Algebra I, erilliskoe to 11.6.2009, ratkaisut (Jouni Luukkainen), 2 sivua, myös kevään 2009 kurssin kotisivulla

1. Määritellään kuvaus $f\colon \mathbb{N} \to \mathbb{N}$ asettamalla $f(0) = 1$ sekä kullakin $n \in \mathbb{N}$ rekursiivisesti

$$f(n+1) = \begin{cases} f(n)/2, & \text{jos } f(n) \text{ on parillinen;} \\ 5f(n)+1, & \text{jos } f(n) \text{ on pariton.} \end{cases}$$

Osoita, että $f(n+7) = f(n)$ kaikilla $n \in \mathbb{N}$, ja määritä f:n kuvajoukko $f(\mathbb{N})$.

Ratk. Lasketaan aluksi $f(n)$ kaikilla $n \leq 7$: $f(0) = 1$, $f(1) = 5 \cdot 1 + 1 = 6$, $f(2) = 6/2 = 3$, $f(3) = 5 \cdot 3 + 1 = 16$, $f(4) = 16/2 = 8$, $f(5) = 8/2 = 4$, $f(6) = 4/2 = 2$ ja $f(7) = 2/2 = 1$. Siis $f(7) = f(0)$.

Olkoon nyt $n \in \mathbb{N}$ mielivaltainen luku, jolla $f(n+7) = f(n)$. Tällöin, jos $f(n)$ on parillinen, niin $f((n+1)+7) = f((n+7)+1) = f(n+7)/2 = f(n)/2 = f(n+1)$, ja jos $f(n)$ on pariton, niin $f((n+1)+7) = f((n+7)+1) = 5 \cdot f(n+7) + 1 = 5 \cdot f(n) + 1 = f(n+1)$; siis molemmissa tapauksissa on $f((n+1)+7) = f(n+1)$.

Näin on induktiolla osoitettu, että $f(n+7) = f(n)$ kaikilla $n \in \mathbb{N}$.

Saadaan, että $f(\mathbb{N}) = \{f(n) \mid n \in \mathbb{N}, n \leq 6\} = \underline{\{1, 2, 3, 4, 6, 8, 16\}}$.

Arvostelusta. Koska f oli määritelty rekursiolla, tarvittiin induktiotodistus. Induktio-oletuksen oli koskettava lukua n selvällä tavalla ("olkoon $n \in \mathbb{N}$ sellainen, jolla $f(n+7) = f(n)$" tai "olkoon $f(n+7) = f(n)$ jollain **tietyllä** $n \in \mathbb{N}$").

2. Käyttämällä Eukleideen algoritmia **a)** osoita, että luvut 725 ja 147 ovat keskenään jaottomat, ja **b)** etsi kokonaisluvut x ja y, joilla $725x + 147y = 1$.

Ratk. Nyt $725 = 4 \cdot 147 + 137$, $147 = 137 + 10$, $137 = 13 \cdot 10 + 7$, $10 = 7 + 3$, $7 = 2 \cdot 3 + 1$ ja $3 = 3 \cdot 1$; siis $\text{syt}(725, 147) = 1$ eli luvut 725 ja 147 ovat keskenään jaottomat.

Näiden yhtälöiden avulla saadaan $\underline{1} = 7 - 2 \cdot 3 = 7 - 2(10 - 7) = -2 \cdot 10 + 3 \cdot 7 = -2 \cdot 10 + 3(137 - 13 \cdot 10) = 3 \cdot 137 - 41 \cdot 10 = 3 \cdot 137 - 41(147 - 137) = -41 \cdot 147 + 44 \cdot 137 = -41 \cdot 147 + 44(725 - 4 \cdot 147) = \underline{44 \cdot 725 - 217 \cdot 147}$.

Arvostelusta. Yksi ratkaisu (x, y) riitti. Eukleideen algoritmia oli myös nimenomaan käytettävä; oikea todistus a)-kohdassa ja oikea ratkaisu b)-kohdassa eivät yksin riittäneet.

3. Olkoon G multiplikatiivinen ryhmä. Määritä ne parit $(a, b) \in G \times G$, joilla kuvaus $f\colon G \to G$, jolla $f(x) = axb$ kaikilla $x \in G$, on ryhmähomomorfismi.

Ratk. Kuvaus f on ryhmähomomorfismi jos ja vain jos $f(xy) = f(x)f(y)$ kaikilla $x, y \in R$. Nyt, jos $x, y \in G$, niin ryhmän G supistussääntöjen nojalla on $f(xy) = f(x)f(y) \iff axyb = axbayb \iff 1 = ba \iff b = a^{-1}$. Siis f on ryhmähomomorfismi jos ja vain jos $\underline{b = a^{-1}}$.

Arvostelusta. Piti olla tarkka: "jos ja vain jos".

4. Olkoon R rengas. Määritä ne parit $(a, b) \in R \times R$, joilla kuvaus $f\colon R \to R$, jolla $f(x) = axb$ kaikilla $x \in R$, on rengashomomorfismi. **Vihje ja varoitus.** Tulos on samantapainen kuin ryhmille tehtävässä 3, mutta todistus on juonikkaampi.

Ratk. Kuvaus f on rengashomomorfismi jos ja vain jos (i) $f(x+y) = f(x) + f(y)$ kaikilla $x, y \in R$, (ii) $f(xy) = f(x)f(y)$ kaikilla $x, y \in R$ ja (iii) $f(1) = 1$. Ehto (i) pätee aina, sillä jos $x, y \in R$, niin $f(x+y) = a(x+y)b = (ax+ay)b = axb + ayb = f(x) + f(y)$. Koska (ii) $\iff axyb = axbayb$ kaikilla $x, y \in R$, niin (ii) pätee, jos $ba = 1$. Toisaalta (iii) $\iff a1b = 1 \iff ab = 1$. Kääntäen, jos (ii) pätee, niin $f(ba) = f(b)f(a)$ eli $abab = abbaab$, josta ehdon $ab = 1$ pätiessä seuraa, että $1 = ba$. Näin ollen f on rengashomomorfismi jos ja vain jos $ab = 1 = ba$ eli $\underline{a \text{ on kääntyvä ja } b = a^{-1}}$.

Arvostelusta. • Kukaan ei ollut huomannut, että ehto $ba = 1$ oli erikseen osoitettava myös välttämättömäksi; kuitenkin juuri tästä seikasta varoitin tehtävänannossa sanalla "juonikkaampi"; tämä kohta olisi ollut 3 pisteen arvoinen ja se olisi myös ollut osattava (muuten helpossa kokeessa) arvosanaa 5 varten.

• Siitä, että R on rengas, $a, b \in R$ ja $ab = 1$, ei välttämättä seuraa, että a ja b olisivat kääntyviä (ja $b = a^{-1}$). Esimerkiksi olkoon $A = \mathbb{Z}^{\mathbb{N}}$, jolloin A on additiivinen Abelin ryhmä pisteittäin määritellyn laskutoimituksensa suhteen, olkoon $R = \mathrm{End}(A)$ ryhmähomomorfismien $f\colon A \to A$ (eli A:n endomorfismien) rengas ja olkoot $f, g \in R$ kuvaukset $f\colon (x_0, x_1, x_2, \dots) \mapsto (x_1, x_2, \dots)$ sekä $g\colon (x_0, x_1, x_2, \dots) \mapsto (0, x_0, x_1, x_2, \dots)$; tällöin $f \circ g = \mathrm{id}_A = 1_R$, mutta f ja g eivät ole bijektioita, joten f ja g eivät ole kääntyviä renkaassa R.

5. Palautetaan mieleen, että jos $n \in \mathbb{N}_+$, niin kokonaislukujen jäännösluokkien modulo n joukko $\mathbb{Z}_n$ on rengas luonnollisten laskutoimitustensa suhteen.

a) Määritä renkaan $\mathbb{Z}_9$ kääntyvien alkioiden multiplikatiivisen ryhmän $G = \mathbb{Z}_9^*$ alkiot ja kertotaulukko.

b) Osoita, että G on syklinen ryhmä, ja anna sopivalla $n \in \mathbb{N}_+$ jokin ryhmäisomorfismi additiiviselta ryhmältä $\mathbb{Z}_n$ ryhmälle G.

c) Määritä G:n kunkin alkion virittämä G:n aliryhmä.

Ratk. a) Laskettaessa kokonaisluvuilla modulo 9 on $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, ja $1 \cdot 1 = 2 \cdot 5 = 4 \cdot 7 = 8^2 = 1$ sekä $3^2 = 6^2 = 0$, joten $G = \{1, 2, 4, 5, 7, 8\}$. Vaihtoehtoisesti G saadaan kaavasta $G = \{\overline{m} \mid m \in \mathbb{Z},\ 0 \le m \le 8,\ \mathrm{syt}(m, 9) = 1\}$. Nyt G:n kertotaulukko on seuraava (käyttämälläni $\mathcal{AMS}$-TEX-koodilla taulukon ulkomuoto jäi vajaaksi):

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

b) Alkio $2 \in G$ virittää G:n, sillä $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 = 7$, $2^5 = 14 = 5$ ja $2^6 = 10 = 1$. Siis $G = \langle 2 \rangle$ on syklinen ryhmä. Kirjoitetaan $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, jossa lasketaan kokonaisluvuilla modulo 6. Tällöin (ryhmähomomorfismin $\mathbb{Z} \to G$, $n \mapsto 2^n$, indusoima) kuvaus $f\colon \mathbb{Z}_6 \to G$, jolla $f(0) = 1$, $f(1) = 2$, $f(2) = 4$, $f(3) = 8$, $f(4) = 7$ ja $f(5) = 5$, on ryhmäisomorfismi. (Tarkemmin merkinnöin f on kuvaus $n_6 \mapsto 2_9^n$.)

c) Koska $2^{-1} = 5$, $4^{-1} = 7$ ja $8^{-1} = 8$, niin ryhmän G alkioiden virittämät G:n (sykliset) aliryhmät ovat $\langle 1 \rangle = \{1\}$, $\langle 5 \rangle = \langle 2 \rangle = G$ edellisen kohdan mukaan, $\langle 7 \rangle = \langle 4 \rangle = \{1, 4, 16, 1\} = \{1, 4, 7\}$ ja $\langle 8 \rangle = \{1, 8\}$.