TEORIJA GRAFOV

Osnovni pojmi

- **graf** G je urejen par $(V(G), E(G))$ množice **vozlišč** (vertex) in **povezav** (edge) med njimi.
- **krajišči** *povezave* sta *vozlišči* $\{u, v\} \in E(G)$ (krajši zapis $uv = \{u, v\}$)
- **soseščina vozlišča** v v je $N_G(v) = \{u \in V(G) : uv \in E(G)\}$
- u **sosed** v, če velja $uv \in E(G)$. (u in v sta **sosednji** vozlišči, pišemo $u \sim v$)
- **stopnja vozlišča** v je $\deg_G(v) = |N_G(v)|$
- **maksimalna stopnja vozlišč** $\Delta(G)$
- r**-regularen graf** je tak graf, da imajo vsa vozlišča stopnjo r.
- **izolirano vozlišče** je vozlišče stopnje 0.
- **matrika sosednosti** grafa G z $V(G) = \{v_1, ..., v_n\}$ je matrika $A(G) \in \mathbb{R}^{n\times n}$ za katero velja:

$$A(G)_{i,j} = \begin{cases} 1; & v_iv_j \in E(G) \\ 0; & \text{sicer} \end{cases}$$

- **incidenčna matrika** grafa G z $V(G) = \{v_1, ..., v_n\}$ in $E(G) = \{e_1, ..., e_m\}$ je matrika $B(G) \in \mathbb{R}^{n\times m}$ za katero velja:

$$B(G)_{i,j} = \begin{cases} 1; & v_i \in e_j \\ 0; & \text{sicer} \end{cases}$$

Lema o rokovanju

Za vsak graf G velja:

$$\sum_{v\in V(G)} deg(v) = 2|E(G)|$$

Posledica: Število vozlišč lihe stopnje v grafu je sodo.

$$\sum_{v\in V(G)} deg(v) = \underbrace{\sum_{v\in V_{\text{sode}}(G)} deg(v)}_{\text{očitno sodo}} + \underbrace{\sum_{v\in V_{\text{lihe}}(G)} deg(v)}_{\text{mora biti sodo}} = \underbrace{2|E(G)|}_{\text{očitno sodo}}$$

Podgrafi

- Graf H **podgraf** grafa G, če je $V(H) \subseteq E(G)$ in $V(H) \subseteq E(G)$. Pišemo $H \subseteq G$.
- Graf H **vpeti podgraf** grafa G, če se razlikuje samo v množici povezav: $V(H) = V(G)$ in $E(H) \subseteq E(G)$.
- **inducirani** ali **porojeni** podgraf H grafa G dobimo tako da iz G odstranimo le nekatera vozlišča (in dotične povezave).

Družine grafov

$[n] = \{1, 2, ..., n\}$
$\mathbb{Z}_n = \{0, 1, ..., n-1\}$

- **polni grafi** $K_n : V(K_n) = [n] \quad E(K_n) = \{ij \mid i \neq j; i, j \in [n]\}$ (vsa vozlišča so sosednja).
- **pot** $P_n : V(P_n) = \mathbb{Z}_n \quad E(P_n) = \{i(i+1) \mid i \in \{0, ..., n-1\}\}$
- **cikel** $C_n : V(C_n) = \mathbb{Z}_n \quad E(C_n) = \{i(i+1) \mid i \in \mathbb{Z}_n\}$ ($\mathbb{Z}_n$ je grupa: $(n-1)+1 = 0$)
- **polni dvodelni graf** $K_{m,n}; m, n \geq 1$:
 $V(k_{m,n}) = \{v_1, ..., v_m\} \cup \{u_1, ..., u_n\}$
 $E(k_{m,n}) = \{v_iu_j \mid i \in [m], j \in [n]\}$
- **kocke** $Q_d; d \geq 1$:
 $V(Q_d) = \left\{\{0,1\}^d\right\} = \{(b_1, ..., b_d) \mid b_i \in \{0, 1\}\}$ ... *to so vsa binarna števila dložine d*
 $E(Q_d) = \{(b_1, ..., b_d)(p_1, ..., p_d) \mid p_1 = b_1, ..., p_i \neq b_i, ..., p_d = b_d\}$ ... *vozlišči sta sosednji, če se razlikujeta le v enem bitu.*
 Q_d je d-regularen graf.
- **posplošeni petersonovi grafi** $P_{n,k};\ n \geq 3;\ 2k < n$
 $V(P_{n,k}) = \{v_0, ..., v_{n-1}\} \cup \{u_0, ..., u_{n-1}\}$

$$\begin{aligned} E(P_{n,k}) = &\{v_iv_{i+1} \mid i \in \mathbb{Z}_n\} \cup \\ &\{\ v_iu_i \quad \mid i \in \mathbb{Z}_n\} \cup \\ &\{u_iu_{i+k} \mid i \in \mathbb{Z}_n\} \end{aligned}$$

- **Petersenov graf** $P = P_{5,2}$

Razširjene definicije grafov

- dopuščamo **zanke** (povezave iz vozlišča v isto vozlišče)
- dovolimo večkratne povezave
- **digrafi** ali grafi usmerjenih povezav (povezave so urejeni pari, vozlišča imajo lahko različno vhodno in izhodno stopnjo)
- **uteženi grafi** (omrežje) $G = (V(G), E(G))$ skupaj s funkcijo $W_V : V(G) \to \mathbb{R}$ in/ali $W_E : E(G) \to \mathbb{R}$

Poti in cikli

- **sprehod** je zaporedje vozlišč, ki so zaporedno sosednja
- **dolžina sprehoda** je število povezav v sprehodu.
- sprehod je **enostaven**, če so vse povezave različne.
- **pot** v grafu G je sprehod v katerem so vsa vozlišča različna.
- sprehod je **sklenjen**, če $v_0 = v_n$.
- **cikel** v grafu G je sklenjen sprehod, kjer so vsa vozlišča razen prvega in zadnjega različna.
- **notranje disjunktne** uv**-poti** so take uv-poti, ki imajo skupni le vozlišči u in v

Vozlišči u in v sta v relaciji $u \approx v$, če med njima obstaja uv-pot (sprehod).
$\approx$ je *ekvivalenčna relacija* in razdeli graf na ekvivalenčne razrede.
Podgrafom, ki jih inducirajo ti ekvivalenčni razredi, rečemo **komponente** grafa.
Število komponent grafa G označimo z $\Omega(G)$

- graf je **povezan**, če ima samo eno komponento.
- **razdalja** $d_G(u, v)$ je dolžina najkrajše uv-poti. Če taka pot ne obstaja je razdalja ∞.
- **premer grafa** $\text{diam}(G)$ je največja razdalja med vozlišči. (G je povezan $\Leftrightarrow$ $\text{diam}(G) < \infty$)
- **notranji premer** ali **ožina** grafa je dolžina najkrajšega cikla.

Dvodelni grafi

Graf G je **dvodelen**, če obstaja razdelitev množice $V(G)$ v množici A in B, tako, da ima vsaka povezava iz $E(G)$ eno krajišče v A in drugo v B.

$$V(G) = A \cup B \quad \text{in} \quad A \cap B = \emptyset$$

Dvodelen graf ne vsebuje lihih ciklov.

Morfizmi grafov

- **homomorfizem** iz G v H je preslikava $f : V(G) \to V(H)$, ki ohranja povezave:

$$u \sim_G v \Rightarrow f(u) \sim_H f(v)$$

- **epimorfizem** je funkcija, ki je *surjektivena* na vozliščih in povezavah.
- **monomorfizem** ali **vložitev** je funkcija, ki je *injektivna* na vozliščih (posledično na povezavah).
- Vložitev $f : G \to H$ je **izometrija**, če ohranja razdalje:

$$\forall u, v \in V(G) : d_H(f(u), f(v)) = d_G(u, v)$$

- Če je $f : V(G) \to V(H)$ bijekcija in sta f in f^{-1} homomorfizma, je f **izomorfizem**.
- Grafa G in H sta **izomorfna** ($G \cong H$), če med njima obstaja izomorfizem. *Izomorfnost grafov pomeni, da se razlikujeta le v poimenovanju vozlišč.*
- **avtomorfizem** je izomorfizem $f : G \to G$. Množico avtomorfizmov grafa G označimo $\text{Aut}(G)$. Če dodamo še operacijo komponiranja, dobimo grupo avtomorfizmov grafa G.

Operacije na grafih

Komplementarni graf

Komplementarni graf $\overline{G}$ grafa G je graf z $V(\overline{G}) = V(G)$ in

$$uv \in E(\overline{G}) \Leftrightarrow uv \notin E(G)$$

$$\overline{\left(\overline{G}\right)} = G$$

$$\text{Aut}(\overline{G}) \cong \text{Aut}(G)$$

Odstranjevanje vozlišč in povezav

Če je $X \subseteq V(G)$, je graf $G - X$ podgraf grafa G **induciran** z vozlišči $V(G) \setminus X$
Če je $F \subseteq E(G)$ potem je $G - F$ upet podgraf z množico povezav $E(G) \setminus F$.
Poljuben podgraf H grafa G lahko zapišemo kot $H = (G - X) - F$.

Skrčitev ali minor

Če je $e \in E(G)$, graf G/e dobimo tako, da identificiramo (združimo) krajišči povezave e, odstranimo zanko in morebitne večkratne povezave. (če delamo z multigrafi, pustimo večkratne povezave)
Če je $F \subseteq E(G)$, graf G/F dobimo tako, da zaporedno skrčimo vse povezave iz F.
Graf H je **minor** grafa G, če obstaja $G' \subseteq G$ in $F' \subseteq E(G')$, da je $H \equiv G'/F'$.

Subdivizije povezav

$G^+(e)$ je graf, ki ga dobimo tako, da povezavo e nadomestimo s potjo dolžine 2 (povezavo e *subdividiramo*).
Graf H je **subdivizija** grafa G, če ga lahko dobimo tako, da subdividiramo povezave v G.

Glajenje povezav

$G^-(u)$ je graf, ki ga dobimo tako, da odstranimo vozlišče u (mora biti stopnje 2) in dodamo povezavo med u-jevimi sosedi.

Kartezični produkt grafov $G \square H$

$$V(G \square H) = V(G) \times V(H)$$

$$E(G \square H) = \{(g,h)(g',h') \mid (g = g' \wedge hh' \in E(H)) \vee (h = h' \wedge gg' \in E(G))\}$$

Lastnosti

- komutativnost $G \square H \cong H \square G$
- enota $G \square K_1 \cong K_1 \square G \cong G$
- asociativnost $(G_1 \square G_2) \square G_3 \cong G_1 \square (G_2 \square G_3)$

k-povezanost grafa

- vozlišče v je **prerezno**, če ima graf $G - v$ več komponent kot G
- povezava e je **prerezna** ali **most**, če ima $G - e$ več komponent kot G.
- množica vozlišč $S \subseteq V(G)$ je **prerez** grafa G, če je $\Omega(G - S) > \Omega(G)$
- množica povezav $F \subseteq E(G)$ je **povezavni prerez** grafa G, če je $\Omega(G - F) > \Omega(G)$
- Graf G je **k-povezan**, če ima vsaj $k+1$ vozlišč in nobena podmnozica z manj kot k vozlišči ni prerezna.
- **povezanost** grafa $\kappa(G)$ je največji k za katerega je graf k-povezan. *Najmanjše stevilo vozlišč, ki jih moramo odstraniti, da graf postane nepovezan*

globalna inačica: Graf G s $k+1$ vozlišči je k-povezan $\Leftrightarrow$ za vsak par vozlišč obstaja k notranjih disjunktnih poti.
lokalna inačica: Če sta u in v nesosednji vozlišči, je maksimalno število notranjih disjunktnih uv-poti enako moči minimalne prerezne množice, ki graf razdeli tako, da sta u in v v različnih komponentah.

Drevesa

- **gozd** je graf brez ciklov
- **drevo** je *povezan* graf brez ciklov
- **list** je vozlišče stopnje 1

Vsako drevo z vsaj 2 vozliščema vsebuje vsaj dva lista.
Za poljuben graf T so ekvivalentne naslednje trditve:

- T je drevo
- za vsak par vozlišč obstaja enolična pot
- T je povezan in vsaka povezava je most
- $|E(T)| = |V(T)| - 1$

Za povezane grafe velja $|E(T)| \geq |V(T)| - 1$

Vpeta drevesa

Vpeto drevo grafa G je vpet podgraf, ki je drevo.
Graf je **povezan** $\Leftrightarrow$ vsebuje vpeto drevo.
Število vpetih dreves v grafu G označimo $T\tau G)$.
Če je e povezava multighafa G je

$$\tau(G) = \underbrace{\tau(G - e)}_{\text{odstranitev}} + \underbrace{\tau(G/e)}_{\text{skrčitev}}$$

$$\tau(G) = \tau(G_1) \cdot \tau(G_2)$$

$G_1, G_2 \subset G$ nimata nobene skupne povezave in le eno skupno vozlišče

Laplaceova matrika $L(G)$ multigrafa G je kvadratna matrika, katere vrstice in stolpci predstavljajo vozlišča.

$$L(G)_{i,j} = \begin{cases} deg(v_i); & i = j \\ -(\text{št. povezav med } v_i \text{ in } v_j); & i \neq j \end{cases}$$

Število vpetih dreves grafa G lahko izračunamo z determinanoto matrike $L(G)$, ki ji odstranimo vrstico in stolpec poljubnega vozlišča.

Prüferjeva koda

T je drevo z vozlišči $1, ..., n$. Po vrsti odstranjujemo liste z najmanjšo oznako in v kodo postavimo oznako soseda ravnokar odstranjenega lista.

Eulerjevi grafi

- **eulerjev sprehod** je sprehod, ki prehodi vsako povezavo grafa natanko enkrat.
- **eulerjev obhod** je sklenjen eulerjev sprehod.
- **eulerjev graf** je graf v katerem obstaja eulerjev obhod.
  - Povezan graf je eulerjev $\Leftrightarrow$ vsa njegova vozlišča so sode stopnje

Eulerjev obhod poiščemo z **eulerjevim algoritmom**.

- Začnemo v poljubnem vozlišču
- Premaknemo se po poljubni povezavi (most izberemo le, če ne gre drugače), ki jo za sabo pobrišemo
- Postopek ponavljamo dokler ne pridemo naokrog

Hamiltonovi grafi

- **hamiltonova pot** P v grafu G je taka, da velja $V(P) = V(G)$ (= vpeta pot)
- **hamiltonov cikel** C v grafu G je tak, da velja $V(C) = V(G)$ (= vpet cikel)
- **hamiltonov graf** je graf v katerem obstaja hamiltonov cikel.
  - Če je $S \subseteq G$ in $\Omega(G - S) > |S|$ G ni hamiltonov.
  - Naj bo G graf z $|V(G)| \geq 3$. Če za vsak par nesosednjih vozlišč u in v grafa G velja:
  $$deg_G(u) + deg_G(v) \geq |V(G)|$$
  je G hamiltonov.
  - Naj bo G graf z $|V(G) \geq 3$. Če za vsako vozlišče u velja
  $$deg(u) \geq \frac{|V(G)|}{2}$$
  je G hamiltonov.

Ravninski grafi

Ranvinski graf, je tak graf, ki ga lahko narišemo tako, da se nobeni povezavi ne sekata. Taki risbi rečemo **ravninska risba grafa**. Rečemo, da je graf **vložen v ravnino**.
Če iz ravninske risbe izrežemo vse črte in točke, dobimo nekaj ločenih območij, ki jim pravimo **lica**. Množico lic označimo z $F(G)$.
Če graf lahko vložimo v ravnino, ga lahko tudi na sfero.
Dolžina lica $l(f)$ je število povezav, ki jih prehodimo, ko obhodimo lice.
Če obhodimo vsa lica v grafu vloženem v ravnino, smo vsako povezavo prehodili dvakrat:

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

Ožina grafa $g(G)$ je dolžina najkrajšega cikla. Če graf nima cikla je $g(G) = \infty$
Očitno je $f(G) \geq g(G)$.
Če je G povezan ravninski graf vložen v ravnino, velja:

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

$$|E(G)| \geq \frac{g(G)}{2} |F(G)|$$

Naj bo G ravninski graf vložen v ravnino:

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

Če je G povezan ravninski graf, ki ni drevo ($g(G) \neq \infty$), velja

$$|E(G)| \leq \frac{g(G)}{g(G) - 2}(|V(G)| - 2)$$

Ker je $g(G) \geq 3$, velja

$$|E(G)| \leq 3|V(G)| - 6$$

Če G nima trikotnikov ($g(G) \geq 4$), velja

$$|E(G)| \leq 2|V(G)| - 4$$

Kuratowski izrek: Graf je ravninski $\Leftrightarrow$ ne vsebuje podgrafa izomorfnega subdiviziji K_5 ali $K_{3,3}$.
Wagnerjev izrek: Graf je ravninski $\Leftrightarrow$ nima minorja izomorfnega K_5 ali $K_{3,3}$.

Barvanje vozlišč

Naj bo K množica baru. Tedaj je preslikava $c : V(G) \to K$ **barvanje grafa** G. Barvanje je **dobro**, če velja:

$$\forall u, v \in V(G) \ : \ uv \in E(G) \Rightarrow c(u) \neq c(v)$$

Če je $k = |K|$ govorimo o k-barvanju. Najmanjši k za katerega obstaja doboro barvanje grafa G, imanujemo **kromatično število** grafa G; oznaka $\chi(G)$.
Če je $H \subseteq G$ je $\chi(H) \leq \chi(G)$.

Požrešni algoritem
Barve označimo z $\mathbb{N}$. Vzamemo poljubni vrstni red vozlišč grafa G. Po vrsti barvamo tako, da vozlišče v_i pobarvamo z najmanjšo možno barvo. Obstaja tak vrstni red, da požrešni algoritem porabi le $\chi(G)$ baru.

Če je G graf, je $\chi(G) \leq \Delta(G) + 1$.
Če je G povezan graf in ni C_{2n+1} ali K_n, je $\chi(G) \leq \Delta(G)$.
Za vsak ravninski graf velja $\chi(G) \leq 4$.

Barvanje povezav

Ko barvamo povezave, zahtevamo, da vse povezave s skupnim krajiščem prejmejo različne barve. Najmanjše število baru za barvanje povezav grafa G je **kromatični index** grafa; oznaka $\chi'(G)$.
Vse povezave vozlišča v dobijo različne barve, zato je $\chi'(G) \geq \Delta(G)$.

$$\chi'(G) \in \{ \underbrace{\Delta(G)}_{\text{razred 1}}, \underbrace{\Delta(G) + 1}_{\text{razred 2}} \}$$

K_{2n} je iz razreda 1, K_{2n+1} pa iz razreda 2. Vsi dvodelni grafi so iz rezreda 1.

OSNOVE ALGEBRE

Algebrske struktre

- **grupoid** $(M, \cdot)$ urejen par z neprazno množico M in zaprto opreacijo $\cdot$.
- **polgrupa** grupoid z asociativno operacijo $\forall x, y, z \in M : (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- **monoid** polgrupa z enoto $\exists e \in M\ \forall x \in M : e \cdot x = x \cdot e = x$.
- **grupa** polgrupa v kateri ima vsak element inverz $\forall x \in M\ \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x = e$.
- **abelova grupa** grupa s komutativno operacijo $\forall x, y \in M : x \cdot y = y \cdot x$.

Potence elementov

Naj bo $(A, \cdot)$ polgrupa in $a \in A$. Potem je potenca a^n, $n \in \mathbb{N}$ induktivno definirana z:

$$a^0 = e \qquad \textbf{in} \qquad a^n = a^{n-1} \cdot a$$

Iz definicije sledi:

$$a^n a^m = a^{n+m} \qquad (a^n)^m = a^{nm}$$

Recimo, da je a obrnljiv:

$$\left(a^{-1}\right)^n = (a^n)^{-1}$$

Množica $\mathbb{Z}_m$

$\mathbb{Z}_m = \{0, 1, ..., m-1\}$
Vpeljemo seštevanje $+_m$ po modulu m in množenje $\cdot_m$ po modulu m.
Dobimo grupo $(\mathbb{Z}_m, +_m)$ in monoid $(\mathbb{Z}_m, \cdot_m)$.

Cayleyeva tabela

Za vsak element množice imamo en stolpec in eno vrstico. V vsakem polju je produkt elementa stolpca in elementa vrstice.

Red elementa

Naj bo $(G, \cdot)$ grupa. Red elemneta a je najmanjše naravno število $n \in \mathbb{N}$, da velja

$$a^n = e$$

Če je grupa končna, tak eksponent vedno obstaja. Pri neskončnih grupah pa je red ∞, če tak n ne obstaja.
Red enote je 1. Enota je tudi edini element grupe, ki ima red 1.

Podgurpe

Naj bo $(G, \cdot)$ grupa. Tedaj je $H \subseteq G$ podgrupa, je je $(H, \cdot)$ grupa.
Če je H podgrupa G in $H \neq G$ pišemo $H \subset G$ (**prava podgrupa**).
$\{e\}$ je vedno podgrupa G (**trivialna grupa**).
Naj bo $(G, \cdot)$ grupa in $\emptyset \neq H \subseteq G$. Tedaj je

$$(H, \cdot) \subseteq (G, \cdot) \Leftrightarrow \forall x, y \in H : x^{-1} y \in H$$

Naj bo $(G, \cdot)$ *končna* grupa in $\emptyset \neq H \subseteq G$. Tedaj je

$$(H, \cdot) \subseteq (G, \cdot) \Leftrightarrow \cdot \text{ je notranja operacija}$$

Ciklična podgrupa

Naj bo $(G, \cdot)$ grupa in $a \in G$. Potem je $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

$$(\langle a \rangle, \cdot) \subseteq (G, \cdot)$$

Podgrupa $(\langle a \rangle, \cdot)$ je **ciklična** podgrupa v G generirana z a.
Če je G grupa ina $a \in G$ tak element, da je $\langle a \rangle = G$, je G **ciklična grupa**, element a pa **generator** grupe G.
Če ima $a \in G$ neskončen red, so vse potence a paroma različni elementi grupe G.
Če ima $a \in G$ končen red, velja

$$\forall i, j \in \mathbb{Z} : a^i = a^j \Leftrightarrow n|(i-j)]$$

$$a^n = e \ \wedge\ a^k = e \Rightarrow n|k$$

Naj bo $G = \langle a \rangle$ ciklična grupa reda n. Potem je

$$G = \langle a^k \rangle \Leftrightarrow \gcd(n, k) = 1$$

Center grupe

Naj bo $(G, \cdot)$ grupa. Potem je **center** grupe $Z(G)$ podmnožica elementov, ki komutirajo z vsemi elementi v G:

$$Z(G) = \{a \in G : ax = xa\ \forall x \in G\}$$

Center grupe G je tudi podgrupa G:

$$(Z(G), \cdot) \subseteq (G, \cdot)$$

Permutacijske grupe

- **Permutacija** množice A je bijektivna funkcija $\pi : A \to A$.
- **Permutacijska grupa** na množici A je množica premutaciji množice A, ki tvorijo grupo za komponiranje funkciji.
- **Simetrična grupa** S_n je permutacijska grupa na $[n]$, ki vsebuje vse permutacije množice $[n]$.
- **Alternirajoča grupa** A_n je grupa vseh sodih permutaciji množice $[n]$

$$A_n \subseteq S_n$$

$$\forall n > 1\ :\ |A_n| \frac{n!}{2}$$

Izomorfizmi grup

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

$$\forall a, b \in G\ :\ \alpha(a \cdot b) = \alpha(a) * \alpha(b)$$

Če je α še bijektivna, je **izomorfizem**.
Če je $G = H$, je α **avtomorfizem**.
Grupi sta **izomorfni**, če med njima obstaja izomorfizem. Pišemo $G \approx H$.
Cayleyev izrek: Vsaka grupa je izomorfna neki permutacijski grupi.
Izomorfizem grup pomeni, da imamo *isti* grupi, le da sta definirani na različna načina.
Grupi G in H z izpmorfizmom $\alpha : G \to H$ imata lastnosti:

- α preslika enoto G v enoto H.
- $\forall a \in G, n \in \mathbb{Z}\ :\ \alpha(a^n) = (\alpha(a))^n$
- $\forall a, b \in G : a\text{in}b\text{komutirata} \Leftrightarrow \alpha(a)\text{in}\alpha(b)\text{komutirata}$
- G je abelova $\Leftrightarrow$ H je abelova
- G je ciklična $\Leftrightarrow$ H je ciklična
- $K \subseteq G \Rightarrow \alpha(K) \subseteq H$

$\vdots$

Odseki grupe

Naj bo G grupa in $H \subseteq G$ ter $a \in G$.

$aH = \{ah : h \in H\}$ ... **levi odsek** grupe G po podgrupi H

$Ha = \{ha : h \in H\}$ ... **desni odsek** grupe G po podgrupi H

Lastnosti odseka:

- $a \in aH$
- $aH = H \Leftrightarrow a \in H$
- bodisi velja $aH = bH$ bodisi $aH \cap bH = \emptyset$
- $aH = bH \Leftrightarrow a^{-1} b \in H$
- $|aH| = |bH|$
- $aH = Ha \Leftrightarrow H = aHa^{-1}$
- $aH \subseteq\Leftrightarrow a \in H$

Lagrange: Če je G končna grupa in $H \subseteq G$, potem $|H|$ deli $|G|$. Število, različnih levih (desnih) *odsekov* po H je $\frac{|G|}{|H|}$.
Red elementa končne grupe deli moč grupe.
Grupa praštevilske moči je *ciklična*.
Če je G končna grupa je $a^{|G|} = e$.
Mali Fermantov izrek: $\forall a \in \mathbb{Z}, p \in \mathbb{P}\ :\ a^p \bmod p = a \bmod p$.

Podgrupe edinke

Podgrupa $H \subseteq G$ je **edinka** ($H \lhd G$), če velja:

$$\forall a \in G\ :\ aH = Ha$$

ekvivalnten pogoj:

$$\forall a \in G\ :\ aHa^{-1} = H$$

Če sta $\{e\} \lhd G$ in $G \lhd G$ edini edinki v G, je G **enostavna grupa**.
Odseki po podgrupi edinki tvorijo grupo. Naj bo G grupa in $H \subseteq G$:

$$G/H = \{aH\ :\ a \in G\} \ \ldots\ \textbf{faktorska grupa} \text{ grupe } G$$

Vpeljimo operacijo v G/H:

$$(aH)(bH) = abH$$

Če je $H \lhd G$, je G/H grupa.
Če je G grupa in $G/Z(G)$ ciklična grupa, je G abelova.

Kolobarji

Kolobar je množica R skupaj z dvema operacijama (oznaka: $+, \cdot$) tako, da velja:

- $(R, +)$ je abelova grupa
- $\forall a, b \in R\ :\ ab \in R$ (zaprtost)
- $\forall a, b, c \in R\ :\ (ab)c = a(bc)$ (asociativnost)
- $\forall a, b, c \in R\ :\ a(b + c) = ab + ac$ (distrubutivnost)
- $\forall a, b, c \in R\ :\ (a + b)c = ac + bc$ (distrubutivnost)

Kolobar je **komutativven**, če $\forall a, b \in R\ :\ ab = ba$. Kolobar je **kolobar z enoto**, če $\exists 1\ \forall a \in R\ :\ \in R : 1a = a1 = a$ element 1 je **enota kolobarja**.
Če sta R in S kolobarja, je njuna **direktna vsota** $R \oplus S$ kartezični produkt $R \times S$ opremljena z operacijama

$$(r, s) + (r', s') = (r + r', s + s') \quad \text{in} \quad (r, s)(r', s') = (rr', ss')$$

Direktna vsota kolobarjev je tudi kolobar.
Direktna vsota komutativnih kolobarjev je komutativen kolobar.
Direktna vsota kolobarjev z enoto je kolobar z enoto.

Lastnosti kolobarjev

- Enota 0 kolobarja za seštevanje je enolična.
- Če ima R enoto 1 za množenje, je enolična.
- Za kolobar R in $a, b \in R$ velja:
  - $0a = a0 = 0$
  - $(-a)b = a(-b) = -(ab)$
  - $(-a)(-b) = ab$
  - Če ima R enoto 1, $(-1)a = -(1a) = -a$

Podkolobarji

Naj bo R kolobar in $S \subseteq R$. Če je S kolobar za isti operaciji kot R, je S **podkolobar** kolobarja R.
Ekvivalentna definicija: S je podkolobar R natanko tedaj, ko:

- $0 \in S$
- $\forall a, b \in S\ :\ a - b \in S$
- $\forall a, b \in S\ :\ ab \in S$

Center kolobarja

Center kolobarja R je

$$\{x \in R \ : \ ax = xa \quad \forall a \in R\}$$

Center kolobarja R je tudi njegov podkolobar.

Delitelji niča in celi kolobarji

Naj bo R komutativen koloboar. Tedaj je $a \in R, \ a \neq 0$ **delitelj niča**, če

$$\exists b \in R, \ b \neq 0 \ : \ ab = 0$$

Cel kolobar je komutativen kolobar z enoto ($1 \neq 0$), ki nima deliteljev niča.
Pravilo krajšanja: Če je R cel kolobar, potem velja
$ab = ac, \ a \neq 0 \Rightarrow b = c$.

Polja in obsegi

Komutaiteven obseg z enoto ($1 \neq 0$) je **polje**, če je vsak element različen od 0 obrnljiv.
Polju, ki pa ni komutativno, pravimo **obseg**.
Polje je cel kolobar (obratno pa ni nujno).
Če je R končen cel kolobar, je R polje.
Naslednje trditve so ekvivalentne:

- $\mathbb{Z}_n$ je cel kolobar
- $\mathbb{Z}_n$ je polje
- n je prašetevilo

Podpolja

Če je F polje, je $K \subseteq F$ podpolje v F natoanko tedaj, ko:

- $1 \in K$
- $\forall a, b \in K \ : \ a - b \in K$
- $\forall a, b \in K, \ b \neq 0 \ : \ ab^{-1} \in K$

Karakteristika kolobarja

Če je R kolobar, $a \in R$ in $n \in \ltimes$, pišemo

$$na = \underbrace{a + a + ... + a}_{n\text{-krat}}$$

Karakteristika kolobarja R je najmanjši $n \in \mathbb{N}$, tako da velja

$$\forall a \in R \ : \ na = 0$$

Če tak n ne obstaja je karakteristika enaka 0. *Oznaka:* $\text{char}R$
Naj bo R kolobar ze enoto. Tedaj velja:

- Če je red 1 v grupi $(R, +)$ enak $n < \infty$, je $\text{char}R = n$.
- Če pa ima 1 v grupi $(R, +)$ neskončen red, je $\text{char}R = 0$.

Če je R cel kolobar, je $\text{char}R \in 0 \cup \mathbb{P}$.

Ideali

imajo pri kolobarjih podobno vlogo kot podgrupe edinke pri grupah.
Podkolobar I kolobarja R je **ideal**, če

$$\forall i \in I; \forall r \in R \ : \ ir \in I \ \wedge ri \in I$$

Če je R kolobar in $I \subseteq R$, je I ideal natanko tedaj, ko velja:

- $0 \in I$
- $\forall i, j \in I \ : \ i - j \in I$
- $\forall i \in I; \forall r \in R \ : \ ir \in I \ \wedge ri \in I$

Če je R kolobar z enoto in ideal I vsebuje obrnljiv element, je $I = R$. Če je F polje, sta njegova edina ideala F in $\{0\}$.
Naj bosta I in J ideala v kolobarju R. Definirajmo operaciji:

- $I + J = \{i + j \ : \ i \in I, \ j \in J\}$
- $IJ = \{i_1 j_1 + ... + i_n j_n : i_k \in I, \ j_k \in J, \ n \in \mathbb{N}\}$

Če sta I in J ideala v R, potem je

- $I + J$ ideala v R
- IJ ideala v R

Naj bo I ideal kolobarja R. Tedaj je množica levih odsekov

$$R/I = \{a + I \ : \ a \in R\}$$

skupaj z operacijama

$$(a + I) + (b + I) = a + b + I$$
$$(a + I)(b + I) = ab + I$$

faktorski kolobar.

Kolobarji polinomov

Naj bo R komutativen kolobar. Tedaj je

$$R[x] = \left\{a_n x^n + ... + a_1 x + a_0 \ : \ a_i \in R, n \in \mathbb{N}_0\right\}$$

kolobar polinomov nad R.
Stopnja polinoma $f(x) \in R[x]$ je m, če $a_m \neq 0$ in $a_i = 0$ za vse $i > m$.
a_m je tedaj **vodilni koeficient**, $a_m x^m$ pa **vodilni člen**.
Ničelni polinom 0 nima niti stopnje, niti vodilnega člena ali koeficienta.
Konstantni polinom $f(x) = a_0$ je bodisi ničelni, bodisi ima stopnjo 0.
Množenje in seštevanje polinomov je definirano:

$$f(x) = a_n x^n + ... + a_0$$
$$g(x) = b_n x^n + ... + b_0$$
$$f(x) + g(x) = (a_n + b_n)x^n + ... + (a_1 + b_1)x + (a_0 + b_0)$$
$$f(x)g(x) = c_{n+n} x^{n+n} + ... + c_1 x + c_0$$
$$c_i = a_0 b_i + a_1 + b_{i-1} + a_2 b_{i-2} + ... + a_i b_0$$

- Če je R komutaitven kolobar, je tudi $R[x]$ komutativen kolobar.
- Če je R cel kolobar, je tudi $R[x]$ cel kolobar.
- Naj bo $R[x]$ cel kolobar in $f(x), g(x) \in R[x]$ neničelna polinoma stopenj n in m.
  - $\deg(f(x) + g(x)) \leq max\{n, m\}$ (ali pa je $f(x) + g(x) = 0$)
  - $\deg(f(x)g(x)) = n + m$.

Izrek o deljenju polinomov: Naj bo F polje in
$f(x), g(x) \in F[x]; \ g(x) \neq 0$, potem obstajata enolična polinoma
$q(x), r(x) \in F[x]$, da velja

$$f(x) = g(x) \cdot \underbrace{q(x)}_{\text{količnik}} + \underbrace{r(x)}_{\text{ostanek}}$$

Kjer je bodisi $r(x) = 0$, bodisi $\deg(r(x)) < \deg(g(x))$.

Ničle polinomov in nerazcepni polinomi

Naj bo F polje. Tedaj je $f(x) \in F[x]$ **nerazcepen polinom**, če

$$\forall f(x), g(x) \in F[x] \ : \ f(x) = g(x)h(x) \Rightarrow g(x) \in F \ \vee \ h(x) \in F$$

sicer, je $f(x)$ **razcepen polinom**.
Naj bo $f(x) \in F[x]$ in $b \in F$. Tedaj lahko izračunamo $f(x)$ v b:
$f(b) = a_n b^n + ... + a_0$.

Naj bo F polje, $f(x) \in F[x]$ in $a \in F$. Potem obstaja $q(x) \in F[x]$, da

$$f(x) = (x - a)q(x) + f(a)$$

Naj bo F polje in $f(x) \in F$. Če je $a \in F$ in velja $f(a) = 0$, je a **ničla polinoma**.

$$a \text{ je ničla } f(x) \Leftrightarrow (x - a) | f(x)$$

- Če ima $f(x)$ ničlo, je razcepen (ni pa nujno obratno).
- Naj bo F polje in $f(x) \in F[x]; \deg(f(x)) \in \{2, 3\}$. Potem je $f(x)$ nerazcepen natanko tedaj, ko nima ničle.
- Neničeln polinom stopnje n ima največ n ničel iz F.