

Insinöörimatematiikka: Diskreetti matematiikka

Demonstraatio 2, 28.2.2023

1. Osoita, että reaalilukuväli $(0, 1)$ on yhtä mahtava joukon $\mathbb{R}$ kanssa. Toisin sanoen, etsi jokin bijektio $f : (0, 1) \rightarrow \mathbb{R}$ tai $f : \mathbb{R} \rightarrow (0, 1)$. Vihje: voit soveltaa esim. funktiota $\arctan$, jotain rationaalifunktiota tai eksponenttifunktion ja rationaalifunktion yhdistelmää.

Mallivastaus: Tunnetusti $\arctan : \mathbb{R} \rightarrow (-\frac{\pi}{2}, \frac{\pi}{2})$ on bijektio. Bijektio $(-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow (0, 1)$ saadaan helposti ensimmäisen asteen polynomifunktiona $g(x) = \frac{1}{\pi}x + \frac{1}{2}$, joten esimerkiksi $f(x) = \frac{1}{\pi} \arctan x + \frac{1}{2}$ on kysytty bijektio $\mathbb{R} \rightarrow (0, 1)$.

Myös $f(x) = \frac{1}{x} + \frac{1}{x-1}$ on ehdot toteuttava bijektio $(0, 1) \rightarrow \mathbb{R}$, koska 1) $\lim_{x \rightarrow 0+} f(x) = \infty$ ja $\lim_{x \rightarrow 1-} f(x) = -\infty$, siis f saa miten tahansa suuria ja pieniä arvoja, 2) f on jatkuva välillä $(0, 1)$ ja 3) f on vähenevä, koska $f'(x) = -\frac{1}{x^2} - \frac{1}{(x-1)^2} < 0$. Kohtien 1) ja 2) perusteella f on surjektio ja kohdan 3) perusteella injektio.

2. Osoita, että $|2^A| = 2^{|A|}$, kun joukko A on äärellinen. Ohje: Tee joukon A alkioista rivi $a_1, \dots, a_n$. Mikä tahansa joukon A osajoukko voidaan valita "poimimalla" näistä jotkut mukaan ja jättämällä muut pois. Kuinka monta tapaa on "poimia" jokin osajoukko?

Mallivastaus: Merkitään alkio $a_1, \dots, a_n$ jonoon ja tämän jonon alapuolelle n -pituinen nollista ja ykkösistä koostuva jono, jossa 1 merkitsee osajoukkoon valintaa ja 0 sen ulkopuolelle jättämistä. Näin ollen kaikki joukon A osajoukot voidaan eksaktisti määritellä n -pituisilla bittijonoilla. Koska näitä on 2^n kpl, on osajoukkoja sama määrä.

Sama asia toisin: Määritellään funktio $f : 2^A \rightarrow \{0, 1\}^{|A|}$ seuraavasti: Jokaista $X \subseteq A$ olkoon

$$f(X) = (\chi_X(a_1), \chi_X(a_2), \dots, \chi_X(a_n)),$$

missä χ_X on osajoukon X *karakteristinen funktio*, jolle $\chi_X(a) = 1$, jos $a \in X$ ja $\chi_X(a) = 0$ jos $a \notin X$. Suoraviivaisesti voidaan todeta, että f on bijektio ja siksi $|2^A| = |\{0, 1\}^{|A|}| = 2^{|A|}$.

3. Liitetään reaalilukujen joukkoon alkio $-\infty$ ja sovitaan, että $-\infty < x$ ja että $-\infty + x = -\infty$ aina, kun $x \in \mathbb{R}$. Määritellään uudeksi yhteenlaskuksi $x \oplus y = \max\{x, y\}$ ja uudeksi kertolaskuksi $x \otimes y = x + y$. Tuleeko joukosta $\mathbb{R} \cup \{-\infty\}$ uusien laskutoimitusten suhteen puolirengas (rengas jossa ei välttämättä ole additiivista vasta-alkioita)?

Mallivastaus: Uusien laskutoimitusten suhteen saadaan puolirengas. Uuden kertolaskun vaihdannais- ja assosiatiiviominaisuudet ovat selvät, koska ne pätevät "vanhalle" yhteenlaskulle, ts. $(x \otimes y) \otimes z = (x + y) + z = x + (y + z) = x \otimes (y \otimes z)$, jne. Voidaan myös todeta, että $\max\{x, y\} = \max\{y, x\}$ ja että $\max\{x, \max\{y, z\}\} = \max\{\max\{x, y\}, z\}$ (vaikka jotkut symboleista olisivat $= -\infty$), joten myös uusi yhteenlasku on vaihdannainen ja assosiatiivinen.

Distributiivilakia varten huomataan, että

$$x \otimes (y \oplus z) = x + \max\{y, z\}$$

ja että

$$(x \otimes y) \oplus (x \otimes z) = \max\{x + y, x + z\},$$

mitkä ovat selvästi samansuuruiset. Neutraalialkio "uuden" yhteenlaskun suhteen on $-\infty$, koska $-\infty \oplus x = \max\{-\infty, x\} = x$.

4. Olkoon H ryhmän G aliryhmä. Osoita että jokainen ryhmän H sivuluokka aH on yhtä mahtava kuin H . Ohje: Osoita, että funktio $f : H \rightarrow aH$, $f(h) = ah$ on bijektio.

Mallivastaus: Ohjeessa mainittu funktio on injektio, koska $f(h_1) = f(h_2) \Leftrightarrow ah_1 = ah_2 \Leftrightarrow h_1 = h_2$. Viimeisin ekvivalenssi perustuu siihen, että alkioilla a on ryhmässä käänteisalkio.

Funktio $f : H \rightarrow aH$, $f(h) = ah$ on sivuluokan määritelmän mukaan surjektio.

5. Osoita, että äärellisessä ryhmässä G aliryhmän H kertaluku $|H|$ jakaa aina koko ryhmän kertaluvun $|G|$. Ohje: Aliryhmän H sivuluokat peittävät koko ryhmän G eikä niillä ole yhteisiä alkioita (miksi?).

Mallivastaus: Jokainen ryhmän g alkio kuuluu johonkin sivuluokkaan, sillä aliryhmässä H on myös ykkösalkio 1 , ja siis $g = g1 \in gH$. Jos toisaalta $g_1H \neq g_2H$, mutta jokin $g \in g_1H \cap g_2H$, olisi $g = g_1h_1 = g_2h_2$, ja näin ollen $g_1 = g_2h_2h_1^{-1} \in g_2H$, mistä seuraisi että $g_1H = g_2H$. Näin ollen sivuluokilla ei voi olla yhteisiä alkioita.

Huomautus: Luennolla todettiin, että $g_1 \sim g_2 \Leftrightarrow g_1H = g_2H$ on ekvivalenssi-relaatio. Sivuluokkien erillisyyden voidaan todeta siis myös tätä kautta.

Edellämainitun perusteella ryhmä G voidaan jakaa sivuluokkiin:

$$G = g_1H \cup g_2H \cup \dots \cup g_nH,$$

joilla ei ole yhteisiä alkioita. Toisaalta kuitenkin jokaisessa sivuluokassa on yhtä monta alkioita (edellinen tehtävä). Näin ollen $|G| = n|H|$, siis $|H|$ jakaa luvun $|G|$.

6. Olkoon R jokin rengas ja I sen ihanne. Osoita, että ehdolla $x - y \in I$ määritelty relaatio $x \equiv y$ on kongruenssi renkaassa R . Ohje: Ensin pitää osoittaa, että $x \equiv y$ on ekvivalenssirelaatio, ja sitten että tämä on yhteensopiva renkaan yhteen- ja kertolaskun suhteen.

Mallivastaus: 1) Koska $x - x = 0 \in I$ (nolla-alkio kuuluu alirenkaaseen), on $x \equiv x$ ja siksi relaatio on refleksiivinen.

2) Olkoon $x \equiv y$, jolloin siis $x - y \in I$. Koska I on alirengas, on myös $y - x \in I$ ja siis relaatio on symmetrinen.

3) Olkoon $x \equiv y$ ja $y \equiv z$. Tällöin $x - z = x - y + y - z \in I$, koska $x - y \in I$ ja $y - z \in I$. Näin ollen relaatio on transitiiivinen.

Oletetaan sitten, että $x \equiv y$ ja $z \equiv w$. Tällöin $x + z - (y + w) = (x - y) + (z - w) \in I$, joten $x + z \equiv y + w$. Lisäksi $xz - yw = xz - yz + yz - yw = (x - y)z + y(z - w) \in I$. Täten $xz \equiv yw$, siis relaatio on yhteensopiva yhteen- ja kertolaskun suhteen.

7. Laadi viiden alkion kunnan $\mathbb{F}_5$ kertotaulu. Ohje: $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.

Vastaus: Koska 5 on alkuluku, saadaan viiden alkion kunta jäännösluokkarengana $\mathbb{Z}/5\mathbb{Z}$. Tavan mukaan voidaan jättää nolla pois kertotaulusta. Esim. $\bar{3} \cdot \bar{4} = \overline{3 \cdot 4} = \overline{12} = \bar{2}$, jne.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

8. Olkoon $\mathbb{F}_2 = \{0, 1\}$ kahden alkion kunta. Osoita että polynomi $x^3+x+1 \in \mathbb{F}_2[x]$ on jaoton. Ohje: Jos polynomi olisi jaollinen, sillä olisi nollakohta kunnassa $\mathbb{F}_2$ (miksi?). Esitä jokin toinen kolmannen asteen polynomi, joka on myös jaoton.

Mallivastaus: Jos merkitään $p(x) = x^3+x+1$, on $p(0) = 1$ ja $p(1) = 1+1+1 = 1$ kunnassa $\mathbb{F}_2$. Näin ollen polynomilla $p(x)$ ei ole nollakohtia eikä siksi myöskään ensimmäisen asteen tekijää. Tämän vuoksi $p(x)$ on jaoton. Sama pätee myös polynomille $x^3 + x^2 + 1$.

9. Laadi kertotaulu kahdeksan alkion kunnalle käyttämällä edellisen tehtävän jaotonta polynomia. Ohje: Luento-esimerkki neljän alkion kunnasta.

Mallivastaus: Kunnan $\mathbb{F}_8$ alkiot saadaan tekijärakenteena $\mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$, jolloin kaikki ihanteen $I = \langle x^3 + x + 1 \rangle$ sivuluokat voidaan esittää käyttämällä korkeintaan toisen asteen polynomeja sivuluokkien edustajina. Nämä ovat $0, 1, x, x+1, x^2, x^2+1, x^2+x$, ja x^2+x+1 . Muodostetaan kertotaulu näitä edustajia käyttämällä.

Esim. $(x+1+I)(x^2+I) = x^3+x^2+I = x^3+x+1+x^2+x+1+I = x^2+x+1+I$. Kertotaulussa jätetään yleensä I merkitsemättä.

Myös esim. $x^3 = x^3 + x + 1 + x + 1 \equiv x + 1$ ja $x^4 = x^4 + x^2 + x + x^2 + x = x(x^3 + x + 1) + x^2 + x \equiv x^2 + x$, koska $x(x^3 + x + 1) \in I$

.	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$