# 1 Cela števila

1. Osnovni izrek o deljenju celih števil
   - Načelo dobre urejenosti v $\mathbb{N}$.
   - Načeli dobre urejenosti v $\mathbb{Z}$.
   - **Izrek.** Osnovni izrek o deljenju celih števil. Ostanek.
2. Največji skupni delitelj
   - **Definicija.** Kadar pravimo, da celo število $k \neq 0$ deli celo število $m$? Zapis.
   - **Definicija.** Delitelj. Število $m$ deljivo s številom $k$.
   - **Definicija.** Skupni delitelj. Največji skupni delitelj.
   - **Izrek.** Obstoj največjega skupnega delitelja. Kako lahko ga zapišemo?
   - **Definicija.** Tuji števili.
   - **Posledica.** Kadar sta števili $m$ in $n$ tuji?
3. Osnovni izrek aritmetike
   - **Definicija.** Praštevila.
   - **Lema.** Evklidova lema.
   - **Izrek.** Osnovni izrek aritmetike.
   - **Izrek.** Ali je praštevil neskončno?

# 2 Uvodni pojmi algebre

1. Binarne operacije
   - **Definicija.** Binarna operacija na množice $S$.
   - *Primer.* Najpomembnejše operacije: seštevanje, množenje in komponiranje. Množica preslikav iz $X$ vase.
   - *Primer.* Navedi primeri in protiprimeri binarnih operacij.
   - **Definicija.** Kadar pravimo, da množica zaprta za operacijo? Notranja operacija.
   - *Primer.* Navedi primeri in protiprimeri množic zaprtih za operacijo.
   - **Definicija.** Zunanja binarna operacija.
   - *Primer.* Navedi primer zunanji operaciji.
   - **Definicija.** Asociativna operacija.
   - **Definicija.** Kadar pravimo, da sta elementa $x$ in $y$ komutirata? Komutativna operacija.
   - *Primer.* Navedi primeri in protiprimeri asociativnih in komutativnih operacij.
   - **Definicija.** Nevtralni element.
   - *Primer.* Navedi primeri nevtralnih elementov za različne operacije na različnih množicah.
   - **Trditev.** Enoličnost nevtralnega elementa.
   - **Definicija.** Levi nevtralni element. Desni nevtralni element.
   - *Opomba.* Kako sta povazana levi in desni nevtralna elementa?
   - *Primer.* Ali lahko obstaja več levih nevtralnih elementov?
2. Polgrupe
   - Kaj je algebrska struktura?
   - **Definicija.** Polgrupa $(S, \star)$.
   - *Primer.* Navedi primeri in protiprimeri polgrup.
   - **Trditev.** Ali lahko oklepaje v polgrupe vedno odpravimo?
   - **Definicija.** Potenca elementa $x \in S$.
   - *Primer.* Kakšne formule veljajo za potence v polgrupi?
3. Monoidi
   - **Definicija.** Monoid $(S, \star)$.
   - *Primer.* Navedi primeri in protiprimeri monoidov.
   - **Definicija.** Levi inverz. Desni inverz. Inverz. Obrnljiv element.
   - **Trditev.** Kadar lahko krajšamo v monoidu?
   - *Primer.* Koliko obrnljivih elementov ima vsak monoid?
   - *Primer.* Naštej obrnljive elemente v $(\mathbb{N}_0, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$.
   - *Primer.* Naj bo $\mathcal{F}(X)$ množica vseh funkcij iz $X$ vase.
     - Kadar $f \in \mathcal{F}(X)$ ima levi inverz? Kadar jih ima več?
     - Kadar $f \in \mathcal{F}(X)$ ima desni inverz? Kadar jih ima več?
     - Kadar $f \in \mathcal{F}(X)$ ima inverz?
   - **Trditev.** Ali so levi in desni inverzi elementa $x \in S$ sovpadata?
   - **Posledica.** Kaj če ima nek element levi in desni inverz?
   - **Posledica.** Kaj velja, če je element $x \in S$ obrnjiv in $yx = 1$?
   - **Posledica.** Koliko lahko inverzov ima obrnjiv element monoida?
   - **Trditev.** Ali je produkt obrnjivih elementov monoida obrnjiv? Kako dobimo inverz produkta?
   - *Opomba.* Kako lahko definiramo potenco obrnjivega elementa monoida za vsa cela števila?

### Rezultati vaj

- Ali je v končnem monoidu levi inverz avtomatično tudi desni inverz?
- Ali je element monoida obrnljiv, če obrnljiva neka njegova potenca?

# 3 Uvod v teorijo grup

1. Grupe
   - **Definicija.** Grupa. Abelova grupa.
   - *Opomba.* Zapiši definicijo grupe preko aksiomov. Enota. Inverz elementa.
   - *Opomba.* Koliko so enot v grupi? Koliko inverzov ima vsak element? Računanje s potenci.
   - *Opomba.* Multiplikativni in aditivni zapis. Dogovor o aditivni grupi.
   - **Trditev.** Pravila krajšanja v grupi.
   - **Definicija.** Končna grupa. Red grupe.
   - **Trditev.** Kako iz monoida dobimo grupo? **Množica obrnljivih elementov monoida**.
2. Primeri grup
   - Navedi primeri in protiprimeri številskih grup za seštevanje in množenje.
   - Kaj je trvialna grupa?
   - Kaj je $(\mathcal{F}(X))^*$? Permutacija. **Simetrična grupa** $\mathrm{Sim}(X)$ množie $S$. Ali je komutativna?
   - **Grupa permutacij** $S_n$ končne množice $[n]$:
     - Ali je vsaka permutacija produkt disjunktnih ciklov?
     - Ali je vsaka permutacija produkt transpozicij?
     - Sode in lihe permutacije. Predznak permutacije. Čemu je enak predznak produkta permutacij?
     - Čemu je enak red grupe $S_n$?
   - Množica vseh realnih $n \times n$ matrik $M_n(\mathbb{R})$:
     - Ali je Abelova grupa za seštevanje?
     - Kaj pa za množenje? **Splošna linearna grupa** $\mathrm{GL}_n(\mathbb{R})$. Ali je Abelova?
     - Ali lahko $\mathbb{R}$ zamenjamo z poljubnim poljem?
   - Opiši simetrije kvadrata. **Diedrska grupa** $D_8$.
     - S čim je enolično določena simetrija?
     - Ali je $D_8$ Abelova?
   - **Diedrska grupa** $D_{2n}$. Opiši elementi $D_{2n}$.
   - **Diedrska grupa** $D_4$ simetrij pravokotnika, ki ne kvadrat.
   - Direktni produkt grup $G_1, G_2, \ldots, G_n$. Direktna vsota grup.
3. Podgrupe
   - **Definicija.** Podgrupa.
   - *Opomba.* Vsaj koliko podgrup ima vsaka grupa? Trvialna podgrupa. Prava podgrupa.
   - *Opomba.* Naj bo $H \leq G$. Ali je enota grupe $G$ vsebovana v $H$?
   - **Trditev.** 3 ekvivalantne trditve o podgrupe $H$ grupe $G$.
   - *Opomba.* Kako karakterizacije podgrupe zgledajo v aditivnem zapisu?
   - **Posledica.** Kadar je končna podmnožica $H$ grupe $G$ podgrupa?
   - *Opomba.* Kakšne oblike inverz vsakega elementa $x \in G$, če je $G$ končna grupa?
   - **Trditev.** Opiši podgrupe grupe $(\mathbb{Z}, +)$.
   - **Trditev.** Ali je poljuben presek podgrup podgrupa?
   - **Definicija.** Produkt podgrup $H$ in $K$ grupe $G$.
   - *Opomba.* Ali je produkt podgrup nujno podgrupa.
   - **Trditev.** Zadosten pogoj, da bi bil produkt podgrup podgrupa.
   - *Opomba.* Kaj velja, če je $G$ Abelova?

4. Primeri podgrup
   - Določi osnovne podgrupe v $(\mathbb{C}, \cdot)^*$. Ali so podgrupe tudi:
     - $\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\}$.
     - $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.
     - $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. **Krožna grupa** $\mathbb{T}$.
     - $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$. **$n$-to koreni enote** $\mathbb{U}_n$.
   - **Alternirajoča grupa** $A_n$.
   - Ali je diedrska grupa $D_{2n}$ podgrupa v $S_n$?
   - Pokaži da so podgrupe grupe $\mathrm{GL}_n(F)$:
     - $\mathrm{SL}_n(F) = \{A \in M_n(F) \mid \det(A) = 1\})$. **Specialna linearna grupa** $\mathrm{SL}_n$.
     - $O_n = \left\{A \in M_n(\mathbb{R}) \mid AA^T = I\right\}$. **Ortogonalna grupa** $O_n$. **Specialna ortogonalna grupa** $SO_n$.
     - $U_n = \left\{A \in M_n(\mathbb{C}) \mid AA^H = I\right\}$. **Unitarna grupa** $U_n$. **Specialna unitarna grupa** $SU_n$.
   - **Trditev.** **Konjugirana podgrupa** podgrupe $H$.
   - **Trditev.** **Center** $Z(G)$ grupe $G$.
   - **Trditev.** **Centralizator** $C_G(a)$ elementa $a$ v $G$.
5. Odseki in Lagrangeev izrek
   Naj bo $G$ grupa in $H \leq G$. Definiramo relacijo na $G$ s predpisom

$$\forall a, b \in G \,.\, a \sim b :\Leftrightarrow a^{-1}b \in H$$

   .
   - **Trditev.** Relacija $\sim$ je ekvialenčna.
   - **Definicija.** Ekvivalenčni razred elementa $a \in G$. Levi odsek grupe $G$ po podgrupi $H$.
   - *Opomba.* Kadar $aH = H$?
   - *Opomba.* Kako pišemo odseke, če je $G$ Abelova?
   - *Primer.* Kaj so odseke, če:
     - $G = (\mathbb{R}^2, +)$, $H$ abscisna os.
     - $G = \mathbb{C}^*$, $H = \mathbb{T}$.
     - $G = S_n$, $H = A_n$.
   - *Opomba.* S kakšno relacijo dobimo desni odseki?
   - *Opomba.* Ali je grupa $G$ disjunktna unija odsekov?
   - **Definicija.** Faktorska (oz. kvocientna) množica.
   - *Opomba.* Ali je $G/H$ nujno grupa?
   - **Lema.** Kadar sta dva odseka enaka?
   - **Definicija.** Indeks podgrupe $H$ v grupi $G$.
   - **Izrek.** Lagrangeev izrek.
   - **Posledica.** Kaj lahko povemo o moči vsake podgrupe končne grupe?
6. Grupa ostankov
   - *Opomba.* Naj bo $G$ Abelova. Kako lahko definiramo seštevanje na $G/H$?
   - **Trditev.** Ali je $(G/H, +)$ Abelova?
   - Naj bo $n \in \mathbb{N}$. Kadar pravimo da sta $a, b \in \mathbb{Z}$ kongruentni po modulu $n$?
   - Karakteriziraj kongruentnost z ostanki.
   - Opiši kongruentnost kot relacijo na $\mathbb{Z}$.
   - *Primer.* **Grupa ostankov** $\mathbb{Z}_n$ po modulu $n$.
   - *Opomba.* Ali za vsak $n \in \mathbb{N}$ obstaja vsaj ena grupa moči $n$?

7. Ciklične grupe
   - Naj bo $G$ grupa, $a \in G$. Kaj je $\langle a \rangle$? Ali je to podgrupa grupe $G$? Ali je Abelova?
   - **Definicija.** Ciklična podgrupa. Ciklična grupa. Generator grupe.
   - *Primer.* Ali so ciklične:
     - $\mathbb{Z}$, $\mathbb{Z}_n$.
     - $\mathbb{U}_n$.
     - $D_4$.
   - **Definicija.** Naj bo $G$ grupa. Naj bo $a \in G$. Red elementa $a$.
   - *Primer.* Katere elemente v grupe $G$ imajo red 1?
   - *Primer.* Določi red:
     - 1 v $\mathbb{Z}$, 1 v $\mathbb{Z}_n$.
     - $e^{\frac{2\pi i}{n}}$ v $\mathbb{U}_n$.
     - Transpozicij v $S_n$.
     - Simetrij v $D_4$.
   - **Trditev.** Karakterizacija reda elementa (kadar je enak $n \in \mathbb{N}$)?
   - **Posledica.** Kadar je končna grupa ciklična?
   - **Posledica.** Naj bo $G$ končna grupa:
     - Kako so povezani redi elementov $a \in G$ in moč $G$?
     - Naj bo $a \in G$. Čemu je enako $a^{|G|}$?
   - **Posledica.** Naj bo $G$ končna grupa. Recimo, da je $|G|$ praštevilo. Kaj lahko povemo o $G$?
8. Generatorji grup
   - **Definicija.** Podgrupa generirana z množico $X$.
   - *Opomba.* Zakaj je definicija smiselna?
   - **Trditev.** Kako izgledajo elementi $\langle X \rangle$?
   - *Opomba.* Kaj če je $G$ Abelova?
   - **Definicija.** Kadar pravimo, da je grupa $G$ generirana z $X$? Generatorji grupe $G$.
   - *Primer.* Obravnavaj primera:
     - S čim je generirana vsaka podgrupa grupe $\mathbb{Z}$?
     - Naj bo $X \subseteq \mathbb{Z}$. Kaj je $\langle X \rangle$?
     - S čim je generirana grupa $\mathbb{Q}^+$?
     - S čim je generirana grupa $D_{2n}$?
     - S čim je generirana grupa $S_n$?
     - S čim je generirana grupa $A_n$, $n \geq 3$?
   - **Definicija.** Končno generirana grupa.
   - *Primer.* Ali je $(\mathbb{Z}, +)$ končno generirana?
   - *Primer.* Pokaži, da $\mathbb{Q}$ ni končno generirana.

**Rezultati z vaj**

1. Grupe
   - Ali je polgrupa z deljenjem grupa?
   - Zadostni pogoj, da je grupa Abelova.
2. Grupa permutacij
   - Kako zapišemo permutacijo kot produkt transpozicij?
   - Kako dobimo inverz $k$-cikla?
   - Konjugiranje cikla.
   - Kadar pravimo, da permutaciji $\pi, \pi' \in S_n$ imata enako zgradbo disjunktnih ciklov?
   - Kako sta povezana komutativnost in konjugiranje?
   - S čim je generirana grupa $S_n$?
3. Diedrska grupa
   - Grupa $D_\infty$.
4. Podgrupe
   - Diagonalna podgrupa.
   - Kaj velja, če unija dveh podgrup podgrupa? Ali isto velja za unijo treh podgrup?
   - Zadostna pogoja, da je presek dveh končnih podgrup trivialen.
   - Naj bosta $H, G \leq G$, $H, G$ končni. Čemu je enaka $|HK|$?
5. Ciklične grupe
   - Kadar je $\mathbb{Z}_n$ vsebuje podgrupo reda $k$? Alo je ta podgrupa enolična?
   - Kaj lahko povemo o vsake podrupe cilkične grupe?
   - Naj bo $k \in \mathbb{Z}_n$. Čemu je enak $\mathrm{red}(k)$? Kadar je $\langle k \rangle = \mathbb{Z}_n$?
   - Kakšna je zveza med $\mathrm{red}(a)$ in $\mathrm{red}(a^{-1})$, $\mathrm{red}(a)$ in $\mathrm{red}(bab^{-1})$ ter $\mathrm{red}(ab)$ in $\mathrm{red}(ba)$?
   - Koliko podgrup ima neskončna grupa?

# 4 Uvod v teorijo kolobarjev

1. Definicije kolobarja, obsega in polja
   - **Definicija.** Kolobar.
   - **Trditev.** 3 lastnosti kolobarja $K$:
     - Množenje z nevtralnim elementom $0 \in K$.
     - Množenje z nasprotnim elementom $-x \in K$. Množenje nasprotnih elementov.
     - Množenje z $-1 \in K$.
   - *Primer.* Trivialni (ničelni) kolobar.
   - **Trditev.** Naj bo $K$ neničeln. Kaj lahko povemo o 0 in 1?
   - **Definicija.** Komutativen kolobar.
   - **Definicija.** Delitelj niča. Levi delitelj niča, desni delitelj niča.
   - *Primer.* Poišči delitelja niča v $M_2(\mathbb{R})$.
   - **Definicija.** Idempotent. Nilpotent.
   - *Primer.* Poišči idempotenti in nilpotenti v $M_2(\mathbb{R})$. Kako so povezani z delitelji niča?
   - *Opomba.* Pravilo krajšanja v kolobarju brez deliteljev niča.
   - **Definicija.** Cel kolobar.
   - **Definicija.** Obseg. Polje.
   - **Trditev.** Ali lahko obrnljiv element delitelj niča? Ali v obsegu so delitelji niča?
   - *Primer.* Ali je $\mathbb{Z}$ cel kolobar? Ali je obseg?
2. Definicija algebre
   - **Definicija.** Vektorski prostor.
   - **Trditev.** 4 lastnosti vektorskega prostora.
   - **Definicija.** Algebra nad poljem $\mathbb{F}$. Realna algebra. Kompleksna algebra.
   - *Primer.* Navedi osnovni primeri kolobarjev, obsegov, polj in algeber.
3. Primeri kolobarjev in algeber
   - Številski kolobarji, polja in algebre.
   - Algebra funkcij $\mathbb{R}^X$. Kaj dobimo, če je $X = \mathbb{N}$? **Algebra realnih zaporedij**.
   - **Kolobar polinomov ene spremenljivke**.
     - **Definicija.** Polinom $f(X)$. Koeficienti polinoma $f(X)$. Kaj so $X^i$?
     - **Definicija.** Kadar sta polinoma enaka? Vsota polinomov. Produkt polinomov.
     - **Definicija.** Kolobar polinomov ene spremenljivke nad kolobarjem $K$. Oznaka.
     - **Trditev.** Karakterizacija komutativnosti kolobarja $K[X]$.
     - **Trditev.** Kadar $K[X]$ nima deliteljev niča?
     - **Posledica.** Kadar je $K[X]$ cel kolobar?
     - Kako naravno postane $K[X]$ algebra? Ali lahko nad $K$?
   - **Kolobar formalnih potenčnih vrst** $K[[X]]$.
   - **Kolobar polinomov več spremenljivk.**
     - **Definicija.** Monom.
     - **Definicija.** Kolobar polinomov dveh spremenljivk. Kolobar polinomov $n$ spremenljivk.
   - Naj bo $K$ cel kolobar. Kako ga povečamo do polja? **Polje ulomkov celega kolobarja** $K$.
     - **Definicija.** Relacija na $K \times K \setminus \{0\}$.
     - **Trditev.** Ali je ekvivalenčna? Oznaka za ekvivalenčni razred elementa $(a, b) \in K \times K \setminus \{0\}$.
     - **Definicija.** Seštevanje in množenje na $K \times K \setminus \{0\}$.
     - *Opomba.* Ali sta seštevanje in množenje dobro definirani.
     - **Trditev.** Ali s tem postane $K \times K \setminus \{0\}$ polje?
     - **Definicija.** Polje $F$ ulomkov celega kolobarja $K$.
     - *Opomba.* Kako kolobar $K$ vložimo v polje $F$? Kaj če je $K$ že polje?
     - *Opomba.* Kaj je polje ulomkov kolobarja $\mathbb{Z}$?
     - **Definicija.** Polje racionalnih funkcij.
   - **Kolobar matrik** $M_n(K)$ nad kolobarjem $K$.
     - Ali je komutativen? Ali ima delitelji niča?
     - Kako dobimo algebro?

- **Kolobar endomorfizmov** $\mathrm{End}_F(V)$ vektorskega prostora $V$ nad poljem $F$.
  - **Definicija.** Linearna preslikava. Endomorfizem vektorskega prostora $V$.
  - **Definicija.** Seštevanje, množenje s skalarji na $\mathrm{End}_F(V)$.
  - Ali je $\mathrm{End}_F(V)$ algebra?
- **Algebra kvaternionov** $\mathbb{H}$.
  - Ali obstaja realna algebra lihe dimenzije več kot 1, ki je obseg?
  - Naj bo $\mathbb{H}$ vektorski prostor z bazo $\{1, i, j, k\}$.
  - **Definicija.** Množenje na $\mathbb{H}$.
  - **Trditev.** Ali je $\mathbb{H}$ algebra?
  - **Definicija.** Kvaternioni.
  - *Opomba.* Ali je $\mathbb{H}$ komutativna?
  - **Definicija.** Konjugirani kvaternion.
  - **Trditev.** Ali je $\mathbb{H}$ obseg?
  - **Definicija.** **Kvaternionska grupa** $Q$.
  - *Opomba.* Ali so $\mathbb{R}, \mathbb{C}, \mathbb{H}$ edini končnorazsežne realne algebre, ki so obsegi?
- **Direktni produkt kolobarjev**.
  - **Definicija.** Direktni produkt kolobarjev.
  - *Opomba.* Kadar direktni produkt kolobarjev ima delitelje niča? Ali je direktni produkt polj tudi polje?
  - **Definicija.** Direktni produkt algeber.

4. Podkolobarji, podalgebre in podpolja
   - **Definicija.** Podkolobar $L$.
   - *Primer.* Zakaj moramo zahtevati, da $1 \in L$?
   - **Definicija.** Podalgebra.
   - *Opomba.* Kaj je podalgebra v jeziku linearne algebre in podkolobarjev?
   - **Definicija.** Podpolje $F$.
   - *Primer.* Zakaj ni zahtevamo, da $1 \in F$?
   - **Definicija.** Razširitev polja.
   - *Primer.* Navedi številski primeri raźširitev.
   - **Trditev.** Karakterizacija podkolobarja.
   - **Trditev.** Karakterizacija podalgebre.
   - **Definicija.** Podobseg.
   - **Trditev.** Karakterizacija podpolja (podobsega).
   - *Opomba.* Ali je presek podkolobarjev, podprostorov, podalgeber in podpolj spet ustrezna podstruktura?
   - *Primer.* Primeri podkolobarjev, podalgeber, podpolj.
     - Navedi primer številskega zaporedja podkolobarjev.
     - Kako lahko opišemo odnos med $\mathbb{R}$ in $\mathbb{C}$?
     - Ali je $K[X]$ podkolobar v kolobarju $K[[X]]$? Kaj pa v $K[X, Y]$?
     - Kakšen odnos med celimi kolobarji in njihovimi polji ulomkov?
     - Množica vseh diagonalnih matrik v $M_n(\mathbb{R})$.
     - Množica vseh zgoraj trikotnih matrik v $M_n(\mathbb{R})$. Kaj pa množica vseh strogo zgoraj trikotnih matrik?
     - **Algebra** $C(X)$ vseh zveznih funkcij.
     - Množica $c$ konvergentnih zaporedij v algebre realnih zaporedij.
     -
   - *Primer.* **Kolobar Gaussovih celih števil** $\mathbb{Z}[i]$.
   - *Primer.* **Center** $Z(K)$ kolobarja $K$.

5. Kolobarji ostankov in karakteristika kolobarja.
   - *Opomba.* Ali je vsak kolobar vsebuje kopijo celih števil?
   - **Definicija.** Karakteristika kolobarja $K$.
   - **Trditev.** 3 lastnosti kolobarja s karakteristiko $n \in \mathbb{N}$.
   - **Posledica.** Kako karakteristiko lahko ima polje?
   - **Definicija.** Množenje v $\mathbb{Z}_n$.
   - **Trditev.** Ali je $\mathbb{Z}_n$ komutativen kolobar? **Kolobar** $\mathbb{Z}_n$ ostankov po modulu $n$.
   - **Lema.** Kaj lahko povemo o končnem celem kolobarju?
   - *Opomba.* Ali predpostavka o komutativnosti odveč? Kaj lahko sklepamo?
   - **Trditev.** Kadar je $\mathbb{Z}_p$ polje?
   - *Primer.* Navedi osnovni primeri kolobarjev in polj s različno karakterizacijo.
   - **Izrek.** Vali Fermatov izrek.
6. Generatorji kolobarjev, algeber in polj
   - **Definicija.** Naj bo $K$ kolobar in $X \subseteq K$. Podkolobar, generiran z $X$.
   - **Definicija.** Generatorji. Končno generiran kolobar.
   - *Opomba.* Zapiši isti definiciji za obseg, polje in algebro.
   - **Trditev.** Opiši podkolobar, generiran z množico $X$.
   - **Trditev.** Opiši podalgebro, generirano z množico $X$.
   - **Trditev.** Opiši podpolje, generirano z množico $X$.
   - *Primer.* Primeri generatorjev.
     - Kaj je podkolobar kolobarja $\mathbb{C}$, generiran z 1?
     - Kaj je podpolje kolobarja $\mathbb{C}$, generirano z 1?
     - Kaj je podkolobar kolobarja $\mathbb{C}$, generiran z $i$?
     - Kaj je podpolje kolobarja $\mathbb{C}$, generirano z $i$?
     - Kaj je podkolobar kolobarja $\mathbb{R}[X]$, generiran z $X$?
     - S čim je generirana realna algebra $\mathbb{R}[X]$?
     - S čim je generirana algebra $M_2(\mathbb{R})$? Čemu je enaka $\dim M_2(\mathbb{R})$.
     - Kaj je podkolobar kolobarja $M_2(\mathbb{R})$, generiran z $E_{12}$ in $E_{21}$?

## Rezultati z vaj

1. Kolobarji, obsegi, polja
   - Kako iz kolobarja brez enote lahko naredimo kolobar z enoto?
   - **Boolov kolobar.** Primer Boolova kolobarja.
2. Algebre
   - Ali je $\mathbb{Z}$ lahko algebra nad kakim poljem?
   - Naj bo $A$ končnorazsežna algebra.
     - Kaj velja za vsak $a \in A \setminus \{0\}$?
     - Kaj če ima $a \in A$ levi ali desni inverz?
     - Recimo, da je $A$ tudi obseg. Kaj lahko povemo o vsaki podalgebri?
   - Algebra kvaternionov.
     - Čemu je enak $Z(\mathbb{H})$? Čemu je enak $Z(Q)$?
     - Kaj lahko povemo o enačbi $h^2 + \alpha h + \beta = 0$ za vsak $h \in \mathbb{H}$?
   - Kolobar $\mathbb{Z}_n$.
     - Kadar je $k \in Z_n$ obrnljiv?
     - Koliko je obrnljivih elementov v $\mathbb{Z}$? Koliko v $\mathbb{Z}_n$? Kaj če je $n$ praštevilo?

# 5 Homomorfizmi

1. Pojem homomorfizma
   - *Primer.* Cayleyeva tabela. Izomorfnost $D_4$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
   - *Primer.* Homomorfizem iz kolobarja $\mathbb{Z}$ v kolobar $\mathbb{Z}_n$.
   - *Opomba.* Kako lahko nasploh opišemo homomorfizem?
   - **Definicija.** Homomorfizem grup (vektorskih prostorov, kolobarjev, algeber).
   - **Definicija.** Izomorfizem, epimorfizem, monomorfizem (oz. vložitev), endomorfizem, avtomorfizem.
   - *Primer.* Ali je $\varphi : \mathbb{R} \to M_2(\mathbb{R}),\ \varphi(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ homomorfizem kolobarjev oz. algeber?
   - *Primer.* Zakaj je smiselen izraz „vložitev“?
     - Naj bosta $G_1$ in $G_2$ grupi. Kako lahko vložimo $G_1$ v $G_1 \times G_2$?
     - Kako lahko vložimo $S_n$ v $S_{n+1}$?
     - Kako lahko polje realnih števil vložimo v polje kompleksnih števil?
     - Kako lahko vložimo kolobar $K$ v kolobar $K[X]$?
     - Kako lahko vložimo cel kolobar v njegovo polje ulomkov?
   - **Trditev.** Kam homomorfizem grup slika enoto in inverz?
   - *Opomba.* Aditivni zapis prejšnje trditve. Kam homomorfizmi kolobarjev oz. algeber slikajo 0 in 1?
   - **Trditev.** Kam homorfizem kolobarjev slika obrnljive elemente?
   - **Definicija.** Slika homomorfizma (homomorfna slika).
   - **Trditev.** Kaj lahko povemo o slike homomorfizma grup (kolobarjev, algeber)?
   - **Definicija.** Jedro homomorfizma. Trivialno jedro.
   - **Trditev.** Karakterizacija injektivnosti homomorfizma.
   - *Primer.* Izomorfizem vs. trivialni homomorfizem grup.
   - **Trditev.** Kaj lahko povemo o kompozitumu homomorfizmov?
   - **Trditev.** Kaj lahko povemo o inverzni preslikavi izomorfizma?
   - **Posledica.** Kaj lahko povemo o množice vseh avtomorfizmov grupe (kolobarja, algebre) za operacijo $\circ$?
   - **Definicija.** Izomorfni grupi.
   - **Trditev.** Ali je izomorfnost ekvivalenčna relacija?
   - *Primer.* Kaj se ohranja pri izomorfizmih?
   - **Trditev.** Karakterizacija izmorfnosti končnorazsežnih vektorskih prostorov.
2. Primeri homomorfizmov grup
   - Naj bo $G$ Abelova. Ali je $x \mapsto x^{-1}$ avtomorfizem? Kaj pa $x \mapsto x^m$? Kaj če $x \mapsto x^{-1}$ avtomorfizem?
   - Izomorfnost $Z$ in $n\mathbb{Z}$, kjer $n \in \mathbb{N}$.
   - Ali obstajajo netrivialni homomorfizmi iz $\mathbb{Z}_n$ v $\mathbb{Z}$?
   - Čemu je izomorfna vsaka neskončna ciklična grupa? Čemu pa končna ciklična grupa?
   - Ali sta $\mathbb{Z}$ in $\mathbb{Z}_n$ edini ciklični grupi?
   - Ali je $z \mapsto |z|$ epimorfizem grup $\mathbb{C}^*$ in $\mathbb{R}^*$? Kaj je njegovo jedro?
   - Izomorfnost $\mathbb{R}$ in $\mathbb{R}^+$ (eksponentna funkcija).
   - Ali je $x \mapsto e^{ix}$ epimorfizem grup $\mathbb{R}$ in $\mathbb{T}$? Kaj je njegovo jedro?
   - Epimorfizem iz $S_n$ v $(\{1, -1\}, \cdot)$. Kaj je njegovo jedro?
   - Epimorfizem iz $\mathrm{GL}_n(F)$ v $F^*$. Kaj je njegovo jedro?
   - Naj bosta $G_1$ in $G_2$ grupi. Projekcija na $G_1$. Vložitev $G_1$ v $G_1 \times G_2$.
   - Kleinova četverka. Čemu je izomorfna vsaka grupa reda 4?
   - **Notranji avtomorfizem** $\varphi_a$ grupe $G$. Kaj lahko povemo o konjugiranih podgrupih?
   - **Grupa** $\mathrm{Aut}(G)$ vseh avtomorfizmov. **Grupa** $\mathrm{Inn}(G)$ vseh notranjih avtomorfizmov.
   - Epimorfizem iz grupe $G$ v grupo $\mathrm{Inn}(G)$. Kaj je njegovo jedro?

3. Primeri homorfizmov kolobarjev
   - Naj bo $K$ komutativen kolobar. **Evalvacijski homomorfizem.**
     - **Definicija.** Vrednost (ali evalvacija) polinoma v elementu $x \in K$.
     - **Definicija.** Evalvacijski homomorfizem iz $K[X]$ v $K$.
     - Kaj je jedro evalvacijskega homomorfizma?
     - Kako ta homomorfizem lahko pospološimo na polinome več spremenljivk?
   - Kako idejo evalvacijskega homomorfizma lahko prenesemo v kolobarje funkcij? Kaj je jedro?
   - **Notranji avtomorfizem** $\varphi_a$ kolobarja $K$.
   - Naj bo $V$ $n$-rasežen vektroski prostor nad $F$. Izomorfnost algeber $\mathrm{End}_F(V)$ in $M_n(F)$.
   - Naj bo $K$ komutativen kolobar z praštevilsko karakteristiko $p$. Brucove sanje. Frobeniusov endomorfizem.
   - Čemu so izomorfni naslednji podkolobarji kolobarja $M_2(F)$:
     - $K_1 = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in \mathbb{R} \right\}$.
     - $K_2 = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$.
     - $K_3 = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$.
     - $K_4 = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid z, w \in \mathbb{C} \right\}$.

# 6 Kvocientne strukture

1. Podgrupe edinke in kvocientne grupe, I
   - *Primer.* Navedi primer grupe $G$ in podgrupe $H$, v kateri operacija $(aH)\cdot(bH)=(ab)H$ ni dobro definirana na $G/H$ (element reda 2).
   - **Definicija.** Podgrupa edinka.
   - *Opomba.* Ali za $N \lhd G$ velja, da $N \leq G$?
   - *Primer.* Primeri edink.
     - Vsaj koliko podgrup edink ima vsaka grupa?
     - Katere podgrupe Abelove grupe so edinke?
     - Ali je $Z(G)$ edinka? Ali je vsaka podgrupa $Z(G)$ edinka?
     - Navedi primeri podgrup, ki niso edinke.
     - Netrivialna edinka. Prava edinka.
   - **Definicija.** Enostavna grupa.
   - **Trditev.** 3 pogoja, ekvivalentnih definicije edinke.
   - *Opomba.* Ali je podgrupa edinka enaka svojim konjugiranim podgrupam?
   - **Trditev.** Kaj lahko povemo o
     - Produktu podgrupe in edinke.
     - Produktu edink.
     - Preseku edink.
   - **Definicija.** Naj bo $N \lhd G$. Definicija množenja na $G/N$.
   - **Izrek.** Ali je $G/N$ grupa? Epimorfizem $\pi : G \to G/N$. Kaj je $\ker \pi$?
   - **Definicija.** Kvocientna grupa. Kanonični epimorfizem.
   - *Primer.* Navedi osnovni primer kvocientne grupe.
   - *Opomba.* Naj bo $G$ končna in $N \lhd G$. Čemu je enaka $|G/N|$?
   - **Trditev.** Kadar je $N \subseteq G$ edinka v $G$ (jedro homomorfizma).
   - **Definicija.** Kvocientni vektorski prostor.
2. Ideali in kvocientni kolobarji, I
   - **Definicija.** Ideal. Levi (desni) ideal.
   - *Primer.* Primeri idealov.
     - Vsaj koliko idealov ima kolobar?
     - Naj bo $K$ kolobar in $a \in K$. Ali je $aK$ desni ideal? **Glavni ideal** $(a)$. Glavni ideali v $\mathbb{Z}$.
     - Kaj je množica matrik oblike $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}, x, y \in \mathbb{R}$ v $M_2(\mathbb{R})$? Poišči še drug podoben ideal.
   - **Trditev.** Naj bo $I \subseteq K$ enostranski ali dvostranski ideal. Zadostni pogoj, da $I = K$.
   - *Opomba.* Ali je ideal zaprt za množenje? Ali je podkolobar?
   - *Opomba.* Kaj so enostranski oz. dvostranski ideali v obsegu?
   - **Definicija.** Enostaven kolobar.
   - **Definicija.** Vsota idealov. Produkt idealov.
   - **Trditev.** Kaj lahko povemo o
     - Vsote idealov.
     - Produktu idealov.
     - Preseku idealov.
   - *Opomba.* Ali trditev velja za enostranske ideale?
   - *Primer.* Uredi po vsebovanosti $IJ,\ I\cap J,\ I+J$. Naj bo $I=4\mathbb{Z},\ J=6\mathbb{Z}$. Izračunaj $IJ,\ I\cap J,\ I+J$.
   - **Definicija.** Naj bo $I \lhd K$. Definicija seštevanja in množenja na $K/I$.
   - **Izrek.** Ali je $K/I$ kolobar? Epimorfizem $\pi : I \to K/I$. Kaj je $\ker \pi$?
   - **Definicija.** Kvocientni kolobar. Kanonični epimorfizem.
   - *Primer.* Navedi osnovni preimer kvocientnega kolobarja.
   - **Trditev.** Kadar je $I \subseteq K$ ideal v $K$ (jedro homomorfizma)?
   - **Definicija.** Ideal algebre. Kvocientna algebra. Kanonični epimorfizem.
   - **Izrek.** Ali so operacije dobro definirane? Jedro Kanoničniga epimorfizma.

3. Izrek o izomorfizmu
   - **Izrek.** 1. izrek o izomorfizmu.
   - Nariši diagram homomorfizmov iz izreka.
4. Podgrupe edinke in kvocientne strukture, II
   - **Izrek.** Čemu je izomorfna vsaka cilična grupa?
   - **Posledica.** Kadar je netrivialna grupa $G$ nima pravih netrivialnih podgrup?
   - **Lema.** Naj bo $G$ grupa, $a \in G$.
     - Naj bo $\mathrm{red}(a) = n$. Kadar je $a^m = 1, m \in \mathbb{Z}$?
     - Naj bo $a \neq 1$ in $a^p = 1$ za neko praštevilo $p$. Kaj potem $\mathrm{red}(a)$?
     - Naj bo $\mathrm{red}(a) = n$ in $N \lhd G$. Kaj lahko povemo o redu odseka $aN$?
   - **Izrek.** Cauchyjev izrek za Abelove grupe.
   - **Lema.** Naj bo $\varphi : G \to G$ homomorfizem grup.
     - Recimo, da $H' \leq G'$. Kaj lahko povemo o $\varphi^*(H')$?
     - Recimo, da $N' \lhd G'$. Kaj lahko povemo o $\varphi^*(N')$?
     - Recimo, da $H \leq G$. Kaj lahko povemo o $\varphi_*(H)$?
     - Recimo, da $N \lhd G$ in je $\varphi$ epimorfizem. Kaj lahko povemo o $\varphi_*(N)$?
   - **Izrek.** Korespondenčni izrek.
5. Primeri ednik in kvocientnih grup
   - Pokaži da $G/\{1\} \cong G$ in $G/G \cong \{1\}$.
   - Kadar je $H \leq \mathbb{Z}_n$?
   - Naj bo $G = (\mathbb{R}^2, +)$, $H$ abscisna os. Čemu je izomorfna $G/H$?
   - Čemu je izomorfna grupa $C^*/\mathbb{T}$?
   - Čemu je izomorfna grupa $S_n/A_n$?
   - Čemu je izomorfna grupa $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$?
   - Naj bo $G_1, G_2$ grupi. $\overline{G_1} := \{(x_1, 1) \mid x_1 \in G_1\} \leq G_1 \times G_2$. Čemu je izomorfna $G_1 \times G_2/\overline{G_1}$?
   - Čemu je izomorfna grupa $G/Z(G)$?
6. Ideali in kvocientni kolobarji, II
   - **Definicija.** Maksimalni ideal.
   - **Izrek.** Naj bo $M$ ideal komutativnega kolobarja. Kadar je $M$ maksimalni ideal?
   - **Izrek.** Kaj lahko povemo o vsakem pravem idealu kolobarja?
   - *Opomba.* Ali isti rezultat velja za enostranski ideali?
7. Primeri idealov in kvocientnih kolobarjev
   - Pokaži da $K/\{0\} \cong K$ in $K/K \cong \{0\}$.
   - Kadar je $p\mathbb{Z}$ maksimalni ideal kolobarja $\mathbb{Z}$?
   - Naj bo $K$ kolobar. Naj bo $I$ množica vseh polinomov iz $K[X]$ s konstantnim členom 0.
     - Ali je $I$ ideal kolobarja $K[X]$? Kako lahko zapišemo vsak odsek $f(x) + I$?
     - Čemu je izomorfen kolobar $K[X]/I$?
     - Kadar je $I$ maksimalni ideal?
   - Naj bo $x \in [a, b]$.
     - Ali je $I_x := \{f \in C[a, b] \mid f(x) = 0\}$ ideal kolobarja $C[a, b]$?
     - Čemu je izomorfen kolobar $C[a, b]/I_x$?
     - Ali je $I_x$ maksimalni ideal?
   - Poišči podobni kot prej ideali direktnega produkta kolobarjev. Čemu je izomorfen kvocient?
   - **Prapolje** $F_o$ polja $F$.
     - Čemu je lahko enako $\mathrm{char} F_0$?
     - Čemu je izomorfno $F_0$?
   - Nekaj o polinomih TODO