Algebra I

Luento 15.2.2012

Helsingin yliopisto

- Tällä luennolla viimeistellään yhden alkion virittämät aliryhmät.

- Sen jälkeen käsitellään lukuteoriaa ja jäännösluokkia.

- Luentotauolla pidetään kuutiokisa.

Kertaluku

Alkion g kertaluku $o(g)$ on sen virittämän aliryhmän $\langle\, g \,\rangle$ kertaluku.

Tulos

Alkion g kertaluku on pienin positiivinen kokonaisluku n, jolla pätee $g^n = e$.

Jos tällaista lukua ei löydy, kertaluku on ääretön.

Loppuyhteenveto

- Jos $g^n = e$ jollakin $n \in \mathbb{N}$, niin $\langle\, g \,\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.

- Jos edellä mainittua lukua ei löydy, niin $\langle\, g \,\rangle$ on ääretön.

Sykliset aliryhmät

- Aliryhmä on syklinen, jos se on yhden alkion virittämä.

- Myös ryhmä itse on aliryhmä. Ryhmää kutsutaan sykliseksi, jos se on yhden alkion virittämä.

Useamman alkion virittämät aliryhmät

Olkoon G ryhmä ja olkoon $S \subset G$.

Joukon S virittämä aliryhmä $\langle S \rangle$ on pienin ryhmän aliryhmä, joka sisältää joukon S.

LUKUTEORIAA

Jaollisuus

Kokonaisluku n on jaollinen kokonaisluvulla m, jos jollain kokonaisluvulla a pätee $n = am$.

Tällöin merkitään $m|n$.

Jakoyhtälö

Jos jako ei mene tasan, siitä jää jakojäännös.

Jakoyhtälö

Olkoot a ja b kokonaislukuja. Oletetaan, että $b \neq 0$. Tällöin on olemassa yksikäsitteiset $q, r \in \mathbb{Z}$, joille pätee

$$a = qb + r \quad \text{ja} \quad 0 \leq r < |b|.$$

Lemman 6.7 todistus

Lemma Olkoon G ryhmä ja g jokin sen alkio. Oletetaan, että positiiviselle kokonaisluvulle n pätee $g^n = e$.

Tällöin

$$\langle\, g \,\rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Jakojäännösten vertailua

Joskus haluamme luokitella kokonaislukuja niiden jakojäännösten perusteella.

Kellonajat ovat tästä esimerkki.

Jakojäännösten vertailua helpottava tulos

Luvuilla a ja b on sama jakojäännös luvulla n jaettaessa, jos ja vain jos $n \mid (a - b)$.

Kongruenssin määritelmä

Jos $n \mid (a - b)$, niin a ja b ovat kongruentit modulo n.

Tällöin merkitään $a \equiv b \pmod{n}$.

Kongruenssin eri tulkintoja

- $a \equiv b \pmod{n}$ jos ja vain jos $n \mid (a - b)$
- $a \equiv b \pmod{n}$ jos ja vain jos jakojäännös on sama luvulla n jaettaessa
- $a \equiv b \pmod{n}$ jos ja vain jos $a = b + kn$ jollain $k \in \mathbb{Z}$

Jäännösluokka

- Luvun 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.

Jäännösluokka

Jäännösluokka voidaan kirjoittaa myös muodossa

$$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}.$$

Jäännösluokkien joukko

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

Jäännösluokkien yhteenlasku

Halutaan määritellä joukossa $\mathbb{Z}_n$ yhteenlasku ehdolla

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

Tulos

Oletetaan, että $a, a', b, b' \in \mathbb{Z}$.

Jos $[a]_n = [a']_n$ ja $[b]_n = [b']_n$, niin

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

Jäännösluokkaryhmä

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

Jäännösluokkaryhmät ovat isomorfisia kellotauluryhmien kanssa.

MATEMATIIKAN KIRJOITTAMISESTA

- Implikaatio- ja ekvivalenssinuoliin liittyvät ongelmat

Esimerkki

Osoitetaan, että kuvaus $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n+1$ on injektio.

Oletetaan, että $m, n \in \mathbb{Z}$. Tällöin pätee

$$m + 1 = n + 1 \;\Rightarrow\; m = n \;\Rightarrow\; \text{Kuvaus on injektio}$$

Mikä tässä on vialla?

Esimerkki

Osoitetaan, että kuvaus $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n+1$ on injektio.

Oletetaan, että $m, n \in \mathbb{Z}$ ja että $f(m) = f(n)$. Tällöin pätee

$$m + 1 = n + 1 \iff m = n.$$

Siis f on injektio.

Mikä tässä on vialla?

Lopputulos

- Käytä implikaatio- ja ekvivalenssinuolia harkiten.
- Tällä kurssilla ne sopivat lähinnä yhtälönratkaisuun.
- Muulloin suomen kielen sanat toimivat paremmin!