9. Algebrat

Monissa sovelluksissa törmätään moduleihin, joissa on modulirakenteen lisäksi määritelty sisäinen bilineaarinen kertolasku. Esimerkiksi matriiseja voidaan paitsi laskea yhteen ja kertoa luvuilla myös kertoa keskenään, ja matriisikertolasku on yhteensopiva sekä yhteenlaskun että skalaarikertolaskun kanssa. Tällaista rakennetta nimitetään algebraksi. Eri lähteissä algebran määritelmään saatetaan lisätä oletuksia kertolaskun ominaisuuksista: sen voidaan esimerkiksi vaatia olevan liitännäinen tai sillä voidaan olettaa olevan neutraalialkio. Tässä materiaalissa oletukset pidetään kuitenkin minimissään.

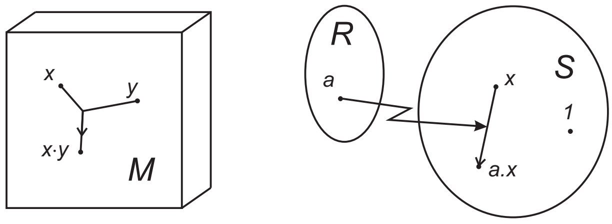
9.1. Perusominaisuudet.

Määritelmä 9.1. Olkoon R vaihdannainen rengas, ja olkoon A jokin R-moduli, jossa on määritelty R-bilineaarinen kertolasku $(x, y) \mapsto x \cdot y$ kaikilla $x, y \in A$. Tällöin modulia A nimitetään *R-algebraksi*. Jos kertolasku on liitännäinen tai vaihdannainen tai jos sillä on neutraalialkio, algebraa kutsutaan vastaavasti *liitännäiseksi*, *vaihdannaiseksi* tai *ykköselliseksi*.

Algebrassa on siis kolme laskutoimitusta: yhteenlasku, kertolasku ja skalaarikertolasku. Yhteenlasku on ryhmälaskutoimitus, osittelulait pätevät molemmille kertolaskuille, ja skalaarikertoimet menevät sisälle sekä summiin että tuloihin. Yleensä kertolaskua merkitään yksinkertaisesti xy jättämällä piste pois. Samoin skalaarikertolaskua voidaan merkitä $a.x = ax$. Jos skalaarikertolaskun ja algebran sisäisen kertolaskun sekoittuminen halutaan välttää, voidaan niille käyttää eri merkintöjä. Esimerkiksi seuraavat laskulait pätevät missä tahansa algebrassa:

$$
\begin{aligned}
(a+b)x &= ax + bx & a(x \cdot y) &= (ax) \cdot y = x \cdot (ay) \\
(x+y) \cdot z &= x \cdot z + y \cdot z & -(x \cdot y) &= (-x) \cdot y = x \cdot (-y) \\
a(x+y) &= ax + ay & 0_R.x &= 0_A \cdot x = x \cdot 0_A = 0_A \\
(-1).x &= -x. & &
\end{aligned}
$$

Liitännäisen ja ykkösellisen algebran kertolasku täyttää renkaan kertolaskun ehdot, joten tällaista algebraa voidaan pitää renkaana (ei välttämättä vaihdannaisena), jossa on lisäksi määritelty skalaarikertolasku. Toisaalta jokainen vaihdannainen rengas R on R-moduli oman sisäisen kertolaskunsa suhteen, ja vaihdannainen rengas R onkin liitännäinen, vaihdannainen ja ykkösellinen R-algebra.



Kuva 16. Algebra on moduli M, jossa on määritelty bilineaarinen kertolasku. Liitännäinen ja ykkösellinen algebra voidaan nähdä myös renkaana S, jossa on määritelty toisen renkaan skalaarikertolasku.

Esimerkkejä algebroista:

- Olkoon R rengas. R-kertoimisten neliömatriisien modulissa $R^{n\times n}$ voidaan määritellä tuttu matriisikertolasku, joka tekee kyseisestä modulista *matriisialgebran.*
- Polynomirenkaassa $R[X_1,\ldots,X_n]$ rengas R voidaan samastaa vakiopolynomien kanssa. Tällöin skalaarikertolasku voidaan määritellä samalla säännöllä kuin polynomikertolasku, jolloin polynomirenkaasta tulee *polynomialgebra.*
- Olkoon R mikä tahansa rengas, ei välttämättä vaihdannainen. Niin kuin ryhmien tapauksessa, R voidaan varustaa renkaan $\mathbb{Z}$ skalaarikertolaskulla $n.a = a+\cdots+a$ (n kertaa). Jokainen rengas on siis $\mathbb{Z}$-algebra. Kuten ryhmillä, tämä on ainoa tapa, jolla $\mathbb{Z}$ voi toimia renkaassa R, joten $\mathbb{Z}$-algebrojen teoria vastaa renkaiden teoriaa.
- Yleisemmin, jos R ja S ovat renkaita ja $f : R \to S$ on rengashomomorfismi, niin S voidaan varustaa skalaarikertolaskulla $a.b = f(a)\cdot b$. Tällöin renkaasta S tulee R-algebra.
- Jos K on kunta, jokainen K-algebra A on vektoriavaruus. Tällöin voidaan puhua muun muassa algebran *dimensiosta.* Jos vektoriavaruudessa on lisäksi määritelty ylimääräistä rakennetta, kuten normi tai topologia, voidaan vastaavasti puhua normillisista tai topologisista algebroista.
- Kompleksilukujen kunta $\mathbb{C}$ on vektoriavaruutena samastettavissa tason $\mathbb{R}^2$ kanssa. Kompleksilukujen kertolasku on yhteensopiva avaruuden $\mathbb{R}^2$ vektorilaskutoimitusten kanssa, joten $\mathbb{C}$ on kaksiulotteinen $\mathbb{R}$-algebra.
- Olkoon M jokin R-moduli. Modulin M sisäisten homomorfismien joukko $\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M)$ on R-algebra, jota kutsutaan M:n *endomorfismialgebraksi.*

Algebrojen ali- ja tekijästruktuurit sekä algebrojen väliset homomorfismit määritellään luonnollisella tavalla niin, että ne säilyttävät sekä modulirakenteen että algebran kertolaskun.

MÄÄRITELMÄ 9.2. R-algebran A alimoduli B on *R-alialgebra*, jos se on modulin A alimoduli ja toteuttaa ehdon

$$x\cdot y \in B \qquad \text{kaikilla } x,y\in B.$$

Alimodulia I kutsutaan *R-ideaaliksi*, jos

$$a\cdot x\in I \quad \text{ja} \quad x\cdot a \in I \qquad \text{kaikilla } a\in A \text{ ja } x\in I.$$

Algebran A ideaalin I suhteen voidaan muodostaa *tekijäalgebra A/I* kuten minkä tahansa modulin yhteydessä. Tekijäalgebran kertolasku toteuttaa kaavan $(a+I)\cdot(b+I) = ab+I$. Se, että tekijärankenteen kertolasku on hyvin määritelty, voidaan todistaa aivan samoin kuin renkaiden yhteydessä, koska siinä ei tarvita A:n kertolaskun liitännäisyyttä eikä ykkösalkiota.

MÄÄRITELMÄ 9.3. Olkoot A ja B kaksi R-algebraa. R-lineaarista kuvausta $\varphi : A\to B$ kutsutaan *R-algebrahomomorfismiksi*, jos

$$\varphi(x\cdot y) = \varphi(x)\cdot\varphi(y) \qquad \text{kaikilla } x,y\in A.$$

Jos A ja B ovat ykkösellisiä, kuvaukselta φ vaaditaan lisäksi, että $\varphi(1_A) = 1_B$.

Algebrahomomorfismin ydin on ideaali, ja algebrahomomorfismeille pätee samanlainen homomorfialause kuten moduleille yleensä.

9.2. Algebrojen kannat. Jos jokin R-algebra on R-modulina vapaa, sitä kutsutaan *vapaaksi algebraksi.* Vapaalla algebralla on siis kanta. Osoittautuu, että kannan alkioiden kertotaulu määrittää koko algebran kertolaskun täysin.

LAUSE 9.4. *Olkoon A vapaa R-algebra, jolla on kanta B.*

i) *Algebra A on liitännäinen, jos ja vain jos $(ab)c = a(bc)$ kaikilla kannan alkioilla $a, b, c \in B$.*
ii) *Algebralla A on ykkösalkio 1, jos ja vain jos $1 \cdot a = a$ kaikilla $a \in B$.*
iii) *Algebra A on vaihdannainen, jos ja vain jos $ab = ba$ kaikilla $a, b \in B$.*

TODISTUS. Tarkastellaan esimerkiksi kohtaa (iii) ja oletetaan, että kannan alkiot ovat keskenään vaihdannaisia. Olkoot $x, y \in A$ mielivaltaisia alkioita. Ne voidaan kirjoittaa kanta-alkioiden lineaarikombinaatioina muodossa $x = \sum_i x_i b_i$ ja $y = \sum_j y_j b_j$. Algebrakertolaskun bilineaarisuuden avulla saadaan

$$\begin{aligned} x \cdot y &= \sum_i x_i b_i \cdot \sum_j y_j b_j = \sum_i x_i \left(\sum_j y_j (b_i \cdot b_j) \right) = \sum_{i,j} x_i y_j (b_i \cdot b_j) \\ &= \sum_{i,j} x_i y_j (b_j \cdot b_i) = \sum_j y_j \left(\sum_i x_i (b_j \cdot b_i) \right) = \sum_j y_j b_j \cdot \sum_i x_i b_i = y \cdot x. \end{aligned}$$

Huomaa, että yllä käytetään hyväksi kerroinrenkaan vaihdannaisuutta. Muut väitteet todistetaan samalla tavalla. □

Olkoon A vapaa R-algebra, jolla on kanta B. Jokainen kannan alkioiden tulo $b_i \cdot b_j$ voidaan kirjoittaa kannan alkioiden lineaarikombinaationa muodossa

$$b_i \cdot b_j = \sum_k c_{ij}^k b_k.$$

Vakioita $c_{ij}^k \in R$ (tässä k on yläindeksi, ei potenssi) kutsutaan algebran *rakennevakioiksi kannan B suhteen.* Kertolaskun bilineaarisuudesta seuraa, että rakennevakioiden tunteminen riittää algebran kertolaskun tuntemiseksi, sillä

$$\sum_i x_i b_i \cdot \sum_j y_j b_j = \sum_{i,j} x_i y_j (b_i \cdot b_j) = \sum_{i,j,k} x_i y_j c_{ij}^k b_k.$$

Kaava antaa kannan alkioista muodostettujen lineaarikombinaatioiden tulon yleisessä tapauksessa. Kääntäen, rakennevakioiden perhe (c_{ij}^k) voidaan valita kullakin i ja j täysin mielivaltaisesti, ja yllä oleva kaava määrittelee tällöin erään bilineaarisen kertolaskun. Kiteytetään nämä havainnot seuraavaan lauseeseen.

LAUSE 9.5. *Olkoon M vapaa R-moduli, jolla on kanta $B = \{b_i\}_{i \in I}$. Olkoon lisäksi $(c_{ij}^k)_{k \in I}$ jokin äärelliskantajainen perhe renkaan R alkioita kaikilla $i, j \in I$. Tällöin modulissa M voidaan määritellä sellainen yksikäsitteinen R-bilineaarinen kertolasku, jonka rakennevakioiksi kannan B suhteen tulevat vakiot c_{ij}^k.*

ESIMERKKI 9.6. Tarkastellaan kaksiulotteista reaaliavaruutta $\mathbb{R}^2$. Merkitään tämän avaruuden luonnollisen kannan vektoreita $1 = (1, 0)$ ja $i = (0, 1)$, ja määritellään kantavektorien kertotaulu seuraavasti:

$\cdot$	1	i
1	1	i
i	i	-1

Tämä $\mathbb{R}$-algebra on selvästi ykkösellinen, liitännäinen ja vaihdannainen. Tällä tavoin määritellään *kompleksilukualgebra*, joka on siis kaksiulotteinen reaalikertoiminen algebra. Kompleksialgebran rakennevakiot on lueteltu alla olevassa taulukossa, missä on merkitty $c_{xy}^z = c_{xy}(z)$.

(x, y)	$(1, 1)$	$(1, i)$	$(i, 1)$	(i, i)
$c_{xy}(1)$	1	0	0	-1
$c_{xy}(i)$	0	1	1	0

Koska kompleksialgebra on vaihdannainen ja jokaisella nollasta poikkeavalla alkiolla on käänteisalkio, kyseessä on kunta.

ESIMERKKI 9.7. *Kvaterniot.* William Hamilton[14] löysi vuonna 1843 kertotaulun neliulotteiselle reaalikertoimiselle algebralle $\mathbb{H}$, jonka hän risti kvaternioiksi[15]. Erityistä kvaternioalgebrassa on se, että kaikilla alkioilla on käänteisalkiot, joten jakolasku on mahdollista. Hamilton oli työskennellyt kauan tietynlaisen kolmiulotteisen algebran löytämiseksi, kun hän ollessaan kävelyllä Dublinissa äkkiä tajusi saavansa ideansa toimimaan, jos lisäisi mukaan neljännen ulottuvuuden. Hän innoistui keksinnöstään niin, että kaiversi siltä seisomalta kvaterniokannan kertolaskusäännöt Broughamin sillan kiveykseen. Jos algebran kantaa merkitään symboleilla 1, i, j ja k, kertotaulu näyttää tältä:

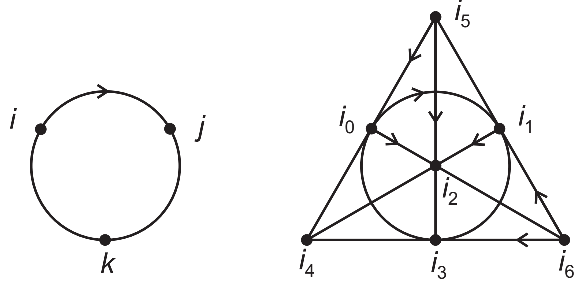
$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Kertotaulusta nähdään, että kvaternioalgebra on liitännäinen ja ykkösellinen. Lisäksi jokaisella nollasta poikkeavalla alkiolla on käänteisalkio: esimerkiksi $(1 + j) \cdot \frac{1}{2}(1 - j) = 1$. Kvaternioalgebra ei kuitenkaan ole vaihdannainen, joten se ei ole kunta. Sen sijaan sitä nimitetään *jakoalgebraksi* (vrt. jakorengas). Kuten kompleksialgebrassa, jokainen ykkösalkiosta poikkeava kanta-alkio on luvun -1 neliöjuuri. Kvaternioita käytettiin kolmiulotteisen reaaliavaruuden geometrian hahmottamiseen ennen vektoriavaruuden käsitteen muotoilua; kvaternioiden avulla voidaan muun muassa muotoilla piste- ja ristitulot sekä kolmiulotteisen avaruuden kierrot.

[14]William Rowan Hamilton, 1805–1865, irlantilainen fyysikko ja matemaatikko

[15]quaternio = nelikkö (lat.)

Normillinen algebra on sellainen, jonka taustalla olevassa vektoriavaruudessa voidaan määritellä kertolaskun kanssa yhteensopiva normi. (Esimerkiksi kompleksilukujen tavallinen normi on $|x + yi| = \sqrt{x^2 + y^2}$.) Voidaan osoittaa, että normillisia reaalisia jakoalgebroja on isomorfiaa vaille olemassa vain neljä: reaaliluvut $\mathbb{R}$, kompleksiluvut $\mathbb{C}$, kvaterniot $\mathbb{H}$ sekä *oktonioalgebra* $\mathbb{O}$, joka on kahdeksanulotteinen epäliitännäinen jakoalgebra. Jos oktonioalgebran kantaa merkitään $\{1, i_0, \ldots, i_6\}$, niin $\pm i_k$ on luvun -1 neliöjuuri jokaisella k.



Kuva 17. Kvaternioiden ja oktonioiden kertotaulut

Kvaternioiden ja oktonioiden kanta-alkioiden kertotaulut käyvät ilmi oheisesta kuvasta. Kahden kanta-alkion tulo on kolmas samalta viivalta löytyvä alkio. Nuolen suunta kertoo tulon etumerkin. Esimerkiksi kvaternioilla pätee $j \cdot i = -k$, ja oktonioilla on voimassa $i_0 \cdot i_1 = i_3$ ja $i_1 \cdot i_4 = -i_2$.

9.3. Ryhmä- ja monoidialgebrat. Olkoon $(G, *)$ jokin ryhmä ja R rengas. Tarkastellaan vapaata R-modulia $R^{(G)}$. Tämän modulin luonnollisen kannan muodostavat alkiot e_g, missä $g \in G$, ja nämä voidaan samastaa vastaavan ryhmän alkion g kanssa. Koska kannan alkiot tällöin kuuluvat ryhmään G, niille voidaan määritellä luonnollinen kertolasku.

Määritelmä 9.8. *Ryhmäalgebra* RG on vapaa R-moduli $R^{(G)}$ varustettuna bilineaarisella kertolaskulla, joka toteuttaa ehdon $g \cdot h = g * h$ kaikilla kannan alkioilla $g, h \in G$.

Kahden ryhmäalgebran mielivaltaisen jäsenen tulo on
$$\sum_i a_i g_i \cdot \sum_j b_j h_j = \sum_{i,j} a_i b_j (g_i * h_j).$$
Ryhmäalgebrat ovat liitännäisiä ja ykkösellisiä, mikä seuraa ryhmäkertolaskun ominaisuuksista ja lauseesta 9.4. Samanlainen konstruktio voidaan tehdä lähtien liikkeellä ryhmän sijaan monoidista, jolloin tuloksena on monoidialgebra.

Esimerkki 9.9. Esitysteoriassa tutkitaan homomorfismeja annetulta ryhmältä G jonkin vektoriavaruuden V kääntyvien lineaarikuvausten ryhmään $GL(V)$. Tällainen kuvaus määrittelee ryhmän G lineaarisen toiminnan avaruudessa V, ja sitä kutsutaan ryhmän *esitykseksi* avaruudessa V. Esityksistä — kuten toiminnoista yleensäkin — on se hyöty, että niitä tutkimalla saadaan paljon tietoa ryhmän rakenteesta.

Nykyisin on tapana sisällyttää esitysteoria modulien teoriaan käyttämällä hyväksi ryhmäalgebran käsitettä. Olkoon V jokin K-kertoiminen vektoriavaruus, ja olkoon $\varphi : G \to GL(V)$ ryhmähomomorfismi, jolloin $\varphi(g)$ on kääntyvä lineaarikuvaus jokaisella $g \in G$. Koska ryhmäalgebra KG on liitännäinen ja ykkösellinen, sitä voidaan pitää renkaana, joka ei kuitenkaan ole vaihdannainen, ellei G ole vaihdannainen. Avaruuteen V voidaan nyt määritellä renkaan KG kanta-alkioiden vasemmanpuoleinen toiminta kaavalla

$$g.x = \varphi(g)(x).$$

Laajentamalla tämä toiminta lineaarisesti koko renkaan KG vasemmaksi toiminnaksi avaruudesta V tulee vasen KG-moduli.

Jokaista esitystä φ vastaa nyt yksikäsitteisesti jokin KG-moduli, ja esitysteoriasta tutut käsitteet voidaan ilmaista yksinkertaisesti modulikäsitteiden avulla. Esimerkiksi esitys on jaoton, jos ja vain jos vastaavalla modulilla ei ole aitoja epätriviaaleja alimoduleita, ja kaksi esitystä ovat keskenään ekvivalentit, jos ja vain jos vastaavat modulit ovat isomorfiset.

9.4. Polynomialgebrat. Polynomit muodostavat renkaita, joissa voidaan määritellä luonnollinen skalaarikertolasku. Tähän asti polynomeja on käsitelty tässä materiaalissa varsin epämuodollisesti ja niihin on sovellettu koulussa opittuja tietoja. Esitetään tässä yhteydessä eräs tapa konstruoida formaalisti R-kertoiminen polynomialgebra.

Olkoon R rengas ja $I = \{1, 2, \dots, n\}$ äärellinen indeksijoukko. Ruvetaan määrittelemään polynomialgebraa $R[X_1, \dots, X_n]$, joka koostuu R-kertoimisista n:n muuttujan polynomeista. Tarkastellaan ensin tulomonoidia $M_n = \mathbb{N}^n$, joka koostuu jonoista $\nu = (\nu_1, \dots, \nu_n)$, missä $\nu_i \in \mathbb{N}$ jokaisella i. Jonojen yhteenlasku määritellään pisteittäin.

Monoidi M_n sisältää konstruoitavan polynomialgebran *monomit.* Ryhdytään kirjoittamaan mielivaltainen alkio $\nu = (\nu_1, \dots, \nu_n) \in M_n$ muodossa

$$X^\nu = X_1^{\nu_1} X_2^{\nu_2} \cdots X_n^{\nu_n}.$$

Jokaisesta jonon ν komponentista ν_i tulee siis muuttujan X_i muodollinen eksponentti. Jos jokin ν_i on nolla, voidaan vastaava X_i^0 jättää merkitsemättä tuloon. Tällöin $X^{e_i} = X_i$, missä $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ (ykkönen i:nnellä paikalla). Kahden jonon μ ja ν summa vastaa nyt muodollista vaihdannaista tuloa:

$$\mu + \nu = X^{\mu+\nu} = X_1^{\mu_1+\nu_1} X_2^{\mu_2+\nu_2} \cdots X_n^{\mu_n+\nu_n}.$$

Esimerkiksi $(2, 1, 0) + (0, 1, 1) = X_1^2 X_2 \cdot X_2 X_3 = X_1^2 X_2^2 X_3$.

Tarkastellaan sitten monoidialgebraa $P_R(I) = RM_n$. Sen alkioina ovat monoidin M_n alkioiden R-kertoimiset lineaarikombinaatiot

$$\sum_\nu a_\nu X^\nu, \qquad \text{missä } a_\nu \in R \text{ ja } \nu \in M_n.$$

Kanta-alkioiden kertolasku saadaan monoidin M_n laskutoimituksesta:

$$X^\mu \cdot X^\nu = X^{\mu+\nu} = X_1^{\nu_1+\mu_1} \cdots X_n^{\nu_n+\mu_n},$$

ja kahden yleisen alkion tulo on

$$\sum_\nu a_\nu X^\nu \cdot \sum_\mu b_\mu X^\mu = \sum_{\nu,\mu} a_\nu b_\mu X^{\nu+\mu}.$$

Huomaa, että algebraan siirryttäessä monoidin yhteenlasku muuttuu algebran kertolaskuksi ja samalla monoidin nolla-alkiosta $X^0 = (0, \dots, 0)$ tulee algebran ykkösalkio.

MÄÄRITELMÄ 9.10. Monoidialgebra $P_R(I)$ on *R-kertoiminen n:n muuttujan polynomialgebra.* Se on liitännäinen, vaihdannainen ja ykkösellinen R-algebra, ja sitä merkitään $R[X_1, \dots, X_n]$. Monoidin M_n alkioita kutsutaan *monomeiksi.*

Polynomialgebra koostuu monomien lineaarikombinaatioista. Tyhjä lineaarikombinaatio on algebran nolla-alkio, ja sitä nimitetään *nollapolynomiksi.* Ykkösalkio on monoidin M_n nolla-alkio $X^0 = (0, \dots, 0)$. Monomin X^ν *aste* on eksponenttien summa $\sum_i \nu_i$, ja polynomin aste on suurin sen sisältämän monomin aste. Nollapolynomin asteeksi määritellään $-\infty$. Esimerkiksi monomin $X_2^5 X_3$ aste on $5 + 1 = 6$.

Polynomia, jonka aste on 0, nimitetään *vakiopolynomiksi* tai *vakioksi.* Kuvaus $\eta : a \mapsto aX^0$ on bijektio renkaan R ja vakiopolynomien välillä, ja sen avulla kerroinrengas voidaan samastaa vakioiden kanssa. Kuvaus η on myös rengashomomorfismi, mistä seuraa, että renkaan skalaarikertolasku yhtyy vakiopolynomien kertolaskuun. Erityisesti η kuvaa renkaan ykkösalkion algebran ykkösalkioksi.

Polynomialgebralle pätee seuraava universaaliominaisuus.

LAUSE 9.11. *Olkoon R rengas ja A jokin liitännäinen, vaihdannainen ja ykkösellinen R-algebra. Olkoon lisäksi $(x_1, \dots, x_n)$ jono A:n alkioita. Tällöin on olemassa yksikäsitteinen algebrahomomorfismi $\varphi : R[X_1, \dots, X_n] \to A$, jolle pätee $\varphi(X_i) = x_i$ jokaisella i.*

TODISTUS. Koska algebra A on liitännäinen ja ykkösellinen, se on kertolaskunsa suhteen monoidi. Määritellään kuvaus $f : M_n \to A$ kaavalla

$$f(X^\nu) = x_1^{\nu_1} \cdots x_n^{\nu_1}.$$

Kuvaus f on monoidihomomorfismi monoidilta M_n algebran A multiplikatiiviselle monoidille, sillä

$$\begin{aligned} f(X^\mu \cdot X^\nu) &= f(X^{\mu+\nu}) = x_1^{\mu_1+\nu_1} \cdots x_n^{\mu_n+\nu_n} \\ &= (x_1^{\mu_1} \cdots x_n^{\mu_n}) \cdot (x_1^{\nu_1} \cdots x_n^{\nu_n}) = f(X^\mu) \cdot f(X^\nu), \end{aligned}$$

ja $f(X^0) = x_1^0 \cdots x_n^0 = 1_A$. (Tässä käytettiin hyväksi A:n vaihdannaisuutta.)

Koska $R[X_1, \dots, X_n]$ on vapaa moduli, jonka kanta on M_n, vapaan modulin universaaliominaisuudesta seuraa, että on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi : R[X_1, \dots, X_n] \to A$, jolle pätee $\varphi(X^\nu) = f(X^\nu)$ kaikilla $X^\nu \in M_n$. Tämä lineaarikuvaus säilyttää lisäksi algebran kertolaskurakenteen, sillä kannan alkioilla pätee

$$\varphi(X^\nu \cdot X^\mu) = f(X^\nu \cdot X^\mu) = f(X^\nu) \cdot f(X^\mu) = \varphi(X^\nu) \cdot \varphi(X^\mu),$$

ja yleinen tapaus seuraa kuvauksen φ sekä algebrakertolaskun lineaarisuusominaisuuksista. Kuvaus φ on siis algebrahomomorfismi, ja lisäksi $\varphi(X_i) = f(X^{e_i}) = x_i$ kaikilla i.

Olkoon sitten φ' toinen algebrahomomorfismi, joka toteuttaa lauseen oletukset. Koska φ' säilyttää kertolaskun, täytyy päteä

$$\varphi'(X^\nu) = \varphi'(X_1^{\nu_1} \cdots X_n^{\nu_n}) = \varphi'(X_1)^{\nu_1} \cdots \varphi'(X_n)^{\nu_n} = x_1^{\nu_1} \cdots x_n^{\nu_1}.$$

Näin ollen kuvaukset φ' ja φ yhtyvät monoidin M_n alkioilla, joten φ:n yksikäsitteisyydestä seuraa, että $\varphi' = \varphi$. □

MÄÄRITELMÄ 9.12. Edellisen lauseen kuvausta φ kutsutaan *sijoitushomomorfismiksi*. Polynomin $f = \sum_\nu a_\nu X^\nu$ arvo sijoitushomomorfismissa on

$$\varphi(f) = \sum_\nu a_\nu x^{\nu_1} \cdots x^{\nu_n},$$

ja sitä merkitään $f(x_1, \ldots, x_n)$.

Sijoitushomomorfismin avulla voidaan määritellä algebran A *polynomifunktio* $(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)$. Tässä kohdassa on syytä huomata ero polynomin ja sen määräämän polynomifunktion välillä. Olkoon esimerkiksi $f = X^2 + X \in \mathbb{Z}_2[X]$. Nyt f ei ole nollapolynomi, mutta $f(x) = 0$ kaikilla $x \in \mathbb{Z}_2$, eli f:n määräämä funktio algebrassa $\mathbb{Z}_2$ on nollafunktio.

Tässä luvussa määriteltiin polynomit äärellisen muuttujajoukon suhteen. On myös mahdollista valita indeksijoukko I äärettömäksi. Tällöin monomimonoidi $M_I = \mathbb{N}^{(I)}$ koostuu alkioperheistä, joissa on vain äärellinen määrä nollasta poikkeavia alkioita. Muuten konstruktio etenee aivan samalla tavalla.