-e)$ v formuli ustreza vpetim drevesom, ki ne vsebujejo povezave e, drugi člen $\tau(G/e)$ pa tistim, ki povezavo e vsebujejo.)

Računanje skrajšamo, če rekurzivno formulo uporabimo tudi na skupini vzporednih povezav.

Trditev 16 *Če je povezava e ena od k vzporednih povezav, potem velja*

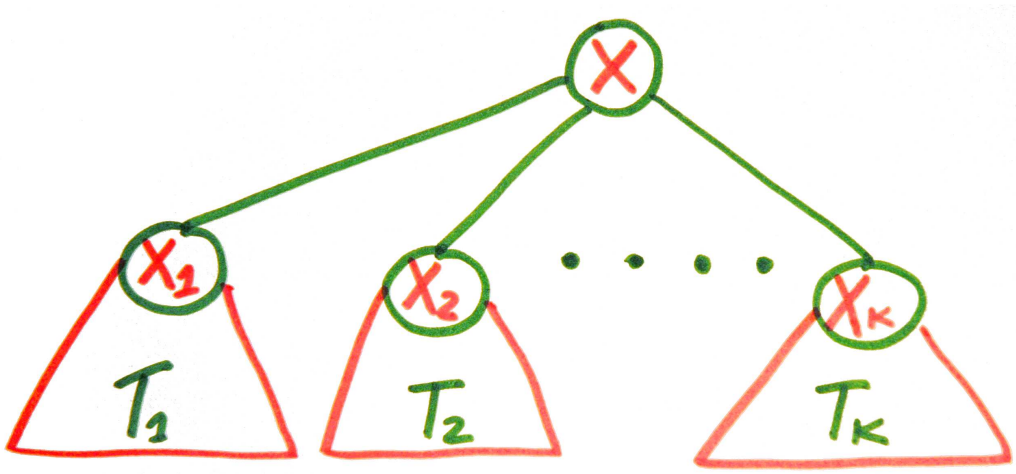
$$\tau(G) = \tau(G - F) + k \cdot \tau(G/e),$$

kjer je F množica vseh z e vzporednih povezav.

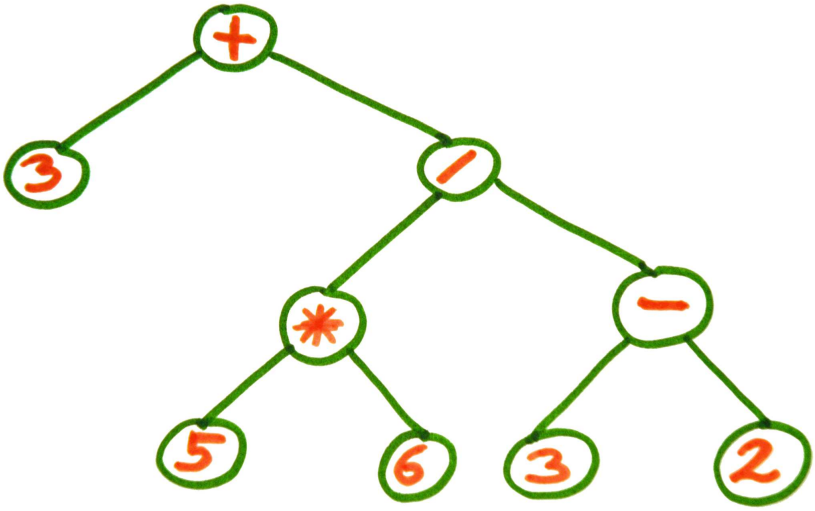
Izrek 17 (Cayley) $\tau(K_n) = n^{n-2}$.

Drevesa s korenom

Drevo T s korenom x je drevo, pri katerem je vozlišče x posebej odlikovano. Pri tem pa rekurzivo velja, da je vsaka komponenta T_i iz $T - x$ drevo s korenom x_i, kjer je x_i tisto vozlišče iz T_i, ki je sosedno z x.



Zgled: Drevo aritmetičnega izraza $3 + (5 * 6)/(3 - 2)$



Pri drevesu s korenom poznamo:

- relacijo oče-sin oz. relacijo prednik-potomec;
- nivoje ter globino.

Omenimo naslednja tipa dreves:

- **dvojiška drevesa:** vsako vozlišče ima največ dva sinova. Dvojiško drevo je **popolno**, če velja
  - vsako vozlišče, ki ni list, ima natanko dva sinova;
  - vsi listi so na enaki razdalji od korena.
- **AVL drevesa:** dvojiško drevo, kjer pri vsakem vozlišču velja, da se višini levega in desnega poddrevesa razlikujeta največ za 1.

Problem 2 *V popolnem dvojiškem drevesu višine k izračunaj:*

- *število vozlišč oz. listov;*
- *povprečni nivo;*
- *povprečno razdaljo od korena.*

Problem 3 *Katera je minimalna višina dvojiškega drevesa, ki vsebuje n elementov?*

Eulerjevi grafi

Sprehod v grafu je **Eulerjev**, če vsebuje vsako povezavo grafa natanko enkrat.

Eulerjev obhod je sklenjen Eulerjev sprehod.

Graf je **Eulerjev**, če vsebuje Eulerjev obhod.

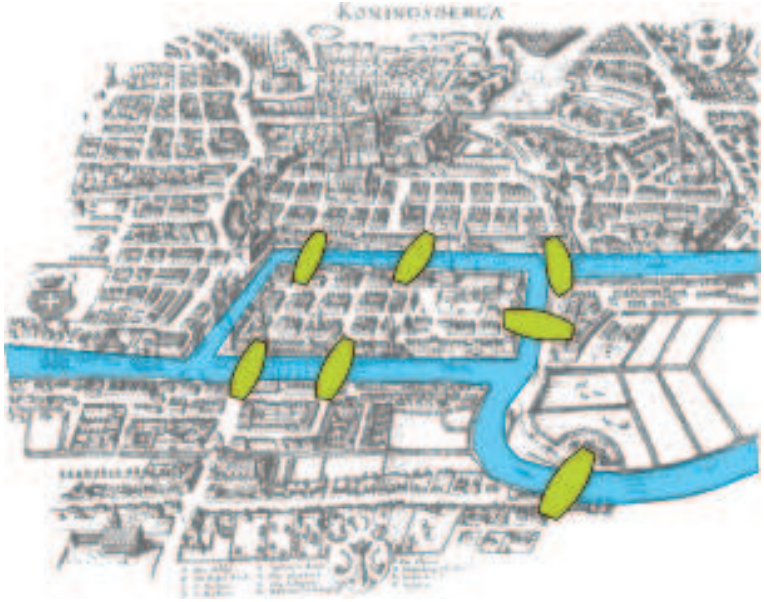
Potrebna pogoja za obstoj Eulerjevega obhoda:

(P1) **Graf je povezan**.

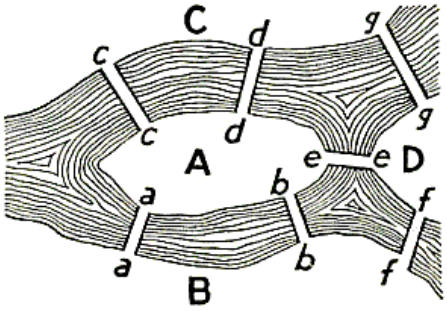
(P2) **Vse točke so sode stopnje**. Saj če med obhodom pridemo v neko točko, moramo iz te točke tudi oditi. Isto velja tudi za začetno točko, ki je enaka končni.

Problem Königsberških mostov

Problem 4 *Ali obstaja obhod mesta, ki bi prečkal vsak most natanko enkrat in se vrnil v izhodišče?*



Euler je leta 1736 dal negativen odgovor.



The Königsberg Bridges.

Izrek 18 *Naj bo G povezan graf. Graf G je Eulerjev natanko takrat, ko so vse točke sode stopnje.*

Dokaz. Dokazovali bomo s pomočjo matematične indukcije po številu povezav m. Pri $m = 0$ je G enak K_1, ta je Eulerjev. Iz G odstranimo cikel C in dobimo nov graf H, kateri ima spet vse točke sode stopnje. Po indukcijski predpostavki je vsaka njegova komponenta Eulerjev graf. Poiščimo zdaj Eulerjev obhod v G. Začnemo v katerikoli točki v cikla C in se sprehajamo po njem, dokler ne pridemo do prve komponente grafa H. Potem opravimo Eulerjev obhod te komponente in se vrnemo na cikel C. Tako nadaljujemo vzdolž C-ja in vsakič, ko pridemo do komponente grafa H, naredimo Eulerjev obhod po njej.

Izrek 19 *Naj bo G povezan graf. G ima Eulerjev sprehod natanko takrat, ko ima največ dve točki lihe stopnje.*

Dokaz.

Fleuryjev algoritem

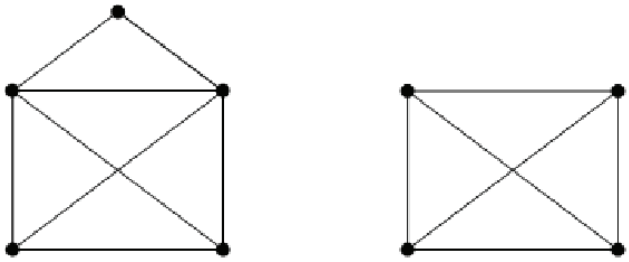
Fleuryjev algoritem najde Eulerjev obhod v Eulerjevem grafu. Algoritem je naslednji:

1. Izberi si začetno točko.
2. Prečkaj poljubno povezavo, le most izberi samo, kadar ni na voljo nobene druge povezave.
3. Prehojeno povezavo odstrani. Prav tako odstrani vse točke, ki so postale izolirane.
4. Končaj, ko ni nobene povezave več.

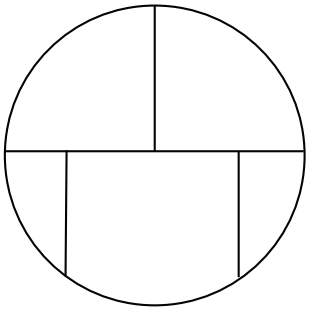
Število potez - razvedrilne naloge iz osnovne šole

Obstoj Eulerjevega sprehoda implicira, da graf lahko narišemo z eno **potezo**.

Nariši v eni potezi vsakega izmed grafov:



Nariši spodnji diagram s čim manj potezami:



Izrek 20 *Naj bo G povezan graf z l lihimi točkami. Število potez, da narišemo G, je $l/2$ za $l > 0$ ter 1 za $l = 0$.*

Dokaz. Če graf nima lihih točk, je Eulerjev, zato ga lahko narišemo z eno potezo.

Naj bo $l > 0$. Očitno mora biti vsaka liha točka krajišče ene poteze. Torej število potez ne more biti manjše od $l/2$.

Naj bodo zdaj $v_1, v_2, \ldots, v_{2k-1}, v_{2k}$ lihe točke grafa G. Grafu G dodamo povezave $v_1v_2, v_3v_4, \ldots, v_{2k-1}v_{2k}$ in tako dobimo nov graf H. Graf H ima vse točke sode stopnje, zato je Eulerjev. Poiščemo Eulerjev obhod v H. Potem odstranimo dodane povezave in obhod grafa H razpade na k poti (oz. potez) grafa G.

Kitajski problem poštarja

Leta 1962 je Meigu Guan podal naslednji problem:

Problem KPP - osnovni: Poišči najkrajši obhod v grafu, ki prehodi vsako povezavo vsaj enkrat.

Motivacija: Poštar želi razdeliti pošto vzdolž ulic enega naselja in se nato vrniti nazaj na pošto. Katero pot naj izbere, da bo najkrajša?

Prevedba na grafih:

- točke grafa so križišča mesta;
- povezave grafa so ulice naselja.

Zgled:

Trditev 21 *Poštar lahko obišče vsako povezavo največ dvakrat.*

Trditev 22 *Naj bo $E(G) = E_1 \cup E_2$, kjer je E_i množica povezav, ki jih poštar prehodi i-krat. Potem je $G - E_2$ največji vpet sod (vsaka točka je sode stopnje) podgraf v G.*

Uteženi kitajski problem poštarja

Naj bo $w : E(G) \to \mathbb{R}^+$

$w(e)$ je **utež** povezave $e \in E(G)$

Paru (G, w) rečemo **uteženi graf**.

Zgled:

Problem KPP - uteženi: Poišči obhod v grafu z najmanjšo skupno težo, ki prehodi vsako povezavo vsaj enkrat.

Hamiltonovi grafi

Vpeti poti v grafu G pravimo **Hamiltonova pot**.

Vpetemu ciklu v grafu G pravimo **Hamiltonov cikel**.

Graf je **Hamiltonov**, če ima Hamiltonov cikel.

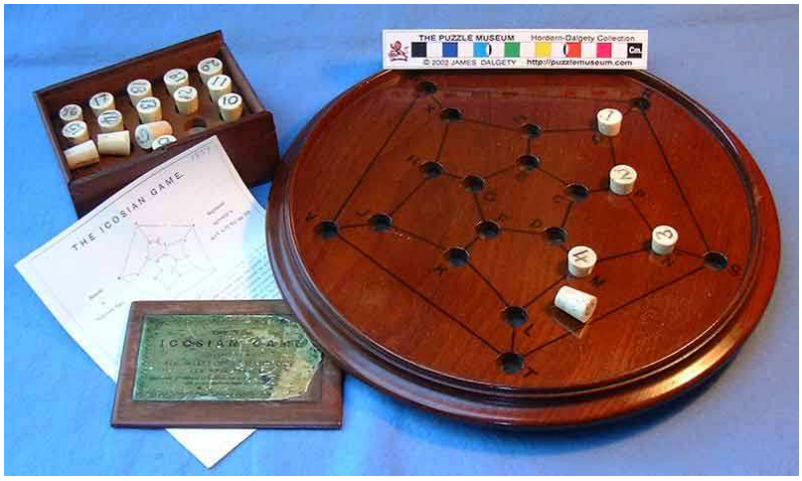
Zgled:

Opomba. Hamiltonova naloga je po svoji formulaciji nekoliko podobna Eulerjevi, a je po svoji zahtevnosti bistveno težja.

Za poljuben graf lahko hitro ugotovimo ali je Eulerjev ali ne. Za ugotavljanje hamiltonosti ni znan noben "preprost" postopek, ki bi bil uporaben za vse grafe.

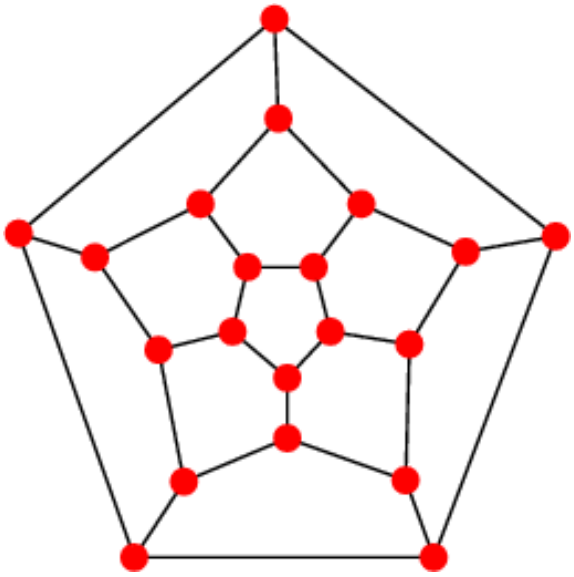
Zgodovina problema

Sir William Rowan Hamilton (1805-1865) - vodilni matematik svojega časa si je izmislil igro: **Potovanje okoli sveta**. Igro je prodal veletrgovcu z igrami za 25 funtov. Igra ni bila komercialno uspešna in kupčija je bila slaba za trgovca.



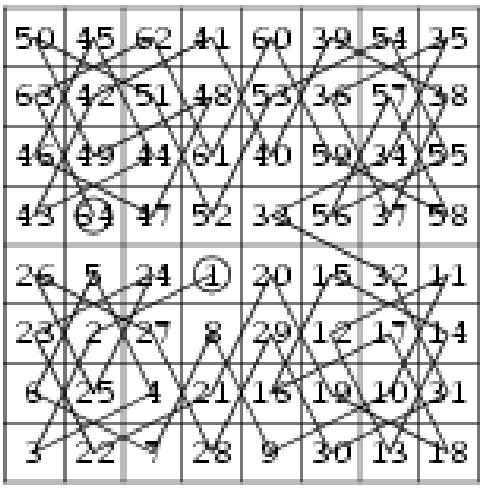
Bistvo igre je poiskati Hamiltonov cikel na dodekaedru, katerega oglišča so označena z začetnimi črkami velemest: Bruselj, Delhi, Zanzibar,... Pri tem je prvih pet črk že izbranih.

Sir Hamilton je pokazal, da vedno obstaja tak cikel, ne glede na izbiro prvih petih zaporednih točk. Problem je rešil s pomočjo ikozaedrskega računa.



Požrešni šahovski konjiček - zgodnejši problem:

Ali lahko skakač obišče vsako polje šahovnice $m \times n$ z zaporedjem skokov in po možnosti zaključi sprehod na začetnem polju?



Problem je ravno iskanje Hamiltonovega cikla. Polja so točke, neko polje pa je povezano z drugim, če lahko skakač iz prvega polja skoči na drugega (črka L).

Zgled:

Potrebni pogoji

Izrek 23 (Osnovni potrebni pogoj) *Če iz grafa G odstranimo k točk in pri tem graf razpade na več kot k komponent, tedaj graf G ni Hamiltonov. Če je komponent več kot $k+1$, potem v grafu G ni niti Hamiltonove poti.*

Dokaz. Recimo, da v grafu G obstaja Hamiltonov cikel oz. pot. Če iz grafa odstranimo k točk, cikel razpade na največ k delov (pomagajmo si s skico), pot pa na največ $k+1$ delov. Vsak od teh delov leži v eni komponenti, na katere razpade graf, in vsaka komponenta vsebuje vsaj en del. Torej graf ne more razpasti na več kot k oz. $k+1$ delov.

□

Zgled:

Posledica 24 *Naj bo G dvodelen graf z razbitjem $V(G) = X \cup Y$. Če je $|X| \neq |Y|$, potem G nima Hamiltonovega cikla. Če velja še $||X| - |Y|| > 1$, potem G ne vsebuje niti Hamiltonove poti.*

Dokaz. Brez izgube splošnosti lahko predpostavimo, da je $|Y| > |X|$. Graf $G - X$ ima potem $|Y|$ komponent in po prejšnjem izreku G ni Hamiltonov. Iz $|Y| \geq |X| + 2$ sledi, da je za graf $G - X$ število komponent $|X| + 2$. Torej graf nima Hamiltonove poti.

□

Zgled:

Zadostni pogoji

Če je neki graf Hamiltonov in mu dodamo še nekaj povezav, potem dobimo spet Hamiltonov graf (Hamiltonov cikel je kar isti kot prej). Torej je za graf z veliko povezavami bolj verjetno, da je Hamiltonov, kot za graf z malo povezavami. Za grafe z "veliko povezavami" poznamo tudi zadostne pogoje za Hamiltonost.

Trditev 25 *Naj bosta u in v taki nesosednji točki grafa G, da je $\deg(u)+\deg(v) \geq |V(G)|$. Potem je graf $G+uv$ Hamiltonov natanko tedaj, ko je G Hamiltonov.*

Dokaz. ($\Rightarrow$) Očitno. Hamiltonov cikel v G je tudi Hamiltonov cikel v $G+uv$.
($\Leftarrow$) Recimo, da je $G+uv$ Hamiltonov. Naj bo C Hamiltonov cikel v $G+uv$. Če povezava uv ni na ciklu, potem je to cikel tudi v G. Zato predpostavimo, da je povezava uv na ciklu C. Zaradi tega je $P = C - uv$ Hamiltonova pot v G. Trdimo, da obstajata zaporedni točki x, y na poti od u do v tako, da je $u \sim y$ in $x \sim v$. Če obstajata taka x in y, potem $u\,P\,x$, xv, $v\,P\,y$, yu tvorijo Hamiltonov cikel. (Pozor: $a\,P\,b$ pomeni kos poti P med točkama a in b) Dokažimo obstoj x in y: Točka u ima $\deg(u)$ sosedov. Recimo, da točka v ni sosednja nobenemu predhodniku teh točk. Za sosede točke v lahko ostane le $|V(G)| - \deg(u) - 1 < \deg(w)$ kandidatov. To pa je protislovje.

□

Izrek 26 (Orejev izrek) *Naj ima graf G vsaj tri točke in naj za poljubni nesosednji točki u in v velja* $\deg(u)+\deg(v) \geq |V(G)|$. *Potem je G Hamiltonov.*

Dokaz. Grafu G dodajamo povezave:

$$G_0 := G, \qquad G_1 = G_0 + u_0v_0, \qquad G_2 = G_1 + u_1v_1, \qquad \ldots \qquad G_p = K_n.$$

Graf G_p je poln graf, zato je Hamiltonov. Iz prejšne trditve sledi, da so vsi grafi G_i Hamiltonovi. Torej je G Hamiltonov.

□

Izrek 27 (Diracov izrek) *Če ima graf G vsaj tri točke in velja* $\deg(w) \geq \frac{1}{2}|V(G)|$ *za vsako točko w, potem je G Hamiltonov.*

Dokaz. Naj za vsako točko w grafa G velja $\deg(w) \geq \frac{|V(G)|}{2}$. Sledi $\deg(u) + \deg(v) \geq \frac{|V(G)|}{2} + \frac{|V(G)|}{2} = |V(G)|$. Po Orejevem izreku sledi, da je G Hamiltonov.

□

Naloga 18 *Ugotovi, ali ima Petersenov graf Hamiltonovo pot oz. cikel.*

Problem trgovskega potnika

Problem 5 *Za dani uteženi polni graf poišči Hamiltonov cikel z najmanjšo utežjo.*

Motivacija: Trgovski potnik želi obiskati nekaj mest in se vrniti v začetno točko tako, da bo vsako mesto obiskal natanko enkrat in bo skupni strošek potovanja najmanjši.

Zgled:

Opomba: Problem trgovskega potnika je posplošitev Hamiltonovega problema.

Grayeve kode

Cikličnemu zaporedju 2^n bajtov, vsak dolžine n bitov, rečemo **Grayeva koda**, če se poljubna dva zaporedna bajta razlikujeta samo v enem bitu.

Te kode so dobile ime po fiziku Franku Grayu (iz Bellovih laboratorijev), ki jih je izumil leta 1953. Grayeve kode imajo široko uporabo v elektrotehniki.

Zgled:

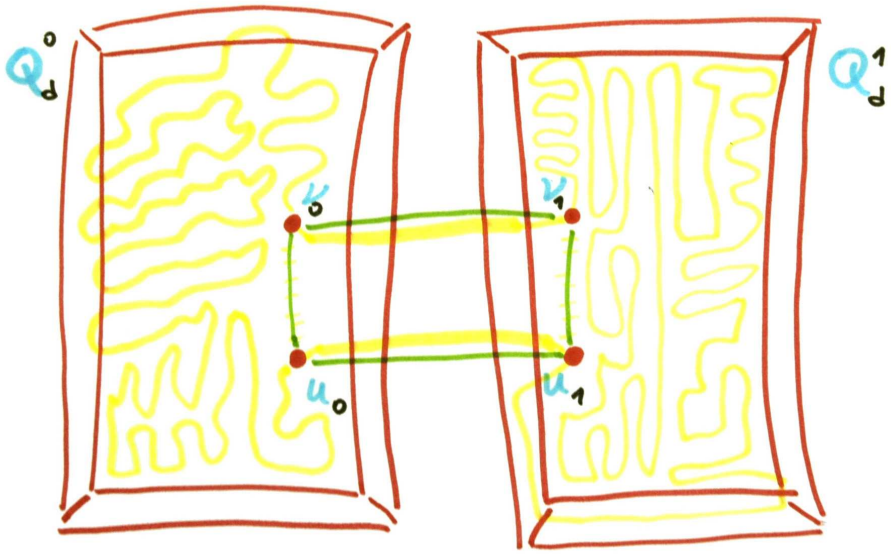
$$000 - 100 - 110 - 010 - 011 - 111 - 101 - 001$$

Opomba: Grayeve kode lahko generiramo kot Hamiltonove cikle hiperkock.

Zgled:

Izrek 28 *Vsaka hiperkocka Q_d $(d \geq 2)$ je Hamiltonov graf.*

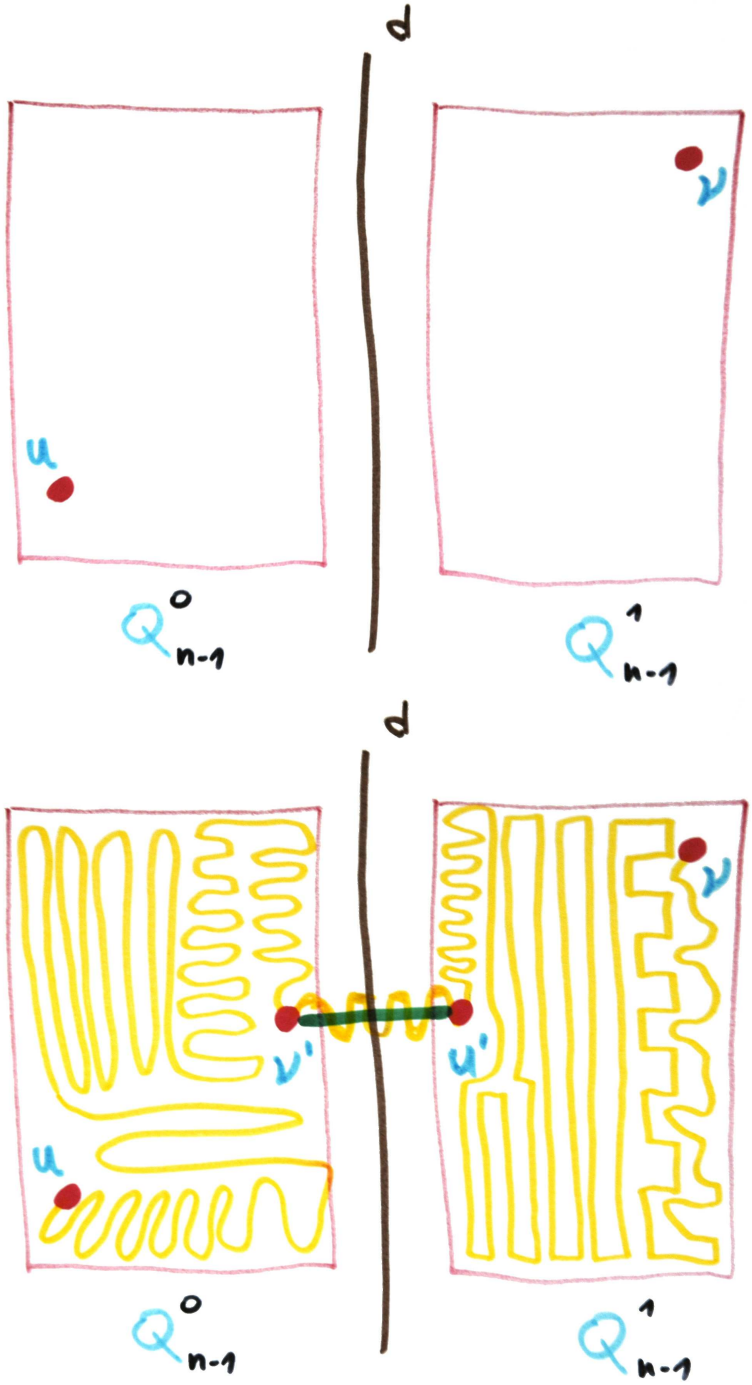
Dokaz. Z indukcijo po d. Preverimo za $d = 2$ ter pokažemo trditev za $d + 1$ ob predpostavki, da velja za d.



□

Vprašanje 1 *Naj bosta u, v dve poljubni točki v Q_n. Ali vedno obstaja Hamitonova pot med u in v?*

Dokaz. Radi bi podobno kot prej pokazali z indukcijo po n.



Domneva Kreverasa. *Naj bo M popolno prirejanje v hiperkocki Q_d ($d \geq 2$). Potem naj bi vedno obstajala Grayeva koda, ki vsebuje vse povezave prirejanja M!*

Usmerjeni grafi - Digrafi

Usmerjena povezava: $a \to b$

Grafu D rečemo **usmerjeni graf** oz. **digraf**, če ima vse povezave usmerjene.

$V(D)$ je **množica točk** digrafa D.

$A(D)$ je **množica usmerjenih povezav** digrafa D.

Zgled:

Usmerjena pot $\overrightarrow{P_n}$

Usmerjeni cikel $\overrightarrow{C_n}$

Temeljni graf

Iz digrafa D lahko dobimo **temeljni graf** G tako, da iz D odstranimo vse usmeritve oz. da usmerjene povezave nadomestimo z neusmerjenimi.

Zgled:

D je **enostaven**, če nima vzporednih povezav in zank.

Trditev 29 *Če je temeljni graf digrafa enostaven, je tudi digraf enostaven.*

Dokaz. Naj bo D digraf, G pa njegov temeljni graf. Ker v G ni vzporednih povezav in zank, jih tudi v D ni. □

Opomba: Obratno ne velja. Digraf D je lahko enostaven, temeljni graf G pa ne.

Vhodna in izhodna stopnja

Naj bo $x \in V(D)$.

Izhodna stopnja $d^+(x)$ je število povezav z začetkom v x.

Vhodna stopnja $d^-(x)$ je število povezav s koncem v x.

Zgled:

Lema 30 (Lema o rokovanju) *V digrafu D velja*

$$\sum_{x \in V(D)} d^+(x) = \sum_{x \in V(D)} d^-(x) = |A(D)|.$$

Dokaz. Najprej preštejemo vse povezave ne glede na njihovo usmerjenost. Vsako povezavo štejemo le enkrat in tako dobimo moč množice $A(D)$. Enako dobimo, če štejemo samo vhodne povezave. Tudi če bi prešteli konce vseh usmerjenih povezave, bi dobili enako. To pa je ravno vsota vseh vhodnih stopenj.

□

Matrike digrafov

D digraf

$V(D) = \{v_1, v_2, \ldots, v_n\}$

$A(D) = \{e_1, e_2, \ldots, e_m\}$

Matrike sosednosti $A(D)$

$$A(D) = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \qquad a_{ij} = \begin{cases} 1, & \text{če } v_i \to v_j \\ 0, & \text{sicer.} \end{cases}$$

Incidenčna matrika $B(D)$

$$B(D) = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} & \ldots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{nm} \end{bmatrix} \qquad b_{ij} = \begin{cases} 1, & \text{če gre } e_j \text{ iz } v_i, \\ -1, & \text{če gre } e_j \text{ v } v_i, \\ 0, & \text{sicer.} \end{cases}$$

Povezanost digrafov

Digraf D je **povezan**, če je njegov temeljni graf povezan. V nasprotnem je **nepovezan**.

Digraf je **krepko povezan**, če v njem obstaja usmerjena pot med poljubnim urejenim parom točk.

Zgled:

Naloga 19 *Temeljni graf krepko povezanega digrafa je brez mostov.*

Rešitev:

Izrek 31 *Naj bo G neusmerjen graf. Povezave grafa G je možno usmeriti, da dobimo krepko povezan digraf natanko takrat, ko je G brez mostov.*

Sprehodi v digrafih

Naslednje pojme definiramo enako kot pri neusmerejenih grafih

- usmerjen sprehod
- usmerjen obhod
- usmerjen cikel
- usmerjena pot

z edino razliko, da se po povezavah lahko premikamo le tako kot so usmerjene.

Lema +. *Če je izhodna stopnja vsake točke digrafa D strogo večja od 0, potem D vsebuje usmerjen cikel.*

Dokaz. Izberimo si poljubno točko v_1 digrafa D. Ker je izhodna stopnja vsake točke digrafa strogo večja od nič, mora obstajati usmerjena povezava z začetkom v točki v_1 in koncem v neki točki v_2. Kar je veljalo za točko v_1, velja tudi za točko v_2 in za vse naslednje točke. Tako dobimo sprehod $v_1, v_2, \ldots, v_i, v_{i+1}, \ldots, v_k, \ldots$ v digrafu D. Vseh točk je končno, iz česar sklepamo, da se morajo točke našega sprehoda začeti ponavljati, recimo $v_i = v_k$. Potem je $v_i, v_{i+1}, \ldots, v_{k-1}$ usmerjen cikel.

□

Lema −. *Če je vhodna stopnja vsake točke digrafa D strogo večja od 0, potem D vsebuje usmerjen cikel.*

Naloga 20 *Naj bodo vse točke grafa G sode. Usmeri vse povezave grafa G tako, da v usmerjenem grafu D, ki ga dobiš, velja*

$$d^+(v) = d^-(v),$$

za vsako točko $v \in V(D)$.

Eulerjevi digrafi

Usmerjen sprehod/obhod je **Eulerjev**, če vsebuje vse usmerjene povezave digrafa.

Povezan digraf je **Eulerjev**, če ima usmerjen Eulerjev obhod.

Zgled:

Naslednja izreka sta zelo podobna "ekvivalentnim" izrekom za neusmerjene grafe.

Izrek 32 *Naj bo D povezan digraf. Potem je D Eulerjev natanko takrat, ko sta vhodna in izhodna stopnja vsake točke enaki.*

Izrek 33 *D ima Eulerjev sprehod natanko takrat, ko velja*

- *D je Eulerjev; ali*
- *Obstajata dve točki a in b v D tako, da je*

$$d^+(a) = d^-(a) + 1 \text{ in } d^-(b) = d^+(b) + 1,$$

ter za vsako drugo točko $v \in V(D)$ velja $d^+(v) = d^-(v)$.

Hamiltonovi digrafi

Povezan digraf D je **Hamiltonov**, če ima usmerjen cikel, ki vsebuje vse točke digrafa. Tak cikel imenujemo **Hamiltonov cikel**.

Hamiltonova pot v digrafu je usmerjena pot, ki vsebuje vse točke tega digrafa.

Zgled:

Izrek 34 (Diracov izrek) *Naj bo D enostaven digraf z $n \geq 3$ točkami. Če za vsako točko v velja*

$$d^+(v) \geq \frac{n}{2} \quad in \quad d^-(v) \geq \frac{n}{2},$$

potem je D Hamiltonov.

Izrek 35 (Orejev izrek) *Naj bo D enostaven digraf z $n \geq 3$ točkami. Če za vsak par točk x in y, tako da ni nobene povezave iz x v y, med katerima ni povezave*

$$d^+(x) + d^-(y) \geq n,$$

potem je D Hamiltonov.

Turnirji

Turnir T je digraf, katerega temeljni graf je poln graf.

Zgled:

Motivacija: Iz športnih turnirjev, kjer vsak igralec igra z vsakim ter neodločen izid ni možen, recimo tenis. Usmerjena povezava $a \to b$ v turnirju pomeni, da igralec a **premaga** igralca b.

Naloga 21 (*a*) *Poišči vse turnirje na dveh oz. treh točkah.*

(*b*) *Poišči vse turnirje z dvema oz. tremi udeleženci (udeležence ločimo, točk pa ne).*

Trditev 36 *Število turnirjev z n udeleženci je $2^{\binom{n}{2}}$.*

Dokaz. Ker ima temeljni graf turnirja na n točkah $\binom{n}{2}$ povezav in vsako tako povezavo lahko usmerimo na dva načina.

□

Izhodna stopnja $d^+(a)$ pomeni **število zmag** igralca a.

Vhodna stopnja $d^-(a)$ pomeni **število porazov** igralca a.

Če je $d^-(a) = 0$, potem je igralec a **zmagovalec** turnirja.

Če je $d^+(a) = 0$, potem je igralec a **poraženec** turnirja.

Naloga 22 *Pokaži, da ima turnir lahko največ enega zmagovalca in največ enega poraženca.*

Tranzitivni turnirji

Turnir T je **tranzitiven**, če za poljubno trojico točk a, b, c velja pogoj: če sta ab in bc usmerjeni povezavi v T, potem je tudi ac usmerjena povezava v T.

Pogoj tranzitivnosti krajše zapišemo takole:

$$\forall\, a, b, c \in V(T) : a \to b \;\text{ in }\; b \to c \;\Rightarrow\; a \to c \qquad (1)$$

Zgled:

Trditev 37 *Turnir T je tranzitiven natanko takrat, ko ne vsebuje nobenega cikla.*

Dokaz. ($\Leftarrow$). Recimo $a \to b$ in $b \to c$. Ker T ne vsebuje ciklov, v T ni povezave $c \to a$. Torej, povezava $a \to c$ je v T. Tako smo pokazali tranzitivni pogoj (1).
($\Rightarrow$). Recimo, da je $a_1 a_2 \cdots a_n a_1$ cikel v T. Torej $a_n \to a_1$. Ker $a_1 \to a_2$ in $a_2 \to a_3$ sledi $a_1 \to a_3$. Podobno iz $a_1 \to a_3$ in $a_3 \to a_4$ sledi $a_1 \to a_4$. Podobno pokažemo, da a_1 premaga $a_4, a_5, \ldots$, ter a_n. A to je protislovje, ker $a_n \to a_1$.

□

Trditev 38 *V tranzitivnem turnirju T zmeraj obstajata zmagovalec in poraženec.*

Dokaz. Recimo, da v T nimamo poraženca. Potem gre iz vsake točke $a \in V(T)$ vsaj ena povezava ven, tj. $\delta^+(G) \geq 1$. Zdaj pa po Lemi + sklepamo, da T vsebuje usmerjen cikel. To pa je v protislovju s prejšno trditvijo.

□

Lestvica je razvrstitev $X_1, X_2, \ldots, X_n$ vseh udeležence turnirja T po nekem kriteriju.

Trditev 39 *Naj bo T tranzitiven turnir z n udeleženci. Potem obstaja lestvica $X_1, X_2, \ldots, X_n$ tako, da X_i premaga vse udeležence, ki mu sledijo na lestvici.*

Dokaz. Po prejšnji trditvi v T obstaja zmagovalec turnirja. Označimo tega udeleženca z X_1.

Zdaj pa obravnavamo turnir $T - X_1$. Ta je tudi tranzitiven, zaradi tega ima zmagovalca, recimo to je X_2.

Potem obravnavamo turnir $T - X_1 - X_2$, pa naj bo X_3 zmagovalec tega turnirja. Postopek ponovimo na $T - X_1 - X_2 - X_3$ in tako naprej.

Na ta način zgeneriramo lestvico $X_1, X_2, \ldots, X_n$ za katero velja, da X_i premaga vse udeležence, ki mu sledijo na lestvici.

□

Naloga 23 *Koliko je tranzitivnih turnirjev na n točkah? Koliko pa z n udeleženci?*

Problem 6 *Ali vedno obstaja lestvica tako, da je vsak udeleženec premagal tistega, ki mu na tej lestvici neposredno sledi.*

Izrek 40 *Vsak turnir ima usmerjeno Hamiltonovo pot.*

Dokaz. Z indukcijo po številu točk n. Izrek očitno velja za $n = 1$. Predpostavimo, da tudi velja za vsak turnir na n točkah. Pokažimo v nekaj korakih, da velja tudi za poljubni turnir T na $n + 1$ točkah $a_1, a_2, \ldots, a_{n+1}$.

1. Odstranimo točko a_{n+1} iz turnirja in tako dobimo turnir $T^* = T - a_{n+1}$ na n točkah. Po indukcijski predpostavki izrek velja za T^*. Torej obstaja usmerjena Hamiltonova pot v T^*, recimo $H = a_1 a_2 \cdots a_{n-1} a_n$.

2. Zdaj točko a_{n+1} vključimo v H tako, da dobimo Hamiltonovo pot v T. Če bi obstajala usmerjena povezava $a_{n+1} \to a_1$, bi imeli Hamiltonovo pot $a_{n+1} a_1 a_2 \cdots a_n$. Zato predpostavimo, da v T obstaja usmerjena povezava $a_1 \to a_{n+1}$.

3. Če bi obstajala povezava $a_{n+1} \to a_2$ v T, bi imeli usmerjeno Hamiltonovo pot $a_1 a_{n+1} a_2 a_3 \cdots a_n$. Zato predpostavimo, da v T obstaja usmerjena povezava $a_2 \to a_{n+1}$.

4. Podobno sklepamo, da v T obstajajo povezave $a_{n+1} \to a_3$, $a_{n+1} \to a_4$, $\cdots$, $a_{n+1} \to a_n$. Od tod pa takoj dobimo, da je $a_1 a_2 \ldots a_n a_{n+1}$ Hamiltonova pot v T. □

Tepena (oz. **poražena**) **skupina** S turnirja T je podmnožica udeležencev, ki so izgubile vse tekme z vsemi udeleženci iz $T \setminus S$. V tem primeru rečemo, da je $T \setminus S$ **zmagovalna skupina**.

Množica povezav med S in $T \setminus S$ je **usmerjen prerez**.

Zgled:

Turnir T je **nerazcepen**, če nima usmerjenih prerezov (oz. nima tepene skupine), sicer je **razcepen**.

Naloga 24 *Pokaži, da v nerazcepnem turnirju nimamo niti zmagovalca niti poraženca.*

Naloga 25 *Ali obstaja turnir, ki je hkrati nerazcepen in tranzitiven?*

Izrek 41 *Turnir T je Hamiltonov natanko takrat, ko je nerazcepen.*

Dokaz. ($\Rightarrow$): Če je T razcepen, potem obstaja tepena skupina A v T. Iz množice A ne moremo priti v zmagovalno skupino B, saj iz množice A ne obstaja nobena povezava, ki bi bila usmerjena navzven iz te množice. Torej ne obstaja usmerjen Hamiltonov cikel v T.

($\Leftarrow$): Naj bo T nerazcepen. Dokaza se lotimo s protislovjem, t.j. predpostavimo, da turnir T ni Hamiltonov.

Trdimo: *Za vsako točko $a \in V(T)$ velja $d^+(a) > 0$.* Sicer, če bi obstajala točka a, za katero to ne velja, potem bi bila množica $\{a\}$ tepena.

Zdaj, po Lemi + sledi, da v T obstaja usmerjen cikel. Naj bo $C = v_1v_2 \cdots v_nv_1$ najdaljši usmerjen cikel v T. Če bi bil C Hamiltonov, bi prišli do protislovja in tako bi bil izrek že dokazan. Zato predpostavimo, da obstajajo točke turnirja T, ki niso v C.

Te točke razdelimo v tri skupine:

- A_1 - udeleženci, ki so z nekaterimi udeleženci cikla C zmagali, z nekaterimi pa izgubili.
- A_2 - udeleženci, ki so premagali vse iz C.
- A_3 - udeleženci, ki so izgubili z vsemi iz C.

Ker C ni Hamiltonov, sledi $A_1 \cup A_2 \cup A_3 \neq \emptyset$.

Trdimo: *A_1 je prazna množica.* Sicer obstaja $a_1 \in A_1$. Lahko najdemo dve sosednji točki $v_i \in C$ in $v_{i+1} \in C$ tako, da obstajata usmerjeni povezavi $v_i a_1$ in $a_1 v_{i+1}$. Tako dobimo usmerjen cikel $C' = v_1 v_2 \cdots v_i a v_{i+1} \cdots v_n v_1$, ki je daljši od C, to pa je protislovje.

Trdimo: $A_2 = \emptyset \Leftrightarrow A_3 = \emptyset$. Če je $A_2 = \emptyset$, je A_3 tepena skupina. To je v nasprotju s predpostavko, da je T nerazcepen, zato je tudi $A_3 = \emptyset$. Če je $A_3 = \emptyset$, je A_2 zmagovalna skupina. Ker je T nerazcepen, je to protislovje.

Ker $A_1 \cup A_2 \cup A_3 \neq \emptyset$, tudi A_2 in A_3 ne bosta prazni (saj smo že ugotovili, da je A_1 prazna). Torej, obstajata $a_2 \in A_2$ in $a_3 \in A_3$ tako, da a_3 premaga a_2 (Če to ne bi držalo, bi bila A_3 tepena skupina). Sedaj razširimo C na $C^+ = v_1 v_2 \cdots v_i a_3 a_2 v_{i+1} \cdots v_n v_1$.

Dobili smo usmerjen cikel C^+, ki je daljši od cikla C. Prišli smo v protislovje, torej je C usmerjen Hamiltonov cikel v T. Tako sklepamo, da je T Hamiltonov. □

Povezanost grafov

Grafu G rečemo, da je **povezan**, če za vsak par točk u, v iz G obstaja pot od točke u do točke v.

Točko v grafa G imenujemo **prerezna točka**, če ima graf $G - v$ več komponent kot G.

Podobno imenujemo povezavo e grafa G **prerezna povezava** ali **most**, če z odstranitvijo te povezave dobimo graf z več komponentami, kot jih je imel prvotni graf G.

Prerezna množica povezav je množica $F \subseteq E(G)$ tako, da ima graf $G - F$ več komponent kot G.

Prerezna množica točk je množica $S \subseteq V(G)$ tako, da ima graf $G - S$ več komponent kot G.

Zgled:

Povezanost po točkah

Graf G je **k-povezan (po točkah)** (za $k \in \mathbf{N}$), če velja

- G ima vsaj $k+1$ točk, ter
- za vsako množico točk $K \subseteq V(G)$ moči $|K| < k$, je graf $G - K$ povezan.

Vprašanje 2 *Kateri so* 0*-povezani in kateri so* 1*-povezani grafi?*

Odgovor:

Vprašanje 3 *Za katere k je hiperkocka Q_3 k-povezan graf?*

Odgovor:

Največje število k, za katero je graf k-povezan, imenujemo **povezanost** grafa G in ga označimo s $\kappa(G)$.

Vprašanje 4 *Kolikšna je $\kappa(Q_3)$?*

Odgovor:

Lastnosti 42 *Pri k-povezanosti velja naslednje:*

(a) $\kappa(G) = 0$ *natanko tedaj, ko je G nepovezan.*

(b) *Če v k-povezanem grafu dodamo novo povezavo, graf ostane k-povezan.*

(c) *V k-povezanem grafu je vsaka točka stopnje $\geq k$.*

(d) *Če velja $k_1 \leq k_2$ in je G k_2-povezan, potem je G tudi k_1-povezan.*

Odgovor: (Trditve so manj ali več očitne.)

Problem 7 *Izračunaj $\kappa(C_n)$, $\kappa(K_n)$ ter $\kappa(K_{n,m})$.*

Rešitev:

Vprašanje 5 *Kateri je najmanjši k-povezan graf?*

Odgovor:

Trditev 43 (Dodajanje točke) *Naj bo G k-povezan graf in označimo z G' graf, ki ga konstruiramo iz grafa G tako, da mu dodamo eno novo točko y z vsaj k sosedi v G. Potem je graf G' k-povezan.*

Dokaz. Dokažimo, da mora poljubna prerezna množica točk S grafa G' imeti moč vsaj k. Recimo, da to ne drži, tj. $|S| < k$. Ločimo naslednje možnosti:

1. Če je $y \in S$, potem množica $S \setminus \{y\}$ razbije graf G. To pa ni možno, ker je graf G k-povezan.

2. Če $y \notin S$ in $N(y) \subseteq S$ (vsi sosedi točke y so vsebovani v množici S), potem je $|S| \geq k$, saj je sosedov po predpostavki vsaj k.

3. Če izključimo prvi dve možnosti, potem točka y in točke iz $N(y) \setminus S$ ležijo v eni komponenti grafa $G' - S$, ki pa ni povezan. Torej mora množica S ločiti tudi graf G. Od tukaj pa dobimo $|S| \geq k$.

□

Povezanost po povezavah

Graf G je **l-povezan po povezavah** (za $l \in \mathbf{N}$), če je za vsako množico povezav $S \subseteq V(G)$ moči $|S| < l$ graf $G - S$ povezan.

Vprašanje 6 *Kateri grafi so* 0*-povezani oz.* 1*-povezani po povezavah?*

Odgovor:

Vprašanje 7 *Za katere l je Petersenov graf P_{10} l-povezan po povezavah?*

Odgovor:

Največje število l, za katero je graf G l-povezan po povezavah, imenujemo **povezanost po povezavah** grafa G in ga označimo z $\lambda(G)$.

Vprašanje 8 *Kolikšna je $\lambda(P_{10})$?*

Odgovor:

Opomba: Povezanost po povezavah lahko definiramo tudi takole: $\lambda(G)$ grafa G je najmanjše število povezav, brez katerih postane graf G nepovezan.

Spomnimo se, da je $\delta(G)$ minimalna stopnja grafa G.

Naloga 26 *Izračunaj κ, λ, δ za spodnji graf.*

Naloga 27 *Za vsak $n \in \mathbb{N}$ poišči graf G, za katerega velja $\kappa(G) = \lambda(G) = \delta(G) = n$.*

Trditev 44 *Za vsak povezan graf G velja*

$$\kappa(G) \leq \lambda(G) \leq \delta(G).$$

Dokaz. Naj ima točka v stopnjo $\delta(G)$ ter naj bo F množica vseh incidenčnih povezav točke v. Graf $G - F$ je nepovezan. Torej velja $\lambda(G) \leq \delta(G)$.

Pokažimo drugo neenakost. Naj bo S prerezna množica povezav moči $\lambda(G)$. Če torej odstranimo te povezave, postane graf $G - S$ nepovezan. Ampak te povezave lahko odstranimo tudi tako, da odstranimo po eno krajišče vsake od teh povezav. Pri odstranitvi točk pazimo, da ne odstranimo vseh točk bodisi v levi množici oz. v desni množici. Takšnih točk je največ $\lambda(G)$, zato velja $\kappa(G) \leq \lambda(G)$.

□

Bloki in 2-povezani grafi

Blok grafa G je maksimalen povezan podgraf brez prereznih točk.

Zgled:

Vprašanje 9 *Kaj so bloki v drevesu?*

Odgovor:

Trditev 45 *Vsak blok B poljubnega grafa G je*

1. *izolirana točka v G; ali*
2. *most v G; ali*
3. *maksimalen 2-povezan podgraf v G.*

Dokaz.

□

Trditev 46 *Veljajo naslednje trditve:*

1. *Če je graf G povezan in nima prereznih točk, potem je sam graf G blok.*
2. *Bloki so po povezavah disjunktni, lahko pa imajo skupne točke. Te so natanko prerezne točke.*
3. *Povezava je blok natanko tedaj, ko je prerezna povezava.*
4. *K_1 ali K_2 sta edina grafa brez prereznih točk, ki nista 2-povezana.*

Dokaz.

□

Trditev 47 (Opis 2-povezanih grafov) *Za graf G na vsaj treh točkah so naslednje trditve ekvivalentne:*

(a) Graf G je 2-povezan.

(b) Graf G ima samo en blok.

(c) Vsak par točk x, y grafa G leži na skupnem ciklu.

(d) Med vsakim parom točk x, y grafa G obstaja par notranje disjunktnih poti.

(e) $\delta(G) \geq 1$ in vsak par povezav grafa G leži na skupnem ciklu.

Dokaz. (Podamo le skico dokaza.)

□

Izrek 48 (Ušesna dekompozicija) *Graf G je 2-povezan natanko tedaj, ko ga lahko zapišemo v obliki*

$$G = C \cup P_1 \cup P_2 \cup \cdots \cup P_k,$$

kjer je C cikel ter so $P_1, P_2, \ldots, P_k$ poti v G, pri čemer ima P_i ima $C \cup P_1 \cup P_2 \cup \cdots \cup P_{i-1}$ skupni natanko obe svoji krajišči.

Dokaz. (Podamo le skico dokaza.)

□

Zgled:

Mengerjev izrek

Naj bo G povezan graf in x, y točki v G.

(x, y)**-pot** je pot v grafu G med točkama x in y.

Dve (x, y)-poti sta **disjunktni po povezavah**, če nimata skupne povezave.

Dve (x, y)-poti sta **disjunktni po točkah**, če nimata nobene skupne točke poleg x in y.

Zgleda:

Izrek 49 (Mengerjev izrek za povezave) *Povezan graf G je k-povezan po povezavah natanko tedaj, ko je med poljubnim parom točk vsaj k po povezavah disjunktnih poti.*

Dokaz. (Naredimo dokaz le v lažjo smer.)

□

Izrek 50 (Mengerjev izrek za točke) *Povezan graf G je k-povezan po točkah natanko tedaj, ko je med poljubnim parom točk vsaj k po točkah disjunktnih poti.*

Dokaz. (Naredimo dokaz le v lažjo smer.)

□

Zgledi:

Ravninski grafi

Naloga iz osnovne šole: Dane so tri hiše ter tri drevesa na travniku. Poveži vsako hišo z vsakim drevesom s potjo, ne da bi se poti sekale.

Vprašanje 10 *Ali lahko dani graf (recimo $K_{3,3}$) narišemo v ravnini brez križanja povezav?*

Graf je **ravninski**, če se ga da narisati v ravnini brez sekanja povezav, razen v skupnih krajiščih.

Tako risanje je **ravninska vložitev** grafa G.

Zgledi:

Vložitev grafa razdeli ravnino na povezane dele, ki jim pravimo lica. Eno od teh lic je neomejeno in ga imenujemo **zunanje lice**.

Množico lic grafa G označimo z $F(G)$.

Dolžina lica f je število povezav, ki ležijo na robu lica (pri tem upoštevamo večkratnost) in jo označimo z $l(f)$.

Zgled:

Za poljuben graf velja lema o rokovanju, za ravninske grafe pa poznamo še eno različico:

Lema o rokovanju za ravninske grafe. *Za vsak ravninski graf G velja*

$$\sum_{f \in F(G)} l(f) = 2\,|E(G)|.$$

Dokaz. Vsaka povezava grafa G meji na natanko dve lici grafa G. Če seštejemo dolžine vseh lic v grafu G, bo torej vsaka povezava šteta natanko dvakrat. Odtod sledi:

$$\sum_{f \in F(G)} l(f) = 2|E(G)|.$$

□

Eulerjeva formula

Izrek 51 (Euler) *Če ima povezan (multi)graf G n vozlišč, e povezav in f lic, potem velja*

$$n - e + f = 2. \tag{2}$$

Dokaz. Z indukcijo po številu vozlišč n. Če je $n = 1$, potem ima graf G eno vozlišče, povezave, če so, pa so zanke. Če je $e = 0$, potem je $f = 1$ in (2) drži. Z vsako dodano zanko na licu se lice razdeli na dva dela. S tem se poveča število povezav in število lic za 1. Torej tudi v tem primeru (2) velja.

Indukcijski korak za $n > 1$: Ker je G povezan, lahko najdemo povezavo, ki ni zanka. Ko tako povezavo skrčimo, dobimo ravninski graf G' z n' vozlišči, m' povezavami in f' lici. Skrčitev ne spremeni število lic, zmanjša pa se število povezav in vozlišč za 1. Torej je $n' = n - 1$, $e' = e - 1$, $f' = f$ in od tod sledi $n - e + f = n' + 1 - (e' + 1) + f' = n' - e' + f' = 2$. □

Zgled:

Trditev 52 *Naj bo G ravninski graf z Ω komponentami. Pokaži, da velja:*

$$|V(G)| - |E(G)| + |F(G)| = 1 + \Omega.$$

Dokaz. Če ima ravninski graf G Ω komponent, potem z dodanimi $\Omega - 1$ povezavami G postane povezan graf, kateremu nismo spremenili število lic. Torej je Eulerjeva formula posplošena za ravninske grafe z Ω komponentami $n - e + f = 2 + \Omega - 1 = \Omega + 1$.

□

Posledica 53 *Vse ravninske vložitve grafa G imajo enako število lic.*

Dokaz. Trditev takoj sledi iz Eulerjeve formule.

Trditev 54 *Če je G enostaven ravninski graf z n vozlišči, e povezavami in f lici ter z vsaj tremi vozlišči, je*

$$e \leq 3n - 6.$$

Če pa je G brez trikotnikov, potem velja

$$e \leq 2n - 4.$$

Dokaz. Dovolj je pogledati za povezane grafe (drugače pa jim dodamo povezave). Če je $n \geq 3$, potem vsako lice v enostavnem grafu vsebuje najmanj 3 povezave in tako dobimo $2e \geq 3f$. Če to zdaj upoštevamo v Eulerjevi formuli, dobimo $e \leq 3n - 6$.

Če G nima trikotnikov, to pomeni, da imajo lica dolžino vsaj 4. V tem primeru pa velja $2e =\geq 4f$ in dobimo po Eulerjevi formuli $e \leq 2n - 4$.

□

Vprašanje 11 *Za katere grafe imamo enačaj v prvi oz. drugi neenačbi?*

Posledica 55 *Grafa K_5 in $K_{3,3}$ nista ravninska.*

Dokaz. Za K_5 imamo $e = 10 > 9 = 3n - 6$. Ker je graf $K_{3,3}$ brez trikotnikov, imamo $e = 9 > 8 = 2n - 4$. Torej imata grafa preveč povezav, da bi bila ravninska.

□

Posledica 56 *Enostavni ravninski graf ima točko stopnje* ≤ 5.

Dokaz. Recimo, G je ravninski graf na n točkah, ki so vse stopnje ≥ 6. Potem velja

$$6\,n \leq \sum_{v \in V(G)} \deg(v) = 2|E(G)| \leq 6\,n - 12.$$

Dualni graf

Dualni graf G^* ravninskega grafa G je ravninski graf, ki ga dobimo tako, da:

1. v vsako lice f grafa G dodamo vozlišče $f^* \in V(G^*)$;
2. za vsako povezavo e grafa G, ki loči lici f_1 in f_2, povežemo vozlišči f_1^* in f_2^* v G^* s povezavo e^*.

Zgledi: K_4**,** Q_3**,** $K_{2,2,2}$**,** $K_{1,a}$

Iz same definicije ter zgornjih zgledov opazimo naslednje:

- lice velikosti k grafa G ustreza točki stopnje k grafa G^*;
- točka stopnje k grafa G ustreza licu grafa G^*;
- povezava grafa G ustreza povezavi grafa G^*;
- zanka v G ustreza mostu v G^*;
- most v G ustreza zanki v G^*;
- cikel grafa G ustreza minimalnemu prerezu grafa G^*;
- minimalni prerez grafa G ustreza ciklu grafa G^*.

Trditev 57 *Naj bo G povezan ravninski graf z v točkami, e povezavami in f lici. Potem ima njegov dualni graf G^* f točk, e povezav in v lic.*

Dokaz. Trditev sledi hitro iz prejšnih opazk.

□

Problem 8 *Naj bo G^* dual grafa G. Poišči dual grafa G^*.*

Rešitev:

Opomba: Različne vložitve grafa G v ravnino lahko določajo različne dualne grafe.

Preverjanje ravninskosti

Graf H je **minor** grafa G, če ga lahko konstruiramo iz nekega podgrafa grafa G z zaporedjem skrčitev povezav. Pravimo, da je graf G **skrčljiv** na graf H.

Zgled:

Graf H je **subdivizija** grafa G, če ga lahko konstruiramo iz grafa G, tako da nekatere povezave v G nadomestimo s potmi dolžine 2 ali več.

Zgled:

Trditev 58 *Če graf G vsebuje subdivizijo grafa K_5 ali $K_{3,3}$, potem G ni ravninski graf.*

Dokaz. Ker K_5 in $K_{3,3}$ nista ravninska grafa.

□

Trditev 59 *Če graf G vsebuje K_5 ali $K_{3,3}$ kot minor, potem G ni ravninski graf.*

Dokaz. Ker K_5 in $K_{3,3}$ nista ravninska grafa.

□

Velja namreč tudi obrat, kar sta prva dokazala Kuratowski ter Wagner:

Izrek 60 (Wagner) *Graf G je ravninski natanko tedaj, ko ne vsebuje grafa K_5 in $K_{3,3}$ kot minorja.*

Izrek 61 (Kuratowski) *Graf G je ravninski natanko tedaj, ko ne vsebuje subdivizij grafov K_5 ali $K_{3,3}$.*

Zgled:

Posledica 62 *Obstaja algoritem, ki v linearnem številu korakov ugotovi ali je dani graf ravninski.*

Posledica 63 (Stein-Tutte) *Vsak 3-povezan ravninski graf ima ravnočrtno, konveksno vložitev v ravnino.*

Zgled:

Debelina grafa

Najmanjše število ravninskih grafov, iz katerega lahko sestavimo graf G, je **debelina** grafa G in jo označimo s $t(G)$.

Zgledi:

Velja: $t(G) = 1$ natanko takrat, ko je G ravninski.

Opomba: Zanke in vzporedne povezave niso pomembne pri debelini grafa $t(G)$. Zato se omejimo na enostavne grafe.

Spodnja meja za $t(G)$

Ni znana formula za $t(G)$. Enostavno pa se da izračunati spodnjo mejo, ki je zelo pogosto tudi prava.

Izrek 64 *Naj bo G enostaven povezan graf z n točkami in m povezavami. Potem je*

(a) $t(G) \geq \lceil \frac{m}{3n-6} \rceil$;

(b) Če je G brez trikotnikov, potem je $t(G) \geq \lceil \frac{m}{2n-4} \rceil$.

Dokaz. (a) Ker ima ravninski graf $\leq 3n-6$ povezav, rabimo vsaj $\frac{m}{3n-6}$ kosov. Trditev (b) pokažemo podobno.

□

Vprašanje 12 *Kakšne spodnje meje nam zagotovi Izrek 64 za grafe K_5, $K_{3,3}$, P_{10}, K_6.*

Odgovor:

Problem 9 *Kakšne spodnje meje nam zagotovi izrek 64 za grafa K_n, $K_{a,b}$.*

Rešitev:

Formula za $t(K_{a,b})$ ni znana, za K_n pa velja naslednji izrek.

Izrek 65 *Debelina polnega grafa K_n je določena z obrazcem:*

$$t(K_n) = \begin{cases} \lfloor \frac{n+7}{6} \rfloor, & \text{za } n \neq 9, 10; \\ 3, & \text{sicer.} \end{cases}$$

Križno število

Križno število $\mathrm{cr}(G)$ grafa G je najmanjše možno število križanj, če G narišemo v ravnini.

Zgledi:

Velja: $\mathrm{cr}(G) = 0$ natanko takrat, ko je G ravninski.

Opomba: Če se dve povezavi sekata več kot enkrat, se ju da prestaviti tako, da zmanjšamo število presečišč na eno ali nič.

Trditev 66 *Vsak graf se da vedno narisati v ravnini tako, da se poljubni dve povezavi sekata največ enkrat.*

Izrek 67 *Za polni graf K_n velja* $\mathrm{cr}(K_n) \geq \frac{1}{5}\binom{n}{4}$.

Problem 10 *Izračunaj* $\mathrm{cr}(K_6)$.

Barvanja grafov

Graf je k-**obarvljiv**, če obstaja preslikava $c : V(G) \to \{1, \ldots, k\}$ tako, da je $c(u) \neq c(v)$ za poljubni sosednji točki u in v grafa G.

Tako preslikavo imenujemo **barvanje** oziroma k-**barvanje** grafa.

Po domače: obarvaj vsako točko grafa z eno izmed k barv tako, da sta poljubni sosednji točki različno pobarvani.

Zgled:

Trditev 68 *Velja:*

- *1-obarvljivi grafi so natanko grafi brez povezav;*
- *2-obarvljivi grafi so natanko dvodelni grafi.*

Dokaz. Trditvi sta očitni.

□

Kromatično število $\chi(G)$ grafa G je najmanjše število k, za katero je G k-obarvljiv.

Velja:

$$\chi(K_n) = n \quad \text{in} \quad \chi(C_n) = \begin{cases} 2, & \text{za } n \text{ sodo število;} \\ 3, & \text{sicer.} \end{cases}$$

Znani niso nobeni potrebni in zadostni pogoji za to, da je $\chi \leq k$, tj. določitev χ je NP-težak problem. Zanimajo nas zgornje oz. spodnje meje χ.

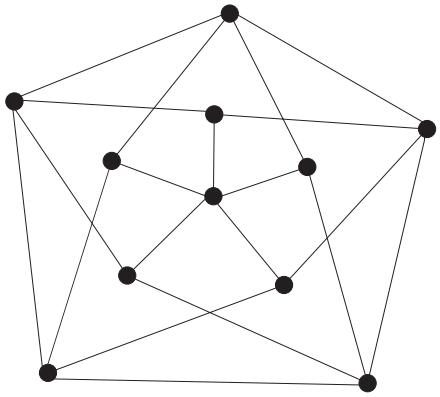
Trditev 69 *Pri barvanju grafov veljajo naslednje lastnosti:*

1. $\chi(G) \leq |V(G)|$ *in enakost velja natanko takrat, ko je* G *poln graf;*
2. *Če je* H *podgraf v* G*, potem je* $\chi(H) \leq \chi(G)$*;*
3. *Če* G *vsebuje kliko na* k *točkah, potem je* $\chi(G) \geq k$*.*

Dokaz. Trditve so manj ali več očitne.

□

Naloga 28 *Pokaži, da za Grötzchev graf* G *velja* $\chi(G) = 4$*.*



Rešitev:

Zveza med Δ in χ

V tem razdelku bomo uporabili okrajšavo $\Delta = \Delta(G)$.

Trditev 70 *Za vsak graf G velja $\chi(G) \leq \Delta + 1$.*

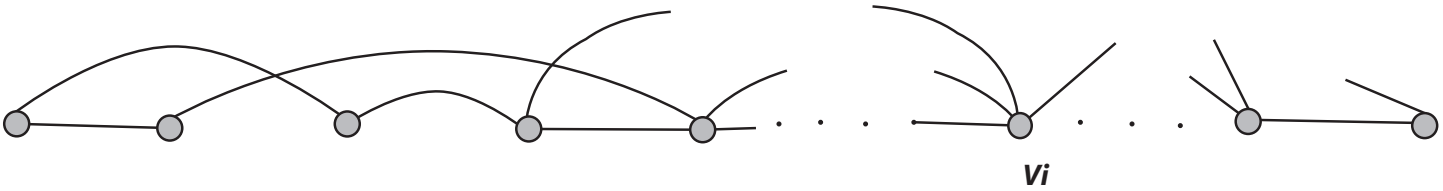
Dokaz. Indukcija po številu točk n grafa G. Očitno velja za $n = 1$. Naj bo $n \geq 2$ in naj bo v poljubna točka v G. Ker je $\Delta(G - v) \leq \Delta$, obstaja barvanje c grafa $G - v$ z $\Delta + 1$ barvami. Točka v ima največ Δ sosedov in vse te točke so že pobarvane.

Ker imamo $\Delta + 1$ barv, je vsaj ena neuporabljena oz. prosta pri sosedih točke v. Uporabimo to barvo na v in tako razširimo barvanje c na cel graf G.

Alternativen dokaz: Točke grafa G linearno razvrstimo

$$v_1 \qquad v_2 \qquad v_3 \qquad \cdots \qquad v_i \qquad \cdots \qquad v_{n-1} \qquad v_n$$

ter v tem vrstnem redu barvamo eno za drugo tako, da vsaki točki priredimo (najmanjšo) prosto barvo. Algoritem pobarva vse točke, ker imamo pri barvanju poljubne točke vsaj eno prosto barvo.



Brooksov izrek

Naloga 29 *Poišči grafe G, za katere velja enačaj $\chi(G) = \Delta + 1$.*

Izrek 71 (Brooks) *Naj bo G graf z maksimalno stopnjo Δ. Če G ni lih cikel niti poln graf na $\Delta + 1$ točkah, potem je $\chi(G) \leq \Delta$.*

Dokaz z uporabo Kempejevih verig $H(a, b)$: Predpostavimo, da je izrek napačen in naj bo G minimalni protiprimer. Ni se težko prepričati, da mora biti $\Delta \geq 3$ ter da je vsaka točka grafa G stopnje Δ. Naj bo n število točk grafa G ter v poljubna točka grafa G. Po minimalnosti obstaja Δ-barvanje grafa $G - v$. V tem barvanju so vse sosede točke v različno obarvane, sicer barvanje lahko razširimo na G. Naj bodo $v_1, v_2, \ldots, v_\Delta$ sosede točke v ter naj bodo ustrezno obarvane z barvami $1, 2, \ldots, \Delta$. Označimo s $H(i, j)$ podgraf grafa G, induciranega s točkami, ki imajo barvo i ali barvo j. Komponento grafa $H(i, j)$, ki vsebuje točko u, označimo s $H_u(i, j)$.

Trditev 1. *Poljubni dve sosedi v_i in v_j točke v sta v isti komponenti grafa $H(i, j)$.*

Če to ni res, potem v komponenti, v kateri je v_i, vse točke z barvo i prebarvamo z barvo j in obratno. Nazadnje v obarvamo z barvo i in dobimo iskano barvanje grafa G.

Trditev 2. *Vsaka točka iz $H_{v_i}(i, j)$, ki je različna od v_i in v_j, je stopnje 2.*

Iz točke v_i se začnimo sprehajati po grafu $H_{v_i}(i, j)$. Naj bo u prva točka, ki jo srečamo, stopnje ≥ 3 ter različna od v_i in v_j. Zagotovo obstaja barva, različna od i in j, s katero ni obarvana nobena od sosed točke u. S to barvo obarvamo točko u in dobimo protislovje iz trditve 1.

Trditev 3. *Za poti $H_{v_j}(i, j)$ in $H_{v_j}(k, j)$ je v_j edina skupna točka.*
Recimo, da je u druga skupna točka teh poti. Tedaj ima točka u štiri sosede, ki so pobarvane z barvami i in k. Zaradi tega obstaja prosta barva, s katero pobarvamo točko u ter dobimo protislovje iz trditve 1.

Ker G ni polni graf, na $\Delta + 1$ točkah obstajata taki v_i in v_j, ki nista sosedi. Naj bo u točka grafa G, ki je obarvana z barvo j ter je sosednja z v_i. Ta točka je različna od v_j. Naj bo $k \neq i$ in $k \neq j$. V $H_{v_i}(i, k)$ točkam zamenjamo barve. V novem barvanju je točka u skupna za poti $H_{v_j}(i, j)$ in $H_{v_j}(k, j)$. To pa nasprotuje trditvi 3 in s tem je dokaz končan.

□

Nekaj zgledov uporabe barvanja grafov

1. V skladišču kemikalij so shranjene kemikalije $C_1, \ldots, C_n$. Zaradi varnosti določene spojine ne smejo biti v istem prostoru. Najmanj koliko ločenih prostorov rabimo v skladišču, da bo shranjevanje varno?

2. Turistična agencija organizira izlete za n skupin. Za vsako skupino vemo, kdaj se njen izlet začne in kdaj se konča. Zanima nas najmanj koliko vodičev potrebuje agencija.

3. Pri letalski družbi poznamo vse polete ter za vsak polet poznamo natančen prihod in odhod letala. Zanima nas minimalno število letal, ki jih agencija potrebuje?

k-degeneriranost

Naj bo G graf in k naravno število. Če je minimalna stopnja vsakega podgrafa H grafa G največ k, potem rečemo, da je G **k-degeneriran**.

Degeneriranost $d(G)$ grafa G je najmanjše število k, za katero je G k-degeneriran t.j.

$$k = \max_{H \subseteq G} \delta(H)$$

Zgled:

Trditev 72 *Če je G k-degeneriran, potem lahko točke grafa razvrstimo*

$$v_1 \quad v_2 \quad v_3 \quad \cdots \quad v_i \quad \cdots \quad v_{n-1} \quad v_n$$

tako, da ima vsaka točka največ k sosedov z manjšim indeksom.

Dokaz. Naj bo G k-degeneriran. G ima točko stopnje največ k. Naj bo to točka v_n (v razvrstitvi jo zapišemo zadnjo). Obravnavamo graf $G - v_n$. Ta graf je prav tako k-degeneriran. Naj bo točka v_{n-1} stopnje največ k (ta točka bo predzadnja v razvrstitvi). Graf $G - v_n - v_{n-1}$ je tudi k-degeneriran in tako nadaljujemo po istem postopku ter razvrstimo vse točke.

□

Trditev 73 *Vsak k-degeneriran graf je $(k+1)$-obarvljiv.*

Dokaz. Po postopku iz prejšnje trditve/dokaza lahko točke razvrstimo tako, da ima vsaka točka največ k povezav do točk z manjšim indeksom. Če barvamo po vrsti, pri posamezni točki v najslabšem primeru dobimo največ k različno obarvanih sosedov, ki so že pobarvani. V tem primeru uporabimo prosto barvo.

□

Posledica 74 *Vsak ravninski graf je 5-degeneriran in zato 6-obarvljiv.*

Dokaz. Naj bo G ravninski graf. Zato ima točko stopnje največ 5 (to smo že pokazali). Vsak njegov podgraf je prav tako ravninski, zato ima tudi stopnjo največ 5. G je 5-degeneriran. Iz prejšne trditve sledi, da je 6-obarvljiv. □

Barvanje zemljevidov

O zgodovini barvanj grafov ne moremo govoriti, ne da bi omenili problem štirih barv. Začelo se je takole. Leta 1852 je Francis Guthrie opazil, da se regionalni zemljevid Anglije da obarvati s štirimi barvami tako, da sta katerikoli dve sosednji regiji različno obarvani. (Regiji sta sosednji le, če imata skupni rob.) Ugotovil je, da so v splošnem potrebne vsaj štiri barve ter je postavil domnevo, da to število barv tudi zadostuje.

Zgled:

Problem štirih barv (Francis Guthrie). *Regije poljubnega zemljevida se lahko obarvajo s štirimi barvami tako, da sta katerikoli dve sosednji regiji različno obarvani.*

Francis Guthrie je povedal zgornjo domnevo svojemu bratu Fredericku. Frederick pa je predstavil ta problem svojemu profesorju DeMorganu. Le-ta je pisal o njem svojemu kolegu Hamiltonu. To pismo je prvi (znani) dokument, v katerem se omenja problem štirih barv.

Problem je bil v celoti pozabljen do leta 1878, ko ga je Artur Cayley omenil članom Londonskega društva matematikov. Leta 1879 je Tait objavil rešitev problema. Tudi Kempe je objavil rešitev. Njuna dokaza pa nista bila popolna. Leta 1890, torej deset let kasneje, je Heawood ugotovil napako v Kempejevem dokazu ter prvi dokazal, da za barvanje zadostuje 5 barv.

Izrek o petih barvah (Heawood). *Vsak ravninski graf je 5-obarvljiv.*

Leta 1969 je Heesch predstavil metodo prenašanja naboja, leta 1977 pa je s to metodo Appelu in Hakenu uspelo rešiti problem. Vendar je dokaz, ki sta ga izpeljala Appel in Haken, zelo dolg ter zahteva računalniško obdelavo podatkov. Bolj enostaven dokaz so našli Robertson, Sanders, Seymour in Thomas, vendar tudi njihov dokaz uporablja računalniško obdelavo podatkov. Torej vsak mora sam presoditi, ali je prav zapisati problem štirih barv kot izrek.

Izrek o štirih barvah (Appel in Haken). *Vsak ravninski graf je 4-obarvljiv.*

Grötzschev izrek pravi, da za ravninske grafe brez trikotnikov lahko potrebno število barv zmanjšamo za 1.

Izrek 75 (Grötzsch) *Vsak ravninski graf brez trikotnikov je 3-obarvljiv.*

Kromatični polinom

Naj bo G enostaven graf in naj bo $P(G,k)$ funkcija števila barvanj grafa G s k-barvami. Potem to funkcijo imenujemo **kromatični polinom** grafa G.

Opomba: $\chi(G)$ je najmanjše pozitivno število k, za katerega velja $P(G,k) > 0$.

Zgled: P_2, P_3, P_n, K_3, K_n, $\bar{K}_n$

Naloga 30 *Izračunaj kromatični polinom za graf* C_4.

Naloga 31 *Naj bo T drevo na n točkah. Izračunaj $P(T, k)$.*

Trditev 76 *Naj bo G graf in $e = xy$ povezava v G. Potem*

$$P(G, k) = P(G - e, k) - P(G/e, k).$$

Dokaz. Radi bi pokazali, da je

$$P(G - e, k) = P(G, k) + P(G/e, k).$$

Število k-barvanj grafa $G - e$ pri katerem sta x in y različno obarvana je $P(G, k)$. Število k-barvanj grafa $G - e$, pri katerem sta x in y enako obarvana, je $P(G/e, k)$. Od tod pa zveza takoj sledi.

□

Trditev 77 *Funkcija $P(G, k)$ je polinom.*

Dokaz.

Naloga 32 *Izračunaj kromatični polinom za graf C_5.*

Barvanja povezav grafa

Podobno kot pri barvanju točk barvamo povezave tako, da bosta poljubni dve sosednji povezavi različno obarvani.

Najmanjše število potrebnih barv, da bi obarvali povezave grafa G, imenujemo **kromatični indeks** grafa G in ga označimo s $\chi'(G)$.

Očitno je, da je $\Delta(G)$ potrebno število barv za barvanje povezav grafa G, t.j. $\Delta(G) \leq \chi'(G)$

Zgled: P_n, C_n, K_4, K_5, Q_3

Problem 11 *Izračunaj* $\chi'(Q_d)$.

Izrek 78 (König) *Naj bo G dvodelen multigraf. Potem je*

$$\chi'(G) = \Delta(G). \tag{3}$$

Barvanje povezav določenega grafa G lahko obravnavamo kot barvanje točk povezavnega grafa $L(G)$.

Spomnimo se $V(L(G)) = E(G)$, dve točki $e, f \in V(L(G))$ pa sta sosednji natanko takrat, ko sta povezavi e in f incidenčni v grafu G.

Trditev 79 *Velja $\chi'(G) = \chi(L(G))$.*

Osupljiv rezultat Vizinga pa pove, da zadostno število barv ni bistveno večje.

Izrek 80 (Vizing) *Naj bo G enostaven graf z maksimalno stopnjo Δ. Potem je*

$$\Delta \leq \chi'(G) \leq \Delta + 1. \tag{4}$$

Vizingov izrek poraja zelo zanimiv problem. Naj bo **razred I** sestavljen iz grafov, za katere velja, da je $\Delta = \chi'$. Grafi, za katere to ne velja, naj tvorijo **razred II**. Za dani graf se lahko vprašamo, v katerem razredu je.

Problem 12 *Kateremu razredu pripada P_{10}?*

Rešitev:

Osnove Algebre

Algebro ločimo na

- **klasično:** reševanje algebrajskih enačb, teorija števil
- **moderno:** raziskovanje algebrskih struktur

Obravnavali bomo:

1. grupoide, polgrupe, monoide, grupe
2. podgrupe, podgrupe edinke
3. ciklične končne, končne grupe
4. kolobarje, obsege, polja
5. polinome
6. teorija števil

Operacije

Naj bo $A \subseteq B$. Preslikava $f : A \times A \to B$ je **dvočlena operacija na** A.

Namesto $f(x, y)$ pišemo $x \cdot y$ oz. xy

Če je $\forall x, y \in A : x \cdot y \in A$, je f **notranja operacija v** A, množica A pa je za operacijo $\cdot$ **trdna** oz. **stabilna**.

Pogosto uporabljene operacije: $+$ seštevanje, $-$ odštevanje, $\cdot$ množenje, $/$ deljenje

Zgledi:

- $+$ je notranja operacija v $\mathbb{N}$;
- $-$ ni notranja operacija v $\mathbb{N}$;
- $-$ je operacija na $\mathbb{N}$ (vzamemo $A = \mathbb{N}$ in $B = \mathbb{Z}$);
- $-$ je notranja operacija v $\mathbb{Z}$.

Vprašanje 13 *Ali je deljenje notranja operacija?*

Odgovor:

Algebrske strukture

Štiri osnovne lastnosti

1. **notranjost**: če $\forall x, y \in A : x \cdot y \in A$;
2. **asociativnost**: $\forall x, y\, z \in A : x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
3. **enota**: $e \in A$ je **enota**, če velja $\forall x \in A : x \cdot e = e \cdot x = x$;
4. **obrnljivost**: $x \in A$ je **obrnljiv**, če $\exists : y \in A : x \cdot y = y \cdot x = e$. Rečemo, da je y inverz x-a.

Algebrska struktura $(A, \cdot)$ je

- **grupoid**, če je $\cdot$ notranja operacija;
- **polgrupa**, če je $\cdot$ notranja in asociativna operacija;
- **monoid**, če je $\cdot$ notranja in asociativna operacija, obstaja enota;
- **grupa**, če je $\cdot$ notranja in asociativna operacija, obstaja enota, vsak element iz A je obrnljiv.

Algebrska struktura $(A, \cdot)$ je **komutativna** oz. **abelova**, če

$$\forall a, b \in A : a \cdot b = b \cdot a$$

Zgledi:

- $(\mathbb{R}, -)$ je grupoid;
- $(\mathbb{R}, +)$ je grupa;
- $(\mathbb{R}, \cdot)$ je monoid;
- $(\mathbb{R}^*, \cdot)$ za $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
- $(\mathbb{Z}_n, +_n)$ je grupa.

Naloga 33 *Kdaj je* $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ *grupa?*

Velja:

- grupoid je polgrupa, če je $\cdot$ asociativna operacija;
- polgrupa je monoid, če ima operacija $\cdot$ enoto;
- monoid je grupa, če je vsak element iz A obrnljiv.

Vprašanje 14 *Kakšna algebrska struktura je* $(\{-1, 1\}, \cdot)$*?*

Odgovor:

Problem 13 *Naj bo* $Q\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$*. Ali je potem* $(Q\sqrt{2} \setminus \{0\}, \cdot)$ *grupa?*

Rešitev:

Trditev 81 *Grupoid* $(A, \cdot)$ *ima največ eno enoto.*

Dokaz. Recimo, da imamo dve enoti e_1, e_2. Obravnavajmo produkt $e_1 \cdot e_2$. Ker je e_1 enota, sledi $e_1 \cdot e_2 = e_2$. In, ker je e_2 enota, sledi $e_1 \cdot e_2 = e_1$. Torej $e_1 = e_2$.

□

Trditev 82 *V monoidu* $(A, \cdot)$ *ima vsak element največ en inverz.*

Dokaz. Recimo, da sta a', a'' inverza za a. Potem velja $a' \cdot a = a \cdot a' = e$ in $a'' \cdot a = a \cdot a'' = e$. Od tod velja:

$$a' = a' \cdot e = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = e \cdot a'' = a''.$$

Torej velja $a' = a''$.

□

Potence v monoidu

Naj bo $(A, \cdot)$ monoid.

Potence elementa $a \in A$ definiramo takole:

$$a^0 = e, \quad a^1 = a, \quad a^n = a \cdot a \cdots a.$$

Velja:

$$a^n \cdot a^m = a^{n+m} \qquad \text{in} \qquad (a^n)^m = a^{nm}.$$

Inverz elementa $a \in A$ označimo z a^{-1} ter definiramo $a^{-n} = (a^{-1})^n$.

Kadar operacijo označimo s $+$, namesto o potencah govorimo o **večkratnikih**. V tem primeru enoto označimo z 0 ter večkratnike elementa $a \in A$ definiramo takole:

$$\begin{aligned} 0 \cdot a &= 0 \\ 1 \cdot a &= a \\ n \cdot a &= a + a + \cdots + a. \end{aligned}$$

Inverz elementa $a \in A$ označimo z $-a$ ter definiramo $(-n)a = n(-a)$.

Množico obrnljivih elementov iz A označimo z A^*.

Naloga 34 *Poišči $\mathbb{Z}_{12}^*$ za $(\mathbb{Z}_{12}, \cdot_{12})$, sestavi Cayleyevo tabelo za $(\mathbb{Z}_{12}^*, \cdot_{12})$ ter ugotovi kakšna je ta algebrska struktura.*

Trditev 83 *Naj bo $(A, \cdot)$ monoid. Potem,*

1. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$;
2. *Če* $x, y \in A^*$, *potem* $x \cdot y \in A^*$;
3. $(A^*, \cdot)$ *je grupa.*

Dokaz. Prva trditev sledi takoj iz naslednjih dveh izpeljav:

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = (x \cdot (y \cdot y^{-1})) \cdot x^{-1} = (x \cdot e) \cdot x^{-1} = x \cdot x^{-1} = e$$

ter

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = (y^{-1} \cdot (x \cdot x^{-1})) \cdot y = (y^{-1} \cdot e) \cdot y = x^{-1} \cdot x = e.$$

Posledica 84 *Algebrske strukure* $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\{-1, 1\}, \cdot)$ *so grupe.*

Kongruenčne relacije

Naj bo $(A, \cdot)$ grupoid in R ekvivalenčna relacija v A.

V faktorski množici A/R želimo definirati operacijo $*$ takole:

$$R[x] * R[y] := R[x \cdot y] \tag{5}$$

Težava. Rezultat je lahko odvisen od izbire predstavnikov oz. operacija $*$ ni dobro definirana.

Definicija 1 *Ekvivalenčna relacija v grupoidu* $(A, \cdot)$ *je* **kongruenčna**, *če*

$$x\,R\,u \;\wedge\; y\,R\,v \;\;\Rightarrow\;\; x \cdot y\,R\,u \cdot v.$$

Trditev 85 *Če je* R *kongruenčna v* $(A, \cdot)$, *potem je operacija* $*$ *v* A/R *s predpisom iz* (5) *dobro definirana.*

Dokaz. Recimo $R[x] = R[u]$ in $R[y] = R[v]$ za poljubne x, y, u, v. Da bo operacija dobro definirana, mora veljati $R[x \cdot y] = R[u \cdot v]$.

Iz $R[x] = R[u]$ sledi $x\,R\,u$ ter iz $R[y] = R[v]$ sledi $y\,R\,v$. In ker je R kongurenčna, sledi $x \cdot y\,R\,u \cdot v$ in od tod $R[x \cdot y] = R[u \cdot v]$, kar je bilo potrebno pokazati. □

$(A/R, *)$ je **faktorski grupoid** za $(A, \cdot)$ glede na R.

Naloga 35 *Pokaži da je* $\equiv \pmod{12}$ *ekvivalenčna relacija v* $\mathbb{Z}$*. Kateri so ekvivalenčni razredi?*

Naloga 36 *Pokaži, da je* $\equiv \pmod{12}$ *kongruenčna relacija za grupo* $(\mathbb{Z}, +)$*. Kako definiramo operacijo* $*$*? Kakšna struktura je* $(\mathbb{Z}/\equiv \pmod{12}, *)$*?*

Naloga 37 *Pokaži, da je* $\equiv \pmod{12}$ *kongruenčna relacija za monoid* $(\mathbb{Z}, \cdot)$*. Kako definiramo operacijo* $*$*? Kakšna struktura je* $(\mathbb{Z}/\equiv \pmod{12}, *)$*?*

Izrek 86 *Naj bo R kongruenčna relacija v grupoidu $(A, \cdot)$. Potem velja*

1. *$\cdot$ komutativna v $A \Rightarrow$ $*$ komutativna v A/R;*
2. *$\cdot$ asociativna v $A \Rightarrow$ $*$ asociativna v A/R;*
3. *e enota v $A \Rightarrow R[e]$ enota v A/R;*
4. *x obrnljiv v $A \Rightarrow R[x]$ obrnljiv v A/R in $R[x]^{-1} = R[x^{-1}]$.*

Dokaz. Vsako trditev obravnavamo posebej:

1. $R[x] * R[y] = R[x \cdot y] = R[y \cdot x] = R[y] * R[x]$.

2. Izpeljimo:

$$\begin{aligned}(R[x] * R[y]) * R[z] &= R[x \cdot y] * R[z] = R[(x \cdot y) \cdot z] \\ &= R[x \cdot (y \cdot z)] = R[x] * (R[y] * R[z])\end{aligned}$$

3. Velja:

$R[x]*R[e] = R[x \cdot e] = R[x]$ ter $R[e]*R[x] = R[e \cdot x] = R[x]$.

Od tod sledi, da je $R[e]$ enota v A/R.

4. Velja:

$R[x]*R[x^{-1}] = R[x \cdot x^{-1}] = R[e]$ ter $R[x^{-1}]*R[x] = R[x^{-1} \cdot x] = R$

Od tod sledi, da je $R[x^{-1}]$ inverz za $R[x]$ v A/R, tj. $R[x]^{-1} = R[x^{-1}]$. □

Posledica 87 *Veljajo naslednje implikacije*

1. *$(A, \cdot)$ je grupoid $\Rightarrow$ $(A/R, *)$ je grupoid;*
2. *$(A, \cdot)$ je polgrupa $\Rightarrow$ $(A/R, *)$ je polgrupa;*

3. $(A, \cdot)$ *je monoid* $\Rightarrow$ $(A/R, *)$ *je monoid;*

4. $(A, \cdot)$ *je grupa* $\Rightarrow$ $(A/R, *)$ *je grupa;*

5. $(A, \cdot)$ *je komutativna struktura* $\Rightarrow$ $(A/R, *)$ *je komutativna struktura.*

Algebrska struktura $(\mathbb{Z}_m, +_m)$

$(\mathbb{Z}, +)$ je abelova grupa

$\equiv \pmod m$ je ekvivalenčna relacija v $\mathbb{Z}$

Faktorska množica $\mathbb{Z}/[\equiv \pmod m] = \{0, 1, \ldots, m-1\} = Z_m$

Velja

$$x \equiv u \pmod m \text{ in } y \equiv v \pmod m \Rightarrow x+y \equiv u+v \pmod m.$$

Torej $\equiv \pmod m$ je kongruenčna relacija v $(\mathbb{Z}, +)$.

Ustrezno operacijo $*$ v Z_m označimo s $+_m$ (seštevanje po modulu m)

Velja

$$x +_m y = (x + y) \pmod m$$

($x +_m y$ izračunamo tako, da seštejemo x in y, nato vzamemo ostanek pri deljenju z m)

Ker je $(\mathbb{Z}, +)$ abelova grupa, po posledici 87 sledi, da je $(\mathbb{Z}_m, +_m)$ abelova grupa.

Algebrska struktura $(\mathbb{Z}_m, \cdot_m)$

$(\mathbb{Z}, \cdot)$ je abelov monoid

Velja

$$x \equiv u \pmod{m} \text{ in } y \equiv v \pmod{m} \Rightarrow x \cdot y \equiv u \cdot v \pmod{m}.$$

Torej $\equiv \pmod{m}$ je kongruenčna relacija v $(\mathbb{Z}, \cdot)$.

Ustrezno operacijo $*$ v Z_m označimo z $\cdot_m$ (množenje po modulu m)

Velja

$$x \cdot_m y = (x \cdot y) \pmod{m}$$

($x \cdot_m y$ izračunamo tako, da zmnožimo x in y, nato vzamemo ostanek pri deljenju z m)

Ker je $(\mathbb{Z}, +)$ abelov monoid, po posledici 87 sledi, da je $(\mathbb{Z}_m, +_m)$ abelov monoid.

Algebrska struktura $(\mathbb{Z}_m^*, \cdot_m)$

$\mathbb{Z}_m^*$ je množica obrnljivih elementov iz $(\mathbb{Z}_m, \cdot_m)$. Potem, je $(\mathbb{Z}_m^*, \cdot_m)$ grupa.

Vprašanje 15 *Kateri elementi so v* $\mathbb{Z}_m^*$*?*

Velja,

$$a \in \mathbb{Z}_m^*, \text{ tj. } a \in \mathbb{Z}_m \text{ obrnljiv za } \cdot_m \Leftrightarrow$$

$$\exists x \in \mathbb{Z}_m : a \cdot_m x = 1 \Leftrightarrow$$

$$\exists x \in \mathbb{Z}_m : a \cdot x \equiv 1 \pmod{m} \Leftrightarrow$$

$$\exists x, y \in \mathbb{Z}_m : ax - 1 = my \Leftrightarrow$$

$$\exists x \in \mathbb{Z}_m : ax - my = 1 \Leftrightarrow$$

$$\gcd(a, m) = 1.$$

Torej,

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m, a \perp m\} \quad \text{in} \quad |\mathbb{Z}_m^*| = \varphi(m).$$

Grupe

Osnovne lastnosti

Algebrska struktura $(A, \cdot)$ je **grupa**, če:

1. velja notranjost, tj. $\forall x, y \in A : x \cdot y \in A$;
2. velja asociativnost, tj. $\forall x, y, z \in A : x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
3. obstaja enota $e \in A$, tj. $\forall x \in A : x \cdot e = e \cdot x = x$;
4. je vsak element iz $x \in A$ obrnljiv, tj. $\exists x^{-1} \in A : x \cdot x^{-1} = x^{-1} \cdot x = e$.

Zgled: Naj bo U_n množica rešitev enačbe $x^n = 1$ v $\mathbb{C}$. Recimo

- $U_1 = \{1\}$
- $U_2 = \{-1, 1\}$
- $U_3 = \{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i\}$
- $U_4 = \{1, i, -1, -i\}$.

Algebrska struktura $(U_n, \cdot)$ je grupa.

Trditev 88 *V grupi $(G, \cdot)$ veljata pravili krajšanja:*

$$a \cdot x = b \cdot x \qquad \Rightarrow \qquad a = b$$

in

$$x \cdot a = x \cdot b \qquad \Rightarrow \qquad a = b.$$

Dokaz. Dokažimo le prvo pravilo, dokaz drugega je podoben.

$$\begin{aligned} a \cdot x &= b \cdot x \qquad /x^{-1} \\ a \cdot x \cdot x^{-1} &= b \cdot x \cdot x^{-1} \\ a \cdot e &= b \cdot e \\ a &= b \end{aligned}$$

□

Trditev 89 *V grupi $(G, \cdot)$ sta enačbi $a \cdot x = b$ in $y \cdot a = b$ enolično rešljivi za vsak par $a, b \in G$.*

Dokaz. Rešitev prve enačbe je $x = a^{-1} \cdot b$. Preverimo,

$$a \cdot x = a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = e \cdot b = b$$

Pokažimo, da je to edina rešitev. Če imamo dve rešitvi x_1, x_2, potem

$$a \cdot x_1 = b \quad \text{in} \quad a \cdot x_2 = b$$

iz tega sledi

$$a \cdot x_1 = a \cdot x_2$$

in po pravilu krajšanja dobimo

$$x_1 = x_2$$

Druge enačbe se lotimo podobno. □

Naloga 38 *V grupi* $(\mathbb{Z}_{12}^*, \cdot_{12})$ *reši* $7 \cdot_{12} x = 11$.

Naloga 39 *V grupi* $(\mathbb{Z}_{97}^*, \cdot_{97})$ *poišči* 26^{-1}.

Posledica 90 *Naj bo a element iz grupe $(G, \cdot)$. Funkcijo f_a definiramo takole:*

$$\forall x \in G : f_a(x) = a \cdot x$$

Potem je f_a bijektivna funkcija.

Dokaz. Injektivnost sledi po trditvi 88, surjektivnost pa po trditvi 89.

Naj bo a element iz grupe $(G, \cdot)$ ter H (končna) podmnožica v G. Definiramo

$$\begin{aligned} \mathbf{aH} &= \{a \cdot h : h \in H\}, \\ \mathbf{Ha} &= \{h \cdot a : h \in H\}, \\ \mathbf{a^{-1}Ha} &= \{a^{-1} \cdot h \cdot a : h \in H\}. \end{aligned}$$

Posledica 91 *Množice definirane zgoraj imajo enako moč, tj.*

$$|a\,H| = |H| = |H\,a| = |a^{-1}\,H\,a|.$$

Dokaz.

Naloga 40 *Sestavi Cayleyjeve tabele za grupe* $(\mathbb{Z}_5, +_5)$ *ter* $(\mathbb{Z}_9^*, \cdot_9)$. *Kakšne lastnosti imajo Cayleyjeve tabele grup?*

Odgovor:

Podgrupe

$H \subseteq G$ je **podgrupa** grupe $(G, \cdot)$, če velja:

1. $x, y \in H \Rightarrow x \cdot y \in H$,
2. $e \in H$,
3. $x \in H \Rightarrow x^{-1} \in H$.

V tem primeru pišemo $(H, \cdot) \leq (G, \cdot)$. Notacijo poenostavimo ter pišemo samo $H \leq G$.

Zgledi: $\{0, 3\}$ ter $\{0, 2, 4\}$ sta podgrupi v $\mathbb{Z}_6$. Množici $\{1, 3\}$ ter $\{0, 3, 5\}$ pa nista podgrupi v $\mathbb{Z}_6$.

Naloga 41 *Naj bo $2\mathbb{Z}$ množica vseh sodih celih števil. Potem je $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.*

Odgovor:

Naloga 42 *Naj bosta H_1 in H_2 podgrupi v G. Potem je*

$$H_1 \cap H_2 \leq G.$$

Odgovor:

Izrek 92 *Naj bo H podmnožica v grupi G. H je podgrupa natanko takrat, ko je*

$$H \neq \emptyset \quad in \quad \forall x, y \in H : x^{-1} \cdot y \in H.$$

Dokaz. ($\Rightarrow$). Ker $H \leq G$ sledi $e \in H$ in od tod $H \neq \emptyset$.

Recimo $x, y \in H$, potem tudi $x^{-1}, y \in H$ in od tod $x^{-1} \cdot y \in H$.

($\Leftarrow$). Ker je $H \neq \emptyset$, lahko izberemo element $x \in H$. Dokažimo vse tri pogoje 1.–3. definicije o podgrupah:

Če postavimo $y := x$, potem

$$x^{-1} \cdot y \in H \Rightarrow x^{-1} \cdot x \in H \Rightarrow e \in H,$$

kar je pogoj 2.

Če postavimo $y := \alpha$ ter $x := e$, potem

$$x^{-1} \cdot y \in H \Rightarrow e \cdot \alpha^{-1} \in H \Rightarrow \alpha^{-1} \in H,$$

kar je pogoj 3.

Pogoj 1. pa izpeljemo takole:

$$x, y \in H \Rightarrow x^{-1}, y \in H \Rightarrow (x^{-1})^{-1} \cdot y \in H \Rightarrow x \cdot y \in H.$$

□

Zgledi:

Trditev 93 *Naj bo $H \leq G$ in $a \in G$. Potem je $a^{-1} H a \leq G$.*

Dokaz. Uporabimo kriterij iz izreka 92. Ker $H \neq \emptyset$, sledi da je tudi $a^{-1} H a \neq \emptyset$. Naj bo $x, y \in a^{-1} H a$.

Potem za neka $h_1, h_2 \in H$ velja

$$x = a^{-1} h_1 a \quad \text{ter} \quad y = a^{-1} h_2 a.$$

Od tod pa sledi

$$x^{-1}y = (a^{-1} h_1 a)^{-1}(a^{-1} h_2 a) = a^{-1} h_1^{-1} a a^{-1} h_2 a = a^{-1} (h_1^{-1}h_2) a.$$

Ker je H podgrupa v G, velja $h_1^{-1}h_2 \in H$. In od tod sledi

$$a^{-1} (h_1^{-1}h_2)a \ \in \ a^{-1} H a$$

t.j.

$$x^{-1}y \ \in \ a^{-1} H a.$$

□

Kriterij iz izreka 92 za končne grupe poenostavimo takole:

Izrek 94 *Naj bo G končna grupa. Potem je $H \leq G$ natanko takrat, ko je H trdna podmnožica.*

Dokaz.

Naloga 43 *Poišči vse podgrupe v $(\mathbb{Z}_6, +_6)$.*

Odgovor:

Lagrangev izrek

Naj bo $H \leq G$ in $x \in G$.

Levi odsek elementa x po podgrupi H je

$$x\,H = \{x \cdot h : h \in H\}.$$

Trditev 95 *Naj bo $H \leq G$ in R relacija v G, definirana s predpisom:*

$$x\,R\,y \Leftrightarrow x\,H = y\,H.$$

Potem velja:

1. *R ekvivalenčna relacija*
2. *$x\,R\,y \Leftrightarrow x^{-1}y \in H$*
3. *$R[x] = x\,H$.*

Dokaz. Prva trditev je očitna. Pokažimo drugo trditev:

$$\begin{array}{rcl} x\,R\,y & \Rightarrow & x\,H = y\,H \quad \Rightarrow \quad x \in y\,H \\ & \Rightarrow & \exists h \in H : x = y \cdot h \\ & \Rightarrow & x^{-1} \cdot y = h^{-1} \in H. \end{array}$$

še v drugo smer

$$\begin{array}{rcl} x^{-1} \cdot y \in H & \Rightarrow & \exists h \in H : x^{-1} \cdot y = h \\ & \Rightarrow & y = x \cdot h \wedge x = y \cdot h^{-1} \\ & \Rightarrow & y\,H \subseteq x\,H \wedge x\,H \subseteq y\,H. \end{array}$$

Za konec pokažimo še tretjo trditev:

$$y \in R[x] \quad \Leftrightarrow \quad x\,R\,y \quad \Leftrightarrow \quad x^{-1} \cdot y \in H \quad \Leftrightarrow \quad y \in xH$$

□

Če je število levih odsekov po podgrupi H končno, ga imenujemo **indeks** podgrupe H v grupi G in ga označimo z $[G : H]$.

Izrek 96 (Lagrangev izrek) *Naj bo G končna grupa in $H \leq G$. Potem je moč grupe G deljiva z močjo podgrupe H in velja formula*

$$|G| = [G : H] \cdot |H|.$$

Dokaz. Naj bo $a \in G$ poljuben element. Pokažimo, da je preslikava $f : H \to a\,H$ bijekcija:

- injektivost: $f(x) = f(y) \quad \Rightarrow \quad a \cdot x = a \cdot y \quad \Rightarrow \quad x = y$

- surjektivnost: $y \in a\,H \quad \Rightarrow \quad \exists x \in H : y = a \cdot x$
  $\Rightarrow \quad \exists x \in H : y = f(x)$

Ker je f bijekcija, sledi

$$|a\,H| = |H|$$

Vsi levi odseki po H imajo enako moč kot podgrupa H. Torej, vsi odseki po H imajo enako moč.

Ker levi odseki sestavljajo razbitje grupe G, dobimo:

$$\begin{aligned} |G| &= \text{vsota moči levih odsekov po } H \\ &= (\text{število levih odsekov}) \cdot (\text{moč odseka}) \\ &= [G : H] \cdot |H| \end{aligned}$$

□

Red elementa in končne grupe

Naj bo G končna grupa in $a \in G$.

Red elementa a je definiran kot najmanjše naravno število n tako, da velja $a^n = e$, tj.

$$\mathrm{red}(a) = \min\{r \in \mathbb{N} : a^r = e\}.$$

Če tak n ne obstaja, pravimo, da ima a red ∞, tj. $\mathrm{red}(a) = \infty$.

Naloga 44 *Poišči red elementov grupe* $(\mathbb{Z}_{12}^*, \cdot_{12})$.

Odgovor:

Problem 14 *Naj bo a element v G reda r. Potem je*

$$H = \{e, a, a^2, \ldots, a^{r-1}\}$$

podgrupa v G.

Dokaz.

Trditev 97 *Naj bo G končna grupa reda n in $a \in G$. Potem velja*

1. $a^{\mathrm{red}(a)} = e$
2. $\mathrm{red}(a) = 1 \Leftrightarrow a = e$
3. $\mathrm{red}(a) \mid n$
4. $a^n = e$.

Dokaz. Pokažimo vsako trditev posebej:

1. Sledi iz definicije.
2. V eno smer: $\mathrm{red}(a) = 1 \quad \Rightarrow \quad a^1 = e \quad \Rightarrow \quad a = e$
   ter v drugo smer: $e^1 = e \quad \Rightarrow \quad \mathrm{red}(e) = 1$.
3. Iz prejšnjega problema sledi, da je $\{e, a, a^2, \ldots, a^{\mathrm{red}(a)-1}\}$ podgrupa v G reda $\mathrm{red}(a)$. Zato po Langrangevem izreku sledi, da $\mathrm{red}(a) \mid n$.
4. Iz prejšnje trditve sledi, da je $n = \mathrm{red}(a)\, k$, za neko naravno število k. Torej,
$$a^n = a^{\mathrm{red}(a)k} = (a^{\mathrm{red}(a)})^k = e^k = e.$$

□

Problem 15 *Poišči vse grupe reda* 4.

Rešitev:

Izrek 98 (Euler) *Če* $\gcd(a, m) = 1$, *potem je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz. Grupa $(\mathbb{Z}_m^*, \cdot_m)$ ima $\varphi(m)$ elementov. Ker je $\gcd(a, m) = 1$, lahko vzamemo, da je $a \in \mathbb{Z}_m^*$. Po zgornji trditvi velja $a^{\varphi(m)} \equiv 1 \pmod{m}$ v $\mathbb{Z}_m^*$. Za $a \in \mathbb{Z}$ pa to pomeni $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Posledica 99 (Mali Fermatov izrek) *Naj bo* $a \in \mathbb{Z}$ *in* p *praštevilo, ki ne deli* a. *Potem je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz. Ker $p \nmid a$ sledi, da $\gcd(p, a) = 1$. In ker je p praštevilo vemo, da $\varphi(p) = p - 1$. Zdaj iz prejšnjega izreka sledi dokaz. □

Izrek 100 (Cauchy) *Naj bo* G *končna grupa moči* n *ter naj bo* p *praštevilo, ki deli* n. *Potem* G *vsebuje element reda* p.

Generatorji ter ciklične grupe

Grupa G je **ciklična**, če obstaja $a \in G$ tako, da je vsak element grupe G enak neki potenci elementa a.

Element a imenujemo **generator** grupe G.

Naloga 45 *Ali je* $(\mathbb{Z}_n, +_n)$ *ciklična? Pošči vse generatorje za grupo* $(\mathbb{Z}_{12}, +_{12})$.

Trditev 101 *Naj bo* G *končna grupa reda* n. *Potem velja:*

$$G \text{ je ciklična grupa} \iff G \text{ vsebuje element reda } n.$$

Posledica 102 *Če je red grupe* G *praštevilo, potem je* G *ciklična grupa.*

Trditev 103 *Naj bo $\mathcal{D}$ neka družina podgrup grupe G. Potem je presek teh podgrup podgrupa v G, tj.*

$$\bigcap_{F \in \mathcal{D}} F \leq G.$$

Dokaz. Dokaz poteka podobno kot pri nalogi 42.

□

Naj bo $S \subseteq G$ neka podmnožica v grupi G. **Najmanjša podgrupa** v G, ki vsebuje S, je

$$\langle S \rangle = \bigcap \{H \leq G : S \subseteq H\}.$$

Množica S **generira** grupo G, če velja $\langle S \rangle = G$.

Opomba: Če je G ciklična grupa, potem obstaja S moči 1, ki generira G.

Če $S = \{a\}$ potem namesto $\langle \{a\} \rangle$ pišemo $\langle a \rangle$.

Naloga 46 *Za grupo* $(\mathbb{Z}_{12}^*, \cdot_{12})$ *izračunaj* $\langle 5 \rangle$, $\langle \{5, 7\} \rangle$, $\langle \{7, 11\} \rangle$, $\langle \{11, 5\} \rangle$.

Naloga 47 *Za grupo* $(\mathbb{Z}_{12}, +_{12})$ *izračunaj* $\langle 3 \rangle$, $\langle 4 \rangle$, $\langle 6 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$, $\langle \{3, 4\} \rangle$.

Cayleyjevi digrafi

Naj bo H grupa ter $S \subseteq H$. **Cayleyjev digraf** $G = \mathrm{Cay}(H; S)$ je definiran takole:

- $V(G) = H$
- $E(G) = \{uv \mid u^{-1}v \in S\}$.

Zgledi: Cayleyjevi digrafi $(\mathbb{Z}_6, \{1\})$, $(\mathbb{Z}_6, \{2, 3\})$

Problem 16 *Nariši hiperkocko Q_3 kot Cayleyjev graf.*

Podgrupe edinke

Naj bo G grupa in $H \leq G$.

H je **edinka**, če velja: $\forall a \in G : a^{-1} H a \subseteq H$.

Pišemo $H \lhd G$.

$\{e\}$ in G sta **trivialni** edinki v G.

Trditev 104 *Naj bo G grupa in H podgrupa v G. Naslednje trditve so enakovredne:*

(i) $H \lhd G$

(ii) $\forall a \in G : a^{-1} H a = H$

(iii) $\forall a \in G : a H = H a$.

Dokaz.

Trditev 105 *V Abelovi grupi je vsaka podgrupa edinka.*

Dokaz.

Izrek 106 *Naj bo R kongruenčna relacija v grupi G. Tedaj je $R[e] \lhd G$.*

Izrek 107 *Naj bo $H \lhd G$. Potem je relacija R definirana kot*

$$a\,R\,b \quad \equiv \quad a\,H = b\,H$$

kongruenčna relacija.

Izrek 108 *Naj bo H podgrupa v G tako, da je $[G : H] = 2$. Potem $H \lhd G$.*

Dokaz. Naj bo $a \in G \setminus H$. Potem sta H in aH leva odseka in zato velja

$$aH \cup H = G \quad \text{ter} \quad aH \cap H = \emptyset.$$

Podobno sta H in Ha desna odseka in zato velja

$$Ha \cup H = G \quad \text{ter} \quad Ha \cap H = \emptyset.$$

Tako sklepamo, da je $aH = Ha$ in od tod, da je H edinka.

Homomorfizmi

Naj bosta $(G, \circ)$ in $(H, *)$ grupi. Preslikava $f : G \to H$ je **homomorfizem**, če velja

$$\forall a, b \in G : f(a \circ b) = f(a) * f(b)$$

Bijektivni homomorfizem je **izomorfizem**. Če je $G = H$, potem izomorfizem imenujemo **avtomorfizem**.

Zgled: Preslikava $h(x) = e^x$ je izomorfizem iz $(\mathbb{R}, +)$ v $(\mathbb{R}^+, \cdot)$.

Trditev 109 *Naj bosta G_1, G_2 ciklični grupi. Velja:*

$$|G_1| = |G_2| \quad \Rightarrow \quad G_1 \cong G_2.$$

Trditev 110 *Veljajo naslednje lastnosti:*

(1) $f(e_G) = e_H$

(2) $f(x^{-1}) = f(x)^{-1}$.

Dokaz. Pokažimo prvo trditev. Velja:

$$f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G).$$

Pokrajšamo z $f(e_G)$ ter tako dobimo $f(e_G) = e_H$.

Druga trditev pa takoj sledi iz:

$$f(x) * f(x^{-1}) = f(x \circ x^{-1}) = f(e_G) = e_H$$

ter

$$f(x^{-1}) * f(x) = f(x^{-1} \circ x) = f(e_G) = e_H.$$

□

Naloga 48 *Ali sta grupi* $(\mathbb{Z}_4, +_4)$ *ter* $(\mathbb{Z}_{12}^*, \cdot_{12})$ *izomorfni?*

Jedro in slika homomorfizma

Naj bo $f : (G, \circ) \to (H, *)$ homomorfizem. **Jedro** homomorfizma f je

$$\ker(f) = \{x \in G : f(x) = e_H\},$$

slika homomorfizma f pa je

$$\mathrm{im}(f) = \{f(x) : x \in G\}.$$

Velja: $\ker(f) \subseteq G$ ter $\mathrm{im}(f) \subseteq H$

Naloga 49 *Pokaži, da je* $h(x) = 3x \pmod{12}$ *homomorfizem iz* $(\mathbb{Z}_{12}, +_{12})$ *v* $(\mathbb{Z}_{12}, +_{12})$. *Izračunaj* $\ker(h)$ *ter* $\mathrm{im}(h)$.

Rešitev:

Trditev 111 *Naj bo $f : G \to H$ homomorfizem. Potem, velja*

- *f je injektiven* $\Leftrightarrow \ker(f) = \{e_G\}$;
- *f je surjektiven* $\Leftrightarrow \mathrm{im}(f) = H$.

Dokaz. Druga trditev je očitna, zato pokažimo le prvo.

($\Rightarrow$). Naj bo f injektivna funkcija. Vemo, da $f(e_G) = e_H$. Za $x \in \ker(f)$ velja $f(x) = e_G$. Zdaj pa iz injektivnosti sledi, da je $x = e_G$. In od tod $\ker(f) = \{e_G\}$.

($\Leftarrow$). Naj bo $\ker(f) = \{e_G\}$. Recimo $f(x) = f(y)$. Potem pa izpeljemo takole

$$\begin{aligned} f(x) &= f(y) \qquad / * f(y)^{-1} \\ f(x) * f(y)^{-1} &= f(y \circ y^{-1}) \\ f(x \circ y^{-1}) &= f(e_G) \\ f(x \circ y^{-1}) &= e_H. \end{aligned}$$

Ker je $\ker(f) = \{e_G\}$, dobimo $x \circ y^{-1} = e_G$ in od tod $x = y$. $\square$

Naloga 50 *Poišči injektiven homomorfizem iz $(\mathbb{Z}_6, +_6)$ v $(\mathbb{Z}_{12}, +_{12})$. Potem pa poišči surjektiven homomorfizem iz $(\mathbb{Z}_{12}, +_{12})$ v $(\mathbb{Z}_6, +_6)$.*

Rešitev:

Trditev 112 *Naj bo $f : G \to H$ homomorfizem. Potem, velja*

- $\ker(f) \lhd G$
- $\mathrm{im}(f) \leq H$.

Dokaz. Z uporabo izreka 92 pokažimo, da je $\ker(f)$ podgrupa. Ker $f(e_G) = e_H$, sledi $e_G \in \ker(f)$ in zato $\ker(f) \neq \emptyset$.

Za poljubni $x, y \in \ker(f)$ velja:

$$f(x^{-1} \circ y) = f(x^{-1}) * f(y) = f(x)^{-1} * f(y) = e_H * e_H = e_H.$$

Torej $x^{-1} \circ y \in \ker(f)$ in od tod sledi, da je $\ker(f)$ podgrupa.

Pokažimo, da je $\ker(f)$ edinka. Naj bosta $h \in \ker(f)$ ter $a \in G$ poljubna. Dovolj bo, da pokažemo, da je $a^{-1} \circ h \circ a \in \ker(f)$. Velja

$$f(a^{-1} \circ h \circ a) = f(a^{-1}) * f(h) * f(a) = f(a)^{-1} * e_G * f(a) = e_G.$$

Iz tega sledi, da je $a^{-1} \circ h \circ a$ v jedru preslikave f. Od tod pa sklepamo, da je $a^{-1} \ker(f)\, a \subseteq \ker(f)$, kar implicira, da je $\ker(f)$ edinka.

Pokažimo drugo trditev. Ker $f(e_G) = e_H$, sledi $\mathrm{im}(f) \neq \emptyset$. Za poljubna $x, y \in \mathrm{im}(f)$ hočemo pokazati, da $x^{-1} * y \in \mathrm{im}(f)$. Potem obstajata a, b za katera velja $f(a) = x$ in $f(b) = y$. Ker

$$f(a^{-1} \circ b) = f(a)^{-1} * f(b) = x^{-1}y,$$

sledi, da $x^{-1} * y \in \mathrm{im}(f)$.

Izrek 113 (Osnovni izrek o izomorfizmu) *Naj bo $f : G \to H$ surjektivni homomorfizem grupe G v grupo H z jedrom $J = \ker(f)$. Potem je $G/J \cong H$.*

Zgled: Preslikava $f(x) = x \pmod{n}$ je homomorfizem iz $(\mathbb{Z}, +)$ v $(\mathbb{Z}_n, +_n)$. Jedro je $\ker(f) = \{n \cdot a : a \in \mathbb{Z}\} = n\,\mathbb{Z}_n$. Velja:

$$\mathbb{Z}/n\,\mathbb{Z} \cong \mathbb{Z}_n.$$

Kartezični produkt grup

Trditev 114 *Naj bosta* $(G, *)$ *in* $(H, \cdot)$ *grupi. Definirajmo algebrsko strukturo* $(G \times H, \circ)$ *takole:*

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2).$$

Pokaži, da je $(G \times H, \circ)$ *grupa.*

Dokaz.

Grupo iz zgornje trditve ponavadi označimo z $(G, *) \times (H, \cdot)$

Naloga 51 *Sestavi Cayleyevo tabelo grupe* $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_3, +_3)$. *Ali je ta grupa izomorfna grupi* $(\mathbb{Z}_6, +_6)$*?*

Odgovor:

Naloga 52 *Ali je* $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_4, +_4)$ *izomorfna grupi* $(\mathbb{Z}_8, +_8)$*?*

Odgovor:

Trditev 115 $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \quad \Leftrightarrow \quad \gcd(m,n) = 1.$

Dokaz.

Naloga 53 *Ali je* $\mathbb{Z}_2^2$ *izomorfna grupi* $(\mathbb{Z}_{12}^*, \cdot_{12})$*?*

Odgovor:

Izrek 116 (Opis končnih Abelovih grup) *Naj bo G končna Abelova grupa, $n = |G|$. Potem obstaja zapis števila n v obliki $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, kjer so p_i praštevila, $p_1 \leq p_2 \leq ... \leq p_k$, $\alpha_i > 0$ tako, da je*

$$G \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$$

Opomba: Za različne zapise dobimo neizomorfne grupe.

Naloga 54 *Poišči vse neizomorfne Abelove grupe moči 72.*

Odgovor:

Naloga 55 *Poišči red elementa $(8, 4, 10)$ v grupi $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.*

Permutacije

Ponovimo iz DS I:

A - končna množica;

$S(A)$ - množica vseh permutacij na A;

$\circ$ - kompozitum oz. produkt funkcij;

$S_n := S(A)$ za $A = \{1, 2, \ldots, n\}$, velja $|S_n| = n!$

Trditev 117 *Velja:*

- *Vsaka permutacija se da (enolično) razcepiti na produkt disjunktnih ciklov.*
- *Vsaka permutacija je bodisi soda ali liha (odvisno od števila transpozicij)*

Zgledi: $(123)(45)$ je liha permutacija, $(125)(34)(6789)$ pa je soda permutacija.

Vemo:

- id je soda permutacija,
- π ter π^{-1} sta enake parnosti,
- Če sta C_1 ter C_2 disjunktna cikla, potem $C_1 \circ C_2 = C_2 \circ C_1$,
- Če je $C = (a_1\, a_2\, \cdots\, a_n)$, potem je $C^{-1} = (a_n\, a_{n-1}\, \cdots\, a_1)$

Naj ima permutacija $\pi \in S_n$ v zapisu k_i ciklov dolžine i, za $i = 1, \ldots, n$.

Potem pravimo, da ima π **ciklično strukturo**

$$(k_1, k_2, \ldots, k_n).$$

Velja

$$1 \cdot k_1 + 2 \cdot k_2 + 3 \cdot k_3 + \cdots + n \cdot k_n = n.$$

Zgled: Permutacija $(123)(45)(56)(7)(89)$ ima ciklično strukturo $(1, 3, 2, 0, 0, 0, 0, 0, 0)$.

Trditev 118 *Naj bo C cikel dolžine m. Potem je* $\mathrm{red}(C) = m$.

Dokaz.

Trditev 119 *Naj bo permutacija π kompozitum tujih ciklov dolžine $m_1, m_2, \ldots, m_k$. Potem je* $\mathrm{red}(\pi) = \mathrm{lcm}(m_1, m_2, \ldots, m_k)$.

Dokaz.

Vaja:

Definiramo relacijo **konjugiranost** $\approx$ na $S(A)$ takole:

$$\pi_1 \approx \pi_2, \qquad \text{če} \quad \exists \tau \in G : \pi_2 = \tau \circ \pi_1 \circ \tau^{-1}$$

Izrek 120 *Permutaciji π in σ sta konjugirani natanko takrat, ko imata enako ciklično strukturo.*

Dokaz. ($\Rightarrow$). Če je $C = (i_1\, i_2\, \cdots\, i_k)$ cikel, potem je

$$\tau \circ C \circ \tau^{-1} = (\tau(i_1)\, \tau(i_2)\, \cdots\, \tau(i_k)).$$

Pri produktu disjunktnih ciklov pa tako učinkuje posebej na vsakem ciklu. Naj bo

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m).$$

Potem je

$$\begin{aligned}
\tau \circ \pi \circ \tau^{-1} &= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ [\tau^{-1} \circ \tau] \circ (b_1\, b_2\, \cdots\, b_l) \circ [\tau^{-1} \circ \tau] \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= [\tau \circ (a_1\, a_2\, \cdots\, a_k) \circ \tau^{-1}] \circ [\tau \circ (b_1\, b_2\, \cdots\, b_l) \circ \tau^{-1}] \circ \cdots [\tau \circ (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1}] \\
&= \big(\tau(a_1)\, \tau(a_2)\, \cdots\, \tau(a_k)\big) \circ \big(\tau(b_1)\, \tau(b_2)\, \cdots\, \tau(b_l)\big) \circ \cdots \big(\tau(c_1)\, \tau(c_2)\, \cdots\, \tau(c_m)\big)
\end{aligned}$$

($\Leftarrow$) Recimo:

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m)$$

in

$$\sigma = (a'_1\, a'_2\, \cdots\, a'_k) \circ (b'_1\, b'_2\, \cdots\, b'_l) \circ \cdots \circ (c'_1\, c'_2\, \cdots\, c'_m).$$

Definiramo funkcijo $\tau : x \mapsto x'$. Očitno, da je τ permutacija iz $S(A)$. Velja pa $\tau \circ \pi \circ \tau^{-1} = \sigma$. To pa vidimo takole:

$$\tau \circ \pi \circ \tau^{-1}(x'_i) = \tau \circ \pi(x_i) = \tau(x_{i+1}) = x'_{i+1} = \sigma(x'_i)$$

□

Naslednja trditev je hitra posledica prejšnjega izreka.

Posledica 121 *Konjugiranost $\approx$ je ekvivalenčna relacija.*

Simetrična grupa

Pokazali bomo, da je $(S(A), \circ)$ grupa. To grupo imenujemo **simetrična grupa** množice A.

Izrek 122 $(S(A), \circ)$ *je grupa.*

Dokaz. Pokažemo po vrsti vse lastnosti grupe.

zaprtost: $f, g \in S(A)$ potem je $f \circ g : A \to A$. Pokazati še moramo, da je $f \circ g$ permutacija, tj. bijekcija.

- *Injektivnost funkcije* $f \circ g$*:*

$$\begin{aligned} (f \circ g)(x) &= (f \circ g)(y) \\ f(g(x)) &= f(g(y)) \\ g(x) &= g(y) \qquad \text{(ker je } f \text{ injektivna)} \\ x &= y \qquad \text{(ker je } g \text{ injektivna)} \end{aligned}$$

- *Surjektivnost funkcije* $f \circ g$*:* Naj bo $y \in A$ poljuben. Ker je f surjektivna, obstaja $z \in A$ tako, da je $y = f(z)$. In, ker je g surjektivna, obstaja $x \in A$ tako, da je $g(x) = z$. Torej, obstaja tak x, da je $(f \circ g)(x) = f(g(x)) = y$.

asociativnost: Sledi iz

$$((f \circ g) \circ h)(x)) = (f \circ g)(h((x)) = f(g(h(x)))$$

in

$$(f \circ (g \circ h))(x)) = f((g \circ h)(x)) = f(g(h(x)))$$

enota: Enota je permutacija $\mathrm{id} : x \mapsto x$.

inverz: Če je $f : A \to A$ bijekcija, potem vemo, da obstaja bijektivna funkcija $f^{-1} : A \to A$ tako, da velja:

$$f^{-1}(f(x)) = x \quad \text{in} \quad f(f^{-1}(x)) = x.$$

To pa je enakovredno pogoju za obstoj inverza v grupi:

$$f^{-1} \circ f = \mathrm{id} \quad \text{in} \quad f \circ f^{-1} = \mathrm{id}.$$

□

Permutacijska grupa je vsaka podgrupa grupe $S(A)$.

Opomba 1 *S_n ni Abelova (tj. komutativna) za $n \geq 3$. Velja:*

$$(12)(23) = (123) \neq (132) = (23)(12).$$

S_3 je najmanjša nekomutativna grupa.

Zgled: $S_3 = \{id, (123), (132), (1)(23), (2)(13), (12)(3)\}$

$A_3 = \{\mathrm{id}, (123), (132)\}$ je podgrupa v S_3. Velja še več, A_3 je edinka v S_3.

Alternirajoča grupa

Alternirajoča grupa A_n je definirana takole

$$A_n = \{f \in S_n \mid f \text{ soda permutacija}\}$$

V naslednjem izreku pa pokažemo, da je A_n grupa.

Izrek 123 *Za A_n ter S_n verja naslednje:*

(1) *A_n je podgrupa v S_n;*

(2) *Indeks grupe S_n po podgrupi A_n je 2, t.j. $[S_n : A_n] = 2$;*

(3) $|A_n| = n!/2$.

Dokaz. (1) Če π, σ sodi, potem $\pi \circ \sigma$ soda permutacija. Torej je A_n grupa.

Definirajmo $F : A_n \to S_n \setminus A_n$ takole

$$F(f) = (12) \circ f.$$

Očitno, F je bijekcija. Zato

$$|A_n| = |S_n \setminus A_n| \text{ ter } |S_n| = |A_n| + |S_n \setminus A_n| = 2|A_n|.$$

Od tod sledita (2) in (3). □

Posledica 124 *Alternirajoča grupa A_n je podgrupa edinka v simetrični grupi S_n.*

Dokaz. Po prejšnjem izreku, je A_n podgupa v S_n z $[S_n : A_n] = 2$. Potem dokaz sledi takoj iz izreka 108.

Cayleyjev izrek

Izrek 125 *Vsaka grupa je izomorfna neki permutacijski grupi.*

Dokaz. Naj bo $(G, *)$ grupa. Za vsak element $a \in G$ definiramo $f_a : G \to G$ z predpisom

$$f_a(x) = a * x.$$

Opazimo, da je f_a permutacija iz $S(G)$

Naj bo $h : G \to S(G)$ tako, da je $h(a) = f_a$

Trdimo, da je h homomorfizem:

$$h(ab)(x) = (a * b) * x = a * (b * x) = f_a(f_b(x)) = (h(a) \circ h(b))(x)$$

Trdimo, da je h injektivna preslikava:

$$h(a) = h(b) \Rightarrow f_a = f_b \Rightarrow \forall x \in G : a * x = b * x \Rightarrow a = b$$

Torej sledi, da je grupa G izomorfna svoji sliki $\mathrm{im}(h)$ v $S(G)$. Ker pa je $\mathrm{im}(h)$ podgrupa iz $S(G)$, je dokaz končan. □

Kolobarji, Obsegi in Polinomi

Definicija kolobarja

Algebrska struktura $(K, +, \cdot)$ je **kolobar**, če velja:

1. $(K, +)$ je Abelova grupa, njeno enoto označimo z 0;
2. $(K, \cdot)$ je polgrupa;
3. operacija $\cdot$ distribuira čez $+$, tj., za vse $a, b, c \in K$ velja:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{in} \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

Operacijam "$+$" in "$\cdot$" v kolobarju K rečemo **seštevanje** in **množenje**.

Kolobar K je:

- **Abelov** oz. **komutativen,** če je množenje komutativno;
- **kolobar z enico**, če je $(K, \cdot)$ monoid oz. obstaja element $1 \in K$ tako, da za vsak $x \in K$ velja:

$$1 \cdot x = x \cdot 1 = x$$

Zgledi:

- $\mathcal{T} = (\{0\}, +, \cdot)$ je najmanjši kolobar, imenujemo ga **trivialni kolobar**;

- **Kolobarji celih, racionalnih, realnih in kompleksnih števil**:

$$(\mathbb{Z}, +, \cdot), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot), \quad (\mathbb{C}, +, \cdot)$$

  To so kolobarji z običajnim seštevanjem in množenjem;

- $(\mathbb{Z}_n, +_n, \cdot_n)$ je **kolobar ostankov po modulu** n;

- $(n\mathbb{Z}, +, \cdot)$ je **kolobar večkratnikov naravnega števila** n;

- $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ je **kolobar realnih funkcij**

$$\begin{aligned} \mathbb{R}^{\mathbb{R}} &= \{f : \mathbb{R} \to \mathbb{R}\} \\ (f+g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x); \end{aligned}$$

- $\mathcal{B} = (\mathcal{P}(M), +, \cap)$ je **Boolov kolobar**

$$A + B = A \setminus B \cup B \setminus A.$$

Delitelji niča

Elementa $a, b \in K \setminus \{0\}$ sta **delitelja niča**, če je $a \cdot b = 0$.

Zgleda:

- $2 \cdot_6 3 = 0$ torej sta 2 in 3 sta delitelja niča v $(\mathbb{Z}_6, +_6, \cdot_6)$.
- $f, g \in \mathbb{R}^{\mathbb{R}}$ podamo takole:

$$f(x) = \begin{cases} 0, & \text{za } x \leq 0 \\ x, & \text{sicer.} \end{cases} \quad \text{in} \quad g(x) = \begin{cases} x, & \text{za } x \leq 0 \\ 0, & \text{sicer.} \end{cases}$$

  Potem za vsak $x \in \mathbb{R}$ velja $f(x) \cdot g(x) = 0$. Torej, f in g sta delitelja niča.

Kolobar K je **cel**, kadar je Abelov in je brez deliteljev niča.

Aditivna potenca

Aditivno m-to potenco elementa a označimo z $\mathbf{m\,a}$, tj.

$$ma = \underbrace{a + a + \cdots + a}_{m}$$

Potem pa velja:

$$\begin{aligned} (m+n)a &= ma + na \\ m(na) &= (mn)a \\ n(a+b) &= na + nb \\ (mn)a \cdot b &= (ma) \cdot (nb) \end{aligned}$$

Absorpcijski element 0

Trditev 126 *V kolobarju je* 0 *absorpcijski element, tj. velja*

$$a \cdot 0 = 0 \cdot a = 0$$

Dokaz. Sklepamo takole:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Podobno pokažemo, da je $0 \cdot a = 0$. □

Naloga 56 *Pokaži, da je* 0 *edini absorpcijski element.*

Odgovor:

Vprašanje 16 *Naj bo* K *kolobar z enico. Ali je lahko* $1 = 0$*?*

Odgovor:

Operacija $-$

Označimo z $-\mathbf{a}$ inverz elementa a v grupi $(A, +)$. Operacijo "$-$" definiramo takole

$$\mathbf{a - b} := a + (-b).$$

Trditev 127 *V kolobarju K velja:*

1. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
2. $(-a) \cdot (-b) = a \cdot b$
3. $a \cdot (b - c) = a \cdot b - a \cdot c$

Dokaz. Iz $(-a)+a = 0$ sledi $(-a)\cdot b+a\cdot b = 0$ in tako dobimo, da je $(-a) \cdot b = -(a \cdot b)$. Podobno pokažemo drugi del prve enakosti.

V dokazu trditve 2 uporabimo dvakrat trditev 1 takole:

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b.$$

Tretjo trditev pa dokažemo takole:

$$a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b - a \cdot c.$$

□

Množica K^*

Naj bo K kolobar z enico. Element a je **obrnljiv**, če

$$\exists b \in K : a \cdot b = b \cdot a = 1.$$

Naj bo $\mathbf{K}^*$ množica obrnljivih elementov kolobarja K. Opazimo, da $0 \notin K^*$.

Trditev 128 *Struktura $(K^*, \cdot)$ je grupa za množenje.*

Obsegi

Kolobar K je **obseg**, če je $K^* = K \setminus \{0\}$, tj. vsak element iz K različen od 0, je obrnljiv.

Komutativen obseg je **polje**, tj. če v obsegu velja $a \cdot b = b \cdot a$ za vse a, b.

Problem 17 *Pokaži, da v poljubnem obsegu ni deliteljev niča.*

Rešitev:

Izrek 129 $(\mathbb{Z}_n, +_n, \cdot_n)$ *je polje natanko takrat, ko je* n *praštevilo.*

Dokaz. ($\Leftarrow$) Naj bo n praštevilo. Potrebno bo pokazati, da je vsak element iz $\mathbb{Z}_n \setminus \{0\}$ obrnljiv. To pa vemo iz DS I: enačba $ax = 1 + yn$ je rešljiva, tako bo $x \in \mathbb{Z}_n$ inverz za a.

($\Rightarrow$) Recimo, da je n sestavljeno število. Potem, je $n = a \cdot b$ za $1 < a, b < n$ in od tod sledi $a \cdot_n b = 0$ v $\mathbb{Z}_n$. Torej, a in b sta delitelja niča. Potem pa iz rešitve prejšnjega problema sledi, da $\mathbb{Z}_n$ ni obseg. $\square$

Vprašanje 17 *Kateri kolobarji iz prvega zgleda*

$$\mathcal{T} \qquad \mathbb{Z} \qquad \mathbb{Q} \qquad \mathbb{R} \qquad \mathbb{C} \qquad n\mathbb{Z} \qquad \mathbb{Z}_n \qquad \mathbb{R}^{\mathbb{R}} \qquad \mathcal{B}$$

so obsegi oz. polja?

Odgovor:

Naloga 57 *V kolobarju* $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ *reši sistem enačb:*

$$\begin{aligned} 3x + 8y &= 7 \\ 6x + 5y &= 4. \end{aligned}$$

Rešitev: Dobimo tri rešitve: $(1, 2)$, $(5, 2)$, $(9, 2)$.

Karakteristika kolobarja

Naj bo K kolobar z enico ter naj bo $r = \mathrm{red}(1)$ v grupi $(K, +)$.

Karakteristika kolobarja K je

$$r(K) = \begin{cases} r, & \text{če je } r \text{ končno število;} \\ 0, & \text{če } r = \infty. \end{cases}$$

Zgledi: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ imajo karakteristiko 0, ker je $n\,1 \neq 0$ za vse $n \in \mathbb{N}$.

Trditev 130 *V kolobarju s karakteristiko r je $r\,x = 0$ za vsak $x \in K$.*

Dokaz. Pokažimo takole:

$$\begin{aligned} r\,x &= \underbrace{x + x + \cdots + x}_{r} = 1 \cdot x + 1 \cdot x + \cdots + 1 \cdot x \\ &= (\underbrace{1 + 1 + \cdots + 1}_{r}) \cdot x = (r1) \cdot x = 0 \cdot x = 0 \end{aligned}$$

□

Trditev 131 *Naj bo K celi kolobar z enoto 1. Potem je karakteristika $r(K)$ bodisi 0 ali praštevilo.*

Dokaz. Naj bo $r = r(K)$ sestavljeno število različno od 0, recimo $r = a\,b$ za $a, b \neq 0, 1$. Potem je $a\,b \cdot 1 = 0$ in od tod $(a1) \cdot (b1) = 0$. Ker $a1 \neq 0$ ter $b1 \neq 0$, dobimo, da sta $a\,1$ in $b\,1$ delitelja niča, kar je protislovje.

Izrek o končnih obsegih

Izrek 132 *Naj bo F končen obseg. Potem velja:*

(a) F je komutativen

(b) $|F|$ je potenca praštevila

(c) grupa $(F \setminus \{0\}, \cdot)$ je ciklična

(d) Naj bo F_1 obseg in $|F_1| = |F|$, potem $F_1 \cong F$.

Končnemu obsegu oz. polju s p^n elementi rečemo **Galoisovo polje reda** n in ga označimo z $\mathbf{GF(p^n)}$.

Polinomi

K je komutativen kolobar;

$K[X]$ je množica vseh polinomov s koeficienti iz K;

Označimo s "$+$" in "$\cdot$" običajno seštevanje in množenje polinomov;

Označimo z $\deg(p)$ stopnjo polinoma $p(x)$;

Zgled: Če v kolobarju $\mathbb{Z}_6[X]$ seštejemo ter zmnožimo polinoma:

$$p(x) = 2x^2 + 3 \quad \text{in} \quad q(x) = 3x + 1\,,$$

dobimo rezultat:

$$\begin{aligned} p(x) + q(x) &= 2x^2 + 3x + 4 \\ p(x) \cdot q(x) &= 6x^3 + 2x^2 + 9x + 3 = 2x^2 + 3x + 3 \end{aligned}$$

V splošnem veljata naslednji neenakosti:

$$\begin{aligned} \deg(p+q) &\leq \max\{\deg(p), \deg(q)\} \\ \deg(p \cdot q) &\leq \deg(p) + \deg(q) \end{aligned}$$

V primeru, da je kolobar cel oz. brez deliteljev niča, imamo zgoraj enačaja.

Trditev 133 *Pokaži, da je* $(K[x], +, \cdot)$ *kolobar.*

Dokaz.

Deljenje polinomov

Naloga 58 *Naj bosta* $f(x) = x^4 + x^3 + 2x + 2$ *in* $g(x) = x^2 + 4$ *polinoma iz* $\mathbb{Z}_5[x]$. *Izračunaj količnik* $q(x)$ *ter ostanek* $r(x)$ *pri deljenju* $f(x)$ *z* $g(x)$.

Polinoma $q(x)$ in $r(x)$ iz zgornjega primera imenujemo **količnik** in **ostanek** pri deljenju $f(x)$ z $g(x)$.

Opomba 2 *Če je* $\deg(g) > 0$, *potem velja* $\deg(r) < \deg(g)$*!*

Evklidov izrek za polinome

Izrek 134 *Naj bo F polje in $f(x)$, $g(x) \in F[x]$, kjer je* $\deg(g) > 0$. *Potem obstajata enolično določena polinoma $q(x), r(x) \in F(x)$ tako, da velja:*

$$f(x) = q(x) \cdot g(x) + r(x) \qquad in \qquad 0 \leq \deg(r) < \deg(g).$$

Dokaz. Označimo s $q(x)$ in $r(x)$ koeficient ter ostanek pri deljenju $f(x)$ z $g(x)$. Očitno za tako podana $q(x)$ in $r(x)$ velja zgornja zveza.

Zdaj pokažemo, da sta $q(x)$ in $r(x)$ enolično določena. Če to ni res, potem obstajata $q'(x)$ in $r'(x)$, za katera velja

$$f(x) = q'(x) \cdot g(x) + r'(x) \qquad \text{in} \qquad 0 \leq \deg(r') < \deg(g).$$

Potem sklepamo, da je

$$(q(x) - q'(x)) \cdot g(x) = r'(x) - r(x)$$

Če $q(x) \neq q'(x)$, potem je leva stran polinom stopnje vsaj $\deg(g)$, desna stran pa polinom stopnje strogo manjše od $\deg(g)$, kar ni možno. Torej $q(x) = q'(x)$ in od tod $r(x) = r'(x)$.

Ničle polinoma

Element $\alpha \in K$ je **ničla** oz. **koren** polinoma $p(x) = a_n x^n + \cdots a_1 x + a_0$, če velja $p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$.

Trditev 135 *Če je α ničla polinoma $p(x)$, potem obstaja polinom $q(x)$ tako, da je*

$$p(x) = (x - \alpha)q(x).$$

Dokaz. Naj bo $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Ker je $p(\alpha) = 0$, sklepamo:

$$\begin{aligned} p(x) &= p(x) - p(\alpha) \\ &= a_n(x^n - \alpha^n) + \cdots + a_1(x - \alpha). \end{aligned}$$

Iz znane zveze

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

sklepamo, da obstaja polinom $q(x)$ stopnje $n-1$, za katerega velja

$$p(x) = (x - \alpha)q(x).$$

□

Posledica 136 *Polinom $p(x) \in K[x] \setminus \{0\}$ stopnje n ima kvečjemu n ničel.*

(Ne)razcepni polinomi

Polinom $p(x) \in K[x]$ je **razcepen** nad $K[x]$, če obstajata polinoma $p_1(x), p_2(x) \in K[x]$ tako, da

$$p(x) = p_1(x) \cdot p_2(x) \qquad \text{in} \qquad 0 < \deg(p_1), \deg(p_2) < \deg(p)$$

Polinomi, ki niso razcepni, so **nerazcepni**.

Vprašanje 18 *Ugotovi, kateri od naslednjih polinomov so razcepni v* $\mathbb{Z}_2[x]$*:*

- $x^2 + 1$
- $x^2 + x + 1$
- $x^3 + x + 1$
- $x^4 + x^2 + 1$

Velja: Vsak polinom stopnje 1 je nerazcepen.

Trditev 137 *Naj bo* $p(x) \in K[x]$ *polinom stopnje 2 ali 3. Potem je* $p(x)$ *razcepen natanko takrat, ko ima ničlo.*

Modulski polinomi

Ostanek pri deljenju polinoma $f(x)$ s polinomom $g(x)$ označimo z $f(x) \mod g(x)$.

Naj bo $m(x)$ polinom stopnje n – **modulski polinom**

Naj bo $K^n[x]$ množica polinomov stopnje manjše od n, tj.

$$K^n[x] = \{p(x) \in K[x] : \deg(p) < n\}.$$

Vprašanje 19 *Naj bo K končen kolobar z m elementi. Koliko elementov ima kolobar polinomov $K^n[x]$?*

Odgovor:

Množenje $\cdot_m$ polinomov iz $K^n[x]$ definiramo takole

$$p(x) \cdot_m q(x) \quad = \quad p(x) \cdot q(x) \mod m(x)$$

Zgled: Zmnoži $f(x) = x^2 + 2$ ter $g(x) = x^2 + x + 1$ v kolobarju polinomov nad $\mathbb{Z}_3$ po modulu $m(x) = x^3 + x + 1$.

Problem 18 *Pokaži, da je* $(K^n[x], +, \cdot_m)$ *kolobar.*

Rešitev:

Galoisova polja $\mathbf{GF(p^n)}$

Izrek 138 *Kolobar* $(K^n[x], +, \cdot_m)$ *nad poljem* K *je polje natanko takrat, ko je modulski polinom* $m(x)$ *nerazcepen.*

Zgled: Sestavi polje $\mathbf{GF(4)}$ tako, da vzameš $m(x) = x^2 + x + 1$ za modulski polinom.

Zgled: Sestavi polje $\mathbf{GF(8)}$ tako, da vzameš $m(x) = x^3 + x^2 + 1$ za modulski polinom.