1 Uvod v teorijo grup

1.1 Grupa permutacij

- Zapis s transpoziciji: $(i_1 i_2 \dots i_n) = (i_1 i_n)(i_1 I_{n-1}) \dots (i_1 i_3)(i_1 i_2)$
- Inverz k-cikla: $(i_1 i_2 \dots i_k)^{-1} = (i_k i_{k-1} \dots i_2 i_1)$
- Konjugiranje: $\pi \in S_n \implies \pi(i_1 i_2 \dots i_k)\pi^{-1} = (\pi(i_1)\pi(i_2) \dots \pi(i_k))$
- Generatorji:
  - $S_n = \langle (12), (13), (1n) \rangle = \langle (12)(23) \dots (n-1, n) \rangle = \langle (12), (12 \dots n) \rangle$

1.2 Diedrska grupa D_{2n}

- $z^k r = r^{-k} z = r^{n-k} z$
- $r^k z$ so zrcaljenja, $(r^k z)^2 = 1$

1.3 Podgrupe

- $H, K \leq G \implies |HK| = \frac{|H||K|}{|H \cap K|}$.

1.4 Ciklične grupe

- Vsaka podgrupa ciklične grupe je ciklična
- Podgrupe v $\mathbb{Z}$ so oblike $n\mathbb{Z}, n \in \mathbb{N}$
- Podgrupe v $\mathbb{Z}_n$ so $\mathbb{Z}_d$, kjer $d \mid n$
- $G = \langle a \rangle, |G| < \infty \implies G = \langle a^k \rangle \iff \gcd(k, n) = 1$
- $k \in Z_n \implies \operatorname{red} k = \frac{n}{\gcd(n,k)}$
- Konjugiranje ohranja red elementa

1.5 Generatorji grup

- Oglejmo množico vseh možnih produktov in inverzov ter pokažemo, da je podgrupa.

1.6 Splošno

- $f : X \to X$ preslikava. Velja:
  - f ima levi inverz: $g \circ f = \mathrm{id}$ natanko tedaj, ko je f injektivna. Če f tudi ni surjektivna, potem ima več levih inverzov.
  - f ima desni inverz: $f \circ h = \mathrm{id}$ natanko tedaj, ko je f surjektivna. Če f tudi ni surjektivna, potem ima več desnih inverzov.

2 Uvod v teorijo kolobarjev

- Kolobar K je Boolov, če $\forall x \in K \,.\, x^2 = x$. Boolov kolobar je komutativen in ima karakteristiko 2.
- Kolobar $\mathbb{Z}$ ni algebra nad nobenim poljem.
- Naj bo A končno-razsežna algebra. Tedaj
  - $\forall a \in A \setminus \{0\} \,.\, (\exists b \in A \setminus \{0\} \,.\, ab = 0 \lor ba = 0) \lor (\exists a^{-1} \,.\, a^{-1}a = aa^{-1} = 1)$.
  - $\forall a \in A \,.\, \exists b \in A \,.\, ab = 1 \lor ba = 1 \implies a^{-1} = b$.
  - Če je A obseg, je vsaka podalgebra podobseg.

2.1 Algebra kvaternionov

- $i^2 = j^2 = k^2 = ijk = -1$
- $Z(\mathbb{H}) = \mathbb{R}, \ Z(Q) = \{-1, 1\}$.
- $\forall h \in \mathbb{H} \, . \, \exists \alpha, \beta \in \mathbb{R} \, . \, h^2 + \alpha h + \beta = 0$, kjer $-\alpha = h + \overline{h}$ in $\beta = h\overline{h}$.

2.2 Kolobar Z_n

- Kolobar Z ima 2 obrnljivih elementa: 1 in -1
- V $\mathbb{Z}_n$ element $k \in \mathbb{Z}_n$ je obrnljiv natanko tedaj, ko $\gcd(k, n) = 1$.
- $|\mathbb{Z}_n^*| = \phi(n)$, kjer je ϕ Eulerjeva funkcija. Če he p praštevilo, potem $|\mathbb{Z}_p| = p - 1$.

2.3 Generatorji

- Poglejmo kaj mora vsebovati kolobar (vedno vsebuje enoto), ki je generiran z neko množico A, ter pokažemo, da je dobljena množica podkolobar.

3 homomorfizem

- Matrike so obrnljive? Morda to je $\mathbb{H}$?

4 Splošno

4.1 Matrike

- Naj bo $A \in M_n(\mathbb{R})$, $\operatorname{rang} A = 1$. Tedaj $\exists \lambda \in \mathbb{R} \, . \, A^2 = \lambda A$. Tako matriko lahko zapišemo tudi v obliki: stolpec krat vrstica.
- $E_{ij} \cdot E_{kl} = \delta_{jk} E_{il}$