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 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?

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** 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 $a^{|G|}$?
     - Kaj če je $|G|$ praštevilo?
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.