Algebra I, erilliskoe to 13.8.2009/ratkaisut (J. Luukkainen), 2 sivua (kurssin K09 kotonakin)

1. Olkoot A ja B joukkoja ja $f\colon A \to B$ sekä $g\colon B \to A$ kuvauksia, joille $g \circ f = \mathrm{id}_A$. Osoita, että f on injektio ja g surjektio.

Ratk. Jos $a, a' \in A$ ja $f(a) = f(a')$, niin $a = (g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a') = a'$. Siis f on injektio.

Jos $a \in A$, niin $b = f(a) \in B$ ja $g(b) = g(f(a)) = (g \circ f)(a) = a$. Siis g on surjektio.

2. Olkoot $a, b \in \mathbb{Z}$ ja $\operatorname{syt}(a, b) = 1$. Osoita, että $\operatorname{syt}(a + b, a - b)$ on 1 tai 2 (kun suurin yhteinen tekijä vaaditaan positiiviseksi).

Ratk. Koska kokonaislukujen a ja b suurin yhteinen tekijä $\operatorname{syt}(a, b)$ on oletuksen mukaan määritelty, niin $a \neq 0$ tai $b \neq 0$. Tällöin myös $a + b \neq 0$ tai $a - b \neq 0$, sillä muutoin $a = \frac{1}{2}((a + b) + (a - b)) = 0$ ja $b = \frac{1}{2}((a + b) - (a - b)) = 0$. Siis $q = \operatorname{syt}(a + b, a - b) \in \mathbb{N}_+$ on määritelty. Nyt q on myös lukujen $2a = (a + b) + (a - b)$ ja $2b = (a + b) - (a - b)$ tekijä. Tällöin $2a = mq$ ja $2b = nq$ eräillä $m, n \in \mathbb{Z}$.

Oletetaan ensin, että $2|q$ eli että $q = 2r$ jollain $r \in \mathbb{N}_+$. Tällöin $2a = 2mr$ ja $2b = 2nr$, jolloin $a = mr$ ja $b = nr$ ja siis $r|a$ ja $r|b$, joten $r|\operatorname{syt}(a, b)$ eli $r|1$, mistä seuraa, että $r = 1$, ja täten, että $q = 2$.

Oletetaan sitten, että $2\not|q$. Koska $2|2a$ eli $2|mq$, koska 2 on alkuluku ja koska $2\not|q$, niin $2|m$; siis $m = 2m'$ jollain $m' \in \mathbb{Z}$. Samoin $n = 2n'$ jollain $n' \in \mathbb{Z}$. Nyt $2a = 2m'q$ ja $2b = 2n'q$, joten $a = m'q$ ja $b = n'q$. Siis $q|a$ ja $q|b$, joten $q|\operatorname{syt}(a, b) = 1$ ja täten $q = 1$.

3. Tarkastellaan epätyhjän joukon X permutaatioryhmää eli bijektioiden $f\colon X \to X$ ryhmää $G = S_X$ laskutoimituksena kuvausten yhdistäminen. Kutsukaamme bijektiota $f\colon X \to X$ joukon X *kierroksi*, jos on olemassa f:stä riippuva piste $a_f \in X$, jolle $f(a_f) = a_f$ ja $f(x) \neq x$, kun $x \in X \setminus \{a_f\}$. Olkoon $K \subset G$ kaikkien X:n kiertojen joukko. Osoita, että joukon K virittämä G:n aliryhmä $\langle K \rangle$ on G:n normaali aliryhmä.

Ratk. Kierron $f \in K$ käänteiskuvauskin on kierto: Kaikilla $x \in X$ on $f^{-1}(x) = x \iff x = f(x) \iff x = a_f$, joten $f^{-1} \in K$ (ja $a_{f^{-1}} = a_f$). Tästä seuraa, että

$$\begin{aligned}\langle K \rangle &= \{1_G\} \cup \{f_1^{e_1} \circ \ldots \circ f_n^{e_n} \mid n \in \mathbb{N}_+,\ f_1, \ldots, f_n \in K,\ e_1, \ldots, e_n \in \{1, -1\}\} \\ &= \{1_G\} \cup \{f_1 \circ \ldots \circ f_n \mid n \in \mathbb{N}_+,\ f_1, \ldots, f_n \in K\}.\end{aligned}$$

Huomataan, että jos $f \in K$ ja $g \in G$, niin $g \circ f \circ g^{-1} \in K$. Itse asiassa kaikilla $x \in X$ on

$$(g \circ f \circ g^{-1})(x) = x \iff g(f(g^{-1}(x))) = x \iff f(g^{-1}(x)) = g^{-1}(x) \iff g^{-1}(x) = a_f \iff x = g(a_f),$$

joten myös $g \circ f \circ g^{-1}$ on kierto (ja $a_{g \circ f \circ g^{-1}} = g(a_f)$).

Olkoon nyt $f \in \langle K \rangle$ ja $g \in G$. Riittää osoittaa, että $g \circ f \circ g^{-1} \in \langle K \rangle$. Jos $f = 1_G = \mathrm{id}_X$, tämä on selvää, sillä $g \circ f \circ g^{-1} = g \circ 1_G \circ g^{-1} = 1_G \in \langle K \rangle$. Muutoin on $f = f_1 \circ \ldots \circ f_n$ eräällä $n \in \mathbb{N}_+$ ja eräillä $f_1, \ldots, f_n \in K$, jolloin

$$g \circ f \circ g^{-1} = (g \circ f_1 \circ g^{-1}) \circ (g \circ f_2 \circ g^{-1}) \circ \ldots \circ (g \circ f_n \circ g^{-1})$$

on eräiden K:n alkioiden tulo, ja siis $g \circ f \circ g^{-1} \in \langle K \rangle$.

Huom. Ei tarvitse aluksi osoittaa, että $f \in K \implies f^{-1} \in K$, vaan tämän sijasta riittäisi myöhemmin huomata, että $(f \in K, g \in G, e = -1) \implies g \circ f^e \circ g^{-1} = (g \circ f \circ g^{-1})^e$.

4. Olkoon R rengas, olkoon $R^{\mathbb{N}}$ kuvausten $f\colon \mathbb{N} \to R$ rengas, laskutoimitukset siis pisteittäin määriteltyinä, ja olkoon $I \subset R^{\mathbb{N}}$ niiden kuvausten $f \in R^{\mathbb{N}}$ joukko, joille on olemassa sellainen f:stä riippuva luku $n_f \in \mathbb{N}$, että $f(n) = 0$, kun $n \in \mathbb{N}$ ja $n \geq n_f$. Osoita, että I on renkaan $R^{\mathbb{N}}$ ideaali.

Ratk. (i) Nollakuvaus $\overline{0}\colon \mathbb{N} \to R$, $n \mapsto 0$, (siis renkaan $R^{\mathbb{N}}$ nolla-alkio) kuuluu selvästi I:hin ($n_{\overline{0}} = 0$ käy); täten $I \neq \emptyset$.

(ii) Olkoon $f, g \in I$; tällöin $(f - g)(n) = f(n) - g(n) = 0 - 0 = 0$, kun $n \geq n_f$ ja $n \geq n_g$ ja siis kun $n \geq \max(n_f, n_g) \in \mathbb{N}$; täten $f - g \in I$ ($n_{f-g} = \max(n_f, n_g)$ kävi).

(iii) Olkoon $f \in I$ ja $g \in R$; tällöin $(fg)(n) = f(n)g(n) = 0 \cdot g(n) = 0$ ja $(gf)(n) = g(n)f(n) = g(n) \cdot 0 = 0$, kun $n \geq n_f$; siis $fg \in I$ ja $gf \in I$ ($n_{fg} = n_f$ ja $n_{gf} = n_f$ kävivät).

Kohtien (i)–(iii) nojalla I on renkaan $R^{\mathbb{N}}$ ideaali.

5. Määritä ne positiiviset kokonaisluvut n, joilla $\mathbb{Z}_n$-kertoimisten polynomien renkaassa $\mathbb{Z}_n[x]$ polynomi $x^5 - 10x + 12$ on jaollinen polynomilla $x^2 + 2$.

Ratk. 1. Koska $\mathbb{Z}_1 = \{0\}$ ja siis myös $\mathbb{Z}_1[x] = \{0\}$, niin $n = 1$ käy. Olkoon nyt $n \in \mathbb{N}$, $n > 1$. Renkaassa $\mathbb{Z}_n[x]$ polynomi $f = x^5 - 10x + 12$ on jaollinen polynomilla $g = x^2 + 2$ jos ja vain jos jollekin polynomille $q = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}_n[x]$, jolla $k \in \mathbb{N}$ ja $a_k \neq 0$, pätee $f = qg$ eli

$$x^5 - 10x + 12 = a_k x^{k+2} + a_{k-1}x^{k+1} + (a_{k-2} + 2a_k)x^k + (a_{k-3} + 2a_{k-1})x^{k-1} + \ldots + (a_0 + 2a_2)x^2 + 2a_1 x + 2a_0.$$

Ehto on siis, että $k + 2 = 5$ eli $k = 3$ ja

$$x^5 - 10x + 12 = a_3 x^5 + a_2 x^4 + (a_1 + 2a_3)x^3 + (a_0 + 2a_2)x^2 + 2a_1 x + 2a_0$$

eli $a_3 = 1$, $a_2 = 0$, $a_1 + 2a_3 = 0$, $a_0 + 2a_2 = 0$, $2a_1 = -10$ ja $2a_0 = 12$ eli täten $a_3 = 1$, $a_2 = 0$, $a_1 = -2$, $a_0 = 0$, $-4 = -10$ ja $0 = 12$. Tässä $-4 = -10 \iff 6 = 0 \implies 12 = 0$. Näin ollen ehdoksi n:lle tulee, että $6 = 0$ renkaassa $\mathbb{Z}_n$ eli että $n|6$ eli siis $\underline{n \in \{1, 2, 3, 6\}}$, ja tällöin on $q = x^3 - 2x$.

Ratk. 2. Olkoon $n \in \mathbb{N}_+$ sellainen, että renkaassa $\mathbb{Z}_n[x]$ polynomi $f = x^5 - 10x + 12$ on jaollinen polynomilla $g = x^2 + 2$. Tällöin $f = qg$ jollakin polynomilla $q \in \mathbb{Z}_n[x]$. Koska $f = x(x^4 - 10) + 12 = x(x^4 - 4) - 6x + 12 = x(x^2 - 2)(x^2 + 2) - (6x - 12)$, niin tällöin $6x - 12 = x(x^2 - 2)(x^2 + 2) - q(x^2 + 2) = hg$, jossa $h = x^3 - 2x - q$. Jos $h \neq 0$, niin $\deg(h) \geq 0$, joten koska g:n johtava kerroin on 1 (koska $h \neq 0$, tapaus $n = 0$ ei nyt tulee kyseeseen), niin $\deg(hg) = \deg(h) + \deg(g) = \deg(h) + 2 \geq 2$. Tämä on ristiriita, sillä $\deg(6x - 12) \leq 1$. Siis $h = 0$ ja täten $6(x-2) = 6x - 12 = 0$. Näin ollen on $6 = 0$ renkaassa Z_n eli $n|6$. Lisäksi $q = x^3 - 2x$. Kääntäen, jos $n|6$ ja $q = x^3 - 2x$, niin $qg = x^5 - 2x^3 + 2x^3 - 4x = x^5 - 4x = x^5 - 4x - 6x + 12 = x^5 - 10x + 12 = f$, joten $g|f$. Ehto on siis $n|6$.