

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 Uvod v teorijo grup

1. Osnovni pojmi teoriji grup

- **Definicija.** Binarna operacija na množici S . Kadar pravimo, da je operacija asociativna. Kadar pravimo, da je operacija komutativna?
- **Definicija.** Polgrupa.
- **Definicija.** Nevtralni element.
- **Trditev.** Ali če v množici S obstaja enota za operacijo $*$, potem je ena sama?
- **Definicija.** Monoid.
- **Definicija.** Levi inverz. Desni inverz. Inverz.
- **Definicija.** Obrnljiv element.
- **Trditev.** Kaj če v monoidu ima element x levi in desni inverz?
- **Posledica.** Koliko inverzov lahko ima obrnljiv element v monoidu?
- **Posledica.** Kaj če je x obrnljiv element monoida in $xy = 1$?
- **Trditev.** Obrnljivost produkta obrnljivih elementov.
- **Definicija.** Grupa. Abelova grupa.
- **Definicija.** Multiplikativni in aditivni zapis operacije. Kdaj jih uporabljamo?
- **Trditev.** Računanje z potenci v grupi. Pravilo krajšanja v grupi.
- **Zgled.** Primeri številskih grup. Simetrična grupa množice X . Grupa permutacij.
- **Zgled.** Grupa simetrij kvadrata. Diedrska grupa D_{2n} moči $2n$.
- **Zgled.** Kako iz monoida dobimo grupo? Splošna linearna grupa $GL_n(\mathbb{F})$.
- **Zgled.** Direktni produkt grup.

2. Grupa permutacij S_n

- **Izrek.** Kako lahko zapišemo vsako permutacijo?
- **Definicija.** Transpozicija.
- **Trditev.** Kako lahko zapišemo vsako permutacijo z pomočjo transpozicij? Koliko je transpozicij v tem zapisu?
- **Definicija.** Soda permutacija. Liha permutacija. Znak permutacije.
- **Trditev.** Znak produkta permutacij.

3. Podgrupe

- **Definicija.** Podgrupa.
- **Opomba.** Kaj sta vedno podgrupi grupe G ? Ali je enota vedno vsebovana v podgrupi? Ali se enota deduje pri monoidih?
- **Trditev.** Dve karakterizaciji podgrupe.
- **Posledica.** Karakterizacija podgrupe končne grupe G .
- **Zgled.**
 - Kakšne so oblike vse prave podgrupe grupe \mathbb{Z} ?
 - Specialna linearna grupa $SL_n(\mathbb{F})$. Grupa ortogonalnih matrik $O_n(\mathbb{F})$. Specialna grupa ortogonalnih matrik $SO_n(\mathbb{F})$.
- **Trditev.** Ali je presek podgrup grupe G podgrupa grupe G ?
- **Definicija.** Produkt podgrup.
- **Zgled.** Ali je produkt podgrup vedno podgrupa?
- **Trditev.** Zadosten pogoj, da je produkt podgrup podgrupa.
- **Zgled.** Konjugiranje podgrupe $H \leq G$ z elementov $a \in G$. Ali je konjugiranje podgrupa?

- **Zgled.** Center $Z(G)$ grupe G . Centralizator $C_a(G)$ elementa $a \in G$. Ali sta podgrupi?
 - **Zgled.** Krožna grupa \mathbb{T} . n -ti koreni enote \mathbf{U}_n . Ali sta podgrupi \mathbb{C}^* ?
 - **Zgled.** Alternirajoča grupa A_n .
4. Odseki podgrup in Lagrangeev izrek
 Naj bo G grupa in $H \leq G$.
- Relacija \sim na G . ki porodi leve odseke.
 - **Trditev.** Ali je relacija \sim ekvivalenčna?
 - **Definicija.** Ekvivalenčni razred elementa $a \in G$.
 - **Definicija.** Ekvivalenčne razredi po relaciji \sim . Levi odseki G po podgrupe H .
 - **Opomba.** Z kakšno ekvivalenčno relacijo dobimo desne odseke?
 - **Definicija.** Kvocientna množica glede na relacijo \sim .
 - **Opomba.** Kaj tvorijo ekvivalenčni razredi glede na množico G ?
 - **Opomba.** Ali je G/H vedno grupa? Kadar sta dva odseka enaka? Ali je G/H končna, če je G končna?
 - **Definicija.** Indeks podgrupe H .
 - **Izrek.** Lagrangeev izrek.
 - **Posledica.** Ključni pomen izreka.
 - **Opomba.** Kako lahko definiramo operacijo na G/H , če je G Abelova?
 - **Trditev.** Ali je s prej definirano operacijo G/H Abelova grupa?
 - **Zgled.** Grupa ostankov po modulu n . Ali za vsako naravno število n obstaja grupa moči n ?
5. Generatorji grup. Ciklične grupe
 Naj bo G grupa ter $X \subseteq G$.
- **Definicija.** Podgrupa, generirana z množico X .
 - **Opomba.** Ali je $\langle X \rangle$ vedno obstaja?
 - **Definicija.** Grupa, generirana z množico X . Generatorji grupe. Končno generirana grupa. Ciklična grupa.
 - **Trditev.** Kako zgledajo elementi $\langle X \rangle$?
 - **Posledica.** Kako zgledajo elementi $\langle x \rangle$?
 - **Zgled.** Generatorji grup \mathbb{Z} in \mathbb{Z}_n .
 - **Zgled.** S čim sta generirani grupi D_{2n} in S_n ? Ali je A_n generirana z 3-cikli?
 - **Zgled.** Ali je grupa \mathbf{U}_n ciklična? Kaj pa D_4 ?
 - **Zgled.** Ali je \mathbb{Q}^* končno generirana?
 - **Definicija.** Red elementa.
 - **Zgled.** Kateri elementi v grupi imajo red 1? Kakšen red imajo transpozicije v grupi S_n ?
 - **Trditev.** Karakterizacija reda elementa.
 - **Posledica.** Kdaj je končna grupa G ciklična?
 - **Posledica.** Kaj lahko povemo o redu elementa a v končni grupi? Kaj če je $|G|$ praštevilo?

Rezultati vaj

1. Monoidi
 - (naloga 2.21) Ali je v končnem monoidu levi inverz avtomatično tudi desni inverz? Kakšno obliko ima?
 - (naloga 2.22) Ali je element monoida obrnljiv, če obrnljiva neka njegova potenca?
2. Grupe
 - (naloga 3.10) Ali je polgrupa z deljenjem grupa?
 - (naloga 3.9) Zadostni pogoj, da je grupa Abelova.
3. Grupa permutacij
 - Kako zapišemo permutacijo kot produkt transpozicij?
 - (naloga 3.13) Kako dobimo inverz k -cikla?
 - (naloga 3.19) Konjugiranje cikla.
 - (naloga 3.20) Kadar pravimo, da permutaciji $\pi, \pi' \in S_n$ imata enako zgradbo disjunktnih ciklov?
 - (naloga 3.21) Kako sta povezana komutativnost in konjugiranje?
 - (naloga 3.103) S čim je generirana grupa S_n ?
4. Diedrska grupa
 - (naloga 3.22) Grupa D_∞ .
5. Podgrupe
 - (naloga 3.31) Diagonalna podgrupa.
 - (naloga 3.60) Naj bosta $H, G \leq G$, H, G končni. Čemu je enaka $|HK|$?
6. Ciklične grupe
 - (naloga 3.71) Kadar je \mathbb{Z}_n vsebuje podgrupo reda k ? Ali je ta podgrupa enolična?
 - (naloga 3.72) Kaj lahko povemo o vsake podgrupe ciklične grupe?
 - (naloga 3.81) Naj bo $k \in \mathbb{Z}_n$. Čemu je enak $\text{red}(k)$? Kadar je $\langle k \rangle = \mathbb{Z}_n$?
 - (naloga 3.85) Ali je konjugiranje ohranja red elementa?

3 Uvod v teorijo kolobarjev

1. Uvod v teorijo kolobarjev

- **Definicija.** Kolobar. Enica kolobarja. Komutativen kolobar.
- **Zgled.** Številski kolobarji. Kolobar matrik. Kolobar \mathbb{R}^X , kjer $X \subseteq \mathbb{R}$.
- **Definicija.** Levi/desni delitelj ničā. Delitelj ničā. Idempotent. Nilpotent.
- **Opomba.** Kako so idempotenti in nilpotenti povezani z delitelji ničā?
- **Opomba.** Ali v kolobarjih brez delitelja ničā velja pravilo krajšanja?
- **Zgled.** Delitelji ničā v $\mathbb{R}^{2 \times 2}$. Idempotenti v poljubnem kolobarju. Nilpotenti v $\mathbb{R}^{n \times n}$.
- **Definicija.** Cel kolobar.
- **Zgled.** Ali je $(\mathbb{Z}, +, \cdot)$ cel kolobar?
- **Definicija.** Obseg. Polje.
- **Zgled.** Številski polja.
- **Trditev.** Ali lahko obrnljiv element kolobarja delitelj ničā?
- **Definicija.** Algebra nad poljem \mathbb{F} .

2. Primeri kolobarjev in algeber

- Kolobar (algebra) kvadratnih matrik. Algebra endomorfizmov.
- Algebra realnih funkcij.
- Polinomi:
 - **Definicija.** Polinom s koeficienti iz kolobarja K .
 - Seštevanje in množenje v $K[X]$.
 - Polinomi več spremenljivk. Kolobar formalnih potenčnih vrst.
 - **Trditev.** Ali je $K[X]$ komutativen, če je K komutativen? Ali je isto velja, če je K brez deliteljev ničā ali K cel?
- Polje ulomkov celega kolobarja K :
 - Ekvivalenčna relacija na $P = K \times (K \setminus \{0\})$.
 - Množenje in seštevanje na P/\sim .
 - **Trditev.** Ali je $(P/\sim, +, \cdot)$ polje?
 - **Zgled.** Polje ulomkov kolobarja \mathbb{Z} .
 - Kako lahko K vložimo v P/\sim ?
- **Trditev.** Potreben pogoj, da je algebra nad \mathbb{R} obseg.
- Algebra kvaternionov:
 - Baza prostora kvaternionov.
 - Definicija množenja v \mathbb{H} .
 - **Definicija.** Kvaternioni. Konjugiran kvaternion.
 - **Trditev.** Ali je \mathbb{H} obseg? Ali je algebra?
 - **Definicija.** Kvaternionska algebra \mathbb{H} . Kvaternionska grupa Q .
- **Zgled.** Ali je direktni produkt polj lahko polje?

3. Podkolobarji, podalgebre, podpolja

- **Definicija.** Podkolobar. Podalgebra. Podpolje.
- **Zgled.** Zakaj moramo zahtevati, da podkolobar vsebuje enico?
- **Definicija.** Razšeritev polja.
- **Trditev.** Karakterizacija podkolobarja.
- **Trditev.** Karakterizacija podalgebre.
- **Trditev.** Karakterizacija podpolja.
- **Zgled.** Številski primeri podkolobarjev. Odnos med celi kolobarji in njihovim

poljem ulomkov.

- **Zgled.** Podkolbar Gaussovih celih števil $\mathbb{Z}[i]$.
 - **Zgled.** Podalgebra zgornje trikotnih matrik v $\mathbb{R}^{n \times n}$. Podalgebra zveznih funkcij v \mathbb{R}^X , kjer $X \subseteq \mathbb{R}$.
 - **Zgled.** Center kolobarja.
 - **Zgled.** Podalgebra konvergentnih zaporedij.
4. Kolobar ostankov in karakteristika kolobarja
- Definicija množenja v \mathbb{Z}_n . Ali je dobra?
 - **Trditev.** Ali je $(\mathbb{Z}_n, +, \cdot)$ komutativen kolobar?
 - **Definicija.** Karakteristika kolobarja.
 - **Zgled.** Določi $\text{char } \mathbb{Z}$ ter $\text{char } \mathbb{Z}_n$.
 - **Trditev.** Naj bo K kolobar s karakteristiko $n > 0$.
 - Čemu je enako $n \cdot x$ za vsak $x \in K$?
 - Kdaj je $m \cdot 1 = 0$?
 - Kaj če je K neničeln kolobar in nima deliteljev nič?
 - **Lema.** Ali je končen cel kolobar vedno polje?
 - **Opomba.** Ali lema še vedno drži brez predpostavki o komutativnosti? Ali so vsi končni obsegi komutativni?
 - **Trditev.** Kdaj je \mathbb{Z}_n polje?
 - **Zgled.** Karakteristika kolobarja matrik $M_k(\mathbb{Z}_n)$, kolobarja polinomov $\mathbb{Z}_n[X]$, polja racionalnih funkcij $\mathbb{Z}_p(X)$.
 - **Izrek.** Mali Fermatov izrek. **TODO: ***
5. Generatorji kolobarjev, algeber, polj
- **Definicija.** Podkolobar (podalgebra, podpolje) generiran z množico X .
 - **Trditev.** Kako zgledajo elementi v podkolobarju (podalgebre, podpolju), ki je generiran z množico X ?
 - **Zgled.**
 - 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
 - (naloga 4.3) Kako iz kolobarja brez enote lahko naredimo kolobar z enoto?
 - (nalogi 4.10-4.11) *Boolov kolobar*. Primer Boolova kolobarja.
2. Algebre
 - (naloga 4.27) Ali je \mathbb{Z} lahko algebra nad kakim poljem?
 - (naloga 4.30) 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.
 - (naloga 4.52) Čemu je enak $Z(\mathbb{H})$? Čemu je enak $Z(Q)$?
 - (naloga 4.56) Kaj lahko povemo o enačbi $h^2 + \alpha h + \beta = 0$ za vsak $h \in \mathbb{H}$?
 - Kolobar \mathbb{Z}_n .
 - Kadar je $k \in \mathbb{Z}_n$ obrnljiv?
 - Koliko je obrnljivih elementov v \mathbb{Z} ? Koliko v \mathbb{Z}_n ? Kaj če je n praštevilo?

4 Homomorfizmi

1. Homomorfizmi

- **Definicija.** Homomorfizem grup.
- **Definicija.** Homomorfizem kolobarjev (polj).
- **Opomba.** Zakaj pri homomorfizmu kolobarjev zahtevamo, da je $f(1) = 1$? Zakaj to ni potrebno pri grupih?
- **Trditev.** Kam homomorfizem slika obrnljive elemente?
- **Definicija.** Homomorfizem algeber.
- **Definicija.** Endomorfizem, monomorfizem (vložitev), epimorfizem, izomorfizem, avtomorfizem.
- **Definicija.** Izomorfni strukturi.
- **Trditev.** Ali je f^{-1} izomorfizem, če je f izomorfizem?
- **Trditev.** Ali je kompozitum homomorfizmov homomorfizem?
- **Definicija.** Slika homomorfizma. Jedro homomorfizma.
- **Trditev.** Ali sta jedro in slika podgrupi (podkolobarji, podalgebre)?
- **Trditev.** Karakterizacija injektivnosti homomorfizma.
- **Zgled.** Potenciranje $a \mapsto a^m$, $m \in \mathbb{Z}$ kot endomorfizem grupe G .
 - Kaj če je $m = -1$?
 - Kaj če je $a \mapsto a^{-1}$ avtomorfizem grupe G ?
- **Zgled.** Izomorfizem grup \mathbb{Z} in $n\mathbb{Z}$
- **Zgled.** Homomorfizem grup \mathbb{Z} in \mathbb{Z}_n . Kaj je $\text{im } f$ ter $\ker f$? Ali obstajajo netrivialni homomorfizmi iz \mathbb{Z}_n v \mathbb{Z} ?
- **Zgled.** Ali je $f : \text{GL}_n(\mathbb{F}) \rightarrow \mathbb{F}^*$, $f(A) = \det A$ epimorfizem grup? Kaj je $\ker f$?
- **Zgled.** Ali je $f : S_n \rightarrow -1, 1$, $f(\pi) = \text{sgn } \pi$ epimorfizem grup? Kaj je $\ker f$?
- **Zgled.** Naj bo G grupa ter $a \in G$. Konjugiranje. Ali je avtomorfizem? Notranji avtomorfizem grupe G .
- **Zgled.** Grupa notranjih avtomorfizmov $\text{Inn } G$ kot podgrupa v grupi $\text{Aut } G$ avtomorfizmov grupe G .
- **Zgled.** Naj bo K komutativen kolobar. Evalvacija polinoma v točki x . Ali je homomorfizem?
- **Zgled.** Brucove sanje. **TODO: ***
- **Zgled.** Čemu so izomorfni naslednji podkolobarji kolobarja $M_2(F)$:
 - $K_1 = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in \mathbb{R} \right\}$.
 - $K_2 = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$.
 - $K_3 = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$.
 - $K_4 = \left\{ \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \mid z, w \in \mathbb{C} \right\}$.

Rezultati z vaj

1. Homomorfizmi

- (naloga 5.4) S čim je vsak homomorfizem natančno določen?
- (nalogi 5.5-5.6) Kdaj obstaja homomorfizem $\varphi : \mathbb{Z} \rightarrow G$, $\varphi(1) = a$? Kdaj obstaja homomorfizem $\varphi : \mathbb{Z}^n \rightarrow G$, $\varphi(1) = a$?
- (naloga 5.20) Kaj lahko reče o homomorfne slike?
- (naloga 5.50) Ali je homomorfna slika idempotenta idempotent?

5 Kvocientne strukture

1. Kvocientne grupe

Naj bo G grupa in $H \leq G$. Kdaj lahko na množici G/H vpeljemo operacijo z predpisom

$$(aH) \cdot (bH) = (ab)H?$$

- **Zgled.** Kdaj ne moremo vpeljati tako operacijo?
- **Definicija.** Podgrupa edinka v G .
- **Zgled.** Kaj so vedno edinki v G ? Enostavne grupe. Center grupe. Kaj so edinki v Abelovih grupah? Nekomutativna grupa, kjer je vsaka podgrupa edinka. Edinki v S_3 .
- **Trditev.** 4 karakterizacije edink.
- **Trditev.** Zadosten pogoj, da je grupa edinka (indeks podgrupe).

Dokaz. Karakterizacija $aH = Ha$. □

- **Zgled.** Ali je $A_n \triangleleft S_n$? Ali je $\langle r \rangle \triangleleft D_{2n}$?
- **Trditev.** Recimo, da $H \leq G$ in $N \triangleleft G$. Kaj lahko povemo o produktu podgrup? Kaj če tudi $H \triangleleft G$? Presek edink.

Dokaz. Definicija podgrupe ednike. □

- **Izrek.** Kvocientna grupa. Epimorfizem π grup G in G/N . Jedro ker π .
- **Izrek.** 1. izrek o izomorfizmu. **TODO: ***
- **Opomba.** Kaj so edinke (jedra)? Kanonični epimorfizem. Diagram.
- **Izrek.** 2. izrek o izomorfizmu.
- **Izrek.** 3. izrek o izomorfizmu.
- **Lema.** Naj bo $\varphi : G \rightarrow H$ homomorfizem grup, $K \subseteq G$, $L \subseteq H$.
 - Zadosten pogoj, da je $\varphi_*(K) \leq H$;
 - Zadosten pogoj, da je $\varphi_*(K) \triangleleft H$;
 - Zadosten pogoj, da je $\varphi^*(L) \leq G$;
 - Zadosten pogoj, da je $\varphi^*(L) \triangleleft G$.
- **Izrek.** Korespondenčni izrek.

2. Uporaba izrekov

- **Trditev.** Opis cikličnih grup do izomorfizma natančno.
- **Trditev.** Opis podgrup v \mathbb{Z}_n .
- **Trditev.** Naj bo G netrivialna grupa. Kdaj nima G pravih netrivialnih podgrup?
- **Lema.** Naj bo G grupa, $N \triangleleft G$ in $a \in G$. Kaj lahko povemo o redu elementa aN , če red elementa a enak $n \in \mathbb{N}$?
- **Izrek.** Cauchyjev izrek za Abelove grupe. **TODO: ***

Dokaz. Indukcija po $n = |G|$. □

- **Zgled.** Čemu so izomorfne grupe S_n/A_n , $GL_n(\mathbb{F})/SL_n(\mathbb{F})$, $G_1 \times G_2/\overline{G_1}$, kjer $\overline{G_1} = \{(g, 1) \mid g \in G_1\}$, in $G/Z(G)$? Ali so kvocienti dobro definirani?

3. Kvocientni kolobarji

Naj bo K kolobar ter $(I, +) \leq (K, +)$. Radi bi na K/I vpeljali množenje z predpisom

$$(a + I) \cdot (b + I) = ab + I.$$

- **Definicija.** Ideal. Levi (desni) ideal.
- **Zgled.** Kaj so vedno ideali v K ? Enostavni kolobarji. aK in Ka kot ideali. Glavni ideal. Ideali v \mathbb{Z} .
- **Zgled.** Desni ideal, ki ni levi v $\mathbb{R}^{2 \times 2}$. Levi ideal, ki ni desni v $\mathbb{R}^{2 \times 2}$. Ali je $\mathbb{R}^{n \times n}$ enostaven?
- **Opomba.** Ideali v algebri.
- **Trditev.** Kvocientni kolobar.
- **Trditev.** Kaj če (levi/desni) ideal vsebuje obrnljiv element?
- **Trditev.** Presek idealov. Produkt idealov. Vsota idealov.
- **Izrek.** 1. izrek o izomorfizmu. **TODO: ***
- **Opomba.** Kaj so ideali (jedra)? Kanonični epimorfizem. Diagram.
- **Izrek.** 2. izrek o izomorfizmu.
- **Izrek.** 3. izrek o izomorfizmu.
- **Izrek.** Korespondenčni izrek.
- **Definicija.** Maksimalen ideal.
- **Izrek.** Karakterizacija maksimalnih idealov. **TODO: ***

Dokaz. (\Rightarrow) Naj bo $a + M \in K/M \setminus \{0\}$. Oglejmo si ideal $M + aK$.

(\Leftarrow) Vzemimo strogo večji od M ideal. □

- **Opomba.** Zakaj potrebujemo predpostavko o komutativnosti?
- **Izrek.** Ali je vsak pravi ideal vsebovan v nekem maksimalnem idealu? **(*)**

6 Klasifikacija končnih Abelovih grup

1. Direktni produkt

Naj bo G grupa.

- **Definicija.** Direktni notranji produkt edink N_1, \dots, N_s .
- **Zgled.** Zapis produkta grup kot produkt edink.
- **Lema.** Karakterizacija kdaj je G notranji direktni produkt edink N_1, \dots, N_s .
- **Definicija.** Komutator elementov $x, y \in G$.
- **Opomba.** Kaj in zakaj meri komutator?
- **Lema.** Recimo, da $M, N \triangleleft G$ in $M \cup N = \{1\}$. Kaj lahko povemo o elementih M in N ?
- **Izrek.** Kaj če G notranji direktni produkt edink N_1, \dots, N_s . **TODO: ***
- **Zgled.**
 - Ali zapis grupe G kot notranji direktni produkt vedno obstaja?
 - Zapiši D_4 kot notranji direktni produkt pravih edink. Čemu je izomorfna D_4 ?
 - Zapiši $GL_n(\mathbb{R})$, kjer je n liho število, kot notranji direktni produkt $SL_n(\mathbb{R})$ in grupe skalarnih matrik. Čemu je enak center grupe $GL_n(\mathbb{R})$?
- **Opomba.** Neskončni notranji produkt. Ali izrek še vedno drži?
- **Definicija.** Naj bo G Abelova. Direktna vsota edink N_1, \dots, N_s .

2. Klasifikacija končnih Abelovih grup

Naj bo G končna Abelova grupa z operacijo seštevanja.

- **Lema.** Recimo, da je $|G| = m \cdot n$, kjer sta m, n tuji. Kako lahko zapišemo G kot direktno vsoto?
- **Zgled.** Dokaži: če sta m, n tuji, potem $\mathbb{Z}_m \oplus \mathbb{Z}_n \approx \mathbb{Z}_{mn}$. Ali je $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \approx \mathbb{Z}_4$?
- **Posledica.** Kako lahko zapišemo vsako grupo moči n ?
- **Definicija.** p -grupa.
- **Opomba.** Ali je vsaka končna Abelova grupa direktna vsota p_i -grup?
- **Lema.** Kdaj je p -grupa ciklična?
- **Lema.** Ali lahko vsako p -grupo zapišemo kot vsoto ciklične podgrupe in neke druge podgrupe?
- **Posledica.** Ali vsako p -grupo lahko zapišemo kot direktno vsoto cikličnih grup? Ali vsako grupo lahko zapišemo kot direktno vsoto cikličnih grup?
- **Opomba.** Kako vidimo, ali dva razcepa Abelovih grup na direktni vsoti cikličnih p_i -grup prestavljata isto grupo do izomorfizma natančno?
- **Izrek.** Kdaj sta končni Abelovi p -grupi izomorfni?
- **Povzetek.** Čemu je izomorfna vsaka končna Abelova grupa? **TODO: ***
- **Zgled.** Poišči vse Abelove grupe moči 432.

3. Klasifikacija končno generiranih Abelovih grup

Naj bo G končno generirana Abelova grupa.

- **Izrek.** Čemu je izomorfna grupa G ? Torzijska podgrupa. Kdaj pravimo, da je G brez torzije? **TODO: ***
- **Opomba.** Kaj je potenca n v izomorfizmu iz prejšnjega izreka?
- **Trditev.** Ali lahko vsako končno generirano Abelovo grupo zapišemo kot direktno vsoto končne Abelove grupe in neke druge?
- **Opomba.** Ali iz tega, da je G Abelova in ima vsak element končen red sledi, da je G končna?

7 Delovanja grup

1. Delovanja grup

Naj bo G grupa in X neprazna množica.

- **Definicija.** Kadar pravimo, da G deluje na X ? Delovanje.
- **Opomba.** Ali pri vektorskih prostorih polje deluje na vektorji? Ali iz 1. pogoja sledi 2. pogoj? Levo in desno delovanje. Kako iz levega delovanja pridemo do desnega?
- **Zgled.** Delovanje porodi homomorfizem $G \rightarrow \text{Sym } X$ in obratno.
- **Definicija.** Jedro delovanja. Zvesto delovanje. Kdaj pravimo, da se G vloži v $\text{Sym } X$?
- **Zgled.**
 - Trivialno delovanje.
 - Levo množenje. Cayleyjev izrek. Levo regularno delovanje.
 - Delovanje grupe G na množico G z konjugiranjem.
 - Naj bo $H \leq G$. Delovanje G na G/H s predpisom $g \cdot hH = (gh)H$.
 - Naj G deluje na množice X . Naj bo Y neprazna množica. Delovanje G na množice Y^X s predpisom $g \cdot f = x \mapsto f(g^{-1} \cdot x)$.
 - Naj bo G deluje na X in na Y . Naj bo Y neprazna množica. Delovanje G na množice Y^X s predpisom $g \cdot f = g * f(g^{-1} \cdot x)$
 - Naj bo V vektorski prostor nad \mathbb{F} . Delovanje grupe avtomorfizmov na množico vektorjev.
 - Naj bo K komutativen kolobar. Gledamo $K[x_1, x_2, \dots, x_n]$. Delovanje S_n na $K[x_1, x_2, \dots, x_n]$ s permutacijo spremenljivk.

2. Orbite, stabilizatorje in fiksne točke delovanj

Naj grupa G deluje na množice X .

- **Definicija.** Orbita elementa $x \in X$. Stabilizator elementa $x \in X$. Množica fiksnih točk elementa $g \in G$. Fiksne točke delovanja.
- **Lema.** Čemu je enak $x \in X$, če $g \cdot x = y$?
- **Trditev.** Ali je $G_x \leq G$?
- **Trditev.** Ekvivalenčna relacija na X , ki jo porodi delovanje. Kaj so ekvivalenčni razredi?
- **Posledica.** Kaj lahko povemo o orbitah? Prostor orbit.
- **Definicija.** Tranzitivno delovanje.
- **Zgled.** Določi orbite, stabilizatorji ter fiksne točke delovanj:
 - Naj bo G deluje na G z levim množenjem. Ali je tranzitivno?
 - Naj bo G deluje na G s konjugiranjem. Konjugirani razred elementa $x \in G$.
 - Naj bo $H \leq G$. G deluje na G/H .
 - Naj bo S_n deluje na $K[x_1, \dots, x_n]$ [le fiksne točke]. Simetrični polinomi.