Algebra I
Harjoitus 11, 20.–24.4.2009
Ratkaisut (MV)
4 sivua

1. Osoita, että $\{a+b\sqrt{3} \mid a,b \in \mathbb{Q}\}$ on $\mathbb{R}$:n alikunta.

Ratkaisu. Merkitään $K = \{a+b\sqrt{3} \mid a,b \in \mathbb{Q}\}$. Tarkistetaan alikuntakriteerin (monisteen Lause 4, s. 95) ehdot:

i) $0 = 0 + 0 \cdot \sqrt{3} \in K$ ja $1 = 1 + 0 \cdot \sqrt{3} \in K$, joten K sisältää ainakin kaksi alkiota.

ii) Olkoot $a, b \in K$. Tällöin $a = a_1 + a_2\sqrt{3}$ ja $b = b_1 + b_2\sqrt{3}$ joillakin $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, joten

$$a - b = (a_1 + a_2\sqrt{3}) - (b_1 + b_2\sqrt{3}) = (a_1 - b_1) + (a_2 - b_2)\sqrt{3} \in K,$$

sillä $a_1 - b_1$ ja $a_2 - b_2$ ovat rationaalilukuja.

iii) Olkoot $a, b \in K$, $b \neq 0$. Voidaan kirjoittaa $a = a_1 + a_2\sqrt{3}$ ja $b = b_1 + b_2\sqrt{3}$ joillakin $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, missä $b_1 \neq 0$ tai $b_2 \neq 0$. Todistetaan, että $b_1 - b_2\sqrt{3} \neq 0$. Tehdään vastaoletus: $b_1 - b_2\sqrt{3} = 0$. Pitää olla $b_2 \neq 0$, sillä muuten $b_1 = b_2\sqrt{3} = 0$ ja saadaan $b = 0$ vastoin oletusta. Siis vastaoletuksesta seuraisi, että $\sqrt{3} = b_1/b_2 \in \mathbb{Q}$, mikä on mahdotonta, joten täytyy olla $b_1 - b_2\sqrt{3} \neq 0$. Luvun b käänteisluvuksi kunnassa $\mathbb{R}$ saadaan siis

$$b^{-1} = \frac{1}{b_1 + b_2\sqrt{3}} = \frac{b_1 - b_2\sqrt{3}}{(b_1 - b_2\sqrt{3})(b_2 + b_2\sqrt{3})} = \frac{b_1}{b_1^2 - 3b_2^2} + \frac{-b_2}{b_1^2 - 3b_2^2}\sqrt{3}.$$

Näin ollen

$$\begin{aligned} ab^{-1} &= (a_1 + a_2\sqrt{3}) \left(\frac{b_1}{b_1^2 - 3b_2^2} + \frac{-b_2}{b_1^2 - 3b_2^2}\sqrt{3} \right) \\ &= \frac{a_1b_1 - 3a_2b_2}{b_1^2 - 3b_2^2} + \frac{b_1a_2 - a_1b_2}{b_1^2 - 3b_2^2}\sqrt{3} \in K, \end{aligned}$$

koska

$$\frac{a_1b_1 - 3a_2b_2}{b_1^2 - 3b_2^2} \quad \text{ja} \quad \frac{b_1a_2 - a_1b_2}{b_1^2 - 3b_2^2}$$

ovat rationaalilukuja.

Siis K on $\mathbb{R}$:n alikunta.

2. Kokonaisalueen R osamääräkunnalle $Q(R)$ ja injektiiviselle rengashomomorfismille $j\colon R \to Q(R)$, jolla R upotetaan $Q(R)$:n alirenkaaksi, todistettiin seuraava *universaalisuusominaisuus*: Jos K on kunta ja $f\colon R \to K$ injektiivinen rengashomomorfismi, niin on olemassa yksikäsitteinen kuntahomomorfismi $\overline{f}\colon Q(R) \to K$, jolla $\overline{f} \circ j = f$.

Osoita, että tämä universaalisuusominaisuus määrää parin $(Q(R), j)$ yksikäsitteisesti (yksikäsitteistä) kuntaisomorfismia vaille. Tarkemmin sanoen, osoita, että jos Q_k on kunta, $j_k\colon R \to Q_k$ on injektiivinen rengashomomorfismi ja parilla (Q_k, j_k) on sama universaalisuusominaisuus kuin parilla $(Q(R), j)$, kun $k = 1, 2$, niin on olemassa yksikäsitteinen kuntaisomorfismi $\varphi\colon Q_1 \to Q_2$, jolla $\varphi \circ j_1 = j_2$.

Huom. Luennoija ilmoitti, että tehtävänannon 1. rivillä alunperin ollut sana "osamäärärenkaalle"oli kirjoitusvirhe.

Ratkaisu. Koska $j_2\colon R \to Q_2$ on injektiivinen, niin oletuksen nojalla on olemassa täsmälleen yksi rengashomomorfismi $\varphi\colon Q_1 \to Q_2$ siten, että $j_2 = \varphi \circ j_1$. Vastaavasti homomorfismin $j_1\colon R \to Q_1$ injektiivisyydestä seuraa, että on olemassa täsmälleen rengashomomorfismi $\psi\colon Q_2 \to Q_1$, jolla $\psi \circ j_2 = j_1$.
Osoitetaan, että $\psi \circ \varphi = \mathrm{id}_{Q_1}$ ja $\varphi \circ \psi = \mathrm{id}_{Q_2}$. Universaalisuusominaisuuden nojalla on olemassa täsmälleen yksi rengashomomorfismi $f\colon Q_1 \to Q_1$ siten, että $j_1 = f \circ j_1$. Selvästi voidaan valita $f = \mathrm{id}_{Q_1}$. Lisäksi

$$(\psi \circ \varphi) \circ j_1 = \psi \circ (\varphi \circ j_1) = \psi \circ j_2 = j_1,$$

joten f:n yksikäsitteisyydestä seuraa, että $\psi \circ \varphi = f = \mathrm{id}_{Q_1}$. Samoin perusteluin nähdään, että koska $(\varphi \circ \psi) \circ j_2 = j_2$ ja $\mathrm{id}_{Q_2} \circ j_2 = j_2$, niin $\varphi \circ \psi = \mathrm{id}_{Q_2}$. Siis ψ on φ:n käänteiskuvaus, joten φ on isomorfismi.

3. Laske $(1 + x)^6$ renkaissa $\mathbb{Z}_3[x]$ ja $\mathbb{Z}_5[x]$.

Ratkaisu. Binomikaavan nojalla

$$\begin{aligned}(1+x)^6 &= \binom{6}{0}x^6 + \binom{6}{1}x^5 + \binom{6}{2}x^4 + \binom{6}{3}x^3 + \binom{6}{4}x^2 + \binom{6}{5}x + \binom{6}{6} \\ &= x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1.\end{aligned}$$

Polynomirenkaassa $\mathbb{Z}_3[x]$ tämä on yhtä kuin $x^6 + \overline{2}x^3 + \overline{1}$ ja polynomirenkaassa $\mathbb{Z}_5[x]$ tämä on yhtä kuin $x^6 + x^5 + x + \overline{1}$.

4. Olkoon $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, jossa $n \geq 1$ ja $a_0 \neq 0 \neq a_n$. Todista: Jos $p/q \in \mathbb{Q}$ (siis $p, q \in \mathbb{Z}$, $q \neq 0$) on f:n nollakohta (kun f tulkitaan $\mathbb{Q}$-kertoimiseksi polynomiksi) ja $\mathrm{syt}(p, q) = 1$, niin p on a_0:n tekijä ja q on a_n:n tekijä.

Ratkaisu. Oletuksen nojalla

$$q^n f(p/q) = a_0q^n + a_1q^{n-1}p + a_2q^{n-2}p^2 + \cdots + a_np^n = 0.$$

Jos merkitään $r = -(a_1q^{n-1} + a_2q^{n-2}p + \cdots + a_np^{n-1})$ ja $s = -(a_0q^{n-1} + \cdots + a_{n-2}qp^{n-2} + a_{n-1}p^{n-1})$, niin edellisestä yhtälöstä nähdään, että

$$a_0q^n = pr \quad \text{ja} \quad a_np^n = qs$$

eli $p|a_0q^n$ ja $q|a_np^n$. Koska $\mathrm{syt}(p, q) = 1$, niin tietysti myös kaikki p:n ja q:n potenssit ovat keskenään jaottomia. Erityisesti $\mathrm{syt}(p, q^n) = \mathrm{syt}(q, p^n) = 1$. Näin ollen $p|a_0$ ja $q|a_n$.

5. Osoita, että polynomien 2 ja x yhdessä virittämä $\mathbb{Z}[x]$:n ideaali ei ole pääideaali.

Ratkaisu. Tehdään vastaoletus: On olemassa $f \in \mathbb{Z}[x]$ siten, että $\langle f \rangle = \langle 2, x \rangle$. Tällöin $f|2$, joten joko $f = \pm 1$ tai $f = \pm 2$. Lisäksi $f|x$, joten joko $f = \pm 1$ tai $f = \pm x$. Ainoa vaihtoehto on siis $f = \pm 1$. Mutta tällöin $\langle 2, x \rangle = \langle \pm 1 \rangle = \mathbb{Z}[x]$. Siis pitäisi olla olemassa sellaiset $a, b \in \mathbb{Z}[x]$, että $2a + xb = 1$. Olkoon $n \in \mathbb{N}$ s.e. $\deg(a), \deg(b) < n$ ja valitaan $a_0, \cdots, a_n, b_0, \cdots, b_{n-1} \in \mathbb{Z}$ s.e. $a = a_0 + \cdots + a_n x^n$ ja $b = b_0 + \cdots + b_{n-1}x^{n-1}$. Tällöin

$$1 = 2a + xb = 2a_0 + (2a_1 + b_0)x + \cdots + (2a_n + b_{n-1})x^n,$$

joten pitää olla $2a_{i+1} + b_i = 0$ kaikilla $i = 0, \ldots, n-1$ ja $2a_0 = 1$. Erityisesti $2|1$, mikä on mahdotonta. Näin ollen vastaoletus on väärä ja $\langle 2, x \rangle$ ei ole pääideaali.

6. Jaa jakokulmamenetelmällä renkaassa $\mathbb{Z}_5[x]$ polynomi $f = x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ polynomilla $g = x^2 + 2x + 3$. Mikä on (vaillinainen) osamäärä ja mikä jakojäännös eli mitkä ovat polynomit q ja r, joilla $f = qg + r$ ja $\deg(r) < \deg(g)$? Tee sitten sama renkaassa $\mathbb{Z}[x]$ ja tutki tulosten yhteyttä. Määritä lopuksi jakokulmatta ratkaisu renkaassa $\mathbb{Z}_7[x]$.

Ratkaisu. Merkitään $f_5 = x^5 + x^4 + \overline{2}x^3 + x^2 + \overline{4}x + 2$ ja $g_5 = x^2 + \overline{2}x + \overline{3}$. Jakokulmasta

$$\begin{array}{rl}
 & x^3 + \overline{4}x^2 + x + \overline{2} \\
\hline
x^2 + \overline{2}x + \overline{3} \;) & x^5 + x^4 + \overline{2}x^3 + x^2 + \overline{4}x + \overline{2} \\
 & \underline{x^5 + \overline{2}x^4 + \overline{3}x^3} \\
 & \quad \overline{4}x^4 + \overline{4}x^3 + x^2 \\
 & \quad \underline{\overline{4}x^4 + \overline{3}x^3 + \overline{2}x^2} \\
 & \quad\quad x^3 + \overline{4}x^2 + \overline{4}x \\
 & \quad\quad \underline{x^3 + \overline{2}x^2 + \overline{3}x} \\
 & \quad\quad\quad \overline{2}x^2 + x + \overline{2} \\
 & \quad\quad\quad \underline{\overline{2}x^2 + \overline{4}x + \overline{1}} \\
 & \quad\quad\quad\quad \overline{2}x + \overline{1}
\end{array}$$

nähdään, että $f_5 = q_5 g_5 + r_5$, missä $q_5 = x^3 + \overline{4}x^2 + x + \overline{2}$ ja $r_5 = \overline{2}x + \overline{1}$. Tehdään sama renkaassa $\mathbb{Z}[x]$:

$$
\begin{array}{rrrrrrrr}
 & & & & x^3 & -x^2 & +x & +2 \\
\cline{5-8}
x^2+2x+3 &)x^5 & +x^4 & +2x^3 & +x^2 & +4x & +2 & \\
 & x^5 & +2x^4 & +3x^3 & & & & \\
\cline{2-5}
 & & -x^4 & -x^3 & +x^2 & & & \\
 & & -x^4 & -2x^3 & -3x^2 & & & \\
\cline{3-6}
 & & & & x^3 & +4x^2 & +4x & \\
 & & & & x^3 & +2x^2 & +3x & \\
\cline{5-7}
 & & & & & 2x^2 & +x & +2 \\
 & & & & & 2x^2 & +4x & +6 \\
\cline{6-8}
 & & & & & & -3x & -4
\end{array}
$$

Nyt $f = qg + r$, missä $q = x^3 - x^2 + x + 2$ ja $r = -3x - 4$.
Mikä tahansa rengashomomorfismi $p\colon R \to R'$, missä R, R' ovat vaihdannaisia renkaita, voidaan laajentaa rengashomomorfismiksi $\varphi\colon R[x] \to R'[x], a_0 + a_1x + \cdots + a_nx^n \mapsto p(a_0) + p(a_1)x + \cdots + p(a_n)x^n$ ja tällöin pätee: Jos $a, b \in R[x]$ ja $b = b_0 + b_1x + \cdots + b_nx$, $b_n \in R^*$, ja jos oletetaan, että $a = cb + d$ joillakin $c, d \in R[x]$, missä $\deg(d) < \deg(b)$, niin tällöin $\varphi(a) = \varphi(c)\varphi(b) + \varphi(d)$, missä edelleen $\deg(\varphi(d)) < \deg(\varphi(b))$. Syy siihen, että $\deg(\varphi(d)) < \deg(\varphi(b))$, on se, että oletuksesta $b_n \in R^*$ seuraa $p(b_n) \in R'^*$, joten erityisesti $p(b_n) \neq 0$ ja siis $\varphi(b)$:n johtava kerroin on $p(b_n)$. Lisäksi polynomin $\varphi(d)$ kertaluku ei tietenkään ainakaan kasva. Jakoyhtälö voidaan siis "siirtää"homomorfismin φ avulla.
Tarkastellaan tapausta, missä $R = \mathbb{Z}$ ja $R' = \mathbb{Z}_5$ ja $p\colon \mathbb{Z} \to \mathbb{Z}_5$ on kuvaus $n \mapsto \overline{n}$. Tällöin $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_5[x]$ on kuvaus $a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n$. Edellisten tulosten yhteys on se, että $f_5 = \varphi(f) = \varphi(qg+r) = \varphi(q)\varphi(g) + \varphi(r) = q_5g_5 + r_5$. Siis jakoyhtälön mukainen esitys $f_5 = q_5g_5 + r_5$ oltaisiin saatu myös esityksestä $f = qg + r$ eikä erillistä jakokulmaa renkaalle $\mathbb{Z}_5[x]$ tarvita.
Käsitellään vielä tapaus $R = \mathbb{Z}$, $R' = \mathbb{Z}_7$ ja $p\colon \mathbb{Z} \to \mathbb{Z}_7$, $n \mapsto \overline{n}$, missä $\overline{n}$ siis tarkoittaa n:n luokkaa mod 7. Nyt $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_7[x]$ on kuvaus $a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n$ ja $f_7 = q_7g_7 + r_7$, missä

$$f_7 = \varphi(f) = x^5 + x^4 + \overline{2}x^3 + x^2 + \overline{4}x + \overline{2}, \quad g_7 = \varphi(g) = x^2 + \overline{2}x + \overline{3},$$
$$q_7 = \varphi(q) = x^3 + \overline{6}x^2 + x + \overline{2} \quad \text{ja} \quad r_7 = \varphi(r) = \overline{4}x + \overline{3}.$$