Esimerkkejä ryhmistä 2

Esimerkki. (VEKTORIRYHMÄT) Vektoriavaruuden $(V,+,\cdot)$ vektorit muodostavat additiivisen Abelin ryhmän. Tämän ryhmän neutraalialkio on nollavektori θ ja vektorin X käänteisalkio on vastavektori $-X$. Tällaisen ryhmän muodostaa esimerkiksi $\mathbb{R}^n = \{(a_1,\ldots,a_n) \mid a_i \in \mathbb{R},\ 1 \leq i \leq n\}$.

Esimerkki. (MATRIISIRYHMÄT) Reaalilukualkioisten $(m \times n)$-matriisien joukko $\mathcal{M}_{m\times n}(\mathbb{R})$ muodostaa additiivisen Abelin ryhmän matriisien yhteenlaskun suhteen. Ryhmän neutraalialkiona on nollamatriisi ja matriisin A käänteisalkiona on $-A$. (Tämä ryhmä kuuluu itse asiassa jo edellisen esimerkin piiriin.)

Säännöllisten $(n \times n)$-matriisien joukko

$$GL_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) \neq 0\}$$

muodostaa multiplikatiivisen ryhmän matriisitulon suhteen. Ryhmän neutraalialkio on identiteettimatriisi I_n ja matriisin A käänteisalkio on käänteismatriisi A^{-1}. Kun $n > 1$, ryhmä $(GL_n(\mathbb{R}),\cdot)$ on esimerkki ryhmästä, joka ei ole Abelin ryhmä.

Esimerkki. (JÄÄNNÖSLUOKKARYHMÄT) Jäännösluokat modulo m muodostavat Abelin ryhmän $(\mathbb{Z}_m,+)$, kun yhteenlasku määritellään seuraavasti $\overline{a}+\overline{b} = \overline{a+b}$. Ryhmän neutraalialkio on jäännösluokka $\overline{0}$ ja jäännösluokan $\overline{a}$ käänteisalkio on jäännösluokka $\overline{-a}$. Ryhmä $(\mathbb{Z}_m,+)$ on esimerkki äärellisestä ryhmästä, sillä $\sharp\mathbb{Z}_m = m$.

Jäännösluokkaa $\overline{a}$ modulo m sanotaan *alkuluokaksi*, jos $\mathrm{syt}(a,m) = 1$. Tämä käsite on hyvin määritelty, sillä

$$\text{jos } \mathrm{syt}(a,m) = 1 \text{ ja } \overline{a} = \overline{a'},\ \text{niin } \mathrm{syt}(a',m) = 1.$$

Todistetaan tämä. Koska $\overline{a} = \overline{a'}$, niin $a = a' + mk$ jollekin kokonaisluvulle k. Koska $\mathrm{syt}(a,m) = 1$, on olemassa sellaiset luvut u ja v, että $1 = ua + vm$. Yhdistämällä nämä saadaan $1 = ua + vm = u(a' + mk) + vm = ua' + (uk + v)m$. Koska luku 1 voidaan esittää lukujen a' ja m monikertojen summana, on $\mathrm{syt}(a',m) = 1$.

Kaikkien alkuluokkien modulo m joukko

$$\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m \mid \mathrm{syt}(a,m) = 1\}$$

muodostaa ryhmän jäännösluokkien kertolaskun $\overline{a}\cdot\overline{b} = \overline{a\cdot b}$ suhteen. Ryhmän neutraalialkio on jäännösluokka $\overline{1}$. Alkuluokan $\overline{a}$ käänteisalkio on se jäännösluokka, joka toteuttaa kongruenssin

$$ax \equiv 1 \pmod{m},$$

silloinhan $\overline{a}\cdot\overline{x} = \overline{a\cdot x} = \overline{1}$. Kuten Diofantoksen yhtälöiden kohdalla todetaan, tällä kongruenssilla on yksikäsitteinen ratkaisu x välillä $0 \leq x \leq m-1$.

Esimerkiksi $\mathbb{Z}_9^* = \{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}\}$.

Linkit:
Ryhmä
Vektoriavaruus
Matriisi
Yksinkertaisia matriiseja
Säännöllinen matriisi
Jäännösluokka
Suurin yhteinen tekijä
Diofantoksen yhtälö