Algebra I

Luento 18.4.2012

Helsingin yliopisto

Luennon aiheet

- Ydin
- Ryhmien homomorfialause
- Polynomien jaollisuus

Määritelmä

Olkoot G ja H ryhmiä. Kuvaus $f\colon G \to H$ on ryhmähomomorfismi, jos kaikilla $x, y \in G$ pätee

$$f(xy) = f(x)f(y).$$

Ydin ja kuva

Olkoon $f\colon G \to H$ ryhmähomomorfismi.

Sen ydin on joukko

$$\operatorname{Ker} f = \{g \in G \mid f(g) = e_H\}$$

ja kuva on joukko

$$\operatorname{Im} f = \{f(g) \mid g \in G\}.$$

Esimerkkejä ytimistä

Homomorfismin $\pi\colon \mathbb{Z} \to \mathbb{Z}_5$, $\pi(a) = [a]_5$ ydin on $5\mathbb{Z}$.

Homomorfismin $f_e\colon G \to H$, $f_e(x) = e_H$ ydin on G.

Homomorfismin $\mathrm{id}_G\colon G \to G$, $\mathrm{id}(x) = x$ ydin on $\{e_G\}$.

Esimerkkejä ytimistä

Määritetään kuvauksen $f\colon 4\mathbb{Z} \to \mathbb{Z}_5$, $f(4n) = [n]_5$ ydin.

Lause

Olkoon $f\colon G \to H$ ryhmähomomorfismi.

Kuvaus f on injektiivinen, jos ja vain jos $\operatorname{Ker} f = \{e_G\}$.

Ydin ja kuva

Olkoon $f\colon G \to H$ ryhmähomomorfismi.

- Kuvaus f on injektio, jos ja vain jos $\operatorname{Ker} f = \{e_G\}$.
- Kuvaus f on surjektio, jos ja vain jos $\operatorname{Im} f = H$.

Lemma

Olkoon $f\colon G \to H$ ryhmähomomorfismi.

Ydin $\operatorname{Ker} f$ on ryhmän G normaali aliryhmä.

Normaalisuuskriteeri

Olkoon G ryhmä ja N sen aliryhmä.

Aliryhmä N on normaali, jos ja vain jos

$$gng^{-1} \in N \quad \text{kaikilla } n \in N \text{ ja } g \in G.$$

KUINKA HOMOMORFISMEISTA SAADAAN ISOMORFISMEJA?

Tutkitaan eilen määriteltyä kuvausta

$$f\colon \mathbb{Z}_6 \to S_3, \quad f([k]_6) = (123)^k.$$

Kuinka siitä saadaan bijektio?

Kuinka homomorfismeista saadaan isomorfismeja?

Homomorfismista täytyy saada bijektio.

- Surjektiivisuus saadaan kuvajoukkoa pienentämällä.
- Injektiivisyys saadaan, kun siirrytään tarkastelemaan tekijäryhmää $\mathbb{Z}_6/\operatorname{Ker} f$.
- Oleellista on, että samassa sivuluokassa olevilla alkioilla on sama kuva.

Ryhmien homomorfialause

Olkoot G ja H ryhmiä, ja olkoon $f\colon G \to H$ ryhmähomomorfismi. Tällöin

$$G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Isomorfismina toimii kuvaus

$$\bar{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f, \quad a\operatorname{Ker} f \mapsto f(a).$$

Esimerkki

Millainen isomorfismi saadaan tseisarvokuvauksesta

$$f\colon (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot), \quad f(x) = |x|?$$

POLYNOMIEN JAOLLISUUS

Olkoon K kunta, ja olkoot $P, Q \in K[X]$.

Polynomi P on jaollinen polynomilla Q, jos on olemassa sellainen polynomi $R \in K[X]$, että $P = RQ$.

Tällöin merkitään $Q \mid P$.

Jaoton polynomi

Olkoon K kunta. Polynomi $P \in K[X]$ on jaoton, jos se ei ole vakiopolynomi eikä kahden positiivista astetta olevan polynomin tulo.

Jakoyhtälö

Olkoon K kunta, ja olkoot $P, S \in K[X]$. Oletetaan, että $S \neq 0$.

Tällöin on olemassa yksikäsitteiset $Q, R \in K[X]$, joille pätee

$$P = QS + R$$

ja joko $R = 0$ tai $\deg(R) < \deg(S)$.

Juuri

Olkoon R vaihdannainen rengas ja olkoon $P \in R[X]$.

Alkio $c \in R$ on polynomin P juuri, jos $P(c) = 0_R$.

Esimerkki

Renkaan $\mathbb{Z}_4$ polynomilla $P = X^5 + 2X^3 + 3$ on juuri $[3]_4$.

Kaikki polynomin juuret voidaan löytää käymällä läpi loputkin renkaan $\mathbb{Z}_4$ alkiot:

$$P([0]_4) = [0]_4^5 + 2 \cdot [0]_4^3 + [3]_4 = [3]_4$$
$$P([1]_4) = [1]_4^5 + 2 \cdot [1]_4^3 + [3]_4 = [1]_4 + [2]_4 + [3]_4 = [2]_4$$
$$P([2]_4) = [2]_4^5 + 2 \cdot [2]_4^3 + [3]_4 = [32]_4 + [16]_4 + [3]_4 = [3]_4$$

Nähdään, että muita juuria ei ole.

Juuret ja jaollisuus

Olkoon K kunta.

Polynomilla $P \in K[X]$ on juuri $c \in K$, jos ja vain jos P on jaollinen polynomilla $X - c$.

Esimerkki

Renkaan $\mathbb{Z}_4$ polynomilla $P = X^5 + 2X^3 + 3$ on juuri $[3]_4$. Siis $X - 3$ jakaa polynomin P.

Siten P ei ole jaoton.

Päättely ei toimi toiseen suuntaan.

Jos polynomilla ei ole juuria, siitä ei voi välttämättä päätellä, että polynomi on jaoton.

Lause

Olkoon K kunta ja $P \in K[X]$ nollasta poikkeava polynomi.

Polynomin P juurten lukumäärä on korkeintaan deg(P).