Sykliset ryhmät

Määritelmä. Ryhmää $(G,*)$ sanotaan *sykliseksi*, jos G on yhden alkion generoima, eli jos on olemassa sellainen $a \in G$, että $< a >= G$.

Lause. Olkoon $(G,*)$ syklinen ryhmä, siis on olemassa sellainen $a \in G$, että $G =< a >$. Olkoon e ryhmän neutraalialkio.

Jos $(G,*)$ on äärellinen ryhmä, niin

$$G = \{e, a, a^2, \ldots, a^{n-1}\},$$

missä positiivinen luku n on pienin sellainen eksponentti, että $a^n = e$.

Jos $(G,*)$ on ääretön ryhmä, niin

$$G = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$$

ja kaikki potenssit a^m $(m \in \mathbb{Z})$ ovat erisuuria, erityisesti $a^m \neq e$ kaikilla kokonaisluvuilla $m \neq 0$.

Todistus. Ryhmän generointi -sivun lauseen perusteella on $G = \{a^m \mid m \in \mathbb{Z}\}$.

Oletetaan ensin, että $(G,*)$ on äärellinen. Silloin kaikki potenssit $a^0, a, a^2, a^3, a^4, \ldots$ eivät voi olla erisuuria, vaan on olemassa sellaiset luvut l ja k, että $a^l = a^k$ ja $l > k$. Koska $a^k * (a^{l-k}) = a^l = a^k = a^k * e$ niin ryhmän yhtälön supistussäännön nojalla $a^{l-k} = e$. Koska $l - k > 0$, on olemassa sellaisia positiivisia kokonaislukuja j, joilla $a^j = e$. Olkoon n pienin näistä.

Jakoalgoritmin mukaan jokainen eksponentti $m \in \mathbb{Z}$ voidaan kirjoittaa muodossa $m = qn + r$, missä $0 \leq r \leq n-1$. Nyt

$$a^m = a^{qn+r} = (a^n)^q * a^r = e^q * a^r = a^r.$$

Siis kaikki joukon G alkiot ovat muotoa a^r, missä $0 \leq r \leq n-1$, siis $G = \{a^0, a, \ldots, a^{n-1}\}$. Kaikki tämän joukon alkiot ovat erisuuria, sillä toistamalla aikaisempi päättely joukon G alkioille löydettäisiin jokin luku t, jolle $a^t = e$ ja $0 \leq t \leq n-1$. Tämä on kuitenkin ristiriidassa luvun n minimaalisuuden kanssa. Siis joukko G on väitettyä muotoa.

Jos G on ääretön ovat kaikki potenssit a^m, missä $m \in \mathbb{Z}$, erisuuria, sillä muuten päädyttäisiin äärelliseen ryhmään kuten edellä. □

Ryhmän kertaluku on määritelmän mukaan ryhmän alkioiden lukumäärä. Määritellään seuraavassa ryhmän alkion kertaluku.

Määritelmä. Olkoon $(G,*)$ ryhmä ja $a \in G$. Alkion a generoiman aliryhmän $(< a >, *)$ kertalukua sanotaan *alkion a kertaluvuksi*. Alkion a kertaluvusta käytetään merkintää $\text{ord}(a)$, siis

$$\text{ord}(a) = \sharp < a > .$$

Edellisestä lauseesta seuraa, että alkio a on (äärellistä) kertalukua n jos ja vain jos n on pienin sellainen eksponentti, jolla $a^n = e$. Tällöin lisäksi alkion a potenssit $a^0 = e, a, a^2, \ldots, a^{n-1}$ ovat kaikki erisuuria. Huomaa, että $\text{ord}(a) = 1$ jos ja vain jos $a = e$.

Linkit:
Huomioita ryhmästä

Jakoalgoritmi

Ryhmän generointi

Ryhmän perusominaisuuksia