Peruskäsitteet

0. Kertausta

Tässä luvussa käydään läpi sellaiset peruskäsitteet ja merkinnät, joiden oletetaan olevan tuttuja aiemmalta algebran kurssilta.

0.1. Laskutoimitukset. Olkoon X joukko. Joukon X *laskutoimitus* on kuvaus $*\colon X \times X \to X$, joka liittää jokaiseen pariin (x, y) yksikäsitteisen alkion joukosta X. Tätä alkiota kutsutaan laskutoimituksen *tulokseksi* ja merkitään tavalliseen tapaan $x*y$. Laskutoimituksella varustettu joukko tarkoittaa paria $(X, *)$. Tämä on yksinkertaisin algebrallinen struktuuri, ja sitä nimitetään toisinaan *magmaksi*.

Joukon X laskutoimitusta $*$ kutsutaan

1) *liitännäiseksi*, jos $(x * y) * z = x * (y * z)$ kaikilla $x, y, z \in X$
2) *vaihdannaiseksi*, jos $x * y = y * x$ kaikilla $x, y \in X$.

Jos laskutoimitus toteuttaa liitännäisyysehdon, sulkeiden sijainti on merkityksetön myös pidemmissä laskulausekkeissa. (Todistetaan induktiolla.) Tällöin kaikki lausekkeet voidaan kirjoittaa ilman sulkeita, ja potenssimerkintä

$$\underbrace{x * x * \cdots * x}_{n \text{ kpl}} = x^n \qquad (n \geq 1)$$

on hyvin määritelty. Jos laskutoimitus on lisäksi vaihdannainen, ei alkioiden järjestyksellä lausekkeessa ole väliä, joten voidaan ottaa käyttöön tulomerkintä

$$x_1 * x_2 * \cdots * x_n = \prod_{i=1}^{n} x_i$$

tai yleisemmin, jos I on jokin äärellinen indeksijoukko:

$$\prod_{i \in I} x_i.$$

Laskutoimituksen *neutraalialkioksi* kutsutaan alkiota e, jolle pätee

$$x * e = e * x = x \qquad \text{kaikilla } x \in X.$$

Jos laskutoimituksella on neutraalialkio, voidaan puhua myös *käänteisalkioista*. Alkio y on alkion x käänteisalkio, jos

$$x * y = y * x = e,$$

missä e on neutraalialkio. Alkion x käänteisalkiota merkitään yleensä x^{-1}. Jos tällainen alkio on olemassa, sanotaan että x on *kääntyvä*.

Laskutoimituksen neutraalialkio on aina yksikäsitteinen, sillä jos e ja e' toteuttavat neutraalisuusehdon, niin

$$e = e * e' = e',$$

joten $e = e'$. Käänteisalkiot ovat yksikäsitteisiä, mikäli laskutoimitus on liitännäinen. Tällöin nimittäin, jos y ja y' ovat molemmat x:n käänteisalkioita, saadaan

$$y = y * e = y * (x * y') = (y * x) * y' = e * y' = y',$$

eli $y = y'$.

Toisinaan puhutaan erikseen myös vasemman- ja oikeanpuoleisista neutraalija käänteisalkioista. Esimerkiksi kuvaus $f\colon X \to X$ on injektiivinen, jos ja vain jos se on vasemmalta kääntyvä (laskutoimituksena kuvausten yhdistäminen) eli on olemassa kuvaus $g\colon X \to X$, jolle pätee $g \circ f = \mathrm{id}$. Voidaan myös näyttää, että kuvaus on surjektiivinen, jos ja vain jos sillä on oikeanpuoleinen käänteisalkio.

Jos laskutoimituksella on neutraalialkio, voidaan määritellä alkion x *kertaluku*. Jos ehto $x^n = e$ pätee jollain positiivisella kokonaisluvulla n, alkion x kertaluku on tällaisista luvuista pienin. Mikäli ehto ei päde, sanotaan kertaluvun olevan ääretön. Neutraalialkio itse on ainoa alkio, jonka kertaluku on 1. Jos alkion kertaluku on 2, alkio on oma käänteisalkionsa.

Neutraalialkio mahdollistaa nollapotenssin ja tyhjän tulon määrittelyn. Jos $m < n$, niin

$$x^0 = e \qquad \text{ja} \qquad \prod_{i=n}^{m} x_i = e.$$

Negatiiviset potenssit voidaan puolesta määritellä käänteisalkion avulla, jos sellainen löytyy:

$$x^{-n} = (x^{-1})^n, \qquad \text{missä } n > 0.$$

(Potenssin kirjoittamisessa vaaditaan tietysti laskutoimituksen liitännäisyyttä.) Näistä määritelmistä seuraavat tutut potenssilait:

$$x^m * x^n = x^{m+n} \qquad \text{ja} \qquad (x^m)^n = x^{m \cdot n},$$

missä m ja n voivat olla mitä tahansa kokonaislukuja; negatiivisten potenssien tapauksessa vaaditaan alkion x kääntyvyyttä.

Tavallisesti laskutoimituksia merkitään joko *multiplikatiivisesti* kertolaskun tapaan tai *additiivisesti* yhteenlaskun tapaan. (Jälkimmäisessä tapauksessa oletetaan käytännössä aina, että laskutoimitus on vaihdannainen.) Oheisesta taulukosta selviävät eri merkintätapojen yksityiskohdat.

	multiplikatiivinen	additiivinen
laskutoimitus	$x \cdot y$ tai xy (tulo)	$x + y$ (summa)
potenssimerkintä	x^n	nx tai $n.x$ (monikerta)
tulomerkintä	$\prod_{i=1}^{n} x_i$	$\sum_{i=1}^{n} x_i$
neutraalialkio	1 (ykkösalkio)	0 (nolla-alkio)
käänteisalkio	x^{-1}	$-x$ (vasta-alkio)

Jos yhteen- tai kertolasku on vaihdannainen, voidaan lisäksi ilman sekaannuksen vaaraa käyttää vastaavaa *erotus-* tai *jakolaskumerkintää*

$$x - y = x + (-y) \qquad \text{tai} \qquad x/y = \frac{x}{y} = xy^{-1}.$$

Joukko X saatetaan myös varustaa useammalla kuin yhdellä laskutoimituksella, tavallisimmin kahdella. Tällöin toinen laskutoimituksista on yleensä vaihdannainen, ja sitä merkitään additiivisesti; toista laskutoimitusta merkitään puolestaan multiplikatiivisesti. Koko rakenne on siis kolmikko $(X, +, \cdot)$. Laskulausekkeissa kertolaskut ajatellaan laskettavaksi ennen yhteenlaskuja, joten esim. $x+y\cdot z$ tarkoittaa lauseketta $x + (y \cdot z)$. Lisäksi sanotaan, että tällaiset laskutoimitukset toteuttavat *osittelulain*, mikäli

$$x \cdot (y + z) = x \cdot y + x \cdot z \qquad \text{ja} \qquad (x + y) \cdot z = x \cdot z + y \cdot z$$

kaikilla $x, y, z \in X$.

0.2. Perusrakenteet. Eräs tavallisimpia algebrallisia rakenteita on ryhmä.

MÄÄRITELMÄ 0.1. Paria $(G, *)$, missä $*$ on joukon G laskutoimitus, nimitetään *ryhmäksi*, mikäli se toteuttaa seuraavat ehdot:

(G0) G on suljettu laskutoimituksen suhteen, eli $x * y \in G$ kaikilla $x, y \in G$.
(G1) Laskutoimitus on liitännäinen.
(G2) Laskutoimituksella on neutraalialkio joukossa G.
(G3) Jokaisella $x \in G$ on käänteisalkio joukossa G.

Huomataan, että ehto (G0) sisältyy itse asiassa jo laskutoimituksen määritelmään. Käänteisalkiot ovat yksikäsitteisiä, koska laskutoimitus on liitännäinen. Mikäli laskutoimitus on lisäksi vaihdannainen, rakennetta nimitetään *vaihdannaiseksi* eli *Abelin*[1] *ryhmäksi*. Eräitä esimerkkejä ryhmistä ovat

- $(\mathbb{Z}, +)$ (Abelin ryhmä)
- $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ (Abelin ryhmiä)
- $(\mathbb{Z}_n, +)$, jäännösluokat varustettuna yhteenlaskulla modulo n (Abelin ryhmä)
- jonkin joukon kaikki bijektiot varustettuna kuvausten yhdistämisellä
- kääntyvät $n \times n$-reaalimatriisit varustettuna matriisien kertolaskulla.

Ryhmälaskutoimituksen tärkein ominaisuus on *sievennyssääntö*. Jos x, y ja z ovat ryhmän alkioita ja e on neutraalialkio, niin

$$x * y = x * z \quad \Rightarrow \quad \underbrace{(x^{-1} * x)}_{e} * y = \underbrace{(x^{-1} * x)}_{e} * z \quad \Rightarrow \quad y = z.$$

Sievennyssääntö käyttää hyväkseen kaikkia ryhmäaksioomia. Tästä säännöstä saadaan myös seuraava aputulos.

LEMMA 0.2. *Olkoon $(G, *)$ ryhmä, neutraalialkiona e. Tällöin kaikilla $x, y \in G$ pätee*

$$x * y = y \qquad \Rightarrow \qquad x = e.$$

Tarkastelemalla kontrapositiota "jos $x \neq e$, niin $x * y \neq y$" voidaan saatu tulos tulkita niin, että ryhmässä millä tahansa neutraalialkiosta poikkeavalla alkiolla kertominen muuttaa kaikkia muita alkioita.

[1] Norjalainen Niels Henrik Abel, 1802–1829, todisti vähintään viidennen asteen yleisten polynomiyhtälöiden ratkeamattomuuden.

Rakennetta, joka toteuttaa edellisestä määritelmästä vain ehdot (G0) ja (G1), nimitetään *puoliryhmäksi*. (Puoliryhmä on siis liitännäinen magma.) Jos rakenne toteuttaa ehdot (G0)–(G2), sitä kutsutaan *monoidiksi*. Esimerkkejä monoideista ovat luonnollisten lukujen vaihdannainen monoidi $(\mathbb{N}, +)$ (neutraalialkiona 0) sekä kaikkien $n \times n$-reaalimatriisien muodostama joukko varustettuna matriisikertolaskulla (neutraalialkio yksikkömatriisi). Esimerkkejä puoliryhmistä ovat $(\mathbb{Z}_+, +)$ (positiiviset kokonaisluvut), sekä minkä tahansa renkaan ideaali (määritelmä seuraa myöhemmin), laskutoimituksena kyseisen renkaan kertolasku.

Kahden laskutoimituksen rakenteista yleisimpiä ovat renkaat ja kunnat.

MÄÄRITELMÄ 0.3. Rakennetta $(R, +, \cdot)$ kutsutaan *renkaaksi*, jos se täyttää seuraavat ehdot:

(R1) Pari $(R, +)$ muodostaa vaihdannaisen ryhmän.
(R2) Pari $(R, \cdot)$ muodostaa monoidin.
(R3) Osittelulaki pätee.

Rengasta nimitetään *vaihdannaiseksi*, mikäli kertolasku on vaihdannainen.

Renkaan kertolaskulla on siis neutraalialkio, jota kutsutaan ykkösalkioksi, ja kertolasku on liitännäinen. Käänteisalkioita ei kuitenkaan välttämättä löydy. Seuraavassa esimerkkejä renkaista:

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$ (modulaariaritmetiikka)
- $n \times n$-reaalimatriisit
- Abelin ryhmän G endomorfismit (homomorfismit $G \to G$) varustettuna pisteittäisellä yhteenlaskulla: $(f + g)(x) = f(x) + g(x)$, ja kuvausten yhdistämisellä.

Renkaan R kääntyvien alkioiden joukkoa merkitään usein R^*. Tämä tulee erityisesti kyseeseen tuttujen lukurenkaiden, kuten renkaiden $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{Z}_n$, kohdalla. Esimerkiksi $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Osittelulaista seuraa, että renkaassa R pätee $0 \cdot x = x \cdot 0 = 0$ kaikilla $x \in R$, sillä

$$0 \cdot x = (0 + 0) \cdot x = (0 \cdot x) + (0 \cdot x),$$

josta yhteenlaskuryhmän sievennyssääntöä käyttämällä saadaan $0 = 0 \cdot x$. Yhtälö $x \cdot 0 = 0$ todistetaan samalla tavalla. Säännöistä $1 \cdot x = x$ ja $0 \cdot x = 0$ seuraa nyt, että jos $0 = 1$, niin rengas koostuu pelkästään nolla-alkiosta (ns. *triviaalirengas*).

Olkoon jatkossa R vaihdannainen rengas, jossa $0 \neq 1$. On mahdollista, että $x \cdot y = 0$, vaikka $x \neq 0 \neq y$ (vrt. matriiseihin). Tällaisessa tapauksessa alkioita x ja y kutsutaan *nollanjakajiksi* tai *nollantekijöiksi*. Mikäli kuitenkin kaikilla $x, y \in R$ pätee

$$x \cdot y = 0 \qquad \Rightarrow \qquad x = 0 \quad \text{tai} \quad y = 0,$$

vaihdannaista rengasta R nimitetään *kokonaisalueeksi*. Kokonaisalueessa ei siis ole nollanjakajia. Esimerkiksi $(\mathbb{Z}, +, \cdot)$ on kokonaisalue.

Erikoistapaus kokonaisalueesta on kunta.

MÄÄRITELMÄ 0.4. Vaihdannaista rengasta $(K, +, \cdot)$ nimitetään *kunnaksi*, jos $0 \neq 1$ ja pari $(K \setminus \{0\}, \cdot)$ muodostaa vaihdannaisen ryhmän.

Vaihdannainen epätriviaali rengas on siis kunta, jos ja vain jos se sisältää kaikkien nollasta poikkeavien alkioidensa käänteisalkiot. Jokainen kunta on kokonaisalue, sillä jos $x \cdot y = 0$ joillain $x, y \in K$, ja $x \neq 0$, niin

$$y = x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 = 0.$$

Lisäksi jokainen äärellinen kokonaisalue on kunta. Jos nimittäin K on äärellinen kokonaisalue ja $x \in K \setminus \{0\}$, niin jokainen x:n (positiivinen) potenssi on nollasta poikkeava. Koska K on äärellinen, niin joillain $n, m \in \mathbb{N}$, $n > m \geq 1$, pätee $x^n = x^m$. Tästä saadaan

$$0 = x^n - x^m = x^m(x^{n-m} - 1).$$

Edelleen, koska K on kokonaisalue ja $x^m \neq 0$, täytyy päteä $x^{n-m} - 1 = 0$. Tällöin $1 = x^{n-m} = x^{n-m-1} \cdot x$, eli x^{n-m-1} on alkion x käänteisalkio.

Tuttuja kuntia ovat lukualueet $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ tavallisine laskutoimituksineen.

0.3. Alirakenteet ja virittäminen. Hyvin yleisesti muotoiltuna laskutoimitusstruktuurin X *alistruktuurilla* tarkoitetaan osajoukkoa $Y \subset X$, jolle pätevät seuraavat ehdot:

- Joukko Y on suljettu kaikkien X:n laskutoimitusten suhteen.
- Joukko Y sisältää kaikkien X:n laskutoimitusten neutraalialkiot.
- Jos alkiolla $x \in Y$ on joukossa X käänteisalkio x^{-1} jonkin laskutoimituksen suhteen, niin $x^{-1} \in Y$.

Nämä ehdot realisoituvat hieman eri muodoissa eri rakenteiden yhteydessä. Ehdoista seuraa, että alistruktuuri on aina samaa tyyppiä kuin ympäröivä struktuuri, esim. alirengas on aina itsekin rengas. Kuitenkaan mikä tahansa renkaan ehdot täyttävä toisen renkaan osajoukko ei välttämättä ole alirengas, koska sen ykkösalkio voi olla eri kuin ympäröivässä renkaassa.

MÄÄRITELMÄ 0.5. Ryhmän $(G, \cdot)$ osajoukko H on G:n *aliryhmä*, jos

(H1) H on suljettu laskutoimituksen suhteen, eli $gh \in H$ kaikilla $g, h \in H$.
(H2) H sisältää ryhmän G neutraalialkion.
(H3) H sisältää kaikkien alkioidensa käänteisalkiot, eli $g^{-1} \in H$ kaikilla $g \in H$.

Tällöin merkitään $H \leq G$.

Ehtoa (H2) ei tarvitse erikseen tarkistaa, jos muut ehdot ovat voimassa ja H on epätyhjä. Tällöin nimittäin löytyy jokin $g \in H$, ja ehdoista seuraa että $g^{-1} \in H$ sekä edelleen $e = g \cdot g^{-1} \in H$. Pienellä päättelyllä saadaan seuraava toisinaan kätevä tulos.

LAUSE 0.6 (Aliryhmäkriteeri). *Ryhmän G osajoukko H on G:n aliryhmä, jos ja vain jos*

(H1) $H \neq \emptyset$
(H2) $gh^{-1} \in H$ *kaikilla* $g, h \in H$.

Toinen aliryhmiin liittyvä erikoisuus mainitaan seuraavassa lauseessa.

LAUSE 0.7. *Ryhmän G osajoukko H on G:n aliryhmä, jos ja vain jos se on ryhmä.*

Lause ei seuraa suoraan aliryhmän määritelmästä, sillä ryhmällä H voisi olla esimerkiksi eri neutraalialkio kuin ryhmällä G. Voisi siis päteä $e' \cdot g = g$ kaikilla $g \in H$, vaikka e' ei olisikaan koko ryhmän G neutraalialkio. Ryhmässä kuitenkin millä tahansa varsinaisesta neutraalialkiosta poikkeavalla alkiolla kertominen muuttaa kaikkia muita alkioita, joten edellä kuvailtuja pienemmässä joukossa toimivia neutraalialkioita ei löydy. Tulos seuraa tästä sekä ympäröivän ryhmän G käänteisalkioiden yksikäsitteisyydestä.

Alkioon g liittyvät aliryhmän H vasen ja oikea *sivuluokka* määritellään joukkoina

$$gH = \{gh \mid h \in H\} \qquad \text{ja} \qquad Hg = \{hg \mid h \in H\}.$$

Voidaan osoittaa, että kaikki tietyn aliryhmän vasemmat (tai yhtä hyvin oikeat) sivuluokat muodostavat koko ryhmän osituksen. Lisäksi, jos aliryhmä on äärellinen, kaikki sivuluokat ovat samankokoisia.[2] Tästä seuraa ryhmäteorian kenties tärkein tulos.

LAUSE 0.8 (Lagrange[3]). *Olkoon G äärellinen ryhmä ja H sen aliryhmä. Tällöin G:n alkioiden lukumäärä on jaollinen aliryhmän H alkioiden lukumäärällä.*

Aliryhmän sivuluokkien lukumäärää nimitetään aliryhmän *indeksiksi* ja merkitään $[G : H]$. Indeksin avulla Lagrangen lause voidaan esittää myös hieman täsmällisemmässä (ja kompaktimmassa) muodossa: $[G : H] = G/H$.

Yleisistä alistruktuuriehdoista saadaan kriteerit myös alirenkaana tai alikuntana olemiselle.

LAUSE 0.9 (Alirengaskriteeri). *Renkaan R osajoukko A on alirengas, jos ja vain jos*

(AR1) $x - y \in A$ *kaikilla* $x, y \in A$
(AR2) $xy \in A$ *kaikilla* $x, y \in A$
(AR3) $1 \in A$ *(kertolaskun neutraalialkio renkaassa R).*

Ehdon (AR1) muotoilussa on käytetty yllä mainittua aliryhmäkriteeriä: kolmas ehto nimittäin takaa, että A on epätyhjä.

LAUSE 0.10 (Alikuntakriteeri). *Kunnan K osajoukko L on alikunta, jos ja vain jos*

(AK1) $L^* \neq \emptyset$
(AK2) $x - y \in L$ *kaikilla* $x, y \in L$
(AK3) $xy^{-1} \in L$ *kaikilla* $x \in L$ *ja* $y \in L^*$.

[2]Myös äärettömän aliryhmän sivuluokat ovat yhtä mahtavia.

[3]Joseph-Louis Lagrange (1736–1813) ei todistanut nimeään kantavaa lausetta, mutta käytti joitain sen erityistapauksia polynomiyhtälöitä koskevassa tutkimuksessaan.

Mikä tahansa struktuurin X osajoukko S ei ole välttämättä alistruktuuri, mutta se voidaan aina täydentää alistruktuuriksi lisäämällä siihen sopivasti alkioita. Pienintä alistruktuuria, joka sisältää joukon S, nimitetään *S:n virittämäksi* alistruktuuriksi ja merkitään $\langle S\rangle$. Voidaan osoittaa, että $\langle S\rangle$ on kaikkien niiden alistruktuurien leikkaus, jotka sisältävät joukon S.

Esimerkiksi ryhmän G osajoukon S virittämä aliryhmä löydetään lisäämällä S:ään tarvittaessa G:n neutraalialkio, kaikki mahdolliset S:n alkioista muodostettavat tulot sekä kaikki S:n alkioiden käänteisalkiot. Tiivistäen tämä voidaan kirjoittaa muotoon

$$\langle S\rangle = \{x_1x_2\cdots x_k \mid k \in \mathbb{N},\, x_i \in S \text{ tai } x_i^{-1} \in S \text{ kaikilla } i \leq k\}.$$

Yhden alkion x virittämää aliryhmää voidaan merkitä $\langle x\rangle$. Jos $G = \langle x\rangle$ jollain $x \in G$, eli koko ryhmä on yhden alkionsa virittämä, ryhmää kutsutaan *sykliseksi*. Merkintä $G = C_n$ tarkoittaa, että G on syklinen ryhmä, jonka virittäjän kertaluku on n (voi olla myös ääretön). Ryhmän C_n alkioiden lukumäärä on n. Esimerkiksi $\mathbb{Z} = C_\infty$. Sykliset ryhmät ovat yksinkertaisimpia vaihdannaisia ryhmiä. Niiden kaikki ali- ja tekijäryhmät ovat myös syklisiä.

0.4. Tulorakenteet. Useimmista algebrallisista rakenteista voidaan muodostaa tulorakenteita karteesisen tulon avulla. Esimerkiksi kahden ryhmän $(G, *)$ ja $(H, \circ)$ *tuloryhmä* on joukko

$$G \times H = \{(g, h) \mid g \in G, h \in H\},$$

jonka laskutoimitus määritellään pisteittäin:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Samalla tavoin voidaan määritellä kahden renkaan R ja S *tulorengas* $R \times S$. Myös useamman, jopa äärettömän monen struktuurin tulo on mahdollinen.

Jos rakenteissa on neutraalialkioina e_1 ja e_2, tulorakenteen neutraalialkio on (e_1, e_2). Samaten käänteisalkioille, mikäli tällaisia on, pätee

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

Edelleen, jos Y_1 ja Y_2 ovat rakenteiden X_1 ja X_2 alirakenteita, niin $Y_1 \times Y_2$ on tulorakenteen $X_1 \times X_2$ alirakenne. Tulorakenteella voi kuitenkin olla myös sellaisia alistruktuureja, jotka eivät itse ole tulomuotoa; esimerkiksi joukko

$$\{(n, n) \mid n \in \mathbb{Z}\}$$

on tulorenkaan $\mathbb{Z} \times \mathbb{Z}$ alirengas, vaikka se ei ole muotoa $A \times B$ millään $\mathbb{Z}$:n alirenkailla A ja B.

Kahden kunnan karteesinen tulo ei ole kunta (ainakaan pisteittäisillä laskutoimituksilla). Tämän näkee esimerkiksi siitä, että millään muotoa $(a, 0)$ olevalla alkiolla ei voi olla käänteisalkiota, koska nollalla ei sellaista ole. Kuitenkin kunnan vaatimuksien mukaan kaikilla muilla paitsi alkiolla $(0, 0)$ pitäisi olla käänteisalkio.

0.5. Homomorfismit. Samantyyppisiä algebrallisia rakenteita voidaan verrata toisiinsa *homomorfismien* avulla. Kuvausta f struktuurista $(X, *)$ struktuuriin $(Y, \circ)$ kutsutaan homomorfismiksi, jos seuraavat ehdot pätevät:

(HM1) $f(x * y) = f(x) \circ f(y)$ kaikilla $x, y \in X$.

(HM2) Jos laskutoimituksella $*$ on neutraalialkio e_X, niin $f(e_X) = e_Y$, missä e_Y on laskutoimituksen $\circ$ neutraalialkio.

Ehdot siis takaavat, että kuvaus säilyttää laskutoimitusten tulokset sekä neutraalialkiot. Jos laskutoimituksia on kaksi tai useampia, ehtojen tulee päteä kunkin laskutoimituksen osalta.

Homomorfismi $f\colon (X, *) \to (Y, \circ)$ kuvaa mahdolliset käänteisalkiot käänteisalkioiksi kaikkien struktuurien tapauksessa. Tämä seuraa yhtälöketjuista

$$f(x) \circ f(x^{-1}) = f(x * x^{-1}) = f(e_X) = e_Y$$
$$\text{ja} \quad f(x^{-1}) \circ f(x) = f(x^{-1} * x) = f(e_X) = e_Y,$$

joiden perusteella $f(x)^{-1} = f(x^{-1})$. Induktiolla saadaan lopulta osoitettua, että

$$f(x^n) = f(x)^n$$

kaikilla kokonaisluvuilla n.

Homomorfismien merkitys on siinä, että ne säilyttävät algebralliset ominaisuudet. Esimerkiksi alistruktuurin kuva homomorfismissa on vastaavanlainen alistruktuuri maalistruktuurissa. Myös liitännäisyys-, vaihdannaisuus- ja ositteluominaisuudet säilyvät. Erityisesimerkki homomorfismista on bijektiivinen eli kääntyvä homomorfismi, jota nimitetään *isomorfismiksi*. Koska se kuvaa struktuurit toisikseen säilyttäen algebralliset ominaisuudet molempiin suuntiin, ovat nämä ns. *isomorfiset struktuurit* täysin samankaltaiset toistensa kanssa, alkioiden ja laskutoimitusten nimeämistä vaille identtiset.

Ryhmien tapauksessa myös homomorfismin kohdalla saadaan muutamia yksinkertaistuksia. Ensinnäkin ryhmien välisen kuvauksen $f\colon (G, *) \to (H, \circ)$ tapauksessa jälkimmäistä homomorfiaehtoa (HM2) ei tarvitse erikseen tarkastella, sillä ensimmäisestä ehdosta seuraa

$$f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G),$$

josta ryhmän H sievennyssäännön avulla tulee $e_H = f(e_G)$.

Toinen seikka liittyy ryhmähomomorfismin *ytimeen*

$$\operatorname{Ker} f = \{x \in G \mid f(x) = e_H\}.$$

Voidaan osoittaa, että kuvaus f on injektiivinen, jos ja vain jos $\operatorname{Ker} f = \{e_G\}$. Kyseinen ehto seuraa injektiivisyydestä, koska $f(e_G) = e_H$. Toinen suunta nähdään seuraavasti: Oletetaan, että $f(x) = f(y)$ joillain $x, y \in G$. Tällöin

$$e_H = f(x) \circ f(y)^{-1} = f(x * y^{-1}),$$

joten $x * y^{-1}$ on ytimessä $\operatorname{Ker} f$. Jos ydin sisältää vain neutraalialkion e_G, niin $x * y^{-1} = e_G$, ja edelleen $x = y$. Tämä osoittaa injektiivisyyden.

Ryhmähomomorfismia koskien voidaan tässä yhteydessä mainita seuraava helposti muistettava sääntö.

LAUSE 0.11. *Homomorfismi f ryhmältä G ryhmään H on*

- *injektiivinen* $\iff \operatorname{Ker} f = \{e_G\}$
- *surjektiivinen* $\iff \operatorname{Im} f = H$.

Rengashomomorfismin $f\colon R \to S$ ydin määritellään nolla-alkion alkukuvana:

$$\operatorname{Ker} f = \{x \in R \mid f(x) = 0\}.$$

Rengashomomorfismin ydin on siis sama kuin renkaan yhteenlaskuryhmään liittyvän vastaavan ryhmähomomorfismin ydin. Tästä seuraa, että myös rengashomomorfismi on injektiivinen, jos ja vain jos sen ydin on triviaali.

Kunnat koostuvat kahdesta vaihdannaisesta ryhmästä, ja tämä mahdollistaa vielä erään yksinkertaistuksen.

LAUSE 0.12. *Jokainen kuntahomomorfismi $f\colon K \to L$ on injektiivinen.*

Tulos seuraa siitä, että rengashomomorfismin ydin on aina *ideaali* (tähän palataan myöhemmin) ja millä tahansa kunnalla K on vain triviaalit ideaalit $\{0\}$ ja K. Vaihtoehto K ei tule kysymykseen, koska $f(1_K) = 1_L \neq 0$. Siispä $\operatorname{Ker} f = \{0\}$, mikä yhteenlaskuryhmässä tulkittuna tarkoittaa sitä, että f on injektiivinen.

0.6. Polynomit[4]**.** Olkoon R rengas. Yhden muuttujan R-kertoimiseksi polynomiksi kutsutaan äärellistä muodollista summaa

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

missä alkiot $a_0, \ldots, a_n$ kuuluvat renkaaseen R. Näitä alkioita kutsutaan polynomin *kertoimiksi* ja symbolia X *muuttujaksi* tai *tuntemattomaksi*. Polynomin *aste* $\deg(f)$ on suurin sellainen n, jolla kerroin a_n on nollasta poikkeava. Nollapolynomin 0 asteeksi määritellään kuitenkin $-\infty$. Kaikkien R-kertoimisten yhden muuttujan polynomien joukkoa merkitään $R[X]$. Tämä joukko on rengas polynomien tavallisen yhteen- ja kertolaskun suhteen. Renkaan R alkiot ovat joukon $R[X]$ *vakiopolynomeja*.

Jos kerroinjoukkona on kunta, voidaan todistaa erittäin käyttökelpoinen jakoyhtälö.

LAUSE 0.13 (Polynomien jakoyhtälö). *Olkoon K kunta, ja olkoot f ja g kaksi K-kertoimista polynomia. Oletetaan, että $g \neq 0$. Tällöin löytyy yksikäsitteiset $q, r \in K[X]$, joille pätee $f = qg + r$ ja $\deg(r) < \deg(g)$.*

Lause todistetaan myöhemmin luvussa 11.3.

Voidaan myös määritellä useamman kuin yhden muuttujan polynomeja. Muuttujien $X_1, \ldots, X_k$ polynomi on muodollinen summa

$$f = \sum_{i=0}^{m} a_i \overline{X}_i,$$

missä kukin $\overline{X}_i$ on muotoa $X_1^{n_1} X_2^{n_2} \cdots X_k^{n_k}$ oleva *monomi*. Monomissa muuttujien X_i kirjoitusjärjestyksellä ei ole väliä: muuttujien ajatellaan olevan keskenään vaihdannaisia. Monomin aste on siinä esiintyvien eksponenttien summa $n_1 + n_2 + \cdots + n_k$, ja polynomin aste on suurin siinä esiintyvän monomin aste.

Kaikkien R-kertoimisten K muuttujan polynomien joukkoa merkitään symbolilla $R[X_1, \ldots, X_k]$. Usein muuttujia merkitään myös muilla kirjaimilla, kuten Y ja Z. Esimerkiksi $XY + 3Z - 2XZ^2 + 10$ on joukon $\mathbb{Z}[X, Y, Z]$ polynomi, jonka aste on monomin XZ^2 aste eli kolme.

[4]Polynomit määritellään ja konstruoidaan täsmällisesti luvussa 9.4.