



Tuomaksen tehtäviä

Tuomas Korppi

Reaalilukujen järjestelmä tavanomaisine laskutoimituksineen on kaikille tuttu, mutta voidaanko reaaliluvuille määritellä muita laskutoimituksia niin, että tutut laskulait säilyvät, eli hienommin sanottuna saadaanko kunnan? Tämänkertaisissa tehtävissä pohdimmekin, voidaanko kunnan yhteenlaskuksi valita reaalilukujen kertolasku.

Hiukan teoriaa

Jos K on joukko, periaatteessa mitä tahansa funktiota $K \times K \rightarrow K$ voidaan pitää laskutoimituksena joukossa K . Meille tutut laskutoimitukset kuitenkin toteuttavat erilaisia laskulakeja, esimerkkinä vaikkapa se, että reaaliluvuille pätee

$$a + (b + c) = (a + b) + c.$$

Abstraktissa algebrassa tutkitaan yleensä sellaisia rakenteita, joiden laskutoimitukset toteuttavat erilaisia laskulakeja. Eräs tällainen rakenne on kunta, jonka määrittelemme seuraavaksi.

Viisikko $(K, \oplus, \otimes, \mathbb{0}, \mathbb{I})$ on kunta, jos K on joukko, $\oplus: K \times K \rightarrow K$, $\otimes: K \times K \rightarrow K$, ja $\mathbb{0}, \mathbb{I} \in K$, sekä seuraavat aksioomat pätevät.

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ kaikilla $a, b, c \in K$.
2. $\mathbb{0} \oplus a = a$ kaikilla $a \in K$.
3. Kaikilla $a \in K$ on olemassa $b \in K$, jolle $a \oplus b = \mathbb{0}$.

4. $a \oplus b = b \oplus a$ kaikilla $a, b \in K$.
5. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ kaikilla $a, b, c \in K$.
6. $\mathbb{I} \otimes a = a$ kaikilla $a \in K$.
7. Kaikilla $a \in K$, $a \neq \mathbb{0}$, on olemassa $b \in K$, jolle $a \otimes b = \mathbb{I}$.
8. $a \otimes b = b \otimes a$ kaikilla $a, b \in K$.
9. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ kaikilla $a, b, c \in K$.
10. $\mathbb{0} \neq \mathbb{I}$.

Kunnassa on siis määritelty yhteen- ja kertolaskut sekä ykkös- ja nolla-alkiot, jotka toteuttavat tavanomaisia laskulakeja. Aksiooman 3 nojalla kaikilla alkioilla on myös vasta-alkio sekä aksiooman 7 nojalla kaikilla nolasta eroavilla alkioilla on käänteisalkio.

Tuttuja kuntia ovat rationaalilukujen kunta, reaalilukujen kunta ja kompleksilukujen kunta, tavallisilla laskutoimituksillaan ja nolla- ja ykkösalkioilla varustettuna. Kunta on kuitenkin määritelty abstraktisti niin, että mikä tahansa joukko, joka on varustettu aksioomat toteuttavilla laskutoimituksilla ja nolla- ja ykkösalkioilla on kunta. On esimerkiksi olemassa kahden alkion kunta, jonka ainoat alkiot ovat $\mathbb{0}$ ja \mathbb{I} ja jossa $\mathbb{0} \oplus \mathbb{I} = \mathbb{I} \oplus \mathbb{0} = \mathbb{I} \otimes \mathbb{I} = \mathbb{I}$ ja $\mathbb{0} \oplus \mathbb{0} = \mathbb{I} \oplus \mathbb{I} = \mathbb{0} \otimes \mathbb{0} = \mathbb{0} \otimes \mathbb{I} = \mathbb{I} \otimes \mathbb{0} = \mathbb{0}$.

Liitteessä annetaan lisää esimerkkejä kunnista. Voit luukaista liitteen tässä välissä, tai siirtyä suoraan tehtäviin.

Tehtävät

Tehtäviin 2–5 vaaditaan paitsi vastaus, myös sen todistus. Tehtävät on pisteytetty, joten voit kokeilla, monenko pisteen edestä saat tehtäviä ratkaistua. Joihinkin tehtäviin on myös vihjeitä, jotka helpottavat tehtävää, mutta vähentävät pistesaalista. Jos luet viiden pisteen vihjeen, saat tehtävästä vain viisi pistettä. Jos luet kolmen pisteen vihjeen, saat tehtävästä vain kolme pistettä, ja jos luet yhden pisteen vihjeen, saat vain yhden pisteen.

Kunnassa voidaan laskea aika pitkälle samalla tavoin kuin reaalityöilläkin. Seuraavassa tehtävässä johdamme hiukan lisää laskulakeja.

Tehtävä 1 (1 piste)

Olkoon $(K, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ kunta. Todista seuraavat väitteet:

1. Jos $a, b, c \in K$, pätee $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$.
2. Jos $a, b \in K$, ja $a \oplus b = \mathbb{O}$, niin myös $b \oplus a = \mathbb{O}$.
3. Jos $a, b \in K$, ja $a \otimes b = \mathbb{I}$, niin myös $b \otimes a = \mathbb{I}$.
4. Jos $a \in K$, $a \oplus \mathbb{O} = a$.
5. Jos $a \in K$, $a \otimes \mathbb{I} = a$.

Lopuissa tehtävissä pohdimme, onko olemassa kunnarakenteita, joissa reaalityöiden kertolasku on kunnan yhteenlasku.

Jos et saa seuraavaa tehtävää tehtyä, on alla yhden pisteen vihje.

Tehtävä 2 (3 pistettä)

Olkoon $\oplus: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, $a \oplus b = ab$ ja $\mathbb{O} = 1$. Onko olemassa paria (\otimes, \mathbb{I}) siten, että $(\mathbb{R}, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ on kunta?

Jos et saa seuraavaa tehtävää tehtyä, on alla viiden pisteen vihje, kolmen pisteen vihje ja yhden pisteen vihje.

Tehtävä 3 (7 pistettä)

Olkoon $\oplus: \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$, $a \oplus b = ab$ ja $\mathbb{O} = 1$. Onko olemassa paria (\otimes, \mathbb{I}) siten, että $(\mathbb{R} \setminus \{0\}, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ on kunta?

Jos et saa seuraavaa tehtävää tehtyä, on alla yhden pisteen vihje.

Tehtävä 4 (3 pistettä)

Olkoon $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$. Olkoon $\oplus: \mathbb{R}_+ \times \mathbb{R}_+ \rightarrow \mathbb{R}_+$, $a \oplus b = ab$ ja $\mathbb{O} = 1$. Olkoon lisäksi $\otimes: \mathbb{R}_+ \times \mathbb{R}_+ \rightarrow \mathbb{R}_+$, $a \otimes b = a^b$. Onko olemassa alkioita \mathbb{I} siten, että $(\mathbb{R}_+, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ on kunta?

Jos et saa seuraavaa tehtävää ratkaistua, on alla viiden pisteen vihje, kolmen pisteen vihje ja yhden pisteen vihje.

Tehtävä 5 (7 pistettä)

Olkoon $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$. Olkoon $\oplus: \mathbb{R}_+ \times \mathbb{R}_+ \rightarrow \mathbb{R}_+$, $a \oplus b = ab$ ja $\mathbb{O} = 1$. Onko olemassa paria (\otimes, \mathbb{I}) siten, että $(\mathbb{R}_+, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ on kunta?

Viiden pisteen vihjeet

(3) Ei ole.

(5) Kyllä on.

Kolmen pisteen vihjeet

(3) Todista ensin seuraavat kaksi lemmaa.

Lemma 1 Olkoon $(K, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ kunta. Tällöin $\mathbb{O} \otimes x = \mathbb{O}$ kaikilla kunnan alkioilla $x \in K$.

Lemma 2 Olkoon $(K, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ kunta, jossa $\mathbb{I} \oplus \mathbb{I} \neq \mathbb{O}$. Olkoon $x \in K$. Tällöin on olemassa $y \in K$, jolle $y \oplus y = x$.

(5) Tutki funktiota $f: \mathbb{R} \rightarrow \mathbb{R}_+$, $f(x) = e^x$. Se on bijektio, ja pätee $f(x + y) = f(x) \oplus f(y)$ kaikilla $x, y \in \mathbb{R}$, sekä $f(0) = \mathbb{O}$.

Yhden pisteen vihjeet

(2) Ei ole.

(3) Kolmen pisteen vihjeen Lemman 1 todistuksessa on hyödyllistä pohtia alkioita $(\mathbb{O} \oplus \mathbb{O}) \otimes x$.

Todista, että kolmen pisteen vihjeen Lemmassa 2 voidaan valita y seuraavasti: Olkoon b sellainen, että $(\mathbb{I} \oplus \mathbb{I}) \otimes b = \mathbb{I}$. Nyt $y = x \otimes b$.

Jotta pääset käyttämään Lemmaa 2 tehtävän ratkaisussa, tee vastaoletus ja tutki tulosta $(\mathbb{I} \oplus \mathbb{I}) \otimes a$, missä $a > 1$.

(4) Ei ole.

(5) Olkoon f kuten kolmen pisteen vihjeessä. Yritä määrittellä \otimes niin, että pätee $f(xy) = f(x) \otimes f(y)$ kaikilla $x, y \in \mathbb{R}$.

Ratkaisut

(1) Näytämme kohdan 1. Muut ovat samankaltaisia, mutta helpompia. $(a \oplus b) \otimes c = c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b) = (a \otimes c) \oplus (b \otimes c)$.

(2) Ei ole. Tehdään vastaoletus: Pari (\otimes, \mathbb{I}) on olemassa. Aksioman 3 nojalla on olemassa $b \in \mathbb{R}$, jolle $0 \oplus b = \mathbb{O}$. Mutta nyt $0b = 1$, mikä ei päde millään $b \in \mathbb{R}$. Ristiriita.

(3) Todistetaan ensin kolmen pisteen vihjeessä annetut lemmat:

Lemma 1: $\mathbb{O} \otimes x = (\mathbb{O} \oplus \mathbb{O}) \otimes x = (\mathbb{O} \otimes x) \oplus (\mathbb{O} \otimes x)$.

On olemassa b siten, että $(\mathbb{O} \otimes x) \oplus b = \mathbb{O}$. Siis $\mathbb{O} = (\mathbb{O} \otimes x) \oplus b = ((\mathbb{O} \otimes x) \oplus (\mathbb{O} \otimes x)) \oplus b = (\mathbb{O} \otimes x) \oplus ((\mathbb{O} \otimes x) \oplus b) = \mathbb{O} \otimes x$.

Lemma 2: Olkoon b sellainen, että $(\mathbb{I} \oplus \mathbb{I}) \otimes b = \mathbb{I}$. Nyt $(x \otimes b) \oplus (x \otimes b) = x \otimes (b \oplus b) = x \otimes ((\mathbb{I} \otimes b) \oplus (\mathbb{I} \otimes b)) = x \otimes ((\mathbb{I} \oplus \mathbb{I}) \otimes b) = x \otimes \mathbb{I} = x$.

Nyt ratkaistaan itse tehtävä, eli osoitetaan, että vaadittua paria ei ole olemassa.

Tehdään vastaoletus: Pari (\otimes, \mathbb{I}) on olemassa.

Olkoon $a > 1$. Nyt $(\mathbb{I} \oplus \mathbb{I}) \otimes a = (\mathbb{I} \otimes a) \oplus (\mathbb{I} \otimes a) = a \oplus a = a^2 \neq 1 = \mathbb{O}$. Siis Lemman 1 nojalla $(\mathbb{I} \oplus \mathbb{I}) \neq \mathbb{O}$.

Olkoon $x < 0$. Lemman 2 nojalla on olemassa $y \in \mathbb{R} \setminus \{0\}$, jolle $y \oplus y = x$, eli $yy = x$. Tämä on kuitenkin ristiriita sen kanssa, että negatiivisilla luvuilla ei ole neliöjuurta.

(4) $a \otimes b = b \otimes a$ ei päde. Esimerkiksi $2^3 \neq 3^2$. Myöskään $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ ei päde. Esimerkiksi $2^{2^3} = 256$, mutta $(2^2)^3 = 64$.

(5) Osoitetaan, että vaadittu pari on olemassa. Tutkitaan funktiota $f: \mathbb{R} \rightarrow \mathbb{R}_+, f(x) = e^x$. Se on bijektio, ja lisäksi pätee $f(x+y) = e^{x+y} = f(x) \oplus f(y)$ sekä $f(0) = \mathbb{O}$.

Määritellään $x \otimes y = f(f^{-1}(x)f^{-1}(y)) = e^{(\ln x)(\ln y)}$, sekä $\mathbb{I} = e$.

Nyt pätee $f(1) = \mathbb{I}$. Olkoot $x, y \in \mathbb{R}$ annettuja, ja merkitään $a = f(x), b = f(y)$. Nyt $a \otimes b = f(f^{-1}(a)f^{-1}(b))$, eli $f(x) \otimes f(y) = f(xy)$.

Nyt kaikki aksiomat voidaan todistaa helposti, kaikki samaa strategiaa käyttäen. Todistamme esimerkkinä aksiomat 9 ja 7.

Ensin 9:

Olkoon $a, b, c \in \mathbb{R}_+$. Olkoot $x, y, z \in \mathbb{R}$ sellaiset, että $f(x) = a, f(y) = b$ ja $f(z) = c$

Nyt $a \otimes (b \oplus c) = f(x) \otimes (f(y) \oplus f(z)) = f(x) \otimes f(y+z) = f(x \otimes (y+z)) = f(xy+xz) = f(xy) \oplus f(xz) = (f(x) \otimes f(y)) \oplus (f(x) \otimes f(z)) = (a \otimes b) \oplus (a \otimes c)$.

Sitten 7:

Olkoon $a \in \mathbb{R}_+, a \neq \mathbb{O}$, annettu. Olkoon $x \in \mathbb{R}$ sellainen, että $f(x) = a$. Koska $f(0) = \mathbb{O}$ ja f on bijektio, $x \neq 0$. Nyt on olemassa $y \in \mathbb{R}$, jolle $xy = 1$. Siis $\mathbb{I} = f(1) = f(xy) = f(x) \otimes f(y) = a \otimes f(y)$. Siis on olemassa $b = f(y)$, jolle $a \otimes b = \mathbb{I}$.

Liite

Esimerkki 1

Tämä esimerkki vaatii hiukan esitietoja lukuteoriasta.

Olkoon p alkuluku. Jos $a \in \mathbb{Z}$, määritetään a :n ekvivalenssiluokka $[a] = \{b \in \mathbb{Z} \mid a \equiv b \pmod{p}\}$. Olkoon $a, b \in \mathbb{Z}$. Havaitaan, että $[a] = [b]$ jos ja vain jos $a \equiv b \pmod{p}$.

Merkitään $\mathbb{Z}_p = \{[a] \mid a \in \mathbb{Z}\}$. Havaitaan, että $\mathbb{Z}_p = \{[0], [1], \dots, [p-1]\}$, eli \mathbb{Z}_p :ssä on p alkioita.

Jos $a, b, c, d \in \mathbb{Z}$, $a \equiv b \pmod{p}$ ja $c \equiv d \pmod{p}$, pätee myös $a+c \equiv b+d \pmod{p}$ ja $ac \equiv bd \pmod{p}$. Siis, jos $[a] = [b]$ ja $[c] = [d]$, pätee myös $[a+c] = [b+d]$ ja $[ac] = [bd]$. Näin ollen voidaan määritellä ekvivalenssiluokkien joukossa laskutoimitukset $\oplus: \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $[x] \oplus [y] = [x+y]$ ja $\otimes: \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $[x] \otimes [y] = [xy]$. Merkitään $\mathbb{O} = [0]$ ja $\mathbb{I} = [1]$.

Nähdään helposti, että $(\mathbb{Z}, +, \times, 0, 1)$ toteuttaa kaikki muut kunta-aksiomat, paitsi aksioma 7 ei toteudu.

Nyt voidaan todistaa helposti, että $(\mathbb{Z}_p, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ toteuttaa kaikki kunta-aksiomat paitsi aksioma 7, johon palaamme hetken päästä. Kaikki muut aksiomat todistetaan samalla strategialla. Näytämme esimerkkinä aksioman 9. Olkoot $[a], [b], [c] \in \mathbb{Z}_p$. Nyt $[a] \otimes ([b] \oplus [c]) = [a] \otimes ([b+c]) = [a(b+c)] = [ab+ac] = [ab] \oplus [ac] = ([a] \otimes [b]) \oplus ([a] \otimes [c])$. Toisena esimerkkinä näytämme aksioman 3. Olkoon $[a] \in \mathbb{Z}_p$. Nyt $a + (-a) = 0$, joten $[a] \oplus [-a] = [a + (-a)] = [0] = \mathbb{O}$.

Olkoon $[a] \in \mathbb{Z}_p, [a] \neq \mathbb{O}$. Nyt a ei ole jaollinen p :llä, joten Fermat'n pienen lauseen nojalla $a^{p-1} \equiv 1 \pmod{p}$. Siis $[a] \otimes [a^{p-2}] = [a^{p-1}] = [1] = \mathbb{I}$. Siis $[a]$:lla on käänteisalkio $[a^{p-2}]$, ja aksioma 7 toteutuu.

Siis $(\mathbb{Z}_p, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ on kunta.

Esimerkki 2

Haluamme määritellä rationaalifunktioiden joukon. Nämä ovat funktioita, jotka saadaan kahden polynomin

osamääränä. Koska nimittäjäpolynomilla voi olla nol-lakohtia, emme voi määrittellä rationaalifunktioita koko \mathbb{R} :ssa. Näin ollen annamme seuraavan määritelmän.

Olkoon

$$K' = \{f: \mathbb{R} \setminus A \rightarrow \mathbb{R} \mid A \subset \mathbb{R} \text{ on äärellinen ja on olemassa reaalikertoimiset polynomit } P, Q, \text{ joille } f(x) = P(x)/Q(x) \text{ aina, kun } f(x) \text{ on määritelty.}\}$$

Määritellään joukossa K' yhteen- ja kertolaskut $\oplus: K' \times K' \rightarrow K'$, $\otimes: K' \times K' \rightarrow K'$ seuraavasti: Olkoot $f, g \in K'$. Asetetaan $(f \oplus g)(x) = f(x) + g(x)$ aina, kun sekä $f(x)$ että $g(x)$ ovat määriteltyjä, ja $(f \otimes g)(x) = f(x)g(x)$ aina, kun sekä $f(x)$ että $g(x)$ ovat määriteltyjä. Määritellään \mathbb{O}' vakiofunktioiksi $\mathbb{O}'(x) = 0$ kaikilla $x \in \mathbb{R}$ ja \mathbb{I}' vakiofunktioiksi $\mathbb{I}'(x) = 1$ kaikilla $x \in \mathbb{R}$.

Havaitaan helposti, että $(K', \oplus, \otimes, \mathbb{O}', \mathbb{I}')$ toteuttaa kaikki muut kunta-aksiomat, paitsi ei aksiomia 3 ja 7. Kaikki muut aksiomat näytetään samalla tavalla. Näytämme esimerkkinä aksioman 9.

Olkoot $f, g, h \in K'$. Aina, kun f, g, h ovat määriteltyjä pisteessä x , pätee $(f \otimes (g \oplus h))(x) = f(x)(g \oplus h)(x) = f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x) = (f \otimes g)(x) + (f \otimes h)(x) = ((f \otimes g) \oplus (f \otimes h))(x)$. Koska funktiot $f \otimes (g \oplus h)$ ja $(f \otimes g) \oplus (f \otimes h)$ on määritelty samoissa pisteissä (ts. aina kun kaikki funktioista f, g, h ovat määriteltyjä), ja ne ovat samoja kaikissa pisteissä, joissa ne on määritelty, $f \otimes (g \oplus h) = (f \otimes g) \oplus (f \otimes h)$.

Rationaalifunktiolla

$$\frac{x+1}{(x+1)(x-1)}$$

ja

$$\frac{1}{x-1}$$

on ainoastaan se ero, että ensimmäinen ei ole määritelty pisteessä -1 . Haluamme kuitenkin ajatella, että nämä ovat sama funktio. Kun tällainen tilanne kohdataan matematiikassa, yleensä muodostetaan ekvivalenssiluokaksi kutsuttu joukko, johon laitetaan kaikki ne oliot, joita halutaan kohdella samoina. Tämän jälkeen jatkossa pelataan ekvivalenssiluokkien joukolla. Näin ollen annamme seuraavat määritelmät:

Olkoon $f \in K'$. Määritellään $[f] = \{g \in K' \mid g(x) = f(x) \text{ kaikilla } x \in \mathbb{R} \setminus A, A \subset \mathbb{R} \text{ on äärellinen}\}$. Olkoon $K = \{[f] \mid f \in K'\}$.

Havaitaan, että jos $[f] = [f']$ ja $[g] = [g']$, niin myös $[f \oplus g] = [f' \oplus g']$ ja $[f \otimes g] = [f' \otimes g']$. Näin ollen voidaan K :ssa määrittellä laskutoimitukset $\oplus: K \times K \rightarrow K$ ja $\otimes: K \times K \rightarrow K$, $[f] \oplus [g] = [f \oplus g]$ ja $[f] \otimes [g] = [f \otimes g]$. Määritellään $\mathbb{O} = [\mathbb{O}']$ ja $\mathbb{I} = [\mathbb{I}']$.

Siitä, että $(K, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ toteuttaa kaikki kunta-aksiomat paitsi 3 ja 7, seuraa helposti, että myös $(K, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ toteuttaa nämä aksiomat. Näytämme esimerkkinä aksioman 9. Olkoon $[f], [g], [h] \in K$. Nyt $[f] \otimes ([g] \oplus [h]) = [f] \otimes ([g \oplus h]) = [f \otimes (g \oplus h)] = [(f \otimes g) \oplus (f \otimes h)] = [f \otimes g] \oplus [f \otimes h] = ([f] \otimes [g]) \oplus ([f] \otimes [h])$.

$(K, \oplus, \otimes, \mathbb{O}, \mathbb{I})$ toteuttaa myös aksiomat 3 ja 7. Näytämme aksioman 7. Aksioma 3 on samankaltainen mutta helpompi.

Olkoon $[f] \in K$, $[f] \neq \mathbb{O}$. Siis lukuunottamatta äärellistä pistejoukkoa $f(x) = P(x)/Q(x)$, missä P ja Q ovat polynomeja, ja P, Q eivät ole identtisesti nolla. Siis P :llä on vain äärellinen määrä nol-lakohtia. Nyt voidaan muodostaa g , $g(x) = Q(x)/P(x)$, joka on määritelty aina, kun $P(x)$ on erisuuri kuin nolla, eli kaikkialla äärellistä määrää pisteitä lukuunottamatta. Siis $g \in K'$ ja $[g] \in K$. Nyt $f(x)g(x) = 1$ aina, kun $f(x), g(x)$ ovat määriteltyjä. Siis $[f] \otimes [g] = [f \otimes g] = \mathbb{I}$. Siis aksioma 7 toteutuu.