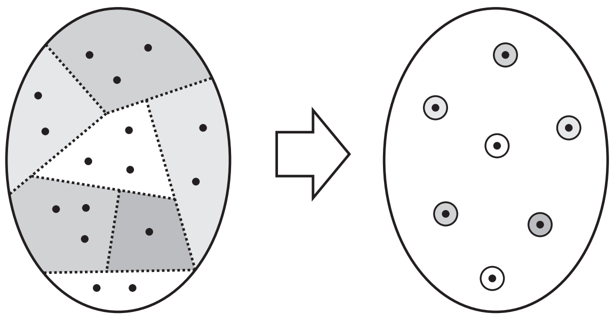
1. Tekijärakenteet

Tässä osassa tarkastellaan tekijärakenteita, kuten tekijäryhmiä ja tekijärenkaita, lähtien liikkeelle mahdollisimman yleisistä periaatteista. Tekijärakenteiden ajatuksena on päästä tarkastelemasta yksityiskohtia silloin, kun se ei ole välttämätöntä. Esimerkiksi annetun kokonaisluvun parillisuuden päättelemiseen tarvitsee tarkastella vain viimeistä numeroa. Yhteenlaskusta puolestaan tiedämme, että kahden luvun summa on parillinen, jos ja vain jos luvut ovat joko molemmat parillisia tai molemmat parittomia. Silloin kun parillisuus on ainoa kiinnostava ominaisuus, selviämme hyvin mistä tahansa yhteenlaskuun liittyvästä ongelmasta tarkkailemalla vain yhteenlaskettavien parillisuutta. Esimerkiksi summan

$$102738471029348 + 1723841702893740 + 172389471029347$$

selvittäminen on työlästä, mutta pelkkä vilkaisu kertoo, että tulos on pariton.

1.1. Ekvivalenssirelaatiot. Minkä tahansa tekijärakenteen taustalla on *ositus*. Ositus jakaa rakenteen X erillisiin epätyhjiin osiin, jotka yhdessä sisältävät kaikki alkuperäisen rakenteen X alkiot. Tekijärakenteen alkioina toimivat sitten nämä osat, ja jokaisen yksittäisen osan sisältämä rakenne jätetään tekijärakenteessa huomiotta.



Kuva 1. Tekijärakenteessa samaan osaan kuuluvat alkiot samastetaan.

Toinen tapa ymmärtää tekijärakennetta on, että ajatellaan *samastettavaksi* samaan osaan sisältyvät alkiot. Tällöin niiden väliset erot ikään kuin tahallisesti unohdetaan. Tämä johtaa luonnollisella tavalla *ekvivalenssirelaation* käsitteeseen. Jos R on jokin kaksipaikkainen relaatio, niin merkintä xRy tarkoittaa, että x on relaatiossa alkion y kanssa.[4] Intuitio antaa olettaa, että kuvatakseen ekvivalenssia (tai "samastamista") kaksipaikkaisen relaation R on toteutettava alla olevat ehdot kaikilla alkioilla x, y, z:

1. R on *refleksiivinen*, eli xRx.
2. R on *symmetrinen*, eli jos xRy, niin yRx.
3. R on *transitiivinen*, eli jos xRy ja yRz, niin xRz.

Nämä ehdot voidaan ottaa ekvivalenssirelaation määritelmäksi.

[4] Tarkasti määriteltynä kaksipaikkainen relaatio R tarkoittaa osajoukkoa järjestettyjen parien joukossa $X \times X$. Alkio x on relaatiossa alkion y kanssa, mikäli $(x, y) \in R$.

Määritelmä 1.1. Kaksipaikkaista relaatiota R joukossa X kutsutaan *ekvivalenssirelaatioksi*, jos se on refleksiivinen, symmetrinen ja transitiivinen. Alkion x sanotaan olevan *ekvivalentti* alkion y kanssa, jos xRy. Alkion x *ekvivalenssiluokaksi relaation R suhteen* nimitetään joukkoa, joka sisältää kaikki x:n kanssa ekvivalentit alkiot:

$$[x]_R = \{y \in X \mid xRy\}.$$

Ekvivalenssiluokkaa voidaan merkitä myös $[x]$ tai $\overline{x}$, jos relaatio on asiayhteydestä selvä. Relaation R kaikkien ekvivalenssiluokkien joukkoa merkitään X/R.

Tietyn ekvivalenssirelaation ekvivalenssiluokat muodostavat aina osituksen. Toisaalta jokainen ositus antaa aiheen määritellä ekvivalenssirelaatio, jossa samaan osaan kuuluvat alkiot ovat keskenään ekvivalentteja. Kaksi ekvivalenssiluokkaa $[x]$ ja $[y]$ ovat samat, jos ja vain jos x on ekvivalentti y:n kanssa. Sanotaan, että sekä x että y ovat tämän ekvivalenssiluokan *edustajia*.

Olkoon nyt $(X, *)$ jokin algebrallinen struktuuri, jonka tekijärakenne halutaan muodostaa. Ideana on valita sopiva ekvivalenssirelaatio $\sim$ samastamaan sellaiset alkiot, joiden eroja ei haluta huomioida. Näin saatavaan ositukseen $X/\sim$ määritellään sitten uusi laskutoimitus $*'$, joka vastaa luonnollisella tavalla alkuperäistä laskutoimitusta:

$$[x] *' [y] = [x * y] \quad \text{kaikilla } x, y \in X.$$

Tässä määritelmässä on eräs ongelma. Laskutoimituksen $*'$ täytyisi liittää jokaiseen pariin $([x], [y])$ yksikäsitteinen kolmas alkio $[x] *' [y]$. Kaavan antama tulos $[x * y]$ riippuu kuitenkin näennäisesti joukon X alkioista x ja y. Kukin ekvivalenssiluokka voi sisältää monia eri alkioita $x_1, x_2, x_3, \ldots$, ja tällöin $[x_1] = [x_2] = [x_3]$, jne. Jotta laskutoimituksen $[x] *' [y]$ tulos olisi yksikäsitteinen, on siis pidettävä huoli siitä, että se ei riipu joukon X alkioista vaan ainoastaan niiden edustamista luokista. Toisinaan sanotaan, että tällöin kaavan antama laskutoimitus on *hyvin määritelty*. Määrittelyn onnistuminen yleisessä tapauksessa vaatii, että laskutoimitus ja ekvivalenssirelaatio ovat tietyllä tavalla yhteensopivat.

Määritelmä 1.2. Olkoon X joukko, jossa on määritelty laskutoimitus $*$ sekä ekvivalenssirelaatio $\sim$. Jos kaikilla $x, x', y, y' \in X$ pätee

$$x \sim x' \quad \text{ja} \quad y \sim y' \qquad \Rightarrow \qquad x * y \sim x' * y',$$

sanotaan, että laskutoimitus $*$ on *yhteensopiva* relaation $\sim$ kanssa.

Yhteensopivuus takaa sen, että tekijärakenteessa voidaan määritellä alkuperäistä laskutoimitusta vastaava laskutoimitus.

Lause 1.3 (Tekijärakenteen määritelmä). *Olkoon $*$ laskutoimitus joukossa X, ja olkoon $\sim$ laskutoimituksen $*$ kanssa yhteensopiva ekvivalenssirelaatio. Tällöin on olemassa joukon $X/\sim$ laskutoimitus $*'$, jolle pätee*

$$[x] *' [y] = [x * y]$$

kaikilla $x, y \in X$.

Todistus. Jotta lauseessa annettu kaava määrittelisi laskutoimituksen $*'$ tuloksen yksikäsitteisesti, täytyy ekvivalenssiluokan $[x' * y']$ olla sama aina, kun $x' \in [x]$ ja $y' \in [y]$. Olkoot siis $x', y' \in X$ sellaisia, että $x' \sim x$ ja $y' \sim y$. Koska laskutoimitus $*$ on yhteensopiva ekvivalenssirelaation kanssa, pätee $x*y \sim x'*y'$. Tällöin

$$[x*y] = [x'*y'],$$

eli laskutoimituksen $*'$ tulos ei riipu luokkien $[x]$ ja $[y]$ edustajien valinnasta, vaan on aina sama luokka $[x*y]$. □

Yleensä tekijärakenteen laskutoimitusta merkitään samalla symbolilla kuin alkuperäisen rakenteen laskutoimitusta, mikäli sekaantumisen vaaraa ei ole.

Mikäli laskutoimituksella on rakenteessa X neutraalialkio, sen ekvivalenssiluokka $[e]$ toimii neutraalialkiona tekijärakenteessa. Tämä nähdään siitä, että $[e]*[x] = [e*x] = [x]$ kaikilla $x \in X$.

Esimerkki 1.4. Tarkastellaan monoidin $(\mathbb{N}, +)$ ositusta parillisiin ja parittomiin lukuihin. Tätä ositusta vastaa ekvivalenssirelaatio

$$n \sim n' \iff n + n' = 2k \quad \text{jollain } k \in \mathbb{N}.$$

Relaatio $\sim$ on yhteensopiva yhteenlaskun kanssa, sillä jos $m+m' = 2k$ ja $n+n' = 2l$, niin

$$(m+n) + (m'+n') = 2k + 2l = 2(k+l) \quad \text{ja} \quad k+l \in \mathbb{N}.$$

Nyt voidaan määritellä laskutoimitus $[m] + [n] = [m+n]$, missä tulos riippuu vain siitä, ovatko m ja n parillisia vai parittomia. Neutraalialkiona toimii $[0]$ eli parillisten lukujen luokka, ts. parillisen luvun lisääminen säilyttää parillisuuden ja parittomuuden. Saatu kaksialkioinen tekijämonoidi on itse asiassa ryhmä, sillä $[1]$ on oma vasta-alkionsa.

Voitaisiin myös tarkastella luonnollisten lukujen jakoa osiin $\{0, 1, 2\}$ (*pienet* luvut) ja $\{3, 4, 5 \dots\}$ (*suuret* luvut). Tätä ositusta kuvaavassa relaatiossa kaksi alkiota ovat ekvivalentteja, jos molemmat ovat pieniä tai molemmat suuria. Ekvivalenssirelaatio ei ole yhteensopiva laskutoimituksen kanssa, sillä kahden pienen luvun summa voi olla joko pieni (esim. $1+1=2$) tai suuri (esim. $2+2=3$). Näin ollen luokkien "pienet" ja "suuret" yhteenlaskua ei voida määritellä.

Esimerkki 1.5. *Erotusmonoidit.* Olkoon $(M, +)$ vaihdannainen monoidi, esim. $(\mathbb{N}, +)$. Yritetään luoda monoidia M vastaava rakenne, jossa kaikki alkiot olisivat kääntyviä. Ideana on muodostaa symbolisia erotuksia $a-b$, joista sitten samastetaan ne, joiden voi ajatella vastaavan samaa alkiota.

Erotuksien muodostamiseksi tarkastellaan tulomonoidia $(M \times M, +)$, jossa yhteenlasku määritellään pisteittäin: $(a,b)+(c,d) = (a+c, b+d)$, ja neutraalialkiona toimii $(0,0)$. Paria (a,b) voidaan nyt pitää symbolisena erotuksena. Tulomonoidissa määritellään relaatio

$$(a,b) \sim (a',b') \iff a + b' + c = a' + b + c \quad \text{jollain } c \in M.$$

Relaatiota voidaan verrata kokonaislukujen laskusääntöihin, joiden mukaan $a-b = a'-b'$, jos ja vain jos $a+b' = a'+b$. Alkio c voidaan jättää ehdosta pois, jos jokainen alkio on *supistuva*, eli jos ehdosta $x+c = y+c$ seuraa $x = y$ (kuten luonnollisilla luvuilla).

On helppo osoittaa, että relaatio $\sim$ on yhteenlaskun kanssa yhteensopiva ekvivalenssirelaatio. Saatavaa tekijärakennetta $M \times M/\sim$ kutsutaan *erotusmonoidiksi.*

Kanoninen kuvaus $a \mapsto [(a,0)]$ liittää alkuperäisen monoidin M erotusmonoidiinsa. Mikäli jokainen alkio on supistuva, kanoninen kuvaus on injektio, ja alkuperäinen monoidi voidaan ajatella erotusmonoidin osajoukkona (esim. $(\mathbb{N},+) \subset (\mathbb{Z},+)$). Erotusmonoidissa jokaisella alkiolla $[(a,b)]$ on vasta-alkio, sillä

$$[(b,a)] + [(a,b)] = [(a+b,a+b)] = [(0,0)].$$

Erotusmonoidin konstruktiota voidaan hieman yleistää valitsemalla aluksi jokin laskutoimituksen suhteen suljettu osajoukko S, jonka alkioista halutaan kääntyviä. Tällöin ekvivalenssin ehdoksi tulomonoidissa tulee

$$(a,b) \sim (a',b') \iff a+b'+c = a'+b+c \quad \text{jollain } c \in S.$$

Tällainen yleisempi konstruktio on tarpeen esimerkiksi silloin, kun monoidista $(\mathbb{Z},\cdot)$ halutaan konstruoida murtoluvut. Joukoksi S on tässä tapauksessa valittava $\mathbb{Z} \setminus \{0\}$. (Multiplikatiivisen merkinnän tapauksessa erotusmonoidia kutsutaan *jakomonoidiksi.*)

1.2. Homomorfismien hajottaminen. Oletetaan, että on määritelty algebrallinen struktuuri $(X,*)$ ja sen tekijästruktuuri X/R ekvivalenssirelaation R suhteen. Kuvausta $\pi : X \to X/R$, $\pi(x) = [x]$, joka liittää jokaiseen alkioon sen edustaman ekvivalenssiluokan, nimitetään *kanoniseksi surjektioksi.* Tekijärakenteen määritelmästä seuraa suoraan, että kanoninen surjektio on aina homomorfismi.

Oletetaan nyt, että on lisäksi määritelty homomorfismi $f : (X,*) \to (Y,\cdot)$. Herää kysymys, voidaanko määritellä sellaista homomorfismia $\overline{f}$ tekijärakenteesta X/R joukkoon Y, joka toteuttaisi ehdon

$$f = \overline{f} \circ \pi.$$

Tämän ehdon toteutuessa sanotaan, että alla oleva kaavio *kommutoi.*

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

Kommutointiehdon merkitys on siinä, että sen toteutuessa voitaisiin kirjoittaa

$$\overline{f}([x]) = f(x),$$

jolloin homomorfismin $\overline{f}$ ominaisuudet olisivat suoraan johdettavissa kuvauksen f ominaisuuksista. Ongelma puolestaan on se, että kuvaus f voi saada eri arvoja sellaisillakin alkioilla, jotka kuuluvat samaan ekvivalenssiluokkaan, kun taas $\overline{f} \circ \pi$ kuvaa tällaiset alkiot aina samalle alkiolle. Ongelma ratkaistaan samalla tavoin kuin tekijärakenteen määrittelyssä.

Määritelmä 1.6. Olkoon X joukko, jossa on määritelty ekvivalenssirelaatio $\sim$. Olkoon f lisäksi kuvaus X:ltä joukkoon Y. Jos kaikilla $x, x' \in X$ pätee

$$x \sim x' \qquad \Rightarrow \qquad f(x) = f(x'),$$

sanotaan, että kuvaus f on *yhteensopiva* ekvivalenssirelaation $\sim$ kanssa.

LAUSE 1.7 (Homomorfismin hajottaminen). *Olkoon f homomorfismi struktuurilta $(X, *)$ struktuuriin $(Y, \cdot)$, ja olkoon $\sim$ joukossa X määritelty laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Jos f on yhteensopiva ekvivalenssirelaation $\sim$ kanssa, niin on olemassa yksikäsitteinen homomorfismi $\overline{f} : X/\sim \to Y$, jolle pätee*

$$f = \overline{f} \circ \pi,$$

missä π on kanoninen surjektio $X \to X/\sim$.

TODISTUS. Olkoot $x, x' \in X$ sellaisia, että $\pi(x) = \pi(x')$. Tällöin $x \sim x'$, ja koska f on yhteensopiva relaation $\sim$ kanssa, myös $f(x) = f(x')$. Koska $f(x')$ on siis sama alkio kaikilla $x' \in [x]$, voidaan kuvauksen $\overline{f}$ arvot määritellä yksikäsitteisesti valitsemalla $\overline{f}([x]) = f(x)$. Näin saatu $\overline{f}$ on homomorfismi, sillä

$$\overline{f}([x] * [y]) = \overline{f}([x * y]) = f(x * y) = f(x) \cdot f(y) = \overline{f}([x]) \cdot \overline{f}([y]),$$

ja mahdollinen neutraalialkion luokka $[e]$ kuvautuu alkiolle $f(e)$, joka on struktuurin Y neutraalialkio. Kuvauksen $\overline{f}$ yksikäsitteisyys seuraa suoraan siitä, että sen on toteutettava kaava $\overline{f}([x]) = f(x)$. □

HUOMAUTUS 1.8. Edellisessä lauseessa mainittu ehto on itse asiassa välttämätön, eli kaavan $f = \overline{f} \circ \pi$ määrittelemä kuvaus on olemassa jos ja vain jos f on yhteensopiva ekvivalenssirelaation kanssa. Huomaa lisäksi, että $\operatorname{Im} \overline{f} = \operatorname{Im} f$.

ESIMERKKI 1.9. Jatketaan esimerkin 1.4 tarkastelua. Niin sanottu *inkluusiokuvaus* $\iota : (\mathbb{N}, +) \to (\mathbb{Z}, +)$, $\iota(n) = n$, on monoidihomomorfismi. Se ei kuitenkaan ole yhteensopiva ekvivalenssirelaation kanssa, sillä esim. $\iota(0) \neq \iota(2)$, vaikka $0 \sim 2$. Tekijämonoidista $\mathbb{N}/\sim$ ei siis saada kuvausta ι vastaavaa homomorfismia kokonaisluvuille. Tämä olisikin mahdotonta: kyseisen homomorfismin kuvassa voisi siis olla korkeintaan kaksi alkiota, mutta toisaalta sen pitäisi olla sama kuin $\operatorname{Im} \iota$, joka on ääretön.

Tarkastellaan sitten kuvausta $g : (\mathbb{N}, +) \to (\{1, -1\}, \cdot)$, $g(n) = (-1)^n$, joka on myös homomorfismi. Jos $n \sim n'$, niin jollain $k \in \mathbb{N}$ pätee

$$g(n) = (-1)^n = (-1)^{2k-n'} = \left((-1)^2\right)^k \cdot \left((-1)^{-1}\right)^{n'} = 1^k \cdot (-1)^{n'} = g'(n).$$

Siispä g on yhteensopiva relaation $\sim$ kanssa. Näin ollen on olemassa homomorfismi $\overline{g} : \mathbb{N}/\sim \to \{1, -1\}$, jolle pätee $[0] \mapsto 1$ ja $[1] \mapsto -1$. Tämä homomorfismi on itse asiassa ryhmäisomorfismi: surjektiivisuus seuraa g:n surjektiivisuudesta ja injektiivisyys esim. siitä, että lähtö- ja maalijoukko ovat samankokoisia.

1.3. Tekijäryhmät. Olkoon G multiplikatiivinen ryhmä. Tekijäryhmään liittyvä ekvivalenssirelaatio saadaan aina ns. normaalin aliryhmän avulla.

MÄÄRITELMÄ 1.10. Aliryhmää $H \leq G$ kutsutaan *normaaliksi*, jos sen vasemmat ja oikeat sivuluokat ovat samat, eli $gH = Hg$ kaikilla $g \in G$. Jos H on G:n normaali aliryhmä, merkitään $H \trianglelefteq G$.

Algebra I:ssä on todistettu seuraava lause.

LAUSE 1.11 (Normaalisuuskriteeri). *Aliryhmä H on normaali ryhmässä G, jos ja vain jos kaikilla $g \in G$ pätee $gHg^{-1} \subset H$ eli*

$$ghg^{-1} \in H \quad \textit{jokaisella } h \in H.$$

Minkä hyvänsä aliryhmän sivuluokat muodostavat aina koko ryhmän osituksen. Jokaista aliryhmää vastaa siis ekvivalenssirelaatio, jossa alkiot ovat ekvivalentteja täsmälleen silloin, kun ne kuuluvat samaan sivuluokkaan. Koska sivuluokat eivät leikkaa toisiaan ja $g \in gH$ kaikilla g, alkiot x ja x' kuuluvat samaan sivuluokkaan, jos ja vain jos $x \in x'H$. Kun aliryhmä on normaali, tämä relaatio on yhteensopiva laskutoimituksen kanssa, mikä seuraavassa todistetaan.

Lause 1.12. *Oletetaan, että $H \trianglelefteq G$. Tällöin ekvivalenssirelaatio*

$$x \sim x' \iff x \in x'H$$

on yhteensopiva laskutoimituksen kanssa.

Todistus. Olkoot $x, x', y, y' \in G$ sellaiset, että $x \in x'H$ ja $y \in y'H$. Erityisesti $x = x'h_1$ ja $y = y'h_2$ joillain $h_1, h_2 \in H$. Nyt $h_1y' \in Hy'$, ja koska H on normaali, $Hy' = y'H$. Täten $h_1y' = y'h_3$ jollain $h_3 \in H$. Lopulta saadaan

$$xy = x'h_1 \cdot y'h_2 = x'y' \cdot h_3h_2 \in (x'y')H,$$

eli $xy \sim x'y'$. □

Normaalin aliryhmän N suhteen voidaan siis muodostaa tekijäryhmä, jossa samastetaan samaan sivuluokkaan kuuluvat alkiot. Tätä tekijäryhmää merkitään G/N. Kääntäen, jokainen ryhmälaskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio liittyy aina johonkin normaaliin aliryhmään.

Lause 1.13. *Oletetaan, että $\sim$ on ryhmässä G määritelty, laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Tällöin neutraalialkion luokka $N = [e]$ on normaali aliryhmä G:ssä, ja kaikilla $g, g' \in G$ pätee $g \sim g'$ jos ja vain jos $g' \in gN$.*

Todistus. Osoitetaan ensin, että N on aliryhmä. Selvästi $e \in N$. Olkoot sitten $g, h \in N$. Tällöin $g \sim e$ ja $h \sim e$, joten $gh \sim ee = e$, koska laskutoimitus on yhteensopiva relaation $\sim$ kanssa. Näin ollen $gh \in N$. Lisäksi

$$e = g^{-1}g \sim g^{-1}e = g^{-1},$$

koska $g \sim e$. Täten $g^{-1} \in N$, ja N on G:n aliryhmä.

Olkoot sitten $g, g' \in G$ sellaiset, että $g \sim g'$. Tällöin $g^{-1}g' \sim g^{-1}g = e$, joten $g^{-1}g' \in N$. Näin ollen

$$g' = g \cdot \underbrace{g^{-1}g'}_{\in N} \in gN.$$

Toisaalta, jos $g' \in gN$, niin $g^{-1}g' \in N$, eli $g^{-1}g' \sim e$. Täten $g' = g \cdot g^{-1}g' \sim ge = g$.

Nyt on osoitettu, että N on G:n aliryhmä, ja kaikilla $g \in G$ pätee $gN = [g]$. Samalla tavoin voidaan osoittaa, että $Ng = [g]$ kaikilla $g \in G$, joten N:n vasemmat ja oikeat sivuluokat ovat samat. Tämä tarkoittaa, että N on normaali. □

Tästä eteenpäin oletetaan aina ryhmistä puhuttaessa, että tekijärakenteeseen liittyvä ekvivalenssirelaatio on muotoa $g \in g'N$.

Ryhmähomomorfismin hajotukselle saadaan seuraava ehto.

Lause 1.14. *Olkoon $f : G \to H$ ryhmähomomorfismi, ja olkoon $N \trianglelefteq G$. Tällöin on olemassa yksikäsitteinen homomorfismi $\overline{f} : G/N \to H$, jolle pätee $\overline{f}([g]) = f(g)$ kaikilla $g \in G$, jos ja vain jos $N \subset \operatorname{Ker} f$.*

Todistus. Oletetaan ensin, että $N \subset \operatorname{Ker} f$. Jos $g' \sim g$ eli $g' \in gN$, niin $g^{-1}g' \in N$. Oletuksen perusteella

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

joten $f(g) = f(g')$. Kuvauksen $\overline{f}$ olemassaolo seuraa nyt lauseesta 1.7.

Oletetaan sitten, että $N \not\subset \operatorname{Ker} f$. Tällöin löytyy jokin $h \in N$, jolle $f(h) \neq 1_H$. Toisaalta $[h] = [1_G]$ ja $f(1_G) = 1_H$, joten millään kuvauksella ei voi päteä $[g] \mapsto f(g)$ kaikilla $g \in G$. □

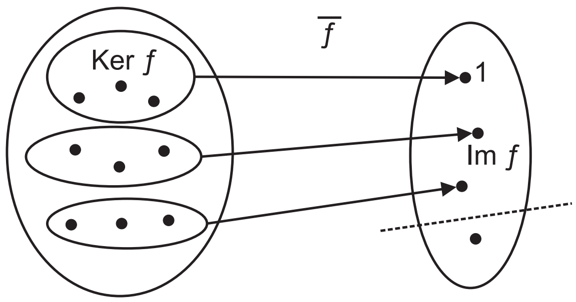
Tunnetusti ryhmähomomorfismin ydin on normaali aliryhmä. Yllä olevasta lauseesta saadaan siten erityistapauksessa $\operatorname{Ker} f = N$ tuttu homomorfialause.

Korollaari 1.15 (Ryhmien homomorfialause). *Olkoon $f : G \to H$ ryhmähomomorfismi. Tällöin ryhmät $G/\operatorname{Ker} f$ ja $\operatorname{Im} f$ ovat isomorfiset.*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
G/\operatorname{Ker} f \arrow[r, dashed, "\cong"] & \operatorname{Im} f \arrow[u, hook, "\iota"']
\end{tikzcd}$$

(Kaavioissa kaksoinuoli viittaa yleensä surjektioon ja koukkunuoli injektioon; tässä ι on inkluusiokuvaus.)

Todistus. Lauseen nojalla löytyy homomorfismi $\overline{f} : G/\operatorname{Ker} f \to H$. Olkoon $g \in G$. Jos $g \not\sim 1_G$, niin $g \notin \operatorname{Ker} f$, joten $\overline{f}([g]) = f(g) \neq 1_H$. Näin ollen $\operatorname{Ker} \overline{f} = \{[1_G]\}$, mistä seuraa kuvauksen $\overline{f}$ injektiivisyys. Rajoittamalla maalijoukko aliryhmään $\operatorname{Im} f$, saadaan kuvauksesta $\overline{f}$ edelleen bijektiivinen homomorfismi $\tilde{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$. □



Kuva 2. Homomorfismi $\overline{f}$ kuvaa ytimen sivuluokat yksi yhteen kuvajoukon alkioille

1.4. Tekijärenkaat. Renkaiden kohdalla on pidettävä huoli siitä, että tekijärakenteeseen liittyvä ekvivalenssirelaatio on yhteensopiva *molempien* laskutoimitusten suhteen. Koska renkaan yhteenlaskuryhmä on vaihdannainen, kaikki sen aliryhmät ovat normaaleja. Kertolaskun mukaanliittämistä varten aliryhmän on lisäksi toteutettava ns. *ideaalisuusehdot*.

MÄÄRITELMÄ 1.16. Renkaan $(R, +, \cdot)$ yhteenlaskuryhmän aliryhmää A kutsutaan *ideaaliksi*, jos kaikilla $r \in R$ ja $a \in A$ pätee

$$ra \in A \qquad \text{ja} \qquad ar \in A.$$

Ensimmäisen ehdon toteuttavia aliryhmiä kutsutaan *vasemmanpuoleisiksi* ideaaleiksi ja toisen ehdon toteuttavia *oikeanpuoleisiksi*.

HUOMAUTUS 1.17. Ideaalisuusehdot muuttuvat ymmärrettäviksi, kun pohditaan kysymystä: "Minkälainen luokka voidaan ottaa tekijärenkaan nolla-alkioksi?" Koska renkaassa pätee aina $r \cdot 0 = 0 \cdot r = 0$, täytyy tämän luokan myös toteuttaa $[r]A = A[r] = A$.

Ideaalin sivuluokat muodostavat osituksen.

LAUSE 1.18. *Olkoon A ideaali renkaassa R. Tällöin ekvivalenssirelaatio*

$$r \sim r' \iff r \in r' + A$$

on yhteensopiva renkaan kertolaskun kanssa.

TODISTUS. Olkoot $x, x', y, y' \in R$ sellaiset, että $x \in x' + A$ ja $y \in y' + A$. Erityisesti $x = x' + a_1$ ja $y = y' + a_2$ joillain $a_1, a_2 \in A$. Koska A on ideaali, tulot $x'a_2$, a_1y' ja a_1a_2 sisältyvät A:han. Näin ollen

$$xy = (x' + a_1)(y' + a_2) = x'y' + \underbrace{x'a_2 + a_1y' + a_1a_2}_{\in A} \in x'y' + A,$$

joten $xy \sim x'y'$. □

Renkaan R tekijärengasta ideaalin A suhteen merkitään tavalliseen tapaan R/A. Kuten ryhmien tapauksessa, myös nyt jokainen laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio on peräisin jostain ideaalista.

LAUSE 1.19. *Oletetaan, että $\sim$ on renkaassa R määritelty, molempien laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio. Tällöin nolla-alkion luokka $A = [0]$ on ideaali renkaassa R, ja kaikilla $r, r' \in R$ pätee $r \sim r'$ jos ja vain jos $r \in r' + A$.*

TODISTUS. Lauseesta 1.13 seuraa, että A on aliryhmä ja sen sivuluokat vastaavat täsmälleen relaation $\sim$ ekvivalenssiluokkia. Tarvitsee siis vain todistaa, että A on ideaali. Olkoot $r \in R$ ja $a \in A$ eli $a \sim 0$. Koska laskutoimitus on yhteensopiva relaation $\sim$ kanssa, niin

$$ra \sim r \cdot 0 = 0 \qquad \text{ja} \qquad ar \sim 0 \cdot r = 0.$$

Tämä tarkoittaa, että $r \in A$. □

Algebra I:ssä on osoitettu, että rengashomomorfismin ydin on aina ideaali. Seuraavien rengashomomorfismien hajotukseen liittyvien lauseiden todistukset sivuutetaan, koska ne ovat aivan samanlaiset kuin ryhmähomomorfismien tapauksessa.

LAUSE 1.20. *Olkoon* $f : R \to S$ *rengashomomorfismi, ja olkoon* A *renkaan* R *ideaali. Tällöin on olemassa yksikäsitteinen rengashomomorfismi* $\overline{f} : R/A \to S$*, jolle pätee* $\overline{f}([r]) = f(r)$ *kaikilla* $r \in R$*, jos ja vain jos* $A \subset \operatorname{Ker} f$.

KOROLLAARI 1.21 (Renkaiden homomorfialause). *Olkoon* $f : R \to S$ *rengashomomorfismi. Tällöin renkaat* $R/\operatorname{Ker} f$ *ja* $\operatorname{Im} f$ *ovat isomorfiset.*