MAT–41150 Algebra 1(s)

Esko Turunen

8. maaliskuuta 2012

Esipuhe

Tämä luentokalvot sisältävät kurssin MAT–41150 Algebra 1(s) keskeiset asiat. Kalvoja täydennetään luennolla esimerkein ja todistuksin. Materiaali perustuu Jyväskylän, Helsingin ja Turun yliopistojen algebran peruskurssien materiaalille, mikä selittää joidenkin osien kummallisen numeroinnin. Kiitokset tekn. yo. Hanna–Kaisa Hurmeelle ja Matti Vaarmalle, jotka ovat koonneet kalvot antamastani käsikirjoituksesta. Kaikki kirjoitus- ym. virheet ovat kuitenkin allekirjoittaneen vastuulla.

Esko Turunen

Sana algebra tulee arabian kielestä (al-jabr), joka tarkoittaa uudelleenyhdistymistä.

- Algebran keksijänä pidetään persialaista Muhammed ibn-Musa al-Khwarizmia (n. 800-840).
- Algebra on geometrian ja analyysin ohella yksi matematiikan päähaaroista.
- Algebrassa tutkimuskohteina ovat laskutoimitusten yleiset ominaisuudet jossakin perusjoukossa, jossa ne on määritelty. Tällaisia laskutoimituksia voivat olla esimerkiksi yhteen- ja kertolasku. Laskutoimitusten määritteleminen joukkoon tuottaa algebran perusrakenteet: ryhmän, renkaan ja kunnan. Esimerkiksi kokonaisluvut muodostavat ryhmän, rationaaliluvut ja reaaliluvut kunnan.

- Koulumatematiikassa algebra tarkoittaa kirjainlaskua, jossa perusjoukon muodostavat rationaali- tai reaaliluvut. Sen tuttuna käyttökohteena on muun muassa polynomin nollakohtien etsiminen ja algebrallisten yhtälöiden ratkaiseminen.
- Moderni algebra on laaja matematiikan alue, jolla tutkimus on ollut viime vuosikymmeninä vilkasta. Siinä perusjoukkona, jossa laskutoimitukset on määritelty, voi olla mikä tahansa joukko, jonka alkiot eivät siis välttämättä ole lukuja.
- Sovelluskohteita modernin algebran tutkimuksessa ovat muun muassa CD-levyjen virheidenkorjausalgoritmit, esimerkiksi CRC-menetelmä.
- Peruskursseilta tuttu lienee Boolen algebra, joka mm vastaa klassisen logiikan rakennetta.

Johdantoa

Epätyhjän joukon A binäärinen laskutoimitus on kuvaus

$$* : A \times A \mapsto A$$

eli sääntö, joka liittää kahteen joukon A alkioon a, a' joukon A alkion $a * a'$. Vastaavalla tavalla voidaan puhua unaarisesta laskutoimisuksesta tai n–paikkaisesta laskutoimituksesta.

Esimerkki (1.1)

(a) Luonnollisten lukujen yhteen– ja kertolasku ovat binäärisiä laskutoimituksia: $(m, n) \mapsto m + n$, $(m, n) \mapsto mn$.
(b) Joukon X kaikki osajoukot, mukaan lukien tyhjä joukko $\emptyset$, muodostavat X:n potenssijoukon $\mathscr{P}(X) = \{A \subseteq X\}$.
Joukkojen leikkaus ja yhdiste ovat binäärisiä laskutoimituksia potenssijoukossa $\mathscr{P}(X) : (A, B) \mapsto A \cap B$, $(A, B) \mapsto A \cup B$.
Joukon A komplementti $\overline{A}$ on unaarinen operaattori $A \mapsto X \backslash A$

Esimerkki (1.1 jatkoa)

(c) Olkoon $X \neq \emptyset$ ja olkoon $\mathscr{F}(X) = \{f : X \mapsto X\}$ (kuvausten joukko). Kuvausten yhdistäminen on binäärinen laskutoimitus joukossa $\mathscr{F}(X) : (f, g) \mapsto f \circ g$.

(d) 2×2 – matriisien summa

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

on binäärinen laskutoimitus.

(e) 2×2 – matriisien kertolasku

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

on binäärinen laskutoimitus. Jatkossa keskitymme lähinnä binäärisiin laskutoimituksiin, joten jätämme sanan binäärinen pois.

Määritelmä (1.2)

Joukon A laskutoimitus $*$ on
(1) assosiatiivinen eli liitännäinen, jos
$a * (b * c) = (a * b) * c$ *aina, kun* $a,b,c \in A$.
(2) kommutatiivinen eli vaihdannainen, jos
$a * b = b * a$ *aina, kun* $a,b \in A$.

Joukon A laskutoimitus $*$ on vasemmalta distributiivinen laskutoimituksen $\oplus$ suhteen, jos $a * (b \oplus c) = (a * b) \oplus (a * c)$ *aina, kun* $a,b,c \in A$. *Se on oikealta distributiivinen laskutoimituksen $\oplus$ suhteen, jos* $(b \oplus c) * a = (b * a) \oplus (c * a)$ *aina, kun* $a,b,c \in A$. *Jos $*$ on oikealta ja vasemmalta distributiivinen laskutoimituksen $\oplus$ suhteen, se on distributiivinen laskutoimituksen $\oplus$ suhteen.*

Näitä lakeja kutsutaan osittelulaeiksi.

Merkintöjä $+$ ja $\cdot$ käytetään yleisesti eri laskutoimituksille. Merkintää $+$ käytetään kuitenkin ainoastaan kommutatiiviselle laskutoimitukselle. Usein kertolasku merkitään ilman pistettä eli $a \cdot b = ab$.

Esimerkki (1.3)

(a) Luonnollisten lukujen yhteen– ja kertolaskulle pätee
(1) $m + n = n + m$ *ja* $mn = nm$ *aina, kun* $m, n \in \mathbb{N}$ *(kommutatiivisuus).*
(2) $m + (n + l) = (m + n) + l$ *ja* $m(nl) = (mn)l$ *aina, kun* $m, n, l \in \mathbb{N}$ *(assosiatiivisuus).*
(3) $m(n + l) = mn + ml$ *aina, kun* $m, n, l \in \mathbb{N}$*, eli kertolasku on distributiivinen yhteenlaskun suhteen.*
(b) Joukon $\mathscr{P}(X)$ *laskutoimituket* $\cup$ *ja* $\cap$ *ovat kommutatiivisia:* $A \cap B = B \cap A$ *ja* $A \cup B = B \cup A$ *aina, kun* $A, B \in \mathscr{P}(X)$.

Esimerkki (1.3 jatkoa)

(c) joukon $\mathscr{F}(X)$ laskutoimitus $\circ$ on assosiatiivinen:
$f \circ (g \circ h) = (f \circ g) \circ h$ aina, kun $f, g, h \in \mathscr{F}(X)$
(d) 2×2 – matriisien yhteenlasku on kommutatiivinen ja assosiatiivinen, kertolasku ei ole kommutatiivinen, mutta on assosiatiivinen.

Määritelmä (1.4)

Olkoon $A \neq \emptyset$, ja olkoon $*$ joukon A laskutoimitus. Alkio $e \in A$ on laskutoimituksen $*$ neutraalialkio jos $e * g = g$ ja $g * e = g$ aina, kun $g \in A$. Alkio $\bar{x} \in A$ on alkion $x \in A$ vasen käänteisalkio, jos $\bar{x} * x = e$, ja oikea käänteisalkio, jos $x * \bar{x} = e$. Jos $\bar{x}$ on alkion x vasen ja oikea käänteisalkio, niin se on alkion x käänteisalkio.

Neutraalialkio on yksikäsitteinen ja tietyin edellytyksin myös alkion x käänteisalkio $\bar{x}$ on yksikäsitteinen.

Jos laskutoimituksesta käytetään tulomerkintää, niin neutraalialkiota merkitään usein 1:llä, ja summamerkintää käytettäessä 0:lla. Alkion x käänteisalkiota merkitään yleensä x^{-1}:llä, summamerkintää käytettäessä kuitenkin käytetään merkintää $-x$.

Esimerkki (1.5)

(a) Luku 0 on luonnollisten lukujen yhteenlaskun neutraalialkio. Luku 1 on luonnollisten lukujen kertolaskun neutraalialkio. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota kummankaan laskutoimituksen suhteen (poikkeukset ?)
(b) Identtinen kuvaus $id(x) = x$ on joukon $\mathscr{F}(X)$ laskutoimituksen $\circ$ neutraalialkio: $id \circ f = f = f \circ id$ aina, kun $f \in \mathscr{F}(X)$. Jos $f \in \mathscr{F}(X)$ on bijektio, sen käänteiskuvaus f^{-1} on kuvauksen f käänteisalkio laskutoimituksen $\circ$ suhteen: $f \circ f^{-1} = id = f^{-1} \circ f$. Muilla joukon $\mathscr{F}(X)$ alkioilla ei ole käänteisalkioita.

Esimerkki (1.5 jatkoa)

(c) Kun varustamme joukon $X \neq \emptyset$ potenssijoukon laskutoimituksella $\setminus$ (joukkojen erotus), niin jokaisella $A \in \mathscr{P}(X)$ pätee $A \setminus \emptyset = A$, joten $\emptyset$ muistuttaa laskutoimituksen $\setminus$ neutraalialkiota. Kuitenkin $\emptyset \setminus A = \emptyset$ aina, kun $A \in \mathscr{P}(X)$, joten $\emptyset$ ei ole laskutoimituksen $\setminus$ neutraalialkio. (Mieti, miksei neutraalialkiota joukossa $\mathscr{P}(X)$ tämän operaation suhteen ole.)
(d) 2×2–matriisien

$$\text{nolla–alkio on matriisi } \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ ja ykkösalkio } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Kaikilla 2×2-matriiseilla ei ole vasenta tai oikeaa käänteisalkiota matriisitulon suhteen, esim. ei ole lukuja a, b, c, d siten, että olisi

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ (totea!)}$$

Lause (1.6)

Olkoon $X \neq \emptyset$, ja olkoon $*$ joukon X laskutoimitus.
(1) Jos on olemassa alkiot $e \in X$ ja $e' \in X$ siten, että $e * g = g$ ja $g * e' = g$ aina, kun $g \in X$, niin $e = e'$ (joten erityisesti neutraalialkio on aina yksikäsitteinen).
(2) Jos $*$ on assosiatiivinen laskutoimitus, jolla on neutraalialkio e, niin
(a) alkiolla $g \in X$ on käänteisalkio, jos ja vain jos sillä on vasen ja oikea käänteisalkio.
(b) jos alkiolla g on käänteisalkio, se on yksikäsitteinen.
(c) jos alkiolla g on käänteisalkio, se on alkion g ainoa vasen (oikea) käänteisalkio.

Todistus.
(1) Harjoitustehtävänä 9.
(2) Todistamme kohdan (a): Jos alkiolla g on käänteisalkio g', niin määritelmän mukaan se on g:n vasen ja oikea käänteisalkio.

Todistus.
(1) Harjoitustehtävänä 9.
(2) Todistamme kohdan (a): Jos alkiolla g on käänteisalkio g', niin määritelmän mukaan se on g:n vasen ja oikea käänteisalkio.
Olkoon kääntäen g' alkion g vasen käänteisalkio, ja olkoon g'' sen oikea käänteisalkio. Tällöin

$$g'' = e * g'' = (g' * g) * g'' = g' * (g * g'') = g' * e = g'.$$

Siis g' on alkion g käänteisalkio. Kohdat (b) ja (c) seuraavat kohdasta (a). □

Tarkastelemme seuraavaksi uusien laskutoimitusten muodostamista tunnettujen laskutoimitusten avulla.

Jos $*$ on joukon A laskutoimitus, ja jos $B \subseteq A$, $B \neq \emptyset$ siten, että $b * b' \in B$ aina, kun $b, b' \in B$, niin $*$ määrittelee indusoidun laskutoimituksen $*|_B$ joukossa B: $b *|_B b' = b * b'$.

Tämä asiantila voidaan ilmaista myös sanomalla, että osajoukko $\emptyset \neq B \subseteq A$ on suljettu laskutoimituksen $*$ suhteen.

Yleensä indusoidulle laskutoimitukselle käytetään samaa merkintää kuin sen indusoimalle laskutoimitukselle $*$: $*|_B = *$.

Esimerkki (1.7)

Olkoon $M_2\mathbb{R}$ reaalisten 2×2-matriisien joukko. Olkoon

$$P = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2\mathbb{R} : c = 0 \right\}.$$

Tällöin kaikille $A, B \in P$ pätee $AB \in P$, joten matriisien kertolasku indusoi laskutoimituksen joukossa P. Sanomme myös, että $M_2\mathbb{R}$:n osajoukko P on suljettu matriisien kertolaskun suhteen.
Jos $*_A$ on laskutoimitus joukossa A ja $*_B$ on laskutoimitus joukossa B, niiden avulla voidaan määritellä laskutoimitus joukossa $A \times B$:

$$((a, b), (a', b')) \mapsto (a *_A a', a *_B b').$$

Tätä laskutoimitusta kutsutaan laskutoimitusten $*_A$ ja $*_B$ tuloksi.
Vastaavalla tavalla voidaan määritellä n–paikkaisia laskutoimituksia.

Esimerkki (1.8)

Luonnollisten lukujen yhteenlaskun avulla saadaan yhteenlasku joukkoon $\mathbb{N} \times \mathbb{N}$*:* $(m, n) + (p, q) = (m + p, n + q)$.

Palautamme mieliin tärkeän ekvivalenssirelaation käsitteen:

Määritelmä (1.9)

Relaatio joukossa A *on joukon* $A \times A$ *osajoukko. Jos* $R \subseteq A \times A$ *on relaatio, usein merkitään* $a\,R\,b \iff (a, b) \in R$ *(jolloin sanotaan, että alkio* a *on relaatiossa* R *alkion* b *kanssa).*
Joukon A *relaatio* R *on*

(1) refleksiivinen, jos $a\,R\,a$ *aina, kun* $a \in A$,
(2) symmetrinen, jos $b\,R\,a$ *aina, kun* $a\,R\,b$,
(3) transitiivinen, jos $a\,R\,c$ *aina, kun* $a\,R\,b$ *ja* $b\,R\,c$,
(4) antisymmetrinen, jos $b = a$ *aina, kun* $a, b \in A$ *ja* $a\,R\,b$ *sekä* $b\,R\,a$.

Määritelmä (1.9. jatkoa)

Jos relaatio on refleksiivinen, symmetrinen ja transitiivinen, se on ekvivalenssirelaatio. Ekvivalenssirelaation merkkinä käytetään usein merkkiä $\sim$; tällöin merkitään $a \sim b$. Jos $\sim$ on ekvivalenssirelaatio, niin jokainen joukon A alkio a määrää ekvivalenssiluokan

$$[a] = \{b \in A : a \sim b\}.$$

Ekvivalenssiluokkien joukkoa merkitään $A / \sim$, ja sitä kutsutaan ekvivalenssirelaatiota $\sim$ vastaavaksi A:n tekijäjoukoksi.

Esimerkki (tärkeä logiikassa)

Olkoon $\mathscr{L}$ logiikan lauseiden joukko. Asettamalla $\alpha \approx \beta$ joss $\vdash \alpha \Rightarrow \beta$ ja $\vdash \beta \Rightarrow \alpha$ saadaan ekvivalenssirelaatio.

Jos relaatio R on refleksiivinen, antisymmetrinen ja transitiivinen, se on osittainen järjestys.

Esimerkki

Relaatio "$\subseteq$" (osajoukko) on osittainen järjestys epätyhjän joukon X potenssijoukossa $\mathscr{P}(X)$. Täydellinen järjestys se ei kuitenkaan ole, ts. ei aina $A \subseteq B$ eikä $B \subseteq A$ $(A, B \in \mathscr{P}(X))$.

Määritelmä (1.10.)

Jos $*$ on laskutoimitus ja $\sim$ on ekvivalenssirelaatio joukossa A, ne ovat yhteensopivat, jos $a * b \sim a' * b'$ aina, kun $a \sim a'$ ja $b \sim b'$. Laskutoimitus $*$ määrää tekijälaskutoimituksen $*$ joukossa $A/\sim$ säännöllä $[a] * [b] = [a * b]$.

Loogiset konnektiivit $\wedge, \vee, \neg$ ovat yhteensopivia ekvivalenssirelaation $\approx$ suhteen. Jos esim. $\alpha \approx \beta$ ja $\gamma \approx \delta$, niin $\alpha \wedge \gamma \approx \beta \wedge \delta$.

Esimerkki (1.11)

Olkoon relaatio $\equiv$ *kokonaislukujen joukossa* $\mathbb{Z}$ *määritelty säännöllä* $a \equiv b$, *jos on olemassa* $k \in \mathbb{Z}$ *siten, että* $b = a + 3k$. *Tällöin* $\equiv$ *on ekvivalenssirelaatio:*

(1) $a = a + 3 \cdot 0$ *aina, kun* $a \in \mathbb{Z}$, *eli* $a \equiv a$ *aina, kun* $a \in \mathbb{Z}$.

Esimerkki (1.11)

Olkoon relaatio $\equiv$ *kokonaislukujen joukossa* $\mathbb{Z}$ *määritelty säännöllä* $a \equiv b$, *jos on olemassa* $k \in \mathbb{Z}$ *siten, että* $b = a + 3k$. *Tällöin* $\equiv$ *on ekvivalenssirelaatio:*

(1) $a = a + 3 \cdot 0$ *aina, kun* $a \in \mathbb{Z}$, *eli* $a \equiv a$ *aina, kun* $a \in \mathbb{Z}$.

(2) jos $b = a + 3k$ *jollain* $k \in \mathbb{Z}$, *niin* $a = b + 3 \cdot (-k)$, *siis ehdosta* $a \equiv b$ *seuraa aina ehto* $b \equiv a$.

Esimerkki (1.11)

Olkoon relaatio $\equiv$ kokonaislukujen joukossa $\mathbb{Z}$ määritelty säännöllä $a \equiv b$, jos on olemassa $k \in \mathbb{Z}$ siten, että $b = a + 3k$. Tällöin $\equiv$ on ekvivalenssirelaatio:

(1) $a = a + 3 \cdot 0$ aina, kun $a \in \mathbb{Z}$, eli $a \equiv a$ aina, kun $a \in \mathbb{Z}$.

(2) jos $b = a + 3k$ jollain $k \in \mathbb{Z}$, niin $a = b + 3 \cdot (-k)$, siis ehdosta $a \equiv b$ seuraa aina ehto $b \equiv a$.

(3) jos $b = a + 3k$ ja $c = b + 3n$ joillain $k, n \in \mathbb{Z}$, niin $c = a + 3(k + n)$, eli jos $a \equiv b$ ja $b \equiv c$, niin $a \equiv c$.

Esimerkki (1.11)

Olkoon relaatio $\equiv$ kokonaislukujen joukossa $\mathbb{Z}$ määritelty säännöllä $a \equiv b$, jos on olemassa $k \in \mathbb{Z}$ siten, että $b = a + 3k$. Tällöin $\equiv$ on ekvivalenssirelaatio:

(1) $a = a + 3 \cdot 0$ aina, kun $a \in \mathbb{Z}$, eli $a \equiv a$ aina, kun $a \in \mathbb{Z}$.

(2) jos $b = a + 3k$ jollain $k \in \mathbb{Z}$, niin $a = b + 3 \cdot (-k)$, siis ehdosta $a \equiv b$ seuraa aina ehto $b \equiv a$.

(3) jos $b = a + 3k$ ja $c = b + 3n$ joillain $k, n \in \mathbb{Z}$, niin $c = a + 3(k + n)$, eli jos $a \equiv b$ ja $b \equiv c$, niin $a \equiv c$.

Huomaa myös, että $a \equiv b$ joss $a - b$ on jaollinen luvulla 3.
Ekvivalenssirelaatiota $\equiv$ kutsutaan kongurenssiksi (modulo 3).
Yhteenlasku on yhteensopiva ekvivalenssirelaation $\equiv$ kanssa:
Jos $a' = a + 3m$ ja $b' = b + 3n$, niin

$$a' + b' = a + b + 3(m + n).$$

Siis kokonaislukujen yhteenlasku määrää laskutoimituksen kolmen alkion joukkoon

$$\mathbb{Z}/_{\equiv} = \{[0], [1], [2]\}.$$

(ekvivalenssiluokat modulo 3)

Lemma (1.12)

Jos $*$ on assosiatiivinen, sen tekijälaskutoimitus on assosiatiivinen. Jos $*$ on kommutatiivinen, myös sen tekijälaskutoimitus on kommutatiivinen.

Todistus. Jos $*$ on kommutatiivinen, niin

$$[a] * [b] = [a * b] = [b * a] = [b] * [a],$$

joten tekijälaskutoimitus on kommutatiivinen. Assosiatiivisuus todistetaan harjoitustehtävässä 12. □

Määritelmä (1.13)

Olkoot E ja E' joukkoja, joiden laskutoimitusta merkitään kertolaskulla. Kuvaus $h\colon E \mapsto E'$ on homomorfismi, jos $h(ab) = h(a)h(b)$ kaikille $a, b \in E$. Bijektiivinen homomorfismi on isomorfismi, ja isomorfismi joukolta E itselleen on automorfismi.

Esimerkki (1.14)

(1) Olkoot $*$ ja $\sim$ laskutoimitus ja ekvivalenssirelaatio joukossa E. Jos ne ovat yhteensopivat, niin luonnollinen kuvaus $\phi : E \mapsto E\ /\ \sim$, $\phi(a) = [a]$, on surjektiivinen homomorfismi. Tämä seuraa määritelmästä: kuvauksen surjektiivisuus on itsestään selvää ja lisäksi kaikille $a, b \in E$ pätee

$$\phi(a) * \phi(b) = [a] * [b] = [a * b] = \phi(a * b).$$

Siten luonnollinen kuvaus ϕ on homomorfismi.

Esimerkki (1.14 jatkoa)

(2) Kuvaus $h : \mathbb{Z} \mapsto M_2\mathbb{R}$,

$$h(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

on homomorfismi, kun kokonaisluvut varustetaan yhteenlaskulla ja $M_2\mathbb{R}$ *varustetaan matriisien kertolaskulla:*

$$h(n+m) = \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = h(n)h(m),$$