LUKU 2

Lineaarialgebraa

2.1. Modulit

Olkoon A rengas.

MÄÄRITELMÄ 2.1.1. *Vasemmanpuolinen A-moduli* on joukko E varustettuna

i) vaihdannaisen ryhmän struktuurilla $(x, y) \mapsto x + y$, ja
ii) renkaan A toiminnalla $(\alpha, x) \mapsto \alpha x$,

jotka toteuttavat seuraavat ehdot kaikilla α, $\beta \in A$ ja x, $y \in E$.

(M1) $\alpha(x + y) = \alpha x + \alpha y$;
(M2) $(\alpha + \beta)x = \alpha x + \beta x$;
(M3) $\alpha(\beta x) = (\alpha\beta)x$;
(M4) $1.x = x$.

Renkaan A toimintaa modulissa E sanotaan *skalaarikertolaskuksi*. Ehdot (M3) ja (M4) merkitsevät, että kyseessä on A:n multiplikatiivisen monoidin toiminta vasemmalta joukossa E. Ehdot (M1) ja (M2) taas tarkoittavat, että skalaarikertolasku on *ositteleva* sekä modulin E että renkaan A yhteenlaskun suhteen.

Jos (M3) korvataan ehdolla

$$(\text{M3}') \ \alpha(\beta x) = (\beta\alpha)x \qquad \text{kaikilla } \alpha,\ \beta \in A,\ x \in E,$$

niin E on *oikeanpuolinen A-moduli*. Tällöin A toimii oikealta E:ssä ja skalaarikertolasku merkitään $(x, \alpha) \mapsto x\alpha$.

Huomautus. Jos A^o on renkaan A *vastarengas*, jonka kertolasku on $(\alpha, \beta) \mapsto \beta\alpha$, niin oikeanpuolinen A-moduli on vasemmanpuolinen A^o-moduli. Periaatteessa on siis riittävää tarkastella vasemmanpuolisia moduleita.

Esimerkkejä. 1) Jokainen reaalinen vektoriavaruus E on $\mathbf{R}$-moduli.

Yleisesti, jos K on kunta, K-moduleita sanotaan K-kertoimisiksi *vektoriavaruuksiksi* ja niiden alkioita *vektoreiksi*.

2) Jokainen vaihdannainen (additiivinen) ryhmä E on $\mathbf{Z}$-moduli varustetuna skalaarikertolaskulla $(n, x) \mapsto n.x$, missä $n.x$ on x:n n:s *kerrannainen* (potenssin additiivinen versio). Ehdot (M2) ja (M3) ovat potenssilait yhteenlaskulla esitettyinä.

3) Rengas A on vasemmanpuolinen (ja oikeanpuolinen) A-moduli, kun kertolasku tulkitaan myös skalaarikertolaskuksi.

Yleisemmin, jos B on toinen rengas ja $\varphi\colon A \to B$ on rengashomomorfismi, niin B varustettuna yhteenlaskullaan ja skalaarikertolaskulla

$$(\alpha, x) \mapsto \varphi(\alpha)x \qquad (\text{tai } (x, \alpha) \mapsto x\varphi(\alpha))$$

on vasemmanpuolinen (tai oikeanpuolinen) A-moduli. (Esimerkiksi

$$\varphi(\alpha\beta)x = (\varphi(\alpha)\varphi(\beta))x = \varphi(\alpha)(\varphi(\beta)x).)$$

4) Reaaliset $n \times n$-matriisit muodostavat renkaan $\mathbf{M}_n(\mathbf{R})$, ja $\mathbf{R}^n$ varustettuna skalaarikertolaskulla $(M, \mathbf{x}) \mapsto M\mathbf{x}$ on vasemmanpuolinen $\mathbf{M}_n(\mathbf{R})$-moduli.

Vastaava pätee, kun reaalilukujen kunnan $\mathbf{R}$ tilalla on jokin muu kunta K tai yleisemmin rengas A.

5) Olkoon E additiivinen vaihdannainen ryhmä ja $\operatorname{End}(E)$ sen endomorfismirengas. Tällöin E varustettuna yhteenlaskullaan ja skalaarikertolaskulla

$$(f, x) \mapsto f.x = f(x)$$

on vasemmanpuolinen $\operatorname{End}(E)$-moduli.

Lineaariset yhdistelmät. Olkoon A rengas, E vasemmanpuolinen A-moduli ja $(a_i)_{i\in I}$ perhe sen alkioita. Jos $(\lambda_i)_{i\in I}$ on A:n alkioperhe, jolla on sama indeksijoukko, niin kaikilla $i \in I$ voidaan muodostaa

$$\lambda_i a_i \in E$$

ja näistä edelleen summa

$$\sum_{i\in I} \lambda_i a_i \in E,$$

jos perheellä $(\lambda_i)_{i\in I}$ on äärellinen kantaja.

Määritelmä 2.1.2. A-modulin E alkio x on E:n alkioperheen $(a_i)_{i\in I}$ A-kertoiminen *lineaarinen yhdistelmä*, jos on olemassa sellainen A:n äärelliskantajainen alkioperhe $(\lambda_i)_{i\in I}$, että

$$x = \sum_{i\in I} \lambda_i a_i.$$

Lineaarikuvaukset. Olkoon A rengas ja olkoot E ja F kaksi A-modulia.

Määritelmä 2.1.3. Kuvaus $u\colon E \to F$ on *lineaarikuvaus* l. *homomorfismi* (tai *A-lineaarinen kuvaus*, *A-homomorfismi*), jos kaikilla x, $y \in E$ ja $\lambda \in A$

i) $u(x + y) = u(x) + u(y)$,
ii) $u(\lambda x) = \lambda u(x)$.

Huomautus. Ehdot voidaan yhdistää yhdeksi kaavaksi

$$u(\lambda x + \mu y) = \lambda u(x) + \mu u(y),$$

kun λ, $\mu \in A$ ja x, $y \in E$, tai yleisemmin, kun $x_i \in E$, $\lambda_i \in A$ $(i \in I)$ ja $\lambda_i \neq 0$ vain äärellisen monella indeksillä $i \in I$, niin

$$u(\sum_{i \in I} \lambda_i x_i) = \sum_{i \in I} \lambda_i u(x_i).$$

Esimerkkejä. 6) Olkoot E ja F vaihdannaisia additiivisia ryhmiä. Tällöin ne ovat myös $\mathbf{Z}$-moduleita, ja jokainen ryhmähomomorfismi

$$u \colon E \to F$$

on myös $\mathbf{Z}$-lineaarinen kuvaus. (Ehto $u(n.x) = n.u(x)$ todistetaan induktiolla, kun $n \geq 0$, ja kaavalla $u(-x) = -u(x)$, kun $n < 0$.)

7) Jokaiseen A-modulin E alkioon a liittyy A-lineaarinen kuvaus

$$u \colon A \to E, \quad \lambda \mapsto \lambda a,$$

ja jokainen homomorfismi $u \colon A \to E$ on tällainen $(a = u(1))$.

Huomautus. Jos E ja F ovat oikeanpuolisia A-moduleita, niin määritelmän ehto ii) saa muodon

$$u(x\lambda) = u(x)\lambda.$$

Merkinnän muutosta lukuunottamatta homomorfismien teoria on sama kuin vasemmanpuolisilla moduleilla.

Kaikkien A-homomorfismien $u \colon E \to F$ joukolle käytetään merkintää $\mathrm{Hom}_A(E, F)$ tai vain $\mathrm{Hom}(E, F)$, jos kerroinrengas A selviää asiayhteydestä.

Jos u, $v \in \mathrm{Hom}(E, F)$, ja kaikilla $x \in E$ asetetaan

$$(u + v)(x) = u(x) + v(x),$$

niin kuvaus $u + v \colon E \to F$ on myös A-homomorfismi. Tällä yhteenlaskulla varustettuna $\mathrm{Hom}_A(E, F)$ on vaihdannainen ryhmä (harj. teht.).

Alimodulit. Olkoon A rengas.

MÄÄRITELMÄ 2.1.4. A-modulin E *alimoduli* F on E:n additiivisen ryhmän aliryhmä, joka on vakaa A:n toiminnan suhteen.

Lyhyesti kirjoitettuina ehdot ovat

$$0 \in F, \quad F + F \subset F, \quad A.F \subset F \text{ (tai } F.A \subset F).$$

Indusoiduilla laskutoimituksilla varustettuna alimoduli F on myös A-moduli, ja kanoninen injektio $j \colon F \to E$ on A-lineaarinen kuvaus.

Esimerkkejä. 8) Kun vaihdannainen ryhmä E tulkitaan $\mathbf{Z}$-moduliksi, niin sen jokainen aliryhmä F on alimoduli.

9) Vektoriavaruuden alimodulit ovat vektoriavaruuksia ja niitä sanotaan *aliavaruuksiksi*.

10) Kun rengasta A tarkastellaan vasemman- tai oikeanpuolisena A-modulina, niin sen alimodulit ovat samat kuin A:n vasemman- tai oikeanpuoliset ideaalit.

Olkoon E A-moduli ja X sen osajoukko. Kaikkien joukon X sisältävien E:n alimodulien leikkaus F on myös E:n alimoduli. Se on pienin X:n sisältävä alimoduli eli joukon X *virittämä E:n alimoduli*, ja X on eräs sen *virittäjäjoukko*. Moduli on *äärellistyyppinen*, jos sillä on äärellinen virittäjäjoukko.

Jos $(a_i)_{i \in I}$ on modulin E alkioperhe, niin joukon $X = \{a_i \mid i \in I\}$ virittämää E:n alimodulia sanotaan myös *perheen $(a_i)_{i \in I}$ virittämäksi alimoduliksi* ja perhettä $(a_i)_{i \in I}$ sen *virittäjäperheeksi*.

LAUSE 2.1.5. *A-modulin E alkioperheen $(a_i)_{i \in I}$ virittämä alimoduli on perheen $(a_i)_{i \in I}$ A-kertoimisten lineaaristen yhdistelmien joukko.*

Todistetaan kuten lause 1.1.8 (harj. teht.).

Tekijämodulit. Olkoon A rengas ja E A-moduli. Jos R on laskutoimitusten kanssa yhteen sopiva ekvivalenssi E:ssä, niin 0:n luokka

$$M = \{x \in E \mid x \equiv 0 \pmod{R}\}$$

on E:n alimoduli.

Kääntäen, jos M on E:n alimoduli, niin ehto

$$x \equiv y \pmod{R} \;\Leftrightarrow\; x - y \in M$$

määrittelee laskutoimitusten kanssa yhteensopivan ekvivalenssirelaation E:ssä. Tällöin E/R varustettuna tekijälaskutoimituksilla on A-moduli, E:n *tekijämoduli* alimodulin M suhteen (tai *tekijäavaruus*, kun E on vektoriavaruus), ja sille käytetään merkintää E/M. Kanoninen kuvaus $p\colon E \to E/M$ on A-lineaarinen.

Esimerkki 11) Jos $\mathfrak{a}$ on renkaan A vasemman- tai oikeanpuolinen ideaali, niin se on A:n alimoduli, ja siten $A/\mathfrak{a}$ on (vasemman- tai oikeanpuolinen) A-moduli. (Rengas se on vain, jos $\mathfrak{a}$ on kaksipuolinen ideaali.)

Homomorfismien *hajotuslause* ja *homomorfialause* pätevät myös moduleilla ja todistetaan samoin kuin ryhmien teoriassa.

LAUSE 2.1.6. *Olkoot E ja F kaksi A-modulia, M modulin E alimoduli, $u\colon E \to F$ homomorfismi ja $p\colon E \to E/M$ kanoninen kuvaus. Tällöin on olemassa homomorfismi $v\colon E/M \to F$, joka toteuttaa ehdon*

$$u = v \circ p,$$

jos ja vain jos

$$M \subset \operatorname{Ker}(u).$$

$$\begin{tikzcd} E \arrow[rr, "u"] \arrow[dr, "p"'] & & F \\ & E/M \arrow[ur, dashed, "v"'] & \end{tikzcd}$$

LAUSE 2.1.7. *Olkoot E ja F kaksi A-modulia ja $u\colon E \to F$ homomorfismi. Tällöin u:n* ydin $\operatorname{Ker}(u) = u^{-1}(0)$ *on E:n alimoduli,* kuva $\operatorname{Im}(u) = u(E)$ *on F:n alimoduli ja u:n kanonisesta hajotelmasta saadaan isomorfismi*

$$\bar{u}\colon E/\operatorname{Ker}(u) \xrightarrow{\sim} \operatorname{Im}(u).$$

Modulien tulot. Olkoon A rengas ja $(E_i)_{i\in I}$ perhe A-moduleita. Tällöin karteesinen tulo

$$E = \prod_{i\in I} E_i$$

varustettuna yhteenlaskulla

$$(x_i) + (y_i) = (x_i + y_i)$$

ja skalaarikertolaskulla

$$\lambda(x_i) = (\lambda x_i) \quad (\lambda \in A)$$

on A-moduli, modulien E_i *tulomoduli*, ja jokainen projektiokuvaus

$$\mathrm{pr}_i \colon E \to E_i$$

on A-lineaarinen.

LAUSE 2.1.8 (Tulon universaaliominaisuus). *Olkoon $(E_i)_{i\in I}$ perhe A-moduleita ja E niiden tulomoduli. Jos F on A-moduli ja $f_i \colon F \to E_i$ on A-homomorfismi kaikilla $i \in I$, niin on olemassa yksikäsitteinen lineaarikuvaus $f \colon F \to E$, joka toteuttaa ehdot*

$$f_i = \mathrm{pr}_i \circ f \quad (i \in I).$$

$$\begin{tikzcd} & E \arrow[dr, "\mathrm{pr}_i"] & \\ F \arrow[ur, dashed, "f"] \arrow[rr, "f_i"'] & & E_i \end{tikzcd}$$

Todistus. Olkoon $f \colon F \to E$ kuvaus, joka täyttää vaaditut ehdot. Jos $x \in F$ ja $f(x) = y = (y_i) \in E$, niin kaikilla $i \in I$

$$f_i(x) = \mathrm{pr}_i(f(x)) = y_i.$$

Kuvaus f on siis yksikäsitteinen ja saadaan kaavasta

$$f(x) = (f_i(x)) \quad (x \in F).$$

Toisaalta tämä kuvaus on A-lineaarinen aina, kun jokainen f_i on A-lineaarinen (harj.teht.). □

Kuvauksia f_i sanotaan homomorfismin f *komponenteiksi* ja usein merkitään $f = (f_i)$ ellei ole sekaannuksen vaaraa.

Jos perheen (E_i) kaikki modulit ovat samat eli $E_i = E$ $(i \in I)$, niin tulomoduli on sama kuin kaikkien kuvausten

$$x \colon I \to E, \quad i \mapsto x_i \in E,$$

muodostama *kuvausmoduli*

$$\prod_{i\in I} E_i = E^I.$$

Jos erityisesti $I = \{1, 2, \dots, n\}$, niin tulomodulille käytetään merkintöjä

$$\prod_{i\in I} E_i = \prod_{i=1}^{n} E_i = E_1 \times E_2 \times \cdots \times E_n$$

ja jos lisäksi $E_i = E$ $(1 \leq i \leq n)$, niin merkitään

$$E \times E \times \cdots \times E = E^n.$$

Modulien suorat summat. Olkoon A rengas, $(E_i)_{i\in I}$ perhe A-moduleita ja

$$F = \prod_{i\in I} E_i$$

tulomoduli. Tällöin modulien E_i additiivisten ryhmien suora summa (eli rajoitettu tulo, ks. 1.3)

$$\bigoplus_{i\in I} E_i = \{(x_i) \mid x_i \in E_i \ (i \in I) \text{ ja } x_i = 0 \text{ melkein kaikilla } i \in I\}$$

on F:n aliryhmä ja vakaa skalaarikertolaskun suhteen. Se on siis tulomodulin F alimoduli, *modulien E_i suora summa.*

Jokaiseen indeksiin $k \in I$ liittyy *kanoninen injektio*

$$j_k \colon E_k \to F, \quad x_k \mapsto (y_i),$$

missä perheen $(y_i) \in F$ alkiot ovat

$$y_i = \begin{cases} x_k & \text{, kun } i = k, \\ 0 & \text{, kun } i \neq k. \end{cases}$$

Se on homomorfismi, jonka komponentit ovat (lause 2.1.8)

$$\operatorname{pr}_i \circ j_k = \begin{cases} \mathrm{Id}_{E_k} & \text{, kun } i = k, \\ 0 & \text{, kun } i \neq k. \end{cases}$$

Kuva $j_k(E_k)$ on suoran summan $E = \bigoplus_{i\in I} E_i$ alimoduli, joka usein samastetaan E_k:n kanssa.

Jos $x = (x_i) \in E$, niin perheen $(j_i(x_i))_{i\in I}$ kantaja on äärellinen ja sen summan

$$x' = (x_i') = \sum_{i\in I} j_i(x_i)$$

i:s jäsen on sama kuin termillä $j_i(x_i)$, eli $x_i' = x_i$. Koska $x_i = \operatorname{pr}_i(x)$ kaikilla $i \in I$, saadaan yksikäsitteinen esitys

$$x = \sum_{i\in I} j_i(\operatorname{pr}_i(x)).$$

Erityisesti nähdään, että suora summa $E = \bigoplus_{i\in I} E_i$ on yhdisteen $\bigcup_{i\in I} j_i(E_i)$ virittämä tulomodulin alimoduli.

Jos I on äärellinen, niin suora summa on sama kuin tulo

$$\bigoplus_{i\in I} E_i = \prod_{i\in I} E_i.$$

Jos erityisesti $I = \{1, 2, \ldots, n\}$, niin merkitään myös

$$\bigoplus_{i\in I} E_i = \bigoplus_{i=1}^{n} E_i = E_1 \oplus E_2 \oplus \cdots \oplus E_n.$$

LAUSE 2.1.9 (Suoran summan universaaliominaisuus). *Olkoon* $(E_i)_{i\in I}$ *perhe A-moduleita ja E perheen suora summa. Jos F on A-moduli ja* $f_i\colon E_i \to F$ *on A-homomorfismi kaikilla* $i \in I$*, niin on olemassa yksikäsitteinen lineaarikuvaus* $g\colon E \to F$*, joka toteuttaa ehdot*

$$f_i = g \circ j_i \quad (i \in I).$$

$$\begin{tikzcd} E_i \arrow[rr, "f_i"] \arrow[dr, "j_i"'] & & F \\ & E \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Todistus. Olkoon $g\colon E \to F$ homomorfismi, joka toteuttaa esitetyt ehdot. Jos x on E:n alkio, niin yhtälöstä

$$x = \sum_{i\in I} j_i(\mathrm{pr}_i(x))$$

seuraa

$$g(x) = \sum_{i\in I} g(j_i(\mathrm{pr}_i(x))) = \sum_{i\in I} f_i(\mathrm{pr}_i(x)),$$

joten g on yksikäsitteinen. Toisaalta tämä kaava myös määrittelee homomorfismin $g\colon E \to F$, joka täyttää vaatimukset (harj. teht.). □

Jos $x = (x_i) \in \bigoplus_{i\in I} E_i$, niin yllä esitetyn nojalla

$$g(x) = \sum_{i\in I} f_i(x_i).$$

Usein tämä kaava merkitään lyhyesti

$$g = \sum_{i\in I} f_i\,,$$

ellei ole sekaannuksen vaaraa.

Jos perheen (E_i) kaikki modulit ovat samat eli $E_i = E$ $(i \in I)$, niin suoralle summalle käytetään merkintää

$$\bigoplus_{i\in I} E_i = E^{(I)}.$$

Sen alkiot voidaan tällöin tulkita kuvauksiksi $x\colon I \to E$, $i \mapsto x_i$, joilla on äärellinen kantaja.

Esimerkki 12) Olkoon E A-moduli ja $(E_i)_{i\in I}$ perhe sen alimoduleita. Jokaisella $i \in I$ olkoon

$$f_i\colon E_i \to E$$

kanoninen injektio. Niiden summana saadaan *kanoninen homomorfismi*

$$g = \sum_{i\in I} f_i\colon \bigoplus_{i\in I} E_i \to E.$$

Jos $x = (x_i) \in \bigoplus_{i\in I} E_i$, niin

$$g(x) = \sum_{i\in I} f_i(x_i) = \sum_{i\in I} x_i.$$

Tätä muotoa olevien E:n alkioiden joukolle käytetään merkintää

$$\sum_{i\in I} E_i = \{\sum_{i\in I} x_i \mid (x_i) \in \bigoplus_{i\in I} E_i\}.$$

Homorfismin g kuvana se on E:n alimoduli, *alimodulien* E_i $(i \in I)$ *summa*.

Kanoninen homomorfismi g ei yleensä ole injektiivinen eikä surjektiivinen.

MÄÄRITELMÄ 2.1.10. A-moduli E on *alimoduliensa* E_i $(i \in I)$ *suora summa*, jos kanoninen homomorfismi

$$g\colon \bigoplus_{i\in I} E_i \to E$$

on bijektiivinen.

Tämä merkitsee, että jokaisella E:n alkiolla x on yksikäsitteinen esitys summana

$$x = \sum_{i\in I} x_i,$$

missä $x_i \in E_i$ $(i \in I)$ ja $x_i \neq 0$ vain äärellisen monella $i \in I$.

Vapaat perheet ja kannat. Olkoon A rengas, E A-moduli ja $(a_i)_{i\in I}$ perhe E:n alkioita. Tarkastellaan lineaarisia yhdistelmiä

$$x = \sum_{i\in I} \xi_i a_i \in E,$$

missä (ξ_i) on äärelliskantajainen A:n alkioperhe eli lyhyesti $(\xi_i) \in A^{(I)}$. Erityisesti jokainen a_i voidaan esittää muodossa

$$a_i = \sum_{j\in I} \delta_{ij} a_j,$$

missä

$$\delta_{ij} = \begin{cases} 1 & \text{, kun } i = j, \\ 0 & \text{, kun } i \neq j, \end{cases}$$

on *Kroneckerin symboli.* Kerroinperhe

$$e_i = (\delta_{ij})_{j\in I} \in A^{(I)}$$

on tällöin Kroneckerin funktio δ_i perheeksi tulkittuna (ks. 1.6).

LAUSE 2.1.11. *Jokaista A-modulin E alkioperhettä $(a_i)_{i\in I}$ vastaa yksikäsitteinen A-lineaarinen kuvaus $g\colon A^{(I)} \to E$, joka toteuttaa ehdot*

$$g(e_i) = a_i \qquad (i \in I).$$

Todistus. Olkoon $g\colon A^{(I)} \to E$ ehdot täyttävä A-homomorfismi. Jos $x = (\xi_i)_{i\in I}$ on äärelliskantajainen A:n alkioperhe, niin se voidaan modulin $A^{(I)}$ alkiona esittää summana (vrt. lemma 1.6.1)

$$x = \sum_{i\in I} \xi_i e_i.$$

Koska g on A-lineaarinen, pätee toisaalta yhtälö

$$g(\sum_{i\in I}\xi_i e_i) = \sum_{i\in I}\xi_i g(e_i).$$

Arvo

$$g(x) = \sum_{i\in I}\xi_i a_i$$

on siten yksikäsitteinen.

Kääntäen tällä kaavalla määritelty kuvaus $g\colon A^{(I)} \to E$ on homomorfismi ja täyttää vaaditut ehdot (harj. teht.). $\square$

Lausetta voidaan pitää A-modulin $A^{(I)}$ *universaaliominaisuutena*. Kun tulkitaan perheet (e_i) ja (a_i) kuvauksiksi $\varphi\colon I \to A^{(I)}$ ja $f\colon I \to E$, saadaan kaavio

$$\begin{tikzcd} I \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & E . \\ & A^{(I)} \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Homomorfismia g sanotaan *perheen $(a_i)_{i\in I}$ määräämäksi lineaarikuvaukseksi.*

Korollaari 2.1.12. *Perhe $(a_i)_{i\in I}$ virittää modulin E, jos ja vain jos sen määräämä lineaarikuvaus $g\colon A^{(I)} \to E$ on surjektiivinen.*

Todistus. Homomorfismin g kuva

$$\mathrm{Im}(g) = \{\sum_{i\in I}\xi_i a_i \mid (\xi_i) \in A^{(I)}\}$$

on perheen $(a_i)_{i\in I}$ A-kertoimisten lineaaristen yhdistelmien joukko eli lauseen 2.1.5 nojalla sen virittämä E:n alimoduli. Perhe virittää siis koko E:n, jos ja vain jos $\mathrm{Im}(g) = E$. $\square$

Yleensä modulin E alkioperheen $(a_i)_{i\in I}$ määräämä lineaarikuvaus g ei ole injektiivinen. Sen ytimen alkioita

$$(\lambda_i) \in \mathrm{Ker}(g),$$

joita siis luonnehtii ehto

$$\sum_{i\in I}\lambda_i a_i = 0,$$

sanotaan *lineaarisiksi relaatioiksi* perheen $(a_i)_{i\in I}$ alkioiden välillä.

Lineaarikuvaus g on injektiivinen, jos ja vain jos sen ydin on $\{0\}$ eli ainoa lineaarinen relaatio on *triviaali lineaarinen relaatio*, missä $\lambda_i = 0$ kaikilla $i \in I$.

Määritelmä 2.1.13. A-modulin E alkioperhe $(a_i)_{i\in I}$ on *vapaa perhe*, jos sen määräämä lineaarikuvaus $g\colon A^{(I)} \to E$ on injektiivinen, ja E:n *kanta*, jos g on bijektiivinen. Jos perhe $(a_i)_{i\in I}$ ei ole vapaa, niin se on *sidottu*.

Moduli E on *vapaa moduli*, jos sillä on kanta.

Korollaarin 2.1.12 nojalla kanta on sama kuin vapaa virittäjäperhe.

Esimerkkejä. 13) Jokainen A-moduli $A^{(I)}$ on vapaa, kantana $(e_i)_{i\in I}$. Erityisesti vapaa vaihdannainen ryhmä $\mathbf{Z}^{(I)}$ (ks. 1.6) on vapaa $\mathbf{Z}$-moduli.

14) Jokainen vektoriavaruus E on vapaa modulina kerroinkuntansa K suhteen. (Tämä todistetaan kuten Lineaarialgebra I:n kurssissa, kun E on äärellistyyppinen. Muulloin käytetään Zornin lemmaa.)

15) Jos $m > 1$ on luonnollinen luku, niin $\mathbf{Z}/m\mathbf{Z}$ ei ole vapaa $\mathbf{Z}$-moduli, koska siinä on m alkiota, mutta $\mathbf{Z}^{(I)}$ on ääretön, kun $I \neq \emptyset$.

Huomautus. Vapaan A-modulin E eri kantojen ei tarvitse olla yhtä mahtavia, vaikka ne olisivat äärellisiä (itse asiassa juuri tällöin).

Kannat ovat yhtä mahtavat, jos A on kunta, eli vektoriavaruuden E *dimensio* on hyvin määritelty (todistetaan kuten Lineaarialgebra I:n kurssissa), ja yleisemmin, jos on olemassa homomorfismi $A \to K$, missä K on kunta (esim. jos A on vaihdannainen; ks. kor. 1.8.4). Tällöin vapaalla A-modulilla on hyvin määritelty *aste*.

Lause 2.1.14 (Vapaan modulin universaaliominaisuus). *Olkoon E vapaa A-moduli, $(a_i)_{i\in I}$ jokin sen kanta ja $(b_i)_{i\in I}$ perhe A-modulin F alkioita. Silloin on olemassa yksi ja vain yksi lineaarikuvaus $f\colon E \to F$, joka toteuttaa ehdot*

$$f(a_i) = b_i \qquad (i \in I).$$

Lisäksi f on

i) *injektiivinen* $\Leftrightarrow$ *perhe (b_i) on vapaa modulissa F,*
ii) *surjektiivinen* $\Leftrightarrow$ *perhe (b_i) virittää modulin F, ja*
iii) *bijektiivinen* $\Leftrightarrow$ *perhe (b_i) on modulin F kanta.*

Todistus. Olkoon $g\colon A^{(I)} \to E$ kannan (a_i) määräämä isomorfismi ja $h\colon A^{(I)} \to F$ perheen (b_i) määräämä lineaarikuvaus.

Jos $f\colon E \to F$ on homomorfismi ja kaikilla $i \in I$

$$f(a_i) = b_i,$$

niin

$$f \circ g\colon A^{(I)} \to F$$

$$\begin{tikzcd} A^{(I)} \arrow[rr, "h"] \arrow[dr, "g"'] & & F \\ & E \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

on homomorfismi, joka täyttää ehdot

$$(f \circ g)(e_i) = f(g(e_i)) = f(a_i) = b_i \quad (i \in I).$$

Toisaalta myös h täyttää samat ehdot, joten lauseen 2.1.11 nojalla

$$f \circ g = h.$$

Koska g on bijektiivinen, on

$$f = h \circ g^{-1}$$

siis yksikäsitteinen. Lisäksi tämä kaava määrittelee aina ehdot toteuttavan homomorfismin.

Viimeinen osa väitteistä seuraa siitä, että perheen (b_i) määräämä homomorfismi h on injektiivinen, surjektiivinen tai bijektiivinen, jos ja vain jos f on samanlainen g:n ollessa isomorfismi. $\square$

Harjoitustehtäviä

1) Olkoon A rengas ja E A-moduli. Osoitettava, että

i) kaikilla $\alpha \in A$ kuvaus $h_\alpha\colon x \mapsto \alpha x$ on E:n additiivisen ryhmän endomorfismi;

ii) kuvaus $\varphi\colon \alpha \mapsto h_\alpha$ on rengashomomorfismi renkaasta A additiivisen ryhmän E endomorfismien renkaaseen $\mathrm{End}(E)$;

iii) jos A on vaihdannainen, niin h_α on A-lineaarinen kaikilla $\alpha \in A$;

iv) $\mathrm{End}_A(E) = \mathrm{Hom}_A(E, E)$ on renkaan $\mathrm{End}(E)$ alirengas.

2) Olkoon M kunnan $\mathbf{Q}$ aliryhmä, joka on $\mathbf{Z}$-modulina äärellistyyppinen. Osoitettava, että $M = \mathbf{Z}x$ jollakin $x \in \mathbf{Q}$.

3) Vaihdannaisen ryhmän E alkio x on *torsioalkio*, jos $nx = 0$ jollakin kokonaisluvulla $n \neq 0$. Osoitettava:

i) $\mathbf{Z}$-moduli E, jossa on torsioalkio $x \neq 0$, ei ole vapaa.

ii) $\mathbf{Z}$-modulissa $\mathbf{Q}$ ei ole torsioalkiota $x \neq 0$, eli se on *torsioton*.

iii) $\mathbf{Q}$ ei ole vapaa $\mathbf{Z}$-moduli. (Vapaassa perheessä voi olla vain yksi alkio.)

Seuraavissa tehtävissä A on rengas ja E vasemmanpuolinen A-moduli.

4) Olkoon $f\colon E \to E$ idempotentti endomorfismi eli $f \circ f = f$. Osoitettava, että

i) $\mathrm{Ker}(f) = \mathrm{Im}(\mathrm{Id}_E - f)$,

ii) $E = \mathrm{Ker}(f) + \mathrm{Im}(f)$,

iii) $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = \{0\}$.

Pääteltävä, että kanoninen homomorfismi $g\colon \mathrm{Ker}(f) \oplus \mathrm{Im}(f) \to E$ on bijektiivinen.

5) Osoitettava, että $\mathrm{Hom}_A(E, A)$ on kaikkien kuvausten $f\colon E \to A$ muodostaman *oikeanpuolisen* A-modulin A^E alimoduli, ns. modulin E *duaali* E^*. (Jos $x \in E$, $x^* \in E^*$ ja $\alpha \in A$, niin $(x^*\alpha)(x) = (x^*(x))\alpha$. Usein merkitään $x^*(x) = \langle x, x^* \rangle$, ja tällöin $\langle x, x^*\alpha \rangle = \langle x, x^* \rangle \alpha$.)

6) Olkoon E vapaa, $(a_i)_{i \in I}$ jokin sen kanta ja $a_i^*\colon E \to A$ ehtojen $a_i^*(a_j) = \langle a_j, a_i^* \rangle = \delta_{ij}$ $(j \in I)$ määräämä lineaarikuvaus kaikilla $i \in I$. Osoitettava:

i) Jos $x^* \in E^*$ ja $(\lambda_i) \in A^{(I)}$, niin $x^* = \sum_{i \in I} a_i^* \lambda_i$, jos ja vain jos $\langle a_j, x^* \rangle = \lambda_j$ kaikilla $j \in I$. (Tutkitaan arvoja kannan alkioilla.)

ii) Perhe $(a_i^*)_{i \in I}$ on vapaa E^*:ssä.

iii) Jos I on äärellinen, niin $(a_i^*)_{i \in I}$ on E^*:n kanta, ns. kannan (a_i) *duaalinen kanta*.

7) Olkoon E vapaa vaihdannainen ryhmä eli $\mathbf{Z}$-moduli $\mathbf{Z}^{(\mathbf{N})}$, $(e_n)_{n\in\mathbf{N}}$ sen kanoninen kanta ja A endomorfismirengas $\mathrm{End}(E)$ (ei vaihdannainen). Olkoot u_1, u_2, v_1 ja $v_2 \in A$ ehtojen $u_1(e_{2n}) = e_n$, $u_1(e_{2n+1}) = 0$, $u_2(e_{2n}) = 0$, $u_2(e_{2n+1}) = e_n$, $v_1(e_n) = e_{2n}$, $v_2(e_n) = e_{2n+1}$ $(n \in \mathbf{N})$ määräämät lineaarikuvaukset. Osoitettava, että

i) $u_1v_1 = 1$, $u_1v_2 = 0$, $u_2v_1 = 0$, $u_2v_2 = 1$ (tarkastellaan arvoja kantavektoreilla) ja siten pari (u_1, u_2) on vapaa vasemmanpuolisessa A-modulissa A (kerrotaan relaatio $\lambda_1u_1 + \lambda_2u_2 = 0$ oikealta v_1:llä ja v_2:lla);

ii) $v_1u_1 + v_2u_2 = 1$, ja siten (u_1, u_2) virittää vasemmanpuolisen A-modulin A (eli u_1:n ja u_2:n virittämä vasemmanpuolinen ideaali on koko A).

Pääteltävä, että (u_1, u_2) on A:n kanta ja että kuvaus $(\lambda_1, \lambda_2) \mapsto \lambda_1u_1 + \lambda_2u_2$ on vasemmanpuolisten A-modulien isomorfismi $A^2 \to A$.

2.2. Tensoritulot

Bilineaariset kuvaukset. Olkoon A vaihdannainen rengas.

MÄÄRITELMÄ 2.2.1. Olkoot E, F ja G kolme A-modulia. Kuvaus $f\colon E \times F \to G$ on A-*bilineaarinen*, kun kaikilla x, x_1, $x_2 \in E$, y, y_1, $y_2 \in F$ ja $\lambda \in A$ pätee

i) $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$,
ii) $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$,
iii) $f(\lambda x, y) = f(x, \lambda y) = \lambda f(x, y)$.

Ehdot voidaan myös ilmaista sanomalla, että osittaiskuvaukset

$$f(\,\cdot\,, y)\colon E \to G, \quad x \mapsto f(x, y),$$

ja

$$f(x, \,\cdot\,)\colon F \to G, \quad y \mapsto f(x, y),$$

ovat A-lineaarisia kaikilla $x \in E$ ja $y \in F$.

Huomautus. Tulolla $E\times F$ on myös A-modulin struktuuri (tulomoduli), mutta bilineaarinen kuvaus $E \times F \to G$ ei ole yleensä lineaarinen.

Bilineaarinen kuvaus tulkitaan tavallisesti laskutoimitukseksi, *yleistetyksi kertolaskuksi.*

Esimerkkejä. 1) Vaihdannaisen renkaan A *kertolasku* on A-bilineaarinen kuvaus $A \times A \to A$. (Seuraa osittelulaeista ja vaihdannaisuudesta: $(\lambda x)y = x(\lambda y) = \lambda(xy)$, kun x, y, $\lambda \in A$.)

2) Reaalisen vektoriavaruuden $\mathbf{R}^n$ *sisätulo*

$$\mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}, \quad (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \cdot \mathbf{y},$$

on $\mathbf{R}$-bilineaarinen *muoto* (ts. sen arvot ovat kerroinkunnassa $\mathbf{R}$).

3) Avaruuden $\mathbf{R}^3$ *ristitulo*

$$\mathbf{R}^3 \times \mathbf{R}^3 \to \mathbf{R}^3, \quad (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \times \mathbf{y},$$

on $\mathbf{R}$-bilineaarinen kuvaus.

4) Reaalisten $n \times n$-matriisien *matriisitulo*

$$\mathbf{M}_n(\mathbf{R}) \times \mathbf{M}_n(\mathbf{R}) \mapsto \mathbf{M}_n(\mathbf{R}), \quad (X, Y) \mapsto XY,$$

on $\mathbf{R}$-bilineaarinen kuvaus. (Mutta ei $\mathbf{M}_n(\mathbf{R})$-bilineaarinen, kun $n > 1$, vaikka $\mathbf{M}_n(\mathbf{R})$ onkin rengas.)

Yleisemmin, jos A on vaihdannainen rengas ja $\mathbf{M}_{m,n}(A)$ on A-kertoimisten $m \times n$-matriisien moduli, niin matriisitulo

$$\mathbf{M}_{m,p}(A) \times \mathbf{M}_{p,n}(A) \to \mathbf{M}_{m,n}(A)$$

on A-bilineaarinen kuvaus.

Jos A on kokonaislukujen rengas $\mathbf{Z}$, niin määritelmän ehto iii)

$$f(nx, y) = f(x, ny) = nf(x, y), \quad n \in \mathbf{Z},$$

seuraa ehdoista i) ja ii) (vaihdannaisten ryhmien homomorfismi on $\mathbf{Z}$-lineaarinen). Kuvaus f on siis $\mathbf{Z}$-bilineaarinen, jos ja vain jos se täyttää ehdot i) ja ii) eli on *biadditiivinen.*

Esimerkki 5) Jos A on rengas (ei välttämättä vaihdannainen) ja E on A-moduli, niin endomorfismirenkaan $\mathrm{End}_A(E)$ kertolasku

$$\mathrm{End}(E) \times \mathrm{End}(E) \to \mathrm{End}(E), \quad (f, g) \mapsto fg = f \circ g,$$

on biadditiivinen kuvaus (osittelulait, ks. esim. 1.7.1). Se on siten myös $\mathbf{Z}$-bilineaarinen kuvaus.

Olkoon A vaihdannainen rengas ja olkoot E, F, G kolme A-modulia. Kaikkien kuvausten

$$f \colon E \times F \to G$$

joukko on A-moduli, tulomoduli $G^{E \times F}$, ja A-bilineaaristen kuvausten muodostama osajoukko

$$\mathcal{L}_2(E, F; G)$$

on sen alimoduli (harj. teht.).

LEMMA 2.2.2. *Olkoon $f \colon E \times F \to G$ A-bilineaarinen kuvaus. Jos $(a_i)_{i \in I} \in E^I$, $(b_i)_{j \in J} \in F^J$, $(\lambda_i)_{i \in I} \in A^{(I)}$ ja $(\mu_j)_{j \in J} \in A^{(J)}$, niin*

$$f(\sum_{i \in I} \lambda_i a_i, \sum_{j \in J} \mu_j b_j) = \sum_{(i,j) \in I \times J} \lambda_i \mu_j f(a_i, b_j).$$

Todistus. Olkoon $x = \sum_{i \in I} \lambda_i a_i \in E$ ja $y = \sum_{j \in J} \mu_j b_j \in F$. Tällöin

$$f(x, y) = \sum_{i \in I} \lambda_i f(a_i, y),$$

koska osittaiskuvaus $f(\,\cdot\,, y)$ on A-lineaarinen. Koska jokainen osittaiskuvaus $f(a_i, \,\cdot\,)$ on myös A-lineaarinen, saadaan edelleen

$$f(x, y) = \sum_{i \in I} \lambda_i \sum_{j \in J} \mu_j f(a_i, b_j),$$

ja väite seuraa, kun kaksoissumma kirjoitetaan yhdeksi summaksi. $\square$

LAUSE 2.2.3. *Olkoot E ja F kaksi vapaata A-modulia, $(a_i)_{i\in I}$ modulin E kanta, $(b_j)_{j\in J}$ modulin F kanta, G jokin A-moduli ja $(c_{ij})_{(i,j)\in I\times J}$ perhe G:n alkioita. Silloin on olemassa yksi ja vain yksi A-bilineaarinen kuvaus $f\colon E\times F\to G$, joka toteuttaa ehdot*

$$f(a_i, b_j) = c_{ij} \qquad (i\in I, j\in J).$$

Todistus. Kaikilla alkioilla $x\in E$ ja $y\in F$ on yksikäsitteiset esitykset

$$x=\sum_{i\in I}\lambda_i a_i, \quad y=\sum_{j\in J}\mu_j b_j,$$

missä $(\lambda_i)\in A^{(I)}$ ja $(\mu_j)\in A^{(J)}$. Jos $f\colon E\times F\to G$ on ehdot täyttävä bilineaarinen kuvaus, niin lemman 2.2.2 mukaan sen arvo

$$f(x,y)=\sum_{(i,j)\in I\times J}\lambda_i\mu_j c_{ij}$$

on yksikäsitteisesti määrätty.

Kääntäen tämä kaava määrittelee ehdot täyttävän kuvauksen kaikilla modulin G perheillä $(c_{ij})_{(i,j)\in I\times J}$ (harj. teht.). □

Esimerkki 6) Olkoon $(\mathbf{e}_i)_{1\le i\le n}$ avaruuden $\mathbf{R}^n$ standardikanta. Tällöin on olemassa yksikäsitteinen $\mathbf{R}$-bilineaarinen muoto

$$f\colon \mathbf{R}^n\times\mathbf{R}^n\to\mathbf{R},$$

joka täyttää ehdot

$$f(\mathbf{e}_i,\mathbf{e}_j)=\mathbf{e}_i\cdot\mathbf{e}_j=\delta_{ij} \qquad (1\le i\le n, 1\le j\le n),$$

ja tämä muoto on tavallinen sisätulo $f(\mathbf{x},\mathbf{y})=\mathbf{x}\cdot\mathbf{y}$.

Tensoritulon konstruktio. Olkoon A vaihdannainen rengas ja olkoot E, F kaksi A-modulia. Tarkastellaan A-bilineaarisia kuvauksia $f\colon E\times F\to G$, missä G on jokin A-moduli. Jos E ja F ovat vapaita, lause 2.2.3 osoittaa, miten tällaiset kuvaukset voidaan saada. Tavoitteena on löytää vastaava yleiseen tilanteeseen soveltuva menettely.

Osoitetaan aluksi, että on olemassa yleisin mahdollinen A-bilineaarinen "tulo"

$$\varphi\colon E\times F\to G, \quad (x,y)\mapsto x\otimes y,$$

joka toteuttaa välttämättömät ehdot

$$\begin{aligned}(x_1+x_2)\otimes y &= x_1\otimes y + x_2\otimes y,\\ x\otimes(y_1+y_2) &= x\otimes y_1 + x\otimes y_2,\\ (\lambda x)\otimes y &= x\otimes(\lambda y)=\lambda(x\otimes y),\end{aligned} \tag{1}$$

kun x, x_1, $x_2\in E$, y, y_1, $y_2\in F$ ja $\lambda\in A$, ja niistä johtuvat yhtälöt, mutta ei muita ehtoja.

Olkoon C vapaa A-moduli $A^{(E\times F)}$, jonka indeksijoukkona on tulojoukko $E\times F$. Sen alkiot ovat äärelliskantajaiset A:n alkioperheet

$$(\xi_{xy})_{(x,y)\in E\times F},$$

ja sillä on kanoninen kanta

$$(e_{xy})_{(x,y)\in E\times F},$$

missä perheen e_{xy} ainoa nollasta eroava jäsen on 1 indeksillä (x,y).

Merkintöjen yksinkertaistamiseksi samastetaan kannan alkiot e_{xy} vastaavien parien $(x,y)\in E\times F$ kanssa. Tällöin jokaiselle C:n alkiolle saadaan yksikäsitteinen esitys kannan alkioiden avulla

$$(\xi_{xy}) = \sum_{(x,y)\in E\times F} \xi_{xy}(x,y).$$

Tällaista esitystä sanotaan parien (x,y) *muodolliseksi A-kertoimiseksi yhdistelmäksi.*

Olkoon G A-moduli. Jokaista kuvausta

$$f\colon E\times F\to G$$

vastaa perheen $(f(x,y))_{(x,y)\in E\times F}$ määräämä lineaarikuvaus

$$\bar f\colon C\to G,$$

joka toteuttaa ehdot (ks. lause 2.1.11)

$$\bar f((x,y)) = \bar f(e_{xy}) = f(x,y) \qquad (x\in E, y\in F)$$

ja yleisesti

$$\bar f\Big(\sum_{x,y}\xi_{xy}(x,y)\Big) = \sum_{x,y}\xi_{xy} f(x,y).$$

Kuvaus f on tällöin A-bilineaarinen, jos ja vain jos $\bar f$ saa arvon 0 kaikilla C:n alkioilla

$$\text{(2)} \qquad \begin{cases} (x_1+x_2,y)-(x_1,y)-(x_2,y),\\ (x,y_1+y_2)-(x,y_1)-(x,y_2),\\ (\lambda x,y)-\lambda(x,y),\\ (x,\lambda y)-\lambda(x,y), \end{cases}$$

missä x, x_1, $x_2\in E$, y, y_1, $y_2\in F$ ja $\lambda\in A$, eli yhtäpitävästi, jos ja vain jos homomorfismin $\bar f$ ydin $\operatorname{Ker}(\bar f)$ sisältää alkioiden (2) virittämän C:n alimodulin D.

Tämä taas merkitsee hajotuslauseen 2.1.6 mukaan, että homorfismilla $\bar f$ on hajotelma

$$\bar f = g\circ\psi\colon C\to C/D\to G,$$

missä $\psi\colon C\to C/D$ on kanoninen homomorfismi tekijämodulille ja $g\colon C/D\to G$ on jokin A-lineaarinen kuvaus.

MÄÄRITELMÄ 2.2.4. Olkoot E ja F kaksi A-modulia. Vapaan modulin $C = A^{(E\times F)}$ tekijämodulia C/D alkioiden (2) virittämän alimodulin D suhteen sanotaan modulien E ja F *tensorituloksi* ja sille käytetään merkintää $E\otimes_A F$.

Jokainen pari $(x, y) \in E \times F$ voidaan tulkita C:n kanta-alkioksi ja sen kanoninen kuva

$$x \otimes y \in E \otimes_A F$$

on *alkioiden* $x \in E$ ja $y \in F$ *tensoritulo*. Nämä toteuttavat ehdot (1), koska yhdistelmät (2) kuvautuvat modulin $E \otimes_A F$ nolla-alkiolle.

Kanoninen kuvaus

$$\varphi\colon E \times F \to E \otimes_A F, \quad (x, y) \mapsto x \otimes y,$$

on siten A-bilineaarinen.

Huomautus. Koska kannan alkiot $(x, y) = e_{xy}$ $(x \in E, y \in F)$ virittävät modulin C, niiden kuvat $x \otimes y$ virittävät tekijämodulin C/D. Jokainen $z \in E \otimes_A F$ on siten äärellinen summa (ks. lause 2.1.5)

$$z = \sum_{i \in I} \lambda_i (x_i \otimes y_i),$$

missä $\lambda_i \in A$, $x_i \in E$ ja $y_i \in F$ $(i \in I)$. Lisäksi voidaan valita $\lambda_i = 1$ $(i \in I)$, koska $\lambda_i(x_i \otimes y_i) = (\lambda_i x_i) \otimes y_i$. Tensoritulon $E \otimes_A F$ alkiot voidaan siis esittää muodossa

$$z = \sum_{i \in I} x_i \otimes y_i,$$

missä $x_i \in E$, $y_i \in F$ $(i \in I)$ ja I on äärellinen. Esitys ei kuitenkaan ole yksikäsitteinen.

LAUSE 2.2.5 (Tensoritulon universaaliominaisuus). *Olkoot E, F ja G kolme A-modulia.*

i) *Jos $g\colon E \otimes_A F \to G$ on lineaarikuvaus, niin*

$$(x, y) \mapsto f(x, y) = g(x \otimes y)$$

on A-bilineaarinen kuvaus $f\colon E \times F \to G$.

ii) *Jos $f\colon E \times F \to G$ on A-bilineaarinen kuvaus, niin on olemassa yksi ja vain yksi lineaarikuvaus $g\colon E \otimes_A F \to G$, joka kaikilla $x \in E$ ja $y \in F$ täyttää ehdon*

$$f(x, y) = g(x \otimes y).$$

$$\begin{tikzcd}
E \times F \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & G \\
& E \otimes_A F \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

Todistus. i) Kuvaus $f\colon (x, y) \mapsto g(x \otimes y)$ on kanonisen kuvauksen $\varphi\colon (x, y) \mapsto x \otimes y$ ja lineaarikuvauksen g yhdistelmä

$$f = g \circ \varphi.$$

Koska φ on A-bilineaarinen, osittaiskuvaukset

$$f(\,\cdot\,, y) = g \circ \varphi(\,\cdot\, \otimes y) \quad \text{ja} \quad f(x, \,\cdot\,) = g \circ \varphi(x, \,\cdot\,)$$

ovat lineaariset kaikilla $x \in E$ ja $y \in F$. Kuvaus f on siten A-bilineaarinen.

ii) Kääntäen, jos $f\colon E \times F \to G$ on A-bilineaarinen kuvaus, niin perheen $(f(x,y))_{(x,y)\in E\times F}$ määräämällä lineearikuvauksella

$$\bar{f}\colon C = A^{(E\times F)} \to G$$

on edellä esitetyin merkinnöin ja perusteluin hajotelma

$$\bar{f}\colon C \xrightarrow{\psi} C/D \xrightarrow{g} G,$$

missä ψ on kanoninen homomorfismi ja $C/D = E \otimes_A F$.

Tällöin kaikilla $x \in E$ ja $y \in F$ pätee

$$g(x\otimes y) = g(\psi((x,y))) = \bar{f}((x,y)) = f(x,y)$$

ja lisäksi g on yksikäsitteinen, koska $\bar{f}$ on yksikäsitteinen ja ψ on surjektiivinen. □

Esimerkki 7) Tensoritulo $(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z})$ on $\{0\}$, kun m, $n \in \mathbf{N}$ ovat keskenään jaottomat, ja siten kaikilla $\mathbf{Z}$-moduleilla G on 0-kuvaus ainoa $\mathbf{Z}$-bilineaarinen kuvaus

$$(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}) \to G.$$

Todistus. On olemassa sellaiset luvut a, $b \in \mathbf{Z}$, että

$$am + bn = 1.$$

(*Bezout'n kaava*; voidaan löytää Eukleideen algoritmilla.) Tensoritulon virittäjät ovat silloin

$$\begin{aligned} x\otimes y = 1(x\otimes y) &= am(x\otimes y) + bn(x\otimes y)\\ &= (amx)\otimes y + x\otimes(bny)\\ &= 0\otimes y + x\otimes 0 = 0, \end{aligned}$$

koska $mx = 0$ ja $ny = 0$, ja siten koko tensoritulo on $\{0\}$. □

Huomautus. Lineaarikuvaus $g\colon E\otimes_A F \to G$ esitetään usein kaavalla

$$g(\sum_i x_i \otimes y_i) = \sum_i f(x_i, y_i),$$

missä $f(x,y)$ on jokin x:n ja y:n lauseke. Lukijalle jää osoitettavaksi, että g on hyvin määritelty, eli

$$\text{jos } \sum_i x_i\otimes y_i = \sum_k x'_k \otimes y'_k, \text{ niin } \sum_i f(x_i,y_i) = \sum_k f(x'_k, y'_k).$$

Oikea tapa tämän todistamiseksi on näyttää, että

$$E\times F \to G, \quad (x,y)\mapsto f(x,y)$$

on A-bilineaarinen kuvaus.

Seuraavassa tuloksessa esiintyy tensoritulon universaaliominaisuus toisessa muodossa.

KOROLLAARI 2.2.6. *Olkoot E, F ja H kolme A-modulia ja olkoon $h\colon E \times F \to H$ A-bilineaarinen kuvaus, joka toteuttaa ehdot*

i) *$h(E \times F)$ virittää modulin H, ja*

ii) *jos G on A-moduli ja $f : E \times F \to G$ on A-bilineaarinen kuvaus, niin on olemassa A-lineaarinen kuvaus $g\colon H \to G$, jolla pätee*

$$f = g \circ h.$$

$$\begin{tikzcd} E \times F \arrow[rr, "f"] \arrow[dr, "h"'] & & G \\ & H \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Tällöin on olemassa yksikäsitteinen isomorfismi $\theta\colon E \otimes_A F \xrightarrow{\sim} H$, joka täyttää ehdon $h = \theta \circ \varphi$.

Todistus. Koska h on A-bilineaarinen, on lauseen 2.2.5 kohdan ii) mukaan olemassa yksikäsitteinen homomorfismi

$$\theta\colon E \otimes_A F \to H,$$

joka toteuttaa ehdon

$$h = \theta \circ \varphi.$$

$$\begin{tikzcd} E \times F \arrow[rr, "h"] \arrow[dr, "\varphi"'] & & H \\ & E \otimes_A F \arrow[ur, dashed, "\theta"'] & \end{tikzcd}$$

On osoitettava, että θ on bijektiivinen.

Koska φ on myös A-bilineaarinen, on ehdon ii) nojalla olemassa homomorfismi

$$g\colon H \to E \otimes_A F,$$

joka täyttää ehdon

$$\varphi = g \circ h.$$

$$\begin{tikzcd} E \times F \arrow[rr, "\varphi"] \arrow[dr, "h"'] & & E \otimes_A F \\ & H \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Tällöin yhdistetty kuvaus $g \circ \theta$ on lineaarinen ja

$$(g \circ \theta) \circ \varphi = g \circ h = \varphi = \mathrm{Id}_{E \otimes_A F} \circ \varphi.$$

$$\begin{tikzcd} E \times F \arrow[rr, "\varphi"] \arrow[dr, "\varphi"'] & & E \otimes_A F \\ & E \otimes_A F \arrow[ur, "g \circ \theta"'] & \end{tikzcd}$$

Lauseen 2.2.5 kohdassa ii) esitetyn yksikäsitteisyyden perusteella on silloin voimassa

$$g \circ \theta = \mathrm{Id}_{E \otimes_A F}.$$

Vastaavasti $\theta \circ g$ on A-homomorfismi ja

$$(\theta \circ g) \circ h = \theta \circ \varphi = h = \mathrm{Id}_H \circ h.$$

$$\begin{tikzcd} E \times F \arrow[rr, "h"] \arrow[dr, "h"'] & & H \\ & H \arrow[ur, "\theta \circ g"'] & \end{tikzcd}$$

Tämä merkitsee, että

$$\theta \circ g = \mathrm{Id}_H$$

pätee kuvassa $h(E \times F)$ ja siksi ehdon i) nojalla koko modulissa H. Siis nähdään, että θ:lla on käänteiskuvaus g. $\square$

Tulos voidaan tulkita sanomalla, että jos moduleilla H ja $E \otimes_A F$ on sama universaaliominaisuus, niin ne ovat isomorfiset. Tämä merkitsee, että tensorituloa käsiteltäessä on harvoin tarpeen palata sen konstruktioon. Pelkkä universaaliominaisuus riittää.

Esimerkki 8) Olkoot $E = A^m = A^I$ ja $F = A^n = A^J$, missä $I = \{1, 2, \dots, m\}$ ja $J = \{1, 2, \dots, n\}$, sekä

$$H = A^{I\times J} = \mathbf{M}_{m,n}(A)$$

A-kertoimisten $m \times n$-matriisien $(a_{ij})_{(i,j)\in I\times J}$ muodostama moduli.

Kuvaus

$$h\colon A^m \times A^n \to \mathbf{M}_{m,n}(A), \quad ((x_i), (y_j)) \mapsto (x_i y_j)$$

on tällöin A-bilineaarinen (vektorien ns. *dyaditulo*). Sen kuva sisältää kaikki matriisit

$$h(e_i, e_j) = E_{ij}, \quad (i \in I, j \in J),$$

joissa on 1 rivillä i sarakkeessa j ja muualla 0. Jokainen matriisi on tällaisten lineaarinen yhdistelmä

$$(a_{ij}) = \sum_{i\in I, j\in J} a_{ij} E_{ij},$$

joten kuva $h(A^m \times A^n)$ virittää koko matriisimodulin $\mathbf{M}_{m,n}(A)$.

Osoitetaan, että korollaarin 2.2.6 ehto ii) on myös voimassa. Olkoon G jokin A-moduli ja $f\colon A^m \times A^n \to G$ A-bilineaarinen kuvaus. Olkoon

$$g\colon \mathbf{M}_{m,n}(A) = A^{(I\times J)} \to G$$

perheen $(f(e_i, e_j))_{(i,j)\in I\times J}$ määräämä lineaarikuvaus, joka täyttää ehdot

$$g(E_{ij}) = f(e_i, e_j) \qquad (i \in I, j \in J).$$

(Ks. lause 2.1.11; (E_{ij}) on kanoninen kanta.)

Tällöin kaikilla $i \in I$ ja $j \in J$ pätee

$$(g \circ h)(e_i, e_j) = g(h(e_i, e_j)) = f(e_i, e_j),$$

joten lauseen 2.2.3 nojalla

$$g \circ h = f.$$

Siis on olemassa kanoninen isomorfismi

$$A^m \otimes_A A^n \xrightarrow{\sim} \mathbf{M}_{m,n}(A).$$

Tensoritulon ominaisuuksia. Olkoon A vaihdannainen rengas.

LAUSE 2.2.7. *Olkoot E ja F kaksi vapaata A-modulia, $(a_i)_{i\in I}$ jokin E:n kanta ja $(b_k)_{k\in K}$ jokin F:n kanta. Tällöin $E \otimes_A F$ on vapaa A-moduli ja $(a_i \otimes b_k)_{(i,k)\in I\times K}$ on sen kanta.*

Todistus. Alkioilla $x \in E$ ja $y \in F$ on yksikäsitteiset esitykset

$$x = \sum_{i\in I} \xi_i a_i, \quad y = \sum_{k\in K} \eta_k b_k,$$

missä $(\xi_i) \in A^{(I)}$ ja $(\eta_k) \in A^{(K)}$. Niiden tensoritulo voidaan siis esittää lineaarisena yhdistelmänä

$$x \otimes y = \sum_{i,k} (\xi_i a_i) \otimes (\eta_k b_k) = \sum_{i,k} \xi_i \eta_k (a_i \otimes b_k).$$

Koska tulot $x \otimes y$ virittävät tensoritulon $E \otimes_A F$, on $(a_i \otimes b_k)_{(i,k) \in I \times K}$ myös sen virittäjäperhe.

Olkoon

$$\sum_{(i,k) \in I \times K} \lambda_{ik}(a_i \otimes b_k) = 0, \qquad (\lambda_{ik}) \in A^{(I \times K)}, \tag{3}$$

jokin lineaarinen relaatio. Osoitetaan, että relaatio on triviaali.

Olkoon $(j,l) \in I \times K$. Lemman 2.2.2 nojalla on olemassa A-bilineaarinen muoto $f\colon E \times F \to A$, jonka määrittelevät ehdot

$$\begin{aligned} &f(a_j, b_l) = 1, \\ &f(a_i, b_k) = 0, \quad \text{kun } (i,k) \neq (j,l). \end{aligned}$$

Vastaava lineaarimuoto $g\colon E \otimes_A F \to A$ (ks. lause 2.2.5) toteuttaa silloin yhtälöt

$$\begin{aligned} &g(a_j \otimes b_l) = 1, \\ &g(a_i \otimes b_k) = 0, \quad \text{kun } (i,k) \neq (j,l). \end{aligned}$$

Soveltamalla kuvausta g lineaariseen relaatioon (3) saadaan

$$0 = g\Big(\sum_{i,k} \lambda_{ik}(a_i \otimes b_k)\Big) = \sum_{i,k} \lambda_{ik} g(a_i \otimes b_k) = \lambda_{jl}.$$

Koska pari $(j,l) \in I \times K$ on mielivaltainen, virittäjäperhe $(a_i \otimes b_k)$ on myös vapaa. □

Huomautus. Tätä lausetta voidaan soveltaa aina, kun kerroinrengas A on kunta, koska jokaisella vektoriavaruudella on kanta.

LAUSE 2.2.8. *Jos E on A-moduli, niin kuvaus $x \mapsto 1 \otimes x$ on isomorfismi*

$$h\colon E \xrightarrow{\sim} A \otimes_A E,$$

ja sen käänteiskuvaus g toteuttaa kaikilla $\lambda \in A$ ja $x \in E$ ehdon

$$g(\lambda \otimes x) = \lambda x.$$

Todistus. Kuvaus h on lineaarinen, koska tensoritulo on bilineaarinen. Toisaalta kuvaus

$$f\colon A \times E \to E, \quad (\lambda, x) \mapsto \lambda x,$$

on A-bilineaarinen modulin osittelulakien ja A:n vaihdannaisuuden nojalla. Vastaava lineaarikuvaus

$$g\colon A \otimes_A E \to E$$

toteuttaa silloin kaikilla $\lambda \in A$ ja $x \in E$ ehdon

$$g(\lambda \otimes x) = \lambda x.$$

Erityisesti kaikilla $x \in E$ saadaan yhtälöt

$$(g \circ h)(x) = g(1 \otimes x) = x$$

ja

$$(h \circ g)(1 \otimes x) = h(x) = 1 \otimes x.$$

Koska alkiot $1 \otimes x$ virittävät modulin $A \otimes_A E$ ($\lambda \otimes x = 1 \otimes \lambda x$), g on h:n käänteiskuvaus. □

Esimerkki 9) Olkoon E vapaa A-moduli ja $(a_i)_{i \in I}$ jokin sen kanta. Koska A on myös vapaa, kantana perhe (1), on $(1 \otimes a_i)_{i \in I}$ lauseen 2.2.7 mukaan modulin $A \otimes_A E$ kanta.

Lauseen 2.2.8 isomorfismi $E \xrightarrow{\sim} A \otimes_A E$ on silloin kantojen bijektion $a_i \mapsto 1 \otimes a_i$ määrittelemä lineaarikuvaus (ks. lause 2.1.14).

LAUSE 2.2.9. *Olkoon E ja F kaksi A-modulia. On olemassa yksikäsitteinen isomorfismi*

$$\sigma\colon E \otimes_A F \xrightarrow{\sim} F \otimes_A E,$$

joka toteuttaa ehdot

$$\sigma(x \otimes y) = y \otimes x \qquad (x \in E, y \in F).$$

Todistus. Kuvaus

$$f\colon E \times F \to F \otimes_A E, \quad (x, y) \mapsto y \otimes x,$$

on A-bilineaarinen, ja sitä vastaa ehdot täyttävä homomorfismi

$$\sigma\colon E \otimes_A F \to F \otimes_A E.$$

Samoin on olemassa lineaarikuvaus

$$\tau\colon F \otimes_A E \to E \otimes_A F,$$

joka toteuttaa ehdot

$$\tau(y \otimes x) = x \otimes y, \qquad (x \in E, y \in F).$$

Tällöin kaikilla $x \in E$ ja $y \in F$ pätee

$$(\tau \circ \sigma)(x \otimes y) = x \otimes y,$$

ja siten

$$\tau \circ \sigma = \mathrm{Id}_{E \otimes_A F},$$

koska alkiot $x \otimes y$ virittävät modulin $E \otimes_A F$.

Vastaavasti todistetaan $\sigma \circ \tau = \mathrm{Id}_{F \otimes_A E}$. Lineaarikuvaus σ on siten isomorfismi. □

Esimerkki 10) Jos E ja F ovat vapaita A-moduleita ja niillä on kannat $(a_i)_{i \in I}$ ja $(b_k)_{k \in K}$, niin $E \otimes_A F$ ja $F \otimes_A E$ ovat myös vapaita (ks. lause 2.2.7) ja niiden kannat $(a_i \otimes b_k)$ ja $(b_k \otimes a_i)$ vastaavat toisiaan kanonisesti.

Lause 2.2.10. *Olkoot E, F ja G kolme A-modulia. On olemassa yksikäsitteinen isomorfismi*

$$\varphi\colon (E \otimes_A F) \otimes_A G \xrightarrow{\sim} E \otimes_A (F \otimes_A G),$$

joka kaikilla $x \in E$, $y \in F$ ja $z \in G$ toteuttaa ehdon

$$\varphi((x \otimes y) \otimes z) = x \otimes (y \otimes z).$$

Todistus. Koska tensoritulon $E \otimes_A F$ alkiot voidaan esittää äärellisinä summina

$$t = \sum_i x_i \otimes y_i, \quad x_i \in E,\ y_i \in F,$$

ja alkiot

$$t \otimes z = \sum_i (x_i \otimes y_i) \otimes z, \quad z \in G,$$

virittävät modulin $(E \otimes_A F) \otimes_A G$, voidaan kaikki sen alkiot esittää alkioiden $(x \otimes y) \otimes z$ ($x \in E$, $y \in F$, $z \in G$) summina. Jos ehdot täyttävä lineaarikuvaus φ on olemassa, se on siis välttämättä yksikäsitteinen.

Olemassaolon todistamiseksi valitaan aluksi jokin $z \in G$. Tällöin $y \mapsto y \otimes z$ on A-lineaarinen kuvaus

$$h_z\colon F \to F \otimes_A G,$$

ja siksi $(x, y) \mapsto x \otimes h_z(y) = x \otimes (y \otimes z)$ on A-bilineaarinen kuvaus

$$E \times F \to E \otimes_A (F \otimes_A G).$$

Vastaava A-lineaarinen kuvaus

$$g_z\colon E \otimes_A F \to E \otimes_A (F \otimes_A G)$$

toteuttaa ehdot

$$g_z(x \otimes y) = x \otimes (y \otimes z) \qquad (x \in E, y \in F).$$

Näin saadaan hyvin määritelty kuvaus

$$g\colon (E \otimes_A F) \times G \to E \otimes_A (F \otimes_A G), \quad (t, z) \mapsto g_z(t).$$

Osoitetaan, että g on A-bilineaarinen. Ensimmäinen osittaiskuvaus

$$t \mapsto g(t, z) = g_z(t)$$

on lineaarinen kaikilla $z \in G$ suoraan konstruktion perusteella.

Olkoot sitten z, z' kaksi G:n alkiota. Tällöin kaikilla $x \in E$ ja $y \in F$ saadaan

$$\begin{aligned}
g_{z+z'}(x \otimes y) &= x \otimes (y \otimes (z + z')) \\
&= x \otimes (y \otimes z + y \otimes z') \\
&= x \otimes (y \otimes z) + x \otimes (y \otimes z') \\
&= g_z(x \otimes y) + g_{z'}(x \otimes y),
\end{aligned}$$

joten lineaarisuuden nojalla

$$g_{z+z'}(t) = g_z(t) + g_{z'}(t)$$

pätee kaikilla summilla $t = \sum_i x_i \otimes y_i \in E \otimes_A F$. Näin saadaan

$$g(t, z + z') = g(t, z) + g(t, z'),$$

ja samalla tavoin todistetaan

$$g(t, \lambda z) = \lambda g(t, z)$$

päteväksi kaikilla $t \in E \otimes_A F$, $\lambda \in A$ ja $z \in G$.

Kuvaus g on siis A-bilineaarinen. Olkoon

$$\varphi\colon (E \otimes_A F) \otimes_A G \to E \otimes_A (F \otimes_A G)$$

vastaava A-lineaarinen kuvaus. Se toteuttaa kaikilla $x \in E$, $y \in F$ ja $z \in G$ vaaditun ehdon

$$\varphi((x \otimes y) \otimes z) = g(x \otimes y, z) = g_z(x \otimes y) = x \otimes (y \otimes z).$$

Vastaavalla tavalla konstruoidaan A-lineaarinen kuvaus

$$\psi\colon E \otimes_A (F \otimes_A G) \to (E \otimes_A F) \otimes_A G,$$

jolla pätevät ehdot

$$\psi(x \otimes (y \otimes z)) = (x \otimes y) \otimes z.$$

Yhdistetyt kuvaukset $\psi \circ \varphi$ ja $\varphi \circ \psi$ kuvaavat silloin modulien virittäjät

$$(x \otimes y) \otimes z \quad \text{ja} \quad x \otimes (y \otimes z)$$

itselleen, joten ne ovat identtisiä kuvauksia. Homomorfismi φ on siis isomorfismi. $\square$

Yhteenveto. Modulien tensoritulo muistuttaa laskutoimitusta, joka on liitännäinen (lause 2.2.10) ja vaihdannainen (lause 2.2.9) ja jossa moduli A toimii neutraalialkiona (lause 2.2.8). Samoin kuin vaihdannaisten monoidien teoriassa voidaan siten määritellä (isomorfiaa vaille) äärellisen monen A-modulin E_1, E_2, $\ldots$, E_n tensoritulo

$$E_1 \otimes_A E_2 \otimes_A \cdots \otimes_A E_n = \bigotimes_{i=1}^{n} E_i = \bigotimes_{1 \le i \le n} E_i,$$

ja erityisesti modulin E *tensoripotenssit* $E^{\otimes n}$ ($n \in \mathbf{N}$, $E^{\otimes 0} = A$).

Harjoitustehtäviä

1) Kompleksilukujen kunta $\mathbf{C}$ on reaalinen vektoriavaruus. Osoitettava, että

i) on olemassa yksikäsitteinen $\mathbf{R}$-lineaarinen kuvaus

$$\varphi\colon \mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \to \mathbf{C} \otimes_{\mathbf{C}} \mathbf{C},$$

joka vie alkioiden tensoritulot $z_1 \otimes z_2 \in \mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$ vastaaville tuloille $z_1 \otimes z_2 \in \mathbf{C} \otimes_{\mathbf{C}} \mathbf{C}$;

ii) kuvaus φ on surjektiivinen mutta ei injektiivinen.

2) Olkoon M $\mathbf{Z}$-moduli, jonka jokainen alkio on torsioalkio. (Esimerkiksi M on äärellinen vaihdannainen ryhmä.) Osoitettava, että

$$M \otimes_{\mathbf{Z}} \mathbf{Q} = \{0\}.$$

3) Tarkastellaan $\mathbf{Z}$-modulien tensorituloa $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q}$. Osoitettava, että

i) on olemassa yksikäsitteinen $\mathbf{Z}$-lineaarinen kuvaus $\varphi\colon \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{Q}$, joka vie tulot $x \otimes y \in \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q}$ tuloille $xy \in \mathbf{Q}$;

ii) $x \otimes 1 = 1 \otimes x$ modulissa $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q}$ kaikilla $x \in \mathbf{Q}$;

iii) kuvaus $\psi\colon x \to x \otimes 1$ on φ:n käänteiskuvaus.

4) Olkoon A vaihdannainen rengas, E vapaa A-moduli, $(e_i)_{i \in I}$ jokin sen kanta ja $(e_i^*)_{i \in I}$ ehtojen $e_i^*(e_j) = \langle e_j, e_i^* \rangle = \delta_{ij}$ $(i,\, j \in I)$ määräämä perhe lineaarikuvauksia $E \to A$. Olkoon F A-moduli. Osoitettava, että

i) jokaiseen indeksiin $i \in I$ liittyy yksikäsitteinen homomorfismi

$$g_i\colon E \otimes_A F \to F,$$

jolla $g_i(x \otimes y) = \langle x, e_i^* \rangle y$ kaikilla $x \in E$ ja $y \in F$;

ii) jos $t = \sum_i e_i \otimes y_i$, missä $(y_i) \in F^{(I)}$, niin $g_i(t) = y_i$ kaikilla $i \in I$;

iii) jos $t \in E \otimes_A F$, niin $g_i(t) = 0$ melkein kaikilla $i \in I$ ja $t = \sum_i e_i \otimes g_i(t)$ (aluksi $t = x \otimes y$, $x = \sum_i \lambda_i e_i$).

Pääteltävä, että jokaisella tensorilla $t \in E \otimes_A F$ on yksikäsitteinen esitys $t = \sum_i e_i \otimes y_i$, missä $(y_i) \in F^{(I)}$.

2.3. Algebrat

Olkoon A vaihdannainen rengas.

MÄÄRITELMÄ 2.3.1. A-*algebra* on joukko E varustettuna

i) A-modulin struktuurilla ja

ii) A-bilineaarisella kuvauksella

$$E \times E \to E, \quad (x, y) \mapsto x.y \text{ (tai } xy),$$

jota sanotaan algebran E *kertolaskuksi.*

Koska bilineaarinen kuvaus on biadditiivinen, A-algebran E kertolasku on osittelева yhteenlaskun suhteen. Sen ei kuitenkaan tarvitse olla liitännäinen. Lisäksi kertolasku toteuttaa ehdot

$$(\alpha x)y = x(\alpha y) = \alpha(xy) \qquad (\alpha \in A,\ x, y \in E).$$

A-algebraa E sanotaan *liitännäiseksi* tai *vaihdannaiseksi*, jos sen kertolasku on liitännäinen tai vaihdannainen. Jos E:n kertolaskulla on neutraalialkio, eli *ykkösalkio* e, niin se on yksikäsitteinen (kuten kaikissa magmoissa) ja algebraa sanotaan *ykköselliseksi.*

Esimerkkejä. 1) A-moduli A kertolaskullaan varustettuna (esim 2.2.1) on liitännäinen, vaihdannainen ja ykkösellinen A-algebra.

2) A-kertoimisten $n \times n$-matriisien rengas $\mathbf{M}_n(A)$ on liitännäinen ja ykkösellinen A-algebra (ks. esim 2.2.4). Ykkösalkio on yksikkömatriisi $I = (\delta_{ij})$.

3) Jokaisen A-modulin M *endomorfismirengas*

$$E = \mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$$

kertolaskullaan $(f, g) \mapsto fg = f \circ g$ varustettuna on ykkösellinen ja liitännäinen A-algebra (harj. teht.).

Homomorfismit. Olkoot E ja E' kaksi A-algebraa.

MÄÄRITELMÄ 2.3.2. Kuvaus $f\colon E \to E'$ on A-algebrojen *homomorfismi*, jos

i) f on A-lineaarinen,
ii) $f(xy) = f(x)f(y)$ kaikilla x, $y \in E$.

Jos lisäksi E ja E' ovat ykkösellisiä, ykkösalkioinaan e ja e', ja $f(e) = e'$, niin homomorfismi f on *ykkösellinen*.

Kaikkien A-algebrahomomorfismien $f\colon E \to E'$ joukko

$$\mathrm{Hom}_{A-\mathrm{alg}}(E, E')$$

on lineaarikuvausten muodostaman A-modulin $\mathrm{Hom}_A(E, E')$ osajoukko, joka ei ole yleensä vakaa yhteenlaskun eikä skalaarikertolaskun suhteen.

Alialgebrat, ideaalit ja tekijäalgebrat. Olkoon E A-algebra.

MÄÄRITELMÄ 2.3.3. Algebran E osajoukko F on E:n *alialgebra*, jos

i) F on modulin E alimoduli,
ii) F on vakaa kertolaskun suhteen.

Indusoiduilla laskutoimituksilla varustettuna alialgebra F on myös A-algebra.

MÄÄRITELMÄ 2.3.4. Algebran E osajoukko $\mathfrak{a}$ on E:n *vasemmanpuolinen* (*oikeanpuolinen* tai *kaksipuolinen*) *ideaali*, jos

i) $\mathfrak{a}$ on modulin E alimoduli,
ii) kaikilla $x \in \mathfrak{a}$ ja $y \in E$ pätee $yx \in \mathfrak{a}$ ($xy \in \mathfrak{a}$ tai kumpikin).

Jos $\mathfrak{a}$ on A-algebran E kaksipuolinen ideaali, niin *kongruenssi*

$$x \equiv y \pmod{\mathfrak{a}} \qquad (\text{eli } x - y \in \mathfrak{a})$$

on E:n laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio (harj. teht.). Tekijäjoukolle käytetään tällöin merkintää

$$E/\mathfrak{a},$$

ja tekijälaskutoimituksilla varustettuna se on A-algebra, algebran E *tekijäalgebra* kaksipuolisen ideaalin $\mathfrak{a}$ suhteen.

Ykkösellisel algebrat. Olkoon E ykkösellinen A-algebra, jolla on ykkösalkio e. Ehdon $\eta(1) = e$ määräämällä A-lineaarisella kuvauksella (ks. lause 2.1.11)

$$\eta\colon A \to E, \quad \alpha \mapsto \alpha e,$$

on tällöin seuraavat ominaisuudet.

1. η on A-algebrojen homomorfismi, sillä kaikilla α, $\beta \in A$ pätee
$$\eta(\alpha).\eta(\beta) = (\alpha e).(\beta e) = (\alpha\beta)(e.e) = (\alpha\beta)e = \eta(\alpha\beta).$$
2. η määrää A-modulin E skalaarikertolaskun, sillä jos $\alpha \in A$ ja $x \in E$, niin $\alpha x = \alpha(e.x) = (\alpha e).x$ eli
$$\alpha x = \eta(\alpha).x\ .$$
3. Kuva $\eta(A)$ on algebran E alialgebra, sillä se on alimoduli ja vakaa kertolaskun suhteen.
4. Jokainen $\eta(A)$:n alkio $\eta(\alpha)$ kommutoi jokaisen E:n alkion x kanssa:
$$\eta(\alpha).x = x.\eta(\alpha),$$
sillä kohdan 2 ohella $\alpha x = \alpha(x.e) = x.(\alpha e) = x.\eta(\alpha)$.

Jos ykkösellinen A-algebra E on lisäksi liitännäinen, niin edellä esitetyt havainnot voidaan muotoilla seuraavasti.

i) Yhteenlaskullaan ja kertolaskullaan varustettuna E on rengas.
ii) Kuvaus $\eta\colon A \to E$ on rengashomomorfismi.
iii) Kuva $\eta(A)$ on E:n alirengas.
iv) $\eta(A)$ sisältyy renkaan E *keskukseen*
$$Z(E) = \{x \in E \mid x.y = y.x \text{ kaikilla } y \in E\},$$
joka on E:n alirengas (ja alialgebra, harj. teht.).

Jos homomorfismi η on injektiivinen, niin $\eta(A)$ on A:n kanssa isomorfinen E:n alirengas ja ne samastetaan usein keskenään.

Esimerkki 4) A-kertoimisten $n \times n$-matriisien rengas $\mathbf{M}_n(A)$ on ykkösellinen ja liitännäinen A-algebra (ks. esim 2.3.2). Sen ykkösalkio on yksikkömatriisi $I = (\delta_{ij})$ ja η kuvaa renkaan A bijektiivisesti lävistäjämatriisien joukolle

$$\eta(A) = A.I = \{(\alpha\delta_{ij}) \mid \alpha \in A\},$$

joka on renkaan $\mathbf{M}_n(A)$ keskus (harj. teht.).

Olkoon nyt kääntäen B rengas ja $\varrho\colon A \to B$ sellainen rengashomomorfimi, jonka kuva $\varrho(A)$ sisältyy B:n keskukseen, mikä pätee aina, kun B on vaihdannainen.

Tällöin B varustettuna skalaarikertolaskulla

$$(\alpha, x) \mapsto \varrho(\alpha)x \ (= x\varrho(\alpha))$$

on *ykkösellinen* ja *liitännäinen A-algebra.*

Usein tarkastellaan vain tällaisia algebroja ja sanotaan, että B on *liitännäinen A-algebra* ja $\varrho\colon A \to B$ on sen *struktuurihomomorfismi* mainitsematta ykkösellisyyttä. Samoin tällaisten algebrojen homomorfismit $f\colon B \to B'$ oletetaan yleensä ykkösellisiksi, vaikka tätä ei erikseen mainittaisi. Tämä merkitsee, että f on rengashomorfismi ja B':n struktuurihomomorfismi on $\varrho' = f \circ \varrho$:

$$\begin{tikzcd} B \arrow[rr, "f"] & & B' \\ & A \arrow[ul, "\varrho"] \arrow[ur, "\varrho'"'] & \end{tikzcd} .$$

Vastaavasti sanotaan ykkösellisiä, liitännäisiä ja vaihdannaisia A-algebroja vain *vaihdannaisiksi* algebroiksi, kun ei ole väärinkäsityksen vaaraa. Ne voidaan siis ajatella vaihdannaisiksi renkaiksi B varustettuina struktuurihomomorfismilla $\varrho\colon A \to B$.

Algebrojen kannat. Olkoon E A-algebra. Se on myös A-moduli, ja *algebran E kannalla* tarkoitetaan E:n kantaa A-modulina. Algebralla E on siis kanta, jos ja vain jos se on A-modulina vapaa.

Olkoon $(a_i)_{i\in I}$ jokin algebran E kanta. Jokaisella tulolla $a_i a_j \in E$ $(i,\, j \in I)$ on tällöin yksikäsitteinen esitys

$$a_i a_j = \sum_{k\in I} \gamma_{ij}^k a_k, \tag{1}$$

missä $(\gamma_{ij}^k)_{k\in I}$ on äärelliskantajainen A:n alkioperhe. Yhtälöiden (1) ryhmää sanotaan algebran E *kertotauluksi* ja sen kertoimia γ_{ij}^k algebran E *rakennevakioiksi* kannan (a_i) suhteen.

Esimerkkejä. 5) Kompleksilukujen kunta $\mathbf{C}$ on vaihdannainen (sekä ykkösellinen ja liitännäinen) $\mathbf{R}$-algebra struktuurihomomorfisminaan kanoninen inkluusio $\mathbf{R} \to \mathbf{C}$. Sillä on kanta $(1, i)$ ja kertotaulu

	1	i
1	1	i
i	i	-1

6) *Kvaternioiden* kunta $\mathbf{H}$ on liitännäinen $\mathbf{R}$-algebra. Sillä on kanta $(1, i, j, k)$ ja kertotaulu

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

7) Jos A on vaihdannainen rengas, niin matriisirengas $\mathbf{M}_n(A)$ on liitännäinen A-algebra (ks. esim. 2.3.2). Sillä on kanoninen kanta

$$(E_{ik})_{1\le i\le n, 1\le k\le n}\,,$$

missä $E_{ik} = (a_{jl})$, $a_{ik} = 1$ ja $a_{jl} = 0$, kun $(j,l) \neq (i,k)$, ja kertotaulu

$$E_{ij}E_{kl} = \delta_{jk}E_{il}.$$

Olkoon kääntäen E vapaa A-moduli ja $(a_i)_{i\in I}$ jokin sen kanta. Jokaista paria $(i,j) \in I \times I$ kohti olkoon $(\gamma_{ij}^k)_{k\in I}$ äärelliskantajainen A:n alkioperhe. Lauseen 2.2.3 perusteella on silloin olemassa yksikäsitteinen A-bilineaarinen kertolasku

$$E \times E \to E, \quad (x,y) \mapsto xy,$$

joka toteuttaa ehdot

$$a_i a_j = \sum_{k\in K} \gamma_{ij}^k a_k \qquad (i \in I, j \in I).$$

Algebran E kertotaulu voidaan siis valita ilman rajoituksia ja se sisältää kaiken tiedon algebran kertolaskusta. Seuraava lause näyttää, miten algebran perusominaisuudet voidaan saada kertotaulusta.

Lause 2.3.5. *Olkoon E A-algebra ja $(a_i)_{i\in I}$ sen kanta.*

i) *E on liitännäinen, jos ja vain jos kaikilla i, j, $k \in I$*

$$(a_i a_j)a_k = a_i(a_j a_k).$$

ii) *E on vaihdannainen, jos ja vain jos kaikilla i, $j \in I$*

$$a_i a_j = a_j a_i.$$

iii) *E:n alkio e on ykkösalkio, jos ja vain jos kaikilla $i \in I$*

$$a_i = e a_i = a_i e.$$

Todistus. Tarkastellaan ensin kohtaa iii). Jos $e \in E$, niin kertolaskun bilineaarisuuden nojalla $x \mapsto ex$ on A-lineaarinen kuvaus $E \to E$. Se on identtinen kuvaus, jos ja vain jos se kuvaa kannan alkiot itselleen: $ea_i = a_i$ kaikilla $i \in I$ (ks. lause 2.1.14). Vastaavasti $x \mapsto xe$ on identtinen kuvaus, jos ja vain jos $a_i e = a_i$ kaikilla $i \in I$.

Kohtaa ii) varten on osoitettava, että kuvaukset

$$E \times E \to E, \quad (x,y) \mapsto xy \text{ ja } (x,y) \mapsto yx,$$

ovat samat, jos ja vain jos ne saavat samat arvot kannan $(a_i)_{i\in I}$ alkioilla. Koska kumpikin kuvaus on A-bilineaarinen, väite seuraa suoraan lauseesta 2.2.3.

Ensimmäinen kohdan perustelu on saman kaltainen kuin kohdan ii), mutta lauseen 2.2.3 todistuksessa esiintyvän kaksoissumman asemasta on käsiteltävä kolminkertaista summaa (harj. teht.). $\square$

Magma-, monoidi- ja ryhmäalgebrat. Olkoon S magma, jonka laskutoimitus on merkitty kertolaskuksi. Olkoon $E = A^{(S)}$ joukon S virittämä vapaa A-moduli. Sillä on kanoninen kanta

$$(e_s)_{s \in S},$$

missä $e_s = (\delta_{s\,t})_{t \in S}$.

Määritellään E:ssä A-bilineaarinen tulo kertotaululla

$$e_s e_t = e_{st} \qquad (s, t \in S)$$

tai yhtäpitävästi rakennevakioilla $\gamma_{s\,t}^{u} = \delta_{st,u}$. Kahden E:n alkion

$$x = \sum_{s \in S} \xi_s e_s, \quad y = \sum_{s \in S} \eta_s e_s$$

tulo on siis

$$xy = \sum_{s \in S} \Big(\sum_{tu = s} \xi_t \eta_u \Big) e_s.$$

Tällöin E on A-algebra, *magman S algebra* A:n suhteen. Jos S on monoidi tai ryhmä, E on vastaavasti *monoidin* tai *ryhmän S algebra.*

Huomautus. Usein samastetaan alkiot $s \in S$ vastaavien E:n kanonisen kannan alkioiden e_s kanssa ja merkitään E:n alkiot muodollisiksi A-kertoimisiksi yhdistelmiksi $\sum_{s \in S} \xi_s s$. Algebran kertolasku on tällöin

$$\Big(\sum_{t \in S} \xi_t t \Big) \Big(\sum_{u \in S} \eta_u u \Big) = \sum_{s \in S} \Big(\sum_{tu = s} \xi_t \eta_u \Big) s.$$

Jos S on monoidi, jonka laskutoimituksena on yhteenlasku (ja se on vaihdannainen), niin sen algebran kanonisen kannan alkioille käytetään myös merkintää $e_s = e^s$ $(s \in S)$. Algebran kertotaulu saa tällöin muodon

$$e^s e^t = e^{s+t} \qquad (s, t \in S).$$

Magma-, monoidi- ja ryhmäalgebrojen ominaisuudet saadaan välittömästi lauseen 2.3.5 avulla:

KOROLLAARI 2.3.6. *Olkoon E magman S algebra renkaan A suhteen.*

i) *Jos S on monoidi, niin E on liitännäinen ja ykkösellinen.*
ii) *Jos S on ryhmä, niin jokainen e_s $(s \in S)$ on kääntyvä E:ssä.*
iii) *Jos S on vaihdannainen, niin algebra E on vaihdannainen.*

Todistus. Jos S on monoidi, niin siinä on neutraalialkio u ja silloin kaikilla $s \in S$ pätee

$$e_u e_s = e_{us} = e_s = e_{su} = e_s e_u.$$

Lauseen 2.3.5 kohdan iii) perusteella $e = e_u$ on siten E:n ykkösalkio.

Lisäksi monoidi S on liitännäinen, jolloin kaikilla s, t, $u \in S$

$$(e_s e_t) e_u = e_{st} e_u = e_{(st)u}$$

on sama kuin $e_s(e_te_u) = e_{s(tu)}$, ja siten E on myös liitännäinen lauseen 2.3.5 kohdan i) nojalla. Samoin nähdään käyttäen kohtaa ii), että E on vaihdannainen, jos S on vaihdannainen.

Lopuksi, jos S on ryhmä, niin jokaisella sen alkiolla s on käänteisalkio $s^{-1} \in S$. Tällöin $e_se_{s^{-1}} = e_u = e_{s^{-1}}e_s$, missä u on S:n neutraalialkio. Alkiolla e_s on siis käänteisalkio $e_{s^{-1}}$. □

Seuraavassa lauseessa tarkastellaan algebraa vain kertolaskullaan varustettuna magmana eli algebran multiplikatiivista magmaa.

Lause 2.3.7 (Magma-algebran universaaliominaisuus). *Olkoon S magma, E sen algebra A:n suhteen, F toinen A-algebra ja $f\colon S \to F$ homomorfismi algebran F multiplikatiiviseen magmaan. Silloin on olemassa yksi ja vain yksi A-algebrahomomorfismi $\bar f\colon E \to F$, joka toteuttaa ehdot*

$$\bar f(e_s) = f(s) \qquad (s \in S).$$

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[dr, "\text{kan}"'] & F \\ & E \arrow[u, dashed, "\bar f"'] \end{tikzcd}$$

Todistus. Perheen $(f(s))_{s\in S}$ määräämä kuvaus (ks. lause 2.1.11)

$$\bar f\colon E \to F$$

on ainoa ehdot täyttävä A-lineaarinen kuvaus. On riittävää osoittaa, että $\bar f$ on myös multiplikatiivinen homomorfismi.

Tarkastellaan kahta kuvausta

$$u\colon (x,y) \mapsto \bar f(xy), \quad v\colon (x,y) \mapsto \bar f(x)\bar f(y)$$

tulosta $E \times E$ moduliin F. Kumpikin on A-bilineaarinen. (Esimerkiksi osittaiskuvaukset $x \mapsto xy \mapsto \bar f(xy)$ ja $x \mapsto \bar f(x) \mapsto \bar f(x)\bar f(y)$ ovat homomorfismien yhdistelminä lineaarisia.) Kanonisen kannan alkioilla ne saavat arvot

$$u(e_s, e_t) = \bar f(e_se_t) = \bar f(e_{st}) = f(st)$$

ja

$$v(e_s, e_t) = \bar f(e_s)\bar f(e_t) = f(s)f(t).$$

Koska f on magmahomomorfismi, kaikilla s, $t \in S$ pätee

$$f(st) = f(s)f(t).$$

Kuvaukset u ja v saavat siis samat arvot kannan $(e_s)_{s\in S}$ alkioilla, joten ne ovat lauseen 2.2.3 nojalla samat; kaikilla x, $y \in E$ on siis voimassa

$$\bar f(xy) = \bar f(x)\bar f(y).$$

Kuvaus $\bar f\colon E \to F$ on siten A-algebrojen homomorfismi. □

Esimerkki 8) (Ryhmien esitysten linearisointi) Olkoon S ryhmä ja V A-moduli. Ryhmän S *esityksellä* V:ssä tarkoitetaan sen toimintaa

$$S \times V \to V, \quad (s,x) \mapsto s.x,$$

joka on A-lineaarinen. Tämä merkitsee, että se toteuttaa kaikilla s, $t \in S$, x, $y \in V$ ja $\alpha \in A$ ehdot

i) $s.(x+y) = s.x + s.y$, $s.(\alpha x) = \alpha(s.x)$,

ii) $s.(t.x) = (st).x$, $e.x = x$ (e on S:n neutraalialkio),

eli yhtäpitävästi

i) $f(s)\colon V \to V$, $x \mapsto s.x$ on A-lineaarinen kuvaus kaikilla $s \in S$,

ii) $f\colon S \to \mathrm{End}_A(V)$ on multiplikatiivinen homomorfismi.

Olkoon $E = A^{(S)}$ ryhmän S algebra. Koska $\mathrm{End}_A(V)$ on A-algebra (ks. esim 2.3.3), homomorfismia f vastaa yksikäsitteinen A-algebrojen homomorfismi

$$\bar{f}\colon E \to \mathrm{End}_A(V),$$

ja tällainen homomorfismi puolestaan vastaa V:ssä E-modulin struktuuria, jonka skalaarikertolasku on

$$E \times V \to V, \quad (u, x) \mapsto u.x = (\bar{f}(u))(x).$$

Nähdään siis, että ryhmän S esitysten teoria A-moduleissa on sama kuin E-modulien teoria.

Harjoitustehtäviä

1) Olkoon A vaihdannainen rengas ja olkoot B, B' kaksi liitännäistä A-algebraa struktuurihomomorfismeinaan $\varrho\colon A \to B$ ja $\varrho'\colon A \to B'$. Osoitettava, että rengashomomorfismi $f\colon B \to B'$ on A-algebrojen homomorfismi, jos ja vain jos $f \circ \varrho = \varrho'$.

2) Osoitettava, että renkaan $M_2(\mathbf{C})$ matriiseilla

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

on sama kertotaulu kuin kvaternioilla i, j, k, ja pääteltävä, että kvaternioalgebra $\mathbf{H}$ on liitännäinen.

3) Olkoon A vaihdannainen rengas, jossa 2 on kääntyvä, $S = \{1, s\}$ kaksialkioinen syklinen ryhmä ja $E = A^{(S)}$ sen algebra A:n suhteen. Osoitettava, että

i) $e = 2^{-1}(1+s)$ on E:n keskeinen idempotentti alkio;

ii) e ja $e' = 1 - e$ muodostavat E:n kannan;

iii) Ae ja Ae' ovat A:n kanssa isomorfisia E:n alialgebroja.

Pääteltävä, että E on isomorfinen tuloalgebran $A \times A$ kanssa (ks. teht. 1.7.6).

2.4. Polynomialgebrat

Olkoon A vaihdannainen rengas. Tässä pykälässä on tavoitteena tarkastella polynomeja, joiden kertoimet ovat renkaassa A ja joissa on useita (mahdollisesti ääretön määrä) tuntemattomia.

Kun rengas A on $\mathbf{R}$ (tai sen alirengas), on tapana tulkita esimerkiksi yhden tuntemattoman polynomit $p = p(X)$ funktioiksi $p\colon \mathbf{R} \to \mathbf{R}$. Algebrassa tämä ei yleisesti käy, koska eri polynomeihin voi liittyä sama funktio. (Esimerkiksi, jos A on äärellinen, kaikkien funktioiden $A \to A$ joukko on myös äärellinen, vaikka jo monomeja X^n ($n \in \mathbf{N}$) on ääretön määrä.)

Ongelman ratkaisemiseksi on määriteltävä polynomit täysin muodollisesti. Ensin konstruoidaan monomit. Ne muodostavat vaihdannaisen monoidin, jonka virittävät polynomien tuntemattomat. Monoidi on vapaa, koska tuntemattomien välillä ei saa olla relaatioita. Polynomit voidaan puolestaan määritellä monomien muodollisina A-kertoimisina yhdistelminä.

Polynomialgebran konstruktio. Olkoon I joukko, jonka alkiot toimivat tuntemattomien indekseinä; esimerkiksi $I = \{1, 2, \dots, n\}$.

Olkoon $M = \mathbf{N}^{(I)}$ joukon I virittämä vapaa vaihdannainen monoidi (ks. 1.6). Sen alkioina ovat funktiot $\nu\colon I \to \mathbf{N}$, joilla on $\nu(i) \neq 0$ vain äärellisen monella indeksillä $i \in I$, ja sillä on vapaa virittäjäperhe $(\delta_i)_{i\in I}$, missä δ_i on Kroneckerin funktio $j \mapsto \delta_{ij}$ $(i, j \in I)$.

Olkoon $P_A(I) = A^{(M)}$ monoidin M algebra renkaan A suhteen. Sillä on kanoninen kanta $(e^\nu)_{\nu\in M}$ ja kertotaulu

$$e^\nu e^\mu = e^{\nu+\mu} \qquad (\nu, \mu \in M).$$

(Indeksit ovat ylhäällä, koska M on additiivinen monoidi.) Sen alkioina ovat lineaariset yhdistelmät

$$\sum_{\nu\in M} \alpha_\nu e^\nu,$$

missä $(\alpha_\nu)_{\nu\in M}$ on äärelliskantajainen A:n alkioperhe. Koska M on vaihdannainen monoidi, sen algebra $P_A(I)$ on *liitännäinen, vaihdannainen* ja *ykkösellinen* A-algebra (korollaari 2.3.6).

Algebran $P_A(I)$ kanonisen kannan alkioille käytetään tavallisesti merkintöjä, joissa esiintyy aakkosten loppupään kirjaimia, usein suuria kirjaimia X, Y, Z. Olkoon esimerkiksi

$$X^\nu = e^\nu \qquad (\nu \in M),$$

jolloin kertotaulu saa muodon

$$X^\nu X^\mu = X^{\nu+\mu} \qquad (\nu, \mu \in M).$$

Kanoninen kuvaus $\nu \mapsto X^\nu$ on tällöin monoidihomorfismi $M \to P_A(I)$ additiivisesta monoidista M algebran $P_A(I)$ multiplikatiiviseen monoidiin.

Vapaan vaihdannaisen monoidin universaaliominaisuuden nojalla (ks. lause 1.6.2) monoidihomomorfismi on yksikäsitteisesti määrätty, kun sen arvot tunnetaan monoidin M virittäjillä δ_i $(i \in I)$. Kun näitä vastaaville kannan alkioille käytetään merkintää

$$X_i = e^{\delta_i} \qquad (i \in I),$$

saadaan muut kanonisen homomorfismin arvot eksponenttimerkinnän avulla:

$$X^\nu = \prod_{i \in I} X_i^{\nu(i)} \qquad (\nu \in M).$$

Näitä alkioita sanotaan algebran $P_A(I)$ *monomeiksi*. Monomin X^ν *aste* on hyvin määritelty luonnollinen luku

$$|\nu| = \sum_{i \in I} \nu(i),$$

koska vain äärellisen moni $\nu(i)$ on nollasta eroava.

Koska $(X^\nu)_{\nu \in M}$ on algebran $P_A(I)$ kanta, jokaisella sen alkiolla on yksikäsitteinen esitys

$$u = \sum_{\nu \in M} \alpha_\nu X^\nu,$$

missä $(\alpha_\nu)_{\nu \in M}$ on äärelliskantajainen A:n alkioperhe. Alkioita sanotaan *A-kertoimisiksi polynomeiksi tuntemattomien X_i suhteen*. Polynomin $u \neq 0$ *aste* $\deg(u)$ on suurin niiden monomien X^ν asteista $|\nu|$, joilla kerroin $\alpha_\nu \neq 0$.

Algebran $P_A(I)$ *ykkösalkio* on ainoa 0-asteinen monomi $X^0 = e^0$. Kanoninen homomorfismi ykköselliseen algebraan (ks. 2.3)

$$\eta\colon A \to P_A(I), \quad \alpha \mapsto \alpha X^0,$$

on injektiivinen. Tavallisesti samastetaan rengas A ja sen kuva

$$\eta(A) = \{\alpha X^0 \mid \alpha \in A\},$$

jonka alkioita sanotaan *vakiopolynomeiksi* tai vain *vakioiksi*. Tällöin siis merkitään $\alpha = \alpha X^0$ ja erityisesti $1 = X^0$.

Universaaliominaisuus. Olkoon A vaihdannainen rengas.

LAUSE 2.4.1. *Olkoon B (ykkösellinen, liitännäinen ja) vaihdannainen A-algebra ja $(x_i)_{i \in I}$ perhe sen alkioita. On olemassa yksi ja vain yksi ykkösellinen homomorfismi $f\colon P_A(I) \to B$, joka toteuttaa ehdot*

$$f(X_i) = x_i \qquad (i \in I).$$

$$\begin{tikzcd} I \arrow[rr, "i \mapsto x_i"] \arrow[dr, "\mathrm{kan}"'] & & B \\ & P_A(I) \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

Todistus. Algebra B yksin kertolaskullaan varustettuna on vaihdannainen monoidi B_m. Vapaan vaihdannaisen monoidin universaaliominaisuuden nojalla (lause 1.6.2) on silloin olemassa yksikäsitteinen monoidihomomorfismi

$$g\colon \mathbf{N}^{(I)} \to B_m,$$

joka täyttää ehdot

$$g(\delta_i) = x_i \qquad (i \in I).$$

Monoidin $\mathbf{N}^{(I)}$ algebran universaaliominaisuuden mukaan (lause 2.3.7) on puolestaan olemassa yksikäsitteinen A-algebrahomomorfismi

$$f\colon P_A(I) \to B,$$

joka toteuttaa ehdot

$$f(X^\nu) = f(e^\nu) = g(\nu) \qquad (\nu \in \mathbf{N}^{(I)}).$$

Tällöin erityisesti kaikilla $i \in I$ pätee

$$f(X_i) = f(e^{\delta_i}) = g(\delta_i) = x_i.$$

Ehdot täyttävä homomorfismi f on siis olemassa.

Jos $f'\colon P_A(I) \to B$ on toinen A-algebrojen homomorfismi, joka toteuttaa samat ehdot $f'(X_i) = x_i$ $(i \in I)$, niin

$$g'\colon \mathbf{N}^{(I)} \to B_m, \quad \nu \mapsto f'(X^\nu),$$

on monoidihomomorfismi ja kaikilla $i \in I$

$$g'(\delta_i) = f'(X^{\delta_i}) = f'(X_i) = x_i.$$

Homomorfismin g yksikäsitteisyyden nojalla g' on sama kuin g, ja silloin myös homomorfismien f' ja f täytyy olla samat. □

Ehdot $g(\delta_i) = x_i$ toteuttava monoidihomomorfismi $g\colon \mathbf{N}^{(I)} \to B_m$ saadaan eksponenttimerkintää käyttäen kaavasta

$$g(\nu) = x^\nu = \prod_{i \in I} x_i^{\nu(i)}.$$

Ehdot $f(X^\nu) = g(\nu)$ täyttävän algebrahomomorfismin $f\colon P_A(I) \to B$ arvot ovat siten

$$f\Big(\sum_\nu \alpha_\nu X^\nu\Big) = \sum_\nu \alpha_\nu x^\nu.$$

Tällöin sanotaan, että polynomin $u \in P_A(I)$ kuva $f(u) \in B$ on saatu polynomista *u sijoittamalla alkiot $x_i \in B$ tuntemattomien X_i paikalle* tai että $f(u)$ on polynomin *u arvo tuntemattomien X_i arvoilla x_i*.

Homomorfismia f sanotaan *sijoitushomomorfismiksi* ja sen arvoille käytetään merkintää

$$f(u) = u((x_i)_{i \in I}).$$

Sijoitushomomorfismin f kuva $\mathrm{Im}(f)$ on algebran B alialgebra, joka sisältää alkiot x_i $(i \in I)$ ja sisältyy jokaiseen nämä alkiot sisältävään B:n alialgebraan. Se on siis *perheen $(x_i)_{i \in I}$ virittämä B:n ali-A-algebra*

$$A[(x_i)_{i \in I}] = \Big\{\sum_\nu \alpha_\nu x^\nu \mid \sum_\nu \alpha_\nu X^\nu \in P_A(I)\Big\}.$$

Vastaavaa merkintää on tapana käyttää myös algebralle $P_A(I)$, kun sen virittäjäperhe on $(X_i)_{i\in I}$:

$$A[(X_i)_{i\in I}] = P_A(I),$$

jolloin sitä sanotaan *tuntemattomien X_i A-kertoimiseksi polynomialgebraksi.*

Sijoitushomomorfismin $f\colon u \mapsto u((x_i)_{i\in I})$ ydin

$$\mathfrak{a} = \{u \in A[(X_i)_{i\in I}] \mid u((x_i)_{i\in I}) = 0\}$$

on algebran $A[(X_i)_{i\in I}]$ ideaali (sekä renkaan ideaali että alimoduli), ja sen alkioita sanotaan perheen $(x_i)_{i\in I}$ alkioiden välisiksi *A-kertoimisiksi polynomirelaatioiksi.*

Lause 2.4.2. *Olkoon B vaihdannainen A-algebra, $(x_i)_{i\in I}$ sen alkioperhe ja $\mathfrak{a}$ perheen alkioiden välisten A-kertoimisten polynomirelaatioiden ideaali. Silloin sijoitushomomorfismin $f\colon u \to u((x_i)_{i\in I})$ kanonisesta hajotelmasta saadaan A-algebrojen isomorfismi*

$$\bar{f}\colon A[(X_i)_{i\in I}]/\mathfrak{a} \xrightarrow{\sim} A[(x_i)_{i\in I}].$$

Todistus. Tulos seuraa välittömästi algebrojen homomorfialauseesta, joka saadaan esimerkiksi yhdistämällä renkaiden ja modulien homomorfialauseet 1.7.10 ja 2.1.7 (tai myös suoralla todistuksella). □

Kun indeksijoukko I on äärellinen, merkitään perheet usein jonoiksi. Esimerkiksi kun $I = \{1, 2, \ldots, n\}$, käytetään sijoitushomomorfismin arvoille merkintää

$$f(u) = u(x_1, x_2, \ldots, x_n)$$

ja alkioiden x_i virittämälle alialgebralle merkintää

$$A[x_1, x_2, \ldots, x_n].$$

Polynomialgebra merkitään silloin vastaavasti

$$A[X_1, X_2, \ldots, X_n].$$

Huomautus. Kun tarkastellaan useita polynomialgebroja, on tarpeen käyttää muitakin merkintöjä kuten esimerkiksi

$$A[(Y_i)_{i\in I}], \quad A[(Z_i)_{i\in I}],$$

tai kun n on pieni kokonaisluku, eri kirjaimia ilman indeksejä kuten

$$A[X], \quad A[X, Y], \quad A[X, Y, Z].$$

Merkinnästä riippumatta olennainen piirre on polynomialgebran universaaliominaisuus eli mahdollisuus sijoitushomomorfismiin.

Harjoitustehtäviä

Seuraavissa tehtävissä A on vaihdannainen rengas.

1) Olkoot $u \in A[X]$ ja $v \in A[Y]$ polynomeja sekä $w = u(v) \in A[Y]$. Olkoon B jokin ykköisellinen, liitännäinen ja vaihdannainen A-algebra ja $y \in B$. Osoitettava, että $w(y) = u(v(y))$. (Tarkastellaan sijoitushomomorfismien $f\colon A[X] \to A[Y]$, $f(X) = v$, ja $g\colon A[Y] \to B$, $g(Y) = y$, yhdistelmää, joka on myös sijoitushomomorfismi.)

2) Olkoon $u \circ v = u(v)$, kun u, $v \in A[X]$. Osoitettava, että $(u \circ v) \circ w = u \circ (v \circ w)$ kaikilla u, v, $w \in A[X]$. (Sovelletaan tehtävää 1 tilanteeseen $A[X] = A[Y] = B$, $y = w$.)

3) Olkoon $u \in A[X]$, $a \in A$ ja $v = u(Y + a) \in A[Y]$. Osoitettava, että

i) $u(a) = v(0)$ (asetetaan $v = Y + a$ ja $y = 0$ tehtävässä 1);
ii) $v(0) = 0$, jos ja vain jos $v \in YA[Y]$;
iii) sijoitushomomorfismi $f\colon A[X] \to A[Y]$, $f(X) = Y + a$ on isomorfismi, ja f^{-1} on sijoitushomomorfismi $g\colon A[Y] \to A[X]$, $g(Y) = X - a$.

Pääteltävä, että $u(a) = 0$, jos ja vain jos $u \in (X - a)A[X]$ eli $X - a$ on u:n tekijä.

4) Olkoon A kokonaisalue. Etsittävä polynomin $X^2 - X$ juuret tulorenkaassa $A \times A$ ja osoitettava:

i) Polynomilla $f \in A[X]$, $f \neq 0$, on enintään $n = \deg(f)$ juurta A:ssa.
ii) Jos A on ääretön ja $f \in A[X_1, \dots, X_n]$, $f \neq 0$, niin $f(x_1, \dots, x_n) \neq 0$ joillakin $x_1, \dots, x_n \in A$. (Induktio n:n suhteen käyttäen esitystä $f = \sum_k f_k X_n^k$, missä $f_k \in A[X_1, \dots, X_{n-1}]$.)

2.5. Derivaattakuvaukset

Olkoon K vaihdannainen rengas. Jos u on tuntemattoman X K-kertoiminen polynomi ja x, ε ovat jonkin vaihdannaisen K-algebran alkioita, niin sijoittamalla $x + \varepsilon$ potensseihin X^n saadaan

$$u(x + \varepsilon) = u(x) + Du(x)\varepsilon + R, \tag{1}$$

missä Du on polynomin u "muodollinen derivaatta" ja

$$R = \varepsilon^2 v(x, \varepsilon),$$

missä v on jokin kahden tuntemattoman polynomi.

Perinteisessä analyysissa, kun K on $\mathbf{R}$ (tai $\mathbf{C}$), tästä kaavasta lasketaan derivaatan arvo $Du(x)$ osoittamalla osamäärän

$$R/\varepsilon = \varepsilon v(x, \varepsilon)$$

raja-arvoksi 0, kun $\varepsilon \to 0$.

Algebrassa ei derivaattaa voida käsitellä raja-arvona. Sen sijaan on helppo konstruoida algebroja, joissa eräiden alkioiden ε neliö on 0, jolloin "jäännöstermi" R häviää kokonaan ja derivaatta voidaan lukea suoraan kehitelmästä (1).

Olkoon A jokin K-algebra. Konstruoidaan uusi K-algebra $A[\varepsilon]$ seuraavasti.

i) K-modulina $A[\varepsilon]$ on tulomoduli $A \times A$;
ii) kertolaskun määrittelee kaava

$$(a, b)(a', b') = (aa', ba' + ab') \qquad (a, a', b, b' \in A).$$

(Kertolasku on K-bilineaarinen, koska sen komponentit $(a, b)(a', b') \mapsto aa'$ ja $(a, b)(a', b') \mapsto ba' + ab'$ ovat K-bilineaarisia.)

Algebran $A[\varepsilon]$ alkiot (a, b) voidaan tulkita kehitelmän (1) oikeaksi puoleksi $a + b\varepsilon$. Kolmatta termiä ei tarvita, koska $(b\varepsilon)(b'\varepsilon) = 0$.

LAUSE 2.5.1. *Olkoon $D\colon A \to A$ K-lineaarinen kuvaus. Tällöin kuvaus $a \mapsto (a, D(a))$ on K-algebrojen homomorfismi $A \to A[\varepsilon]$, jos ja vain jos kaikilla a, $b \in A$ on voimassa*

$$D(ab) = D(a)b + aD(b)\,.$$

Todistus. Kuvaus on aina K-lineaarinen, koska sen komponentit Id_A ja D ovat oletuksen mukaan K-lineaarisia. Se on lisäksi homomorfismi kertolaskun suhteen, jos ja vain jos kaikilla a, $b \in A$ pätee

$$(ab, D(ab)) = (a, D(a))(b, D(b)) = (ab, D(a)b + aD(b))$$

eli yhtäpitävästi $D(ab) = D(a)b + aD(b)$. □

MÄÄRITELMÄ 2.5.2. Kuvaus $D\colon A \to A$ on K-algebran A *derivaattakuvaus*, jos se on K-lineaarinen ja toteuttaa *Leibnizin säännön*

$$D(ab) = D(a)b + aD(b) \qquad (a, b \in A).$$

Huomautus. Derivaattakuvausten arvoja merkittäessä jätetään usein sulkumerkit pois lausekkeiden yksinkertaistamiseksi: $D(a) = Da$.

Esimerkki 1) Olkoon A polynomialgebra $K[X]$, jolla on kanta $(X^n)_{n\in\mathbf{N}}$. Tällöin ehtojen

$$DX^n = nX^{n-1} \qquad (n \in \mathbf{N})$$

määräämä lineaarikuvaus $D\colon A \to A$ on K-derivaattakuvaus. (Koska Leibnizin ehto on bilineaarinen, on riittävää todistaa se kannan alkioilla (ks. lause 2.2.3):

$$D(X^n X^m) = D(X^{n+m}) = (n+m)X^{n+m-1},$$

$$DX^n\, X^m + X^n\, DX^m = nX^{n+m-1} + mX^{n+m-1}.)$$

LEMMA 2.5.3. *Jos A on ykkösellinen, liitännäinen tai vaihdannainen K-algebra, niin samoin on $A[\varepsilon]$.*

Todistus. Jos A:ssa on ykkösalkio 1, niin $(1, 0)$ on algebran $A[\varepsilon]$ ykkösalkio kuten välittömästi nähdään.

Jos A on liitännäinen, niin kaikilla a, a', a'', b, b', $b'' \in A$

$$((a, b)(a', b'))(a'', b'') = (aa'a'', ba'a'' + ab'a'' + aa'b'')$$

ja sama arvo saadaan tulolle $(a, b)((a', b')(a'', b''))$.

Samoin, jos A on vaihdannainen, niin $A[\varepsilon]$ on vaihdannainen. $\square$

Kanoninen injektio

$$A \to A[\varepsilon], \quad a \mapsto (a, 0),$$

on K-algebrojen homomorfismi ($D = 0$ on derivaattakuvaus). Tavallisesti samastetaan A kuvansa kanssa ja merkitään $a = (a, 0)$, kun $a \in A$. Jos lisäksi merkitään $\varepsilon = (0, 1)$, niin algebran $A[\varepsilon]$ alkioille saadaan yksikäsitteiset esitykset

$$(a, b) = a + b\varepsilon \qquad (a, b \in A).$$

Tällöin $a\varepsilon = \varepsilon a$ kaikilla $a \in A$ ja $\varepsilon^2 = 0$.

Jos erityisesti A on vaihdannainen, niin $A[\varepsilon]$ on myös A-algebra, jolla on kanta $(1, \varepsilon)$ ja kertotaulu

$$\begin{array}{c|cc} & 1 & \varepsilon \\ \hline 1 & 1 & \varepsilon \\ \varepsilon & \varepsilon & 0 \end{array}\ .$$

Tällöin $A[\varepsilon]$ on alkion ε virittämä A-algebra. Se on isomorfinen tekijäalgebran $A[X]/\mathfrak{a}$ kanssa (lause 2.4.2), missä $\mathfrak{a} = A[X]X^2$ on alkion ε A-kertoimisten polynomirelaatioiden ideaali.

Lause 2.5.4. *Olkoon A polynomialgebra $K[(X_i)_{i\in I}]$ ja $(u_i)_{i\in I}$ sen alkioperhe. Silloin on olemassa yksi ja vain yksi A:n K-derivaattakuvaus D, joka toteuttaa ehdot*

$$DX_i = u_i \qquad (i \in I).$$

Todistus. Lemman 2.5.3 nojalla $A[\varepsilon]$ on ykkösellinen, liitännäinen ja vaihdannainen K-algebra. Siihen voidaan siten soveltaa lausetta 2.4.1.

Osoitetaan ensin, että ehdot täyttävä derivaattakuvaus D on yksikäsitteinen, jos sellainen on olemassa. Olkoon $D\colon A \to A$ jokin K-derivaattakuvaus. Lauseen 2.5.1 mukaan kuvaus

$$f\colon A \to A[\varepsilon], \quad a \mapsto (a, Da),$$

on tällöin K-algebrahomomorfismi. Jos $DX_i = u_i$, kaikilla $i \in I$, niin $f(X_i) = (X_i, u_i)$, ja siten f on sijoitushomomorfismi

$$a \mapsto a((X_i, u_i)_{i\in I}).$$

Silloin $f(a) = (a, Da)$ on yksikäsitteisesti määrätty, ja samoin on Da yksikäsitteinen.

Olemassaolon osoittamiseksi tarkastellaan sijoitushomomorfismia

$$f\colon A \to A[\varepsilon], \quad a \mapsto a((X_i, u_i)_{i\in I})\,.$$

Koska projektiokuvaus $\mathrm{pr}_1\colon (a, b) \mapsto a$ on algebrahomomorfismi

$$p\colon A[\varepsilon] \to A,$$

yhdistetty kuvaus

$$g = p \circ f\colon A \to A$$

on myös K-algebrojen homomorfismi. Se on siis sijoitushomomorfismi, ja koska kaikilla $i \in I$

$$g(X_i) = p(f(X_i)) = p(X_i, u_i) = X_i,$$

se on identtinen kuvaus.

Sijoitushomomorfismilla f on siten muoto $f(a) = (a, Da)$, missä D on algebran A derivaattakuvaus. Lisäksi ehdosta $f(X_i) = (X_i, u_i)$ seuraa $DX_i = u_i$ kaikilla $i \in I$. $\square$

Esimerkki 2) Polynomialgebran $A = K[(X_i)_{i\in I}]$ jokaista tuntematonta X_i kohti on olemassa yksikäsitteinen K-derivaattakuvaus, ns. i:s *osittaisderivaattakuvaus*

$$D_i = \frac{\partial}{\partial X_i}\colon A \to A,$$

joka toteuttaa ehdot

$$D_i X_j = \delta_{ij} \qquad (j \in I).$$

Derivaattakuvauksilla on algebrassa samanlaisia ominaisuuksia kuin analyysissakin. Seuraavassa on eräs esimerkki.

KOROLLAARI 2.5.5. *Jos D on jokin K-algebran $A = K[X_1, X_2, \ldots, X_n]$ derivaattakuvaus, niin kaikilla $u \in A$ pätee*

$$Du = \sum_{i=1}^{n} D_i u \, DX_i.$$

Todistus. Tarkastellaan summalausekkeen määrittelemää kuvausta

$$D'\colon A \to A, \quad u \mapsto \sum_{i=1}^{n} D_i u \, DX_i.$$

Koska D_i:t ovat K-algebran A derivaattakuvauksia, samoin ovat kuvaukset $u \mapsto D_i u \, DX_i (= DX_i . D_i u)$ ja myös niiden summa D'.

Lisäksi jokaisella indeksillä $1 \leq j \leq n$ saadaan

$$D' X_j = \sum_{i=1}^{n} D_i X_j \, DX_i = \sum_{i=1}^{n} \delta_{ij} \, DX_i = DX_j.$$

Lauseen 2.5.4 yksikäsitteisyyden nojalla on siis $D' = D$. $\square$

Huomautus. Vastaava tulos on voimassa jokaisessa polynomialgebrassa $A = K[(X_i)_{i\in I}]$:

$$Du = \sum_{i\in I} D_i u \, DX_i.$$

Summa on hyvin määritelty, koska jokainen polynomi $u \in A$ sisältää vain äärellisen monta tuntematonta, ja siten osittaisderivaattojen perheellä $(D_i u)_{i\in I}$ on äärellinen kantaja.

Harjoitustehtäviä

Olkoon K vaihdannainen rengas.

1) Osoitettava, että $a \in K$ on polynomin $u \in K[X]$ *yksinkertainen juuri* eli $u = (X - a)v$, missä $v \in K[X]$ ja $v(a) \neq 0$, jos ja vain jos $u(a) = 0$ mutta $Du(a) \neq 0$.

2) Olkoon A polynomialgebra $K[X_1, X_2]$ ja B sen alialgebra $K[X_1]$. Osoitettava, että $D_1 u \in B$ ja $D_2 u = 0$, kun $u \in B$. (Tarkastellaan homomorfismeja $B \to A[\varepsilon]$, $u \mapsto (u, D_1 u)$ ja $u \mapsto (u, D_2 u)$.)

LUKU 3

Jaollisuus

Tässä luvussa tarkastellaan jaollisuuskysymyksiä renkaissa. Vaikka eräät osat teoriaa on mahdollista esittää yleisemminkin, tarkastelu rajoitetaan kokonaisalueisiin, joissa tulokset voidaan viedä pisimmälle. Kokonaisalueella tarkoitetaan vaihdannaista rengasta, joka ei ole nollarengas ja jossa jokainen nollasta eroava alkio on säännöllinen (ei nollanjakaja). Erityisesti jokainen vaihdannainen kunta on kokonaisalue.

3.1. Jaollisuusrelaatio

Olkoon A kokonaisalue. Sen nollasta eroavien alkioiden joukko $P = A \setminus \{0\}$ on tällöin vakaa kertolaskun suhteen:

$$PP \subset P$$

ja sisältää ykkösalkion; se on siis renkaan A multiplikatiivisen monoidin alimonoidi. Jaollisuustutkimusten tavoitteena on tämän monoidin rakenteen selvittäminen.

Monesti on tarkoituksenmukaista laajentaa jaollisuus renkaassa A koskemaan myös sen jakokunnan K alkioita. Tämän nollasta eroavien alkioiden joukko on kääntyvien alkioiden ryhmä $K^* = K \setminus \{0\}$ ja voidaan samastaa monoidin P jakoryhmän P_P kanssa (määr. 1.2.8).

Määritelmä 3.1.1. Olkoot x, $y \in K^*$. Jos $y = zx$ jollakin $z \in P$, niin sanotaan, että x *jakaa* y:n eli x on y:n *tekijä* ja että y on *jaollinen* x:llä eli x:n *kerrannainen* renkaan A suhteen.

Ehto "x jakaa y:n" merkitään lyhyesti $x \mid y$, ja se voidaan kirjoittaa muotoon $y \in xP$ tai yhtäpitävästi $x^{-1}y \in P$. Sen negaatiolle käytetään merkintää $x \nmid y$.

Huomautus. Toisinaan jaollisuusrelaatio $x \mid y$ laajennetaan koko kuntaan K ehdolla $y \in xA$. Tällöin siis 0 on jokaisen alkion $x \in K$ kerrannainen.

Lemma 3.1.2. *Olkoot x, y, $z \in K^*$. Tällöin*

i) $x \mid x$;
ii) *jos* $x \mid y$ *ja* $y \mid z$, *niin* $x \mid z$;
iii) *jos* $x \mid y$, *niin* $xz \mid yz$;
iv) *jos* $x \mid y$ *ja* $x \mid z$, *niin* $x \mid y + z$.

Todistus. i) Ehdosta $1 \in P$ seuraa $x \in xP$. ii) Jos $y \in xP$ ja $z \in yP$, niin $z \in xPP \subset xP$. iii) Jos $y \in xP$, niin $yz \in xzP$. iv) Jos $y \in xP$ ja $z \in xP$, niin $y + z \in x(P + P) \subset xA$. □

Kohdat i) ja ii) merkitsevät. että jaollisuusrelaatio on refleksiivinen ja transitiivinen eli *esijärjestys*. Kohdasta iii) taas seuraa, että se on *yhteensopiva* ryhmän K^* kertolaskun kanssa:

$$x_1 \mid y_1 \text{ ja } x_2 \mid y_2 \;\Rightarrow\; x_1x_2 \mid y_1y_2.$$

Huomautus. Kohta iii) pätee myös kääntäen: kaikilla x, y, $z \in K^*$

$$xz \mid yz \;\Rightarrow\; x \mid y.$$

(Kerrotaan käänteisalkiolla z^{-1}.)

Liittoalkiot. Vaikka jaollisuusrelaatio on esijärjestys, se ei yleensä ole järjestys, koska antisymmetria puuttuu. Kaksi eri alkiota x, $y \in K^*$ voivat kumpikin jakaa toisensa. Järjestetty joukko voidaan kuitenkin muodostaa siirtymällä ekvivalenssiluokkiin.

MÄÄRITELMÄ 3.1.3. Alkiot x, $y \in K^*$ ovat toistensa *liittoalkioita*, jos

$$x \mid y \quad \text{ja} \quad y \mid x.$$

Liittoalkiorelaatio on selvästi symmetrinen ja lisäksi lemman 3.1.2 kohtien i) ja ii) nojalla refleksiivinen ja transitiivinen; se on siis *ekvivalenssirelaatio*. Se on myös yhteensopiva kertolaskun kanssa kuten jaollisuusrelaatio.

Yhteensopivuuden vuoksi ykkösalkion liittoalkioiden joukko on multiplikatiivisen ryhmän K^* aliryhmä (lause 1.3.6). Se on renkaan A kääntyvien alkioiden ryhmä

$$A^* = \{x \in A \mid x \neq 0, x^{-1} \in A\},$$

joka on suurin renkaaseen A sisältyvä K^*:n aliryhmä. Jaollisuutta käsiteltäessä sen alkioita sanotaan usein renkaan A *yksiköiksi*.

Alkioiden $x \in K^*$ liittoalkioluokat ovat tällöin niiden sivuluokat aliryhmän A^* suhteen (lause 1.3.6) ja niiden joukko on tekijäryhmä

$$K^*/A^*.$$

Kaksi alkiota x, $y \in K^*$ ovat siis toistensa liittoalkioita, jos ja vain jos $x^{-1}y \in A^*$ eli $y = ux$ jollakin $u \in A^*$.

Jaollisuusrelaatio on yhteensopiva liittoalkiorelaation kanssa transitiivisuutensa nojalla, joten liittoalkioluokkien välille voidaan määritellä tekijärelaatio asettamalla

$$xA^* \leq yA^* \;\Leftrightarrow\; x \mid y.$$

Relaatio on refleksiivinen ja transitiivinen kuten jaollisuusrelaatio ja lisäksi antisymmetrinen suoraan liittoalkiorelaation määritelmän perusteella. Se on siten *järjestysrelaatio*. Se on myös yhteensopiva kertolaskun kanssa kuten jaollisuusrelaatio, mikä merkitsee, että K^*/A^* on *järjestetty ryhmä*.

Alkion $x \in K^*$ luokkaa xA^* sanotaan myös sen *divisoriksi* $\operatorname{div}(x)$. Jaollisuusrelaatio saa tällöin muodon

$$x \mid y \;\Leftrightarrow\; \operatorname{div}(x) \leq \operatorname{div}(y).$$

Divisorien laskutoimitus merkitään yhteenlaskuksi:

$$\operatorname{div}(xy) = \operatorname{div}(x) + \operatorname{div}(y).$$

Yksikköjen $u \in A^*$ divisori on $\operatorname{div}(u) = 0$.

Monoidi $P = A \setminus \{0\}$ sisältää alkioittensa liittoalkiot, ja liittoalkioluokkien joukko on tekijämonoidi P/A^*. Se on järjestetyn ryhmän K^*/A^* alimonoidi, joka koostuu ehdon $xA^* \geq A^*$ täyttävistä luokista eli *positiivisista divisoreista* $\operatorname{div}(x) \geq 0$. Jokainen divisori on kahden positiivisen divisorin erotus.

Jaottomat alkiot. Jokainen kokonaisalueen A alkio $x \neq 0$ on jaollinen itsellään ja liittoalkioillaan sekä lisäksi ykkösalkiolla ja sen liittoalkioilla eli yksiköillä $u \in A^*$. Näitä voidaan pitää alkion x *epäaitoina tekijöinä.*

MÄÄRITELMÄ 3.1.4. Alkio $p \in A$ on *jaoton*, jos $p \neq 0$, $p \notin A^*$ ja p:n ainoat tekijät renkaassa A ovat sen liittoalkiot ja yksiköt.

Järjestetyssä tekijäryhmässä K^*/A^* ehto merkitsee, että liittoalkioluokka pA^* on minimaalinen kaikkien neutraalialkiota A^* suurempien alkioiden xA^* $(x \in A \setminus \{0\}, x \notin A^*)$ joukossa eli $\operatorname{div}(p)$ on *minimaalinen aidosti positiivinen divisori.*

Esimerkki 1) Olkoon A kunnan $\mathbf{C}$ alirengas $\mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[i\sqrt{5}]$. Osoitetaan, että alkio $p = 2$ on jaoton A:ssa.

Ensinnäkin se ei ole yksikkö, koska $2^{-1} = 1/2 \notin A$. Olkoon sitten 2 kahden A:n alkion tulo:

$$2 = (x + yi\sqrt{5})(u + vi\sqrt{5}), \qquad x, y, u, v \in \mathbf{Z}.$$

Kompleksilukujen moduleista saadaan tällöin yhtälö

$$4 = |2|^2 = (x^2 + 5y^2)(u^2 + 5v^2).$$

Koska oikean puolen tekijät ovat positiivisia kokonaislukuja, on olemassa kolme mahdollisuutta:

$$x^2 + 5y^2 = 1,\ 2 \text{ tai } 4.$$

Tämä on mahdollista vain, jos $y = 0$ ja $x = \pm 1$ tai $x = \pm 2$. Edellisessä tapauksessa tekijä $x + yi\sqrt{5}$ on yksikkö ja jälkimmäisessä tapauksessa alkion 2 liittoalkio. Siis $p = 2$ on jaoton renkaassa $A = \mathbf{Z}[\sqrt{-5}]$.

Samalla tavalla voidaan osoittaa, että esimerkiksi alkiot 3 ja $1 \pm i\sqrt{5}$ ovat jaottomia A:ssa.

LAUSE 3.1.5. *Olkoon $p \in A$, $p \neq 0$ ja $p \notin A^*$. Jos kaikilla $x, y \in A \setminus \{0\}$ pätee ehto*

$$\text{(P)} \qquad p \mid xy \;\Rightarrow\; p \mid x \text{ tai } p \mid y,$$

niin p on jaoton.

Todistus. Olkoon $x \in A \setminus \{0\}$ jokin alkion p tekijä. On osoitettava, että x on joko yksikkö tai p:n liittoalkio.

Oletuksen mukaan $p = xy$ jollakin $y \in A \setminus \{0\}$. Tällöin p jakaa tulon xy, ja siten ehdon (P) ollessa voimassa pätee $p \mid x$ tai $p \mid y$. Edellisessä tapauksessa x on p:n liittoalkio. Jos taas $p \mid y$, niin ehdosta $xy \mid y$ seuraa $x \mid 1$, ja silloin x on yksikkö. □

Huomautus. Kaikki jaottomat alkiot eivät välttämättä toteuta ehtoa (P), ellei renkaassa ole voimassa yksikäsitteinen jako alkutekijöihin. Alkioita, jotka sen toteuttavat, sanotaan toisinaan *alkualkioiksi.*

Esimerkki 2) Alkio $p = 2$ on jaoton renkaassa $A = \mathbf{Z}[\sqrt{-5}]$ (esim. 3.1.1). Se ei kuitenkaan toteuta ehtoa (P), koska se jakaa tulon

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$$

mutta ei kumpaakaan sen tekijöistä.

Harjoitustehtäviä

1) Olkoon $A = \mathbf{Z}[\sqrt{-5}]$. Osoitettava, että luvut 3 ja $2 + \sqrt{-5}$ ovat jaottomia renkaassa A ja että $2 + \sqrt{-5}$ jakaa luvun $9 = 3 \cdot 3$ mutta ei lukua 3.

2) Olkoon A pääideaalirengas. Osoitettava, että alkio $p \in A$ on jaoton, jos ja vain jos $p \neq 0$ ja p:n virittämä ideaali on maksimaalinen.

3) Olkoon A kokonaisalue ja K sen jakokunta. Olkoot a ja b kaksi K^*:n alkiota, joilla on suurin yhteinen tekijä $d \in K^*$ (ts. $c|d$, jos ja vain jos $c|a$ ja $c|b$, kun $c \in K^*$). Osoitettava, että $m = ab/d$ on a:n ja b:n pienin yhteinen kerrannainen.

3.2. Faktoriaaliset renkaat

Olkoon A kokonaisalue. Tässä pykälässä tutkitaan, millä ehdoilla joukon $P = A \setminus \{0\}$ alkiot voidaan esittää oleellisesti yksikäsitteisesti jaottomien alkioiden tuloina. Aivan yksikäsitteinen esitys ei yleensä voi olla, koska jaottomat alkiot voidaan korvata liittoalkioillaan. Siksi on aluksi valittava näiden joukosta sopivat edustajat.

Olkoon $(p_i)_{i \in I}$ perhe A:n jaottomia alkioita, jossa on jokaisesta liittoalkioluokasta yksi alkio, eli A:n *jaottomien alkioiden edustajisto.*

Esimerkki 1) Kokonaislukujen renkaassa $\mathbf{Z}$ alkuluvut $2, 3, 5, \ldots$, muodostavat jaottomien alkioiden edustajiston. Toinen edustajisto saadaan alkulukujen vastaluvuista.

Tavoite voidaan nyt täsmällisemmin esittää muodossa: Jokaisella alkiolla $x \in P$ on yksikäsitteinen esitys

$$x = u \prod_{i \in I} p_i^{n_i},$$

missä $u \in A^*$ on yksikkö ja $(n_i) \in \mathbf{N}^{(I)}$ on äärelliskantajainen perhe.

Yhtäpitävästi tämä merkitsee, että jokaisella P:n liittoalkioluokalla $xA^* \in P/A^*$ on yksikäsitteinen esitys

$$xA^* = \prod_{i\in I} p_i^{n_i} A^* = \prod_{i\in I} (p_i A^*)^{n_i}$$

tai vielä

$$\operatorname{div}(x) = \sum_{i\in I} n_i \operatorname{div}(p_i),$$

missä $(n_i) \in \mathbf{N}^{(I)}$. Tällöin tekijämonoidi P/A^* on isomorfinen vapaan vaihdannaisen monoidin $\mathbf{N}^{(I)}$ kanssa.

Vastaavat esitykset voidaan ulottaa kokonaisalueen A jakokuntaan K, jolloin eksponentit n_i voivat olla myös negatiivisia. Monoidin $\mathbf{N}^{(I)}$ tilalle tulee silloin vapaa vaihdannainen ryhmä $\mathbf{Z}^{(I)}$. Tämä on tarkastelujen kannalta edullista, koska ryhmien käsittely on yleensä helpompaa kuin monoidien käsittely.

Olkoon nyt $(p_i)_{i\in I}$ jokin perhe A:n nollasta eroavia alkioita. Tutkitaan mahdollisuuksia esittää kunnan K alkioita alkioiden p_i tuloina ja osamäärinä. Olkoon

$$\varphi\colon \mathbf{Z}^{(I)} \to K^*/A^*$$

perheeseen $(p_i A^*)_{i\in I}$ liittyvä homomorfismi (lause 1.6.2)

$$(n_i)_{i\in I} \mapsto \prod_{i\in I} p_i^{n_i} A^*.$$

Edellä on nähty, että K^*/A^* on järjestetty ryhmä. Vapaa ryhmä $\mathbf{Z}^{(I)}$ on myös järjestetty ryhmä, kun se varustetaan järjestyksellä

$$(n_i)_{i\in I} \le (m_i)_{i\in I} \iff n_i \le m_i \quad (i \in I).$$

Homomorfismi φ säilyttää tällöin järjestyksen, koska ehdoista $n_i \le m_i$ $(i \in I)$ seuraa

$$\prod_{i\in I} p^{n_i} \mid \prod_{i\in I} p^{m_i}.$$

Tämä merkitsee, että φ on *järjestettyjen ryhmien homomorfismi.* Tavoitteena on selvittää, milloin φ on järjestettyjen ryhmien isomorfismi.

Huomautus. Tähän ei riitä, että φ on bijektiivinen. Lisäksi vaaditaan, että käänteinen homomorfismi φ^{-1} myös säilyttää järjestyksen, eli että positiivisten divisorien monoidi P/A^* vastaa monoidia $\mathbf{N}^{(I)}$.

LEMMA 3.2.1. *Jos φ on järjestettyjen ryhmien isomorfismi, niin*

i) *jokainen p_i $(i \in I)$ on jaoton,*
ii) *jokainen jaoton $p \in A$ on yhden ja vain yhden alkion p_i $(i \in I)$ liittoalkio,*
iii) *jokainen jaoton $p \in A$ toteuttaa ehdon* (P) *(*ks. lause 3.1.5*).*

Todistus. i) Olkoon j jokin joukon I alkio. Tarkastellaan alkion p_j tekijöitä $x \in P$. Kun φ on isomorfismi, jokaisella alkiolla $x \in K^*$ on yksikäsitteinen esitys

$$x = u \prod_{i \in I} p_i^{n_i},$$

missä $u \in A^*$ ja $(n_i) \in \mathbf{Z}^{(I)}$. Järjestyksen säilyessä ehto $x \in P$ eli $1 \mid x$ on yhtäpitävä relaatioiden $0 \leq n_i$ $(i \in I)$ kanssa. Vastaavasti x on alkion $p_j = \prod_{i \in I} p_i^{\delta_{ij}}$ tekijä, jos ja vain jos $n_i \leq \delta_{ij}$ kaikilla $i \in I$.

Yhdessä ehdot merkitsevät, että $n_i = 0$, kun $i \neq j$ ja

$$n_j = 0 \quad \text{tai} \quad n_j = 1.$$

Edellisessä tapauksessa $x = u$ on yksikkö ja jälkimmäisessä tapauksessa $x = up_j$ on p_j:n liittoalkio. Koska muita mahdollisuuksia ei ole, p_j on jaoton.

ii) Olkoon $p \in P$. Kun φ on isomorfismi, on olemassa yksikäsitteinen esitys

$$p = u \prod_{i \in I} p_i^{n_i},$$

missä $u \in A^*$ ja $(n_i) \in \mathbf{N}^{(I)}$. Jos p on jaoton, niin $n_i > 0$ jollakin $i \in I$, koska $p \notin A^*$. Tällöin p_i jakaa p:n, joten sen täytyy olla p:n liittoalkio. Kun tuloesitys on yksikäsitteinen, myös i on yksikäsitteinen.

iii) Olkoon $p \in P$ jaoton ja olkoot x, y kaksi P:n alkiota. Kun φ on järjestettyjen ryhmien isomorfismi, on olemassa yksikäsitteiset tuloesitykset

$$x = u \prod_{i \in I} p_i^{n_i}, \qquad u \in A^*,\ (n_i) \in \mathbf{N}^{(I)},$$

ja

$$y = v \prod_{i \in I} p_i^{m_i}, \qquad v \in A^*,\ (m_i) \in \mathbf{N}^{(I)}.$$

Lisäksi kohdan ii) nojalla

$$p = ep_j = e \prod_{i \in I} p_i^{\delta_{ij}}$$

joillakin $e \in A^*$ ja $j \in I$. Ehto $p \mid xy$, eli $\operatorname{div}(p) \leq \operatorname{div}(x) + \operatorname{div}(y)$, on tällöin yhtäpitävä epäyhtälöiden

$$\delta_{ij} \leq n_i + m_i \qquad (i \in I)$$

kanssa. Koska n_i, $m_i \in \mathbf{N}$ $(i \in I)$, nämä supistuvat ehdoksi

$$1 = \delta_{jj} \leq n_j + m_j,$$

joka merkitsee, että $n_j > 0$ tai $m_j > 0$ eli yhtäpitävästi

$$p \mid x \quad \text{tai} \quad p \mid y.$$

Jaoton alkio p toteuttaa siis ehdon (P). □

LAUSE 3.2.2. *Olkoon A kokonaisalue, K sen jakokunta ja $P = A \setminus \{0\}$. Seuraavat ehdot ovat yhtäpitävät.*

a) *K^*/A^* on isomorfinen jonkin järjestetyn ryhmän $\mathbf{Z}^{(I)}$ kanssa.*

b) *Jokainen jaoton alkio $p \in A$ toteuttaa ehdon* (P), *ja lisäksi*

(MIN) *jokainen epätyhjä divisorijoukko $E \subset P/A^*$ sisältää minimaalisen alkion.*

Todistus. a) $\Rightarrow$ b): Olkoon $\varphi\colon \mathbf{Z}^{(I)} \to K^*/A^*$ jokin järjestettyjen ryhmien isomorfismi. Tällöin kaikilla $i \in I$ pätee

$$\varphi(\delta_i) \geq \varphi(0) = 1A^*,$$

koska $\delta_i = (\delta_{ij})_{j \in I} \geq 0$. Tämä merkitsee, että

$$\varphi(\delta_i) = p_i A^* = \operatorname{div}(p_i)$$

jollakin $p_i \in P$, joten φ on perheeseen $(p_i A^*)_{i \in I}$ liittyvä isomorfismi. Jokainen jaoton $p \in A$ toteuttaa siten ehdon (P) (lemma 3.2.1, iii).

Ehdon (MIN) todistamiseksi tarkastellaan epätyhjää osajoukkoa $E \subset K^*/A^*$. Sen alkioilla on yksikäsitteinen esitys

$$\operatorname{div}(x) = \sum_{i \in I} n_i \operatorname{div}(p_i),$$

missä $(n_i) \in \mathbf{N}^{(I)}$. Valitaan näiden joukosta sellainen, jonka *aste*

$$\deg(\operatorname{div}(x)) = \sum_{i \in I} n_i \geq 0$$

on pienin mahdollinen. Silloin $\operatorname{div}(x)$ on minimaalinen joukossa E.

b) $\Rightarrow$ a): Olkoon $(p_i)_{i \in I}$ jokin A:n jaottomien alkioiden edustajisto. Perheeseen $(p_i A^*)_{i \in I}$ liittyvä homomorfismi

$$\varphi\colon \mathbf{Z}^{(I)} \to K^*/A^*, \qquad (n_i) \mapsto \prod_{i \in I} p_i^{n_i} A^*,$$

on tällöin järjestetty homomorfismi.

Osoitetaan aluksi, että φ on surjektiivinen, kun ehto (MIN) on voimassa. Tätä varten on riittävää näyttää, että $\operatorname{Im}(\varphi)$ sisältää tällöin positiivisten divisorien monoidin P/A^*, koska tämä virittää koko divisorien ryhmän K^*/A^*.

Olkoon $E = P/A^* \setminus \operatorname{Im}(\varphi)$. Jos E ei ole tyhjä, niin siinä on minimaalinen alkio $\operatorname{div}(x) = xA^*$, missä $x \in P$. Jos x on jaoton, niin $xA^* = p_i A^*$ jollakin $i \in I$, koska $(p_i)_{i \in I}$ on jaottomien alkioiden edustajisto. Tämä on kuitenkin mahdotonta, koska $p_i A^*$ on kuvassa $\operatorname{Im}(\varphi)$.

Alkion x täytyy siis olla jaollinen, eli

$$x = yz$$

joillakin P:n alkioilla y ja z, joista kumpikaan ei ole kääntyvä. Tällöin pätee

$$\operatorname{div}(x) = \operatorname{div}(y) + \operatorname{div}(z), \quad \operatorname{div}(y) > 0,\ \operatorname{div}(z) > 0$$

ja siten $\operatorname{div}(y) < \operatorname{div}(x)$ ja $\operatorname{div}(z) < \operatorname{div}(x)$. Minimaalisuuden nojalla $\operatorname{div}(y)$ ja $\operatorname{div}(z)$ ovat silloin kuvassa $\operatorname{Im}(\varphi)$, ja samoin on niiden summa $\operatorname{div}(x)$ vastoin oletusta. Ristiriita osoittaa, että E on tyhjä, ja että siten φ on surjektiivinen.

Todistuksen päätteeksi näytetään, että

$$\varphi^{-1}(P/A^*) = \mathbf{N}^{(I)},$$

kun jokainen jaoton alkio $p \in A$ toteuttaa ehdon (P). Tämä merkitsee, että kaikilla $(n_i) \in \mathbf{Z}^{(I)}$

$$\prod_{i \in I} p_i^{n_i} \in P \;\Leftrightarrow\; n_i \geq 0 \quad (i \in I).$$

Koska P sisältää alkiot p_i, on selvää, että se sisältää myös tulon $\prod_{i \in I} p^{n_i}$, kun $n_i \geq 0$ $(i \in I)$.

Oletetaan sitten kääntäen, että $(n_i) \in \mathbf{Z}^{(I)}$ ja $\prod_{i \in I} p_i^{n_i} \in P$. Olkoot I^+ ja I^- ehtojen $n_i > 0$ ja $n_i < 0$ määrittelemät I:n osajoukot. Silloin ehdosta

$$\prod_{i \in I} p_i = \prod_{i \in I^+} p_i^{n_i} (\prod_{i \in I^-} p_i^{-n_i})^{-1} \in P,$$

seuraa

$$\prod_{i \in I^-} p_i^{|n_i|} \mid \prod_{i \in I^+} p_i^{n_i}.$$

Jos tällöin $j \in I^-$, niin p_j on vasemmanpuolisen tulon tekijä ja jakaa siten tulon $\prod_{i \in I^+} p_i^{n_i}$. Soveltamalla toistuvasti ehtoa (P) nähdään, että p_j jakaa jonkin tekijöistä p_i $(i \in I^+)$. Koska kumpikin on jaoton, p_i:n ja p_j:n täytyy olla toistensa liittoalkioita. Tämä on kuitenkin mahdotonta, koska $i \neq j$ ja $(p_i)_{i \in I}$ on jaottomien alkioiden edustajisto. Joukon I^- täytyy siis olla tyhjä, ja siten pätee $n_i \geq 0$ kaikilla $i \in I$.

Homomorfismi φ ytimen muodostavat ne perheet $(n_i) \in \mathbf{Z}^{(I)}$, jotka toteuttavat ehdon $\prod_{i \in I} p_i^{n_i} \in A^*$ eli yhtäpitävästi

$$\prod_{i \in I} p_i^{n_i} \in P \quad \text{ja} \quad \prod_{i \in I} p_i^{-n_i} \in P.$$

Yllä esitetyn nojalla tämä merkitsee, että $n_i = 0$ kaikilla $i \in I$, kun jokainen jaoton $p \in A$ toteuttaa ehdon (P). Homomorfismi φ on siten bijektiivinen, kun kohdan b) ehdot ovat voimassa. Se on tällöin myös järjestettyjen ryhmien isomorfismi, koska positiivisten alkioiden alimonoidit vastaavat toisiaan:

$$\varphi(\mathbf{N}^{(I)}) = P/A^*.$$

□

MÄÄRITELMÄ 3.2.3. Rengas A on *faktoriaalinen*, jos se on kokonaisalue ja järjestetty ryhmä K^*/A^*, missä K on A:n jakokunta, on isomorfinen jonkin järjestetyn ryhmän $\mathbf{Z}^{(I)}$ kanssa.

Edellä esitetyn mukaan määritelmä on yhtäpitävä seuraavan kanssa.

Jos $(p_i)_{i\in I}$ on kokonaisalueen A jaottomien alkioiden edustajisto, niin jokaisella alkiolla $x \in A \setminus \{0\}$ (tai $x \in K^*$) on yksikäsitteinen esitys

$$x = u \prod_{i\in I} p_i^{n_i},$$

missä $u \in A^*$ ja $(n_i) \in \mathbf{N}^{(I)}$ (tai $(n_i) \in \mathbf{Z}^{(I)}$).

Lause 3.2.2 antaa välttämättömät ja riittävät ehdot renkaan faktoriaalisuudelle.

Esimerkkejä. 2) Kokonaislukujen rengas on faktoriaalinen. Tämä on hyvin tunnettua ja todistetaan seuraavassa uudelleen.

3) Rengas $A = \mathbf{Z}[i\sqrt{5}]$ ei ole faktoriaalinen, koska siinä on jaottomia alkioita, jotka eivät toteuta ehtoa (P) (ks. esim. 3.1.2). Esimerkiksi luvulla 6 on kaksi tuloesitystä

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}),$$

missä tekijät 2, 3 ja $1 \pm i\sqrt{5}$ ovat jaottomia renkaassa A (ks. esim. 3.1.1) mutta eivät toistensa liittoalkioita, koska $A^* = \{1, -1\}$.

Eukleideen renkaat.

MÄÄRITELMÄ 3.2.4. Rengas A on *Eukleideen rengas*, jos se on kokonaisalue, ja on olemassa kuvaus $w\colon P = A \setminus \{0\} \to \mathbf{N}$, joka toteuttaa ehdot

i) $w(xy) \geq w(y)$ kaikilla x, $y \in P$;
ii) jos a, $b \in P$, niin on olemassa sellaiset q, $r \in A$, että $a = bq + r$ ja $r = 0$ tai $w(r) < w(b)$.

Kuvausta w sanotaan toisinaan *Eukleideen normiksi.* Ehdosta i) seuraa

$$\text{jos } x, y \in P \text{ ja } x \mid y, \text{ niin } w(x) \leq w(y).$$

Tällöin siis erityisesti $w(x) = w(y)$ aina kun x ja y ovat toistensa liittoalkioita.

Esimerkkejä. 4) Kokonaislukujen rengas $\mathbf{Z}$ on Eukleideen rengas, sillä $w(x) = |x|$ toteuttaa ehdot i) ja ii).

5) Polynomirengas $A = K[X]$ on Eukleideen rengas, kun K on kunta. Tällöin voidaan valita $w(f) = \deg(f)$, kun $f \neq 0$.

6) *Gaussin kokonaislukujen* rengas

$$A = \mathbf{Z}[i] = \{x + yi \mid x, y \in \mathbf{Z}\}$$

on Eukleideen rengas norminaan modulin neliö

$$w(x + yi) = |x + yi|^2 = x^2 + y^2 \in \mathbf{N}.$$

Todistus. i) Jos x, $y \in A \setminus \{0\}$, niin $|x|^2 \geq 1$ ja siten

$$w(xy) = |xy|^2 = |x|^2|y|^2 \geq |y|^2 = w(y).$$

ii) Olkoot a, $b \in A \smallsetminus \{0\}$. Osamäärä a/b voidaan kirjoittaa muotoon

$$a/b = \alpha + \beta i,$$

missä α, $\beta \in \mathbf{Q}$, koska A:n jakokunta on $\mathbf{Q}(i)$. Valitaan sellaiset kokonaisluvut u ja v, että

$$|\alpha - u| \le \tfrac{1}{2}, \quad |\beta - v| \le \tfrac{1}{2}.$$

Tällöin $q = u + vi \in A$ ja

$$\begin{aligned} |a - bq|^2 &= |(\alpha + \beta i) - (u + vi)|^2 |b|^2 \\ &= [(\alpha - u)^2 + (\beta - v)^2]|b|^2 \\ &\le \tfrac{1}{2}|b|^2 < |b|^2. \end{aligned}$$

□

Kaikki nämä esimerkkirenkaat ovat faktoriaalisia. Tämän todistamiseksi esitetään ensin aputulos.

LEMMA 3.2.5. *Eukleideen renkaan jokainen ideaali on pääideaali.*

Todistus. Olkoon A Eukleideen rengas, $\mathfrak{a}$ sen ideaali ja w jokin Eukleideen normi A:ssa. Koska $\{0\}$ on pääideaali, voidaan olettaa, että $\mathfrak{a}$:ssa on alkioita $a \neq 0$. Niistä voidaan valita sellainen, jolla $w(a)$ on pienin mahdollinen. Osoitetaan, että tällöin a virittää $\mathfrak{a}$:n.

Jokainen $b \in \mathfrak{a}$ voidaan esittää muodossa $b = aq + r$, missä q, $r \in A$ ja $r = 0$ tai $w(r) < w(a)$. Tällöin $r = b - aq \in \mathfrak{a}$, koska $\mathfrak{a}$ on ideaali. Jos $r \neq 0$, niin $w(a)$:n minimaalisuuden nojalla olisi $w(r) \ge w(a)$ vastoin edellä esitettyä. Siis täytyy olla $r = 0$ ja siten $b = aq$ on a:n virittämässä ideaalissa. □

LAUSE 3.2.6. *Jokainen Eukleideen rengas on faktoriaalinen.*

Todistus. Olkoon A Eukleideen rengas, $P = A \smallsetminus \{0\}$ ja $w\colon P \to \mathbf{N}$ Eukleideen normi. On riittävää osoittaa, että lauseen 3.2.2 ehto (MIN) on voimassa, ja että jokainen jaoton $p \in A$ toteuttaa ehdon (P) (ks. lause 3.1.5).

Olkoon E monoidin P/A^* epätyhjä osajoukko. Eukleideen normin arvo $w(a) \in \mathbf{N}$ on vakio jokaisessa liittoalkioluokassa $\operatorname{div}(a) = aA^*$. Valitaan $\operatorname{div}(a) \in E$ siten, että $w(a)$ on pienin mahdollinen. On riittävää osoittaa, että $\operatorname{div}(a)$ on tällöin minimaalinen joukossa E.

Olkoon $\operatorname{div}(b) \in E$ ja $\operatorname{div}(b) \le \operatorname{div}(a)$ eli $b \mid a$. Näytetään, että tällöin $\operatorname{div}(b) = \operatorname{div}(a)$. Joka tapauksessa on ehdon ii) nojalla olemassa alkiot q, $r \in A$, jotka toteuttavat ehdot

$$b = aq + r, \quad r = 0 \text{ tai } w(r) < w(a).$$

Toisaalta ehdosta $b \mid a$ seuraa $a = pb$ jollakin $p \in P$. Tällöin saadaan

$$(1 - pq)b = r.$$

Jos $1 - pq \neq 0$, niin $w(r) \ge w(b)$ ehdon i) mukaan. Mutta tällöin olisi $w(b) < w(a)$ vastoin arvon $w(a)$ minimaalisuutta. Siis täytyy olla

$r = 0$, joten $a \mid b$ ja $\mathrm{div}(b) = \mathrm{div}(a)$ kuten oli osoitettava. Ehto (MIN) on siten voimassa.

Olkoon $p \in A$ jaoton ja olkoot x, y kaksi P:n alkiota, joiden tulo on jaollinen p:llä. On osoitettava, että p jakaa ainakin toisen alkioista x ja y.

Oletetaan, että x ei ole jaollinen p:llä. Koska alkioiden x ja p virittämä ideaali on pääideaali (lemma 3.2.5), sillä on virittäjä

$$d = ax + bp,$$

missä a, $b \in A$. Tällöin d jakaa sekä x:n että p:n. Koska p on jaoton, d on joko yksikkö tai p:n liittoalkio. Jos se olisi p:n liittoalkio, niin x olisi jaollinen p:llä vastoin oletusta.

Siten d:llä on käänteisalkio d' renkaassa A. Jokainen alkio $y \in A$ voidaan siis kirjoittaa muotoon

$$y = yd'd = (ad')xy + (byd')p,$$

joten se on jaollinen p:llä, kun xy on sillä jaollinen. Jaoton alkio p toteuttaa siis ehdon (P). □

Huomautus. Ei ole vaikeaa osoittaa, että jokainen pääideaalirengas on faktoriaalinen (harj. teht.)

Harjoitustehtäviä

Olkoon A kokonaisalue, K sen jakokunta ja $P = A \setminus \{0\}$.

1) Olkoon E järjestetyn joukon P/A^* epätyhjä osajoukko. Osoitettava:

i) Jos E:ssä ei ole minimaalista alkiota, niin P:ssä on sellainen jono $(x_n)_{n \in \mathbf{N}}$, että $x_{n+1} \mid x_n$ ja $x_n \nmid x_{n+1}$ kaikilla $n \in \mathbf{N}$.

ii) Jos $x_n \in P$ $(n \in \mathbf{N})$, $x_{n+1} \mid x_n$ kaikilla $n \in \mathbf{N}$ ja perheen $(x_n)_{n \in \mathbf{N}}$ virittämä ideaali $\mathfrak{a} \subset A$ on pääideaali, niin $\mathfrak{a} = Ax_n$ jollakin $n \in \mathbf{N}$ ja siten $x_n \mid x_k$ kaikilla $k \in \mathbf{N}$.

Pääteltävä, että E:ssä on minimaalinen alkio, jos A on pääideaalirengas.

2) Olkoot $x, y \in P$ keskenään jaottomat, ts. jos $z \in K^*$, $z|x$ ja $z|y$, niin $z|1$, eli 1 on x:n ja y:n suurin yhteinen tekijä. Osoitettava:

i) Jos $z \in P$, $x|z$ ja $y|z$, niin $xy|z$, eli xy on x:n ja y:n pienin yhteinen kerrannainen.

ii) Jos $z \in P$ ja $x \mid yz$, niin $x \mid z$ (*Eukleideen lemma*).

3) Olkoon A pääideaalirengas, $p \in A$ jaoton, $x \in A$ ja $p \nmid x$. Osoitettava:

i) $ap + bx = 1$ joillakin $a, b \in A$.

ii) p ja x ovat keskenään jaottomat.

Pääteltävä (tehtävien 1 ja 2 avulla), että pääideaalirengas A on faktoriaalinen.

4) Olkoon p alkuluku. Osoitettava:

i) Jos p ei ole jaoton renkaassa $\mathbf{Z}[i]$, niin $p = x^2 + y^2$ joillakin $x, y \in \mathbf{Z}$ ja siten $p = 2$ tai $p \equiv 1 \pmod 4$.

ii) Jos $p = 4k + 1$, $k \in \mathbf{N}$, niin on olemassa $x \in \mathbf{Z}$, jolla $x \not\equiv 0$ ja $x^{2k} - 1 \not\equiv 0 \pmod p$, ja tällöin $p \mid (x^{2k} + 1)$. ($(\mathbf{Z}/p\mathbf{Z})^*$ on syklinen, esim. 4.7.5.)

iii) Jos $p \mid (x^2 + y^2)$, missä $x, y \in \mathbf{Z}$ eivät ole jaollisia p:llä, niin p ei ole jaoton $\mathbf{Z}[i]$:ssä.

Pääteltävä, että p on jaoton renkaassa $\mathbf{Z}[i]$, jos ja vain jos $p \equiv 3 \pmod 4$.

5) Etsittävä luvun $21 + 27i$ alkutekijähajotelma renkaassa $\mathbf{Z}[i]$.

6) Olkoon $A = \mathbf{Z}[\sqrt{2}]$, $K = \mathbf{Q}(\sqrt{2})$ renkaan A jakokunta ja $N(\alpha) = x^2 - 2y^2$ alkion $\alpha = x + y\sqrt{2} \in K$ *normi* $(x, y \in \mathbf{Q})$. Osoitettava:

i) $N(\alpha\beta) = N(\alpha)N(\beta)$ kaikilla $\alpha, \beta \in K$.

ii) $N(\alpha) \in \mathbf{Z}$, kun $\alpha \in A$.

iii) Jos $\alpha \in K$, niin $|N(\alpha - a)| < 1$ jollakin $a \in A$.

Pääteltävä, että A on Eukleideen rengas. ($w(a) = |N(a)|$.)

3.3. Polynomien jaollisuus

Tässä pykälässä tarkastellaan yhden ja useamman muuttujan polynomeja, joiden kerroinrenkaana on kokonaisalue A.

LAUSE 3.3.1. *Olkoon A kokonaisalue. Jos f, $g \in A[X]$ ja $f \neq 0$, $g \neq 0$, niin $fg \neq 0$ ja $\deg(fg) = \deg(f) + \deg(g)$. Erityisesti $A[X]$ on kokonaisalue.*

Todistus. Olkoot $\deg(f) = n$, $\deg(g) = m$ ja

$$f = \sum_{k=0}^{n} a_k X^k, \quad g = \sum_{l=0}^{m} b_l X^l,$$

missä $a_n \neq 0$ ja $b_m \neq 0$. Tällöin

$$fg = \sum_{p=0}^{n+m} c_p X^p,$$

missä $c_{n+m} = a_n b_m \neq 0$, koska A on kokonaisalue. Siten $fg \neq 0$ ja

$$\deg(fg) = n + m = \deg(f) + \deg(g).$$

□

KOROLLAARI 3.3.2. *Vakion $a \in A$, $a \neq 0$, tekijät polynomirenkaassa $A[X]$ ovat samat kuin sen tekijät renkaassa A.*

Todistus. Jos $f \in A[X]$ ja $f \mid a$, niin $a = fg$ jollakin $g \in A[X]$, $g \neq 0$. Tällöin

$$\deg(f) + \deg(g) = \deg(a) = 0,$$

joten f ja g ovat kumpikin vakioita. □

Seurauksena korollaarista saadaan erityisesti

$$A[X]^* = A^*,$$

koska alkion 1 tekijät ovat vakioita, ja

$$p \in A \text{ on jaoton } A[X]\text{:ssä} \Leftrightarrow p \text{ on jaoton } A\text{:ssa.}$$

LEMMA 3.3.3. *Vakio $c \in A$, $c \neq 0$, jakaa polynomin $f = \sum_i a_i X^i$ renkaassa $A[X]$, jos ja vain jos c jakaa f:n kertoimet a_i $(i \in \mathbf{N})$ A:ssa.*

Todistus. Jos f on jaollinen c:llä, niin $f = cg$ jollakin

$$g = \sum_i b_i X^i \in A[X],$$

ja tällöin jokainen $a_i = cb_i$ on jaollinen c:llä. Käänteinen väite on selvä. □

MÄÄRITELMÄ 3.3.4. Polynomi $f \in A[X]$, $f \neq 0$, on *primitiivinen*, jos sen kertoimien yhteiset tekijät A:ssa ovat kääntyviä.

Esimerkki 1) Jokainen jaoton polynomi on primitiivinen (ks. lemma 3.3.3). Polynomi $f = X^2 - 1$ on primitiivinen mutta ei jaoton.

LAUSE 3.3.5 (Gaussin lemma). *Jos A on faktoriaalinen rengas ja f, $g \in A[X]$ ovat primitiivisiä polynomeja, niin fg on primitiivinen.*

Todistus. Olkoon A faktoriaalinen ja olkoot

$$f = \sum_{i \in \mathbf{N}} a_i X^i, \quad g = \sum_{j \in \mathbf{N}} b_j X^j$$

primitiivisiä polynomeja. Jos

$$fg = \sum_{k \in \mathbf{N}} \Big(\sum_{i+j=k} a_i b_j \Big) X^k.$$

ei ole primitiivinen, niin sen kertoimilla on yhteinen tekijä $c \in A$, $c \neq 0$, joka ei ole yksikkö. Tällöin c:llä on jaoton tekijä $p \in A$, joka toteuttaa ehdot

$$p \mid \sum_{i+j=k} a_i b_j \qquad (k \in \mathbf{N}).$$

Koska f ja g ovat primitiivisiä, kaikki kertoimet a_i ja b_j eivät ole jaollisia p:llä. Olkoot n, $m \in \mathbf{N}$ pienimmät luvut, joilla

$$p \nmid a_n \quad \text{ja} \quad p \nmid b_m.$$

Tällöin p jakaa summassa

$$(a_0 b_{n+m} + \cdots + a_{n-1} b_{m+1}) + a_n b_m + (a_{n+1} b_{m-1} + \cdots a_{m+n} b_0)$$

ensimmäisen ja viimeisen osasumman, ja koska koko summa on p:llä jaollinen, p jakaa myös keskimmäisen termin:

$$p \mid a_n b_m.$$

Tämä on kuitenkin mahdotonta, koska A:n ollessa faktoriaalinen jaoton alkio p toteuttaa ehdon (P) (lause 3.2.2, b). Tulon fg täytyy siten olla primitiivinen. □

Olkoon K kokonaisalueen A jakokunta. Polynomirengas $K[X]$ on tällöin Eukleideen rengas (esim. 3.2.5) ja siksi faktoriaalinen (lause 3.2.6). Renkaan $K[X]$ jakokunta on *murtolausekkeiden* kunta $K(X)$, jonka alkiot ovat esitettävissä osamäärinä f/g, missä f, $g \in K[X]$ ja $g \neq 0$.

Huomautus. Jokainen osamäärä f/g voidaan laventaa muotoon

$$(af)/(ag),$$

missä $a \in A$, $a \neq 0$, ja af, $ag \in A[X]$. Tämä osoittaa, että $K(X)$ on myös kokonaisalueen $A[X]$ jakokunta.

LEMMA 3.3.6. *Jos A on faktoriaalinen, niin jokaisella polynomilla $f \in K[X]$, $f \neq 0$, on esitys*

$$f = cg,$$

missä $c \in K^*$ ja $g \in A[X]$ on primitiivinen. Tällöin vakio $a \in K^*$ jakaa polynomin f, jos ja vain jos se jakaa c:n.

Todistus. Olkoon A faktoriaalinen, $(p_i)_{i \in I}$ sen jaottomien alkioiden edustajisto ja

$$f = \sum_{k=0}^{n} a_k X^k, \quad a_0, \ldots, a_n \in K.$$

Olkoon H niiden indeksien $k \in [0, n]$ joukko, joilla $a_k \neq 0$. Jokaisella indeksillä $k \in H$ on tällöin olemassa yksikäsitteinen esitys

$$a_k = u_k \prod_{i \in I} p_i^{n_{ki}},$$

missä $u_k \in A^*$ ja $(n_{ki})_{i \in I} \in \mathbf{Z}^{(I)}$.

Jokaisella $i \in I$ olkoon

$$n_i = \min_{k \in H} n_{ki} \in \mathbf{Z}.$$

Perheellä $(n_i)_{i \in I}$ on äärellinen kantaja, koska kaikkiaan vain äärellisen moni n_{ki} on $\neq 0$. Tällöin $c = \prod_{i \in I} p_i^{n_i}$ on hyvin määritelty K^*:n alkio, ja kaikilla $k \in H$ pätee

$$c^{-1} a_k = u_k \prod_{i \in I} p_i^{n_{ki} - n_i} \in A,$$

koska $n_i \leq n_{ki}$ $(i \in I)$. Polynomi

$$g = c^{-1} f = \sum_{k=0}^{n} b_k X^k$$

on siten renkaassa $A[X]$.

Olkoon nyt $a \in K^*$ vakio. Osoitetaan, että a jakaa f:n, jos ja vain jos se jakaa c:n. Olkoon

$$a = u \prod_{i \in I} p_i^{m_i},$$

missä $u \in A^*$ ja $(m_i) \in \mathbf{Z}^{(I)}$. Lemman 3.3.3 nojalla a on f:n tekijä, jos ja vain jos se jakaa jokaisen kertoimen a_k $(k \in H)$. Tämä taas merkitsee, että kaikilla $i \in I$ pätee

$$m_i \leq n_{ki} \qquad (k \in H).$$

Koska n_i on pienin luvuista n_{ki}, ehto on yhtäpitävä sen kanssa, että $m_i \leq n_i$ $(i \in I)$ eli $a \mid c$. Lemman viimeinen väite on siten todistettu.

Lopuksi on osoitettava, että g on primitiivinen, eli että jokainen vakio $a \in A$, $a \neq 0$, joka jakaa polynomin g kertoimet, on yksikkö.

Jos a jakaa g:n kertoimet, niin se jakaa g:n. Tällöin ac jakaa polynomin $f = cg$ ja siten yllä esitetyn nojalla $ac \mid c$ eli yhtäpitävästi $a \mid 1$. Vakio a on siis yksikkö, mikä osoittaa, että polynomi g on primitiivinen. □

Lause 3.3.7. *Jos A on faktoriaalinen rengas, niin myös $A[X]$ on faktoriaalinen.*

Todistus. Olkoon A faktoriaalinen rengas ja olkoon $(p_i)_{i \in I}$ sen jaottomien alkioiden edustajisto. Polynomirengas $K[X]$, missä K on A:n jakokunta, on myös faktoriaalinen. Olkoon $(q_j)_{j \in J}$ jokin $K[X]$:n jaottomien alkioiden edustajisto. Voidaan olettaa, että jokainen q_j on alirenkaassa $A[X]$ ja primitiivinen (lemma 3.3.6).

Olkoon $f \neq 0$ renkaan $A[X]$ jakokunnan $K(X)$ alkio. Koska $K[X]$ on faktoriaalinen, on olemassa yksikäsitteinen esitys

$$f = c \prod_{j \in J} q_j^{m_j},$$

missä $c \in K^* = K[X]^*$ ja $(m_j) \in \mathbf{Z}^{(J)}$. Renkaan A faktoriaalisuuden nojalla on edelleen olemassa yksikäsitteinen esitys

$$c = u \prod_{i \in I} p_i^{n_i},$$

missä $u \in A^*$ ja $(n_i) \in \mathbf{Z}^{(I)}$. Näin saadaan tuloesitys

$$f = u \prod_{i \in I} p_i^{n_i} \prod_{j \in J} q_j^{m_j},$$

joka on edellä esitetyn perusteella myös yksikäsitteinen, ja siten ryhmien isomorfismi

$$\varphi\colon \mathbf{Z}^{(I \cup J)} \to K(X)^*/A^*.$$

Renkaan $A[X]$ faktoriaalisuuden todistamiseksi on vielä näytettävä, että φ on järjestettyjen ryhmien isomorfismi. Kun $f \in K(X)^*$ on esitetty tulona kuten yllä, on siis osoitettava, että f:n divisori on positiivinen, eli $f \in A[X]$, jos ja vain jos

$$n_i \geq 0 \quad (i \in I) \quad \text{ja} \quad m_j \geq 0 \quad (j \in J).$$

Ehdon riittävyys on selvä, koska $p_i \in A$ $(i \in I)$ ja $q_j \in A[X]$ $(j \in J)$. Oletetaan kääntäen, että $f \in A[X]$. Tällöin f on myös renkaassa $K[X]$, joten sen faktoriaalisuuden perusteella $m_j \geq 0$ kaikilla $j \in J$.

Koska jokainen polynomi q_j on primtiivinen ja A on faktoriaalinen, tulo

$$g = \prod_{j \in J} q_j^{m_j} \in A[X]$$

on Gaussin lemman 3.3.5 nojalla myös primitiivinen. Koska $f = cg$, missä

$$c = u \prod_{i \in I} p_i^{n_i} \in K^*,$$

ja $f \in A[X]$ eli $1 \mid f$, niin lemman 3.3.6 perusteella $1 \mid c$ eli $c \in A$. Tästä taas seuraa $n_i \geq 0$ $(i \in I)$, kun A on faktoriaalinen. □

Huomautus. Todistuksessa on esitetty eräs renkaan $A[X]$ jaottomien alkioiden edustajisto. Sen avulla nähdään, että jaottomia alkioita on kahta tyyppiä:

i) Renkaan A jaottomat alkiot up_i $(u \in A^*, i \in I)$.
ii) Renkaassa $K[X]$ jaottomat primitiiviset polynomit $uq_j \in A[X]$ $(u \in A^*, j \in J)$.

Induktiolla saadaan välittömästi seuraava tulos.

KOROLLAARI 3.3.8. *Jos rengas A on faktoriaalinen, niin $A[X_1, \ldots, X_n]$ on faktoriaalinen kaikilla $n \in \mathbf{N}$.*

Erityisesti jokainen polynomirengas $K[X_1, \ldots, X_n]$ $(n \in \mathbf{N})$, missä K on kunta, on faktoriaalinen.

Eisensteinin kriteerio.

LAUSE 3.3.9. *Olkoon A faktoriaalinen rengas ja $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ primitiivinen polynomi, jonka aste on $n > 0$. Jos on olemassa sellainen A:n jaoton alkio p, että $p \mid a_i$, kun $i < n$, mutta $p^2 \nmid a_0$, niin f on jaoton.*

Todistus. Olkoon f kahden renkaan $A[X]$ polynomin

$$g = \sum_i b_i X^i, \quad h = \sum_j c_i X^j$$

tulo ja $p \in A$ jaoton alkio, joka toteuttaa esitetyt ehdot. Tällöin

$$a_k = \sum_{i+j=k} b_i c_j \qquad (0 \leq k \leq n).$$

Koska f on primitiivinen, sen kerroin a_n ei ole jaollinen p:llä. Siten eivät myöskään kaikki kertoimet b_i tai c_j voi olla jaollisia p:llä.

Olkoot r ja s pienimmät indeksit, joilla $p \nmid b_r$ ja $p \nmid c_s$. Tällöin $p \nmid b_r c_s$, koska jaoton alkio p toteuttaa ehdon (P) (ks. lause 3.2.2), mutta $p \mid b_i c_j$, kun $i < r$ tai $j < s$. Summa

$$a_{r+s} = \sum_{i+j=r+s} b_i c_j$$

ei siten voi olla jaollinen p:llä. Tämä merkitsee, että $r + s = n$, koska $p \mid a_k$, kun $k < n$.

Lisäksi $r \leq \deg(g)$, $s \leq \deg(h)$ ja

$$n = \deg(f) = \deg(g) + \deg(h).$$

Siis täytyy olla $r = \deg(g)$ ja $s = \deg(h)$.

Toisaalta b_0 ja c_0 eivät kumpikin voi olla jaollisia p:llä, koska oletuksen mukaan $a_0 = b_0 c_0$ ei ole jaollinen neliöllä p^2. Tämä merkitsee, että $r = 0$ tai $s = 0$, ja että siten toinen tekijöistä g ja h on vakio. Koska f on primitiivinen, tämän vakion täytyy olla yksikkö. Siis f on jaoton polynomi renkaassa $A[X]$. $\square$

Huomautus. Jos K on A:n jakokunta, niin primitiivinen jaoton polynomi $f \in A[X]$ on jaoton myös renkaassa $K[X]$ (ks. lause 3.3.7, *Huom.*). Eisensteinin kriteeriota voidaan siten käyttää jaottomuuden tutkimiseen renkaassa $K[X]$.

Esimerkki 2) Olkoon p alkuluku. Kaikki primitiiviset p:nnet ykkösenjuuret $\zeta \in \mathbf{C}$ ovat polynomin

$$f = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbf{Z}[X]$$

juuria. Osoitetaan, että polynomi f on jaoton renkaassa $\mathbf{Z}[X]$ ja siten myös renkaassa $\mathbf{Q}[X]$, eli että se on primitiivisten ykkösenjuurten minimaalipolynomi kunnan $\mathbf{Q}$ suhteen.

Tarkastellaan renkaan $\mathbf{Z}[X]$ automorfismia, jossa $X \mapsto X + 1$. Sijoittamalla $X + 1$ tuntemattoman paikalle yhtälöön

$$(X - 1)f(X) = X^p - 1$$

saadaan

$$Xf(X + 1) = (X + 1)^p - 1 = X^p + pX^{p-1} + \cdots + pX$$

ja siten

$$f(X + 1) = X^{p-1} + pX^{p-2} + \cdots + p,$$

missä kaikki kertoimet ensimmäisen jälkeen ovat jaollisia p:llä. Eisensteinin kriteerion nojalla $f(X + 1)$ on siis jaoton renkaassa $\mathbf{Z}[X]$.

Jos nyt $f = gh$, missä $g, h \in \mathbf{Z}[X]$, niin $f(X+1) = g(X+1)h(X+1)$. Tämä on kuitenkin mahdollista vain, jos $g = \pm 1$ tai $h = \pm 1$; polynomi f on siis myös jaoton.

Harjoitustehtäviä

1) Tutkittava, mitkä seuraavista polynomeista ovat jaottomia renkaassa $\mathbf{Z}[X, Y]$:

$X^2 + Y^2 - 1,\ X^2 - Y^2 - X,\ X^2 - Y^2,\ X^3 - Y^2 - X,\ X^3 - Y^3 + X^2.$

(Eisensteinin kriteerio esim. renkaassa $A[Y]$, $A = \mathbf{Z}[X]$.)