Algebra
Syksy 2009
Kertausta 1. välikokeeseen, ratkaisut.

1. Osoita, että jos $a \equiv b (\mathrm{mod}\, 2n)$, niin $a^2 \equiv b^2 (\mathrm{mod}\, 4n)$.

   Todistus. $a \equiv b (\mathrm{mod}\, 2n) \Leftrightarrow a - b = 2kn$ jollekin $k \in \mathbb{Z}$. Tällöin

   $$\begin{aligned} a &= b + 2kn \\ \Rightarrow a^2 &= b^2 + 4knb + 4k^2n^2 \\ &= b^2 + 4n(kb + k^2n). \end{aligned}$$

   Joten $a^2 - b^2 = 4nq$ jollekin $q \in \mathbb{Z}$, eli $a^2 \equiv b^2 (\mathrm{mod}\, 4n)$. □

2. Osoita, että jos p on alkuluku ja $p \mid a^n$, niin $p^n \mid a^n$. *Todistus.* Oletuksen mukaan $p \mid aaaa \cdots a$, joten $p \mid a$, koska p on alkuluku. Siis $a = kp$ jollakin $k \in \mathbb{Z}$. Eli $a^n = k^n p^n \Rightarrow p^n \mid a^n$ □

3. Ratkaise lineaariset kongruenssit (ilmoita vastaukset pienimmän ei-negatiivisen jäännöksen avulla)

   a) $3x \equiv 6 (\mathrm{mod}\, 8)$,

   b) $128x \equiv 833 (\mathrm{mod}\, 1001)$,

   c) $58x \equiv 2 (\mathrm{mod}\, 32)$.

   Ratkaisu. a) Helposti nähdään, että ratkaisu on $x \equiv 2 (\mathrm{mod}\, 8)$.
   b) Eukleideen algoritmilla saadaan $\mathrm{syt}(128, 1001) = 1$, josta lineaarikombinaatioksi saadaan $1 = (-39)1001 + 305 \cdot 128$, josta $833 = 128(833 \cdot 305) - (39 \cdot 833)1001$, eli $x \equiv 833 \cdot 305 \equiv 254065 (\mathrm{mod}\, 1001)$. Koska $254065 = 253 \cdot 1001 + 812$, niin $x \equiv 812 (\mathrm{mod}\, 1001)$.
   c) Koska $\mathrm{syt}(58, 32) = 2$ ja $2 \mid 2$, niin yhtälöllä on ratkaisuja. Kirjoitetaan yhtälö muodossa $58x - 2 = 32k, k \in \mathbb{Z}$ ja jaetaan kahdella. Saadaan $29x - 1 = 16k \Leftrightarrow 29x \equiv 1 (\mathrm{mod}\, 16)$. Nyt $\mathrm{syt}(29, 16) = 1$, joten ratkaisu on muotoa $[x_0]_{16}$, missä x_0 on eräs ratkaisu. Etsitään x_0 Eukleideen algoritmin avulla ja saadaan $x_0 = 5$. Vastaus on siis kongruenssiluokka $[5]_{16}$.

4. Muodostaako pari $(\mathbf{R} \setminus \{0\}, *)$ ryhmän, jos

   $$a * b = |a|\, b,$$

   missä $|a|$ on luvun a itseisarvo?

   Ratkaisu. Ei, sillä laskutoimituksella $*$ ei ole yksikäsitteistä neutraalialkiota joukossa $\mathbf{R} \setminus \{0\}$.

5. Osoita, että yhden alkion sisältävä joukko voi muodostaa laskutoimituksen kanssa ryhmän.

   Todistus. Olkoon e neutraalialkio. Näytetään, että pari $(\{e\}, \circ)$ on ryhmä.
   Neutraalialkion määritelmän mukaan $e \circ e = e$, joten $\circ$ on laskutoimitus joukossa $\{e\}$.
   Laskutoimitus $\circ$ on selvästi liitännäinen; $e \circ (e \circ e) = e = (e \circ e) \circ e$.
   Neutraalialkio $e \in \{e\}$.
   Koska $e^{-1} = e$, niin käänteisalkio kuuluu joukkoon $\{e\}$. Siis $(\{e\}, \circ)$ on ryhmä.

   □

6. Olkoot $(G_1, \circ)$ ja $(G_2, *)$ ryhmiä ja $e_2 \in G_2$ neutraalialkio. Osoita, että kuvaus $f : G_1 \to G_2$, $f(x) = e_2$ on homomorfismi.

   Todistus. Olkoot $a, b \in G_1$. Nyt

   $$f(a \circ b) = e_2 = e_2 * e_2 = f(a) * f(b),$$

   joten f on homomorfismi. □

7. Osoita, että kuvaus $f : \mathbb{R} \to \mathbb{R}$, $f(x) = e^x$, on homomorfismi ryhmältä $(\mathbb{R}, +)$ ryhmälle $(\mathbb{R} \setminus \{0\}, \cdot)$.

   Todistus. Olkoot $x, y \in \mathbb{R}$. Nyt

   $$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y),$$

   joten f on homomorfismi. □

8. Näytä, että kuvaus $g : \mathbb{Z}_{18} \to \mathbb{Z}_3$, $g([x]_{18}) = [2x]_3$, on homomorfismi ja etsi ko. kuvauksen ydin.

   Ratkaisu. Homomorfisuus: Olkoot $x, y \in \mathbb{Z}_{18}$.

   $g([x+y]_{18}) = [2(x+y)]_3 = [2x+2y]_3 = [2x]_3 + [2y]_3 = g([x]_{18}) + g([y]_{18})$.

   Ydin: $\mathrm{Ker} f = \{0, 3, 6, 9, 12, 15\}$.

9. Tutki, onko kuvaus $f : \mathbb{R}_+ \to \mathbb{R}_+$ isomorfismi ryhmältä $(\mathbb{R}_+, \cdot)$ itselleen, kun

   a) $f(x) = 3x$,

   b) $f(x) = \sqrt{x}$.

Ratkaisu. a) Sääntö f, $f(x) := 3x$, on todella funktio $\mathbb{R}_+ \to \mathbb{R}_+$.

Edelleen $f(ab) = 3ab$ ja $f(a)f(b) = 3a3b = 9ab$. Esimerkiksi, kun $a = 1$ ja $b = 1$, on $f(ab) \neq f(a)f(b)$. Siis funktio ei ole homomorfismi, eikä täten isomorfismikaan.

b) Samoin f, $f(x) := \sqrt{x}$, on funktio $\mathbb{R}_+ \to \mathbb{R}_+$. Tunnetusti se on bijektio. Se on myös homomorfismi, sillä positiiviluvuilla on

$$f(ab) = \sqrt{ab} = \sqrt{a}\sqrt{b} = f(a)f(b).$$

Kyseessä on siis isomorfismi joukolta itselleen.