

Algebra I

20.3.2014

Helsingin yliopisto
Matematiikan ja tilastotieteen laitos
Johanna Rämö

Sivuluokkien ominaisuuksia

Lause

Olkoon G ryhmä, jolla on aliryhmä H , ja olkoot $a, b \in G$. Seuraavat ehdot ovat yhtäpitävät:

1. $a^{-1}b \in H$
2. $a \in bH$
3. $b \in aH$
4. $aH = bH$.

Lagrangen lause

Lause

Olkoon G äärellinen ryhmä, jolla on aliryhmä H . Aliryhmän H kertaluku jakaa ryhmän G kertaluvun, ja

$$[G : H] = \frac{|G|}{|H|}.$$

Lause

Jäännösluokkien joukossa \mathbb{Z}_n voidaan määritellä yhteenlasku kaavalla

$$[a]_n + [b]_n = [a + b]_n.$$

Todistus:

Oletetaan, että $[a]_n = [a']_n$ ja $[b]_n = [b']_n$.

Nyt $a \equiv a' \pmod{n}$ ja $b \equiv b' \pmod{n}$, joten lauseen 7.18 nojalla

$a + b \equiv a' + b' \pmod{n}$.

Näin ollen $[a + b]_n = [a' + b']_n$.

Lause 7.18

Lause

Olkoot $a, b, c, d \in \mathbb{Z}$, ja olkoon n positiivinen kokonaisluku. Tällöin seuraavat väitteet pätevät:

a) Jos $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$, niin

$$a + c \equiv b + d \pmod{n} \quad \text{ja} \quad ac \equiv bd \pmod{n}.$$

b) Jos $ca \equiv cb \pmod{n}$ ja $\text{sy}(c, n) = 1$, niin $a \equiv b \pmod{n}$.

c) Jos $a \equiv b \pmod{kn}$ jollakin $k \in \mathbb{Z}$, niin $a \equiv b \pmod{n}$.

Epäselittämistä

Todistuksessa: Oletetaan, että $[a]_n = [a']_n$.

Selityksessä: Oletetaan, että sivuluokat $[a]_n$ ja $[a']_n$ ovat samoja.

Kyseessä ei ole selitys, vaan saman asian sanominen toisin sanankääntein. Se ei tuota lisää tietoa, eikä linkitä asioita toisiinsa.

Epäselittämistä

Todistuksessa: Oletetaan, että $[a]_n = [a']_n$.

Selityksessä: OK, ymmärrän, että todistuksessa oletetaan $[a]_n = [a']_n$.

Kyseessä ei ole selitys, vaan oman ymmärryksen raportointi. Se ei tuota lisää tietoa, eikä linkitä asioita toisiinsa.