

Algebra 1: Renkaat ja kunnat Tentti 10.3.2026

Muista perustella kaikki vastauksesi huolellisesti!

Tehtävien pisteytys: 10+4+6+6+4

Olkoon

$$S = \left\{ \begin{pmatrix} a & b \\ 5b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \subset M_2(\mathbb{R})$$

ja olkoon

$$\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}.$$

Olkoon $\psi: \mathbb{Z}[\sqrt{5}] \rightarrow M_2(\mathbb{R})$ kuvaus

$$\psi(x + y\sqrt{5}) = \begin{pmatrix} x & y \\ 5y & x \end{pmatrix}.$$

Tunnetusti $M_2(\mathbb{R})$ on rengas ja $\mathbb{Z}[\sqrt{5}]$ on renkaan $\mathbb{R}$ alirengas.

1. (a) Osoita, että ψ on rengashomomorfismi.
- (b) Osoita, että S on renkaan $M_2(\mathbb{R})$ alirengas.
- (c) Osoita, että $2 + \sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ on yksikkö.
- (d) Osoita, että renkaassa S on äärettömän monta yksikköä.

Ratkaisu. (a) Huomataan aluksi, että $\psi(1_{\mathbb{Z}[\sqrt{5}]}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{M_2(\mathbb{R})}$.

Olkoot $a + b\sqrt{5}, a' + b'\sqrt{5} \in S$. Tällöin

$$\begin{aligned} \psi((a + b\sqrt{5}) + (a' + b'\sqrt{5})) &= \psi((a + a') + (b + b')\sqrt{5}) = \begin{pmatrix} a + a' & b + b' \\ 5(b + b') & a + a' \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ 5b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ 5b' & a' \end{pmatrix} = \psi(a + b\sqrt{5}) + \psi(a' + b'\sqrt{5}). \end{aligned}$$

Lisäksi

$$\psi((a + b\sqrt{5})(a' + b'\sqrt{5})) = \psi((aa' + 5bb') + (ab' + a'b)\sqrt{5}) = \begin{pmatrix} aa' + 5bb' & ab' + a'b \\ 5(ab' + a'b) & aa' + 5bb' \end{pmatrix}.$$

ja

$$\psi(a + b\sqrt{5})\psi(a' + b'\sqrt{5}) = \begin{pmatrix} a & b \\ 5b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ 5b' & a' \end{pmatrix} = \begin{pmatrix} aa' + 5bb' & ab' + a'b \\ 5(ab' + a'b) & aa' + 5bb' \end{pmatrix},$$

joten $\psi(a + b\sqrt{5})\psi(a' + b'\sqrt{5}) = \psi((a + b\sqrt{5})(a' + b'\sqrt{5}))$.

(b) Proposition 3.23(1) nojalla $S = \psi(\mathbb{Z}[\sqrt{5}])$ on renkaan $M_2(\mathbb{R})$ alirengas.¹

(c) $(2 + \sqrt{5})(-2 + \sqrt{5}) = -4 + 5 = 1$.

(d) Koska $2 + \sqrt{5} \neq \pm 1$, sen kaikki potenssit ovat eri lukuja keskenään. Proposition 4.1 nojalla $(2 + \sqrt{5})^k \in \mathbb{Z}^\times[\sqrt{5}]$ kaikilla $k \in \mathbb{N}$. Jos $u \in \mathbb{Z}^\times[\sqrt{5}]^\times$, niin $\psi(u) \in S^\times$, sillä²

$$\psi(u)\psi(u)^{-1} = \psi(uu^{-1}) = \psi(1) = 1_{M_2(\mathbb{R})}.$$

Kuvaus ψ on selvästi injektio, joten väite seuraa.

¹Tämän voi toki tarkastaa aliryhmätestilläkin.

²Katso Proposition 4.7 todistus.

2. (a) Määritä renkaan $\mathbb{Z}/10\mathbb{Z}$ yksiköt ja nollan jakajat.
 (b) Määritä renkaan $\mathbb{Z}/10\mathbb{Z}$ jokaisen yksikön käänteisalkio.

Ratkaisu. Proposition 5.16 nojalla $a + 10\mathbb{Z}$ on yksikkö, jos ja vain jos $\text{syt}(a, 10) = 1$. Tämä pätee, kun $a \in \{1, 3, 7, 9\}$. Muut nollasta poikkeavat alkio $a + 10\mathbb{Z}$, kun $a \in \{2, 4, 5, 6, 8\}$ ovat nollan jakajia. Lasku osoittaa, että

$$\begin{aligned}(1 + 10\mathbb{Z})^2 &= 1 + 10\mathbb{Z}, \\(9 + 10\mathbb{Z})^2 &= (-1 + 10\mathbb{Z})^2 = 1 + 10\mathbb{Z}, \\(3 + 10\mathbb{Z})(7 + 10\mathbb{Z}) &= 21 + 10\mathbb{Z} = 1 + 10\mathbb{Z}.\end{aligned}$$

Siis

$$\begin{aligned}(\pm 1 + 10\mathbb{Z})^{-1} &= \pm 1 + 10\mathbb{Z}, \\(3 + 10\mathbb{Z})^{-1} &= (7 + 10\mathbb{Z}).\end{aligned}$$

3. Esitä polynomi

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

jaottomien polynomien tulona.

Ratkaisu. Laskemalla huomataan, että $P(0) = 1$, $P(1) = 5$, $P(2) \equiv 6 \pmod{7}$, $P(3) \equiv 1 \pmod{7}$, $P(4) \equiv 4 \pmod{7}$, $P(5) \equiv 4 \pmod{7}$ ja $P(6) \equiv P(-1) \equiv 0 \pmod{7}$. Siis $6 + 7\mathbb{Z}$ on polynomin $P(X)$ ainoa juuri. Koska $-6 \equiv 1 \pmod{7}$, saamme $(X + 1) \mid P(X)$. Lasku esimerkiksi jakokulmassa osoittaa, että

$$P(X) = (X + 1)(X^3 + 3X^2 + X + 1). \quad (*)$$

Jokainen polynomin $X^3 + 3X^2 + X + 1$ juuri olisi polynomin $P(X)$ juuri, joten $-1 + 7\mathbb{Z}$ on ainoa mahdollinen juuri. Kuitenkin $(-1)^3 + 3(-1)^2 - 1 + 1 = 2 \not\equiv 0 \pmod{7}$, joten kolmannen asteen polynomilla $X^3 + 3X^2 + X + 1$ ei ole juuria. Siis se on jaoton, joten (*) on haluttu esitys.

4. (a) Osoita, että $1 + 2\mathbb{Z}$ on polynomin $P(X) \in (\mathbb{Z}/2\mathbb{Z})[X]$ juuri, jos ja vain jos polynomilla $P(X)$ on parillinen määrä nollasta poikkeavia kertoimia.

(b) Osoita, että on kunta, jossa on täsmälleen 32 alkioita. (Vastaukseksi ei riitä todeta, että tallainen kunta on luentojen Lauseen 7.35 nojalla.)

Ratkaisu. (a) Nollasta poikkeava kerroin on aina 1. Jos polynomilla P on k nollasta poikkeavaa kerrointa, niin $P(1) = k \equiv 0 \pmod{2}$, jos ja vain jos k on parillinen.

(b) Seurauksen 7.33 ja Lauseen 7.27 nojalla riittää löytää jaoton viidennen asteen polynomi renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$. Kohdan (a) nojalla tällaisella polynomilla on pariton määrä nollasta poikkeavia kertoimia. Lisäksi vakiotermi tulee olla 1, koska muuten polynomi on jaollinen ensimmäisen asteen polynomilla X . Tämän karsinnan perusteella on 8 ehdokasta $X^5 + X^4 + 1$, $X^5 + X^3 + 1$, $X^5 + X^2 + 1$, $X^5 + X + 1$, $X^5 + X^4 + X^3 + X^2 + 1$, $X^5 + X^4 + X^3 + X + 1$, $X^5 + X^4 + X^2 + X + 1$, $X^5 + X^3 + X^2 + X + 1$.

Kohdan (a) nojalla on yksi jaoton toisen asteen polynomi $X^2 + X + 1$ ja kaksi jaotonta kolmannen asteen polynomia $X^3 + X^2 + 1$ ja $X^3 + X + 1$. Näiden tuloina saadaan kaksi viidennen asteen polynomia $X^5 + X + 1$ ja $X^5 + X^4 + 1$. Jaottomia viidennen asteen polynomeja on siis kuusi.

Renkaan R alkio x on *idempotentti*, jos $x^2 = x$.

Jos renkaan B kaikki alkio ovat idempotentteja, niin B on *Boolean rengas*.

5. Olkoon B Boolean rengas.

(a) Osoita, että $2x = 0$ kaikille $x \in B$.

(b) Määritä $B^\times$.

Ratkaisu. (a) Olkoon $x \in B$. Tällöin

$$2x = (2x)^2 = 4x = 2x + 2x.$$

Koska $(B, +)$ on ryhmä, väite seuraa supistussäännön nojalla.

(b) Boolean renkaan määritelmän nojalla $x(x - 1) = 0$ kaikille $x \in B$. Jos $x \in B - \{0, 1\}$, niin $x - 1 \neq 0$, joten x on nollanjakaja. Proposition 5.3 nojalla x ei ole yksikkö, joten $B^\times = \{1\}$.