Renkaat ja kunnat 2021

Harjoitus 3: ratkaisuja

1. Osoita, että kokonaislukujen kertolasku on yhteensopiva kongruenssin kanssa.

Ratkaisu. Olkoon $q \in \mathbb{N} - \{0, 1\}$. Olkoot $a, a', b, b' \in \mathbb{Z}$ siten, että $a \equiv a' \mod q$ ja $b \equiv b' \mod q$. Tällöin $a' = a + kq$ jollain $k \in \mathbb{Z}$ ja $b' = b + nq$ jollain $n \in \mathbb{Z}$. Tällöin

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b' - b) + (a' - a)b = a'nq + kqb = (a'n + kb)q\,,$$

joten $a'b' \equiv ab \mod q$.

2. Muodosta yhteen- ja kertolaskun laskutaulut kongruenssiluokilla modulo 2 ja modulo 6.

Ratkaisu. Renkaan $\mathbb{Z}/2\mathbb{Z}$ laskutaulut ovat

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

ja renkaan $\mathbb{Z}/6\mathbb{Z}$ laskutaulut ovat

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	4	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

3. Todista Propositio 3.23(2).

Ratkaisu. Olkoot $x, y \in \phi^{-1}(S')$. Tällöin $\phi(x), \phi(y) \in S'$. Siis

$$\phi(x + y) = \phi(x) + \phi(y) \in S' \quad \text{ja} \quad \phi(xy) = \phi(x)\phi(y) \in S'\,,$$

koska ϕ on rengasisomorfismi ja S' on renkaan R' alirengas. Siis $x + y, xy \in \phi^{-1}(S')$.

Proposition 3.5(2) nojalla $\phi(-1_R) = -1_{R'}$. Koska S' on renkaan R' alirengas, pätee $-1_{R'} \in S'$. Siis $-1_R \in \phi^{-1}(S')$. Alirengastestin[1] nojalla $\phi^{-1}(S')$ on renkaan S alirengas.

4. Todista Lemma 3.28.

Ratkaisu. Olkoon $x \in R$. Tällöin kertolaskun neutraalialkion määritelmän, monikerran määritelmän, distributiivisuuden ja assosiatiivisuuden, monikerran määritelmän, karakteristikan määritelmän ja Proposition 3.9(1) nojalla

$$qx = q\,(1_R x) = 1_R x + 1_R x + \cdots + 1_R x = (1_R + 1_R + \cdots + 1_R)x = (q1_R)x = 0_R x = 0_R\,.$$

[1] Propositio 3.15

5. Osoita, että renkaalla $\mathbb{Z}$ ei ole muita alirenkaita kuin $\mathbb{Z}$.

Ratkaisu. Olkoon S renkaan $\mathbb{Z}$ alirengas. Määritelmän mukaan $1 \in S$, Lemman 3.14 nojalla $0 \in S$ ja esimerkiksi alirengastestin nojalla $-1 \in S$. Alirenkaana S on vakaa yhteenlaskun suhteen, joten kaikki lukujen 1 ja -1 monikerrat kuuluvat alirenkaaseen S. Siis $\mathbb{Z} \subset S$, joten $S = \mathbb{Z}$.

6. Olkoon $q \in \mathbb{N} - \{0, 1\}$. Osoita, että ei ole rengashomomorfismia jäännösluokkarenkaalta $\mathbb{Z}/q\mathbb{Z}$ renkaaseen $\mathbb{Z}$.

Ratkaisu. Oletetaan, että $\phi\colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}$ on rengashomomorfismi. Tällöin $\phi(1 + q\mathbb{Z}) = 1$ ja Lemman 3.18 nojalla $\phi(0 + q\mathbb{Z}) = 0$. Siis

$$\begin{aligned}0 = \phi(0 + q\mathbb{Z}) &= \phi(q(1 + q\mathbb{Z})) = \phi((1 + q\mathbb{Z}) + (1 + q\mathbb{Z}) + \cdots + (1 + q\mathbb{Z})) \\ &= \phi(1 + q\mathbb{Z}) + \phi(1 + q\mathbb{Z}) + \cdots + \phi(1 + q\mathbb{Z}) = 1 + 1 + \cdots + 1 = q\,,\end{aligned}$$

mikä on ristiriita.

Ratkaisu (Toinen tapa)**.** Jos olisi rengashomomorfismi $\phi\colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}$, niin Proposition 3.23(1) nojalla $\phi(\mathbb{Z}/q\mathbb{Z})$ olisi renkaan $\mathbb{Z}$ alirengas. Tehtävän 5 nojalla siis $\phi(\mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}$ mutta tämä on mahdotonta, koska $\phi(\mathbb{Z}/q\mathbb{Z})$ on äärellinen joukko.

7. Sievennä lauseke $(a+b)^p$ kommutatiivisessa renkaassa, jonka karakteristika on alkuluku p. Miksi oletamme, että p on alkuluku?

Ratkaisu. Jos $1 \leqslant k \leqslant p - 1$, niin $\binom{p}{k}$ on jaollinen luvulla p. Tämä johtuu siitä, että $\binom{p}{k}$ on kokonaisluku ja lausekkeen $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ osoittajassa on alkuluku p mutta nimittäjässä sitä ei ole. Siis binomikaavan[2] nojalla ja koska Lemman 1.27 ja Proposition 3.28 nojalla $(pn)x = p(nx) = 0$ kaikille $n \in \mathbb{N}$ ja kaikille $x \in R$, saamme

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p = a^p + b^p\,.$$

Jos p ei olisi alkuluku, lauseke $(a + b)^p$ ei sievenisi yhtä hyvin. Esimerkiksi $\binom{4}{2} = 6$ ei ole jaollinen luvulla 4 ja renkaassa $\mathbb{Z}/4\mathbb{Z}$ pätee

$$\big((1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z})\big)^4 = (2 + 4\mathbb{Z})^4 = 0 \neq 2 + 4\mathbb{Z} = (1 + 4\mathbb{Z})^2 + (1 + 4\mathbb{Z})^4\,.$$

8. Olkoon K kommutatiivinen rengas, jonka karakteristika on alkuluku p. Olkoon $\phi\colon K \to K$ kuvaus $\phi(a) = a^p$. Osoita, että ϕ on rengashomomorfismi.

Ratkaisu. Tehtävän 7 nojalla $\phi\colon (K, +) \to (K, +)$ on homomorfismi:

$$\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b)$$

kaikille $a, b \in K$. Koska kertolasku on kommutatiivinen,

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$$

kaikille $a, b \in K$, joten $\phi\colon (K, \cdot) \to (K, \cdot)$ on homomorfismi. Lisäksi $\phi(1) = 1^p = 1$.

[2] Lemma 3.12