Renkaat ja Kunnat 25.1.2021

Prop. 3.9(1) $0_R x = 0_R$.

$$0_R + x \overset{0_R\text{:n määr.}}{=} x \overset{1_R\text{:n määr.}}{=} 1_R x \overset{0_R\text{:n määr.}}{=} (0_R + 1_R)x \overset{\text{distr.}}{=} 0_R x + 1_R x \overset{1_R\text{:n määr.}}{=} 0_R x + x$$

$(R,+)$ on ryhmä. Supistussääntö $\Rightarrow$ $0_R x = 0_R$.

Jäännösluokkarenkaat

Määr. Olk $q \in \mathbb{N} - \{0,1\}$. Luvut $a, b \in \mathbb{Z}$ ovat kongruentteja mod q, jos on $k \in \mathbb{Z}$ s.e. $a = b + kq$. Merk. $a \equiv b \mod q$.

Luvun $a \in \mathbb{Z}$ kongruenssiluokka on $a + q\mathbb{Z} = \{ b \in \mathbb{Z} : b \equiv a \mod q \}$
$= \{ a + kq : k \in \mathbb{Z} \}$.

1

Havainto: Jos $a, a' \in \mathbb{Z}$, niin pätee joko $a + q\mathbb{Z} = a' + q\mathbb{Z}$ tai
$a + q\mathbb{Z} \cap a' + q\mathbb{Z} = \emptyset$.

Kongruenssiluokkien (mod q) joukko on

$$\mathbb{Z}/q\mathbb{Z} = \{a + q\mathbb{Z} : a \in \mathbb{Z}\} \underset{\uparrow}{=} \{0 + q\mathbb{Z}, 1 + q\mathbb{Z}, \ldots, (q-1) + q\mathbb{Z}\}$$

<u>Jakoyhtälö</u> (Prop. A.1)

Huom. $\underline{\#(\mathbb{Z}/q\mathbb{Z}) = q}$.

Määr. Olk. $*$ laskutoimitus joukossa $\mathbb{Z}$. $*$ on <u>yhteensopiva</u> kongruenssin kanssa mod q, jos aina kun $a \equiv a' \bmod q$ ja $b \equiv b' \bmod q$ pätee $a * b \equiv a' * b' \bmod q$.

Lemma Kokonaislukujen $+$ ja $\cdot$ ovat yhteensopivia kongruenssin kanssa mod q.

Tod. Tark. yhteenlaskua:

olk. $a \equiv a' \mod q$ $\Rightarrow \exists k, l \in \mathbb{Z}$ s.e. $a = a' + kq$

$b \equiv b' \mod q$ $\qquad b = b' + lq$

$$a+b = a'+b' + (k+l)q$$

$$\Rightarrow a+b \equiv a'+b' \mod q.$$

Kertolasku harj.

Seuraus: Kokonaislukujen tin jä o:n avulla saad. laskutoimitukset kongr. luokkien joukkoon:

$$(a+q\mathbb{Z}) + (b+q\mathbb{Z}) = (a+b) + q\mathbb{Z}$$

$$(a+q\mathbb{Z})(b+q\mathbb{Z}) = ab + q\mathbb{Z}$$

Havaintoja. Kuvaus $\begin{cases} \pi : \mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z}, +, \cdot) \\ \pi(x) = x + q\mathbb{Z} \end{cases}$ on 2 laskut var. joukkojen surj. homomorfismi:

olk $a, b \in \mathbb{Z}$, $\pi(a) + \pi(b) = (a+q\mathbb{Z}) + (b+q\mathbb{Z}) = (a+b) + q\mathbb{Z}$

$$= \pi(a+b)$$

$$\pi(a)\pi(b) = (a+q\mathbb{Z})(b+q\mathbb{Z}) = ab + q\mathbb{Z} = \pi(ab).$$

Surj. selvää: $c + q\mathbb{Z} = \pi(c)$

③

Prop. 1.5: $0 + q\mathbb{Z} = \pi(0)$ on $\mathbb{Z}/q\mathbb{Z}$:n +:n n.a.

$1 + q\mathbb{Z} = \pi(1)$ on $\mathbb{Z}/q\mathbb{Z}$:n $\cdot$:n n.a.

Prop. 1.10: Kongr. luokkien + ja $\cdot$ ovat assos. ja komm.

$$(a+q\mathbb{Z})(-a+q\mathbb{Z}) = (a-a)+q\mathbb{Z} = 0+q\mathbb{Z}$$

$\Rightarrow$ $(\mathbb{Z}/q\mathbb{Z}, +)$ on kommutatiivinen ryhmä.

$$(a+q\mathbb{Z})\big((b+q\mathbb{Z})+(c+q\mathbb{Z})\big) = (a+q\mathbb{Z})((b+c)+q\mathbb{Z})$$

$$= a(b+c)+q\mathbb{Z} \underset{\uparrow}{=} (ab+ac)+q\mathbb{Z} = (ab+q\mathbb{Z})+(ac+q\mathbb{Z})$$

$\mathbb{Z}$:n distr.

$$= (a+q\mathbb{Z})(b+q\mathbb{Z}) + (a+q\mathbb{Z})(c+q\mathbb{Z})$$

$\rightarrow$ distributiivisuus OK.

$\rightarrow$ $\underbrace{(\mathbb{Z}/q\mathbb{Z}, +, \cdot)}_{\mathbb{Z}/q\mathbb{Z}}$ on komm. rengas ja $\pi : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ on renkashomomorfismi.

Jäännösluokkarengas mod q

$\pi(a) = a + q\mathbb{Z}$

Esimerkki 2.11. Yhteen- ja kertolaskun laskutaulut kongruenssiluokilla modulo 4

$\mathbb{Z}/4\mathbb{Z}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ja modulo 5

$\mathbb{Z}/5\mathbb{Z}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

.

Merk. laskutaulussa kongr. luokkaa $a + q\mathbb{Z}$ edustajalla $a \in \{0, 1, \dots, q-1\}$.

$(2+4\mathbb{Z})(2+4\mathbb{Z}) = (4+4\mathbb{Z}) = 0+4\mathbb{Z}$ $\quad (0 \equiv 4 \mod 4)$

Olkoot R ja R' renkaita. Kuvaus $\phi : R \to R'$ on *rengashomomorfismi*, jos se on kahdella laskutoimituksella varustetujen joukkojen homomorfismi, jolle pätee $\phi(1) = 1$.

Bijektiivinen rengashomomorfismi on *rengasisomorfismi*.

$\varphi(1_R) = 1_{R'}$

Esim. $X \neq \emptyset$, R rengas.

$\mathcal{F}(X,R) = \{ f : X \to R \}$ funktiorengas

$(f+g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)g(x)$.

Yhteenlaskun n.a. on funktio $0 : X \to R$, $0(x) = 0_R \ \forall x \in X$.

Kertolaskun — " — $1 : X \to R$, $1(x) = 1_R \ \forall x \in X$.

Funktion $f \in \mathcal{F}(X,R)$ vasta-alkio on $-f \in \mathcal{F}(X,R)$, $(-f)(x) = -(f(x))$.

Olk. $a \in X$. $E_a : \mathcal{F}(X,R) \to R$, $E_a(f) = f(a) \ \forall f \in \mathcal{F}(X,R)$.

evaluaatio

E_a on rengashomomorfismi: Olk. $f,g \in \mathcal{F}(X,R)$. $E_a(f+g) = (f+g)(a) = f(a) + g(a)$
$= E_a(f) + E_a(g)$.

• samoin.

$E_a(1) = 1(a) = 1_R$

Propositio 3.20. *(1) Jos $f\colon R \to S$ ja $g\colon S \to T$ ovat rengashomomorfismeja, niin $g \circ f$ on rengashomomorfismi.*

(2) Rengashomomorfismi $f\colon R \to S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $\bar{f}\colon S \to R$, jolle $\bar{f} \circ f = \mathrm{id}_R$ ja $f \circ \bar{f} = \mathrm{id}_S$.

Todistus. Harjoitustehtävät 1.4 ja 3.9. □

Määr. Olk. $\varphi: R \to R'$ rengashomomorfismi

$$\operatorname{Ker}\varphi = \{x \in R : \varphi(x) = 0_{R'}\} = \varphi^{-1}(0_{R'})$$

on φ:n ydin. (Kernel)

Prop. 3,21. Rengashomomorfismi on injektio, jos ja vain jos sen ydin on $\{0\}$.