Ryhmät 15.3.2021

luennot ma 10–12
ti 12–14

Harjoitusvastaanotto
ke 14– n. 15
= 14.15

harjoitukset: kirj. palautus tiistain klo 12 luentoon mennessä
ratkaisuja kotisivulla sen jälkeen.
tehtävät kurssimateriaalissa, numerot kotisivulla.
(12.3 —)

hyvityksiä tenttiin
24 p.

20% → 1 p
40% → 2 p
60% → 3 p
80% → 4 p

Sisältö $(\mathbb{Z},+)$

- Ryhmät $(G,*)$
  assos. laskut.
  $(a*b)*c = a*(b*c)$

homomorfismit, aliryhmät.

- Esimerkkejä: $(\mathbb{Z}/q\mathbb{Z},+)$, lin. algebran ryhmiä
  permutaatioryhmät → symm. ryhmät S_n = bijektiot $\{1,\dots,n\} \circlearrowleft$

- ryhmän ja aliryhmien suhde
  → Lagrangen lause
- tekijäryhmät
- ryhmät ja geometria.

$(G,*)$ ryhmä $\quad g \in G \quad \langle g \rangle = \{ g^k : k \in \mathbb{Z} \}$ on g:n virittämä syklinen aliryhmä.

$$g^k = \underbrace{g * g * \cdots * g}_{k \text{ kpl}} \qquad k \geq 1$$

g:n käänteisalkio

$$g^k = \underbrace{(g^{-1}) * (g^{-1}) * \cdots * (g^{-1})}_{-k \text{ kpl}} \qquad k \leq -1$$

$g^0 =$ G:n neutr. alkio

8. Ryhmät

Määr. Olk. $(G,*)$ laskutoimituksella varustettu joukko. $(G,*)$ on ryhmä, jos

1) $*$ on assosiatiivinen (liitännäinen):

$$(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$$

2) $*$:llä on neutraalialkio (n.a.):

$$\exists\ e \in G \text{ s.e. } \left.\begin{array}{l} e*g = g \\ g*e = g \end{array}\right\} \forall g \in G$$

3) Jokaisella $g \in G$ on käänteisalkio $g^{-1} \in G$: $\quad g * g^{-1} = e = g^{-1} * g$

$*$ on laskutoimitus joukossa $G \neq \emptyset$:

$*$ on kuvaus $*: G \times G \longrightarrow G$

$$G \times G \ni (g_1, g_2) \longmapsto g_1 * g_2 \in G$$

Esim. $+$ on laskutoimitus $\mathbb{Z}$:ssa:

$$k, l \in \mathbb{Z} \quad \leadsto \quad \underset{\mathbb{Z}\times\mathbb{Z}}{\overset{\cap}{(k,l)}} \overset{+}{\longmapsto} k+l$$

$+$:n n.a. on $0 \in \mathbb{Z}$: $\quad 0 + k = k = k + 0 \quad \forall k \in \mathbb{Z}$.

$k + (-k) = k - k = 0 = (-k) + k \quad$ vastaluku on käänteisalkio.

Esim. • $(\mathbb{Z}, +)$ on ryhmä, samoin $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

$(\mathbb{Z}, \cdot)$ ei ole ryhmä: Esim. alkiolla $2 \in \mathbb{Z}$ ei ole käänteisalkiota / lukua

$0 \in \mathbb{Z}$ —— " ——

$0 \cdot k = 0 \neq 1 \quad \forall k \in \mathbb{Z}$.

ei ole $\cdot$:n neutr. alkio

• $\mathbb{Q}^\times = (\mathbb{Q} - \{0\}, \cdot)$, $\mathbb{Q} - \{0\} = \mathbb{Q} \setminus \{0\}$

• assos ok.

$1 \cdot q = q \quad \forall q \in \mathbb{Q} - \{0\}$

$q = \frac{a}{b}$, $a, b \in \mathbb{Z} - \{0\}$ $\qquad \underbrace{\frac{b}{a}}_{\in \mathbb{Q} - \{0\}} \cdot \frac{a}{b} = 1 = \frac{a}{b} \cdot \frac{b}{a}$

$(\mathbb{R} - \{0\}, \cdot) = \mathbb{R}^\times$

$\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ ovat ryhmiä.

• $a, b \in \mathbb{Z}$, $q \in \mathbb{N} - \{0, 1\}$. a ja b ovat <u>kongruentteja</u> mod $q \Leftrightarrow a - b = kq$ jollain $k \in \mathbb{Z}$

$\Leftrightarrow a - b \in q\mathbb{Z} = \{qk : k \in \mathbb{Z}\}$. Merk. $a \equiv b \mod q$.

a:n <u>kongruenssiluokka</u> on $a + q\mathbb{Z} = \{b \in \mathbb{Z} : a \equiv b \mod q\}$

$= \{a + qk : k \in \mathbb{Z}\}$

$$\mathbb{Z}/q\mathbb{Z} = \{a + q\mathbb{Z} : a \in \mathbb{Z}\} \overset{\text{jakoyhtälö}}{=} \{0 + q\mathbb{Z}, 1 + q\mathbb{Z}, \dots, (q-1) + q\mathbb{Z}\}, \quad \underbrace{\#}_{\text{alkioiden lkm}} \mathbb{Z}/q\mathbb{Z} = q$$

(3)

laskutoimitukset $\mathbb{Z}/q\mathbb{Z}$:ssa

$$(a+q\mathbb{Z})+(b+q\mathbb{Z}) = (a+b)+q\mathbb{Z}$$

$$(a+q\mathbb{Z})(b+q\mathbb{Z}) = ab+q\mathbb{Z}.$$

$\underbrace{(\mathbb{Z}/q\mathbb{Z},+)}_{\mathbb{Z}/q\mathbb{Z}}$ on ryhmä: $+$ on assos. (ks. luku 2)

$$(0+q\mathbb{Z})+(a+q\mathbb{Z}) = (\underbrace{0+a}_{a})+q\mathbb{Z} \quad : \quad 0+q\mathbb{Z} \text{ on n.a}$$

$$\shortparallel$$

$$(a+q\mathbb{Z})+(0+q\mathbb{Z})$$

$$(a+q\mathbb{Z})+(-a+q\mathbb{Z}) = (a-a)+q\mathbb{Z} = 0+q\mathbb{Z}$$

$$\shortparallel$$

$$(-a+q\mathbb{Z})+(a+q\mathbb{Z})$$

$(a+q\mathbb{Z})$:n käänteisalkio
vasta-alkio.

Merkintöjä: • Usein käytetään laskutoimitukselle merkkiä $+$. additiivinen ryhmä

kommutatiiviselle n.a. $0 = 0_G$

Joukon A laskutoimitus $*$ on **kommutatiivinen**, jos $a*b = b*a \ \forall a,b \in A$

vaihdannainen

multiplikatiivinen ryhmä

• Usein laskutoimitus kirj. kuten **kertolasku** (ilman laskut. merkkiä).

Esim. matriisien kertolasku $A, B \in M_n(\mathbb{R}) = \{ n \times n$ $\mathbb{R}$-kertoimiset matriisit $\}$, $\cdot$

matr. kertolasku

$AB \in M_n(\mathbb{R})$ n.a merkintöjä $e \in G$, $e' \in G'$

1