Algebra 1: Renkaat ja kunnat

Tentti 17.3.2021

Muista perustella vastauksesi huolellisesti!
Saat käyttää apunasi kurssimateriaalia, luentojen valkotauluja ja harjoitustehtävien ratkaisuja.
Viittaa ratkaisuissasi luentomateriaalin tuloksiin.

Olkoon

$$S = \left\{ \begin{pmatrix} a & b \\ 7b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \subset \mathrm{M}_2(\mathbb{R})$$

ja olkoon

$$\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}\,.$$

Olkoon $\psi\colon \mathbb{Z}[\sqrt{7}] \to \mathrm{M}_2(\mathbb{R})$ kuvaus

$$\psi(x + y\sqrt{7}) = \begin{pmatrix} x & y \\ 7y & x \end{pmatrix}\,.$$

Tunnetusti $\mathrm{M}_2(\mathbb{R})$ on rengas ja $\mathbb{Z}[\sqrt{7}]$ on renkaan $\mathbb{R}$ alirengas.

1. (a) Osoita, että ψ on rengashomomorfismi.

(b) Osoita, että S on renkaan $\mathrm{M}_2(\mathbb{R})$ alirengas.

(c) Osoita, että $8 + 3\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$ on yksikkö.

(d) Osoita, että renkaassa S on äärettömän monta yksikköä.

Ratkaisu. (a) Huomataan aluksi, että $\psi(1_{\mathbb{Z}[\sqrt{7}]}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{\mathrm{M}_2(\mathbb{R})}$.

Olkoot $a + b\sqrt{7}, a' + b'\sqrt{7} \in S$. Tällöin

$$\begin{aligned}\psi((a + b\sqrt{7}) + (a' + b'\sqrt{7})) &= \psi((a + a') + (b + b')\sqrt{7}) = \begin{pmatrix} a + a' & b + b' \\ 7(b + b') & a + a' \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ 7b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ 7b' & a' \end{pmatrix} = \psi(a + b\sqrt{7}) + \psi(a' + b'\sqrt{7})\,.\end{aligned}$$

Lisäksi

$$\psi((a + b\sqrt{7})(a' + b'\sqrt{7})) = \psi((aa' + 7bb') + (ab' + a'b)\sqrt{7}) = \begin{pmatrix} aa' + 7bb' & ab' + a'b \\ 7(ab' + a'b) & aa' + 7bb' \end{pmatrix}\,.$$

ja

$$\psi(a + b\sqrt{7})\psi(a' + b'\sqrt{7}) = \begin{pmatrix} a & b \\ 7b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ 7b' & a' \end{pmatrix} = \begin{pmatrix} aa' + 7bb' & ab' + a'b \\ 7(ab' + a'b) & aa' + 7bb' \end{pmatrix}\,,$$

joten $\psi(a + b\sqrt{7})\psi(a' + b'\sqrt{7}) = \psi((a + b\sqrt{7})(a' + b'\sqrt{7}))$.

(b) Proposition 3.23(1) nojalla $S = \psi(\mathbb{Z}[\sqrt{7}])$ on renkaan $\mathrm{M}_2(\mathbb{R})$ alirengas.[1]

(c) $(8 + 3\sqrt{7})(8 - 3\sqrt{7}) = 64 - 63 = 1$.

(d) Koska $8 + 3\sqrt{7} \neq \pm 1$, sen kaikki potenssit ovat eri lukuja keskenään. Proposition 4.1 nojalla $(8 + 3\sqrt{7})^k \in \mathbb{Z}^\times[\sqrt{7}]$ kaikilla $k \in \mathbb{N}$. Jos $u \in \mathbb{Z}^\times[\sqrt{7}]^\times$, niin $\psi(u) \in S^\times$, sillä $\psi(u)\psi(u)^{-1} = \psi(uu^{-1}) = \psi(1) = 1_{\mathrm{M}_2(\mathbb{R})}$. Kuvaus ψ on selvästi injektio, joten väite seuraa.

[1] Tämän voi toki tarkastaa aliryhmätestilläkin.

2. Olkoon R rengas, jossa on vähintään kaksi alkiota. Oletetaan, että kaikille $x \in R$ pätee $x^2 = x$.

(a) Olkoon $r \in R - \{0_R, 1_R\}$. Osoita, että r on nollan jakaja.

(b) Montako yksikköä renkaassa R on?

(c) Osoita, että renkaan R karakteristika on 2.

(d) Osoita, että R on kommutatiivinen rengas.

Ratkaisu. (a) Yhtälö $x^2 = x$ on yhtäpitävä yhtälön $x(x-1) = 0_R$ kanssa. Olkoon $x \in R - \{0_R, 1_R\}$. Tällöin $x \neq 0_R$ ja $x - 1 \neq 0_R$ mutta $x(x-1) = 0_R$. Siis x on nollan jakaja.

(b) Ainoa yksikkö on 1_R, koska 0 ei ole yksikkö ja (a)-kohdan ja Proposition 5.4 nojalla muut renkaan R alkiot eivät ole yksiköitä.

(c) $2\,1_R = (2\,1_R)^2 = 4\,1_R$, joten vähentämällä molemmilta puolilta $2\,1_R$ saadaan $2\,1_R = 0_R$.

(d) Olkoot $x, y \in R$. Tällöin

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y\,.$$

Siis $xy = -yx = yx$, koska (c)-kohdan nojalla $r = -r$ kaikilla $r \in R$.

3. Olkoon R rengas ja olkoon $L \subset R$ ideaali. Olkoon

$$A = \{r \in R : r\ell = 0_R \ \text{ kaikilla } \ \ell \in L\}\,.$$

Osoita, että A on ideaali.

Ratkaisu. Huomataan ensin, että $0_R r = 0_R$ kaikilla $r \in R$, joten erityisesti $0_R \ell = 0_R$ kaikilla $\ell \in L$. Siis $0_R \in A$, joten A ei ole tyhjä.

Jos $a, b \in A$, niin distributiivisuuden nojalla

$$(a-b)\ell = a\ell - b\ell = 0_R - 0_R = 0_R\,.$$

Siis $a - b \in A$. Jos $r \in R$ ja $a \in A$, niin assosiatiivisuuden ja joukon A määritelmän nojalla $(ra)\ell = r(a\ell) = r =_R = 0_R$, joten $ra \in A$.

Koska L on ideaali, pätee $r\ell \in L$ kaikilla $r \in R$. Assosiatiivisuuden nojalla kaikille $a \in A$ ja kaikille $r \in R$ saadaan siis $(ar)\ell = a(r\ell) = 0_R$, joten $ar \in A$.

4. Olkoot $P(X) = X^2 + 1 \in (\mathbb{Z}/7\mathbb{Z})[X]$ ja $Q(X) = X^2 + 3 \in (\mathbb{Z}/7\mathbb{Z})[X]$.

(a) Ovatko polynomit $P(X)$ ja $Q(X)$ jaottomia?

(b) Mitä voit päätellä tekijärenkaista $(\mathbb{Z}/7\mathbb{Z})[X]/(P(X))$ ja $(\mathbb{Z}/7\mathbb{Z})[X]/(Q(X))$ (a)-kohdan nojalla?

(c) Anna esimerkki nollan jakajasta renkaassa $(\mathbb{Z}/7\mathbb{Z})[X]/(P(X))$ tai $(\mathbb{Z}/7\mathbb{Z})[X]/(Q(X))$.

Ratkaisu. (a) Seurauksen 6.17 nojalla toisen asteen kuntakertoiminen polynomi on jaoton, jos ja vain jos sillä ei ole juurta. Kerroinrengas $\mathbb{Z}/7\mathbb{Z}$ on kunta Seurauksen 5.16 nojalla ja $\deg P(X) = \deg Q(X) = 2$, joten riittää tarkastaa, onko näillä polynomeilla juuria. Lasku osoittaa, että

$$\begin{aligned}
P(0 + 7\mathbb{Z}) &= 1 + 7\mathbb{Z}\,,\\
P(1 + 7\mathbb{Z}) = P(6 + 7\mathbb{Z}) &= 2 + 7\mathbb{Z}\,,\\
P(2 + 7\mathbb{Z}) = P(5 + 7\mathbb{Z}) &= 5 + 7\mathbb{Z}\,,\\
P(3 + 7\mathbb{Z}) = P(4 + 7\mathbb{Z}) &= 3 + 7\mathbb{Z}\,,
\end{aligned}$$

joten polynomilla $P(X)$ ei ole juuria. Siis $P(X)$ on jaoton. Koska

$$Q(c) = P(c) + 2 + 7\mathbb{Z}$$

kaikille $c \in \mathbb{Z}/7\mathbb{Z}$, huomaamme helposti, että $Q(2 + 7\mathbb{Z}) = Q(5 + 7\mathbb{Z}) = 0$, joten polynomilla $Q(X)$ on juuret $2 + \mathbb{Z}/7\mathbb{Z}$ ja $5 + 7\mathbb{Z}$. Siis $Q(X)$ ei ole jaoton ja pätee itse asiassa $Q(X) = (X + 2)(X + 5)$.

(b) Rengas $(\mathbb{Z}/7\mathbb{Z})[X]/(P(X)$ on kunta Lauseen 7.32 nojalla. [2]

(c) Alkiot $X+2+(Q(X))$ ja $X+5+(Q(X))$ ovat nollan jakajia renkaassa $(\mathbb{Z}/7\mathbb{Z})[X]/(Q(X)$, sillä

$$(X + 2 + (Q(X)))(X + 5 + (Q(X))) = Q(X) + (Q(X)) = 0 + (Q(X)) \,.$$

Tehtävien pisteytys: 7+7+4+6=24

[2]Tämä riittää vastaukseksi, koska se tulee suoraan tuosta lauseesta. Lisäksi pätee kyllä, että $(\mathbb{Z}/7\mathbb{Z})[X]/(Q(X)$ ei ole kunta, tämä ilmenee konkreettisesti kohdan c) vastauksessa.