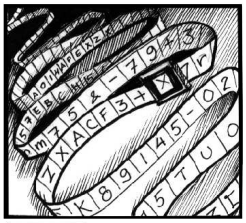


Neljän alkion kunta, solitaire-peli ja taikaneliöt

Kalle Ranto* ja *Petri Rosendahl
Matematiikan laitos, Turun yliopisto

Nykyisissä tietoliikennesovelluksissa käytetään paljon tekniikoita, jotka perustuvat niin sanottujen *äärellisten kuntien* teoriaan. Esimerkiksi matkapuhelimissa käytettyjen virheitä korjaavien koodien, spektrinhajautuskoodien ja salausmenetelmien esittäminen ilman äärellisiä kuntia on käytännössä mahdotonta. Tässä kirjoituksessa esittelemme yksinkertaisen esimerkin äärellisestä kunnasta ja sovellamme sitä solitaire-pelin analysointiin ja taikaneliöiden konstruointiin.

Algebrallisen kunnan laskusäännöt

Karkeasti ottaen algebrallinen kunta on sellainen systeemi, jossa voidaan suorittaa yhteen-, vähennys-, kerto- ja jakolaskuja, ja jossa kaikki tavanomaiset laskulait ovat voimassa. Toisin sanoen kunnan alkioilla lasketaan samaan tapaan kuin reaaliluvuilla $\mathbb{R}$. Koska tämä ei ole riittävän tarkka määritelmä matemaatikolle, sanomme seuraavaksi saman asian hieman toisin.

Määritelmä 1. Joukko K varustettuna kahdella laskutoimituksella $+$ ja $\cdot$ on *kunta*, jos seuraavat ehdot toteutuvat:

1. $(x+y)+z = x+(y+z)$ ja $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ aina kun $x, y, z \in K$,
2. $x+y = y+x$ ja $x\cdot y = y\cdot x$ aina kun $x, y \in K$,
3. joukossa K on sellainen alkio 0, että $x+0 = x$ aina kun $x \in K$,
4. jokaista $x \in K$ kohti on sellainen alkio $-x$, että $x+(-x) = 0$,
5. joukossa K on sellainen alkio 1, että $1\cdot x = x$ aina kun $x \in K$,
6. jokaista $x \in K$, $x \neq 0$, kohti on sellainen alkio x^{-1}, että $x\cdot x^{-1} = 1$,
7. $x\cdot(y+z) = x\cdot y + x\cdot z$ aina kun $x, y, z \in K$.

Joukossa K oletetaan myös olevan vähintään kaksi alkiota.

Yllä mainittu alkio 0 on kunnan K nolla-alkio ja 1 on ykkösalkio.

Alkiota $-x$ sanotaan alkion x vasta-alkioksi ja sen avulla kunnassa määritellään vähennyslasku

$$x - y = x + (-y).$$

Alkiota x^{-1} sanotaan alkion x käänteisalkioksi ja se antaa jakolaskun

$$\frac{x}{y} = x \cdot y^{-1},$$

kun $y \neq 0$. Kunnassa voidaan myös alkio korottaa potenssiin

$$x^n = \underbrace{x \cdot \cdots \cdot x}_{n \text{ kpl}}.$$

Esimerkki 1. Tavallisimpia esimerkkejä kunnista ovat rationaalilukujen joukko $\mathbb{Q}$, reaalilukujen joukko $\mathbb{R}$ ja kompleksilukujen joukko $\mathbb{C}$, kun näissä laskutoimitukset ovat tavalliset yhteen- ja kertolaskut. Sen sijaan kokonaislukujen joukko $\mathbb{Z}$ ei muodosta kuntaa yhteen- ja kertolaskun suhteen, sillä esimerkiksi alkiolla 2 ei ole käänteisalkiota joukossa $\mathbb{Z}$ (ks. Määritelmän 1 ehto 6).

Neljän alkion kunta

Hieman eksoottisempi esimerkki kunnasta on neljän alkion kunta $\mathbb{F}_4$, jota seuraavassa tarkastellaan lähemmin.

Olkoon $\mathbb{F}_4$ neljän alkion joukko $\{0, 1, \alpha, \beta\}$, jonka laskutoimitukset $+$ ja $\cdot$ määritellään Taulukon 1 mukaisesti. Silloin $\mathbb{F}_4$ toteuttaa Määritelmän 1 ehdot eli se on kunta. Selvästikin 0 on kunnan nolla-alkio ja 1 ykkösalkio. Voit halutessasi tarkistaa ehtojen toteutumisen muutamin esimerkein.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Taulukko 1: Neljän alkion kunnan yhteen- ja kertolaskutaulut.

Tehtävä 1. Tarkista laskutauluja käyttäen seuraavat faktat:

(a) Heti nähdään, että $\beta = \alpha^2$ ja $\beta = \alpha + 1$.

(b) Kukin alkio on itsensä vasta-alkio, sillä $x + x = 0$ olipa $x \in \mathbb{F}_4$ mikä hyvänsä.

(c) Koska $\alpha\beta = 1$, alkion α käänteisalkio on β ja β:n käänteisalkio on α.

(d) Helposti todetaan, että $\alpha^n = 1$ jos ja vain jos n on jaollinen kolmella.

(e) Tauluista tai kohdista (a) ja (b) saadaan tärkeä relaatio $\alpha^2 + \alpha + 1 = 0$.

Kunta $\mathbb{F}_4$ tarjoaa yksinkertaisen esimerkin *äärellisestä kunnasta* (Esimerkin 1 kunnat olivat äärettömiä). Näiden teoria on nykyään vilkkaan tutkimuksen kohteena, ja onpa äärellisille kunnille omistettu oma aikakauslehtikin *Finite Fields and Their Applications*.

Esimerkki 2 ($\star$). (Tämän esimerkin ja ($\star$):llä merkityt tehtävät voi hypätä yli.) Voit lukea Tauno Metsänkylän Solmu-artikkelin [4] ja laskea luvuilla $\{0, 1, 2, 3, 4\}$ modulo 5. Tämä tarkoittaa, että yhteen- ja kertolasku menee muuten normaalisti, mutta tuloksessa kiinnostaa ainoastaan jakojäännös 5:llä jaettaessa, jolloin lopputulos saadaan edelleen esitettyä luvuilla 0–4. Esimerkiksi

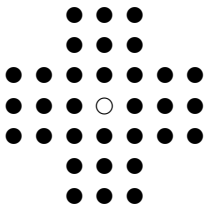
$$\begin{aligned} 1 + 4 = 5 &\equiv 0 \pmod 5, \\ 1 - 3 = -2 &\equiv 3 \pmod 5, \\ 4 \cdot 4 = 16 &\equiv 1 \pmod 5 \quad \text{ja} \\ \frac{3}{4} \equiv 3 \cdot 4 = 12 &\equiv 2 \pmod 5, \text{ koska } 4^{-1} = 4. \end{aligned}$$

Tehtävä 2 ($\star$). Varmista itsellesi, että Esimerkin 2 joukko $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ on viiden alkion kunta, kun laskutoimitukset tehdään modulo 5.

Itse asiassa voidaan osoittaa, että edellisen esimerkin kaltainen joukko on kunta aina kun lasketaan modulo jokin alkuluku (esim. $2, 3, 5, 7, 11, \ldots$). Lisäksi tiedetään, että on olemassa n:n alkion äärellinen kunta tarkalleen silloin, kun n on jokin alkuluvun potenssi (esim. 2^2 tai 3^5).

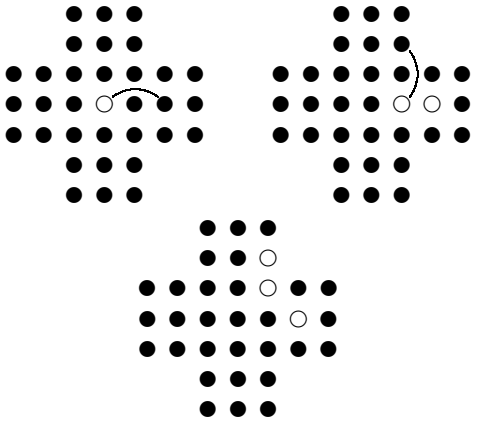
Solitaire-peli

Seuraavassa esitellään pari kombinatoriikan alaan laskettavaa äärellisten kuntien sovellusta. Useimmille tutun solitaire-pelin lauta ja alkutilanne näkyy Kuvassa 1.



Kuva 1: Englantilainen solitaire-lauta.

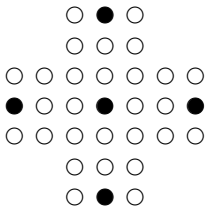
Pelin alkutilanteessa laudan jokaisessa reiässä keskimäistä lukuunottamatta on nappula. Sallitussa siirrossa pelaaja hyppää nappulalla joko vaaka- tai pystysuoraan vieressä olevan nappulan yli sen takana olevaan tyhjään ruutuun, ja poistaa ylihypätyn nappulan (ks. Kuvan 2 siirtoja). Pelaajan tavoitteena on saada poistetuksi kaikki laudan nappulat yhtä lukuunottamatta.



Kuva 2: Esimerkki kahdesta ensimmäisestä siirrosta.

Kysymys. Mihin pelilaudan kohtaan viimeinen nappula voi jäädä?

Tämän kysymyksen selvittämiseen käytämme kunnan $\mathbb{F}_4$ aritmetiikkaa. Ajattelemme pelilaudan pisteet xy-koordinaatiston osajoukoksi niin, että laudan keskipiste on origossa, ja pisteiden koordinaatit ovat kokonaislukuja. Pelilaudan pisteille pätee siis $-3 \leq x \leq 3$ ja $-3 \leq y \leq 3$ (kuitenkaan esim. piste (2,2) ei ole englantilaisella laudalla).



Kuva 3: Mahdolliset paikat viimeiselle nappulalle.

Olkoon X niiden pelilaudan pisteiden joukko, joissa on nappula. Muodostetaan joukon X avulla kunnan $\mathbb{F}_4$ alkiot $A(X)$ ja $B(X)$ kaavoilla

$$A(X) = \sum_{(x,y)\in X} \alpha^{x+y} \quad \text{ja} \quad B(X) = \sum_{(x,y)\in X} \alpha^{x-y}.$$

Esimerkki 3. Olkoon $X = \{(1,0),(1,1),(1,2)\}$ kolmen allekkaisen pisteen joukko ja lasketaan

$$\begin{aligned} B(X) &= \alpha^{1-0} + \alpha^{1-1} + \alpha^{1-2} = \alpha^1 + \alpha^0 + \alpha^{-1} \\ &= \alpha + 1 + \alpha^2 = 0. \end{aligned}$$

Kannattaa huomata, että relaatiosta $\alpha^3 = 1$ seuraa esim. $\alpha^{-1} = \alpha^2$. ($\star$ Esimerkin 2 hengessä voidaan sanoa, että alkion α eksponenteilla lasketaan modulo 3.)

Samoin mille tahansa kolmen vierekkäisen (tai allekkaisen) nappulan joukolle X on voimassa $A(X) = 0 = B(X)$. Tästä saadaan seuraava tulos.

Tehtävä 3. Osoita, että alkutilanteessa $A(X) = 1$ ja $B(X) = 1$.

Esimerkki 4. Jos vaikkapa pisteessä (x, y) oleva nappula siirretään pisteessä $(x + 1, y)$ olevan nappulan yli ja tässä siirrossa nappuloihin liittyvä joukko X muuttuu joukoksi Y, niin alkioiden erotus $A(Y) - A(X)$ on

$$\alpha^{x+2+y} - \alpha^{x+1+y} - \alpha^{x+y} = \alpha^{x+y}\left(\alpha^2 + \alpha + 1\right) = 0.$$

Samoin todetaan muidenkin siirtojen jälkeiselle joukolle Y, että $A(Y) = A(X)$. Laskut on helppo suorittaa myös arvon $B(X)$ tapauksessa.

Tehtävä 4. Jos sallitussa siirrossa nappuloihin liittyvä joukko X muuttuu joukoksi Y, niin osoita, että $A(X) = A(Y)$ ja $B(X) = B(Y)$.

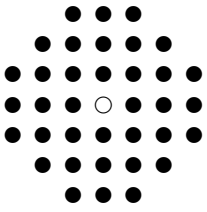
Oletamme nyt, että pelaaja on onnistunut pääsemään yhden nappulan lopputilanteeseen. Olkoon viimeisen nappulan koordinaatit (x, y). Tehtävien 3 ja 4 nojalla täytyy siis olla

$$\alpha^{x+y} = \alpha^{x-y} = 1.$$

Koska $\alpha^n = 1$ tarkalleen silloin, kun 3 jakaa luvun n, niin pienellä päättelyllä saadaan, että 3 jakaa molemmat luvut x ja y. Näin ollen viimeinen nappula voi olla vain jossakin ruuduista $(0,0)$, $(0,3)$, $(3,0)$, $(0,-3,)$ ja $(-3,0)$ (ks. Kuva 3).

Kokeilu osoittaa, että yhden nappulan lopputilanne on todella mahdollinen (ja ratkaisun löytää helposti www-sivuiltakin). Symmetrian nojalla voidaan myös sanoa, että jos jokin yo. lopputilanteista on mahdollinen, niin ne kaikki ovat (mieti tilannetta ennen viimeistä siirtoa).

Kuvassa 1 olevaa lautaa sanotaan englantilaiseksi laudaksi. Joskus näkee käytettävän myös ranskalaista pelilautaa, ks. Kuva 4.



Kuva 4: Ranskalainen solitaire-lauta.

Tehtävä 5. Osoita, että ranskalaisella solitairella ei ole ratkaisua, kun aloituksessa oleva tyhjä paikka on origossa (ts. tällöin ei päästä yhden nappulan lopputilanteeseen).

Solitairen ja kunnan $\mathbb{F}_4$ yhteys on esitetty alunperin artikkelissa [2]. Lisätietoa solitaire-pelistä löytyy esimerkiksi kirjasta [1] ja www-sivuilta, muunmuassa `www.geocities.com/gibell.geo/pegsolitaire/`

Latinalaiset neliöt

Edellisessä Solmussa [5] tehtiin 3×3 -taikaneliöitä. Esitämme nyt yleisen menetelmän, jolla äärellisistä kunnista saadaan taikaneliöitä. Konstruktiot löytyvät ainakin kirjasta [3].

Määritelmä 2. *Latinalainen neliö* on $n\times n$ -taulukko, jonka jokaisessa rivissä ja sarakkeessa kukin luvuista $0,\ldots,n-1$ esiintyy tasan kerran. Jos tämä ehto pitää paikkansa myös molemmille lävistäjille, sanotaan, että latinalainen neliö on *diagonaalinen*.

Voimme konstruoida 4×4 -latinalaisia neliöitä kunnan $\mathbb{F}_4$ avulla, kunhan sovimme alkioiden esittämisestä numeroilla $\{0,1,2,3\}$. Se voidaan tehdä esimerkiksi seuraavasti (kunnan alkiot vasemmalla, numerot oikealla):

$$(1)\qquad 0\leftrightarrow 0 \qquad 1\leftrightarrow 1 \qquad \alpha\leftrightarrow 2 \qquad \beta\leftrightarrow 3$$

Nyt jokaiselle kunnan $\mathbb{F}_4$ nollasta poikkeavalle alkiolle $x\neq 0$ määrittelemme neliön L_x, jonka i:nnen rivin ja j:nnen sarakkeen komponentti on

$$(2)\qquad L_x(i,j)=i\cdot x+j.$$

Tässä laskut suoritetaan kunnassa $\mathbb{F}_4$ käyttäen vastaavuutta (1). Neliön rivien ja sarakkeiden numerointi aloitetaan nollasta eli $i,j\in\{0,1,2,3\}$.

Esimerkki 5. Lasketaan malliksi neliön L_1 komponentteja. Vasemman ylänurkan $(0,0)$ koordinaatit vastaavat kunnan alkiota 0 ja laskusta $L_1(0,0)=0\cdot 1+0=0$ saamme yläkulmaan numeron 0. Loput ylärivistä menee samaan tyyliin $L_1(0,j)=0\cdot 1+j=j$, koska ykkösalkion kerroin on 0.

Lasketaan vielä malliksi neliön L_1 komponentit kohdissa $(1,2)$ ja $(2,3)$. Laskut menevät silloin $L_1(1,2)=1\cdot 1+\alpha=1+\alpha=\beta\leftrightarrow 3$ ja $L_1(2,3)=\alpha\cdot 1+\beta=\alpha+\beta=1$. Loppujen komponenttien laskeminen jää harjoitustehtäväksi. Kaiken kaikkiaan saamme kolme latinalaista neliötä

$$L_1=\begin{bmatrix}0&1&2&3\\1&0&3&2\\2&3&0&1\\3&2&1&0\end{bmatrix},\ L_\alpha=\begin{bmatrix}0&1&2&3\\2&3&0&1\\3&2&1&0\\1&0&3&2\end{bmatrix}\ \text{ja}$$

$$L_\beta=\begin{bmatrix}0&1&2&3\\3&2&1&0\\1&0&3&2\\2&3&0&1\end{bmatrix}.$$

Huomaamme, että esimerkin neliöt ovat toistensa rivipermutaatioita eli saamme kaikki neliöt vaihtelemalla neliön L_1 rivejä sopivasti keskenään. Lisäksi kaikissa neliöissä ensimmäinen rivi on suuruusjärjestyksessä. L_1 on niin sanotussa standardimuodossa, jossa myös ensimmäinen sarake on suuruusjärjestyksessä, ja vieläpä symmetrinen. Toisaalta L_1 ei ole diagonaalinen, mutta L_α ja L_β ovat.

Tehtävä 6. Mieti, miksi kaavan (2) avulla saatavat neliöt ovat latinalaisia.

Määritelmä 3. Kahden $n\times n$ -latinalaisen neliön L ja L' sanotaan olevan *ortogonaaliset*, jos ottamalla molemmista neliöistä samat komponentit pareiksi $(L(i,j),L'(i,j))$ saadaan kaikki mahdolliset n^2 lukuparia $(0,0),(0,1),\ldots,(n,n)$.

Esimerkki 6. Tarkistetaan, ovatko edellisen esimerkin neliöt L_1 ja L_α ortogonaaliset. Voimme muodostaa kahdesta neliöstä yhdisteneliön, jonka komponentit ovat vastaavat komponenttien parit. Esimerkiksi

$$(L_1,L_\alpha)=\begin{bmatrix}(0,0)&(1,1)&(2,2)&(3,3)\\(1,2)&(0,3)&(3,0)&(2,1)\\(2,3)&(3,2)&(0,1)&(1,0)\\(3,1)&(2,0)&(1,3)&(0,2)\end{bmatrix}.$$

Näemme, että kaikki parit esiintyvät tarkalleen kerran, joten L_1 ja L_α ovat ortogonaaliset.

Tehtävä 7. Tarkista samoin, että myös neliöt (L_1,L_β) ja (L_α,L_β) sisältävät kaikki mahdolliset parit.

Voidaan todistaa, että suurin määrä pareittain ortogonaalisia $n\times n$ -latinalaisia neliöitä on korkeintaan $n-1$. Esimerkkimme antaa siis mahdollisimman suuren tällaisen joukon.

Tehtävä 8 ($\star$). Kaava (2) toimii kaikille äärellisille kunnille. Ota siis viiden alkion kunta $\mathbb{F}_5$ Esimerkistä 2, laske siihen liittyvät latinalaiset neliöt L_1, L_2, L_3 ja L_4 ja tarkista, että ne ovat keskenään ortogonaaliset. Näyttävätkö neliöt säännöllisemmiltä kuin neljän alkion kunnasta saadut?

Taikaneliöt

Määritelmä 4. *Taikaneliö* on $n\times n$ -taulukko, jossa kukin luvuista $1,2,\ldots,n^2$ esiintyy tasan kerran ja jonka rivien, sarakkeiden ja lävistäjien summat ovat yhtäsuuret.

Voimme konstruoida $n\times n$ -taikaneliön kahdesta diagonaalisesta ja keskenään ortogonaalisesta $n\times n$-latinalaisesta neliöstä L ja L' seuraavasti: lasketaan taikaneliön $T_{L,L'}$ komponentit säännöllä

$$(3)\qquad T_{L,L'}(i,j)=L(i,j)\cdot n+L'(i,j)+1.$$

Tällä kertaa laskut suoritetaan normaalisti kokonaisluvuilla.

Esimerkki 7. Muodostetaan ortogonaalisten ja diagonaalisten neliöiden L_α ja L_β avulla 4×4 -taikaneliö. Kirjoitamme kaavan (3) taulukkomuodossa

$$T_{L_\alpha, L_\beta} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix} \cdot 4 + \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix} + 1$$
$$= \begin{bmatrix} 1 & 6 & 11 & 16 \\ 12 & 15 & 2 & 5 \\ 14 & 9 & 8 & 3 \\ 7 & 4 & 13 & 10 \end{bmatrix},$$

missä kaikki laskut tehdään komponenteittain. Esimerkiksi vasempaan yläkulmaan tulee $0 \cdot 4 + 0 + 1 = 1$. Voit tarkistaa, että neliön T_{L_α, L_β} rivien, sarakkeiden ja lävistäjien summa todella on aina sama.

Tehtävä 9. Osoita, että $n \times n$ -taikaneliön rivien summa on aina $\frac{1}{2}n(n^2+1)$.

Tehtävä 10. Mieti, miksi kaavan (3) avulla saadaan taikaneliöitä. Yritä todistaa se. Mitä tapahtuu, jos latinalaiset neliöt eivät ole diagonaalisia? Onko T_{L_1, L_α} Määritelmän 4 mukainen taikaneliö?

Tehtävä 11 ($\star$). Muodosta 5×5 -taikaneliö käyttäen Tehtävän 8 latinalaisia neliöitä L_2 ja L_3 (vastaus alla). Miksei neliöitä L_1 ja L_4 voi käyttää?

$$\begin{bmatrix} 1 & 7 & 13 & 19 & 25 \\ 14 & 20 & 21 & 2 & 8 \\ 22 & 3 & 9 & 15 & 16 \\ 10 & 11 & 17 & 23 & 4 \\ 18 & 24 & 5 & 6 & 12 \end{bmatrix}$$

Viitteet

1. E. R. Berlekamp, J. H. Conway, R. K. Guy: *Winning Ways for your mathematical plays*, 2. nide, sivut 697–734, Academic Press, 1982.

2. N. de Bruijn: A solitaire game and its relation to a finite field, J. Recreational Math., 5, sivut 133–137, 1972.

3. C. J. Colbourn, J. H. Dinitz (eds.): The CRC Handbook of Combinatorial Designs, CRC Press, 1996.

4. T. Metsänkylä: Kongruenssi – lukuteorian kätevä apuväline, Solmu 3/1997–1998.

5. Taikasummat ja -tulot, Solmu 1/2005, `http://nrich.maths.org/` .