Tampereen yliopisto

Elina Nieminen

MONOIDIT

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Marraskuu 2019

TIIVISTELMÄ

Elina Nieminen: Monoidit
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Marraskuu 2019

Tässä kandidaatintyössä tarkastellaan erästä algebrallista struktuuria, monoidia. Monoidi koostuu jostakin joukosta sekä siihen liitetystä laskutoimituksesta. Työssä perehdytään myös monoidin ominaisuuksiin, kuten alimonoidiin, transformaatiomonoidiin, erilaisiin generoituihin monoideihin sekä monoidin isomorfismiin.

Avainsanat: monoidit

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisältö

1 Johdanto

Käsittelemme tässä tutkielmassa erästä abstraktia algebrallista struktuuria, monoidia, ja sen ominaisuuksia.

Algebra on matematiikan ala, joka tutkii muun muassa laskutoimituksia ja pyrkii vertailemaan niitä niiden ominaisuuksien perusteella. Muutamiin tämän tutkielman kannalta tärkeisiin ominaisuuksiin tutustumme luvussa 2.

Kun liitämme laskutoimituksen johonkin lukujoukkoon, esimerkiksi yhteenlaskun kokonaislukujen joukkoon, saamme algebrallisen struktuurin. Kyseisiä struktuureja on useanlaisia, ja ne eroavat toisistaan laskutoimitukselle asetettavien ehtojen perusteella. Luvussa 3.1 käsittelemme niitä laskutoimituksen ominaisuuksia, jotka vaaditaan siihen, että algebrallinen struktuuri olisi monoidi. Sen jälkeen luvuissa 3.2 ja 3.3 esittelemme muutaman monoidin ominaisuuden, alimonoidin ja transformaatiomonoidin.

Luvussa 4 siirrymme monoidin sovelluksiin. Määrittelemme ensin luvussa 4.1 generoidun monoidin, jonka jälkeen luvussa 4.2 vapaan generoidun monoidin, joka voidaan johtaa suoraan generoidusta monoidista. Vapaa generoitu monoidi on ehkä monoidin mielenkiintoisin sovellus, ja sillä saadaan sovellettua monoidia muun muassa ohjelmointiin sekä kirjoitettuun kieleen.

Lopuksi määrittelemme vielä luvussa 5 monoideille morfismin ja isomorfismin sekä esittelemme muutamia lauseita näitä määritelmiä hyödyntäen.

Oletamme, että lukijalla on perustiedot joukko-opista. Päälähteenä käytämme Gilbertin ja Nicholsonin teosta *Modern Algebra with Applications*. Lisäksi käytämme lähdekirjoina Häsän ja Rämön teosta *Johdatus abstraktiin algebraan* sekä Kolmanin ja Busbyn teosta *Discrete Mathematical Structures in Computer Science*.

2 Esitiedot

2.1 Käsitteistä ja merkinnöistä

Tässä muutama huomautus tekstissä käyttämistämme käsitteistä ja merkinnöistä.

Merkitsemme usein määritelmissä laskutoimitusta merkillä $\star$, tällä tarkoitamme mitä tahansa laskutoimitusta. Kutsumme sen tulosta sanalla *tulo*. Tällä ei ole aina välttämättä mitään tekemistä kertolaskun tulon kanssa.

Kun liitämme laskutoimituksen johonkin joukkoon, käytämme merkintää $(\mathbb{Z}, \cdot)$, missä ensimmäisenä sulkeissa on jokin joukko ja toisena joukkoon yhdistetty laskutoimitus. Tämä esimerkkimerkintä siis tarkoittaa kokonaislukujen joukkoa varustettuna kertolaskulla.

2.2 Laskutoimitusten ominaisuuksista

Tässä luvussa palautamme mieleen muutaman laskutoimituksiin liittyvän ominaisuuden, joita tarvitsemme monoidin käsitteen ymmärtämiseen. Määrittelemme laskutoimitusten liitännäisyyden, vaihdannaisuuden sekä neutraalialkion.

Määritelmä 2.1. Olkoon S mikä tahansa joukko ja olkoot x ja y joukon S mitkä tahansa kaksi alkiota. Laskutoimitus $\star$ on *määritelty joukossa* S, jos tulo $x \star y$ kuuluu joukkoon S.

(Ks. [2, s. 31])

Määritelmä 2.2. Olkoon S mikä tahansa joukko ja olkoot x, y ja z joukon S mitkä tahansa kolme alkiota. Joukon S laskutoimitus $\star$ on *liitännäinen* joukossa S, jos seuraava ehto pätee:

1. $x \star (y \star z) = (x \star y) \star z$.

(Ks. [2, s. 33])

Käytännössä liitännäisyys tarkoittaa sitä, että voimme poistaa lausekkeesta sulut ilman, että tulo muuttuu. Esimerkiksi yhteen- ja kertolasku ovat liitännäisiä kokonaislukujen joukossa. Sen sijaan vähennyslasku ei ole kokonaislukujen joukossa liitännäinen.

Määritelmä 2.3. Olkoon S mikä tahansa joukko ja olkoot x ja y joukon S mitkä tahansa kaksi alkiota. Joukon S laskutoimitus $\star$ on *vaihdannainen* joukossa S, jos seuraava ehto pätee:

1. $x \star y = y \star x$.

(Ks. [2, s. 33])

Käytännössä vaihdannaisuus tarkoittaa sitä, että voimme vaihtaa kahden alkion paikkaa keskenään lausekkeessa ilman, että tulo muuttuu. Esimerkiksi yhteen- ja kertolasku ovat vaihdannaisia kokonaislukujen joukossa, mutta vähennyslasku ei.

Määritelmä 2.4. Olkoon S mikä tahansa joukko ja olkoon x joukon S mikä tahansa alkio. Joukon S alkio e on joukon S *neutraalialkio* laskutoimituksen $\star$ suhteen, jos seuraavat ehdot pätevät:

1. $e \star x = x$,

2. $x \star e = x$.

(Ks. [2, s. 35])

Käytännössä tällä tarkoitetaan sitä, että kun neutraalialkiolle ja mille tahansa muulle joukon alkiolle suoritetaan laskutoimitus, toinen alkio pysyy muuttumattomana. Esimerkiksi kokonaislukujen yhteenlaskun neutraalialkio on luku 0 ja kertolaskun luku 1.

Yllä esiteltyjen ominaisuuksien sekä *käänteisalkion* (ks. esim. [2, s. 36]) avulla saisimme määriteltyä myös erään toisen algebrallisen struktuurin, *ryhmän* (ks. esim. [2, s. 42]). Ryhmällä ja monoidilla on paljon hyvin samankaltaisia ominaisuuksia. Kaikki ryhmät ovat myös monoideja, kuten tulemme luvussa 3.1 huomaamaan.

2.3 Kuvauksista

Tässä luvussa esittelemme muutamia kuvauksiin liittyviä ominaisuuksia, joita tarvitsemme myöhemmin monoidin sovelluksissa. Kuvauksella tarkoitamme tässä funktiota joltain joukolta toiselle.

Määritelmä 2.5. Olkoot A ja B mitkä tahansa kaksi joukkoa. Kuvaus $f\colon A \to B$ on *injektio*, jos kullekin maalijoukon B alkiolle kuvautuu korkeintaan yksi lähtöjoukon A alkio.

(Ks. [2, s. 23])

Määritelmä 2.6. Olkoot A ja B mitkä tahansa kaksi joukkoa. Kuvaus $f\colon A \to B$ on *surjektio*, jos jokaiselle maalijoukon B alkiolle kuvautuu vähintään yksi lähtöjoukon A alkio.

(Ks. [2, s. 23])

Määritelmä 2.7. Olkoot A ja B mitkä tahansa kaksi joukkoa. Kuvaus $f\colon A \to B$ on *bijektio*, jos se on sekä injektio että surjektio. Tällöin jokaiselle maalijoukon B alkiolle kuvautuu tasan yksi lähtöjoukon A alkio.

(Ks. [2, s. 23])

Määritelmä 2.8. Olkoot A, B ja C mitkä tahansa kolme joukkoa ja olkoot $f\colon A \to B$ sekä $g\colon B \to C$ kuvauksia. Olkoon a mikä tahansa joukon A alkio. *Yhdistetty kuvaus* $g \circ f\colon A \to C$ määritellään seuraavalla ehdolla:

1. $(g \circ f)(a) = g(f(a))$.

(Ks. [2, s. 24])

Käyttäessämme yhdistettyä kuvausta on muistettava huomioida, että ensimmäisen kuvauksen maalijoukon ja toisen kuvauksen lähtöjoukon on oltava samat. Muuten määritelmä ei toimi.

Lause 2.9. *Olkoon $f\colon A \to B$ mikä tahansa kuvaus. Tällöin*

1. *on olemassa kuvaus $f^{-1}\colon B \to A$, jos ja vain jos kuvaus f on bijektio,*

2. *kuvaus f^{-1} on bijektio.*

Todistus. (vrt. [3, s. 161])

1. Todistamme yhtäpitävän lauseen "f^{-1} ei ole kuvaus, jos ja vain jos kuvaus f ei ole bijektio".

Oletamme ensin, että f^{-1} ei ole kuvaus. Tällöin jollain alkiolla $b \in B$ on olemassa kuva $f^{-1}(b)$ siten, että tuloksia on vähintään kaksi, olkoot nämä a_1 ja $a_2 \in A$. Siis $f(a_1) = b = f(a_2)$, joten kuvaus f ei ole tässä tapauksessa bijektio. Toinen vaihtoehto on, että on olemassa alkio $b' \in B$, jolla $f^{-1}(b')$ ei ole olemassa. Silloin kuvaus f ei ole surjektio eli se ei myöskään ole bijektio.

Teemme saman toiseen suuntaan. Oletamme, että kuvaus f ei ole bijektio. Silloin f ei ole injektio tai se ei ole surjektio. Tarkastelemme ensin tapausta, jossa kuvaus f ei ole injektio. Tällöin $f(a_1) = f(a_2) = b$ kahdella alkiolla a_1 ja $a_2 \in A$. Tällöin $f^{-1}(b)$ sisältää sekä tulosvaihtoehdon a_1 että a_2, joten f^{-1} ei ole kuvaus. Tarkastelemme

vielä tapausta, jossa kuvaus f ei ole surjektio. Tällöin on olemassa alkio $b' \in B$ jolle ei ole olemassa alkiota a joukossa A, jolle pätisi $f(a) = b'$. Tällöin, koska alkiolta b' ei kuvaudu mitään joukkoon A, ei f^{-1} ole kuvaus.

Näin ollen alkuperäinen väittämä "$f^{-1} : B \to A$ on kuvaus jos ja vain jos kuvaus f on bijektio" on tosi.

2. Koska $(f^{-1})^{-1} = f$, niin kohdan i) todistus osoittaa, että f^{-1} on bijektio. □

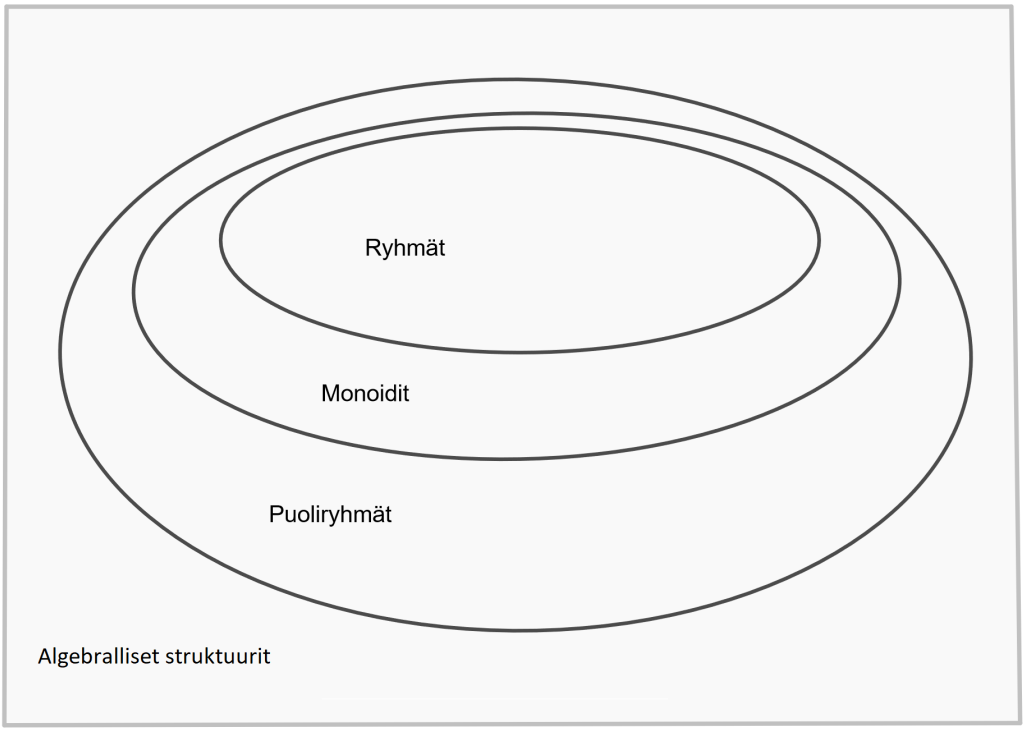
Huomautus. Lähdekirjassa esitetty lauseen 2.9 todistus on vajavainen eikä se todista lausetta. Todistuksesta puuttuu kokonaan maininta tapauksesta, jossa joukko B sisältää alkion, joka ei kuvaudu minnekään. Todistuksessa käsitellään vain tapausta, jossa joukon B alkiot kuvautuvat kahdelle eri alkiolle joukossa A. Todistusta on tässä täydennetty.

3 Monoidi

3.1 Monoidin määritelmä

Tässä luvussa esittelemme monoidin määritelmän sekä siihen liittyviä esimerkkejä. Esittelemme myös vaihdannaisen monoidin sekä todistamme neutraalialkion yksikäsitteisyyden.

Monoidi on algebrallinen struktuuri, jossa yhdistämme jonkin laskutoimituksen johonkin lukujoukkoon. Voimme laajentaa algebrallisten struktuurien joukkoa vielä *puoliryhmiin* ja ryhmiin, jonka mainitsimme jo aikaisemmin. Näitä struktuureita emme tässä tekstissä käsittele sen tarkemmin. Erilaiset struktuurit tekevät lukujoukkojen ja laskutoimitusten tarkastelusta laajempaa ja monipuolisempaa. Struktuurit menevät osittain myös päällekkäin (katso kuva 3.1). Kaikki monoidit ovat puoliryhmiä ja vastaavasti kaikki ryhmät ovat monoideja. Tämä ei kuitenkaan päde toiseen suuntaan, kaikki puoliryhmät eivät ole monoideja eivätkä kaikki monoidit ryhmiä. Struktuurien päällekkäisyyden vuoksi niillä on paljon samankaltaisia ominaisuuksia, kuten esimerkiksi *aliryhmä*, *alimonoidi* ja *alipuoliryhmä*.



Kuva 3.1. Algebralliset struktuurit.

Määritelmä 3.1. Olkoon M mikä tahansa joukko. Joukko M on laskutomituksen $\star$ suhteen *monoidi*, jos seuraavat ehdot pätevät:

1. laskutoimitus $\star$ on määritelty joukossa M,
2. laskutoimitus $\star$ on liitännäinen joukossa M,
3. joukossa M on olemassa neuraalialkio laskutoimituksen $\star$ suhteen.

(Ks. [1, s. 137])

Esimerkiksi kokonaislukujen joukko varustettuna kertolaskulla $(\mathbb{Z}, \cdot)$ on monoidi.

Esimerkki 3.2. Olkoon joukko $M = \{a, b\}$ ja olkoon laskutoimitus $\star$ määritelty seuraavanlaisesti:

$\star$	a	b
a	a	b
b	b	b

Osoita, että $(M, \star)$ on monoidi. (Ks. [3, s. 315, tehtävä 1b])

Ratkaisu. Laskutoimitus $\star$ on selvästi määritelty joukossa M, sillä tulot taulukossa ovat vain joukon M alkioita. Tarkastellaan seuraavaksi, onko laskutoimitus $\star$ on liitännäinen. Taulukon mukaan

$$a \star (b \star a) = a \star b = b,$$

$$(a \star b) \star a = b \star a = b.$$

Voimme todeta saman kaikissa muissakin tapauksissa eli laskutoimitus $\star$ on liitännäinen.

Näemme taulukosta suoraan, että neutraalialkio joukolle M laskutoimituksen $\star$ suhteen on alkio a, koska $a \star a = a$, $b \star a = b$ ja $a \star b = b$. Näin ollen voimme todeta, että $(M, \star)$ on monoidi. □

Määritelmä 3.3. Olkoon $(M, \star)$ monoidi. Tällöin $(M, \star)$ on *vaihdannainen monoidi*, jos laskutoimitus $\star$ on vaihdannainen joukossa M.

(Ks. [1, s. 137])

Esimerkiksi luonnolliset luvut yhteen- sekä kertolaskun suhteen ovat vaihdannaisia monoideja, koska ne ovat monoideja ja yhteen- ja kertolasku ovat vaihdannaisia luonnollisten lukujen joukossa.

Esimerkki 3.4. Osoita, että $(\mathbb{Z}, \star)$ on vaihdannainen monoidi, kun laskutoimitus $\star$ on määritelty seuraavasti, alkioiden x ja y ollessa joukon $\mathbb{Z}$ mitkä tahansa kaksi alkiota:

$$x \star y = x + y - xy.$$

(Ks. [3, s. 315, tehtävä 11])

Ratkaisu. Koska kokonaislukujen yhteen-, vähennys- ja kertolaskusta voi seurata vain kokonaislukuja, on laskutoimitus $\star$ määritelty joukossa $\mathbb{Z}$. Osoitamme seuraavaksi, että laskutoimitus $\star$ on liitännäinen:

$$\begin{aligned} x \star (y \star z) &= x \star (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - yz - xy - xy + xyz, \end{aligned}$$

$$\begin{aligned} (x \star y) \star z &= (x + y - xy) \star z \\ &= (x + y - xy) + z - z(x + y - xy) \\ &= x + y - xy + z - xz - yz + xyz \\ &= x \star (y \star z). \end{aligned}$$

Näin ollen voimme todeta laskutoimituksen $\star$ olevan liitännäinen joukossa $\mathbb{Z}$. Osoitamme vielä, että joukolle $\mathbb{Z}$ on olemassa neutraalialkion laskutoimituksen $\star$ suhteen. Oletamme, että $e \star x = x$. Tällöin pätevät seuraavat yhtälöt:

$$\begin{aligned} e + x - ex &= x, \\ e + x - x - ex &= 0, \\ e - ex &= 0, \\ e(1 - x) &= 0. \end{aligned}$$

Täten $e \star x = x \ \ \forall x \in \mathbb{Z}$ jos ja vain jos $e = 0$. Eli joukolla $\mathbb{Z}$ on neutraalialkio $e = 0$ laskutoimituksen $\star$ suhteen.

Nyt olemme osoittaneet, että $(\mathbb{Z}, \star)$ on monoidi. Seuraavaksi osoitamme vielä, että se on vaihdannainen monoidi. Osoitamme siis, että laskutoimitus $\star$ on vaihdannainen joukossa $\mathbb{Z}$. Koska tiedämme, että kokonaislukujen yhteen- ja kertolasku ovat vaihdannaisia, voimme todeta seuraavan:

$$x \star y = x + y - xy = x + y + (-1)(xy) = y + x + (-1)(yx) = y + x - yx = y \star x.$$

Siis laskutoimitus $\star$ on vaihdannainen joukossa $\mathbb{Z}$ ja siten $(\mathbb{Z}, \star)$ on vaihdannainen monoidi. □

Lause 3.5. *Olkoon $(M, \star)$ monoidi ja olkoon alkio e joukon M neutraalialkio laskutoimituksen $\star$ suhteen. Neutraalialkio e on yksikäsitteinen.*

Todistus (ks. [3, s. 308]). Todistamme lauseen käyttämällä vastaoletusta. Oletamme, että alkiot e_1 sekä e_2 ovat molemmat joukon M neutraalialkioita laskutoimituksen $\star$ suhteen. Nyt koska e_1 on neutraalialkio joukolle M, niin pätee $e_1 \star e_2 = e_2$. Ja koska e_2 on neutraalialkio joukolle M, niin pätee $e_1 \star e_2 = e_1$. Näin ollen $e_1 = e_2$ siis monoidin neutraalialkio on yksikäsitteinen. □

3.2 Alimonoidi

Määrittelemme tässä luvussa monoidille alimonoidin sekä esittelemme muutaman lauseen, joissa hyödynnämme alimonoidin määritelmää. Alimonoidin määritelmä on sovellettavissa samankaltaisena myös ryhmän aliryhmälle ja puoliryhmän alipuoliryhmälle.

Määritelmä 3.6. Olkoon $(M, \star)$ monoidi ja olkoon joukko S joukon M epätyhjä osajoukko. Joukko S varustettuna laskutoimituksella $\star$ on monoidin $(M, \star)$ *alimonoidi*, jos seuraavat ehdot pätevät:

1. laskutoimitus $\star$ on määritelty joukossa S,
2. joukon M neutraalialkio e kuuluu joukkoon S.

(Ks. [3, s. 309])

Esimerkiksi monoidi itse on itsensä alimonoidi. Samoin, jos joukko $S = \{e_M\}$, missä e_M on joukon M neutraalialkio ja $(M, \star)$ on monoidi, niin $(S, \star)$ on monoidin $(M, \star)$ alimonoidi. Alimonoidi on aina myös itsekin monoidi. (Ks. [3, s. 309])

Lause 3.7. *Olkoon $(M, \star)$ monoidi sekä olkoot $(S, \star)$ ja $(T, \star)$ sen alimonoideja. Leikkaus $S \cap T$ varustettuna laskutoimituksella $\star$, $(S \cap T, \star)$, on tällöin myös monoidin $(M, \star)$ alimonoidi.*

(Ks. [3, s. 315, tehtävä 18])

Todistus. Jotta $(S \cap T, \star)$ olisi monoidin $(M, \star)$ alimonoidi, on laskutoimituksen $\star$ oltava määritelty leikkauksessa $S \cap T$. Koska $(S, \star)$ ja $(T, \star)$ ovat monoidin $(M, \star)$ alimonoideja, on laskutoimitus $\star$ määritelty sekä joukossa S että joukossa T. Näin ollen pätee, että kun a ja b ovat mitä tahansa joukon S alkioita, myös tulo $a \star b \in S$. Sama pätee tietenkin myös joukolle T.

Koska leikkaus sisältää joukkojen yhteiset alkiot, voimme valita leikkauksesta $S \cap T$ mitkä tahansa kaksi alkiota x ja y, jolloin tulo $x \star y$ sisältyy sekä joukkoon S että joukkoon T. Näin ollen tulo sisältyy myös leikkaukseen $S \cap T$. Siis laskutoimitus $\star$ on määritelty leikkauksessa $S \cap T$.

Alimonoidin määritelmä vaatii myös neutraalialkion sisältymisen alimonoidiin. Olkoon alkio e joukon M neutraalialkio laskutoimituksen $\star$ suhteen. Koska $(S, \star)$ ja $(T, \star)$ ovat monoidin $(M, \star)$ alimonoideja, kuuluu neutraalialkio e niihin molempiin. Koska neutraalialkio e kuuluu sekä joukkoon S että joukkoon T, kuuluu se myös niiden leikkaukseen $S \cap T$.

Näin ollen $(S \cap T, \star)$ on monoidin $(M, \star)$ alimonoidi. □

Määrittelemme seuraavaa lausetta varten käsitteen *idempotentti*.

Määritelmä 3.8. Olkoon x joukon M alkio ja olkoon $(M, \star)$ monoidi. Alkio x on *idempotentti*, jos $x^2 = x \star x = x$.

(Ks. [3, s. 315, tehtävä 21])

Lause 3.9. *Olkoon $(M, \star)$ vaihdannainen monoidi (ks määritelmä 3.3). Olkoon X joukko, joka koostuu kaikista joukon M idempotenteista. Tällöin joukko X on monoidin M alimonoidi.*

(Ks. [3, s. 315, tehtävä 21])

Todistus. Olkoot a ja b joukon X alkioita. Tällöin $a = a \star a$ ja $b = b \star b$. Tästä seuraa seuraava yhtälö: $a \star b = (a \star a) \star (b \star b)$. Koska monoidin määritelmän mukaan laskutoimitus $\star$ on liitännäinen, pätee seuraava: $a \star b = a \star a \star b \star b$. Ja koska $(M, \star)$ on vaihdannainen monoidi, pätee seuraava:

$$a \star b = a \star b \star a \star b \ = (a \star b) \star (a \star b) = (a \star b)^2.$$

Siis kun alkiot a ja b ovat idempotentteja, myös $a \star b$ on idempotentti eli kuuluu joukkoon X. Seuraavaksi, olkoon e joukon M neutraalialkio. Neutraalialkio itsessään on idempotentti, koska $e \star e = e$ niin $e \in X$. Näin ollen joukko X on joukon M alimonoidi. □

3.3 Transformaatiomonoidi

Tässä luvussa käsittelemme erästä lausetta liittyen monoidin määritelmään ja sen todistusta. Transformaatiolla tarkoitamme tässä yhteydessä jotain kuvausta joukolta itseensä. Tämä kuvaus ei välttämättä ole bijektio. Käytämme tässä luvussa aiemmin määrittelemäämme yhdistettyä kuvausta (ks. määritelmä 2.8).

Lause 3.10. *Olkoon M mikä tahansa joukko ja olkoon $M^M = \{f : M \to M\}$ joukko, joka sisältää kaikki kuvaukset joukolta M itseensä. Tällöin $(M^M, \circ)$ on monoidi, jota kutsumme transformaatiomonoidiksi.*

Todistus (ks. [1, s. 138]). Olkoot f ja g joukon M^M mitkä tahansa kaksi kuvausta. Tällöin myös yhdistetty kuvaus $f \circ g$ kuuluu joukkoon M^M. Yhdistetty kuvaus $\circ$ on aina liitännäinen, koska jos $f, g, h, \in M^M$, niin

$$(f \circ (g \circ h))(x) = f(g(h(x))) \text{ ja}$$
$$((f \circ g) \circ h)(x) = f(g(h(x))) \quad \forall a \in M.$$

Neutraalialkio yhdistetylle kuvaukselle $\circ$ on kuvaus $1_M : M \to M$, missä $1_M(x) = x$. Täten $(M^M, \circ)$ on monoidi. □

Esimerkki 3.11. Olkoon joukko $X = \{0, 1\}$. Esitä transformaatiomonoidin $(X^X, \circ)$ laskutoimitustaulu.

Ratkaisu. Joukko X^X sisältää neljä alkiota: e, f, g ja h. Määrittelemme ne seuraavanlaisesti:

$$e(0) = 0, \quad f(0) = 0, \quad g(0) = 1, \quad h(0) = 1,$$
$$e(1) = 1, \quad f(1) = 0, \quad g(1) = 0, \quad h(1) = 1.$$

Nyt esimerkiksi yhdistetty kuvaus $(f \circ h)(0) = f(h(0)) = f(1) = 0$. Samoin $(f \circ h)(1) = f(h(1)) = f(1) = 0$. Näin ollen $f \circ h = f$. Samalla tavalla voimme laskea muutkin yhdistetyt kuvaukset ja saamme muodostettua seuraavanlaisen laskutoimitustaulun muunnosmonoidille $(X^X, \circ)$.

$\circ$	e	f	g	h
e	e	f	g	h
f	f	f	f	f
g	g	h	e	f
h	h	h	h	h

(Ks. [1, s. 138]). □

Itse asiassa jokainen monoidi voidaan esittää transformaatiomonoidina Cayleyn esityslauseen avulla. Emme tässä pureudu esityslauseeseen sen tarkemmin, mutta sen perusidea on, että jokainen ryhmä on isomorfinen erään symmetrisen ryhmän aliryhmän kanssa. Voimme soveltaa tätä myös monoideille. (Ks. [1, s. 71 & s. 138])

Monoidien tapauksessa transformaatiomonoidi vastaa ryhmän symmetristä ryhmää, koska symmetrinen ryhmä sisältää kaikki kuvaukset kyseisen ryhmän lukujoukolta itseensä. Tämä siis tarkoittaa sitä, että monoidi $(M, \star)$ on isomorfinen (ks. luku 5) transformaatiomonoidin $(M^M, \circ)$ kanssa. Voimme siis esittää monoidin $(M, \star)$ transformaatiomonoidina $(M^M, \circ)$ siten, että muodostamme joukolle M kaikki mahdolliset kuvaukset joukolta M itseensä.

Esimerkiksi monoidi $(\mathbb{Z}, \cdot)$ on Cayleyn esityslauseen perusteella isomorfinen transformaatiomonoidin $(\mathbb{Z}^{\mathbb{Z}}, \circ)$ kanssa, missä joukko $\mathbb{Z}^{\mathbb{Z}}$ sisältää kaikki kuvaukset juokolta $\mathbb{Z}$ itseensä. Esimerkin 3.11 tapaan voisimme muodostaa transformaatiomonoidille laskutoimitustaulun, joka esittäisi kaikki yhdistetyt kuvaukset kaikista joukon $\mathbb{Z}$ transformaatioista.

4 Generoidut monoidit

4.1 Generoitu monoidi

Tässä luvussa perehdymme generoituun monoidiin, jonka määritelmä auttaa meitä ymmärtämään seuraavassa luvussa 4.2 käsiteltävän vapaan generoidun monoidin määritelmän.

Koska monoidin laskutoimitus $\star$ on liitännäinen (ks. määritelmä 3.1), voimme jättää sulut kirjoittamatta. Voimme siis kirjoittaa esimerkiksi seuraavanlaisesti:

$$x \star (y \star z) = x \star y \star z.$$

Tästä seuraa, että missä tahansa monoidissa $(M, \star)$, neutraalialkion ollessa $e \in M$, minkä tahansa alkion $a \in M$ potenssit voidaan kirjoittaa seuraavanlaisesti:

$$a^0 = e, \quad a^1 = a, \quad a^2 = a\star a, \quad a^3 = a\star a\star a = a\star a^2, \ldots, \quad a^n = a\star a^{n-1} \quad \forall\, n \in \mathbb{N}.$$

(Ks. [1, s. 139])

Määritelmä 4.1. Olkoon $(M, \star)$ mikä tahansa monoidi ja olkoon m joukon M mikä tahansa alkio. Olkoon joukko A joukon M jokin osajoukko, eli $A \subset M$. Monoidi $(M, \star)$ on *generoitu osajoukolla* A, jos seuraava ehto pätee:

1. $m = a_1^{r_1} \star a_2^{r_2}\star, \cdots, \star a_n^{r_n}$ joillain $a_1, a_2, \ldots, a_n \in A$.

(Ks. [1, s. 139])

Käytännössä määritelmä tarkoittaa sitä, että jokainen joukon M alkio m voidaan kirjoittaa osajoukon A alkioiden tulona.

Esimerkiksi monoidi $(\mathbb{Z}_+, \cdot)$ on generoitu kaikilla alkuluvuilla.

Myös monoidi $(\mathbb{N}, +)$, eli luonnollisten lukujen joukko varustettuna yhteenlaskulla, on generoitu, tosin vain yhdellä alkiolla, luvulla 1. Jokainen alkio joukossa $\mathbb{N}$ voidaan kirjoittaa n kokoisena summana lukuja 1, $n \in \mathbb{N}$. Esimerkiksi luku $4 \in \mathbb{N}$ voidaan kirjoittaa muodossa $1 + 1 + 1 + 1 = 4$. Tässä tapauksessa osajoukko, jolla monoidi $(\mathbb{N}, +)$ on generoitu, on joukko $A = \{1\}$.

Tällainen yhdellä alkiolla generoitu monoidi on niin kutsuttu *syklinen monoidi*. Esimerkiksi monoidi $(\mathbb{Z}, +)$ ei ole syklinen, sillä se tarvitsee generointiin kaksi alkiota, luvut -1 ja 1.

(Ks. [1, s. 139])

Määritelmä 4.2. Monoidi $(M, \star)$ on *syklinen monoidi*, jos se on generoitu jollain joukon M osajoukolla A ja joukko A sisältää vain yhden alkion.

(Ks. [1, s. 139])

4.2 Vapaa generoitu monoidi

Monoideja esiintyy välillä jopa hieman yllättävissä paikoissa. Esimerkiksi kirjoitettu kieli voidaan luokitella eräänlaiseksi monoidiksi, tällöin kyseessä on *vapaa generoitu monoidi*. Joukkona on tässä tapauksessa aakkosten joukko ja laskutoimituksena *konkatenaatio*. Konkatenaatiolla tarkoitamme kahden merkkijonon kirjoittamista peräkkäin yhteen. Merkitsemme tässä luvussa konkatenaatiota merkillä $\bullet$, erottaaksemme sen tuntemattomasta laskuoperaatiosta $\star$. Näin ollen esimerkiksi lu $\bullet$ ku = luku. (Ks. [1, s. 140])

Tässä luvussa esittelemme ensin yhden apulauseen, jonka avulla määrittelemme vapaan generoidun monoidin. Sen jälkeen esittelemme muutaman esimerkin vapaan generoidun monoidin sovelluksista.

Määrittelemme seuraavanlaisesti. Olkoon A jokin joukko ja olkoon A^n joukko joukon A alkioiden kaikista n-pituisista konkatenaatioista. Näin ollen, jos $A = \{a, b\}$, niin $A^2 = \{aa, ab, ba, bb\}$. Määrittelemme tyhjän joukon $A^0 = \{\lambda\}$, missä λ tarkoittaa 0-mittaista sanaa..

Olkoon A^* joukko kaikista konkatenaatioista joukosta A:

$$A^* = A^0 \cup A^1 (= A) \cup A^2 \cup A^3 \cup \cdots = \bigcup_{n=0}^{\infty} A^n.$$

Apulause 4.3. Edellä määritelty joukko A^* varustettuna konkatenaatiolla, eli $(A^*, \bullet)$, on monoidi.

Todistus (ks. [1, s. 140]). Kun suoritamme kahdelle merkkijonolle konkatenaation, ei voi syntyä kuin saman merkkijoukon alkioita, koska alkiot eivät konkatenaatiossa muutu. Siis konkatenaatio on määritelty joukossa A^*. Konkatenaatio on myös liitännäinen:

$$\begin{aligned} &s \bullet (u \bullet t) = s \bullet ut = sut, \\ &(s \bullet u) \bullet t = su \bullet t = sut = s \bullet (u \bullet t) \quad \forall s, u, t \in A^*. \end{aligned}$$

Neutraalialkio on tyhjä sana λ, koska $s \bullet \lambda = s$ ja $\lambda \bullet \ s = s \quad \forall s \in A^*$ □

Määritelmä 4.4. Olkoon A^* joukko kaikista konkatenaatioista joukosta A, kuten edellä määriteltiin. Monoidi $(A^*, \bullet)$ on *vapaa generoitu monoidi*. Vapaan generoidun monoidin alkioita kutsumme *sanoiksi*.

(Ks. [1, s. 140])

Jos joukko A koostuu vain yhdestä alkiosta a, niin joukko $A^* = \{\lambda, a, aa, aaa, \ldots\}$. Tällöin esimerkiksi $aa \bullet aaa = aaaaa$. Tämä vapaa generoitu monoidi $(A^*, \bullet)$ on vaihdannainen.

Kuten jo luvun alussa totesimme, saamme myös kirjoitetusta kielestä monoidin. Tähän mennessä olemme kuitenkin käsitelleet vain yksittäisiä sanoja. Kun lisäämme joukkoon A myös välilyönnin (merkitsemme tässä $\square$) ja pisteen sekä isot kirjaimet, saamme muodostettua lauseita. Nyt siis joukko $A = \{A, B, C, \ldots, a, b, c, \ldots, \square, .)\}$ ja $(A^*, \bullet)$ on vapaa generoitu monoidi. Tällöin esimerkiksi sana $Monoidi \in A^*$. Voimme yhdistellä sanoja konkatenaation avulla käyttäen välilyöntiä $\square$ sanojen välissä. Esimerkiksi $Monoidi \bullet t\square ov \bullet at\square ki \bullet voja. = Monoidit\square ovat\square kivoja$. On kuitenkin huomattava, että joukko A^* sisältää aivan kaikki mahdolliset yhdistelmät joukon A alkioista. Siis myös ne sanat, jotka eivät tarkoita mitään, esimerkiksi $ghjns \in A^*$.

Tietokone saa informaation lukuina 0 ja 1 sekä niistä muodostuvista merkkijonoista. Nämä merkkijonot ovat konkatenaatioita ja siten joukon $\{0, 1\}$ voidaan katsoa generoivan vapaan monoidin konkatenaation suhteen. Tällöin $A^* = \{\lambda,\ 0,\ 1,\ 00,\ 01,\ 10,\ 11,\ 000,\ 001, \ldots\}$. Esimerkiksi $0111 \bullet 01001 = 011101001$ ja $01001 \bullet 0111 = 010010111$. Voimme tämän perusteella todeta, että A^* ei ole kuitenkaan vaihdannainen.

Edellisten esimerkkien perusteella on helppo todeta, että kun a on n-pituinen merkkijono ja b on m-pituinen merkkijono, $a \bullet b$ on $n + m$-pituinen merkkijono.

(Ks. [1, s. 140])

5 Monoidin isomorfismi

Tässä luvussa määrittelemme isomorfismin käsitteen monoideille. Sitä ennen määrittelemme kuitenkin monoidin morfismin.

Käytämme tässä luvussa laskutoimituksille merkintää $\star'$ merkinnän $\star$ lisäksi, jotta erottaisimme eri monoidien laskutoimitukset toisistaan. Laskutoimitus $\star'$ ei välttämättä liity mitenkään laskutoimitukseen $\star$.

Määritelmä 5.1. Olkoot $(M, \star)$ ja $(S, \star')$ kaksi mitä tahansa monoidia. Olkoot e_M ja e_S niiden neutraalialkiot. Kuvaus $f\colon M \to S$ on *morfismi* monoidista $(M, \star)$ monoidiin $(S, \star')$, jos seuraavat ehdot pätevät:

1. $f(x \star y) = f(x) \star' f(y) \quad \forall x, y \in M$,
2. $f(e_M) = e_S$.

(Ks. [1, s. 141])

Esimerkiksi, olkoon kuvaus $f\colon (\mathbb{N}, +) \to (\mathbb{Z}_+, \cdot)$ sellainen, että $f(n) = n^2$. Tämä kuvaus on morfismi, sillä $f(n+m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m) \quad \forall m, n \in \mathbb{N}$.

Kuvaus $f\colon (\mathbb{N}, +) \to (\mathbb{N}, +)$, $f(x) = x^2$ ei sen sijaan ole morfismi, sillä $f(x+y) = (x+y)^2$, kun taas $f(x)+f(y) = x^2+y^2$. Siis esimerkiksi $f(1+1) = 4$ ja $f(1)+f(1) = 2$.

(Ks. [1, s. 141])

Määritelmä 5.2. Olkoot $(M, \star)$ ja $(S, \star')$ kaksi mitä tahansa monoidia. Näiden välillä on *isomorfismi* eli $(M, \star) \cong (S, \star')$, jos seuraavat ehdot pätevät:

1. Monoidien $(M, \star)$ ja $(S, \star')$ välillä on morfismi,
2. Kuvaus $f : M \to S$ on bijektio.

(Ks. [1, s. 141])

Esimerkki 5.3. Olkoot joukot $M = \{a, b, c\}$ ja $S = \{x, y, z\}$. Olkoot $(M, \star)$ ja $(S, \star')$ monoideja, kun laskutoimitukset $\star$ ja $\star'$ on määritelty seuraavasti:

$\star$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\star'$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

Olkoon kuvaus f määritelty seuraavasti: $f(a) = y, f(b) = x, f(c) = z$. Kun sijoitamme kuvauksen f tauluun $\star$, saamme taulun $\star'$. Saamme seuraavat tulot:

$$f(a \star a) = f(a) = y = y \star' y = f(a) \star' f(a),$$
$$f(a \star b) = f(b) = x = y \star' x = f(a) \star' f(b),$$
$$f(b \star b) = f(c) = z = x \star' x = f(b) \star' f(b) \text{ ja niin edelleen.}$$

Näin ollen monoidit $(M, \star)$ ja $(S, \star')$ ovat isomorfisia keskenään eli $(M, \star) \cong (S, \star')$. (Ks. [3, s. 312])

Lause 5.4. *Olkoot $(M, \star)$ ja $(S, \star')$ monoideja ja olkoot niiden neutraalialkiot e_M ja e_S. Olkoon kuvaus $f : M \to S$ isomorfismi eli $(M, \star) \cong (S, \star')$. Tällöin $f(e_M) = e_S$.*

Todistus (ks. [3, s. 312])*.* Koska kuvaus f on isomorfismi, se on bijektio ja silloin myös surjektio. Tällöin, kun b on mikä tahansa joukon S alkio, sille on olemassa kuva $f(a) = b$, jollain $a \in M$. Nyt voimme kirjoittaa seuraavanlaisesti: $a = a \star e_M$ ja $b = f(a) = f(a \star e_M) = f(a) \star' f(e_M) = b \star' f(e_M)$. Samoin $a = e_M \star a$ ja $b = f(e_M) \star' b$. Näin ollen pätee seuraava: $b = b \star' f(e_M) = f(e_M) \star' b$ kaikilla $b \in S$. Siis $f(e_M)$ on joukon S neutraalialkio eli $f(e_M) = e_S$. □

Lause 5.5. *Olkoot $(M, \star)$ ja $(S, \star')$ monoideja ja olkoon kuvaus $f : M \to S$ isomorfismi. Tällöin on olemassa kuvaus f^{-1}, joka on isomorfismi.*

Todistus (vrt. [3, s. 310])*.* Koska isomorfismin määritelmän (5.2) mukaan f on bijektio, niin lauseen 2.9 mukaan on olemassa kuvaus $f^{-1} : S \to M$ siten, että kuvaus f^{-1} on bijektio. Olkoot alkiot x ja y joukon S mitkä tahansa kaksi alkiota. Koska kuvaus f on bijektio, se on myös surjektio, joten on olemassa sellaiset alkiot $a, b \in M$, joille pätee $f(a) = x$ sekä $f(b) = y$. Nyt $a = f^{-1}(x)$ ja $b = f^{-1}(y)$. Tällöin pätevät seuraavat yhtälöt:

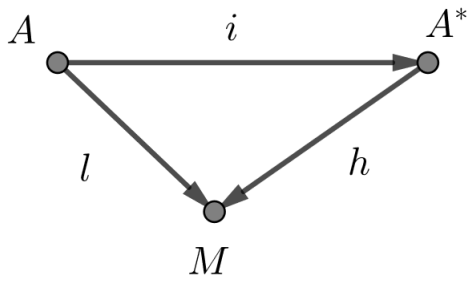
$$\begin{aligned} f^{-1}(x \star' y) &= f^{-1}(f(a) \star' f(b)), \\ &= f^{-1}(f(a \star b)), \\ &= (f^{-1} \circ f)(a \star b), \\ &= a \star b, \\ &= f^{-1}(x) \star f^{-1}(y). \end{aligned}$$

Näin ollen kuvaus f^{-1} on isomorfismi. □

Lause 5.6. *Olkoon* $(A^*, \bullet)$ *vapaa generoitu monoidi joukon A suhteen (ks määritelmä 4.4). Olkoon* $i\colon A \to A^*$ *kuvaus, joka kuvaa jokaisen joukon A alkion a sitä vastaavaan sanaan pituudeltaan* 1*, eli* $i(a) = a, \forall a \in A$*.*

Olkoon $(M, \star')$ *monoidi. Tällöin, jos* $l\colon A \to M$ *on jokin kuvaus, niin on olemassa morfismi* $h\colon (A^*, \bullet) \to (M, \star')$ *siten, että* $h \circ i = l$*.*

Tätä havainnollistamme kuvassa 5.1.



Kuva 5.1. Kuvaukset lauseessa 5.6

Todistus (ks. [1, s. 141])*.* Jotta h toteuttaisi yhdistetyn kuvauksen $h \circ i = l$ (ks. määritelmä 2.8), niin kuvauksen h on oltava määritelty 1-mittaisten sanojen joukossa siten, että $h(a) = l(a)$, koska $h \circ i(a) = h(i(a)) = h(a)$.

Olkoon a sana, jonka pituus on $n \geq 2$. Joukossa A^* kirjoitamme sanan a muodossa $b \bullet c$, missä sanan b pituus on $n - 1$ ja sanan c pituus 1. Tällöin pätee seuraava:

$$h(a) = h(b \bullet c) = h(b) \star' h(c) = h(b) \star' l(c).$$

Seuraavaksi voisimme määritellä vastaavasti kuvauksen h sanalle b ja niin edelleen, kunnes voimme kirjoittaa kuvauksen $h(a)$ kokonaan kuvauksen l avulla. Nyt jos kirjoitamme sanan $a = a_1 \bullet a_2 \bullet \cdots \bullet a_n$, missä $a_i \in A$, niin edellisen perusteella voimme kirjoittaa seuraavasti:

$$h(a) = l(a_1) \star' l(a_2) \star' \cdots \star' l(a_n).$$

Näin ollen morfismin määritelmän 5.1 ensimmäinen kohta pätee. Lisäksi on pädettävä seuraava: $h(e_{A^*}) = e_M$. Joukon A^* neutraalialkio on aiemmin määrittelemämme λ. Koska $h(\lambda) \star' h(a) = h(\lambda \bullet a) = h(a)$ ja $h(a) \star' h(\lambda) = h(a \bullet \lambda) = h(a)$ niin $h(\lambda) = e_M$. Näin ollen $h\colon (A^*, \bullet) \to (M, \star')$ on morfismi.

□

Lähteet

[1] Gilbert, William J. & Nicholson, W. Keith. *Modern Algebra with Applications*. Second Edition. New Jersey. John Wiley & Sons Inc. 2004.

[2] Häsä, Jokke & Rämö, Johanna. *Johdatus abstraktiin algebraan*. Helsinki. Gaudeamus, 2012.

[3] Kolman, Bernard & Busby, Robert C. *Discrete Mathematical Structures in Computer Science*. Second Edition. United States of America. Prentice-Hall International. 1987.