LUKU 0

Kuvausten hajottaminen

Tässä luvussa tarkastellaan eräitä kuvausten yhdistämiseen liittyviä kysymyksiä, joita kohdataan toistuvasti lähes kaikissa ns. *abstraktin algebran* konstruktioissa.

Olkoot X, Y ja Z joukkoja. Jos $f\colon X \to Y$ ja $g\colon Y \to Z$ ovat kuvauksia, joista edellisen maali Y on sama kuin jälkimmäisen lähtö, niin voidaan muodostaa uusi kuvaus, kuvausten f ja g *yhdistelmä*

$$h = g \circ f\colon X \to Z$$

asettamalla $h(x) = g(f(x))$ kaikilla $x \in X$.

0.1. Kuvausten yleiset hajotelmat

Ongelman asettelu. Olkoot X, Y ja Z kolme joukkoa kuten yllä, ja olkoon lisäksi annettu kuvaus $h\colon X \to Z$ sekä toinen kuvauksista $f\colon X \to Y$ ja $g\colon Y \to Z$. Tarkastellaan seuraavia kysymyksiä.

i) Kun f on annettu, milloin on olemassa sellainen kuvaus g, että

$$h = g \circ f. \qquad \begin{tikzcd} X \arrow[rr, "h"] \arrow[dr, "f"'] & & Z \\ & Y \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

ii) Milloin tämän ehdon täyttävä kuvaus g on yksikäsitteinen?

Vastaavat kysymykset voidaan asettaa, kun kuvaus g on annettu.

i) Kun g on annettu, milloin on olemassa sellainen kuvaus f, että

$$h = g \circ f. \qquad \begin{tikzcd} X \arrow[rr, "h"] \arrow[dr, dashed, "f"'] & & Z \\ & Y \arrow[ur, "g"'] & \end{tikzcd}$$

ii) Milloin tämän ehdon täyttävä kuvaus f on yksikäsitteinen?

Huomautus. Muodollisesti kuvausten yhdistäminen muistuttaa kertolaskua, varsinkin jos kirjoitetaan lyhyesti gf merkinnän $g \circ f$ asemasta. Niinpä yllä olevat kysymykset esitetään toisinaan muodossa: Milloin kuvauksesta h voidaan "erottaa tekijä" f (tai g)? Hieman täsmällisemmin voidaan kysyä, milloin h voidaan *hajottaa kulkemaan kuvauksen f (tai g) kautta.*

Yksikäsitteisyys. Yllä esitettyihin kuvausten yksikäsitteisyyttä koskeviin kysymyksiin on vastaus seuraavassa lauseessa, jonka todistaminen jääköön harjoitustehtäväksi.

LAUSE 0.1.1 (Kuvausten supistussääntö). *Olkoot X, Y ja Z joukkoja.*

i) *Jos kuvaus $f\colon X \to Y$ on surjektiivinen, niin kaikilla kuvauksilla g, $g'\colon Y \to Z$ pätee*

$$g \circ f = g' \circ f \;\Rightarrow\; g = g'.$$

Kääntäen, jos tämä on voimassa ja $\mathrm{Card}(Z) \geq 2$, *niin f on surjektiivinen.*

ii) *Jos kuvaus $g\colon Y \to Z$ on injektiivinen, niin kaikilla kuvauksilla f, $f'\colon X \to Y$ pätee*

$$g \circ f = g \circ f' \;\Rightarrow\; f = f'.$$

Kääntäen, jos tämä on voimassa ja $X \neq \emptyset$, niin g on injektiivinen.

Huomautus. Vastaavia tuloksia kohdataan usein tilanteissa, joissa ainakin osalla joukoista X, Y ja Z on jokin algebrallinen struktuuri ja eräille kuvauksista on asetettu lisäehtoja. Tällöin surjektiivisuus tai injektiivisyys voidaan korvata väljemmillä ehdoilla.

Olemassaolo.

LAUSE 0.1.2 (Kuvausten hajotuslause). *Olkoot X, Y ja Z joukkoja ja $h\colon X \to Z$ kuvaus.*

i) *Olkoon $f\colon X \to Y$ surjektiivinen kuvaus. Silloin on olemassa kuvaus $g\colon Y \to Z$, jolla $h = g \circ f$, jos ja vain jos kaikilla x, $x' \in X$ pätee*

$$f(x) = f(x') \;\Rightarrow\; h(x) = h(x').$$

ii) *Olkoon $g\colon Y \to Z$ kuvaus. Silloin on olemassa kuvaus $f\colon X \to Y$, jolla $h = g \circ f$, jos ja vain jos*

$$h(X) \subset g(Y).$$

Todistus. i) Ehdon välttämättömyys on selvä, koska kaikilla X:n alkioilla x ja x' yhtälöstä $f(x) = f(x')$ seuraa $g(f(x)) = g(f(x'))$.

Kääntäen, jokainen $y \in Y$ on jonkin alkion $x \in X$ kuva $f(x)$, kun f on surjektiivinen. Ehdon ollessa voimassa kuva $h(x) \in Z$ ei tällöin riipu x:n valinnasta, ja siten voidaan määritellä

$$g(y) = h(x).$$

ii) Ehdon välttämättömyys on jälleen selvä, koska $g(f(X)) \subset g(Y)$. Kääntäen, jos $h(X) \subset g(Y)$, niin jokaisen alkion $x \in X$ kuva $h(x)$ on g:n kuvassa $g(Y)$, eli

$$h(x) = g(y) \quad \text{jollakin } y \in Y,$$

ja tällöin voidaan asettaa $f(x) = y$. □

Huomautus. Jos Z on epätyhjä, niin kuvausta f ei tarvitse olettaa surjektiiviseksi kohdassa i). Silloin $g(y) \in Z$ voidaan valita mielivaltaisesti, jos $y \in Y$ ei ole f:n kuvassa.

0.2. Kuvausten kanoniset hajotelmat

Edellä on nähty, että kuvausten hajotelmissa injektiivisillä ja surjektiivisilla kuvauksilla on erityinen rooli. Sovelluksissa esiintyvät hajotelmat ovat usein sellaisia, joissa injektiot tai surjektiot ovat luonnollisella tavalla muodostettuja ns. *kanonisia* kuvauksia.

Olkoot X ja Y joukkoja sekä $f\colon X \to Y$ kuvaus. Jokaiseen Y:n osajoukkoon A liittyy *kanoninen injektio*

$$j\colon A \to Y,$$

jonka kuva $j(A)$ on A. Tällöin saadaan välittömästi (0.1.2):

LAUSE 0.2.1. *Kuvauksella $f\colon X \to Y$ on hajotelma $f = j \circ g$, jos ja vain jos $f(X) \subset A$.*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, dashed, "g"'] & & Y \\ & A \arrow[ur, "j"'] & \end{tikzcd}$$

Kuvaus g on yksikäsitteinen (0.1.1), ja sanotaan, että se on saatu kuvauksesta f *rajoittamalla maali osajoukoksi* A.

Myös surjektioita muodostetaan usein kanonisesti lähtien ekvivalensseista. Jokaiseen ekvivalenssirelaatioon R joukossa X liittyy *tekijäjoukko* X/R, jonka alkioina ovat ekvivalenssiluokat relaatiossa R. Kuvaus, joka jokaiseen X:n alkioon x liittää sen ekvivalenssiluokan $p(x)$ on tällöin *kanoninen surjektio*

$$p\colon X \to X/R.$$

Algebrassa alkioiden x, $x' \in X$ ekvivalenttisuus merkitään tavallisesti

$$x \equiv x' \pmod{R},$$

mikä on siis yhtäpitävää sen kanssa, että $p(x) = p(x')$.

Ekvivalenssirelaation R kolme ehtoa, *refleksiivisyys, symmetrisyys* ja *transitiivisuus*, ovat tällöin, että kaikilla x, y, $z \in X$

i) $x \equiv x \pmod{R}$;
ii) jos $x \equiv y \pmod{R}$, niin $y \equiv x \pmod{R}$;
iii) jos $x \equiv y \pmod{R}$ ja $y \equiv z \pmod{R}$, niin $x \equiv z \pmod{R}$.

MÄÄRITELMÄ 0.2.2. Kuvaus $f\colon X \to Y$ *sopeutuu* ekvivalenssiin R joukossa X, jos kaikilla x, $x' \in X$ pätee

$$x \equiv x' \pmod{R} \;\Rightarrow\; f(x) = f(x').$$

Yleinen kuvausten hajotuslause 0.1.2 saa tällöin muodon:

LAUSE 0.2.3. *Kuvauksella $f\colon X \to Y$ on hajotelma $f = g \circ p$, jos ja vain jos f sopeutuu ekvivalenssiin R.*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \\ & X/R \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Kuvaus g on yksikäsitteinen, ja sanotaan, että se on saatu f:stä *siirtymällä tekijäjoukkoon* ekvivalenssin R suhteen.

Tärkeä erikoistapaus on se, jossa R on kuvaukseen $f\colon X \to Y$ *liittyvä* ekvivalenssirelaatio:

$$x \equiv x' \pmod{R} \iff f(x) = f(x').$$

Tällöin f sopeutuu relaatioon R ja lisäksi tekijäjoukkoon siirtymällä saatu kuvaus $g\colon X/R \to Y$ on injektiivinen. Kääntäen, jos g on injektiivinen, niin R on välttämättä kuvaukseen f liittyvä ekvivalenssi.

Vastaavasti lausetta 0.2.1 voidaan soveltaa joukon Y osajoukkoon $A = f(X)$, Tämä on ainoa tilanne, jossa hajotelman kuvaus $g\colon X \to A$ on surjektiivinen.

Jokainen kuvaus voidaan hajottaa peräkkäin kummallakin yllä esitetyllä kanonisella tavalla kolmeen osaan. Lopputulos on riippumaton toimitusten järjestyksestä, ja saadaan:

LAUSE 0.2.4. *Olkoot X ja Y joukkoja, $f\colon X \to Y$ kuvaus ja R kuvaukseen f liittyvä ekvivalenssirelaatio X:ssä. Silloin on olemassa kuvauksen f* kanoninen hajotelma

$$f\colon X \xrightarrow{p} X/R \xrightarrow{g} f(X) \xrightarrow{j} Y,$$

missä p on kanoninen surjektio, j on kanoninen injektio, ja g on (f:stä riippuva) bijektio.

Harjoitustehtäviä

1) Olkoot X, Y ja Z joukkoja ja $\mathrm{Card}(Z) \geq 2$. Osoitettava, että kuvaus $f\colon X \to Y$ on surjektiivinen, jos ja vain jos kaikilla kuvauksilla $g, g'\colon Y \to Z$ ehdosta $g \circ f = g' \circ f$ seuraa $g = g'$.

2) Olkoot X, Y ja Z joukkoja ja $X \neq \emptyset$. Osoitettava, että kuvaus $g\colon Y \to Z$ on injektiivinen, jos ja vain jos kaikilla kuvauksilla $f, f'\colon X \to Y$ ehdosta $g \circ f = g \circ f'$ seuraa $f = f'$.

LUKU 1

Algebralliset struktuurit

Tyypillinen matemaattinen objekti on “joukko varustettuna tietyt ehdot täyttävällä *struktuurilla*.” Matematiikassa tarvitaan monenlaisia struktuureita. Lukujen teoriassa ja yleisemmin algebrassa tärkeimpiä struktuureja ovat *laskutoimitukset*. Niiden ohella esiintyy muita kuten *järjestysrelaatiot*. Keskeisiä topologisia struktuureja ovat taas *metriikat* ja yleisemmin *topologiat*. Mutkikkaampia struktuureja saadaan yhdistämällä tällaisia perusstruktuureja. Esimerkiksi reaalilukujen teoria sisältää useita laskutoimituksia (yhteen- ja kertolaskut riittäisivät, muut voidaan johtaa näistä), järjestyksen, metriikan (erotuksen itseisarvo) ja topologian (avoimet joukot).

Struktuureilta vaadittavia ehtoja sanotaan tavallisesti *aksioomiksi*. Tässä luvussa tarkastellaan keskeisiä algebrassa esiintyviä struktuureita ja niihin liittyviä aksioomia.

1.1. Laskutoimitukset

MÄÄRITELMÄ 1.1.1. Olkoon E joukko. *Laskutoimitus* joukossa E on kuvaus $f\colon E \times E \to E$. Kuvauksen arvo $f(x, y)$ parilla $(x, y) \in E \times E$ on tällöin laskutoimituksen *tulos* E:n alkioilla x ja y.

Laskutoimituksilla ja niiden tuloksilla on tavallisesti niitä tarkemmin kuvaava nimi. Samoin eri laskutoimitusten tuloksille käytetään erilaisia merkintöjä.

Esimerkkejä. 1) Reaalilukujen joukossa $\mathbf{R}$ on kaksi peruslaskutoimitusta: *yhteenlasku* $(x, y) \mapsto x + y$ ja *kertolasku* $(x, y) \mapsto x \cdot y$ (tai xy), joiden tuloksia sanotaan *summaksi* ja *tuloksi*.

2) Reaalikertoimisten n-rivisten neliömatriisien joukossa $\mathbf{M}_n(\mathbf{R})$ on kaksi laskutoimitusta: matriisien *yhteenlasku* $(A, B) \mapsto A + B$ ja *kertolasku* $(A, B) \mapsto AB$.

3) Olkoon X mielivaltainen joukko ja E kaikkien kuvausten $f\colon X \to X$ muodostama joukko X^X. Jos kuvaukset f ja g ovat E:ssä, niin ne voidaan yhdistää ja *yhdistelmä* $f \circ g$ on samoin E:ssä. Kuvausten yhdistäminen $(f, g) \mapsto f \circ g$ on siten laskutoimitus E:ssä.

4) Olkoon A mielivaltainen joukko ja E kaikkien sen osajoukkojen joukko eli potenssijoukko $\mathcal{P}(A)$. Jos X ja Y ovat A:n osajoukkoja, niin samoin ovat niiden *yhdiste* $X \cup Y$ ja *leikkaus* $X \cap Y$. Kuvaukset $(X, Y) \mapsto X \cup Y$ ja $(X, Y) \mapsto X \cap Y$ ovat siis laskutoimituksia joukossa E.

Laskutoimituksella varustettu joukkoa sanotaan *magmaksi*. Jokainen yllä esitetty joukko varustettuna jollakin mainituista laskutoimituksista on siis magma.

Magman struktuurille eli laskutoimitukselle ei aseteta mitään ehtoja. Se on siten yksinkertaisin algebrallinen struktuuri. Muissa algebrallisissa struktuureissa laskutoimituksilla on lisäominaisuuksia ja niitä voi struktuuriin sisältyä useita. Jokainen algebrallinen objekti on siten myös magma, mahdollisesti useallakin tavalla. Magmojen teoria ei ole laaja, mutta vastineeksi sitä voidaan soveltaa kaikissa algebrallisissa struktuureissa.

Tässä pykälässä magman laskutoimitus merkitään usein symbolilla $\top$ ("top") sen osoittamiseksi, että laskutoimitus voi olla mikä tahansa: yhteenlasku, kertolasku tai jotakin muuta.

Esimerkki 5) Olkoon E magma ja olkoon $(x, y) \mapsto x \top y$ sen laskutoimitus. Tällöin $(x, y) \mapsto y \top x$ on myös laskutoimitus E:ssä, ns. *vastakkainen laskutoimitus*. Tällä varustettuna joukko E on magma, jota sanotaan alkuperäisen magman *vastamagmaksi*.

Homomorfismit. Olkoot E ja E' magmoja; kummankin laskutoimitus olkoon $(x, y) \mapsto x \top y$.

MÄÄRITELMÄ 1.1.2. Kuvaus $f\colon E \to E'$ on *homomorfismi*, kun kaikilla pareilla $(x, y) \in E \times E$ pätee

$$f(x \top y) = f(x) \top f(y).$$

Jos tällöin $E = E'$, niin f on E:n *endomorfismi*.

Huomautus. Jos f on *bijektiivinen homomorfismi*, niin on helppo osoittaa, että sen käänteiskuvaus f^{-1} on myös homomorfismi. Tällöin sanotaan, että f on *isomorfismi*. Vastaava tulos pätee kaikilla algebrallisilla struktuureilla.

Tilanne on toinen esim. topologisilla struktuureilla, missä homomorfismeja vastaavat jatkuvat kuvaukset. Tällainen kuvaus voi olla bijektiivinen ilman, että sen käänteiskuvaus olisi jatkuva.

Liitännäisyys.

MÄÄRITELMÄ 1.1.3. Laskutoimitus $(x, y) \mapsto x \top y$ joukossa E on *liitännäinen* eli *assosiatiivinen*, jos kaikilla E:n alkioilla x, y, z pätee

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

Liitännäisellä laskutoimituksella varustettuna E on *liitännäinen magma*.

Esimerkkejä. 6) Reaalilukujen yhteen- ja kertolasku ovat liitännäisiä.

7) Matriisien yhteen- ja kertolasku ovat liitännäisiä.

8) Jos X on joukko, niin kuvausten yhdistäminen on liitännäinen laskutoimitus joukossa $E = X^X$.

9) Joukon A osajoukkojen yhdisteen ja leikkauksen muodostamiset ovat liitännäisiä laskutoimituksia potenssijoukossa $E = \mathcal{P}(A)$.

10) Liitännäisen magman vastamagma on myös liitännäinen.

11) Kolmiulotteisen vektoriavaruuden $\mathbf{R}^3$ ristitulo $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \times \mathbf{y}$ ei ole liitännäinen.

Jos x, y ja z ovat liitännäisen magman E alkioita, niin merkinnästä $(x \top y) \top z$ voidaan jättää sulkumerkit pois ilman sekaannuksen vaaraa. Yleisemmin, jos $n > 0$ ja x_1, x_2, ..., x_n ovat E:ssä, niin määritellään rekursiivisesti

$$x_1 \top x_2 \top \cdots \top x_n = (x_1 \top \cdots \top x_{n-1}) \top x_n.$$

Tälle alkiolle käytetään myös lyhyitä merkintöjä

$$\mathop{\top}_{i=1}^{n} x_i, \qquad \mathop{\top}_{1 \leq i \leq n} x_i$$

tai yleisemmin

$$\mathop{\top}_{i \in I} x_i,$$

missä $I = \{1, 2, \ldots, n\}$. Viimeistä merkintää voidaan käyttää myös, kun I on mikä tahansa epätyhjä äärellinen täysin järjestetty joukko.

Näin määritellyillä iteroiduilla laskutoimituksilla on liitännäisessä magmassa seuraava ominaisuus

$$x_1 \top \cdots \top x_n = (x_1 \top \cdots \top x_p) \top (x_{p+1} \top \cdots \top x_n), \quad 1 \leq p \leq n-1,$$

jonka todistaminen jääköön lukijalle harjoitustehtäväksi. Soveltamalla tätä toistuvasti saadaan *yleistetty liitäntälaki*:

LAUSE 1.1.4. *Olkoon E liitännäinen magma, x_1, ..., x_n jono sen alkioita ja $0 = p(0) < p(1) < \ldots < p(m) = n$. Silloin pätee*

$$x_1 \top \cdots \top x_n = \mathop{\top}_{j=0}^{m-1} (x_{p(j)+1} \top \cdots \top x_{p(j+1)}).$$

Tärkeä erikoistapaus on se, jossa alkioina x_1, ..., x_n on sama magman E alkio x. Kaikilla $n \geq 1$ saadaan tällöin alkion x n:s *potenssi*

$$\overset{n}{\top} x = x \top \cdots \top x,$$

missä x esiintyy oikealla puolella n kertaa. Jos magman laskutoimituksena on kertolasku (ns. *multiplikatiivinen merkintä*), käytetään tietenkin normaalia potenssimerkintää

$$x^n = x \cdots x.$$

Jos taas laskutoimituksena on yhteenlasku (*additiivinen merkintä*), sanotaan potenssia alkion x n:nneksi *kerrannaiseksi*, ja se merkitään

$$nx = x + \cdots + x.$$

Soveltamalla yleistettyä liitäntälakia jonoon, jossa toistuu liitännäisen magman alkio x, saadaan kaikilla kokonaisluvuilla n, $m \geq 1$ seuraavat *potenssilait*

$$\overset{n+m}{\top} x = (\overset{n}{\top} x) \top (\overset{m}{\top} x),$$

$$\overset{nm}{\top} x = \overset{n}{\top}(\overset{m}{\top} x),$$

jotka multiplikatiivisin ja additiivisin merkinnöin ovat myös tuttuja:

$$x^{n+m} = x^n x^m, \quad x^{nm} = (x^m)^n,$$

$$(n+m)x = nx + mx, \quad (nm)x = n(mx).$$

Vakaat osajoukot.

MÄÄRITELMÄ 1.1.5. Magman E osajoukko A on *vakaa* (laskutoimituksen $\top$ suhteen), jos $x \top y \in A$ aina kun $x \in A$ ja $y \in A$. Kuvaus $(x, y) \mapsto x \top y$ joukosta $A \times A$ joukkoon A on tällöin $\top$:n *indusoima laskutoimitus* A:ssa ja sillä varustettuna A on E:n *alimagma*.

Vakaitten osajoukkojen leikkaukset ovat edelleen vakaita. Jokainen magman E osajoukko X sisältyy johonkin vakaaseen osajoukkoon A', esim. koko joukkoon E. Olkoon A tällaisten X:n sisältävien vakaiden osajoukkojen leikkaus. Se on myös vakaa ja sisältää X:n.

Joukko A on silloin pienin X:n sisältävä E:n vakaa osajoukko eli *osajoukon X virittämä E:n vakaa osajoukko* (tai *alimagma*).

Tällöin sanotaan myös, että X *virittää* alimagman A, tai että X on A:n *virittäjäjoukko.*

Seuraavien lauseiden todistukset jätetään harjoitustehtäviksi.

LAUSE 1.1.6. *Olkoot E, F magmoja ja $f\colon E \to F$ homomorfismi.*

i) *E:n vakaan osajoukon A kuva $f(A)$ on vakaa F:ssä.*
ii) *F:n vakaan osajoukon B alkukuva $f^{-1}(B)$ on vakaa E:ssä.*
iii) *E:n osajoukon X virittämän vakaan E:n osajoukon A kuva $f(A)$ on kuvajoukon $f(X)$ virittämä F:n vakaa osajoukko.*
iv) *Jos $g\colon E \to F$ on toinen homomorfismi, niin*

$$A = \{x \in E \mid f(x) = g(x)\}$$

on E:n vakaa osajoukko.

KOROLLAARI 1.1.7. *Olkoot E, F magmoja, f, $g\colon E \to F$ homomorfismeja ja X jokin E:n virittäjäjoukko. Jos $f(x) = g(x)$ kaikilla $x \in X$, niin $f = g$.*

Todistus. Lauseen 1.1.6 mukaan $A = \{x \in E \mid f(x) = g(x)\}$ on E:n vakaa osajoukko. Jos se sisältää kaikki E:n virittäjäjoukon X alkiot, niin se on välttämättä koko E, ja siten $f = g$. □

LAUSE 1.1.8. *Olkoon E liitännäinen magma, X sen osajoukko ja X' joukko, jonka muodostavat alkiot*

$$x_1 \top x_2 \top \cdots \top x_n,$$

missä $n \geq 1$ ja $x_i \in X$ $(1 \leq i \leq n)$. Tällöin X' on X:n virittämä E:n vakaa osajoukko.

Vaihdannaisuus.

MÄÄRITELMÄ 1.1.9. Olkoon E magma, jonka laskutoimitus on $\top$. Kaksi E:n alkiota x ja y ovat *vaihdannaiset*, eli ne *kommutoivat*, jos

$$y \top x = x \top y.$$

Laskutoimitus $\top$ on *vaihdannainen* eli *kommutatiivinen*, jos kaikki E:n alkiot kommutoivat keskenään. Tällöin E on *vaihdannainen magma.*

Huomautus. Vaihdannainen magma on siis sama kuin sen vastamagma.

Esimerkkejä. 12) Reaalilukujen yhteenlasku ja kertolasku ovat vaihdannaisia laskutoimituksia.

13) Matriisien yhteenlasku on vaihdannainen laskutoimitus mutta kertolasku ei yleensä ole vaihdannainen.

14) Jos X on joukko, jossa on vähintään kaksi alkiota, niin kuvausten yhdistäminen joukossa $E = X^X$ ei ole vaihdannainen laskutoimitus.

15) Joukon A osajoukkojen yhdisteen ja leikkauksen muodostamiset ovat vaihdannaisia laskutoimituksia potenssijoukossa $\mathcal{P}(A)$.

16) Kolmiulotteisen vektoriavaruuden $\mathbf{R}^3$ ristitulo ei ole vaihdannainen laskutoimitus, sillä $\mathbf{y} \times \mathbf{x} = -\mathbf{x} \times \mathbf{y}$.

Tärkeimmät laskutoimitukset algebrassa ovat sekä liitännäisiä että vaihdannaisia. Tällaisia voidaan soveltaa myös useaan alkioon missä järjestyksessä tahansa. Tarkemmin:

Olkoon E *liitännäinen ja vaihdannainen* magma, ja olkoon $(x_i)_{i\in I}$ epätyhjä äärellinen perhe E:n alkioita. Jos I:ssä on n alkiota i_1, i_2, $\dots$, i_n, niin E:n alkio

$$\mathop{\top}_{j=1}^{n} x_{i_j} = x_{i_1} \top x_{i_2} \top \cdots \top x_{i_n}$$

on *riippumaton järjestyksestä* i_1, i_2, $\dots$, i_n. Sille voidaan siten käyttää lyhyttä merkintää

$$\mathop{\top}_{i\in I} x_i,$$

vaikka I ei olisi järjestetty joukko.

Liitännäisen ja vaihdannaisen kertolaskun ja yhteenlaskun tapauksessa on perinteisesti tapana käyttää omia erikoismerkintöjään:

$$\prod_{i\in I} x_i = x_{i_1} x_{i_2} \cdots x_{i_n}$$

ja

$$\sum_{i\in I} x_i = x_{i_1} + x_{i_2} + \cdots + x_{i_n}.$$

Tekijämagmat. Olkoon E magma, jonka laskutoimitus on $\top$. Olkoon R jokin ekvivalenssirelaatio E:ssä ja $p\colon E \to E/R$ kanoninen surjektio tekijäjoukolle.

Jos E/R on myös magma (laskutoimituksena $\top$) ja p on homomorfismi, niin kaikilla E:n alkioilla x ja y alkion $x \top y$ ekvivalenssiluokka $p(x \top y)$ on sama kuin $p(x) \top p(y)$ ja riippuu siten vain x:n ja y:n ekvivalenssiluokista $p(x)$ ja $p(y)$. Seuraavan määritelmän ominaisuus on siis silloin voimassa.

MÄÄRITELMÄ 1.1.10. Laskutoimitus $\top$ ja ekvivalenssi R joukossa E ovat *yhteensopivat*, jos kaikilla E:n alkioilla x, x', y ja y' ehdoista

$$x \equiv x', \quad y \equiv y' \pmod R$$

seuraa

$$x \top y \equiv x' \top y' \pmod R.$$

Huomautus. Laskutoimitusten kanssa yhteensopivia ekvivalenssirelaatioita sanotaan usein *kongruensseiksi.*

Jos laskutoimitus $\top$ ja ekvivalenssirelaatio R ovat yhteensopivat, niin tekijäjoukossa E/R on yksikäsitteinen laskutoimitus $\top$, joka kaikilla E:n alkioilla x ja y toteuttaa ehdon

$$p(x) \top p(y) = p(x \top y).$$

Tällä varustettuna E/R on E:n *tekijämagma*, ja kanoninen surjektio $p\colon E \to E/R$ on homomorfismi.

Tekijämagman perusominaisuus ilmenee seuraavassa lauseessa.

LAUSE 1.1.11 (Homomorfismin hajotuslause). *Olkoot E ja F magmoja, $f\colon E \to F$ homomorfismi, E/R E:n tekijämagma ja $p\colon E \to E/R$ kanoninen homomorfismi.*

Tällöin f:llä on hajotelma $f = g \circ p$, missä $g\colon E/R \to F$ on homomorfismi, jos ja vain jos f sopeutuu ekvivalenssiin R.

$$\begin{tikzcd} E \arrow[rr, "f"] \arrow[dr, "p"'] & & F \\ & E/R \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Todistus. Lauseen 0.2.3 nojalla f voidaan esittää yhdistelmänä $g \circ p$, missä $g\colon E/R \to F$ on jokin kuvaus, jos ja vain jos f sopeutuu ekvivalenssiin R. Toisaalta on helppo nähdä, että jokainen ehdon toteuttava kuvaus g on homomorfismi, kun f on homomorfismi, koska p on surjektiivinen (harj. teht.). $\square$

Harjoitustehtäviä

1) Olkoon E liitännäinen magma ja $x_1, \ldots, x_n \in E$. Todistettava yleistetty liitäntälaki

$$x_1 \top \cdots \top x_n = (x_1 \top \cdots \top x_p) \top (x_{p+1} \top \cdots \top x_n) \qquad (1 \leq p \leq n-1).$$

2) Olkoon $\mathbf{R}^3$ magma, jonka laskutoimituksena on ristitulo. Etsittävä joukon $X = \{\mathbf{i}, \mathbf{j}\}$ (kaksi kantavektoria) virittämä vakaa osajoukko.

3) Olkoon $f\colon E \to F$ magmojen homomorfismi. Todistettava:

i) E:n vakaan osajoukon A kuva $f(A)$ on vakaa F:ssä;
ii) F:n vakaan osajoukon B alkukuva $f^{-1}(B)$ on vakaa E:ssä;
iii) E:n osajoukon X virittämän vakaan osajoukon A kuva $f(A)$ on kuvan $f(X)$ virittämä F:n vakaa osajoukko;
iv) F:n osajoukon Y virittämän vakaan osajoukon B alkukuva $f^{-1}(B)$ sisältää alkukuvan $f^{-1}(Y)$ virittämän E:n vakaan osajoukon.

4) Olkoot E, F magmoja ja f, $g\colon E \to F$ kaksi homomorfismia. Osoitettava, että

$$A = \{x \in E \mid f(x) = g(x)\}$$

on E:n vakaa osajoukko.

5) Olkoon E liitännäinen magma, X sen osajoukko ja X' joukko, jonka muodostavat alkiot

$$x_1 \top x_2 \top \cdots \top x_n,$$

missä $n \geq 1$ ja $x_1, x_2, \ldots, x_n \in X$. Osoitettava, että X' on joukon X virittämä E:n vakaa osajoukko.

6) Olkoon $f\colon E \to F$ magmojen homomorfismi, E/R E:n tekijämagma ja $p\colon E \to E/R$ kanoninen homomorfismi. Todistettava hajotuslause: $f = g \circ p$, missä $g\colon E/R \to F$ on homomorfismi, jos ja vain jos f sopeutuu ekvivalenssiin R.

1.2. Neutraalialkiot ja käänteisalkiot

MÄÄRITELMÄ 1.2.1. Magman E alkio e on *neutraalialkio* (laskutoimituksen $\top$ suhteen), jos kaikilla E:n alkioilla x pätee

$$e \top x = x = x \top e.$$

Huomautus. Jos myös e' on neutraalialkio, niin $e = e \top e' = e'$. Neutraalialkio on siis yksikäsitteinen, jos sellainen on olemassa.

Kun laskutoimitus on kertolasku, neutraalialkiota sanotaan *ykkösalkioksi* ja sille käytetään merkintää 1. Yhteenlaskun tapauksessa neutraalialkio on taas *nolla-alkio* 0.

MÄÄRITELMÄ 1.2.2. *Ykköysellinen magma* on magma, jossa on neutraalialkio. *Monoidi* on ykköysellinen liitännäinen magma.

Jos E ja E' ovat monoideja, niin *monoidihomomorfismi* $f\colon E \to E'$ on homomorfismi, joka vie E:n neutraalialkion E':n neutraalialkiolle (eli *ykköysellinen homomorfismi*).

Esimerkkejä. 1) Neliömatriisien joukko $\mathbf{M}_n(\mathbf{R})$ kertolaskullaan varustettuna on monoidi. Sen neutraalialkiona on matriisi I, jonka kertoimet lävistäjällä ovat 1 ja muualla 0.

2) Jos X on joukko, niin joukko $E = X^X$ varustettuna kuvausten yhdistämisellä on monoidi. Sen neutraalialkiona on X:n identtinen kuvaus Id_X, jolle myös käytetään merkintää 1_X.

3) Jokainen rengas A on monoidi kertolaskun suhteen, ns. *renkaan A multiplikatiivinen monoidi*. Sen neutraalialkiona on renkaan ykkösalkio 1.

4) Olkoon E monoidi ja A sen alimagma. Jos A sisältää E:n neutraalialkion, niin se on myös monoidi, E:n *alimonoidi*. Kanoninen injektiokuvaus $i\colon A \to E$ on tällöin monoidihomomorfismi. (A voi myös olla monoidi, jolla on eri neutraalialkio, jolloin se ei ole E:n alimonoidi.)

5) Monoidin E jokainen tekijämagma E/R on myös monoidi, E:n *tekijämonoidi*, ja kanoninen surjektio $p\colon E \to E/R$ on monoidihomomorfismi.

6) Luonnollisten lukujen joukko $\mathbf{N}$ on vaihdannainen monoidi sekä yhteenlaskun että kertolaskun suhteen. Neutraalialkioina ovat 0 ja 1.

7) Jokaisen joukon A potenssijoukko $\mathcal{P}(A)$ on vaihdannainen monoidi sekä yhdisteen että leikkauksen muodostamisen suhteen. Neutraalialkioina ovat $\emptyset$ ja A.

Olkoon E monoidi (laskutoimituksena $\top$) ja e sen neutraalialkio. Koska laskutoimitus on liitännäinen, voidaan E:n alkiot $x_1, x_2, \ldots, x_n$ yhdistää ilman sulkumerkkejä ja merkitä lyhyesti

$$\mathop{\top}_{i\in I} x_i = x_1 \top x_2 \top \cdots \top x_n,$$

missä $I = \{1, 2, \ldots, n\}$, kun $n \geq 1$. Monoidissa tämä merkintä voidaan laajentaa *tyhjän perheen* tapaukseen $(x_i)_{i\in\emptyset}$ $(n = 0)$ asettamalla

$$\mathop{\top}_{i\in\emptyset} x_i = e.$$

Erityisesti jokaisen E:n alkion x 0:s *potenssi* on siis

$$\overset{0}{\top} x = e.$$

Näin määritellen potenssilait

$$\overset{n+m}{\top} x = (\overset{n}{\top} x) \top (\overset{m}{\top} x),$$

$$\overset{nm}{\top} x = \overset{n}{\top}(\overset{m}{\top} x)$$

pysyvät voimassa kaikilla luonnollisilla luvuilla n ja m arvo 0 mukaan luettuna.

Monoidissa voidaan myös tietyin ehdoin yhdistää laskutoimituksella äärettömän alkioperheen $(x_i)_{i\in I}$ alkiot, kun perheen *kantaja*

$$S = \{i \in I \mid x_i \neq e\}$$

on *äärellinen*. Jos tällöin

a) indeksijoukko I on täysin järjestetty, tai
b) monoidi E on vaihdannainen (tai ainakin alkiot x_i kommutoivat keskenään),

niin äärellisen perheen $(x_i)_{i \in S}$ alkiot voidaan yhdistää yksikäsitteisesti, ja siten voidaan määritellä *muodollisesti ääretön* yhdistelmä

$$\top_{i \in I} x_i = \top_{i \in S} x_i.$$

Huomautus. Tässä S:n tilalla voi olla mikä tahansa sen sisältävä I:n äärellinen osajoukko.

Kääntyvät alkiot.

MÄÄRITELMÄ 1.2.3. Olkoon E ykkösellinen magma, $\top$ sen laskutoimitus ja e sen neutraalialkio. Olkoot x ja x' E:n alkioita.
Tällöin x' on x:n

vasemmanpuolinen käänteisalkio,	jos $x' \top x = e$,
oikeanpuolinen käänteisalkio,	jos $x \top x' = e$, ja
käänteisalkio,	jos $x \top x' = e = x' \top x$.

Vastaavasti x on *vasemmalta kääntyvä*, *oikealta kääntyvä* tai *kääntyvä*, jos sillä on vasemmanpuolinen käänteisalkio, oikeanpuolinen käänteisalkio tai käänteisalkio.

Ryhmä on monoidi, jonka jokainen alkio on kääntyvä.

Esimerkki 8) Olkoon X joukko ja $E = X^X$ varustettuna laskutoimituksella $\circ$. Tällöin kuvaus $f \in E$ on

– vasemmalta kääntyvä, jos ja vain jos se on injektiivinen,
– oikealta kääntyvä, jos ja vain jos se on surjektiivinen, ja
– kääntyvä, jos ja vain jos se on bijektiivinen.

Lisäksi kuvauksen f

– vasemmanpuolinen käänteisalkio r on sen *retraktio*: $r \circ f = \mathrm{Id}_X$,
– oikeanpuolinen käänteisalkio s on sen *sektio*: $f \circ s = \mathrm{Id}_X$, ja
– käänteisalkio f^{-1} on sen *käänteiskuvaus*.

Huomautus. Vasemman- tai oikeanpuolisen käänteisalkion ei tarvitse yleensä olla yksikäsitteinen kuten esimerkissäkin nähdään. Tilanne on toinen, jos kumpikin käänteisalkio on olemassa.

LAUSE 1.2.4. *Monoidin E alkio x on kääntyvä, jos ja vain jos se on vasemmalta ja oikealta kääntyvä.*

Tällöin x:llä on yksikäsitteinen käänteisalkio, joka on myös sen ainoa vasemman- tai oikeanpuolinen käänteisalkio.

Todistus. Jokainen kääntyvä alkio on sekä oikealta että vasemmalta kääntyvä suoraan määritelmän perusteella.

Olkoon kääntäen E:n alkiolla x vasemmanpuolinen käänteisalkio x' ja oikeanpuolinen käänteisalkio x''. Laskutoimituksen liitännäisyyden nojalla saadaan silloin

$$x' = x' \top e = x' \top (x \top x'') = (x' \top x) \top x'' = e \top x'' = x''.$$

Tämä merkitsee, että x' (ja x'') on x:n käänteisalkio ja lisäksi yksikäsitteinen. $\square$

Esimerkki 9) Matriisimonoidissa $\mathbf{M}_n(R)$ (esim. 1.2.1) jokainen vasemmalta (tai oikealta) kääntyvä matriisi on myös oikealta (tai vastaavasti vasemmalta) kääntyvä ja sillä on yksikäsitteinen käänteismatriisi.

Multiplikatiivisesti merkityssä monoidissa alkion x käänteisalkiolle käytetään tavallisesti merkintää x^{-1}. Additiivisesti merkityssä monoidissa sitä sanotaan *vasta-alkioksi* ja merkitään $-x$:llä.

LAUSE 1.2.5. *Olkoot x ja y monoidin E alkioita, joilla on käänteisalkiot x' ja y'. Silloin $x \top y$ on kääntyvä, ja $y' \top x'$ on sen käänteisalkio.*

Todistus. Liitännäisyyden nojalla saadaan

$$(y' \top x') \top (x \top y) = y' \top (x' \top x) \top y = y' \top e \top y = y' \top y = e,$$

ja siten $y' \top x'$ on alkion $x \top y$ vasemmanpuolinen käänteisalkio. Samoin nähdään, että se on oikeanpuolinen käänteisalkio. $\square$

Tulos voidaan esittää myös seuraavasti.

KOROLLAARI 1.2.6. *Monoidin E kääntyvien alkioiden joukko E^* on E:n vakaa osajoukko.* $\square$

Lisäksi E^* on E:n alimonoidi, sillä neutraalialkio on aina kääntyvä, ja se sisältää jokaisen alkionsa käänteisalkion, sillä tämä on myös kääntyvä. Alimonoidi E^* on siis ryhmä, monoidin E (suurin) *aliryhmä.*

Esimerkkejä. 10) Renkaan A kääntyvillä alkioilla tarkoitetaan sen multiplikatiivisen monoidin kääntyviä alkioita. Niiden joukko

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

on ryhmä, renkaan A *kääntyvien alkioiden ryhmä.*

Esimerkiksi kokokonaislukujen renkaassa $\mathbf{Z}^* = \{1, -1\}$ on kahden alkion syklinen ryhmä, rationaalilukujen kunnassa taas $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ on ääretön.

11) Olkoon X joukko ja $E = X^X$ laskutoimituksella $\circ$ varustettu monoidi. Esimerkin 1.2.8 mukaan on silloin

$$E^* = \{f \mid f\colon X \to X \text{ on bijektio}\}.$$

Tämä ryhmä on joukon X *symmetrinen ryhmä* eli *täysi permutaatioryhmä*, ja sille käytetään merkintää $\mathfrak{S}_X$.

Olkoon x monoidin E kääntyvä alkio ja x' sen käänteisalkio. Lauseen 1.2.5 nojalla on silloin $\overset{n}{\top}\, x$ myös kääntyvä kaikilla $n \in \mathbf{N}$, ja sen käänteisalkio on $\overset{n}{\top}\, x'$. Siten voidaan määritellä alkion x *negatiiviset potenssit* eksponenteilla $n < 0$ asettamalla

$$\overset{n}{\top}\, x = \overset{-n}{\top}\, x'.$$

Erityisesti saadaan siis x:n käänteisalkiolle merkintä

$$\overset{-1}{\top}\, x = x'.$$

Myös nähdään, että potenssilait pätevät edelleen kaikilla kokonaislukueksponenteilla n ja m.

Jakomonoidi. Algebrassa esiintyy usein tilanteita, joissa monoidin, tai yleisemmin jonkin yhdistetyn struktuurin alkio ei ole kääntyvä, mutta saadaan kääntyväksi, kun struktuuria laajennetaan sopivasti.

Perinteinen esimerkki on luonnollisten lukujen additiivisen monoidin $\mathbf{N}$ laajennus kokonaislukujen ryhmäksi $\mathbf{Z}$. Monoidissa $\mathbf{N}$ vain 0 on kääntyvä yhteenlaskun suhteen, mutta ryhmässä $\mathbf{Z}$ jokaisella alkiolla on vasta-alkio.

Vastaava kertolaskua koskeva esimerkki on kokonaislukujen renkaan laajennus rationaalilukujen kunnaksi. Multiplikatiivisessa monoidissa $\mathbf{Z}$ vain 1 ja -1 ovat kääntyviä, kun taas $\mathbf{Q}$:ssa jokaisella alkiolla nollaa lukuunottamatta on käänteisalkio.

Näissä esimerkeissä käytetty menettely on helposti yleistettävissä. Olkoon E jokin *vaihdannainen* monoidi. Merkintöjen yksinkertaistamiseksi olkoon sen laskutoimituksena kertolasku.

Olkoon S jokin E:n osajoukko. Tarkoituksena on etsiä monoidin E laajennus E_S, jossa kaikki S:n alkiot ovat kääntyviä. Jos esimerkiksi $E = \mathbf{Z}$ ja $S = \mathbf{Z} \setminus \{0\}$, niin E_S voisi olla $\mathbf{Q}$.

Konstruktion perusajatuksena on täydentää monoidia E muodollisesti osamäärillä e/s, missä e on neutraalialkio ja s käy läpi joukon S. Tällöin mukaan on otettava myös kaikki tulot

$$a(e/s_1)(e/s_2)\cdots(e/s_n) = a/p,$$

missä $a \in E$, $s_i \in S$ $(1 \le i \le n)$ ja $p = s_1 s_2 \cdots s_n$.

Olkoon S' joukon S virittämä E:n alimonoidi. Sen muodostavat tulot (vrt. 1.1.8)

$$\prod_{i=1}^{n} s_i = s_1 s_2 \cdots s_n,$$

missä $s_i \in S$ $(1 \le i \le n)$. (Neutraalialkio e saadaan, kun $n = 0$.)

Määritellään karteesisessa tulossa $E \times S'$ kertolasku asettamalla

$$(a,p)(b,q) = (ab, pq).$$

Laskutoimitus on edelleen sekä liitännäinen että vaihdannainen, ja sillä on neutraalialkio (e,e). Tulo $E \times S'$ on siten vaihdannainen monoidi (ns. monoidien E ja S' *tulomonoidi*).

Tarkastellaan tulossa $E \times S'$ alkioiden $x = (a,p)$ ja $y = (b,q)$ välistä relaatiota R:

$$aqs = bps \text{ jollakin } s \in S'.$$

Huomautus. Jos alkiot $s \in S'$ ovat *supistuvia*, eli ehdosta $aqs = bps$ seuraa $aq = bp$, niin s voidaan jättää pois. Yleisessä monoidissa tämä ei kuitenkaan ole mahdollista.

LEMMA 1.2.7. *R on kertolaskun kanssa yhteensopiva ekvivalenssi.*

Todistus. On ilmeistä, että relaatio R on refleksiivinen ja symmetrinen. Transitiivisuuden osoittamiseksi olkoot $x = (a, p)$, $y = (b, q)$ ja $z = (c, r)$ kolme $E \times S'$:n alkiota, jotka toteuttavat ehdot

$$x \equiv y, \quad y \equiv z \pmod{R},$$

eli

$$aqs = bps, \quad brt = cqt$$

joillakin s, $t \in S'$. Näistä seuraa

$$ar(stq) = bpsrt = cp(stq),$$

missä $stq \in S'$, ja siten pätee $x \equiv z \pmod{R}$.

Olkoot sitten $x = (a, p)$, $y = (b, q)$, $x' = (a', p')$ ja $y' = (b', q')$ neljä tulon $E \times S'$ alkiota, jotka toteuttava ehdot

$$x \equiv y, \quad x' \equiv y' \pmod{R}.$$

Tällöin siis

$$aqs = bps, \quad a'q's' = b'p's'$$

joillakin s, $s' \in S'$, ja siten

$$(aa')(qq')(ss') = (bb')(pp')(ss'),$$

missä $ss' \in S'$. Tämä merkitsee, että $xx' = (aa', pp')$ ja $yy' = (bb', qq')$ täyttävät ehdon

$$xx' \equiv yy' \pmod{R}.$$

$\square$

Lemman nojalla voidaan muodostaa magman $E \times S'$ tekijämagma $E_S = (E \times S')/R$, joka on myös vaihdannainen monoidi, neutraalialkiona parin (e, e) luokka.

MÄÄRITELMÄ 1.2.8. Monoidi E_S on vaihdannaisen monoidin E *jakomonoidi* nimittäjäjoukon S suhteen.

Toisinaan jakomonoidia sanotaan *osamäärämonoidiksi* ja myös *erotusmonoidiksi*, kun laskutoimituksena on yhteenlasku.

Parin $(a, p) \in E \times S'$ luokalle jakomonoidissa E_S käytetään merkintää a/p (ja erotusmonoidissa vastaavasti $a - p$). Tällöin neutraalialkio on e/e ja kertolasku saadaan kaavasta

$$(a/p)(b/q) = ab/pq.$$

Relaation R määritelmän nojalla ehto

$$a/p = a'/p'$$

on voimassa, jos ja vain jos $ap's = a'ps$ jollakin $s \in S'$. Erityisesti yhtälö

$$a/p = as/ps$$

on yleispätevä kaikilla $s \in S'$.

Kuvaus $\varepsilon \colon E \to E_S$, $a \mapsto a/e$, vie kahden monoidin E alkion a ja b tulon kuvien tulolle

$$ab/e = (a/e)(b/e)$$

ja monoidin E neutraalialkion e jakomonoidin E_S neutraalialkiolle e/e. Se on siten monoidihomomorfismi, ja sitä sanotaan *kanoniseksi homomorfismiksi.*

Jokaisen joukon S alkion s kuva $\varepsilon(s) \in E_S$ on kääntyvä ja sillä on käänteisalkio

$$\varepsilon(s)^{-1} = e/s,$$

koska $(s/e)(e/s) = s/s = e/e$.

Huomautus. Kanoninen homomorfismi ε ei välttämättä ole injektiivinen, sillä ehto $as = bs$ voi olla voimassa jollakin $s \in S'$ ja siten $a/e = b/e$, vaikka olisi $a \neq b$. Jos kuitenkin jokainen S':n alkio on supistuva, niin ε on injektiivinen.

Seuraavassa lauseessa esitetään jakomonoidin perusominaisuus, joka osoittaa, että konstruktio on paras mahdollinen silloinkin, kun kanoninen homomorfismi ei ole injektiivinen eikä jakomonoidia E_S siten voida joukkona pitää monoidin E laajennuksena.

LAUSE 1.2.9. *Olkoon E vaihdannainen monoidi, S sen osajoukko, E_S jakomonoidi nimittäjäjoukon S suhteen ja $\varepsilon \colon E \to E_S$ kanoninen homomorfismi. Jos F on vaihdannainen monoidi ja $f \colon E \to F$ on sellainen homomorfismi, että joukon $f(S)$ alkiot ovat kääntyviä F:ssä, niin on olemassa yksikäsitteinen homomorfismi $\bar{f} \colon E_S \to F$, joka täyttää ehdon $\bar{f} \circ \varepsilon = f$.*

$$\begin{tikzcd} E \arrow[rr, "f"] \arrow[dr, "\varepsilon"'] & & F \\ & E_S \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Todistus. Olkoon $\bar{f}$ jokin ehdon toteuttava homomorfismi. Monoidin E_S alkiot ovat a/p, missä $a \in E$ ja p on joukon S virittämässä E:n alimonoidissa S', ja tällöin pätee

$$(a/p)\varepsilon(p) = ap/pe = a/e = \varepsilon(a).$$

Soveltamalla homomorfismia $\bar{f}$ saadaan

$$\bar{f}(a/p)\bar{f}(\varepsilon(p)) = \bar{f}(\varepsilon(a))$$

eli

$$\bar{f}(a/p)f(p) = f(a).$$

Toisaalta $f(p)$ on tulo joukon $f(S)$ alkioista, jotka oletuksen mukaan ovat kääntyviä F:ssä. Siten $f(p)$ on myös kääntyvä F:ssä, ja tästä seuraa

$$\bar{f}(a/p) = f(a)f(p)^{-1}.$$

Homomorfismi $\bar{f}$ on siis yksikäsitteinen, jos sellainen on olemassa.

Olemassaolon osoittamiseksi tarkastellaan kuvausta

$$g\colon E \times S' \to F,$$

missä $(a,p) \mapsto f(a)f(p)^{-1}$. Jos (a,p) ja (a',p') ovat tulomonoidin $E \times S'$ alkioita, niin

$$\begin{aligned} g((a,p)(a',p')) &= g(aa',pp') \\ &= f(aa')f(pp')^{-1} \\ &= f(a)f(a')(f(p)f(p'))^{-1} \\ &= f(a)f(a')f(p')^{-1}f(p)^{-1}, \end{aligned}$$

ja koska F on vaihdannainen, tämä on edelleen

$$f(a)f(p)^{-1}f(a')f(p')^{-1} = g(a,p)g(a',p').$$

Lisäksi neutraalialkion (e,e) kuva $f(e)f(e)^{-1}$ on neutraalialkio. Kuvaus g on siten monoidihomomorfismi.

Määritelmän mukaan E_S on monoidin $E \times S'$ tekijämonoidi ekvivalenssirelaation R suhteen. Homomorfismin $\bar{f}$ olemassaolon todistamiseksi osoitetaan, että g sopeutuu ekvivalenssiin R.

Olkoot (a,p) ja (a',p') kaksi tulon $E \times S'$ alkiota, jotka toteuttavat ehdon

$$(a,p) \equiv (a',p') \pmod{R}.$$

Tällöin siis $ap's = a'ps$ jollakin $s \in S'$. Koska f on homomorfismi, tästä seuraa

$$f(a)f(p')f(s) = f(a')f(p)f(s)$$

ja, koska $f(s)$ on kääntyvä, edelleen

$$f(a)f(p') = f(a')f(p).$$

Kun $f(p)$ ja $f(p')$ ovat myös kääntyviä, saadaan

$$f(a)f(p)^{-1} = f(a')f(p')^{-1}$$

eli $g(a,p) = g(a',p')$. Homomorfismi g sopeutuu siis ekvivalenssiin R.

Hajotuslauseen 1.1.11 nojalla on olemassa yksikäsitteinen homomorfismi $\bar{f}\colon (E \times S')/R \to F$, joka toteuttaa ehdon

$$\bar{f}(a/p) = g(a,p) = f(a)f(p)^{-1}$$

kaikilla $a/p \in E \times S'$. Tästä seuraa välittömästi, että $\bar{f}$ on monoidihomomorfismi ($\bar{f}(e/e)$ on neutraalialkio) ja $\bar{f} \circ \varepsilon = f$. $\square$

Lauseen tulos voidaan tulkita seuraavasti. Jokainen monoidin E_S alkioiden $\varepsilon(a)$ ($a \in E$) algebrallinen ominaisuus (esim. yhtälö) on voimassa myös monoidissa F alkioilla $f(a)$, koska ominaisuus säilyy homomorfismissa $\bar{f}$. Esimerkiksi, jos a, $b \in E$ ja $\varepsilon(a) = \varepsilon(b)$, niin myös $f(a) = f(b)$.

Tämä ilmaistaan usein sanomalla, että E_S (ja ε) on *universaalinen* (yleispätevä, "paras mahdollinen") ehdolla

"*joukon S alkioiden kuvat ovat kääntyviä.*"

Harjoitustehtäviä

1) Olkoon A joukko ja B sen osajoukko ($B \neq \emptyset, A$). Olkoon $E = \mathcal{P}(A)$ laskutoimituksella

$$\text{a) } (X, Y) \mapsto X \cap Y \text{ tai b) } (X, Y) \mapsto X \cup Y$$

varustettu monoidi. Tutkittava, onko
i) $F = \mathcal{P}(B)$ monoidin E alimonoidi,
ii) $X \mapsto X \cup B$ monoidihomomorfismi $E \to E$,
iii) $X \mapsto X \cap B$ monoidihomomorfismi $E \to E$ tai $E \to F$.

Seuraavissa tehtävissä $m \geq 1$ ja n ovat luonnollisia lukuja.

2) Osoitettava, että lukujen $x, y \in \mathbf{N}$ välinen relaatio

$$x = y \text{ tai } (x \geq n \text{ ja } y \geq n \text{ ja } m \mid x - y)$$

on ekvivalenssirelaatio $R_{m,n}$ joukossa $\mathbf{N}$.

3) Osoitettava, että additiivisen monoidin $\mathbf{N}$ yhteenlasku ja ekvivalenssirelaatio $R = R_{m,n}$ (teht. 2) ovat yhteensopivat, ja kuvailtava tekijämonoidia $E = \mathbf{N}/R$ ("ϱ-monoidi").

4) Olkoon E monoidi ja $f \colon \mathbf{N} \to E$ monoidihomomorfismi, joka ei ole injektiivinen ($\mathbf{N}$ on additiivinen monoidi). Osoitettava, että homomorfismiin f liittyvä ekvivalenssirelaatio on $R_{m,n}$ eräillä luonnollisilla luvuilla $m \geq 1$ ja n.

5) Olkoon E tekijämonoidi $\mathbf{N}/R$, missä $R = R_{m,n}$, ja $\varepsilon \colon E \to E_E$ sen kanoninen homomorfismi erotusryhmäänsä E_E. Olkoot $\bar{x}$, $\bar{y} \in E$ lukujen x, $y \in \mathbf{N}$ luokat. Osoitettava, että $\varepsilon(\bar{x}) = \varepsilon(\bar{y})$, jos ja vain jos $x \equiv y \pmod{m}$. (Jos $\bar{x} + \bar{z} = \bar{y} + \bar{z}$ jollakin $\bar{z} \in E$, niin tämä pätee myös, kun $\bar{z}$ on jonkin luvun $z \geq n$ luokka.)

6) Olkoon E tekijämonoidi $\mathbf{N}/R_{m.n}$. Osoitettava, että kanoninen homomorfismi $\varepsilon \colon E \to E_E$ on surjektiivinen ja ryhmä E_E isomorfinen tekijäryhmän $\mathbf{Z}/m\mathbf{Z}$ kanssa. (E_E:n alkiot ovat $\bar{x} - \bar{y} = \varepsilon(\bar{x}) - \varepsilon(\bar{y})$, missä $\bar{x}, \bar{y} \in E$, ja kongruenssilla $x \equiv y + z \pmod{m}$ on aina ratkaisuja $z \in \mathbf{N}$. Homomorfismi $E_E \to \mathbf{Z}/m\mathbf{Z}$ saadaan universaaliominaisuudesta.)

1.3. Ryhmät

Tässä pykälässä kerrataan ja täydennetään ryhmien teoriaa. Laskutoimitus merkitään kertolaskuna ellei toisin mainita. Ryhmien ei tarvitse olla vaihdannaisia.

Homomorfismit. Olkoot G ja H ryhmiä sekä $e \in G$ ja $e' \in H$ niiden neutraalialkiot. Kumpikin ryhmä on myös magma, ja kuvaus $f\colon G \to H$ on (magmojen) homomorfismi, kun kaikilla $x, y \in G$ pätee

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

LEMMA 1.3.1. *Jokainen homomorfismi $f\colon G \to H$ on ykkösellinen ja toteuttaa kaikilla $x \in G$ ehdon*

$$f(x^{-1}) = f(x)^{-1}.$$

Todistus. Yhtälöstä $ee = e$ seuraa $f(e)f(e) = f(e)$ ja edelleen

$$f(e) = f(e)f(e)^{-1} = e',$$

koska $f(e)$ on kääntyvä ryhmässä H. Homomorfismi f on siten ykkösellinen.

Jos $x \in G$, niin ehdoista $xx^{-1} = e = x^{-1}x$ seuraa edellä esitetyn nojalla

$$f(x)f(x^{-1}) = f(e) = e' = f(x^{-1})f(x),$$

eli $f(x^{-1})$ on $f(x)$:n käänteisalkio. □

Ryhmien välisiä homomorfismeja sanotaan usein *ryhmähomomorfismeiksi*. Jokainen ryhmähomomorfismi on siis myös monoidihomomorfismi.

Aliryhmät. Määritelmän 1.2.3 mukaan ryhmä on monoidi, jonka jokainen alkio on kääntyvä. Siksi on luonnollista määritellä ryhmän aliryhmä alimonoidiksi, joka sisältää alkioidensa käänteisalkiot.

MÄÄRITELMÄ 1.3.2. Ryhmän G *aliryhmä* on G:n osajoukko H, joka toteuttaa ehdot:

i) H sisältää G:n neutraalialkion e.
ii) H on vakaa, eli jos $x \in H$ ja $y \in H$, niin $xy \in H$.
iii) Jos $x \in H$, niin $x^{-1} \in H$.

Huomautus. Ehdot voidaan esittää lyhyemmin muodossa

i) $H \neq \emptyset$, ja
ii) jos $x \in H$ ja $y \in H$, niin $xy^{-1} \in H$,

kuten Algebra I:n kurssissa osoitetaan. (Tosin $H \neq \emptyset$ todennetaan melkein aina näyttämällä, että H sisältää neutraalialkion.)

Olkoon G ryhmä ja X jokin sen osajoukko. Tarkastellaan kaikkia G:n aliryhmiä H', jotka sisältävät joukon X. Niiden leikkaus H on myös G:n aliryhmä ja lisäksi pienin kaikista niistä aliryhmistä, jotka sisältävät X:n.

Tällöin sanotaan, että H on X:n *virittämä G:n aliryhmä*, ja että X *virittää aliryhmän H* eli on *aliryhmän H virittäjäjoukko.*

On selvää, että aliryhmä H sisältää joukon X alkioiden käänteisalkiot. Toisinaan on hyödyllistä tietää, että näiden joukko

$$X^{-1} = \{x^{-1} \mid x \in X\}$$

yhdessä X:n kanssa virittää aliryhmän H jo monoidina.

LAUSE 1.3.3. *Jos X on ryhmän G epätyhjä osajoukko, niin X:n virittämä aliryhmä on joukon $Y = X \cup X^{-1}$ virittämä vakaa osajoukko.*

Lauseen 1.1.8 nojalla tämä merkitsee, että joukon X virittämän aliryhmän alkiot ovat tulot

$$x_1 x_2 \cdots x_n,$$

missä $n \geq 1$ ja $x_i \in X \cup X^{-1}$ $(1 \leq i \leq n)$. Esimerkiksi neutraalialkio voidaan esittää muodossa $e = xx^{-1}$, missä x on mikä tahansa X:n alkio. Lauseen todistus jääköön harjoitustehtäväksi.

KOROLLAARI 1.3.4. *Jos ryhmän G osajoukon X alkiot kommutoivat keskenään, niin X:n virittämä aliryhmä on vaihdannainen.*

Todistus. Olkoot x ja y joukon X alkioita. Kun tulot yx ja xy ovat samat, ovat niiden käänteisalkiot myös samat: $x^{-1}y^{-1} = y^{-1}x^{-1}$. Kertomalla yhtälö $yx = xy$ vasemmalta ja oikealta alkiolla y^{-1} saadaan lisäksi $xy^{-1} = y^{-1}x$.

Joukon $Y = X \cup X^{-1}$ alkiot kommutoivat siten keskenään ja samoin kommutoivat niiden tulot, jotka muodostavat X:n virittämän aliryhmän. □

Huomautus. Ryhmän osajoukon X virittämälle aliryhmälle käytetään toisinaan merkintää $\langle X \rangle$. Jos erityisesti X:n alkiot luetellaan, esim. $X = \{x\}$ tai $X = \{x, y\}$, niin merkitään lyhyesti $\langle x \rangle$, $\langle x, y \rangle$, jne.

Tekijäryhmät. Olkoon G ryhmä ja R ekvivalenssirelaatio G:ssä. Jos R on yhteensopiva G:n laskutoimituksen kanssa, niin neutraalialkion ekvivalenssiluokka

$$H = \{x \in G \mid x \equiv e \pmod R\}$$

on G aliryhmä. (Esimerkiksi, jos $x \in H$, niin yhteensopivuuden nojalla

$$e = x^{-1}x \equiv x^{-1}e = x^{-1} \pmod R,$$

eli $x^{-1} \in H$.)

Lisäksi kaikilla x, $y \in G$ pätee

$$\begin{aligned} y \equiv x \pmod R \ &\Leftrightarrow\ x^{-1}y \equiv x^{-1}x = e \pmod R \\ &\Leftrightarrow\ x^{-1}y \in H \\ &\Leftrightarrow\ y \in xH. \end{aligned}$$

Alkion $x \in G$ ekvivalenssiluokka relaatiossa R on siis

$$xH = \{xz \mid z \in H\}$$

eli x:n *vasen sivuluokka* aliryhmän H suhteen. Pieni muutos päättelyssä osoittaa, että sama ekvivalenssiluokka on myös x:n *oikea sivuluokka*

$$Hx = \{zx \mid z \in H\}.$$

Siten välttämättä kaikilla $x \in G$ saadaan

$$xH = Hx$$

eli yhtäpitävästi

$$xHx^{-1} = H.$$

MÄÄRITELMÄ 1.3.5. Ryhmän G aliryhmä H on G:n *normaali aliryhmä*, jos kaikilla $x \in G$

$$xHx^{-1} = H.$$

Huomautus. Ehdon osoittamiseksi on riittävää todentaa seuraava *normaalisuuskriteeri*

$$xHx^{-1} \subset H \quad \text{kaikilla } x \in G.$$

(Sillä tällöin myös $x^{-1}H(x^{-1})^{-1} \subset H$ ja siten $H \subset xHx^{-1}$.)

Yhteenvetona yllä esitetyistä tarkasteluista saadaan seuraava tulos.

LAUSE 1.3.6. *Ekvivalenssi R ryhmässä G on yhteensopiva G:n laskutoimituksen kanssa, jos ja vain jos se voidaan esittää muodossa*

$$x^{-1}y \in H, \quad (\textit{tai } yx^{-1} \in H)$$

missä H on G:n normaali aliryhmä.

Todistus. Ehdon välttämättömyys on näytetty edellä. Kääntäen jokaiseen normaaliin aliryhmään H liittyvä ekvivalenssirelaatio R on yhteensopiva ryhmän laskutoimituksen kanssa. Jos näet

$$x \equiv x', \quad y \equiv y' \pmod R$$

eli $x' \in xH$ ja $y' \in yH$, niin

$$x'y' \in xHyH = xy(y^{-1}Hy)H = xyHH = xyH,$$

koska $y^{-1}Hy = H$, ja siten

$$xy \equiv x'y' \pmod R.$$

□

Välittömästi nähdään, että tekijämonoidi G/R on ryhmä, ryhmän G *tekijäryhmä* aliryhmän H suhteen ja sille käytetään merkintää

$$G/H = G/R.$$

Vastaavasti ekvivalenssirelaatio R merkitään

$$x \equiv y \pmod H \quad (\Leftrightarrow x^{-1}y \in H).$$

Homomorfismien hajotelmat. Olkoot G ja G' ryhmiä neutraalialkioinaan e ja e', ja olkoon $f\colon G \to G'$ homomorfismi. Olkoon R kuvaukseen f liittyvä, eli ehdon

$$f(x) = f(y),$$

määrittelemä ekvivalenssi G:ssä. Se on yhteensopiva G:n laskutoimituksen kanssa, koska f on homomorfismi.

Jos $f(x) = f(x')$ ja $f(y) = f(y')$, niin

$$f(xy) = f(x)f(y) = f(x')f(y') = f(x'y').$$

Lauseen 1.3.6 nojalla neutraalialkion e luokka

$$H = \{x \in G \mid f(x) = e'\} = f^{-1}(e')$$

on silloin G:n *normaali* aliryhmä, ja relaatio R voidaan esittää muodossa

$$f(x) = f(y) \;\Leftrightarrow\; x^{-1}y \in H.$$

Normaali aliryhmä H on homomorfismin f *ydin* ja sille käytetään merkintää

$$\mathrm{Ker}(f) = f^{-1}(e') \subset G.$$

Vastaavasti f:n *kuva*

$$\mathrm{Im}(f) = f(G) \subset G'$$

on ryhmän G' aliryhmä, joka ei kuitenkaan yleensä ole normaali.

Homomorfismin f *kanoninen hajotelma* (0.2.4) on silloin

$$f\colon G \xrightarrow{p} G/\mathrm{Ker}(f) \xrightarrow{\tilde{f}} \mathrm{Im}(f) \xrightarrow{j} G',$$

missä p on kanoninen homomorfismi, $\tilde{f}$ on isomorfismi (*homomorfialause*, A I) ja j on kanoninen injektio.

Erityisesti nähdään, että f on injektiivinen, jos ja vain jos p on bijektiivinen, eli

$$f \text{ on injektiivinen } \;\Leftrightarrow\; \mathrm{Ker}(f) = \{e\},$$

ja vastaavasti

$$f \text{ on surjektiivinen } \;\Leftrightarrow\; \mathrm{Im}(f) = G'.$$

Lause 1.3.7 (Homomorfismien hajotuslause). *Olkoot G, G' ja H ryhmiä sekä $f\colon G \to G'$ ja $p\colon G \to H$ homomorfismeja.*

Jos p on surjektiivinen, niin on olemassa sellainen homomorfismi $f'\colon H \to G'$, että

$$f = f' \circ p,$$

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "p"'] & & G' \\ & H \arrow[ur, dashed, "f'"'] & \end{tikzcd}$$

jos ja vain jos

$$\mathrm{Ker}(p) \subset \mathrm{Ker}(f).$$

Tällöin f' on yksikäsitteinen, ja lisäksi

$$\mathrm{Ker}(f') = p(\mathrm{Ker}(f)), \quad \mathrm{Im}(f') = \mathrm{Im}(f).$$

Todistus. Ehdon välttämättömyys on ilmeinen. Jos näet $f = f' \circ p$, niin ehdosta $x \in \mathrm{Ker}(p)$ seuraa $f(x) = f'(p(x)) = f'(e) = e' \in G'$.

Käänteisen väitteen todistamiseksi oletetaan, että p on surjektiivinen, jolloin kuvauksen f' yksikäsitteisyys seuraa kuvausten supistussäännöstä 0.1.1. Koska p ja f ovat homomorfismeja, niihin liittyvät ekvivalenssirelaatiot ovat (lause 1.3.6)

$$x^{-1}y \in \mathrm{Ker}(p) \quad \text{ja} \quad x^{-1}y \in \mathrm{Ker}(f).$$

Jos tällöin $\mathrm{Ker}(p) \subset \mathrm{Ker}(f)$, niin hajotuslauseen 0.1.2 ehdot ovat voimassa, joten ehdon $f = f' \circ p$ täyttävä kuvaus f' on olemassa. Helposti nähdään, että se on myös homomorfismi (lause 1.1.11).

Lisäksi ehdosta $f = f' \circ p$ seuraa

$$\mathrm{Ker}(f) = p^{-1}(f'^{-1}(e')) = p^{-1}(\mathrm{Ker}(f')),$$

ja siten $p(\mathrm{Ker}(f)) = \mathrm{Ker}(f')$, koska p on surjektiivinen. Samasta syystä myös pätee

$$\mathrm{Im}(f') = \mathrm{Im}(f).$$

□

KOROLLAARI 1.3.8. *Olkoot f, f' ja p kuten yllä. Silloin*

$$f' \text{ on injektiivinen} \Leftrightarrow \mathrm{Ker}(f) = \mathrm{Ker}(p),$$

ja

$$f' \text{ on surjektiivinen} \Leftrightarrow f \text{ on surjektiivinen.}$$

Todistus. Ehto $\mathrm{Ker}(f) = \mathrm{Ker}(p)$ merkitsee, että aliryhmä

$$\mathrm{Ker}(f') = p(\mathrm{Ker}(f))$$

on triviaali, mistä ensimmäinen väite seuraa. Toinen on ilmeinen. □

Isomorfialauseet. Olkoon G ryhmä, jonka laskutoimitus on tavalliseen tapaan merkitty kertolaskuksi. Jos A ja B ovat G:n osajoukkoja, niin otetaan käyttöön merkintä

$$AB = \{ab \mid a \in A, b \in B\}$$

sille G:n osajoukolle, jonka muodostavat kaikki mahdolliset A:n ja B:n alkioiden tulot.

Huomautus. Vastaava merkintä käy myös monoideissa tai jopa magmoissa. Tällöin tietenkin täytyy käyttää laskutoimituksen mukaista merkintätapaa, esim. $A + B$ tai $A \top B$.

LAUSE 1.3.9 (1. isomorfialause). *Olkoon G ryhmä ja N sen normaali aliryhmä. Jos H on G:n aliryhmä, niin HN on G:n aliryhmä, $H \cap N$ on H:n normaali aliryhmä ja kanonisesta injektiosta $H \to HN$ saadaan tekijäryhmiin siirtymällä isomorfismi*

$$H/(H \cap N) \xrightarrow{\sim} HN/N.$$

$$\begin{tikzcd}[column sep=small] & HN \arrow[dl, dash] \arrow[dr, dash] & \\ H & & N \\ & H \cap N \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

Todistus. Yhdistetystä homomorfismista

$$f\colon H \xrightarrow{j} G \xrightarrow{p} G/N,$$

missä j on kanoninen injektio ja p kanoninen surjektio, saadaan ryhmien homomorfialauseen nojalla isomorfimi

$$\tilde{f}\colon H/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f).$$

Lisäksi f:n ydin on se osa p:n ytimestä N, joka sisältyy aliryhmään H, eli

$$\mathrm{Ker}(f) = H \cap N.$$

Erityisesti $H \cap N$ siis on H:n normaali aliryhmä.

Toisaalta kuvan $\mathrm{Im}(f) = p(H)$ muodostavat H:n alkioiden sivuluokat aliryhmän N suhteen. Siten kaikilla $x \in G$ pätee

$$p(x) \in \mathrm{Im}(f) \;\Leftrightarrow\; p(x) = p(y) \text{ jollakin } y \in H.$$

Tämä merkitsee samaa kuin

$$x \in p(y) = yN \text{ jollakin } y \in H$$

eli yhtäpitävästi $x \in HN$, ja näin saadaan yhtälö

$$p^{-1}(\mathrm{Im}(f)) = HN.$$

Erityisesti HN on aliryhmän alkukuvana G:n aliryhmä.

Todistuksen päättämiseksi on riittävää osoittaa, että $\mathrm{Im}(f)$ on sama kuin HN/N. Tämä seuraa yllä esitetystä, koska p:n surjektiivisuuden nojalla

$$\mathrm{Im}(f) = p(HN) = \{xN \mid x \in HN\} = HN/N.$$

□

Esimerkki 1) Olkoon $n \geq 1$ luonnollinen luku ja $G = \mathfrak{S}_n$ kaikista joukon $X = \{1, 2, \ldots, n\}$ permutaatioista koostuva symmetrinen ryhmä $\mathfrak{S}_X$ (esim. 1.2.11). Parilliset permutaatiot muodostavat sen aliryhmän $N = \mathfrak{A}_n$, jota sanotaan n:n alkion *alternoivaksi ryhmäksi*.

Jos $n \geq 2$, niin $\mathfrak{A}_n$ on ryhmän $\mathfrak{S}_n$ normaali aliryhmä ja sillä on kaksi sivuluokkaa: parilliset permutaatiot ja parittomat permutaatiot. Siten tekijäryhmä

$$G/N = \mathfrak{S}_n/\mathfrak{A}_n \cong \mathbf{Z}/2\mathbf{Z}$$

on kahden alkion syklinen ryhmä.

Itse asiassa jokainen aliryhmä, jolla on kaksi sivuluokkaa on normaali.

Permutaatiot, jotka pitävät luvun n paikallaan, muodostavat ryhmän $\mathfrak{S}_n$ aliryhmän

$$H = \{s \in \mathfrak{S}_n \mid s(n) = n\},$$

joka on isomorfinen ryhmän $\mathfrak{S}_{n-1}$ kanssa. Jos nyt $n \geq 3$, niin ryhmässä H on myös parittomia permutaatioita. Tulo HN sisältää silloin N:n kummankin sivuluokan, joten $HN = G$ ja siksi

$$HN/N \cong \mathbf{Z}/2\mathbf{Z}.$$

Toisaalta ryhmän $H \cong \mathfrak{S}_{n-1}$ parillisten permutaatioiden muodostama aliryhmä $H \cap N$ on isomorfinen ryhmän $\mathfrak{A}_{n-1}$ kanssa. Näin saadaan 1. isomorfialauseen mukainen tulos:

$$H/(H \cap N) \cong \mathfrak{S}_{n-1}/\mathfrak{A}_{n-1} \cong \mathbf{Z}/2\mathbf{Z}.$$

Lause 1.3.10 (2. isomorfialause). *Olkoon G ryhmä, ja olkoot H ja N sen normaaleja aliryhmiä. Jos $N \subset H$, niin H/N on tekijäryhmän G/N normaali aliryhmä, ja kanonisesta homomorfismista $G \to G/N$ saadaan tekijäryhmiin siirtymällä isomorfismi*

$$G/H \xrightarrow{\sim} (G/N)/(H/N).$$

Todistus. Olkoon $f\colon G \to G/N$ kanoninen homomorfismi $x \mapsto xN$. Aliryhmän H kuva

$$f(H) = \{xN \mid x \in H\} = H/N$$

on silloin G/N:n aliryhmä (vrt. lause 1.1.6 i). Itse asiassa se on normaali aliryhmä. Jos näet $x' \in G/N$ ja $y' \in H/N$, niin $x' = f(x)$ ja $y' = f(y)$ joillakin $x \in G$ ja $y \in H$, ja silloin

$$x'y'(x')^{-1} = f(xyx^{-1}) \in f(H) = H/N,$$

koska xyx^{-1} kuuluu normaaliin aliryhmään H. Siten voidaan muodostaa tekijäryhmä $(G/N)/(H/N)$.

Olkoon $g\colon G/N \to (G/N)/(H/N)$ kanoninen homomorfismi. Yhdistetty kuvaus

$$h = g \circ f\colon G \to (G/N)/(H/N)$$

on silloin surjektiivinen homomorfismi, ja sen ydin on

$$\mathrm{Ker}(h) = f^{-1}(\mathrm{Ker}(g)) = f^{-1}(H/N) = H.$$

Ryhmien homomorfialauseen nojalla saadaan siten isomorfismi

$$G/H = G/\mathrm{Ker}(h) \xrightarrow{\sim} \mathrm{Im}(h) = (G/N)/(H/N).$$

□

Esimerkki 2) Olkoot $G = \mathbf{Z}$, $H = m\mathbf{Z}$ ja $N = mn\mathbf{Z}$, missä m, $n \geq 1$. Silloin $G/N = \mathbf{Z}/mn\mathbf{Z}$ on syklinen ryhmä, jossa on mn alkiota, ja sen aliryhmässä $H/N = m\mathbf{Z}/mn\mathbf{Z}$ on n alkiota, nimittäin sivuluokat

$$mk + mn\mathbf{Z} \quad (0 \leq k < n).$$

Tekijäryhmä $(G/N)/(H/N)$ on tällöin myös syklinen ja sen alkioiden lukumäärä on Lagrangen lauseen nojalla $mn/n = m$.

Toisaalta $G/H = \mathbf{Z}/m\mathbf{Z}$ on samoin syklinen ja sen kertaluku on m.

Tulot. Olkoon $(E_i)_{i\in I}$ perhe joukkoja. Sen *karteesisen tulon*

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

alkioina ovat kaikki perheet $(x_i)_{i\in I}$, missä $x_i \in E_i$ $(i \in I)$.

Jos jokainen E_i on magma, laskutoimituksenaan $\top_i$, niin joukossa E voidaan määritellä *laskutoimitusten* $\top_i$ *tulo*

$$((x_i), (y_i)) \mapsto (x_i \top_i y_i).$$

Tällä varustettuna E on magmojen E_i $(i \in I)$ *tulomagma*. Kanoniset projektiot

$$\mathrm{pr}_i \colon E \to E_i, \quad (x_i) \mapsto x_i, \quad (i \in I)$$

ovat silloin homomorfismeja, tulon E *projektiohomomorfismeja*.

On välittömästi nähtävissä, että tulomagma on liitännäinen tai vaihdannainen, jos kaikki magmat E_i ovat sellaisia. Edelleen, jos jokaisella magmalla E_i on neutraalialkio e_i, niin tulomagmalla on neutraalialkio $e = (e_i)$. Jos siis jokainen E_i on monoidi, niin E on monoidi, monoidien E_i $(i \in I)$ *tulomonoidi*.

Olkoon erityisesti $(G_i)_{i\in I}$ ryhmäperhe, jonka jokaisen ryhmän laskutoimitus on merkitty kertolaskuna. Tällöin tulomonoidissa

$$G = \prod_{i\in I} G_i$$

jokaisella alkiolla $x = (x_i)$ on käänteisalkio $x^{-1} = (x_i^{-1})$. Se on siten ryhmä, *ryhmien* G_i $(i \in I)$ *tulo*.

Ne tulon G alkiot $(x_i)_{i\in I}$, joilla $x_i \neq e_i$ vain äärellisen monella indeksillä $i \in I$, eli joiden *kantaja*

$$\{i \in I \mid x_i \neq e_i\}$$

on äärellinen, muodostavat G:n aliryhmän

$$G' = \prod_{i\in I} G_i,$$

jota sanotaan *rajoitetuksi tuloksi*. Jos I on äärellinen, niin se on sama kuin (rajoittamaton) tulo.

Jos ryhmät G_i ovat vaihdannaisia, ja niiden laskutoimituksena on yhteenlasku, niin rajoitettua tuloa sanotaan *suoraksi summaksi*, ja sille käytetään merkintää

$$G' = \bigoplus_{i\in I} G_i.$$

Jokaiseen indeksiin $i_0 \in I$ liittyy *kanoninen injektiohomomorfismi*

$$\iota_{i_0} \colon G_{i_0} \to \prod_{i\in I} G_i,$$

missä alkion $x \in G_{i_0}$ kuva on se perhe $\iota_{i_0}(x) = (x_i)_{i\in I}$, missä $x_{i_0} = x$ ja $x_i = e_i$, kun $i \neq i_0$.

Tavallisesti ryhmät G_{i_0} samastetaan kuviensa $\mathrm{Im}(\iota_{i_0})$ kanssa. Silloin jokainen äärelliskantajainen perhe $x = (x_i) \in G'$ on jäsentensä tulo (tai suoran summan tapauksessa summa):

$$x = \prod_{i \in I} x_i \quad (\text{tai } \sum_{i \in I} x_i).$$

Erityisesti nähdään, että rajoitettu tulo G' on yhdisteen $\bigcup_{i \in I} G_i \subset G$ *virittämä aliryhmä.*

Harjoitustehtäviä

1) Olkoon G ryhmä ja H sen epätyhjä vakaa osajoukko. Osoitettava, että H on G:n aliryhmä, jos se on äärellinen. (Tarkastellaan jonoa $(x^n)_{n \geq 1}$, kun $x \in H$.)

2) Olkoot G ja H ryhmiä, $f\colon G \to H$ homomorfismi, N f:n ydin ja H' H:n aliryhmä. Osoitettava:
i) $G' = f^{-1}(H')$ on G:n aliryhmä ja $N \subset G'$;
ii) jos H' on H:n normaali aliryhmä, niin G' on G:n normaali aliryhmä;
iii) jos f on surjektiivinen, niin $f(G') = H'$ ja f:n rajoittumasta saadaan (homomorfialauseen avulla) isomorfismi $G'/N \xrightarrow{\sim} H'$.

3) Olkoot G ja H ryhmiä, $f\colon G \to H$ homomorfismi, N f:n ydin ja G' G:n aliryhmä. Osoitettava:
i) $H' = f(G')$ on H:n aliryhmä;
ii) $f^{-1}(H') = G'N = NG'$;
iii) jos G' on G:n normaali aliryhmä ja f on surjektiivinen, niin H' on H:n normaali aliryhmä.

4) Olkoot m ja n keskenään jaottomia luonnollisia lukuja (> 0), $p_1\colon \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ ja $p_2\colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ kanoniset homomorfismit ja

$$f\colon \mathbf{Z} \to (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$$

homomorfismi $x \mapsto (p_1(x), p_2(x))$. Osoitettava:
i) $\mathrm{Ker}(f) = mn\mathbf{Z}$;
ii) f:stä saatu homomorfismi $\bar{f}\colon \mathbf{Z}/mn\mathbf{Z} \to (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$ on bijektiivinen;
iii) f on surjektiivinen.

1.4. Toiminnat

Olkoon E joukko. Tarkastellaan kuvauksia $f_\alpha\colon E \to E$, missä α käy läpi jonkin joukon A. Tällainen kuvausperhe vastaa kuvausta

$$A \times E \to E, \quad (\alpha, x) \mapsto f_\alpha(x),$$

joka puolestaan voidaan algebrassa tulkita *laskutoimitukseksi.*

Esimerkki 1) Olkoon E jokin reaalinen vektoriavaruus ja $A = \mathbf{R}$. Tällöin *skalaarikertolaskua*

$$\mathbf{R} \times E \to E, \quad (\alpha, x) \mapsto \alpha x$$

vastaa kuvausperhe $(f_\alpha)_{\alpha \in \mathbf{R}}$, missä

$$f_\alpha \colon x \mapsto \alpha x$$

on avaruuden E *homotetia* (venyttävä tai kutistava).

Olkoon $(f_\alpha)_{\alpha \in A}$ kuten yllä, ja oletetaan lisäksi, että seuraavat ehdot ovat voimassa.

i) $f_e = \mathrm{Id}_E$ jollakin $e \in A$.
ii) Jos α, $\beta \in A$, niin $f_\alpha \circ f_\beta = f_\gamma$ jollakin $\gamma \in A$.

Huomautus. Jos ehdot eivät ole voimassa, niin perhettä (f_α) voidaan täydentää lisäämällä siihen identtinen kuvaus sekä kaikki sen kuvausten yhdistelmät.

Ehtojen ollessa voimassa, joukossa A voidaan määritellä laskutoimitus $(\alpha, \beta) \mapsto \alpha\beta = \gamma$, missä γ täyttää ehdon (ii). Jos lisäksi $f_\gamma \neq f_{\gamma'}$, aina kun $\gamma \neq \gamma'$, laskutoimitus on yksikäsitteinen ja liitännäinen, sillä

$$(f_\alpha \circ f_\beta) \circ f_\gamma = f_\alpha \circ (f_\beta \circ f_\gamma).$$

Lisäksi ehdon (i) määrittelemä alkio $e \in A$ on neutraalialkio, joten A on monoidi.

Nämä tarkastelut voidaan yleistää seuraavasti. Olkoon M monoidi, jonka laskutoimitus on merkitty kertolaskuksi ja neutraalialkio on e.

MÄÄRITELMÄ 1.4.1. Olkoon E joukko. Kuvaus $\alpha \mapsto f_\alpha$ monoidista M joukkoon E^E on M:n *toiminta* joukossa E, jos

i) $f_e = \mathrm{Id}_E$, ja
ii) $f_{\alpha\beta} = f_\alpha \circ f_\beta$ kaikilla α, $\beta \in M$.

Koska E^E varustettuna kuvausten yhdistämistoimituksella on monoidi, ehdot merkitsevät, että kuvaus $\alpha \mapsto f_\alpha$ on monoidihomomorfismi

$$M \to E^E.$$

Monoidin M toiminnalla varustettua joukkoa E sanotaan *M-joukoksi.*

Toiminta tulkitaan tavallisesti laskutoimitukseksi (*tuloksi*) ja sille käytetään merkintää

$$M \times E \to E, \quad (\alpha, x) \mapsto f_\alpha(x) = \alpha.x \text{ (tai } \alpha x).$$

Tällöin määritelmän ehdot saavat seuraavan muodon:

i) $ex = x$, ja
ii) $(\alpha\beta)x = \alpha(\beta x)$

kaikilla α, $\beta \in M$, $x \in E$.

Esimerkkejä. 2) Olkoon M reaalilukujen kunnan $\mathbf{R}$ multiplikatiivinen monoidi (esim. 1.2.3). Jokainen reaalinen vektoriavaruus E on tällöin M-joukko skalaarikertolaskun määrittelemällä toiminnalla (esim. 1.4.1) varustettuna.

3) Olkoon M reaalikertoimisten neliömatriisien multiplikatiivinen monoidi $\mathbf{M}_n(\mathbf{R})$ (ks. esim. 1.2.1). Matriisien ja vektorien kertolasku määrittelee tällöin monoidin M toiminnan $(A, x) \mapsto Ax$ joukossa $\mathbf{R}^n$.

Toisinaan määritelmän ehto (ii) korvataan ehdolla

$$\text{ii}') \ f_{\alpha\beta} = f_\beta \circ f_\alpha,$$

joka merkitsee, että $\alpha \mapsto f_\alpha$ on M:n *vastamonoidin* M^o toiminta E:ssä. Jos merkitään $f_\alpha(x) = x\alpha$, niin ehto saa muodon

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

Tällöin sanotaan, että M *toimii oikealta* joukossa E. Sen vastamonoidi M^o toimii siis silloin määritelmän 1.4.1 mukaisesti eli *vasemmalta* joukossa E.

Esimerkki 4) Olkoon M monoidi. Jokaiseen alkioon $x \in M$ liittyy kaksi kuvausta

i) $\gamma_x \colon M \to M$, $y \mapsto xy$, ja
ii) $\delta_x \colon M \to M$, $y \mapsto yx$,

jotka kaikilla x, $y \in M$ toteuttavat ehdot

$$\gamma_{xy} = \gamma_x \circ \gamma_y, \quad \delta_{xy} = \delta_y \circ \delta_x.$$

Saadaan siis kaksi M:n *kanonista toimintaa* joukossa $E = M$:

i) toiminta vasemmalta: $x \mapsto \gamma_x$, ja
ii) toiminta oikealta: $x \mapsto \delta_x$.

Homomorfismit. Olkoon M monoidi.

MÄÄRITELMÄ 1.4.2. Olkoot E ja F kaksi M-joukkoa. Kuvaus $f \colon E \to F$ on *M-joukkojen homomorfismi* eli *M-morfismi*, jos kaikilla $\alpha \in M$ ja $x \in E$ pätee

$$f(\alpha x) = \alpha f(x).$$

Esimerkki 5) Olkoon M kunnan $\mathbf{R}$ multiplikatiivinen monoidi ja olkoot E, F kaksi reaalista vektoriavaruutta. Tällöin E ja F ovat M-joukkoja (esim. 1.4.2) ja jokainen lineaarikuvaus $f \colon E \to F$ on M-morfismi.

Vakaat osajoukot.

MÄÄRITELMÄ 1.4.3. Olkoon M monoidi ja E M-joukko, toimintanaan $\alpha \mapsto f_\alpha$. Joukon E osajoukko A on *vakaa* M:n toiminnan suhteen, jos kaikilla $\alpha \in M$

$$f_\alpha(A) \subset A.$$

Vakaa osajoukko A on myös M-joukko, kun se varustetaan *indusoidulla toiminnalla* $\alpha \mapsto g_\alpha$, missä

$$g_\alpha \colon x \mapsto \alpha x = f_\alpha(x) \in A, \quad \text{kun } x \in A.$$

Esimerkki 6) Olkoon M reaalilukujen multiplikatiivinen monoidi ja E reaalinen vektoriavaruus varustettuna skalaarikertolaskun määrittelemällä toiminnalla (esim. 1.4.2). Jokainen aliavaruus $F \subset E$ on tällöin vakaa osajoukko, sillä kaikilla $\alpha \in \mathbf{R}$ pätee

$$f_\alpha(F) = \{\alpha x \mid x \in F\} = \alpha F \subset F.$$

LAUSE 1.4.4. *Olkoon M monoidi, E M-joukko ja A sen osajoukko. Tällöin joukko*

$$M_A = \{\alpha \in M \mid \alpha A \subset A\}$$

on M:n alimonoidi.

Todistus. Jos α, $\beta \in M_A$, niin $\alpha\beta \in M_A$, koska

$$(\alpha\beta)A = \alpha(\beta A) \subset \alpha A \subset A.$$

Lisäksi M_A sisältää neutraalialkion e, koska $eA = A$. Siten se on M:n alimonoidi. □

Alimonoidia M_A sanotaan osajoukon A *vakauttajaksi.* Jos $A = \{a\}$ jollakin $a \in E$, niin ehto $\alpha A \subset A$ on sama kuin $\alpha a = a$. Vakauttajaa $M_{\{a\}}$ sanotaan alkion a *kiinnittäjäksi*, ja sille käytetään merkintää

$$M_a = \{\alpha \in M \mid \alpha a = a\}.$$

Jos erityisesti M on ryhmä G, niin kiinnittäjä G_a on G:n aliryhmä, sillä ehdosta $\alpha a = a$ seuraa

$$\alpha^{-1}a = \alpha^{-1}\alpha a = ea = a.$$

Esimerkki 7) Osajoukko $A = \{a\}$ on vakaa M:n toiminnan suhteen, jos ja vain jos vain jos $M_a = M$, eli M *kiinnittää* alkion a. Kaikkien M:n kiinnittämien alkioiden joukolle käytetään merkintää

$$E^M = \{x \in E \mid \alpha x = x \text{ kaikilla } \alpha \in M\}.$$

Se on E:n vakaa osajoukko, ja samoin on sen jokainen osajoukko.

Radat. Olkoon G ryhmä ja E jokin G-joukko. Tarkastellaan seuraavaa relaatiota R:

$$x \in E \text{ ja } y \in E \text{ ja } y = \alpha x \text{ jollakin } \alpha \in G.$$

LEMMA 1.4.5. *Relaatio R on ekvivalenssi joukossa E.*

Todistus. Ekvivalenssin kolme ehtoa vastaavat suoraan ryhmän ja sen toiminnan perusominaisuuksia:

Refleksiivisyys seuraa neutraalialkion $e \in G$ olemassaolosta:

$$x = ex,$$

symmetrisyys käänteisalkion olemassaolosta:

$$y = \alpha x \;\Rightarrow\; x = \alpha^{-1}y$$

ja transitiivisuus ryhmän laskutoimituksesta:

$$y = \alpha x,\; z = \beta y \;\Rightarrow\; z = (\beta\alpha)x.$$

$\square$

Alkion $x \in E$ ekvivalenssiluokka relaatiossa R on

$$Gx = \{\alpha x \mid \alpha \in G\},$$

ja sitä sanotaan x:n *radaksi* G:n toiminnassa. Tekijäjoukko E/R, jonka siis muodostavat kaikki radat, merkitään tavallisesti

$$E/G,$$

tai myös $G\backslash E$, kun G toimii vasemmalta ja merkintä E/G halutaan varata tapaukseen, jossa G toimii oikealta.

Esimerkkejä. 8) G-joukon E alkion x rata on $\{x\}$, jos ja vain jos G kiinnittää x:n (esim. 1.4.7). Muulloin radassa on ainakin kaksi alkiota.

9) Olkoon G kunnan $\mathbf{R}$ multiplikatiivinen ryhmä

$$\mathbf{R}^* = \mathbf{R} \setminus \{0\}.$$

Ryhmä $\mathbf{R}^*$ toimii jokaisessa reaalisessa vektoriavaruudessa E (esim. 1.4.2) ja sen radat ovat

i) $\mathbf{R}^*.0 = \{0\}$ (erikoistapaus) ja

ii) $\mathbf{R}^*.x$ $(x \neq 0)$ eli suora $\mathbf{R}x \subset E$ origoa lukuunottamatta.

Tekijäjoukko $(E \setminus \{0\})/\mathbf{R}^*$ on ns. *projektiivinen avaruus* $\mathbf{P}E$.

Esimerkki 10) Jokaiseen ryhmän G alkioon x liittyy kuvaus

$$f_x \colon G \to G, \quad y \mapsto xyx^{-1},$$

ns. *konjugointi* alkiolla x. Kuvaus $x \mapsto f_x$ on G:n toiminta joukossa G. Alkioita xyx^{-1} $(x \in G)$ sanotaan alkion $y \in G$ *konjugaateiksi* ja niiden joukko, eli alkion y rata, on y:n *konjugaattiluokka* ryhmässä G:

$$\{xyx^{-1} \mid x \in G\}.$$

Esimerkki 11) Jokainen ryhmän G aliryhmä H toimii G:ssä sekä vasemmalta että oikealta, toimintana ryhmän laskutoimitus. Radat ovat oikeat ja vasemmat *sivuluokat*

$$Hx \text{ ja } xH \quad (x \in G),$$

ja tekijäjoukoille käytetään merkintöjä $H\backslash G$ ja G/H.

Homogeeniset joukot.

MÄÄRITELMÄ 1.4.6. Ryhmän G toiminta joukossa E on *transitiivinen*, jos E on jonkin alkionsa rata. Tällöin E on *homogeeninen G-joukko*.

Ehto merkitsee, että E on epätyhjä ja että jokaista sen alkioparia (x, y) kohti on olemassa sellainen $\alpha \in G$, että $y = \alpha x$.

Esimerkkejä. 12) Jos E on G-joukko, niin jokainen rata $Gx \subset E$ $(x \in E)$ on homogeeninen G-joukko.

13) Olkoon E vektoriavaruus $\mathbf{R}^3$ ja $G = O_3(\mathbf{R})$ sen ortogonaalisten muunnosten muodostama ryhmä. Tällöin yksikköpallon pinta $S^2 \subset \mathbf{R}^3$ ja muutkin origokeskiset pallopinnat ovat homogeenisia G-joukkoja.

14) Jos H on ryhmän G aliryhmä, niin G toimii transitiivisesti vasemmalta vasempien sivuluokkien joukossa G/H:

$$G \times G/H \to G/H, \quad (g, xH) \mapsto gxH.$$

Samoin G toimii transitiivisesti oikealta joukossa $H\backslash G$:

$$(Hx, g) \mapsto Hxg.$$

Olkoon G ryhmä, E homogeeninen G-joukko ja a sen alkio. Kuvaus

$$g\colon G \to E, \quad x \mapsto xa,$$

on tällöin surjektiivinen. Tarkastellaan siihen liittyvää ekvivalenssirelaatiota R alkioiden x, $y \in G$ välillä:

$$g(x) = g(y) \;\Leftrightarrow\; xa = ya \;\Leftrightarrow\; a = x^{-1}ya.$$

Relaatio R on siis sama kuin

$$x^{-1}y \in H,$$

missä

$$H = G_a = \{x \in G \mid xa = a\}$$

on alkion a kiinnittäjä. Sen ekvivalenssiluokat ovat vasemmat sivuluokat xH $(x \in G)$, ja niiden joukko on (esim. 1.4.11)

$$G/R = G/H.$$

Kuvauksen g kanoninen hajotelma on siten

$$\begin{tikzcd} G \arrow[rr, "g"] \arrow[dr, "p"'] & & E \\ & G/H \arrow[ur, "f"'] & \end{tikzcd},$$

missä $f\colon G/R \to g(G) = E$ on bijektiivinen.

Lause 1.4.7. *Olkoon G ryhmä, E homogeeninen G-joukko, a joukon E alkio ja H sen kiinnittäjä. Tällöin on olemassa yksikäsitteinen G-joukkojen isomorfismi*

$$f\colon G/H \to E,$$

joka toteuttaa ehdon $f(H) = a$.

Todistus. Joukon G/H alkiot ovat sivuluokat xH $(x \in G)$. Jos $f\colon G/H \to E$ on G-morfismi ja $f(H) = a$, niin

$$f(xH) = f(x.H) = xf(H) = xa.$$

Kuvaus f on siis välttämättä yksikäsitteinen.

Toisaalta yllä on nähty, että kuvauksen $g\colon G \to E$, $x \mapsto xa$, kanonisesta hajotelmasta saadaan bijektiivinen kuvaus $f\colon G/H \to E$, joka kaikilla $x \in G$ täyttää ehdon

$$f(xH) = xa.$$

Kuvaus f on lisäksi G-morfismi, koska kaikilla x, $y \in G$ pätee

$$f(x.yH) = xya = xf(yH),$$

ja se on siten G-joukkojen isomorfismi. $\square$

Esimerkki 15) Homogeenisessa G-joukossa E on vain yksi alkio a, kun G kiinnittää a:n (esim. 1.4.7). Toisaalta tämä merkitsee, että a:n kiinnittäjä H on koko ryhmä G, ja siten myös tekijäjoukossa $G/H = G/G$ on vain yksi alkio.

KOROLLAARI 1.4.8. *Olkoon G ryhmä ja E homogeeninen G-joukko. Jos G on äärellinen, niin E on äärellinen ja sen alkioiden lukumäärä on*

$$\mathrm{Card}(E) = (G : H) = \mathrm{Card}(G)/\mathrm{Card}(H),$$

missä H on jonkin E:n alkion kiinnittäjä.

Todistus. Lauseen 1.4.7 nojalla homogeenisella joukolla E on sama mahtavuus kuin sivuluokkien joukolla G/H. Koska jokaisessa sivuluokassa xH $(x \in G)$ on yhtä monta alkiota kuin H:ssa, sivuluokkien lukumäärä, eli aliryhmän H *indeksi* G:ssä, on

$$(G : H) = \mathrm{Card}(G)/\mathrm{Card}(H),$$

kun G on äärellinen (Lagrangen lause). $\square$

Esimerkki 16) Olkoon $G = \mathfrak{S}_n$ joukon $E = \{1, 2, \ldots, n\}$ symmetrinen ryhmä (esim. 1.3.1). Se toimii transitiivisesti joukossa E, joka on siten homogeeninen G-joukko. Alkion $n \in E$ kiinnittäjän $H = G_n$ muodostavat kaikki E:n osajoukon $\{1, 2, \ldots, n-1\}$ permutaatiot. Se voidaan siten samastaa symmetrisen ryhmän $\mathfrak{S}_{n-1}$ kanssa.

Korollaarin nojalla pätee silloin

$$\frac{\mathrm{Card}(\mathfrak{S}_n)}{\mathrm{Card}(\mathfrak{S}_{n-1})} = \mathrm{Card}(E) = n\,,$$

josta rekursiivisesti seuraa

$$\mathrm{Card}(\mathfrak{S}_n) = n!\,.$$

KOROLLAARI 1.4.9. *Olkoon G ryhmä ja E äärellinen G-joukko. Jos F on E:n* ratojen edustajisto *eli osajoukko, joka sisältää yhden alkion jokaisesta radasta, niin*

$$\mathrm{Card}(E) = \sum_{x \in F} (G : G_x)$$

tai yhtäpitävästi

$$\mathrm{Card}(E) = \mathrm{Card}(E^G) + \sum_{x \in F \setminus E^G} (G : G_x)\,.$$

Todistus. Kun F on ratojen edustajisto, E on erillinen yhdiste radoista Gx ($x \in F$), ja ensimmäinen yhtälö seuraa, koska lauseen 1.4.7 nojalla

$$\mathrm{Card}(Gx) = \mathrm{Card}(G/G_x) = (G : G_x)\,.$$

Toinen saadaan, kun summasta erotetaan ne termit, joissa $G_x = G$ eli x kuuluu joukkoon E^G (esim. 1.4.7). □

Esimerkki 17) Kun ryhmää G tarkastellaan G-joukkona konjugoinnilla varustettuna (esim. 1.4.10), sen alkion a kiinnittäjän määrittelee ehto

$$xax^{-1} = a$$

eli yhtäpitävästi $xa = ax$, ts. a ja x kommutoivat. Kiinnittäjä on siten sama kuin alkion a *keskittäjä* ryhmässä G

$$C_G(a) = \{x \in G \mid xa = ax\}\,,$$

ja se on koko G, jos ja vain jos a kuuluu ryhmän G *keskukseen*

$$Z = \{x \in G \mid xy = yx \text{ kaikilla } y \in G\}\,.$$

Keskus on G:n alkioiden keskittäjien leikkauksena aliryhmä ja se on triviaalisti normaali.

Kun G on äärellinen ryhmä ja C on jokin sen konjugaattiluokkien edustajisto, saadaan korollaarista 1.4.9 ryhmän G *luokkayhtälö*

$$\mathrm{Card}(G) = \mathrm{Card}(Z) + \sum_{x \in C \setminus Z} (G : C_G(x))\,.$$

Harjoitustehtäviä

1) Todistettava *Cayleyn lause*: Jokainen ryhmä on isomorfinen jonkin permutaatioryhmän eli symmetrisen ryhmän aliryhmän kanssa. (Tarkastellaan kuvausta $x \mapsto \gamma_x$, missä γ_x on siirto x:llä vasemmalta ryhmässä.) Mikä olisi vastaava tulos monoideilla?

2) Olkoon G ryhmä ja $f_x(y) = xyx^{-1}$ kaikilla $x, y \in G$. Osoitettava, että f_x on G:n automorfismi, ns. *sisäinen automorfismi*, kaikilla $x \in G$, ja että $x \mapsto f_x$ on G:n toiminta G:ssä, ns. *konjugointi*.

3) Olkoon G ryhmä. Osoitettava:
i) Kuvaus $\alpha \mapsto \alpha^{-1}$ on G:n isomorfismi vastaryhmälleen.
ii) Jos $(x, \alpha) \mapsto x\alpha$ on G:n toiminta oikealta joukossa E, niin $(\alpha, x) \mapsto \alpha x = x\alpha^{-1}$ on G:n toiminta vasemmalta E:ssä.

4) Olkoon G ryhmä ja H sen aliryhmä. Osoitettava, että tekijäjoukoilla G/H ja $H\backslash G$ on sama mahtavuus, H:n *indeksi* $(G : H)$, ja että H on G:n normaali aliryhmä, jos sen indeksi on 2. (G:n toiminta $H\backslash G$:ssä voidaan muuttaa vasemmalle teht. 3 avulla.)

5) Olkoon G ryhmä, E G-joukko ja F joukko. Kaikilla $\alpha \in G$ ja kuvauksilla $f\colon E \to F$ olkoon $f\alpha\colon E \to F$ kuvaus $x \mapsto f(\alpha x)$ ja $\alpha f\colon E \to F$ kuvaus $x \mapsto f(\alpha^{-1}x)$. Osoitettava, että $(f, \alpha) \mapsto f\alpha$ on G:n toiminta oikealta ja $(\alpha, f) \mapsto \alpha f$ G:n toiminta vasemmalta kuvausten $f\colon E \to F$ joukossa F^E.

1.5. Ratkeavat ja nilpotentit ryhmät

Tässä pykälässä tarkastellaan ryhmien rakennetta ja erityisesti sellaisia ominaisuuksia, joilla on merkittävä rooli algebrallisten yhtälöiden teoriassa.

MÄÄRITELMÄ 1.5.1. Ryhmän G *kompositiojono* on äärellinen jono $(G_i)_{0 \le i \le n}$ G:n aliryhmiä, missä $G_0 = G$, $G_n = \{e\}$ ja G_{i+1} on G_i:n normaali aliryhmä, kun $0 \le i \le n-1$.

Tekijäryhmät G_i/G_{i+1} ovat tällöin kompositiojonon *tekijät*.

Kompositiojonon tekijät ovat yksinkertaisempia kuin koko ryhmä, ja ne selvittävät ainakin osittain ryhmän rakennetta. Epäisomorfisilla ryhmillä voi kuitenkin olla kompositiojonoja, joiden tekijät ovat isomorfiset.

Esimerkkejä. 1) Olkoot H, H' ryhmiä ja olkoon $G = H \times H'$ tuloryhmä. Tällöin $G_1 = \{e\} \times H'$ on kanonisen projektiohomomorfismin $\mathrm{pr}_1\colon H \times H' \to H$ ytimenä G:n normaali aliryhmä. Jos asetetaan $G_2 = \{e\} \times \{e\}$, saadaan kompositiojono

$$G \supset G_1 \supset G_2,$$

jonka tekijät ovat $G/G_1 \cong H$ ja $G_1/G_2 \cong H'$.

2) Jos H on G:n normaali aliryhmä, niin $G \supset H \supset \{e\}$ on kompositiojono ja sen tekijät ovat G/H ja H.

Yleensä G ei ole isomorfinen tuloryhmän $(G/H) \times H$ kanssa, eli H ei ole G:n *suora tekijä*.

3) Olkoon G symmetrinen ryhmä $\mathfrak{S}_3$ ja H parillisten permutaatioiden Id, $(1\,2\,3)$ ja $(1\,2\,3)^2 = (1\,3\,2)$ muodostama alternoiva ryhmä $\mathfrak{A}_3$, joka on G:n normaali aliryhmä (ks. esim 1.3.1). Tällöin $G/H = \mathfrak{S}_3/\mathfrak{A}_3 \cong \mathbf{Z}/2\mathbf{Z}$ ja $H \cong \mathbf{Z}/3\mathbf{Z}$, mutta $\mathfrak{S}_3$ ei voi olla isomorfinen tulon

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$$

kanssa, koska tämä on vaihdannainen mutta $\mathfrak{S}_3$ ei ole.

Tarkastellaan seuraavaksi ryhmiä, joiden kompositiojonojen ainoa epätriviaali tekijä on koko ryhmä.

MÄÄRITELMÄ 1.5.2. Ryhmä G on *yksinkertainen*, jos se ei ole triviaali ryhmä $\{e\}$, mutta sen ainoat normaalit aliryhmät ovat G ja $\{e\}$.

Esimerkki 4) Jos p on alkuluku, niin syklinen ryhmä $G = \mathbf{Z}/p\mathbf{Z}$ on yksinkertainen, sillä aliryhmän kertaluvun täytyy olla p:n tekijä eli joko p tai 1.

Huomautus. Yleisesti nähdään (harj. teht.), että seuraavat ehdot ryhmälle G ovat yhtäpitävät.

a) $G \neq \{e\}$ ja sen ainoat aliryhmät ovat G ja $\{e\}$;
b) $G \cong \mathbf{Z}/p\mathbf{Z}$, missä p on alkuluku;
c) $\mathrm{Card}(G)$ on alkuluku;
d) G on yksinkertainen ja vaihdannainen.

Esimerkki 5) Alternoiva ryhmä $\mathfrak{A}_n$ on yksinkertainen, kun $n \geq 5$ (ks. esim. Hungerford, s. 49, tai Lang (3. p.), s. 32). Samoin $\mathfrak{A}_3 \cong \mathbf{Z}/3\mathbf{Z}$ on yksinkertainen. Sen sijaan $\mathfrak{A}_4$ ei ole yksinkertainen, koska sillä on epätriviaali normaali aliryhmä

$$H = \{s \in \mathfrak{A}_4 \mid s^2 = e\} = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

(Jos $s^2 = e$, niin myös $(tst^{-1})^2 = tst^{-1}tst^{-1} = e$ kaikilla $t \in \mathfrak{A}_4$.)

Jordanin-Hölderin lause. Jokainen kompositiojonon ryhmä on edellisen ryhmän normaali aliryhmä. Sen ei kuitenkaan tarvitse olla tätä edeltävän ryhmän normaali aliryhmä. Tämä merkitsee, että kompositiojonon osajono ei aina ole kompositiojono.

Toisaalta on kuitenkin mahdollista, että kompositiojono on laajemman kompositiojonon osajono. Tässä pykälässä tarkastellaan sellaisia kompositiojonoja, joita ei voi oleellisesti laajentaa.

MÄÄRITELMÄ 1.5.3. Ryhmän G kompositiojono on *Jordanin-Hölderin jono*, jos se on aidosti aleneva eikä ole minkään muun aidosti alenevan kompositiojonon osajono.

Seuraava tulos esittää vaihtoehtoisen tavan luonnehtia Jordanin-Hölderin jonot.

LAUSE 1.5.4. *Ryhmän G kompositiojono on Jordanin-Hölderin jono, jos ja vain jos sen tekijät ovat yksinkertaisia.*

Todistus. Olkoon $(G_i)_{0\leq i\leq n}$ jokin G:n kompositiojono. Jos jokin sen tekijä G_i/G_{i+1} ei ole yksinkertainen, niin sillä on epätriviaali normaali aliryhmä H'. Tämä voidaan esittää tekijäryhmänä

$$H' = H/G_{i+1},$$

missä H on G_i:n aliryhmä, joka sisältää G_{i+1}:n.

Tällöin H on G_i:n normaali aliryhmä, koska H' on normaali tekijäryhmässä G_i/G_{i+1}, ja G_{i+1} on puolestaan normaali H:ssa, koska se on normaali suuremmassa ryhmässä G_i. Jonoa $(G_i)_{0\leq i\leq n}$ voidaan silloin laajentaa asettamalla H ryhmien G_i ja G_{i+1} väliin, joten se ei ole Jordanin-Hölderin jono.

Kääntäen, jos jono ei ole Jordanin-Hölderin jono, niin jossakin laajemmassa kompositiojonossa on jonkin ryhmän G_i normaali aliryhmä H, joka sisältää aidosti ryhmän G_{i+1}. Tällöin tekijällä G_i/G_{i+1} on epätriviaali normaali aliryhmä H/G_{i+1}, joten se ei ole yksinkertainen. $\square$

Esimerkki 6) Kompositiojono $\mathfrak{S}_n \supset \mathfrak{A}_n \supset \{e\}$ on Jordanin-Hölderin jono, kun $n = 3$ tai $n \geq 5$, koska tällöin sen tekijät $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbf{Z}/2\mathbf{Z}$ ja $\mathfrak{A}_n$ ovat yksinkertaiset (ks. esim. 1.5.5).

Lauseen nojalla jokaisen Jordanin-Hölderin jonon viimeistä edellinen jäsen on yksinkertainen ryhmä, koska se on samalla jonon tekijä. Jos ryhmällä on Jordanin-Hölderin jono, niin sillä on ainakin yksi yksinkertainen aliryhmä. Esimerkiksi $\mathbf{Z}$ on ryhmä, jolla tällaista ei ole, eikä sillä siten ole Jordanin-Hölderin jonoa. (Jokainen epätriviaali aliryhmä on isomorfinen $\mathbf{Z}$:n kanssa.)

Jokaisella äärellisellä ryhmällä on kuitenkin Jordanin-Hölderin jono. Aidosti alenevan kompositiojonon pituus ei näet voi ylittää ryhmän mahtavuutta. Jokainen tällainen jono, jonka pituus on maksimaalinen, on siten Jordanin-Hölderin jono.

Jos ryhmällä on Jordanin-Hölderin jono, niitä voi olla useita. Kaikilla on kuitenkin oleellisesti samat tekijät.

Esimerkki 7) Ryhmällä $G = \mathbf{Z}/6\mathbf{Z}$ on kaksi Jordanin-Hölderin jonoa

$$\mathbf{Z}/6\mathbf{Z} \supset 2\mathbf{Z}/6\mathbf{Z} \supset \{0\}$$

ja

$$\mathbf{Z}/6\mathbf{Z} \supset 3\mathbf{Z}/6\mathbf{Z} \supset \{0\},$$

joiden tekijät ovat isomorfiset ryhmien $\mathbf{Z}/2\mathbf{Z}$ ja $\mathbf{Z}/3\mathbf{Z}$ kanssa.

Lause 1.5.5 (Jordan-Hölder). *Ryhmän kahden eri Jordanin-Hölderin jonon tekijät ovat parittain isomorfiset jossakin järjestyksessä.*

Todistus sivuutetaan. (Ei vaikea, mutta ei aivan lyhyt; ks. esim. Hungerford, s. 111, tai Lang (3. p.), s. 22.)

Ratkeavat ryhmät. Tarkastellaan nyt ryhmiä, joilla on kompositiojono, jonka tekijät eivät ole pelkästään yksinkertaisia vaan lisäksi vaihdannaisia (ks. esim. 1.5.4 ja sen jälkeistä huomautusta).

Määritelmä 1.5.6. Äärellinen ryhmä G on *ratkeava*, jos sillä on kompositiojono, jonka tekijät ovat syklisiä ja niiden kertaluvut ovat alkulukuja.

Ehdon toteuttava kompositiojono on siis Jordanin-Hölderin jono, koska tekijät ovat yksinkertaisia (lause 1.5.4), ja kaikilla Jordanin-Hölderin jonoilla on sama ominaisuus (lause 1.5.5).

Huomautus. On riittävää, että ryhmällä on kompositiojono, jonka tekijät ovat äärellisiä syklisiä (tai yleisemmin vaihdannaisia) ryhmiä, sillä tällainen jono voidaan täydentää Jordanin-Hölderin jonoksi, jolla on vaadittu ominaisuus.

Esimerkkejä. 8) Ryhmät $\mathfrak{S}_3$, $\mathfrak{S}_4$ ja $\mathfrak{A}_4$ ovat ratkeavia. Niillä on kompositiojonot, joiden tekijäin kertaluvut ovat 2 tai 3:

$$\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{e\}$$

ja

$$\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset H \supset H' \supset \{e\},$$

missä (ks. esim. 1.5.5)

$$H = \{s \in \mathfrak{A}_4 \mid s^2 = e\}$$

ja

$$H' = \{e, (1\,2)(3\,4)\}.$$

9) Ryhmät $\mathfrak{S}_n$ ja $\mathfrak{A}_n$ eivät ole ratkeavia, kun $n \geq 5$. Tämä seuraa esimerkiksi siitä, että

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \{e\}$$

on Jordanin-Hölderin jono, jossa tekijät eivät ole syklisiä (ks. esim. 1.5.6). Myös suora todistus on mahdollinen.

Todistus. Olkoon $(G_i)_{0 \leq i \leq n}$ kompositiojono, jossa G_0 on $\mathfrak{S}_n$ tai $\mathfrak{A}_n$ ja jokainen tekijä G_i/G_{i+1} $(0 \leq i \leq n-1)$ on vaihdannainen.

Jokainen 3-sykli $(i\,j\,k)$ $(i, j, k \in \{1, \ldots, n\})$ on parillinen, joten se on G_0:ssä. Olkoon d suurin indeksi, jolla G_d sisältää kaikki 3-syklit. Osoitetaan, että tällöin $(i\,j\,k) \in G_{d+1}$.

Koska $n \geq 5$, välillä $\{1, \ldots, n\}$ on lukujen i, j, k lisäksi ainakin kaksi lukua p ja q. Tällöin 3-syklit $s = (i\,j\,p)$ ja $t = (i\,k\,q)$ ovat G_d:ssä, ja suoraan laskemalla saadaan yhtälö

$$r = (i\,j\,k) = sts^{-1}t^{-1}.$$

Jos $\bar{r}$, $\bar{s}$ ja $\bar{t}$ ovat syklien r, s ja t luokat tekijäryhmässä G_d/G_{d+1}, niin

$$\bar{r} = \bar{s}\bar{t}\bar{s}^{-1}\bar{t}^{-1} = \bar{e}$$

kun G_d/G_{d+1} on vaihdannainen. Tämä merkitsee, että $r = (i\,j\,k)$ on aliryhmässä G_{d+1}.

Mutta sama todistus pätee jokaisella 3-syklillä, joten ne kaikki ovat aliryhmässä G_{d+1}. Tämä on ristiriidassa luvun d maksimaalisuuden kanssa. Siis kompositiojonoa, jossa tekijät olisivat vaihdannaisia, ei voi olla olemassa, ja siten $\mathfrak{S}_n$ ja $\mathfrak{A}_n$ eivät ole ratkeavia. □

Esimerkkejä. 10) Jokainen äärellinen vaihdannainen ryhmä on ratkeava, sillä tällaisella ryhmällä on Jordanin-Hölderin jono $(G_i)_{0 \leq i \leq n}$, missä jokainen G_i on vaihdannainen. Tällöin tekijät G_i/G_{i+1} ovat yksinkertaisia (lause 1.5.4) ja myös vaihdannaisia, joten ne ovat syklisiä ja niiden kertaluvut ovat alkulukuja (ks. esim. 1.5.4, huom.).

11) Kaikki äärelliset ryhmät, joiden kertaluku on pariton, ovat ratkeavia (Feit, W. - Thompson, J.G.: Solvability of groups of odd order, Pacific J. Math. 13, 1963, 775-1029).

Huomautus. Tulos voidaan myös esittää seuraavissa yhtäpitävissä muodoissa.

i) Ainoat yksinkertaiset ryhmät, joiden kertaluku on pariton, ovat sykliset ryhmät $\mathbf{Z}/p\mathbf{Z}$, missä p on alkuluku.

ii) Jos äärellinen yksinkertainen ryhmä ei ole vaihdannainen, niin sen kertaluku on parillinen.

Seuraavassa lauseessa esitetään eräitä ratkeavien ryhmien perusominaisuuksia.

Lause 1.5.7.

i) *Ratkeavan ryhmän aliryhmät ja tekijäryhmät ovat ratkeavia.*
ii) *Jos ryhmän normaali aliryhmä ja vastaava tekijäryhmä ovat ratkeavia, niin ryhmä on ratkeava.*

Todistus sivuutetaan. (Ei kovin hankala. Käsitellään harjoitustehtävissä.)

p-ryhmät. Olkoon p alkuluku.

Määritelmä 1.5.8. Äärellinen ryhmä, jonka kertaluku on p:n potenssi, on *p-ryhmä.*

Jokaisen p-ryhmän G kertaluvun tekijät ovat p:n potensseja. Siten G:n aliryhmät ja tekijäryhmät ovat myös p-ryhmiä. Yleisemmin G:n jokaisen aliryhmän indeksi ja jokaisen homogeenisen G-joukon mahtavuus (lause 1.4.7) on p:n potenssi.

Lause 1.5.9. *Jokainen p-ryhmä on ratkeava.*

Todistus. Olkoon G ryhmä, jonka kertaluku on p^r. Todistetaan G ratkeavaksi induktiolla r:n suhteen. Jos $r = 0$, väite on triviaalisti tosi. Siis voidaan olettaa, että $r > 0$ ja että jokainen p-ryhmä, jonka kertaluku on pienempi kuin p^r, on ratkeava

Jos G:n alkio x ei kuulu sen keskukseen Z, niin x:n keskittäjä $C_G(x)$ on G:n aito aliryhmä, ja indeksi $(G : C_G(x))$ on siten jaollinen p:llä. Luokkayhtälöstä (esim. 1.4.17) seuraa silloin

$$\operatorname{Card}(G) \equiv \operatorname{Card}(Z) \pmod p.$$

Koska $r > 0$, kummankin ryhmän G ja Z kertaluku on jaollinen p:llä. Erityisesti Z on G:n epätriviaali normaali aliryhmä ja siten tekijäryhmä G/Z on induktio-oletuksen mukaan ratkeava. Toisaalta Z on vaihdannaisena ryhmänä ratkeava (esim. 1.5.10). Ryhmä G on siis lauseen 1.5.7 nojalla ratkeava. □

Esimerkki 12) Jos p on alkuluku ja $r \in \mathbf{N}$, niin syklinen ryhmä $\mathbf{Z}/p^r\mathbf{Z}$ on p-ryhmä. Sillä on Jordanin-Hölderin jono

$$\mathbf{Z}/p^r\mathbf{Z} \supset p\mathbf{Z}/p^r\mathbf{Z} \supset p^2\mathbf{Z}/p^r\mathbf{Z} \supset \cdots \supset p^r\mathbf{Z}/p^r\mathbf{Z} = \{0\},$$

jonka jokainen tekijä on isomorfinen ryhmän $\mathbf{Z}/p\mathbf{Z}$ kanssa.

Sylowin aliryhmät. Olkoon G äärellinen ryhmä ja p alkuluku.

Määritelmä 1.5.10. Ryhmän G aliryhmä P on G:n *Sylowin p-aliryhmä*, kun se toteuttaa ehdot

i) P on p-ryhmä,
ii) indeksi $(G : P)$ ei ole jaollinen p:llä.

Esimerkki 13) Olkoon G symmetrinen ryhmä $\mathfrak{S}_p$. Sen jokainen p-sykli, esim. $(1\,2\,3\cdots p)$, virittää syklisen aliryhmän P, jonka kertaluku on p. Koska indeksi $(G:P)=(p-1)!$ ei ole jaollinen p:llä, P on G:n Sylowin p-aliryhmä.

Lisäksi jokainen p-sykli $(i_1\,i_2\,i_3\cdots i_p)$ voidaan kirjoittaa muotoon $\sigma(1\,2\,3\cdots p)\sigma^{-1}$, missä $\sigma\colon k\mapsto i_k$. Siten sen virittämä Sylowin aliryhmä on ryhmän P konjugaatti $\sigma P\sigma^{-1}$.

Lause 1.5.11 (Sylow). *Jokaisella äärellisellä ryhmällä G on Sylowin p-aliryhmä G_p.*

Todistus. Ryhmän G kertaluku olkoon $n=p^r m$, missä $p\nmid m$. Tarkastellaan joukkoa E, jonka muodostavat G:n p^r-alkioiset osajoukot. Se on G-joukko, toimintanaan $(g,X)\mapsto gX$.

Joukon E mahtavuus

$$\mathrm{Card}(E)=\binom{n}{p^r}=\frac{n(n-1)\cdots(n-p^r+1)}{1\cdot 2\cdots p^r}$$

ei ole jaollinen p:llä, koska i ja $(p^r m-i)$ ovat jaolliset samoilla p:n potensseilla, kun $1\le i\le p^r-1$. Silloin on olemassa E:n alkio X, jonka radan alkioiden lukumäärä $(G:G_X)$ (lause 1.4.7) ei ole jaollinen p:llä, ja siten aliryhmän G_X kertaluku on potenssin p^r kerrannainen.

Toisaalta G_X:n kertaluku ei voi olla suurempi kuin $\mathrm{Card}(X)=p^r$. Jos näet x on jokin X:n alkio, niin $gx\in gX=X$, kun $g\in G_X$, joten $g\mapsto gx$ on injektiivinen kuvaus $G_X\to X$. Kiinnittäjän G_X mahtavuus on siis p^r, ja se on siten G:n Sylowin p-aliryhmä. □

Huomautus. Joukko X on eräs ryhmän G_X oikea sivuluokka $G_X x$.

Lause 1.5.12. *Olkoon G äärellinen ryhmä.*

i) *Ryhmän G Sylowin p-aliryhmät ovat toistensa konjugaatteja.*
ii) *Jokainen G:n aliryhmä, joka on p-ryhmä, sisältyy johonkin G:n Sylowin p-aliryhmään.*

Todistus. Olkoon P jokin G:n Sylowin p-aliryhmä. Jos H on G:n aliryhmä, niin homogeeninen G-joukko $E=G/P$ on myös H-joukko. Jos H on lisäksi p-ryhmä, niin korollaarin 1.4.9 nojalla

$$\mathrm{Card}(E)\equiv\mathrm{Card}(E^H)\pmod{p}.$$

Koska $\mathrm{Card}(E)=(G:P)$ ei ole jaollinen p:llä, E^H ei voi olla tyhjä. Olkoon $x=gP$ jokin sen alkio. Ehdosta $hx=x$ kaikilla $h\in H$ seuraa silloin $HgP=gP$. Siten $Hg\subset gP$, eli H sisältyy P:n konjugaattiin gPg^{-1}, joka on myös G:n Sylowin p-aliryhmä.

Jos H on Sylowin p-aliryhmä, niin se on sama kuin gPg^{-1}, koska kummankin alkioiden lukumäärä on korkein p:n potenssi, joka jakaa G:n kertaluvun. □

Nilpotentit ryhmät. Osoitettaessa p-ryhmiä ratkeaviksi (lause 1.5.9) nähtiin, että epätriviaalin p-ryhmän G keskus ei supistu yksin neutraalialkioksi. Koska keskus $Z = G^1$ on normaali aliryhmä, voidaan muodostaa tekijäryhmä G/G^1, joka on myös p-ryhmä. Tämän keskus on puolestaan G^2/G^1, missä G^2 on G:n normaali aliryhmä. Näin jatkaen saadaan ryhmän G kompositiojono $(G_i)_{0 \leq i \leq n}$, missä jokainen $G_i = G^{n-i}$ on G:n normaali aliryhmä ja G_{i-1}/G_i on G/G_i:n keskus, kun $1 \leq i \leq n$.

Tässä kappaleessa tarkastellaan ryhmiä, joilla on saman tyyppinen kompositiojono. Ne ovat kaikki ratkeavia, koska jonon tekijät ovat vaihdannaisia.

LAUSE 1.5.13. *Olkoon G äärellinen ryhmä. Seuraavat ehdot ovat yhtäpitävät:*

a) *G:llä on kompositiojono $(G_i)_{0 \leq i \leq n}$, missä jokainen G_i on G:n normaali aliryhmä ja G_{i-1}/G_i sisältyy G/G_i:n keskukseen, kun $1 \leq i \leq n$.*
b) *G:n Sylowin p-aliryhmät ovat normaaleja aliryhmiä.*
c) *G on isomorfinen p-ryhmien tulon kanssa.*

Todistus. a) $\Rightarrow$ b): Olkoon p alkuluku ja P G:n Sylowin p-aliryhmä. Kun $(G_i)_{0 \leq i \leq n}$ on G:n kompositiojono, missä jokainen G_i on normaali aliryhmä, tulot G_iP ovat G:n aliryhmiä (lause 1.3.9). Lisäksi P on myös G_iP:n Sylowin p-aliryhmä, koska $(G_iP : P)$ on indeksin $(G : P)$ tekijä eikä siten ole jaollinen p:llä.

Olkoon G_i sellainen, että P on G_iP:n normaali aliryhmä; esim. $i = n$, jolloin $G_iP = P$. Osoitetaan, että P on myös ryhmän $G_{i-1}P$ normaali aliryhmä, jos $i > 0$ ja G_{i-1}/G_i sisältyy ryhmän G/G_i keskukseen.

Olkoot $s \in G_{i-1}$ ja $x \in P$. Niiden luokat $\bar{s}$, $\bar{x} \in G/G_i$ toteuttavat ehdon $\bar{s}\bar{x} = \bar{x}\bar{s}$, kun $\bar{s}$ on G/G_i:n keskuksessa. Tällöin $sx = txs$ jollakin $t \in G_i$, ja siten $sxs^{-1} = tx \in G_iP$. Sylowin aliryhmän P konjugaatti sPs^{-1} (ryhmässä $G_{i-1}P$) sisältyy siis aliryhmään G_iP, ja silloin se on myös tämän Sylowin p-aliryhmä.

Toisaalta jokainen G_iP:n Sylowin p-aliryhmä on P:n konjugaatti ryhmässä G_iP (lause 1.5.12). Koska P on oletettu tämän normaaliksi aliryhmäksi, täytyy siis olla $sPs^{-1} = P$ (siinäkin tapauksessa, että $s \notin G_i$). Tästä seuraa, että P on $G_{i-1}P$:n normaali aliryhmä, koska $(sx)P(sx)^{-1} = sxPx^{-1}s^{-1} = sPs^{-1}$ kaikilla $x \in P$.

Alenevalla induktiolla voidaan nyt päätellä, että P on ryhmän $G = G_0P$ normaali aliryhmä, kun kohdan a) ehdot ovat voimassa.

b) $\Rightarrow$ c): Olkoon I luvun $\mathrm{Card}(G)$ alkutekijöiden joukko, ja jokaista $p \in I$ kohti olkoon P_p jokin G:n Sylowin p-aliryhmä. Tällöin $\mathrm{Card}(P_p) = p^{\nu(p)}$ jollakin $\nu(p) > 0$, ja $\mathrm{Card}(G) = \prod_{p \in I} p^{\nu(p)}$. Oletetaan, että ryhmät P_p ovat G:n normaaleja aliryhmiä.

Olkoot p, $q \in I$, $p \neq q$, sekä $x \in P_p$ ja $y \in P_q$. Tarkastellaan G:n alkiota $t = xyx^{-1}y^{-1}$. Koska $x^{-1} \in P_p$, myös $yx^{-1}y^{-1} \in P_p$, kun P_p on normaali aliryhmä, ja siten $t = x(yx^{-1}y^{-1}) \in P_p$. Samalla tavoin nähdään, että $t = (xyx^{-1})y^{-1} \in P_q$. Koska $P_p \cap P_q$ on sekä p- että q-ryhmä, se supistuu neutraalialkioksi; siis $t = e$, eli $xy = yx$.

Olkoon $(x_p) \in \prod_{p \in I} P_p$. Koska alkiot x_p kommutoivat keskenään, tulo $\prod_{p \in I} x_p$ on hyvin määritelty ja kuvaus

$$\varphi\colon \prod_{p \in I} P_p \to G, \quad (x_p) \mapsto \prod_{p \in I} x_p,$$

on homomorfismi. Sen kuva sisältää ryhmät P_p, joten sen kertaluku on jaollinen luvuilla $p^{\nu(p)}$. Koska $\mathrm{Card}(G)$ on näiden pienin yhteinen kerrannainen, φ on surjektiivinen ja siksi isomorfismi.

c) $\Rightarrow$ a): Olkoon I äärellinen joukko alkulukulukuja, ja jokaista $p \in I$ kohti olkoon P_p jokin p-ryhmä. Osoitetaan induktiolla $\mathrm{Card}(I)$:n suhteen, että tuloryhmällä $G = \prod_{p \in I} P_p$ on kohdan a) ehdot täyttävä kompositiojono, mikä on ilmeistä, kun $I = \emptyset$.

Voidaan olettaa, että G on tulo $H \times P$, missä P on p-ryhmä ja H on ryhmä, jolla on kompositiojono $(H_i)_{0 \leq i \leq m}$, missä H_i on H:n normaali aliryhmä ja H_{i-1}/H_i sisältyy H/H_i:n keskukseen, kun $1 \leq i \leq m$. Toisaalta edellä on nähty, että p-ryhmällä P on kompositiojono $(P_j)_{1 \leq j \leq r}$, jolla on vastaavat ominaisuudet. Jos asetetaan $n = m+r$, $G_i = H_i \times P$, kun $0 \leq i \leq m$, ja $G_i = \{e\} \times P_{i-m}$, kun $m \leq i \leq n$, saadaan G:n kompositiojono, joka täyttää kohdan a) ehdot. $\square$

MÄÄRITELMÄ 1.5.14. Ryhmä G on *nilpotentti*, kun se täyttää lauseen 1.5.13 ehdon a).

Huomautus. Sanaa 'nilpotentti' käytetään yleisesti osoittamaan, että jokin laskutoimitus riittävän usein toistettuna johtaa triviaaliin tulokseen. Edellisen määritelmän kohdalla kysymyksessä ei kuitenkaan ole ryhmän varsinainen laskutoimitus vaan se, jonka tuloksena on alkioiden x ja y *kommutaattori* $(x, y) = xyx^{-1}y^{-1}$.

Jos ryhmällä G on kompositiojono $(G_i)_{0 \leq i \leq n}$, joka täyttää lauseen ehdon a), niin $(x, y) \in G_1$ kaikilla $x, y \in G$, koska G/G_1 on vaihdannainen. Samoin $(x, y) \in G_{i+1}$ aina kun $y \in G_i$, joten n-kertainen kommutaattori on $(x_0, (x_1, \dots, (x_{n-1}, x_n) \dots)) = e$ kaikilla x_0, x_1, ..., $x_n \in G$. Ei ole vaikeaa nähdä, että tämä ominaisuus on yhtäpitävä ehdon a) kanssa. (Esim. G_i voi olla i-kertaisten kommutaatoreiden virittämä aliryhmä.)

Harjoitustehtäviä

1) Olkoon G ryhmä. Osoitettava, että seuraavat ehdot ovat yhtäpitävät:

i) $G \neq \{e\}$, ja G:n ainoat aliryhmät ovat G ja $\{e\}$.

ii) $G \cong \mathbf{Z}/p\mathbf{Z}$, missä p on alkuluku.
iii) $\mathrm{Card}(G)$ on alkuluku.
iv) G on yksinkertainen ja vaihdannainen.

2) Olkoon $(G_i)_{0\le i\le n}$ ryhmän G kompositiojono, H G:n aliryhmä ja $H_i = H \cap G_i$, kun $0 \le i \le n$. Osoitettava, että $(H_i)_{0\le i\le n}$ on H:n kompositiojono, ja että H_i/H_{i+1} on isomorfinen ryhmän G_i/G_{i+1} aliryhmän kanssa, kun $0 \le i < n$ (1. isomorfialause). Pääteltävä, että H on ratkeava, jos G on ratkeava.

3) Olkoon $(G_i)_{0\le i\le n}$ ryhmän G kompositiojono, N G:n normaali aliryhmä, $H = G/N$ ja $H_i = G_iN/N$, kun $0 \le i \le n$. Osoitettava, että $(H_i)_{0\le i\le n}$ on H:n kompositiojono, ja että H_i/H_{i+1} on isomorfinen ryhmän G_i/G_{i+1} tekijäryhmän kanssa, kun $0 \le i < n$. ($H_i = p(G_i)$, kun $p\colon G \to H$ on kanoninen homomorfismi, ja yhdistetyn homomorfismin $G_i \to H_i \to H_i/H_{i+1}$ ydin sisältää G_{i+1}:n.) Pääteltävä, että H on ratkeava, jos G on ratkeava.

4) Olkoon G ryhmä ja N sen normaali aliryhmä. Osoitettava, että G on ratkeava, jos N ja G/N ovat ratkeavia. (Esitetään G/N:n kompositiojono muodossa $(G_i/N)_{0\le i\le n}$.)

1.6. Vapaat vaihdannaiset ryhmät ja monoidit

Olkoon M vaihdannainen monoidi, jonka laskutoimitus on merkitty yhteenlaskuksi, ja olkoon X jokin sen virittäjäjoukko. Lauseen 1.1.8 nojalla kaikki M:n alkiot voidaan esittää summina

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n,$$

missä $n \in \mathbf{N}$ ja $x_i \in X$ $(1 \le i \le n)$. (Erityisesti 0 saadaan, kun $n = 0$.) Alkioiden x_i järjestyksellä ei ole merkitystä, koska M on vaihdannainen, vain tiedot niiden lukumääristä tarvitaan.

Jos merkitään $\alpha(x)$:llä alkion $x \in X$ lukumäärää jonossa (x_i), eli

$$\alpha(x) = \mathrm{Card}\{i \mid 1 \le i \le n, x_i = x\} \in \mathbf{N},$$

niin vain äärellisen moni luvuista $\alpha(x)$ on nollasta eroava, ja saadaan esitys

$$\sum_{i=1}^{n} x_i = \sum_{x\in X} \alpha(x).x\ .$$

Jos M on ryhmä, ja X virittää sen ryhmänä, saadaan samanlainen esitys, jossa alkiot x_i ovat joko x tai $-x$ jollakin $x \in X$ (lause 1.3.3). Tällöin kertoimet $\alpha(x)$ määritellään alkioiden x ja $-x$ lukumäärien erotuksena, ja ne voivat saada myös negatiivisia kokonaislukuarvoja.

Yleensä monoidin (tai ryhmän) M alkioiden esitys kertoimien $\alpha(x)$ avulla ei ole yksikäsitteinen. Yhtälöitä

$$\sum_{x\in X} \alpha(x).x = \sum_{x\in X} \beta(x).x,$$

missä $\alpha \neq \beta$, sanotaan *relaatioiksi* virittäjien $x \in X$ välillä.

Jos relaatiota ei ole, niin sanotaan, että X on M:n *vapaa virittäjäjoukko* (l. *kantajoukko*). Tällöin jokaista M:n alkiota vastaa yksikäsitteinen kerroinfunktio α. Tästä huomiosta saadaan lähtökohta yleiselle konstruktiolle.

Konstruktio. Olkoon X joukko. Tarkastellaan kaikkien X:n kokonaislukuarvoisten funktioiden joukkoa

$$\mathbf{Z}^X = \{\alpha \mid \alpha\colon X \to \mathbf{Z}\}.$$

Yhteenlaskulla

$$(\alpha+\beta)(x) = \alpha(x) + \beta(x) \quad (\alpha, \beta \in \mathbf{Z}^X, x \in X)$$

varustettuna se on vaihdannainen ryhmä. (Itse asiassa $\mathbf{Z}^X$ on ryhmien $G_x = \mathbf{Z}$ $(x \in X)$ tulo. Funktiot α voidaan tulkita perheiksi $(\alpha(x))_{x\in X}$.)

Olkoon

$$S_\alpha = \{x \in X \mid \alpha(x) \neq 0\} \subset X$$

funktion (tai perheen) $\alpha \in \mathbf{Z}^X$ *kantaja*. Tällöin

$$\mathbf{Z}^{(X)} = \{\alpha \mid \alpha\colon X \to \mathbf{Z},\ S_\alpha \text{ on äärellinen}\}$$

on ryhmän $\mathbf{Z}^X$ aliryhmä. (Sama kuin ryhmien $G_x = \mathbf{Z}$ *rajoitettu tulo* eli *suora summa* $\bigoplus_{x\in X} G_x$.)

Virittäjät. Olkoon X joukko kuten edellä. Jokaista sen alkiota x vastaa *Kroneckerin funktio* $\delta_x \in \mathbf{Z}^{(X)}$, jonka määrittelevät ehdot

$$\delta_x(y) = \begin{cases} 1 & \text{, kun } y = x, \\ 0 & \text{, kun } y \neq x. \end{cases}$$

LEMMA 1.6.1. *Ryhmän $\mathbf{Z}^{(X)}$ kaikilla alkioilla α on esitys*

$$\alpha = \sum_{x\in X} \alpha(x).\delta_x\ .$$

Todistus. Yhtälön oikean puolen summa on hyvin määritelty, koska perheen $(\alpha(x))_{x\in X}$ kantaja S_α on äärellinen, ja sen arvo on äärellinen summa

$$\alpha' = \sum_{x\in S_\alpha} \alpha(x).\delta_x\ .$$

Kaikilla $y \in X$ pätee tällöin

$$\alpha'(y) = \sum_{x\in S_\alpha} \alpha(x).\delta_x(y) = \begin{cases} \alpha(y).1 & \text{, jos } y \in S_\alpha, \\ 0 & \text{, jos } y \notin S_\alpha, \end{cases}$$

eli α':n arvot ovat samat kuin α:n arvot. $\square$

Lemman nojalla Kroneckerin funktiot virittävät koko ryhmän $\mathbf{Z}^{(X)}$. Niiden välillä ei myöskään ole relaatioita, koska ehdosta

$$\sum_{x\in X}\alpha(x).\delta_x=\sum_{x\in X}\beta(x).\delta_x$$

seuraa välittömästi $\alpha=\beta$. Siis saadaan:

$$\{\delta_x \mid x\in X\} \text{ on ryhmän } \mathbf{Z}^{(X)} \text{ vapaa virittäjäjoukko.}$$

Usein samastetaan joukon X alkio x ja sitä vastaava Kroneckerin funktio δ_x, ja merkitään lyhyesti

$$\alpha=\sum_{x\in X}\alpha(x).x,$$

kun $\alpha\in\mathbf{Z}^{(X)}$. Tällaista esitystä sanotaan alkioiden $x\in X$ *muodolliseksi* $\mathbf{Z}$*-kertoimiseksi yhdistelmäksi*. Näin tulkittuna X on ryhmän $\mathbf{Z}^{(X)}$ vapaa virittäjäjoukko, ja sanotaan, että $\mathbf{Z}^{(X)}$ on joukon X virittämä *vapaa vaihdannainen ryhmä*.

Kun rajoitetaan funktioiden α arvot luonnollisiksi luvuiksi, saadaan $\mathbf{Z}^{(X)}$:n alimonoidi

$$\mathbf{N}^{(X)}=\{\alpha \mid \alpha\colon X\to\mathbf{N},\ S_\alpha \text{ on äärellinen}\},$$

jota sanotaan joukon X virittämäksi *vapaaksi vaihdannaiseksi monoidiksi*.

Universaaliominaisuus.

Lause 1.6.2. *Olkoon X joukko, M vaihdannainen monoidi (tai ryhmä) ja f kuvaus $X\to M$. Tällöin on olemassa yksi ja vain yksi monoidihomomorfismi $g\colon\mathbf{N}^{(X)}\to M$ (tai $g\colon\mathbf{Z}^{(X)}\to M$), joka kaikilla $x\in X$ täyttää ehdon*

$$g(\delta_x)=f(x).$$

Kun M on additiivinen,

$$g(\alpha)=\sum_{x\in X}\alpha(x).f(x)$$

kaikilla $\alpha\in\mathbf{N}^{(X)}$ (tai $\alpha\in\mathbf{Z}^{(X)}$).

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\text{kan}"'] & & M \\
& \mathbf{N}^{(X)} \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

Todistus. Olkoon $g\colon\mathbf{N}^{(X)}\to M$ monoidihomomorfismi. Jos $x\in X$, niin $g(n.\delta_x)=n.g(\delta_x)$ kaikilla $n\in\mathbf{N}$, kuten induktiolla nähdään. Jos g toteuttaa ehdon $g(\delta_x)=f(x)$, kun $x\in X$, ja $\alpha\in\mathbf{N}^{(X)}$, niin Lemman 1.6.1 nojalla saadaan

$$g(\alpha)=g(\sum_{x\in S_\alpha}\alpha(x).\delta_x)=\sum_{x\in S_\alpha}\alpha(x).g(\delta_x)=\sum_{x\in X}\alpha(x).f(x).$$

Sama pätee, kun M on ryhmä ja $\alpha\in\mathbf{Z}^{(X)}$, koska

$$g(n.\delta_x)=-g(-n.\delta_x)=-(-n).g(\delta_x),$$

jos $n \in \mathbf{Z}$, $n < 0$. Joka tapauksessa ehdon täyttävä g on yksikäsitteinen.

Määritellään nyt kuvaus $g\colon \mathbf{N}^{(X)} \to M$ kaavalla

$$g(\alpha) = \sum_{x \in X} \alpha(x).f(x).$$

Tällöin $g(0) = \sum_{x \in X} 0.f(x) = 0$ kuten monoidihomomorfismilta vaaditaan. Jos lisäksi α, $\beta \in \mathbf{N}^{(X)}$, niin

$$g(\alpha + \beta) = \sum_{x \in X} (\alpha(x) + \beta(x)).f(x) = \sum_{x \in X} (\alpha(x).f(x) + \beta(x).f(x))$$

potenssilain nojalla, ja koska M on vaihdannainen, tämä summa on sama kuin

$$\sum_{x \in X} \alpha(x).f(x) + \sum_{x \in X} \beta(x).f(x) = g(\alpha) + g(\beta).$$

Kuvaus $g\colon \mathbf{N}^{(X)} \to M$ on siis monoidihomomorfismi. Jos M on ryhmä, niin samoilla kaavoilla saadaan ryhmähomomorfismi $g\colon \mathbf{Z}^{(X)} \to M$.

Lopuksi, jos $y \in X$, niin

$$g(\delta_y) = \sum_{x \in X} \delta_y(x).f(x) = \delta_y(y).f(y) = f(y).$$

$\square$

Huomautus. Jos M:n laskutoimitus on merkitty kertolaskuna, niin on tarkoituksenmukaista tulkita kuvaus f alkioperheeksi $u = (u_x)_{x \in X}$. Tällöin ehdon $g(x) = u_x$ toteuttava homomorfismi g saadaan *eksponenttimerkintää* käyttävästä kaavasta

$$g(\alpha) = u^\alpha = \prod_{x \in X} u_x^{\alpha(x)}.$$

Harjoitustehtäviä

1) Olkoon $n \in \mathbf{N}$ ja $\mathbf{Z}^n$ joukon $X = \{1, 2, \ldots, n\}$ virittämä vapaa vaihdannainen ryhmä. Osoitettava, että $(\mathbf{Z}^n : 2\mathbf{Z}^n) = 2^n$. (Konstruoidaan surjektiivinen homomorfismi $\mathbf{Z}^n \to (\mathbf{Z}/2\mathbf{Z})^n$, jonka ydin on $2\mathbf{Z}^n$.) Pääteltävä, että $\mathbf{Z}^n$ ja $\mathbf{Z}^m$ $(n, m \in \mathbf{Z})$ ovat isomorfiset vain, jos $n = m$. Luku n on vapaan ryhmän $\mathbf{Z}^n$ *aste.*

2) Osoitettava, että jokainen vaihdannainen ryhmä on isomorfinen jonkin vapaan vaihdannaisen ryhmän tekijäryhmän kanssa.

1.7. Renkaat

MÄÄRITELMÄ 1.7.1. *Rengas* on joukko A varustettuna kahdella laskutoimituksella, yhteenlaskulla ja kertolaskulla, jotka toteuttavat seuraavat ehdot.

(R1) Yhteenlaskulla varustettuna A on vaihdannainen ryhmä.
(R2) Kertolasku on liitännäinen ja A:ssa on sen suhteen neutraalialkio.
(R3) Kertolasku on *ositteleva* l. *distributiivinen* yhteenlaskun suhteen, ts. kaikilla x, y, $z \in A$

$$(x+y).z = x.z + y.z, \quad x.(y+z) = x.y + x.z \ .$$

Rengas A on *vaihdannainen*, jos $xy = yx$ kaikilla x, $y \in A$. Yhteenlaskun ja kertolaskun neutraalialkioille käytetään tavallisesti merkintöjä 0 ja 1. (Yleensä $0 \neq 1$. Jos $0 = 1$, niin rengas on *nollarengas* $A = \{0\}$.)

Esimerkki 1) Olkoon G vaihdannainen (additiivinen) ryhmä ja olkoon

$$E = \mathrm{End}(G) = \{f \mid f\colon G \to G \text{ on homomorfismi}\}$$

sen endomorfismien joukko. Jos f, $g \in E$ ja määritellään kuvaukset $f+g$ ja fg asettamalla

$$(f+g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(g(x))$$

kaikilla $x \in X$, niin $f+g$ ja fg ovat myös G:n endomorfismeja. Tällöin E on rengas, vaihdannaisen ryhmän G *endomorfismirengas*. (Neutraalialkiot ovat $0\colon x \mapsto 0$ ja $1 = \mathrm{Id}_G$.)

Esimerkki 2) Jos $(A_i)_{i\in I}$ on rengasperhe, niin tulojoukko

$$A = \prod_{i\in I} A_i$$

varustettuna renkaiden A_i laskutoimitusten tuloilla

$$(x_i) + (y_i) = (x_i + y_i), \quad (x_i)(y_i) = (x_i y_i)$$

on rengas, *renkaiden A_i tulo*. (A on renkaiden A_i additiivisten ryhmien tuloryhmä (R1) ja multiplikatiivisten monoidien tulomonoidi (R2). Ehto (R3) seuraa välittömästi.)

Homomorfismit.

MÄÄRITELMÄ 1.7.2. Olkoot A ja B renkaita. Kuvaus $f\colon A \to B$ on *homomorfismi*, jos kaikilla x, $y \in A$

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$

ja lisäksi $f(1) = 1$.

Ehdot merkitsevät siis, että f on ryhmähomomorfismi yhteenlaskun suhteen ja monoidihomomorfismi kertolaskun suhteen.

Alirenkaat.

MÄÄRITELMÄ 1.7.3. Renkaan A osajoukko B on A:n *alirengas*, jos se on A:n additiivinen aliryhmä, vakaa kertolaskun suhteen ja sisältää A:n ykkösalkion (eli on multiplikatiivinen alimonoidi).

Alirengas B on myös rengas. Ehdot voidaan kirjoittaa lyhyesti muotoon

$$0 \in B, \; B + B \subset B, \; -B \subset B, \; B.B \subset B, \; 1 \in B.$$

Esimerkki 3) Olkoon A rengas ja X sen osajoukko. Tällöin kaikkien joukon X sisältävien A:n alirenkaiden leikkaus B on myös A:n alirengas. Se on pienin osajoukon X sisältävä alirengas eli X:n *virittämä A:n alirengas.*

Tyhjän osajoukon virittämä alirengas on $B = \{n.1 \mid n \in \mathbf{Z}\}$, koska jokainen alirengas sisältää ykkösalkion 1.

Ideaalit.

MÄÄRITELMÄ 1.7.4. Renkaan A osajoukko $\mathfrak{a}$ on A:n *vasemmanpuolinen* (*oikeanpuolinen* tai *kaksipuolinen*) *ideaali*, jos se on A:n additiivinen aliryhmä ja ehdoista $a \in A$, $x \in \mathfrak{a}$ seuraa $ax \in \mathfrak{a}$ ($xa \in \mathfrak{a}$ tai kumpikin näistä).

Kaksipuolista ideaalia sanotaan usein vain *ideaaliksi*. Erityisesti tätä nimitystä käytetään, kun rengas A on vaihdannainen. Ehdot voidaan lyhyesti esittää muodossa

$$0 \in \mathfrak{a}, \quad \mathfrak{a} + \mathfrak{a} \subset \mathfrak{a}, \quad A.\mathfrak{a} \subset \mathfrak{a} \quad (\mathfrak{a}.A \subset \mathfrak{a}),$$

koska näistä jo seuraa viimeinen ehto $-\mathfrak{a} = (-1).\mathfrak{a} \subset \mathfrak{a}$.

Esimerkki 4) Jos X on renkaan A osajoukko, niin leikkaus kaikista joukon X sisältävistä A:n vasemmanpuolisista, oikeanpuolisista tai kaksipuolisista ideaaleista, on edelleen samantyyppinen ideaali, osajoukon *X virittämä* A:n vasemmanpuolinen, oikeanpuolinen tai kaksipuolinen *ideaali.*

Seuraava lause osoittaa, miten ideaalin alkioita voidaan esittää ns. *lineaarisina yhdistelminä.*

LAUSE 1.7.5. *Olkoon A rengas, $(x_i)_{i\in I}$ sen alkioperhe ja $\mathfrak{a}$ joukko, jonka muodostavat summat*

$$\sum_{i\in I} a_i x_i \quad (tai \; \sum_{i\in I} x_i a_i),$$

missä $(a_i)_{i\in I}$ on A:n alkioperhe, jonka kantaja on äärellinen. Tällöin $\mathfrak{a}$ on alkioiden x_i joukon virittämä (eli perheen (x_i) virittämä) A:n vasemmanpuolinen (tai oikeanpuolinen) ideaali.

Todistus jääköön harjoitustehtäväksi.

MÄÄRITELMÄ 1.7.6. Renkaan A vasemmanpuolinen ideaali on *maksimaalinen.* jos se on maksimaalinen A:n aitojen vasemmanpuolisten ideaalien $\mathfrak{a} \neq A$ joukossa.

LAUSE 1.7.7 (Krull). *Olkoon A rengas ja $\mathfrak{a}$ sen vasemmanpuolinen ideaali. Jos $\mathfrak{a} \neq A$, niin A:ssa on maksimaalinen vasemmanpuolinen ideaali $\mathfrak{m}$, joka sisältää $\mathfrak{a}$:n.*

Todistus. Olkoon S kaikkien niiden A:n vasemmanpuolisten ideaalien $\mathfrak{a}'$ joukko, jotka toteuttavat ehdon

$$\mathfrak{a} \subset \mathfrak{a}' \neq A.$$

Olkoon $(\mathfrak{a}_i)_{i \in I}$ perhe joukon S ideaaleja. Jos perhe on täysin järjestetty, eli kaikilla $i,\, j \in I$ pätee

$$\mathfrak{a}_i \subset \mathfrak{a}_j \quad \text{tai} \quad \mathfrak{a}_j \subset \mathfrak{a}_i,$$

niin $\mathfrak{b} = \bigcup_{i \in I} \mathfrak{a}_i$ on myös A:n vasemmanpuolinen ideaali. Lisäksi $\mathfrak{b} \neq A$, koska ehdoista $1 \notin \mathfrak{a}_i$ seuraa $1 \notin \mathfrak{b}$, Siten ideaali $\mathfrak{b}$ kuuluu joukkoon S ja sisältää kaikki ideaalit $\mathfrak{a}_i$. Zornin lemman nojalla joukossa S on siis maksimaalinen alkio. $\square$

Huomautus. Erityisesti jokaisessa renkaassa $A \neq \{0\}$ on maksimaalinen vasemmanpuolinen ideaali. (Voidaan valita $\mathfrak{a} = \{0\}$.)

Tekijärenkaat. Olkoon A rengas ja olkoon R laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio A:ssa. Tällöin alkion 0 luokka

$$\mathfrak{a} = \{x \mid x \equiv 0 \pmod R\}$$

on renkaan A kaksipuolinen ideaali, sillä

i) $0 \in \mathfrak{a}$,
ii) $\mathfrak{a} + \mathfrak{a} \subset \mathfrak{a}$ seuraa yhteensopivuudesta yhteenlaskun kanssa (jos $x \equiv 0$ ja $y \equiv 0$, niin $x + y \equiv 0 + 0 = 0$), ja
iii) $A.\mathfrak{a} \subset \mathfrak{a}$ ja $\mathfrak{a}.A \subset \mathfrak{a}$ seuraavat yhteensopivuudesta kertolaskun kanssa (jos $a \in A$ ja $x \equiv 0$, niin $a.x \equiv a.0 = 0$ ja $x.a \equiv 0.a = 0$).

Kääntäen, jos $\mathfrak{a}$ on renkaan A kaksipuolinen ideaali, niin ehdon

$$x - y \in \mathfrak{a}$$

määrittelemä relaatio on ekvivalenssi A:ssa, ns. *kongruenssi modulo* $\mathfrak{a}$, ja sille käytetään merkintää

$$x \equiv y \pmod{\mathfrak{a}} \quad \text{tai} \quad x \equiv y\ (\mathfrak{a}).$$

Lisäksi relaatio on yhteensopiva renkaan A yhteenlaskun ja kertolaskun kanssa:

$$\text{jos } x \equiv y\ (\mathfrak{a}) \text{ ja } x' \equiv y'\ (\mathfrak{a}), \text{ niin}$$
$$x + x' \equiv y + y'\ (\mathfrak{a}) \text{ ja } xx' \equiv yy'\ (\mathfrak{a})$$

kuten välittömästi nähdään. (Esimerkiksi

$$xx' - yy' = x(x' - y') + (x - y)y' \in \mathfrak{a}.)$$

Renkaan A tekijäjoukolle kongruenssin modulo $\mathfrak{a}$ suhteen käytetään merkintää $A/\mathfrak{a}$. Yhteenlaskun ja kertolaskun tekijälaskutoimituksilla varustettuna se on rengas (ehdot (R1-3) periytyvät), ja kanoninen kuvaus $\pi\colon A \to A/\mathfrak{a}$ on homomorfismi.

Määritelmä 1.7.8. Rengas $A/\mathfrak{a}$ on renkaan A *tekijärengas* kaksipuolisen ideaalin $\mathfrak{a}$ suhteen.

Lause 1.7.9 (Homomorfismien hajotuslause). *Olkoot A ja B renkaita, $f\colon A \to B$ rengashomomorfismi ja $\mathfrak{a}$ renkaan A kaksipuolinen ideaali. Jos $f(\mathfrak{a}) = \{0\}$, niin on olemassa yksikäsitteinen homomorfismi $\bar{f}\colon A/\mathfrak{a} \to B$, joka toteuttaa ehdon*

$$f = \bar{f} \circ \pi.$$

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & B \\ & A/\mathfrak{a} \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Todistus. Ehto $f(\mathfrak{a}) = \{0\}$ merkitsee, että kanonisen homomorfismin π ydin sisältyy homomorfismin f ytimeen. Ryhmähomomorfismien hajotuslauseen 1.3.7 nojalla on siten olemassa yksikäsitteinen additiivisten ryhmien homomorfismi $\bar{f}\colon A/\mathfrak{a} \to B$, jolla $f = \bar{f} \circ \pi$.

Toisaalta f on homomorfismi myös renkaiden kertolaskun suhteen, joten $\bar{f}$ on multiplikatiivinen homomorfismi lauseen 1.1.11 perusteella. Koska tekijärenkaan $A/\mathfrak{a}$ ykkösalkio on $\pi(1)$ ja $\bar{f}(\pi(1)) = f(1) = 1$, on $\bar{f}$ siis rengashomomorfismi. □

Lause 1.7.10 (Renkaiden homomorfialause). *Olkoot A ja B renkaita, ja olkoon $f\colon A \to B$ homomorfismi. Silloin*

i) *f:n ydin $\mathfrak{a} = f^{-1}(0)$ on A:n kaksipuolinen ideaali,*
ii) *f:n kuva $B' = f(A)$ on B:n alirengas, ja*
iii) *f:n kanonisesta hajotelmasta*

$$f\colon A \xrightarrow{\pi} A/\mathfrak{a} \xrightarrow{\bar{f}} B' \xrightarrow{j} B,$$

missä π on kanoninen surjektio ja j kanoninen injektio, saadaan renkaiden isomorfismi

$$\bar{f}\colon A/\mathfrak{a} \xrightarrow{\sim} B'.$$

Todistus jääköön harjoitustehtäväksi.

Jakorenkaat. Olkoon A vaihdannainen rengas ja S sen osajoukko. Tällöin A kertolaskullaan varustettuna on vaihdannainen monoidi, ja siten voidaan muodostaa sen jakomonoidi A_S nimittäjäjoukon S suhteen (ks. määr. 1.2.8). Kanoninen kuvaus $\varepsilon\colon A \to A_S$ on monoidihomomorfismi.

Lemma 1.7.11. *Monoidissa A_S on yksi ja vain yksi yhteenlasku, joka toteuttaa ehdot*

i) *A_S varustettuna tällä yhteenlaskulla ja kertolaskullaan on vaihdannainen rengas;*
ii) *ε on rengashomomorfismi.*

Todistus. Olkoot x ja y monoidin A_S alkiota. Ne voidaan esittää muodossa

$$x = a/p, \quad y = b/q,$$

missä a, $b \in A$ ja nimittäjät p, q ovat S:n virittämässä alimonoidissa S'. Laventamalla voidaan nimittäjät muuttaa samoiksi, ja saadaan

$$x = aq/pq = \varepsilon(aq)\varepsilon(pq)^{-1}, \quad y = \varepsilon(bp)\varepsilon(pq)^{-1}.$$

Jos tällöin A_S:ssä on ehdot toteuttava yhteenlasku, niin

$$\begin{aligned} x + y &= (\varepsilon(aq) + \varepsilon(bp))\varepsilon(pq)^{-1} \\ &= \varepsilon(aq + bp)\varepsilon(pq)^{-1} \\ &= (aq + bp)/pq. \end{aligned}$$

Yhteenlasku on siten yksikäsitteinen.

Yhteenlaskun olemassaolon todistamiseksi on osoitettava, että yllä esitetty summan arvo on riippumaton valinnoista. Olkoot

$$x = a'/p', \quad y = b'/q', \quad (a', b' \in A,\ p', q' \in S')$$

samojen alkioiden toiset esitykset. Jakomonoidin määritelmän mukaan pätevät tällöin yhtälöt

$$ap's = a'ps, \quad bq't = b'qt$$

eräillä alimonoidin S' alkioilla s ja t. Kun kerrotaan yhtälöt tuloilla $qq't$ ja $pp's$, ja lasketaan yhteen puolittain, saadaan

$$(aq + bp)(p'q')(st) = (a'q' + b'p')(pq)(st).$$

Koska $st \in S'$, tästä seuraa yhtälö

$$(aq + bp)/pq = (a'q' + b'p')/p'q',$$

ja siten summa $x + y$ on hyvin määritelty. Harjoitustehtäväksi jää sen osoittaminen, että A_S on rengas ja ε on rengashomomorfismi. $\square$

Kun jakomonoidi A_S varustetaan lemman esittelemällä yhteenlaskulla, sille käytetään usein merkintää $A[S^{-1}]$, joka tarkoittaa rengasta A laajennettuna joukon S alkioiden käänteisalkioilla.

MÄÄRITELMÄ 1.7.12. Rengas $A[S^{-1}]$ on renkaan A *jakorengas* nimittäjäjoukon S suhteen.

Huomautus. Kanoninen homomorfismi $\varepsilon\colon A \to A[S^{-1}]$ on injektiivinen vain, jos jokainen $s \in S$ on *säännöllinen* (ei nollanjakaja), eli kaikilla $x \in A$ pätee

$$sx = 0 \ \Rightarrow\ x = 0.$$

(Ehto $\varepsilon(x) = 0$ merkitsee, että $sx = 0$ jollakin $s \in S$.)

Esimerkki 5) Olkoon S renkaan A säännöllisten alkioiden joukko, (joka on A:n multiplikatiivinen alimonoidi.) Tällöin $A[S^{-1}]$ on A:n *täysi jakorengas* ja kanoninen homomorfismi $\varepsilon\colon A \to A[S^{-1}]$ on injektiivinen.

Tavallisesti A samastetaan kuvansa $\varepsilon(A)$ kanssa täyden jakorenkaan $A[S^{-1}]$ alirenkaaksi. Jos A on kokonaisalue, niin kaikki sen alkiot $s \neq 0$ ovat säännöllisiä ja täysi jakorengas on A:n *jakokunta*.

LAUSE 1.7.13 (Jakorenkaan universaaliominaisuus). *Olkoot A ja B kaksi vaihdannaista rengasta, $f\colon A \to B$ rengashomomorfismi ja S renkaan A osajoukko, jonka kuvan $f(S)$ alkiot ovat kääntyviä renkaassa B.*

Silloin on olemassa yksikäsitteinen homomorfismi $\bar{f}\colon A[S^{-1}] \to B$, joka toteuttaa ehdon

$$f = \bar{f} \circ \varepsilon.$$

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\varepsilon"'] & & B \\ & A[S^{-1}] \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Todistus. Jakomonoidin universaaliominaisuuden (lause 1.2.9) nojalla on olemassa yksikäsitteinen monoidihomomorfismi $\bar{f}\colon A_S \to B$, joka täyttää ehdon $f = \bar{f} \circ \varepsilon$. On siis riittävää osoittaa, että $\bar{f}$ on myös additiivisten ryhmien homomorfismi.

Olkoot a/p ja b/q kaksi A_S:n alkiota. Silloin

$$a/p + b/q = (aq + bp)/pq = \varepsilon(aq + bp)\varepsilon(pq)^{-1}.$$

Koska $\bar{f}$ on multiplikatiivinen monoidihomomorfismi, tästä seuraa

$$\bar{f}(a/p + b/q) = \bar{f}(\varepsilon(aq + bp))\bar{f}(\varepsilon(pq)^{-1}) = \bar{f}(\varepsilon(aq + bp))\bar{f}(\varepsilon(pq))^{-1},$$

ja edelleen, koska $f = \bar{f} \circ \varepsilon$ on rengashomomorfismi,

$$\begin{aligned} \bar{f}(a/p + b/q) &= f(aq + bp)f(pq)^{-1} \\ &= (f(a)f(q) + f(b)f(p))f(p)^{-1}f(q)^{-1} \\ &= f(a)f(p)^{-1} + f(b)f(q)^{-1} \\ &= \bar{f}(a/p) + \bar{f}(b/q). \end{aligned}$$

□

Huomautus. Renkaan B ei tarvitse olla vaihdannainen, sillä kuvan $f(A)$ alkiot kommutoivat joka tapauksessa keskenään ja myös joukon $f(S)$ alkioiden käänteisalkioiden kanssa.

Harjoitustehtäviä

1) Olkoon G vaihdannainen ryhmä. Osoitettava, että sen endomorfismien joukon $\mathrm{End}(G)$ kertolasku on ositteleva yhteenlaskun suhteen.

2) Etsittävä kaikki renkaat, joissa on 4 alkiota. (4 erilaista.)

3) Olkoon A rengas, $(x_i)_{i\in I}$ perhe A:n alkioita ja $\mathfrak{a}$ joukko, jonka muodostavat summat

$$\sum_{i\in I} a_i x_i,$$

missä $(a_i)_{i\in I}$ on äärelliskantajainen perhe A:n alkioita. Osoitettava, että $\mathfrak{a}$ on joukon $X = \{x_i \mid i \in I\}$ virittämä renkaan A vasemmanpuolinen ideaali.

4) Olkoon A rengas, X sen osajoukko ja $\mathfrak{a}$ joukko, jonka muodostavat summat

$$\sum_{i\in I} a_i x_i b_i,$$

missä I on äärellinen joukko, a_i, $b_i \in A$ ja $x_i \in X$ kaikilla $i \in I$. Osoitettava, että $\mathfrak{a}$ on joukon X virittämä renkaan A kaksipuolinen ideaali.

5) Olkoon p alkuluku ja $S = \{s \in \mathbf{Z} \mid s \not\equiv 0 \pmod{p}\}$. Osoitettava, että

i) rationaaliluvut a/s, missä $s \in S$, muodostavat kunnan $\mathbf{Q}$ alirenkaan A;
ii) on olemassa yksikäsitteinen homomorfismi $\mathbf{Z}[S^{-1}] \to \mathbf{Q}$; se on injektiivinen ja sen kuva on A;
iii) on olemassa yksikäsitteinen homomorfismi $\mathbf{Z}[S^{-1}] \to \mathbf{Z}/p\mathbf{Z}$; se on surjektiivinen ja sen ydin on $p\mathbf{Z}[S^{-1}]$;
iv) A/pA on isomorfinen äärellisen kunnan $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ kanssa, ja pA on renkaan A maksimaalinen ideaali.

6) Renkaan A alkio e on *keskeinen*, jos $ex = xe$ kaikilla $x \in A$, ja *idempotentti*, jos $e^2 = e$. Olkoon $e \in A$ keskeinen idempotentti alkio. (Esim. $e = (1, 0)$ tulorenkaassa $A_1 \times A_2$.) Osoitettava:

i) $A_1 = Ae$ on rengas, samoin $A_2 = A(1-e)$ ($1-e$ on myös keskeinen idempotentti alkio);
ii) kuvaus $x \mapsto (xe, x(1-e))$ on isomorfismi renkaalta A tulorenkaalle $A_1 \times A_2$.

1.8. Kunnat

MÄÄRITELMÄ 1.8.1. Rengas K on *kunta*, jos $K \neq \{0\}$ ja jokainen K:n alkio $x \neq 0$ on kääntyvä.

Kuntaa, joka ei ole vaihdannainen, sanotaan myös *vinokunnaksi*. Kunnan K kääntyvien alkioiden ryhmä on $K^* = K \setminus \{0\}$.

Kunnan K *alikunta* on alirengas L, joka on kunta eli sisältää jokaisen alkionsa $x \neq 0$ käänteisalkion. Tällöin K on puolestaan kunnan L *ylikunta*.

Esimerkkejä. 1) Kunnan K kaikkien alikuntien leikkaus P on kunta. Se on pienin K:n alikunta, ns. K:n *alkukunta*.

Alkukunta P sisältää ykkösalkion kerrannaiset $n.1$ ($n \in \mathbf{Z}$), ja ne muodostavat sen alirenkaan A. Jos $n.1 \neq 0$, kun $n \neq 0$, niin K:n *karakteristika* $\operatorname{char}(K)$ on 0 ja $A \cong \mathbf{Z}$. Muulloin $\operatorname{char}(K)$ on pienin luku $p > 0$, jolla $p.1 = 0$; se on alkuluku ja $A \cong \mathbf{Z}/p\mathbf{Z}$.

Pienin K:n alikunta on A:n jakokunta; siis saadaan

$$P \cong \begin{cases} \mathbf{Q} & \text{, kun } \operatorname{char}(K) = 0, \\ \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} & \text{, kun } \operatorname{char}(K) = p > 0. \end{cases}$$

2) Jos X on kunnan K osajoukko, niin leikkaus kaikista joukon X sisältävistä K:n alikunnista on K:n alikunta L, osajoukon X *virittämä K:n alikunta.*

Erityisesti alkukunta P on tyhjän osajoukon virittämä alikunta.

LAUSE 1.8.2. *Rengas A on kunta, jos ja vain jos $A \neq \{0\}$ ja A:n ainoat vasemmanpuoliset ideaalit ovat A ja $\{0\}$.*

Todistus. Olkoon A kunta, jolloin $A \neq \{0\}$ määritelmän mukaan. Olkoon $\mathfrak{a}$ jokin A:n vasemmanpuolinen ideaali. Jos se ei ole $\{0\}$, niin se sisältää alkion $a \neq 0$. Silloin a:lla on käänteisalkio $a^{-1} \in A$, ja siten jokainen $x \in A$ voidaan esittää muodossa

$$x = (xa^{-1})a \in \mathfrak{a}.$$

Tällöin siis on välttämättä $\mathfrak{a} = A$.

Oletetaan kääntäen, että $A \neq \{0\}$ ja että A:n ainoat vasemmanpuoliset ideaalit ovat A ja $\{0\}$. Olkoon $x \in A$, $x \neq 0$. On osoitettava, että x on kääntyvä.

Joukko Ax on A:n vasemmanpuolinen ideaali, joka ei ole $\{0\}$, koska $x \neq 0$. Oletuksen nojalla on siis $Ax = A$, ja siksi on erityisesti olemassa sellainen $x' \in A$ että $x'x = 1$.

Tällöin myös $x' \neq 0$ (koska $1 \neq 0$), ja toistamalla päättely nähdään, että $x''x' = 1$ jollakin $x'' \in A$. Alkio x' on siten sekä vasemmalta että oikealta kääntyvä. Lauseen 1.2.4 nojalla se on silloin kääntyvä, käänteisalkionaan $x = x''$. □

Huomautus. Vastaava tulos pätee myös oikeanpuolisilla ideaaleilla.

KOROLLAARI 1.8.3. *Olkoon A rengas ja $\mathfrak{a}$ sen kaksipuolinen ideaali. Tällöin tekijärengas $A/\mathfrak{a}$ on kunta, jos ja vain jos $\mathfrak{a}$ on A:n maksimaalinen vasemmanpuolinen ideaali.*

Todistus. Renkaan $A/\mathfrak{a}$ vasemmanpuoliset ideaalit ovat $\mathfrak{b}/\mathfrak{a}$, missä $\mathfrak{b}$ on $\mathfrak{a}$:n sisältävä A:n vasemmanpuolinen ideaali. Tästä seuraa välittömästi, että

i) $A/\mathfrak{a} \neq \{0\}$, jos ja vain jos $\mathfrak{a} \neq A$, ja
ii) $A/\mathfrak{a}$:n ainoat vasemmanpuoliset ideaalit ovat $A/\mathfrak{a}$ ja $\{0\} = \mathfrak{a}/\mathfrak{a}$, jos ja vain jos A:n ainoat $\mathfrak{a}$:n sisältävät vasemmanpuoliset ideaalit ovat A ja $\mathfrak{a}$.

Nämä ehdot merkitsevät, että $\mathfrak{a}$ on A:n maksimaalinen vasemmanpuolinen ideaali, ja toisaalta lauseen 1.8.2 mukaan, että $A/\mathfrak{a}$ on kunta. □

Huomautus. Ideaali $\mathfrak{a}$ voi olla maksimaalinen A:n kaksipuolisten ideaalien joukossa olematta maksimaalinen vasemmanpuolinen ideaali.

Esimerkki 3) Olkoon A reaalisten 2×2-matriisien muodostama rengas. Sen ainoat kaksipuoliset ideaalit ovat A ja $\{0\}$ (harj. teht.). Nollaideaali $\{0\}$ ei kuitenkaan ole maksimaalinen vasemmanpuolinen ideaali, koska A ei ole kunta. (Kaikki matriisit $X \neq 0$ eivät ole kääntyviä.)

KOROLLAARI 1.8.4. *Jokaisella vaihdannaisella renkaalla $A \neq \{0\}$ on tekijärengas, joka on kunta.*

Todistus. Krullin lauseen 1.7.7 perusteella A:ssa on maksimaalinen vasemmanpuolinen ideaali $\mathfrak{m}$. Tällöin $\mathfrak{m}$ on kaksipuolinen ideaali, koska A on vaihdannainen. Korollaarin 1.8.3 mukaan tekijärengas $A/\mathfrak{m}$ on kunta. □

Harjoitustehtäviä

1) Olkoon A rengas ja $\mathfrak{a}$ sen kaksipuolinen ideaali. Osoitettava, että tekijärenkaan $A/\mathfrak{a}$ vasemmanpuoliset ideaalit ovat $\mathfrak{b}/\mathfrak{a}$, missä $\mathfrak{b}$ on $\mathfrak{a}$:n sisältävä A:n vasemmanpuolinen ideaali.

2) Olkoon K kunta ja A K-kertoimisten 2×2-matriisien rengas $\mathbf{M}_2(K)$.

i) Olkoon $X \in A$, $X \neq 0$. Osoitettava, että jokainen matriisi $Y \in A$, jossa on 3 nollaa, voidaan esittää muodossa $Y = MXN$, missä M, $N \in A$. (Myös näissä voi olla 3 nollaa.)

ii) Osoitettava, että A:n ainoat kaksipuoliset ideaalit ovat A ja $\{0\}$.

iii) Etsittävä A:n vasemmanpuolinen ideaali, joka ei ole A eikä $\{0\}$.