Renkaat ja kunnat 2021

Harjoitus 7: ratkaisuja

1. Todista Lemma 7.14.

Ratkaisu. Olkoon K kommutatiivinen rengas. Olkoot $a \in K$ ja $u \in K^\times$. Olkoon $x = ka \in (a)$. Tällöin $x = ka = ku^{-1}ua \in (ua)$. Vastaavasti, jos $y = kua \in (ua)$, niin $y = (ku)a \in (a)$. Siis $(a) = (ua)$.

2. Olkoon R rengas ja olkoon $\mathscr{I} \subset R$ ideaali. Renkaan R yhteenlasku on yhteensopiva ideaalin $\mathscr{I}$ määräämän ekvivalenssirelaation kanssa.

Ratkaisu. Olkoon $\sim$ ideaalin $\mathscr{I}$ määräämä ekvivalenssirelaatio. Jos $a \sim a' \mod q$ ja $b \sim b' \mod q$, niin $a - a', b - b' \in \mathscr{I}$. Tällöin

$$a + b - (a' + b') = (a - a') + (b - b') \in \mathscr{I}\,,$$

joten $a + b \sim a' + b'$.

3. Määritä tekijärenkaan $R = (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + 1)$ laskutaulut. Mitkä renkaan R alkiot ovat yksiköitä? Onko rengas R kunta?

Ratkaisu. Valitaan ekvivalenssiluokille edistajat $0, 1, X, X + 1$ ja muodostetaan laskutaulut:

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

ja

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	1	$X+1$
$X+1$	0	$X+1$	$X+1$	0

.

Laskutaulusta näemme, että alkiot $1 + (X^2 + 1)$ ja $X + (X^2 + 1)$ ovat yksiköitä. Renkaassa R on nollan jakaja $X + 1 + (X^2 + 1)$, joten R ei ole kunta.

4. Olkoon $P(X) = X^3 + 2X + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$. Onko $P(X)$ jaoton polynomi? Onko tekijärengas $(\mathbb{Z}/5\mathbb{Z})[X]/(P(X))$ kunta? Montako alkiota tekijärenkaassa $(\mathbb{Z}/5\mathbb{Z})[X]/(P(X))$ on?

Ratkaisu. Kolmannen asteen polynomilla $P(X)$ ei ole juuria, sillä $0^3 + 2\,0 + 1 = 1 \not\equiv 0 \mod 5$, $1^3 + 2 + 1 = 4 \not\equiv 0 \mod 5$ ja $2^3 + 2\,2 + 1 = 13 \not\equiv 0 \mod 5$. Polynomi $P(X)$ on jaoton Seurauksen 6.17 nojalla. Siis tekijärengas $(\mathbb{Z}/5\mathbb{Z})[X]/(P(X))$ on kunta, jossa on 125 alkiota.

5. Olkoon K kommutatiivinen rengas ja olkoon Olkoon $P(X) = X^3 + 1 \in K[X]$. Osoita, että $X + (P(X)) \in K[X]/(P(X))$ on yksikkö.

Ratkaisu.

$$\begin{aligned}(X+(P(X))(-X^2+P(X)) &= -X^3+(P(X)) \\ &= -X^3+X^3+1+(P(X)) = 1+(P(X))\,.\end{aligned}$$

6. Olkoon $\mathscr{I}$ kommutatiivisen renkaan K ideaali ja olkoon $a \in K$. Osoita, että

$$\mathscr{N} = \{ak+m : k \in K, m \in \mathscr{I}\}$$

on renkaan K ideaali.

Ratkaisu. Joukko $\mathscr{N}$ ei ole tyhjä, sillä esimerkiksi $0 = a\,0+0 \in \mathscr{N}$. Olkoot $k_1, k_2 \in K$ ja olkoot $m_1, m_2 \in \mathscr{I}$. Tällöin $k_1 - k_2 \in K$, koska $+$ on laskutoimitus ja $m_1 - m_2 \in \mathscr{I}$, koska $\mathscr{I}$ on ideaali. Siis

$$(ak_1+m_1)-(ak_2+m_2) = a(k_1-k_2)+(m_1-m_2) \in \mathscr{N}\,.$$

Jos $r, k \in K$ ja $m \in \mathscr{I}$, niin $rm \in \mathscr{I}$, koska $\mathscr{I}$ on ideaali, joten

$$r(ak+m) = a(rk)+rm \in \mathscr{N}\,.$$

Ideaalitestin nojalla $\mathscr{N}$ on ideaali.

7. Olkoon K kokonaisalue ja olkoon $a \in K - \{0\}$ alkio, joka ei ole jaoton. Osoita, että (a) ei ole maksimaalinen ideaali.

Ratkaisu. Koska a ei ole jaoton, on $b, c \in K - \{K^\times \cup \{0\}\}$, joille $a = bc$. Siis $a \in (b)$. Jos $(b) = K$, niin $1 = kb$ jollain $k \in K$, joten b olisi yksikkö. Siis (b) on aito ideaali. Jos $b \in (a)$, niin $a \mid b$. Harjoitustehtävän 5.3(2) nojalla tästä seuraa $a = ub$ jollain yksiköllä u. Kertolaskun supistussäännön nojalla $c = u$, mutta tämä on ristiriita, sillä c ei ole yksikkö. Siis (a) on aidon ideaalin (b) aito osajoukko, joten (a) ei ole maksimaalinen.

Ratkaisu. Tarkastetaan, että polynomilla ei ole juuria. Väite seuraa Lauseesta 7.26 ja Seurauksesta 7.32.

8. Osoita, että on kunta, jossa on 9 alkiota.

Ratkaisu. Lauseen 7.26 ja Seurausten 7.32 ja 6.17 nojalla riittää löytää toisen asteen polynomi $P(X) \in (\mathbb{Z}/3\mathbb{Z})[X]$, jolla ei ole juuria. On helppo tarkastaa, että X^2+1 on tällainen: $P(0) = 0^2+1 = 1 \not\equiv 0 \mod 3$, $P(1) = 1^2+1 = 1 \not\equiv 0 \mod 3$ ja $P(2) = 2^2+1 \equiv 2 \not\equiv 0 \mod 3$.