Algebra I, korvaava 2. kurssikoe ma 11.5.2009/ratkaisut (J. Luukkainen), 2 sivua (myös kurssin kotisivulla)

1. Olkoot G_1 ja G_2 (multiplikatiivisia) ryhmiä ja N_i ryhmän G_i normaali aliryhmä, kun $i = 1, 2$. Osoita ryhmien homomorfialauseen avulla, että $N = N_1 \times N_2$ on tuloryhmän $G = G_1 \times G_2$ normaali aliryhmä ja että tekijäryhmä G/N on isomorfinen ryhmän $(G_1/N_1) \times (G_2/N_2)$ kanssa. **Ohje.** Olkoon $p_i \colon G_i \to G_i/N_i$ kanoninen surjektio, kun $i = 1, 2$, ja olkoon $f \colon G \to (G_1/N_1) \times (G_2/N_2)$ kuvaus $(x_1, x_2) \mapsto (p_1(x_1), p_2(x_2))$. Osoita, että f on surjektiivinen homomorfismi ja että $\mathrm{Ker}(f) = N$.

Ratk. Kuvaus f on ryhmähomomorfismi, sillä jos $z = (x_1, x_2) \in G$ ja $z' = (x_1', x_2') \in G$, niin

$$\begin{aligned} f(zz') &= f((x_1, x_2)(x_1', x_2')) = f(x_1x_1', x_2x_2') = (p_1(x_1x_1'), p_2(x_2x_2')) \\ &= (p_1(x_1)p_1(x_1'), p_2(x_2)p_2(x_2')) = (p_1(x_1), p_2(x_2))(p_1(x_1'), p_2(x_2')) = f(z)f(z'). \end{aligned}$$

Kuvaus f on surjektio, sillä jos $u = (u_1, u_2) \in (G_1/N_1) \times (G_2/N_2)$, niin kummallakin $i = 1, 2$ on $u_i = p_i(x_i)$ jollain $x_i \in G_i$, ja tällöin $z = (x_1, x_2) \in G$ sekä $f(z) = u$.

Nyt $\mathrm{Ker}(f) = N$, sillä alkiolle $z = (x_1, x_2) \in G$ on $z \in \mathrm{Ker}(f) \iff f(z) = 1_{(G_1/N_1)\times(G_2/N_2)} \iff (p_1(x_1), p_2(x_2)) = (1_{G_1/N_1}, 1_{G_2/N_2}) \iff (x_1 \in N_1 \text{ ja } x_2 \in N_2) \iff z \in N_1 \times N_2 = N$.

Ylläolevien tulosten ja ryhmien homomorfialauseen nojalla $N = \mathrm{Ker}(f)$ on G:n normaali aliryhmä ja f indusoi halutun ryhmäisomorfismin $G/N \to (G_1/N_1) \times (G_2/N_2)$, $zN \mapsto f(z)$, kun $z \in G$.

2. a) Osoita, että multiplikatiiviset ryhmät $\mathbb{Z}_{175}^*$ ja $\mathbb{Z}_{200}^*$ eivät ole isomorfiset laskemalla näiden ryhmien kertaluvut eli alkioiden lukumäärät.

b) Osoita, että ryhmä $\mathbb{Z}_7^*$ ja additiivinen ryhmä $\mathbb{Z}_6$ ovat isomorfiset.

Ratk. a) Jos $n \in \mathbb{N}_+$, niin multiplikatiivisen ryhmän $\mathbb{Z}_n^*$ kertaluku $|\mathbb{Z}_n^*|$ on Eulerin φ-funktion arvo $\varphi(n)$ (itse asiassa, jos $m \in \mathbb{Z}$ ja $0 \le m \le n-1$, niin $\overline{m} \in \mathbb{Z}_n^*$ eli $\overline{m}$ on renkaan $\mathbb{Z}_n$ kääntyvä alkio jos ja vain jos $\mathrm{syt}(m, n) = 1$). Toisaalta tiedetään, että

$$\varphi(n) = n \prod_{p \in \mathbb{P},\, p \mid n} \left(1 - \frac{1}{p}\right),$$

jossa $\mathbb{P}$ on alkulukujen joukko. Nyt

$$\begin{aligned} |\mathbb{Z}_{175}^*| &= \varphi(175) = \varphi(5^2 \cdot 7) = 5^2 \cdot 7 \cdot (1 - 1/5) \cdot (1 - 1/7) = 5(5-1)(7-1) = 5 \cdot 4 \cdot 6 = 120 \quad \text{ja} \\ |\mathbb{Z}_{200}^*| &= \varphi(200) = \varphi(2^3 \cdot 5^2) = 2^3 \cdot 5^2 \cdot (1 - 1/2) \cdot (1 - 1/5) = 2^2 \cdot 5 \cdot (2-1)(5-1) = 4 \cdot 5 \cdot 1 \cdot 4 = 80, \end{aligned}$$

joten $|\mathbb{Z}_{175}^*| \neq |\mathbb{Z}_{200}^*|$. Tästä tietysti seuraa, että ryhmät $\mathbb{Z}_{175}^*$ ja $\mathbb{Z}_{200}^*$ eivät ole isomorfiset.

b) Nyt $|\mathbb{Z}_7^*| = \varphi(7) = 7 - 1 = 6$ (itse asiassa $\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{0\} = \{1, 2, 3, 4, 5, 6\}$), joten riittää osoittaa, että $\mathbb{Z}_7^*$ on syklinen, sillä tällöin $\mathbb{Z}_7^*$ on isomorfinen ryhmän $\mathbb{Z}_6$ kanssa. Koska $2^2 = 4$ ja $2^3 = 8 = 1$ ryhmässä $\mathbb{Z}_7^*$, ei alkio 2 kelpaa virittäjäksi. Mutta $3^2 = 9 = 2$, $3^3 = 6$, $3^4 = 18 = 4$, $3^5 = 12 = 5$ ja $3^6 = 15 = 1$ ryhmässä $\mathbb{Z}_7^*$, joten alkio 3 virittää ryhmän $\mathbb{Z}_7^*$.

3. Olkoon R rengas. Alkioiden $a, b \in R$ *kommutaattori* on alkio $[a, b] = ab - ba \in R$.

a) Olkoon I renkaan R ideaali. Osoita, että seuraavat kolme ehtoa ovat yhtäpitävät:

(i) $[a, b] \in I$ kaikilla $a, b \in R$.

(ii) $c[a, b] \in I$ kaikilla $a, b, c \in R$.

(iii) $[a, b]c \in I$ kaikilla $a, b, c \in R$.

Ohje. Osoita (iii)$\Longrightarrow$(i)$\Longrightarrow$(ii)$\Longrightarrow$(iii). Huomaa, että $[a, b]c - c[a, b]$ on itsekin kommutaattori.

b) Osoita, että kullekin R:n ideaalille I pätee, että tekijärengas R/I on kommutatiivinen jos ja vain jos I sisältää R:n kaikki kommutaattorit.

Ratk. a) (iii)$\Longrightarrow$(i) saadaan valinnalla $c = 1$.

(i)$\Longrightarrow$(ii) seuraa siitä, että kerrottaessa ideaalin I alkio vasemmalta (tai oikealta) R:n alkiolla saadaan I:n alkio.

Oletetaan (ii). Jos $a, b, c \in R$, niin $[a,b]c - c[a,b] = [[a,b],c]$, joten $[a,b]c = c[a,b] + 1[[a,b],c] \in I$, sillä ideaali I sisältää aina kahden alkionsa summan. Siis (iii) pätee.

Huom. a)-kohta osoittaa, että R:n kommutaattorien joukon virittämä R:n ideaali (eli pienin kommutaattorit sisältävä [molemminpuoleinen] ideaali) $I_c = \{\sum_{k=1}^{n} c_k[a_k,b_k]d_k \mid n \in \mathbb{N},\ a_k, b_k, c_k, d_k \in R, \text{ kun } 1 \le k \le n\}$ saadaan jo, kun valitaan $d_k = 1$ kaikilla k [siis I_c = kommutaattorien virittämä R:n vasemmanpuoleinen ideaali] tai kun valitaan $c_k = 1$ kaikilla k [siis I_c = kommutaattorien virittämä R:n oikeanpuoleinen ideaali].

b) Olkoon ensin I sellainen R:n ideaali, että rengas R/I on kommutatiivinen eli että renkaan R/I kertolasku on vaihdannainen. Jos nyt $a, b \in R$, niin $(a+I)(b+I) = (b+I)(a+I)$, joten $[a,b] + I = (ab - ba) + I = (a+I)(b+I) - (b+I)(a+I) = 0_{R/I} = I$ ja siis $[a,b] \in I$.

Olkoon sitten I sellainen R:n ideaali, että $[a,b] \in I$ kaikilla $a, b \in R$. Jos nyt $x, y \in R/I$, niin $x = a + I$ ja $y = b + I$ joillain $ab \in R$, ja tällöin $xy - yx = (a+I)(b+I) - (b+I)(a+I) = (ab - ba) + I = [a,b] + I = I = 0_{R/I}$, joten $xy = yx$. Siis rengas R/I on kommutatiivinen.

Huom. b)-kohta osoittaa, että I_c on pienin niistä R:n ideaaleista I, joilla R/I on kommutatiivinen.

4. Määritä renkaassa $\mathbb{Z}_3[x]$ polynomien $f = x^3 + x^2 + x + 1$ ja $g = x^2 + 2$ suurin yhteinen tekijä pääpolynomina d (siis d:n johtavan kertoimen on oltava $= 1$) ja esitä d muodossa $uf + vg$ joillain $u, v \in \mathbb{Z}_3[x]$.

Ratk. Kerroinrengas $\mathbb{Z}_3$ on kunta, koska 3 on alkuluku. Voidaan käyttää Eukleideen algoritmia. Jaetaan f jakokulmassa g:llä:

$$\begin{array}{rl} & \quad\ \ x + 1 \\ \cline{2-2} x^2 + 2) & x^3 + x^2 + \ \ x + 1 \\ & \underline{x^3 \qquad + 2x} \\ & \quad\ \ x^2 + 2x + 1 \\ & \quad\ \underline{x^2 \qquad + 2} \\ & \qquad\ \ 2x + 2 \end{array}$$

jossa sovellettiin kahdesti $\mathbb{Z}_3$:n tulosta $1 - 2 = -1 = 2$. Saadaan $f = (x+1)g + (2x+2)$. Jaetaan sitten g jakokulmassa polynomilla $h = 2x + 2$:

$$\begin{array}{rl} & \quad\ \ 2x + 1 \\ \cline{2-2} 2x + 2) & x^2 \qquad + 2 \\ & \underline{x^2 + x} \\ & \qquad\ \ 2x + 2 \\ & \qquad\ \underline{2x + 2}, \end{array}$$

jossa sovellettiin kahdesti $\mathbb{Z}_3$ tulosta $2 \cdot 2 = 4 = 1$ ja kerran tulosta $-1 = 2$. Saadaan $g = (2x+1)h$. Siis $h = 2x + 2$ on eräs f:n ja g:n suurin yhteinen tekijä. Koska $h = 2(x+1)$ ja $2 \in \mathbb{Z}_3^*$, niin $d = \underline{x+1}$ on vaadittu (yksikäsitteinen) pääpolynomiratkaisu $d = \text{syt}(f, g)$.

Nyt $f = (x+1)g + h$, joten $2d = h = f - (x+1)g = f + (2x+2)g$. Koska $\mathbb{Z}_3$:ssa on $2^{-1} = 2$, niin täten $d = 2h = \underline{2f + (x+1)g}$ on vaadittu esitys.

Vaihtoehtoisesti $\text{syt}(f, g)$ voidaan löytää etsimällä f:lle ja g:lle tekijöiden järjestystä vaille yksikäsitteiset esitykset jaottomien pääpolynomien tulona. Huomataan, että $f(0) = 1$, $f(1) = 1$ ja $f(2) = 0$, jolloin $(x-2)|f$ eli $(x+1)|f$; tällöin vaikkapa jakokulmassa jakamalla f:lle saadaan esitys $f = (x+1)(x^2+1)$; tässä taas polynomi $k = x^2 + 1$ on jaoton, sillä muutoin k:lla olisi nollakohta, jonka silloin täytyisi olla f:n nollakohta 2, ja kuitenkin $k(2) = 2$. Sitten huomataan, että $g(0) = 2$, $g(1) = 0$ ja $g(2) = 0$, jolloin $(x-1)|g$ ja $(x-2)|g$, mistä seuraa, että $g = (x-1)(x-2) = (x+2)(x+1)$. Nämä ovat siis halutut f:n ja g:n esitykset. Esityksistä voidaan lukea, että $d = \underline{x+1}$ on vaadittu f:n ja g:n suurin yhteinen tekijä pääpolynomina. **Mutta** u ja v, joilla $d = uf + vg$ eli joilla $1 = u(x^2+1) + v(x+2)$, pitää taas etsiä vaikkapa Eukleideen algoritmilla.