Renkaat ja kunnat 2021

Harjoitus 6: ratkaisuja

1. Jaa polynomi
$$P(X) = X^3 + 2X^2 + 3X + 2$$
polynomilla
$$Q(X) = 2X^2 + 3X + 1$$
(1) polynomirenkaassa $\mathbb{Q}[X]$ ja
(2) polynomirenkaassa $(\mathbb{Z}/7\mathbb{Z})[X]$.

Ratkaisu. (1) $X^3 + 2X^2 + 3X + 2 = (\frac{1}{2}X + \frac{1}{4})(2X^2 + 3X + 1) + \frac{7}{4}(X + 1)$.

$$\begin{array}{r|rrrr}
 & \frac{1}{2}X & +\frac{1}{4} & & \\ \hline
2X^2 + 3X + 1 & X^3 & +2X^2 & +3X & +2 \\ \hline
 & \mp X^3 & \mp\frac{3}{2}X^2 & \mp\frac{1}{2}X & \\ \hline
 & & \frac{1}{2}X^2 & +\frac{5}{2}X & +2 \\
 & & \mp\frac{1}{2}X^2 & \mp\frac{3}{4}X & \mp\frac{1}{4} \\ \hline
 & & & \frac{7}{4}X & +\frac{7}{4}
\end{array}$$

(2) $X^3 + 2X^2 + 3X + 2 = (4X + 2)(2X^2 + 3X + 1)$.

$$\begin{array}{r|rrrr}
 & 4X & +2 & & \\ \hline
2X^2 + 3X + 1 & X^3 & +2X^2 & +3X & +2 \\ \hline
 & \mp X^3 & \mp 5X^2 & \mp 4X & \\ \hline
 & & 4X^2 & +6X & +2 \\
 & & \mp 4X^2 & \mp 6X & \mp 2 \\ \hline
 & & & & 0
\end{array}$$

2. Todista Seuraus 6.17.

Ratkaisu. Olkoon K kunta ja olkoon $P(X) \in K[X]$ polynomi, jonka aste on 2 tai 3. Osoitetaan, että $P(X)$ ei ole jaoton, jos ja vain jos sillä on juuri.

Jos polynomilla $P(X)$ on juuri $c \in K$, niin Proposition 6.16 nojalla $(X - c) \mid P(X)$. Proposition 6.10 nojalla polynomit $(X - c)$ ja $P(X)$ eivät ole yksiköitä, sillä kummankin aste on vähintään 1 Proposition 6.8 nojalla. Siis $P(X)$ ei ole jaoton.

Jos $P(X)$ ei ole jaoton, niin on polynomit $Q(X), R(X) \in K[X]$, jotka eivät ole yksiköitä ja joille pätee $P(X) = Q(X)R(X)$. Proposition 6.10 nojalla $\deg P(X), \deg Q(X) \geqslant 1$. Jos $\deg P(X) = 2$, niin Proposition 6.8 nojalla
$$2 = \deg P(X) = \deg Q(X) + \deg R(X)\,,$$
joten $\deg P(X) = \deg Q(X) = 1$. Jos $\deg P(X) = 3$, niin Proposition 6.8 nojalla
$$3 = \deg P(X) = \deg Q(X) + \deg R(X)\,,$$

joten $\{\deg P(X), \deg Q(X)\} = \{1, 2\}$. Molemmissa tapauksissa $P(X)$ on jaollinen ensimmäisen asteen polynomilla, olkoon tämä polynomi $Q(X)$. Ensimmäisen asteen polynomilla $Q(X)$ on juuri $c \in K$, sillä K on kunta. Siis $P(c) = Q(c)R(c) = 0$, joten polynomilla $P(X)$ on juuri.

3. Mitkä polynomit $aX^2 + bX + c \in \mathbb{R}[X]$ ovat jaottomia?

Ratkaisu. Olkoon $P(X) = aX^2 + bX + c$. Jos $a = 0$ ja $b = 0$, niin $P(X)$ on 0 tai yksikkö, joten se ei ole jaoton. Jos $a = 0$ ja $b \neq 0$, niin $P(X)$ on ensimmäisen asteen polynomina jaoton. Jos $a \neq 0$, niin polynomin $P(X)$ juuret saadaan tutulla kaavalla

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

jos $b^2 \geqslant 4ac$. Jos taas $b^2 < 4ac$, niin juuria ei ole. Seurauksen 6.17 nojalla $P(X)$ on siis jaoton, jos $b^2 < 4ac$

4. (a) Onko polynomi $X^2 - 2 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?
(b) Onko polynomi $X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?

Ratkaisu. (a) Olkoon $P(X) = X^2 - 2$. Tällöin $P(0) = -2 \neq 0$, $P(1) = P(4) = -1 \neq 0$, $P(2) = P(3) = 2 \neq 0$, joten polynomilla $P(X)$ ei ole juuria. Seurauksen 6.17 nojalla se on jaoton.
(b) Olkoon $Q(X) = X^2 + 1$. $Q(x) = P(x) + 3$ kaikilla $x \in \mathbb{Z}/5\mathbb{Z}$, joten $Q(2) = Q(3) = 0$. Seurauksen 6.17 nojalla $Q(X)$ ei ole jaoton.

5. Todista Propositio 7.7.

Ratkaisu. Ideaalitestin jälkimmäinen ehto on sama kuin ideaalin määritelmän jälkimmäinen ehto. Jos $A \subset R$ on ideaali, niin A on ryhmän $(R, +)$ aliryhmä. Tällöin kaikille $a, b \in A$ pätee $a - b \in A$, joten ideaalitestin ensimmäinen ehto seuraa.

Oletetaan, että ideaalitestin ehdot (1) ja (2) ovat voimassa epätyhjälle osajoukolle $A \subset R$. Osoitetaan, että A on aliryhmä. Oletuksen mukaan joukossa A on ainakin yksi alkio. Olkoot $a, b \in A$. Ehdon (1) nojalla $0 = a - a \in A$, joten ehdon (1) nojalla $-b = 0 - a \in A$. Siis $a + b = a - (-b) \in A$. Siis A on vakaa ja $+$ indusoi joukkoon A assosiatiivisen laskutoimituksen. Edellä nähtiin, että $0 \in A$ ja jokaisella joukon A alkiolla on vasta-alkio, joten A on ryhmän $(R, +)$ aliryhmä.

6. Todista Propositio 7.12(1).

Ratkaisu. Koska $\mathscr{I}$ on ideaali, se ei ole tyhjä joukko. Siis $\phi(\mathscr{I}) \neq \varnothing$. Olkoot $a, b \in \phi(\mathscr{I})$. Tällöin $a = \phi(a_0)$ ja $b = \phi(b_0)$ joillain $a_0, b_0 \in \mathscr{I}$. Koska ϕ on homomorfismi ja $\mathscr{I}$ on ideaali, saamme

$$a - b = \phi(a_0) - \phi(b_0) = \phi(a_0 - b_0) \in \phi(\mathscr{I}).$$

Olkoon $a \in \phi(\mathscr{I})$ ja olkoon $s \in \phi(R)$. Tällöin $a = \phi(a_0)$ ja $s = \phi(s_0)$ ja

$$sa = \phi(s_0)\phi(a_0) = \phi(s_0 a_0) \in \phi(\mathscr{I}),$$

koska $s_0 a_0 \in \mathscr{I}$. Ideaalitestin nojalla $\phi(\mathscr{I})$ on renkaan $\phi(R)$ ideaali.

7. Olkoot $\mathscr{I}_i$, $i \in I$, renkaan R ideaaleja. Osoita, että $\bigcap_{i\in I} \mathscr{I}_i$ on renkaan R ideaali.

Ratkaisu. Jokainen ideaali $\mathscr{I}_i$ sisältää alkion 0_R, joten $0_R \in \bigcap_{i\in I} \mathscr{I}_i$.

Olkoot $x, y \in \bigcap_{i\in I} \mathscr{I}_i$. Tällöin $x, y \in I_i$ jokaisella $i \in I$. Ideaalitestin mukaan $x - y \in \mathscr{I}$ kaikilla $i \in I$, joten $x - y \in \bigcap_{i\in I} \mathscr{I}_i$.

Olkoon $x \in \bigcap_{i\in I} \mathscr{I}_i$ ja olkoon $r \in R$. Tällöin $x \in I_i$ jokaisella $i \in I$. Ideaalitestin mukaan $cx \in \mathscr{I}$ kaikilla $i \in I$, joten $cx \in \bigcap_{i\in I} \mathscr{I}_i$.

Ideaalitestin nojalla $\bigcap_{i\in I} \mathscr{I}_i$ on ideaali.

8. Olkoon K kommutatiivinen rengas. Olkoot $a_1, a_2, \ldots a_n \in K$. Osoita, että

$$\{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in K\}$$

on renkaan K ideaali.

Ratkaisu. Olkoon

$$A = \{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in K\}$$

Valitsemalla $x_1 = 1$ ja $x_2 = x_3 = \cdots = x_k = 0$ näemme, että $a_1 \in A$, joten $A \neq \varnothing$. Olkoot $s, t \in A$. Tällöin $s = x_1a_1 + x_2a_2 + \cdots + x_na_n$ ja $t = y_1a_1 + y_2a_2 + \cdots + y_na_n$ joillain $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in K$. Yhteenlaskun kommutatiivisuuden ja distributiivisuuden nojalla

$$s - t = (x_1 - y_1)a_1 + (x_2 - y_2)a_2 + \cdots + (x_n - y_n)a_n \in A$$

ja kaikille $r \in K$ pätee distributiivisuuden ja assosiatiivisuuden nojalla

$$rs = r(x_1a_1 + x_2a_2 + \cdots + x_na_n) = (rx_1)a_1 + (rx_2)a_2 + \cdots + (rx_n)a_n \in A\,.$$

Ideaalitestin nojalla A on ideaali.