Algebra I

Luento 21.2.2012

Helsingin yliopisto

Luennon aiheet

- Mitä sykliset ryhmät ja aliryhmät olivatkaan?
- Jäännösluokkien yhteenlasku
- Useamman alkion virittämät aliryhmät

Jäännösluokka

- Kokonaisluvun a jäännösluokka modulo n on joukko

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

- Lukua a kutsutaan jäännösluokan $[a]_n$ edustajaksi.

Jäännösluokilla laskeminen

Halutaan määritellä jäännösluokille yhteenlasku

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

Silloin jäännösluokkien joukko $\mathbb{Z}_n$ käyttäytyy kuten kellotauluryhmä K_n.

Ongelma

Esimerkiksi $[4]_6 = [-8]_6$. Nyt voidaan laskea summa $[4]_6 + [3]_6$ kahdella eri tavalla.

1. $[4]_6 + [3]_6 = [7]_6 = [1]_6$

2. $[4]_6 + [3]_6 = [-8]_6 + [3]_6 = [-5]_6$

Tuleeko tästä ongelmia?

Tulos

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

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

Kongruenssin laskusääntöjä

Olkoot $a, b, c, d \in \mathbb{Z}$. Jos $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$ niin

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

Jäännösluokkaryhmä

Jäännösluokkien joukko $\mathbb{Z}_n$ on ryhmä, kun laskutoimituksena on yhteenlasku.

Sykliset ryhmät ovat isomorfisia

Jos syklinen ryhmä on ääretön, se on isomorfinen ryhmän $\mathbb{Z}$ kanssa.

Sykliset ryhmät ovat isomorfisia

Jos syklisessä ryhmässä on n alkiota, se on isomorfinen ryhmän $\mathbb{Z}_n$ kanssa.

Syklisen ryhmän aliryhmät

Syklisen ryhmän kaikki aliryhmät ovat syklisiä.

Useamman alkion virittämät aliryhmät

Olkoon G ryhmä ja $S \subset G$.

Joukon S virittämä aliryhmäon pienin ryhmän G aliryhmä, joka sisältää joukon S.

Tätä aliryhmää merkitään $\langle S \rangle$.

Esimerkki

Määritetään ryhmän S_4 aliryhmä $\langle (13), (24) \rangle$

Mitä kaikkea aliryhmässä pitää olla?

$$(13)^2 = (1)$$
$$(24)^2 = (1)$$
$$(13) \cdot (24) = (13)(24)$$
$$(24) \cdot (13) = (24)(13) = (13)(24)$$
$$(13)^{-1} = (13)$$
$$(24)^{-1} = (24).$$