II Vaihdannaiset renkaat

1. Peruskäsitteitä

Kerrataan ensin tällä kurssilla tarvittavia, suurelta osin Algebra I:stä tuttuja algebrallisten rakenteiden määritelmiä. Käydään ensin läpi yhden laskutoimituksen rakenteen tietosanakirjamaisesti, esimerkeittä.

1.1. Määritelmä. Yhden laskutoimituksen rakenne $(S, *)$ on *puoliryhmä*, jos laskutoimitus $*$ on *liitännäinen* eli kaikilla $x, y, z \in S$ pätee

$$(x * y) * z = x * (y * z).$$

1.2. Määritelmä. Puoliryhmä $(M, *)$ on *monoidi*, jos laskutoimituksella $*$ on *neutraalialkio* e, jolle

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

kun $x \in M$. Jos laskutoimitusta merkitään yhteenlaskusymbolilla +, niin neutraalialkiota nimitetään yleensä *nolla-alkioksi* ja merkitään symbolilla 0, jos taas kertolaskusymbolilla, niin neutraalialkiota nimitetään tavanomaisesti *ykkösalkioksi* ja merkitään symbolilla 1.

1.3. Määritelmä. Monoidi $(G, \cdot)$ on *ryhmä*, jos jokaisella $x \in G$ on *käänteisalkio* y, jolle

$$x \cdot y = y \cdot x = e.$$

Käänteisalkiota merkitään yleensä $y = x^{-1}$, paitsi, että käänteisalkioita yhteenlaskujen suhteen kutsutaan *vasta-alkioiksi* ja merkitään $y = -x$.

1.4. Määritelmä. Ryhmä $(A, +)$ on *Abelin ryhmä*, jos laskutoimitus + on vaihdannainen, ts. kaikille $x, y \in G$ pätee

$$x + y = y + x.$$

Kaikkiaan siis saadaan: Yhden laskutoimituksen rakenne $(A, +)$ on *Abelin ryhmä*, jos

1) + on liitännäinen eli kaikilla $x, y, z \in A$ pätee

$$(x + y) + z = x + (y + z),$$

2) laskutoimituksella + on neutraalialkio e, jolle

$$x + e = e + x = x,$$

kun $x \in A$,

3) jokaisella $x \in A$ on vasta-alkio $-x$, jolle

$$x + (-x) = (-x) + x = e$$

ja

4) $+$ on vaihdannainen, ts. kaikille $x, y \in A$ pätee

$$x + y = y + x.$$

Siirrytään tarkastelussa kahden laskutoimituksen rakenteisiin:

1.5. Määritelmä. Kahden laskutoimituksen rakenne $(R, +, \cdot)$ on *pseudorengas*, jos

1) $(R, +)$ on Abelin ryhmä,
2) $(R, \cdot)$ on puoliryhmä ja
3) yhteen- ja kertolasku osittelevat molemmilta puolilta, ts.

$$x(y + z) = xy + xz \text{ ja } (x + y)z = xz + yz,$$

kun $x, y, x \in R$.

1.6. Määritelmä. Kahden laskutoimituksen rakenne $(R, +, \cdot)$ on *rengas*, jos

1) $(R, +)$ on Abelin ryhmä,
2) $(R, \cdot)$ on monoidi ja
3) yhteen ja kertolasku osittelevat molemmilta puolilta.

(Pseudo)rengas on *vaihdannainen*, jos sen kertolasku on vaihdannainen.

Renkaat $(R, +, \cdot)$ ovat siis *yksiköllisiä* pseudorenkaita, ts. niissä kertolaskulla on neutraalialkio eli on olemassa sellainen $1 \in R$, että kaikille $x \in R$ pätee $x \cdot 1 = 1 \cdot x = x$.

Varoitus: Terminologia ei valitettavasti rengasteoriassa ole yhtenäistä, vaan eri lähteissä renkaalla tarkoitetaan eri asioita. Joskus renkaaksi nimitetään luentojen pseudorengasta, joskus vaihdannaista rengasta.

1.7. Esimerkki.

Seuraavista esimerkeistä suuri osa on Algebra I:stä tuttuja, joten perustelut enimmäkseen ohitetaan. Kohdan d perustelu lykätään myöhemmäksi.

a) Tutut lukujoukot $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat renkaita tavanomaisilla yhteen- ja kertolaskuilla varustettuina.

b) $\mathbb{Z}_m = (\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ on rengas, kun $m \in \mathbb{Z}_+$.

c) Kaikki ylläolevat ovat vaihdannaisia renkaita. Reaalisten 2×2-matriisien rengas $(M_2(\mathbb{R}), +, \cdot)$ ei ole vaihdannainen, missä

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}.$$

d *Gaussin kokonaisluvut* muodostavat renkaan $(G, +, \cdot)$, missä

$$G = \{ a + bi \mid a, b \in \mathbb{Z} \}.$$

e) Toisaalta joukkoa $X = \{ a + b\omega \mid a, b \in \mathbb{Z} \}$, missä $\omega = \sqrt[3]{2}$, ei voi varustaa tavanomaisilla laskutoimituksilla niin, että syntyisi rengas, sillä X ei ole kertolaskun suhteen suljettu (HT).

f) Rakenteet $(m\mathbb{Z}, +, \cdot)$ ovat pseudorenkaita, vaan eivät renkaita, kun $m \in \mathbb{Z}_+$ ja $m \geqslant 2$. Mikään alkioista $x \in m\mathbb{Z}$ ei nimittäin toteuta yhtälöä $x^2 = x$, jonka ykkösalkiot aina toteuttavat.

1.8. Määritelmä. Pseudorengas $\boldsymbol{S} = (S, +', \cdot')$ on pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ *alipseudorengas*, jos $S \subseteq R$ ja $\boldsymbol{S}$ perii laskutoimitukset $\boldsymbol{R}$:ltä, ts. $+' = +|(S \times S)$ ja $\cdot' = \cdot|(S \times S)$. Siis kun $x, y \in S$, niin $x +' y = x + y$ ja $x \cdot' y = x \cdot y$.

Jos tässä tässä $\boldsymbol{S}$ ja $\boldsymbol{R}$ ovat jopa renkaita ja $\boldsymbol{S}$ ei ole ainoastaan renkaan $\boldsymbol{R}$ alipseudorengas, vaan pätee myös $1_{\boldsymbol{S}} = 1_{\boldsymbol{R}}$ eli renkailla on samat ykkösalkiot, niin rengasta $\boldsymbol{S}$ kutsutaan renkaan $\boldsymbol{R}$ *alirenkaaksi*.

Huomautus. Renkaan $\boldsymbol{R}$ alipseudorengas $\boldsymbol{S}$ ei ole siis automaattisesti alirengas, vaikka se itsessään olisikin rengas, sillä on mahdollista, että $1_{\boldsymbol{S}} \neq 1_{\boldsymbol{R}}$ (esimerkkejä laskuharjoituksissa).

1.9. Lause. *(Alipseudorengaskriteetit) Jos $\boldsymbol{S} = (S, +', \cdot')$ on pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ alipseudorengas, niin kaikilla $x, y \in S$ pätee $x - y \in S$ ja $x \cdot y \in S$. Lisäksi $S \neq \emptyset$. Kääntäen: Jos $S \neq \emptyset$ on R:n sellainen osajoukko, että kaikilla $x, y \in S$ pätee $x - y \in S$ ja $x \cdot y \in S$, niin $(S, +', \cdot')$ on $\boldsymbol{R}$:n alipseudorengas, missä $+' = +|(S \times S)$ ja $\cdot' = \cdot|(S \times S)$ ovat perityt laskutoimitukset.*

Todistus. Olkoon $\boldsymbol{S} = (S, +', \cdot')$ pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ alipseudorengas. Tällöin kaikilla $x, y \in S$ pätee $x +' y \in S$, koska $\boldsymbol{S}$ on pseudorengas. Koska $\boldsymbol{S}$ perii $\boldsymbol{R}$:n laskutoimitukset, niin $x + y = x +' y \in S$. Vastaavasti päätellään $x \cdot y \in S$, ts. perimisehdoista seuraa, että joukon S tulee olla $\boldsymbol{R}$:n laskutoimitusten suhteen suljettu. Koska $(S, +')$ on Abelin ryhmä, niin alkiolla $y \in S$ on vasta-alkio $-y \in S$. Siis kun $x, y \in S$, niin $x, -y \in S$ ja $x - y = x + (-y) \in S$. Lopuksi huomataan, että $S \neq \emptyset$, sillä $0 \in S$.

Oletetaan kääntäen, että $S \neq \emptyset$, $S \subseteq R$ ja S on suljettu $\boldsymbol{R}$:n vähennys- ja kertolaskujen suhteen. Tällöin S on myös suljettu yhteenlaskun suhteen, sillä kaikilla $x, y \in S$ pätee $0 = x - x \in S$ ja $x + y = x - (-y) = x - \underbrace{(0 - y)}_{\in S} \in S$. Siis $\boldsymbol{S} = (S, +', \cdot')$, missä $+' = +|(S \times S)$ ja $\cdot' = \cdot|(S \times S)$, on kahden laskutoimituksen rakenne, jossa on $\boldsymbol{R}$:stä perityt laskutoimitukset. Algebra I:llä on osoitettu, että S:n epätyhjyydestä ja vähennyslaskun suhteen sulkeutuneisuudesta seuraa, että $(S, +')$ on Abelin ryhmä. Rakenteen $\boldsymbol{S}$ kertolaskun liitännäisyys ja osittelulaki seuraavat nyt siitä, että ne ovat universaaleja ominaisuuksia (kaikille kolmikoille pätee tietty yhtälö), jotka kaikki periytyvät $\boldsymbol{R}$:stä $\boldsymbol{S}$:ään. Siis $\boldsymbol{S}$ on pseudorengas. □

1.10. Lause. *(Alirengaskriteetit) Jos $\boldsymbol{S} = (S, +', \cdot')$ on renkaan $\boldsymbol{R} = (R, +, \cdot)$ alirengas, niin*

1) $1_{\boldsymbol{R}} \in S$
2) $x - y \in S$, *kun* $x, y \in S$ *ja*
3) $x \cdot y \in S$, *kun* $x, y \in S$.

Kääntäen: Jos $S \subseteq R$ toteuttaa ehdot 1–3, niin $(S, +', \cdot')$ on $\boldsymbol{R}$:n alirengas, missä $+' = +|(S \times S)$ ja $\cdot' = \cdot|(S \times S)$ ovat perityt laskutoimitukset.

Todistus. Koska alirenkaat ovat erityisesti alipseudorenkaita, niin ehdot 2 ja 3 seuraavat edellisestä lauseesta. Ehto 1 seuraa taas suoraan alirenkaan määritelmästä. Käänteinen väite seuraa samaten lauseesta ja määritelmästä, sillä jos $1 \in S$, niin $S \neq \emptyset$. □

Huomautus. Koska sekaannuksen vaara on yleensä olematon, alirakenteen laskutoimituksia merkitään useimmiten samoilla symboleilla kuin ylirakenteen, ts. yo. alirakennetta merkitään $\boldsymbol{S} = (S, +, \cdot)$.

1.11. Esimerkki.

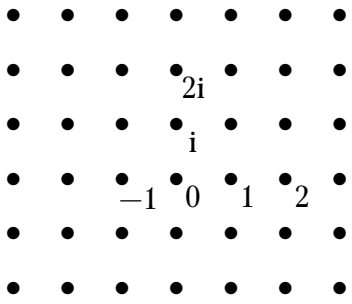
a) Merkitään $G = \{ a + bi \mid a, b \in \mathbb{Z} \}$, ts. G on Gaussin kokonaislukujen joukko. $(G, +, \cdot)$ on $(\mathbb{C}, +, \cdot)$:n alirengas, sillä $1 = 1 + 0 \cdot i \in G \subseteq \mathbb{C}$ ja kun $a, b \in \mathbb{Z}$, niin

$$(a + bi) - (c + di) = \underbrace{(a - c)}_{\in \mathbb{Z}} + \underbrace{(b - d)}_{\in \mathbb{Z}} i \in G$$

ja

$$(a + bi) \cdot (c + di) = \underbrace{(ac - bd)}_{\in \mathbb{Z}} + \underbrace{(bc + ad)}_{\in \mathbb{Z}} i \in G.$$

Gaussin kokonaislukuja tarkasteltaessa on hyvä pitää mielessä niiden geometrinen tulkinta: Kun joukon G pisteet sijoitetaan kompleksilukujen tasoon, ne muodostavat hilapisteistön.



b) Merkitään $\omega = \sqrt[3]{2}$ ja $Y = \{ a + b\omega + c\omega^2 \mid a, b, c \in \mathbb{Z} \}$. Tällöin $(Y, +, \cdot)$ on $(\mathbb{C}, +, \cdot)$:n alirengas (HT).

Huomautus. Yleensä kohdassa a merkittäisiin $G = \mathbb{Z}[i]$ ja tässä kohdassa $Y = \mathbb{Z}[\omega]$, mutta ko. merkintään liittyy se sisäänrakennettu oletus, että joukko on renkaan perusjoukko, jota tässä pyrittiin nimenomaan selvittämään. Näistä merkinnöistä tarkemmin myöhemmin.

1.12. Määritelmä. Pseudorenkaan $(R, +, \cdot)$ alkio a *jakaa* alkion $b \in R$, $a \mid b$, jos on olemassa $r \in R$, jolle $ra = b$. Voidaan myös sanoa, että a on alkion b *tekijä*.

Huomautus. Tarkemmin ottaen voitasiin erotella toisistaan oikealta ja vasemmalta jakamiset, jotka eroavat sen mukaan, kirjoitetaanko ehto muotoon $ra = b$ vai $ar = b$, ja jopa yleisempi tekijärelaatio, jossa vaaditaan kertoimien r, s olemassaoloa, joille $ras = b$. Koska tämän kurssin kiinnostus kohdistuu tekijärelaatioon siinä rajoitetussa tilanteessa, jossa rengas on vaihdannainen tai jopa kokonaisalue, erottelun tekeminen on tässä epäoleellista.

1.13. Esimerkki. a) Renkaassa $(\mathbb{Z}, +, \cdot)$ pätee $2 \nmid 3$, mutta renkaassa $(\mathbb{Q}, +, \cdot)$ on voimassa $2 \mid 3$, sillä $3 = \frac{3}{2} \cdot 2$.

1.14. Lause. *Pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ jakorelaatio on transitiivinen, ts. jos $a \mid b$ ja $b \mid c$, niin $a \mid c$, kun $a, b, c \in R$. Renkaassa $\boldsymbol{R}$ jakorelaatio on myös refleksiivinen eli kaikilla $a \in R$ pätee $a \mid a$.*

Todistus. Olkoot $a, b, c \in R$ alkiot, joille $a \mid b$ ja $b \mid c$. Tällöin on olemassa kertoimet $r, s \in R$, joille $ra = b$ ja $sb = c$. Tästä seuraa

$$c = sb = s(ra) = (sr)a \text{ eli } a \mid c.$$

Jos $\boldsymbol{R}$ on rengas, niin jokaisella $a \in R$ pätee $a = 1 \cdot a$ eli $a \mid a$. □

Lauseen tuloksen voi ilmaista niin, että renkaan jakorelaatio on kvasijärjestys. Koska pseudorenkaassa $\boldsymbol{R} = (R, +, \cdot)$ pätee aina $0 \cdot a = 0$, niin $a \mid 0$, kun $a \in R$. 0 on siis tässä mielessä jakojärjestyksen suurin alkio. Jos $\boldsymbol{R}$ on rengas, niin vastaavasti kaikilla $a \in R$ on voimassa $a = a \cdot 1$ eli $1 \mid a$, joten pienin alkio tässä mielessä on 1. Koska kyse on vain kvasijärjestyksestä, niin pienimpiä alkioita voi tosin olla useita.

1.15. Esimerkki. Varustetaan perusjoukko

$$^{\mathbb{R}}\mathbb{R} = \{ f \mid f\colon \mathbb{R} \to \mathbb{R} \}$$

pisteittäisillä laskutoimituksilla:

$$f + g\colon \mathbb{R} \to \mathbb{R}, \quad (f + g)(x) = f(x) + g(x),$$
$$f \cdot g\colon \mathbb{R} \to \mathbb{R}, \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

Voidaan osoittaa, että näin syntyvä rakenne $\boldsymbol{R} = (^{\mathbb{R}}\mathbb{R}, +, \cdot)$ on rengas; analysoidaan sen jakojärjestystä. Merkitään

$$\operatorname{supt}(f) = \{ x \in \mathbb{R} \mid f(x) \neq 0 \},$$

kun $f \in {}^{\mathbb{R}}\mathbb{R}$. Jos alkioille $f, g \in {}^{\mathbb{R}}\mathbb{R}$ pätee $f \mid g$ ja kohdassa $x \in \mathbb{R}$ on voimassa $f(x) = 0$, niin myös $g(x) = 0$, sillä jollakin $h \in {}^{\mathbb{R}}\mathbb{R}$ pätee $g = h \cdot f$ ja siten $g(x) = h(x)f(x) = 0$. Siis relaatiosta $f \mid g$ seuraa $\operatorname{supt}(f) \supseteq \operatorname{supt}(g)$. Kääntäen: jos $\operatorname{supt}(f) \supseteq \operatorname{supt}(g)$, niin voidaan määritellä

$$h\colon \mathbb{R} \to \mathbb{R},\ h(x) = \begin{cases} g(x)f(x)^{-1}, & \text{kun } x \in \operatorname{supt}(g) \\ 0, & \text{muuten,} \end{cases}$$

jolloin $g = h \cdot f$ ja siten $f \mid g$.

Renkaassa $\boldsymbol{R}$ nolla-alkio on nollakuvaus $0\colon \mathbb{R} \to \mathbb{R}$, $0(x) = 0$, jonka pystyy jakamaan tekijöihin epätriviaaleilla tavoilla: Kun $a \in \mathbb{R}$, merkitään

$$\delta_a\colon \mathbb{R} \to \mathbb{R},\ \delta_a(x) = \begin{cases} 1, & \text{kun } x = a \\ 0, & \text{muuten.} \end{cases}$$

Jos $a, b \in \mathbb{R}$ ovat eri lukuja, niin $\delta_a \cdot \delta_b = 0$. Näiden ns. nollatekijöiden olemassaolo on rengasteorian kannalta usein tilannetta komplisoiva asia.

1.16. Määritelmä. Vaihdannainen rengas $\boldsymbol{R} = (R, +, \cdot)$ on *kokonaisalue*, jos se toteuttaa *supistussäännön*: kaikilla $a, b, c \in R$, jos $ab = ac$ ja $a \neq 0$, niin $b = c$.

1.17. Lause. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas. Tällöin $\boldsymbol{R}$ on kokonaisalue, jos ja vain jos tulon nollasääntö on voimassa eli kun $a, b \in R$ ja $ab = 0$, niin $a = 0$ tai $b = 0$.*

Todistus. Jos $\boldsymbol{R}$ on kokonaisalue ja $ab = 0$, mutta $a \neq 0$, niin supistussäännön mukaan yhtälöstä $ab = a \cdot 0$ seuraa $b = 0$.

Oletetaan kääntäen, että tulon nollasääntö on voimassa vaihdannaisessa renkaassa $\boldsymbol{R}$. Olkoon $a, b, c \in R$ alkioita, joille $ab = ac$ ja $a \neq 0$. Tällöin

$$ab = ac \Rightarrow a(b-c) = ab - ac = 0 \underset{(a \neq 0)}{\Rightarrow} b - c = 0 \Rightarrow b = c. \quad \square$$

1.18. Lause. *Olkoon* $(R, +, \cdot)$ *pseudorengas ja* a, b, c, r, s *sen alkioita, joille* $a \mid b$ *ja* $a \mid c$. *Tällöin* $a \mid rb + sc$.

Todistus. Koska $a \mid b$ ja $a \mid c$, niin on olemassa alkiot $x, y \in R$, joille $xa = b$ ja $ya = c$. Siis

$$rb + sc = r(xa) + s(ya) = (rx + sy)a,$$

joten $a \mid rb + sc$. $\square$

1.19. Määritelmä. Vaihdannaisen renkaan $\boldsymbol{R}$ alkiota u kutsutaan *yksiköksi*, jos $u \mid 1$.

1.20. Esimerkki.

a) Kokonaislukujen renkaan yksiköt ovat 1 ja -1.
b) Missä tahansa kunnassa $\boldsymbol{K} = (K, +, \cdot)$ yksikköjä ovat kaikki nollasta eroavat alkiot, sillä kun $k \in K \setminus \{0\}$, niin $k \cdot k^{-1} = 1$, joten $k \mid 1$.
c) Renkaassa ykkösalkio on aina yksikkö.

Edellä todettiin jo, että jakorelaatio on kvasijärjestys. Kvasijärjestys ei välttämättä toteuta antisymmetrisyyttä, mikä tarkasteltavassa tapauksessa tarkoittaa, että on mahdollista, että eri alkioille a ja b pätee $a \mid b$ ja $b \mid a$.

1.21. Määritelmä. Pseudorenkaan $\boldsymbol{R}$ alkiot a ja b ovat *liittoalkioita*, jos $a \mid b$ ja $b \mid a$.

1.22. Lause. *Olkoon* $\boldsymbol{R} = (R, +, \cdot)$ *kokonaisalue ja* $a, b \in R$. *Tällöin* a *ja* b *ovat liittoalkioita, jos ja vain jos jollakin yksiköllä* $u \in R$ *pätee* $b = ua$.

Todistus. Jos a ja b ovat liittoalkioita, niin joillakin $u \in R$ ja $v \in R$ pätee $b = ua$ ja $a = vb$. Jos $a = 0$, niin $b = u \cdot 0 = 0$ ja $b = 0 = 1 \cdot 0 = 1 \cdot a$. Oletetaan siis, että $a \neq 0$. Koska

$$1 \cdot a = a = vb = v(ua) = (vu)a,$$

niin supistussäännön (ja vaihdantalain) nojalla $vu = 1$, joten $u \mid 1$. Siis u on yksikkö, jolle $b = ua$.

Oletetaan kääntäen, että jollakin yksiköllä u pätee $b = ua$. Selvästi $a \mid b$, mutta lisäksi havaitaan, että koska u on yksikkö, niin on olemassa $v \in R$, jolle $uv = 1$. Siis $vb = v(ua) = (uv)a = 1 \cdot a = a$, joten myös $b \mid a$. Siis a ja b ovat liittoalkioita. $\square$

1.23. Lause. *Olkoon* $\boldsymbol{R} = (R, +, \cdot)$ *vaihdannainen rengas. Merkitään* $U(\boldsymbol{R})$*:llä renkaan* $\boldsymbol{R}$ *yksiköiden joukkoa. Tällöin* $(U(\boldsymbol{R}), \cdot)$ *on Abelin ryhmä.*

Todistus. Koska renkaassa $\boldsymbol{R}$ on ykkösalkio, niin $1 \in U(\boldsymbol{R})$. Jos $u \in R$ on yksikkö eli $u \mid 1$, niin on olemassa $v \in R$, jolle $vu = 1$. Koska $\boldsymbol{R}$ on vaihdannainen rengas, niin $uv = vu = 1$,

mistä seuraa, että myös $v = u^{-1}$ on yksikkö. Siis $U(\boldsymbol{R})$ on käänteisalkioiden suhteen suljettu. Kun $u, v \in U(\boldsymbol{R})$, niin

$$(v^{-1}u^{-1})uv = v^{-1}(u^{-1}u)v = v^{-1} \cdot 1 \cdot v = v^{-1} \cdot v = 1,$$

joten $uv \mid 1$ eli $uv \in U(\boldsymbol{R})$. Siis $U(\boldsymbol{R})$ on suljettu myös kertolaskun suhteen. Rakenteessa $(U(\boldsymbol{R}), \cdot)$ on voimassa liitäntälaki ja vaihdantalaki, koska ne ovat kertolaskulle voimassa myös renkaassa $\boldsymbol{R}$. Koska rakenteella $(U(\boldsymbol{R}), \cdot)$ on myös neutraalialkio ja kullakin sen alkiolla käänteisalkiot, se on Abelin ryhmä. □

2. Polynomirenkaat

2.1. Lause. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannaisen renkaan $\boldsymbol{S} = (S, +, \cdot)$ alirengas ja $t \in S$. Tällöin on olemassa suppein $\boldsymbol{S}$:n alirengas $\boldsymbol{R}' = (R', +, \cdot)$, jolle $R \subseteq R'$ ja $t \in R'$. Lisäksi*

$$R' = \{\, a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R \,\}.$$

Todistus. Merkitään

$$R' = \{\, a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R \,\}$$

ja todistetaan, että R':lla on halutut ominaisuudet.

Olkoon $(\boldsymbol{R}^*, +, \cdot)$ $\boldsymbol{S}$:n alirengas, jolle $R \subseteq R^*$ ja $t \in R^*$. (Tällaisia on tietenkin olemassa, sillä $\boldsymbol{S}$ on itse tällainen.) Induktiolla seuraan suoraan, että $t^n \in R^*$ kaikilla $n \in \mathbb{Z}_+$. Tästä seuraa edelleen, että kaikilla $a \in R$ ja $n \in \mathbb{Z}_+$ pätee $at^n \in R^*$. Siis kaikille $n \in \mathbb{Z}_+$ ja $a_0, \ldots, a_n \in R$ pätee

$$a_0 + a_1 t + \cdots + a_n t^n \in R^*,$$

ts. $R' \subseteq R^*$.

$\boldsymbol{R}' = (R', +, \cdot)$ on siis suppein $\boldsymbol{S}$:n alirengas, jolle $R \subseteq R'$ ja $t \in R'$, kunhan osoitetaan, että $\boldsymbol{R}'$ on ylipäänsä alirengas. Ensiksikin havaitaan, että $1 \in R \subseteq R'$. Olkoot $a, b \in R'$, jolloin on olemassa $m, n \in \mathbb{Z}_+$, $a_0, \ldots, a_m \in R$ ja $b_0, \ldots, b_n \in R$, joille $a = a_0 + \cdots + a_m t^m$ ja $b = b_0 + \cdots + b_n t^n$. Lisäämällä esityksiin tarvittaessa nollakertoimia voidaan olettaa, että $m = n$. Tarkistetaan muutkin alirengaskriteerit: Koska vaihdantalait pätevät,

$$\begin{aligned} a - b &= (a_0 + a_1 t \cdots + a_n t^n) - (b_0 + b_1 t \cdots + b_n t^n) \\ &= (a_0 - b_0) + (a_1 - b_1)t \cdots + (a_n - b_n)t^n \in R' \end{aligned}$$

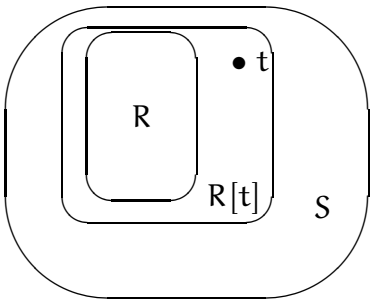
ja

$$\begin{aligned} ab &= (a_0 + a_1 t \cdots + a_n t^n) \cdot (b_0 + b_a t \cdots + b_n t^n) \\ &= \Big(\sum_{j=0}^{m} a_j t^j\Big)\Big(\sum_{k=0}^{n} b_k t^k\Big) = \sum_{j=0}^{m}\sum_{k=0}^{n}(a_j t^j)(b_k t^k) \\ &= \sum_{j\in\{0,\ldots,m\},\, k\in\{0,\ldots,n\}} a_j b_k t^{k+j} = \sum_{i=0}^{m+n} \underbrace{\left(\sum_{j=0}^{m} a_j b_{i-j}\right)}_{\in R} t^i \in R'. \quad \square \end{aligned}$$

2.2. Merkintä. Edellisen lauseen perusteella merkitään

$$R[t] = \{ a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R \},$$

kun rengas $\boldsymbol{R} = (R, +, \cdot)$ on vaihdannainen rengas ja t on jonkin $\boldsymbol{R}$:n rengaslaajennuksen $\boldsymbol{S}$ alkio.



Huomautus. Edellisen lauseen voisi muotoilla myös yleisemmillä oletuksilla pseudorenkaille. Ykkösalkion olemassaolosta ja jopa vaihdannaisuuden vaatimuksista olisi mahdollista luopua, mutta silloin suppein alkion t sisältävä $\boldsymbol{R}$:n rengaslaajennus olisi vaikeampi kuvailla. Koska lause on alustusta polynomirenkaiden tarkasteluun ja polynomirenkaita harvoin tarkastellaan tapauksissa, joissa on kerroinrengas on kovin epäsäännöllinen, niin nämä yleistykset jätetään tässä esittämättä.

2.3. Esimerkki.

a) Tarkastellaan edellistä lausetta seuraavassa tilanteessa: Kokonaislukujen rengas $(\mathbb{Z}, +, \cdot)$ on kompleksilukujen kunnan $(\mathbb{C}, +, \cdot)$ alirengas ja $i \in \mathbb{C}$. Koska $i^2 = -1$, $i^3 = -i$ ja $i^4 = 1$, niin yleisemmin pätee kaikilla $k \in \mathbb{N}$

$$i^{4k} = 1,\ i^{4+1} = i,\ i^{4k+2} = -1 \text{ ja } i^{4k+3} = -i.$$

Tästä seuraa

$$\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \},$$

ts. Gaussin kokonaislukuihin päädytään lisäämällä kokonaislukuihin imaginaariyksikkö.

b) Toisaalta jos kokonaislukujen tilalle vaihdetaan rationaalilukujen kunta $(\mathbb{Q}, +, \cdot)$, jota laajennetaan (renkaana) alkiolla π, niin päädytään renkaaseen $(\mathbb{Q}[\pi], +, \cdot)$, missä

$$\mathbb{Q}[\pi] = \Big\{ \sum_{k=0}^{n} a_k \pi^k \;\Big|\; k \in \mathbb{N},\ a_0, \ldots, a_k \in \mathbb{Q} \Big\}.$$

Tässä tapauksessa $\mathbb{Q}[\pi]$:lle ei voi kirjoittaa yksinkertaisempaa esitystä, sillä tunnetusti π on transkendenttiluku, mikä tarkoittaa, että $\sum_{k=0}^{n} a_k \pi^k \neq 0$, mikäli jokin kertoimista $a_0, \ldots, a_k \in \mathbb{Q}$ eroaa nollasta. Tästä seuraa, että $\sum_{k=0}^{n} a_k \pi^k \neq \sum_{k=0}^{n} b_k \pi^k$, jos $a_i \neq b_i$ jollakin $i \in \{0, \ldots n\}$.

Esimerkki herättää sen luonnollisen kysymyksen, voidaanko annettua rengasta aina laajentaa jollain sellaisella alkiolla, että laajennukseen syntyvien polynomilausekkeiden välillä

ei olisi epätriviaaleja riippuvuuksia. Seuraava määritelmä on myönteinen vastaus tähän kysymykseen.

2.4. Määritelmä. Vaihdannaisen renkaan $\boldsymbol{R} = (R, +, \cdot)$ polynomirengas on $\boldsymbol{R}[x] = (R[x], +, \cdot)$, missä

$$\begin{aligned}\boldsymbol{R}[x] &= \{\, (a_0, a_1, a_2, \ldots, a_n, \ldots) \mid a_i \in R, \text{ vain äärellisen monella } i \in \mathbb{N} \text{ pätee } a_i \neq 0 \,\} \\ &= \{\, a : \mathbb{N} \to R \mid \operatorname{supt}(a) \text{ on äärellinen} \,\}\end{aligned}$$

ja

$$\operatorname{supt}(a) = \{\, i \in \mathbb{N} \mid a_i \neq 0 \,\},$$

varustettuna seuraavilla yhteen- ja kertolaskuilla: kun $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots) \in R[x]$, niin

$$a + b = (a_0 + b_0, a_1 + b_1, \ldots) = (a_n + b_n)_{n \in \mathbb{N}}$$

ja

$$ab = \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_{n \in \mathbb{N}} = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots).$$

Seuraava tulos on käyty läpi Algebra 1:ssä.

2.5. Lause. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas. Tällöin sen polynomirengas on myös vaihdannainen rengas. Jos $\boldsymbol{R}$ on kokonaisalue, myös $\boldsymbol{R}[x]$ on.* □

2.6. Merkintä. Määritelmän tilanteessa merkitään

$$x = (0, 1, 0, 0, 0, \ldots).$$

Havaitaan, että kaikilla $k \in \mathbb{N}$ pätee

$$x^k = (\underbrace{0, \ldots, 0}_{k \text{ kpl}}, 1, 0, 0, \ldots),$$

mistä edelleen seuraa, että kaikilla $n \in \mathbb{N}$ ja $a_0, a_1, \ldots, a_n \in R$ pätee

$$\sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + \cdots + a_n x^n = (a_0, a_1, a_2, \cdots, a_n, 0, 0, \ldots).$$

Renkaan $\boldsymbol{R}[x]$ alkioita kutsutaan R-kertoimisiksi *polynomeiksi*, ja polynomin $a \in R[x]$ *aste* $\deg(a) = \max\{\, i \in \mathbb{N} \mid a(i) \neq 0 \,\}$, jos $a \neq 0$. Asetetaan lisäksi $\deg(0) = -\infty$. Yhtäpitävästi: $\deg(a) = n \in \mathbb{N}$ tarkoittaa, että on olemassa $a_0, a_1, \ldots, a_n \in R$, $a_n \neq 0$, joille

$$a = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + \cdots + a_n x^n.$$

Huomautus. Näennäisesti merkinnät 2.2 ja 2.6 ovat keskenään ristiriitaisia: toisaalta $\boldsymbol{R}[x]$ viittaa polynomirenkaaseen, toisaalta jos $\boldsymbol{S}$ on tuo polynomirengas, niin $\boldsymbol{R}[x]$:n voi ymmärtää olevan renkaan $\boldsymbol{R}$ suppein laajennus, joka sisältää alkion x. Edellä tehty tarkastelu kuitenkin osoittaa, että ristiriita on vain näennäinen.

2.7. Lause. *Olkoon* $\boldsymbol{R} = (R, +, \cdot)$ *vaihdannainen rengas ja* $a, b \in R[x]$. *Tällöin*

$$\deg(a + b) \leqslant \max\{\deg(a), \deg(b)\} \text{ ja } \deg(ab) \leqslant \deg(a) + \deg(b).$$

Yhtäsuuruudet pätevät seuraavilla lisäoletuksilla: Jos $\deg(a) \neq \deg(b)$, *niin* $\deg(a + b) = \max\{\deg(a), \deg(b)\}$. *Jos* $\boldsymbol{R}$ *on kokonaisalue, niin* $\deg(ab) = \deg(a) + \deg(b)$.

Todistus. Jos $a = 0$ tai $b = 0$, niin on ilmeistä, että väitteet pätevät. Oletetaan siis, että $a, b \neq 0$ ja merkitään $m = \deg(a)$ ja $n = \deg(b)$. Merkitään $a = \sum_{i=0}^{m} a_i x^i$ ja $b = \sum_{j=0}^{n} b_j x^j$, missä $a_m \neq 0$ ja $b_n \neq 0$. Merkitään $a_i = 0$ ja $b_j = 0$, kun $i, j \in \mathbb{N}$, $i > m$ ja $j > n$. Tällöin

$$a + b = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i)x^i \Rightarrow \deg(a + b) \leqslant \max\{m, n\}$$

ja tulossa

$$ab = \left(\sum_{i=0}^{k} a_i b_{k-i} \right)_{k \in \mathbb{N}}$$

kerroin $\sum_{i=0}^{k} a_i b_{k-i}$ on nolla, kun $k \in \mathbb{N}$, $k > m + n$, sillä tällöin kaikilla $i \in \{0, \ldots, k\}$ joko $i > m$ tai $j > n$. Tässä käytettiin siis polynomin muodollista määritelmää, jonka mukaan polynomit a ja b ovat R:n alkioiden jonoja, ja saatiin selville, että

$$ab = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k \text{ ja } \deg(ab) \leqslant m + n.$$

Jos $\boldsymbol{R}$ on kokonaisalue, niin asteen $m+n$ kerroin ab:ssa on $a_m b_n \neq 0$, joten $\deg(ab) = m+n$. Jos $\deg(a) \neq \deg(b)$, niin asteen $\max\{m, n\}$ kerroin $a + b$:ssä on $a_{\max\{m,n\}} + b_{\max\{m,n\}}$ on joko $a_m \neq 0$ tai $b_n \neq 0$, mistä seuraa $\deg(a + b) = \max\{m, n\}$. □

Rengasteorian keskeisenä esimerkkinä algebran peruskursseilla on kokonaislukujen rengas $(\mathbb{Z}, +, \cdot)$, jonka rinnalle tässä kohoaa reaalilukujen polynomirengas $(\mathbb{R}[x], +, \cdot)$ toiseksi keskeiseksi esimerkiksi. Kun rengasteoriaan tutustuu kokonaislukujen rengasta mielessä pitäen, havaitsee opettavaisen seikan, nimittäin että paljon alkeellista lukuteoriaa pystytään tulkitsemaan algebrallisesti. Esimerkiksi jaollisuusrelaatio ja sen monet ominaisuudet yleistyvät varsin suoraviivaisesti yksiköllisiin vaihdannaisiin renkaisiin. Myöhemmin paneudumme niihin asioihin, jotka ovat jääneet selvittämättä: miten alkulukujen käsite yleistyy renkaisiin, ja onko aritmetiikan peruslauseella, joka koskee kokonaislukujen alkulukuesityksiä, vastineensa. Myös kongruenssilaskennalla on luonnollinen algebrallinen tulkintansa, nimittäin kokonaislukujen renkaan tekijärenkaiden avulla, mihin tartumme seuraavaksi.

3. Homomorfismit, ideaalit ja tekijärenkaat

3.1. Määritelmä. *Homomorfismi* pseudorenkaasta $\boldsymbol{R} = (R, +, \cdot)$ pseudorenkaaseen $\boldsymbol{S} = (S, +', \cdot')$ on kuvaus $h\colon R \to S$, jolle pätee

$$h(x + y) = h(x) +' h(y) \quad \text{ja} \quad h(x \cdot y) = h(x) \cdot' h(y),$$

kun $x, y \in R$. *Homomorfismi* renkaasta $\boldsymbol{R} = (R, +, \cdot)$ renkaaseen $\boldsymbol{S} = (S, +', \cdot')$ on kuvaus $h\colon R \to S$, joka toteuttaa lisäksi ehdon

$$h(1_{\boldsymbol{R}}) = h(1_{\boldsymbol{S}}).$$

Jos halutaan selventää, minkätyyppisestä homomorfismista on kyse, voidaan edellisessä tapauksessa puhua *pseudorengashomomorfismeista* ja jälkimmäisessä *rengashomomorfismeista*.

Jos homomorfismi on injektio, sitä kutsutaan *monomorfismiksi*, ja jos surjektio, niin *epimorfismiksi*. Jos h on sekä mono- että epimorfismi, niin se on *isomorfismi*, mitä merkitään $h\colon \boldsymbol{R} \cong \boldsymbol{S}$. Homomorfismia (pseudo)renkaasta $\boldsymbol{R}$ itselleen kutsutaan *endomorfismiksi* ja isomorfismia *automorfismiksi*.

3.2. Määritelmä. Pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ osajoukko $I \subseteq R$ on pseudorenkaan $\boldsymbol{R}$ *ideaali*, jos

a) $(I, +, \cdot)$ on $\boldsymbol{R}$:n alipseudorengas ja
b) kaikilla $x \in I$ ja $r \in R$ pätee $rx, xr \in I$.

Huomautus. Tässä esitetyt ehdot voidaan purkaa alipseudorengaskriteerin 1.9 avulla. Näistä kriteereistä se, joka kertoo, että I on suljettu kertolaskun suhteen, on heikompi kuin ehto b, joten tällöin jäljelle jäävät ehto b ja

a') $I \neq \emptyset$ ja kaikilla $x, y \in I$ pätee $x - y \in I$.

3.3. Määritelmä. Joukon R ekvivalenssirelaatio $\sim$ on pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ *kongruenssi*, jos kaikilla $x, x', y, y' \in R$, joille $x \sim x'$ ja $y \sim y'$, pätee $x+y \sim x'+y'$ ja $xy \sim x'y'$. Kongruenssia vastaava *tekijäpseudorengas* $\boldsymbol{R}/\!\sim = (R/\!\sim, +, \cdot)$ on pseudorengas, jonka perusjoukko on

$$R/\!\sim \; = \{\, [x]_\sim \mid x \in R \,\},$$

missä $[x]_\sim = \{\, y \in R \mid x \sim y \,\}$ on alkion x ekvivalenssiluokka kongruenssissa $\sim$. $R/\!\sim$ on siis kongruenssia $\sim$ vastaava ositus. Laskutoimitukset määritellään niin, että

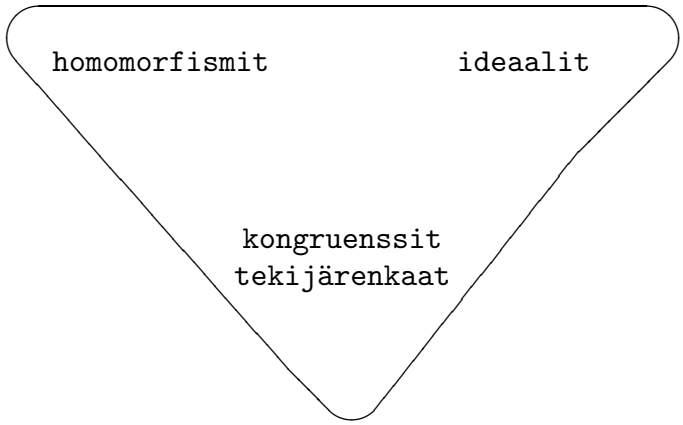
$$[x]_\sim + [y]_\sim = [x + y]_\sim$$

ja

$$[x]_\sim \cdot [y]_\sim = [x \cdot y]_\sim$$

Huomautus. Kongruenssilta siis vaaditaan täsmälleen se, että edellä määritellyt laskutoimitukset ovat hyvinmääriteltyjä.

Edellä on esitetty kolmeen eri käsiteluokkaan liittyvät määritelmät:



Kuvio pyrkii korostamaan sitä, että vaikka kyse on muodoltaan hyvin erilaisista käsitteistä, niin rengasteoriassa nämä muodostavat vain erilaiset näkökulmat pohjimmiltaan samaan asiaan. Aloitetaan luomalla yhteys ideaalien ja kongruenssien välille.

3.4. Lause. *Olkoon* $\boldsymbol{R} = (R, +, \cdot)$ *pseudorengas ja* $\sim$ *sen kongruenssi. Tällöin* $I = [0]_\sim = \{ x \in R \mid x \sim 0 \}$ *on pseudorenkaan* $\boldsymbol{R}$ *ideaali. Lisäksi kaikilla* $x, y \in R$ *pätee*

$$x \sim y \iff x + I = y + I,$$

missä $x + I = \{ x + t \mid t \in I \}$. *Kääntäen: Jos* I *on* $\boldsymbol{R}$*:n ideaali, niin ehdolla* $x \sim y \iff x + I = y + I$ *määritelty ekvivalenssirelaatio on kongruenssi, jolle* $I = [0]_\sim$

Todistus. Olkoon $\sim$ pseudorenkaan $\boldsymbol{R}$ kongruenssi ja $I = [0]_\sim$. Triviaalisti $I \neq \emptyset$. Olkoot $x, y \in I$, $r \in R$. Tällöin $x \sim 0$ ja $y \sim 0$. Koska $\sim$ on kongruenssi, niin ehdoista $y \sim 0$ ja $-y \sim -y$ seuraa $y + (-y) \sim 0 + (-y)$ eli $0 \sim -y$. Edelleen $x \sim 0, -y \sim 0 \Rightarrow x - y = x + (-y) \sim 0 + 0 = 0$. Siis $x - y \in I$ ja I on vähennyslaskun suhteen suljettu. Lopuksi havaitaan, että koska $x \sim 0$ ja $r \sim r$, niin $x \cdot r \sim 0 \cdot r = 0$ ja $r \cdot x \sim r \cdot 0 = 0$. Siis $xr, rx \in I$. Tämä osoittaa, että I on $\boldsymbol{R}$:n ideaali.

Olkoot $x, y \in R$. Koska joka tapauksessa $y \sim y$ ja $-y \sim -y$, niin

$$\begin{aligned} x \sim y &\iff (-y) + x \sim (-y) + y = 0 \\ &\iff x - y = -y + x \in I \iff x + I = y + \underbrace{(-y) + x + I}_{=I} = y + I. \end{aligned}$$

Olkoon kääntäen I pseudorenkaan $\boldsymbol{R}$ ideaali. Määritellään joukon R ekvivalenssirelaatio $\sim$ ehdolla

$$x \sim y \iff x + I = y + I \iff x - y \in I,$$

kun $x, y \in R$. (Koska relaatio $\sim$ vastaa kuvausta $x \mapsto x + I$, on selvää, että se on ekvivalenssirelaatio.) Tarkastetaan, että $\sim$ on kongruenssi. Olkoot $x, y, x', y' \in R$. Jos $x \sim x'$ ja $y \sim y'$, niin $x - x' \in I$ ja $y - y' \in I$, joten

$$(x + y) - (x' + y') = (x - x') + (y - y') \in I$$

ja

$$xy - x'y' = xy - xy' + xy' - x'y' = \underbrace{x(y - y')}_{\in I} + \underbrace{(x - x')y'}_{\in I} \in I,$$

joten $x + y \sim x' + y'$ ja $xy \sim x'y'$.

Koska kaikilla $x \in R$ pätee $x \sim 0 \iff x = x - 0 \in I$, niin $I = [0]_\sim$. □

Seuraavaksi luodaan yhteys homomorfismien ja ideaalien välille.

3.5. Määritelmä. Olkoon h homomorfismi pseudorenkaasta $(R, +, \cdot)$ pseudorenkaaseen $(S, +, \cdot)$. Tällöin joukkoa

$$\operatorname{Ker} h = \{ x \in R \mid h(x) = 0 \} = h^{-1}\{0\}$$

kutsutaan kuvauksen h *ytimeksi*, ja joukkoa

$$\operatorname{Im} h = \{ h(x) \mid x \in R \} = h[R]$$

kuvaksi.

3.6. Lause. *Olkoon h homomorfismi pseudorenkaasta $\boldsymbol{R} = (R, +, \cdot)$ pseudorenkaaseen $(S, +, \cdot)$. Tällöin* $\operatorname{Ker} h$ *on $\boldsymbol{R}$:n ideaali ja* $(\operatorname{Im} h, +, \cdot)$ *on $\boldsymbol{S}$:n alipseudorengas.*

Todistus. Määritellään pseudorenkaan $\boldsymbol{R}$ ekvivalenssi $\sim$ ehdon $x \sim y \iff h(x) = h(y)$, kun $x, y \in R$, avulla. Ekvivalenssi on kongruenssi, sillä kun $x \sim x'$ ja $y \sim y'$, niin $h(x) = h(x')$ ja $h(y) = h(y')$, mistä kuvauksen h homomorfisuuden nojalla seuraa

$$h(x + y) = h(x) + h(y) = h(x') + h(y') = h(x' + y')$$

ja

$$h(x \cdot y) = h(x) \cdot h(y) = h(x') \cdot h(y') = h(x' \cdot y')$$

eli $x + y \sim x' + y'$ ja $xy \sim x'y'$.

Edellisen lauseen perusteella

$$[0]_\sim = \{ x \in R \mid x \sim 0 \} = \{ x \in R \mid h(x) = h(0) = 0 \} = h^{-1}\{0\} = \operatorname{Ker} h$$

on pseudorenkaan $\boldsymbol{R}$ ideaali.

Osoitetaan seuraavaksi, että $(\operatorname{Im} h, +, \cdot)$ on pseudorenkaan $\boldsymbol{S}$ alipseudorengas. Selvästi $\operatorname{Im} h \neq \emptyset$. Olkoot $a, b \in \operatorname{Im} h$,ts. joillakin $x, y \in R$ pätee $h(x) = a$ ja $h(y) = b$. Tällöin

$$a - b = h(x) - h(y) = h(x) + h(-y) = h(x + (-y)) = h(x - y)$$

ja

$$ab = h(x)h(y) = h(xy),$$

joten $a - b, ab \in \operatorname{Im} h$, ts. $(\operatorname{Im} h, +, \cdot)$ täyttää alipseudorengaskriteerit. □

3.7. Seuraus. *Olkoon h homomorfismi renkaasta $\boldsymbol{R} = (R, +, \cdot)$ renkaaseen $(S, +, \cdot)$. Tällöin* $\operatorname{Ker} h$ *on $\boldsymbol{R}$:n ideaali ja* $(\operatorname{Im} h, +, \cdot)$ *on $\boldsymbol{S}$:n alirengas.*

Todistus. Lauseeseen verrattuna oletus on vahvistunut sen verran, että vaaditaan $h(1_{\boldsymbol{R}}) = 1_{\boldsymbol{S}}$, mistä seuraa, että $1_{\boldsymbol{S}} \in \operatorname{Im} h$. Tämä takaa sen, että $(\operatorname{Im} h, +, \cdot)$ ei ole pelkästään $\boldsymbol{R}$:n alipseudorengas, vaan jopa alirengas. □

3.8. Esimerkki. Olkoon $\boldsymbol{R} = (R, +, \cdot)$ pseudorengas ja $\sim$ sen kongruenssi.

a) Tällöin kuvaus $p\colon R \to R/\sim$, $p(x) = [x]_\sim$ on homomorfismi pseudorenkaasta $\boldsymbol{R}$ tekijäpseudorenkaaseen $\boldsymbol{R}/\sim$ suoraan laskutoimitusten määritelmien nojalla: kun $x, y \in R$, niin

$$p(x + y) = [x + y]_\sim = [x]_\sim + [y]_\sim = p(x) + p(y) \text{ ja}$$
$$p(x \cdot y) = [xy]_\sim = [x]_\sim \cdot [y]_\sim = p(x)p(y).$$

Kuvausta p kutsutaan usein *kanoniseksi homomorfismiksi*. Koska tekijäpseudorenkaan nolla-alkio on $[0]_\sim = p(0)$, niin

$$\operatorname{Ker} p = \{\, x \in R \mid p(x) = [0]_\sim \,\} = \{\, x \in R \mid [x]_\sim = [0]_\sim \,\} = \{\, x \in R \mid x \sim 0 \,\} = [0]_\sim.$$

Kaikki pseudorenkaiden ideaalit ovat siis homomorfismien ytimiä: Olkoon I pseudorenkaan $\boldsymbol{R}$ ideaali. Ideaalia I vastaava kongruenssi $\sim$ määräytyy ehdosta $x \sim y \iff x - y \in I$. Tällöin $I = [0]_\sim = \operatorname{Ker} p$, kun p on kuten edellä.

b) Olkoon $a \in R$ ja oletetaan, että $\boldsymbol{R}$ on vaihdannainen rengas. Osoitetaan, että on olemassa yksikäsitteinen homomorfismi $e_a\colon R[x] \to R$, jolle $e_a|R = \mathrm{id}_R$ (ts. kaikilla $t \in R$ pätee $e_a(t) = t$) ja $e_a(x) = a$. Oletetaan ensin, että tällainen on olemassa. Tällöin kaikille $s_0, \ldots, s_n \in R$ pätee

$$e_a\left(\sum_{i=0}^{n} s_i x^i\right) \underset{(+:\text{n hom.ehto})}{=} \sum_{i=0}^{n} e_a(s_i x^i) \underset{(\cdot:\text{n hom.ehto})}{=} \sum_{i=0}^{n} e_a(s_i) e_a(x)^i = \sum_{i=0}^{n} s_i a^i.$$

Kuvauksen e_a arvo on siis joka kohdassa välttämättä tietty, joten koko kuvaus on yksikäsitteisesti määrätty. Toisaalta on helppoa osoittaa, että kuvaus

$$e_a\colon R[x] \to R,\ e_a\left(\sum_{i=0}^{n} s_i x^i\right) = \sum_{i=0}^{n} s_i a^i$$

on todella homomorfismi. (HT)

On varsin luonnollista merkitä $e_a(f) = f(a)$, kun $f \in R[x]$, vaikka f ei ole kuvaus, vaan polynomi. Merkinnässä polynomit ja polynomifunktiot siis samastetaan keskenään, vaikka eri polynomeja voi vastata samat polynomifunktiot.

Sijoitushomomorfismin e_a ydin on

$$\operatorname{Ker} e_a = \{\, f \in R[x] \mid f(a) = e_a(f) = 0 \,\} = \{\, f \in R[x] \mid a \text{ on } f\text{:n juuri} \,\}.$$

Jatkossa tällä tematiikalla eli alkion suhteella niihin polynomeihin, joiden juuri se on, on keskeinen merkitys tällä kurssilla.

Kongruenssien ja ideaalien välisen vastaavuuden vuoksi seuraava sopimus on luonnollinen.

3.9. Merkintä. Pseudorenkaan $\boldsymbol{R} = (R, +, \cdot)$ tekijäpseudorengasta merkitään yleensä $\boldsymbol{R}/I$ $(= \boldsymbol{R}/\sim_I)$ ja perusjoukkoa R/I $(= R/\sim_I)$, missä $\sim_I$ on $\boldsymbol{R}$:n ideaalia I vastaava kongruenssi. Huomattakoon myös, että kaikille $a \in R$ pätee

$$[a]_{\sim_I} = \{\, b \in R \mid b \sim_I a \,\} = \{\, b \in R \mid b - a \in I \,\}$$
$$= \{\, b \in R \mid \exists t \in I : b = a + t \,\} = \{\, a + t \mid t \in I \,\} = a + I.$$

3.10. Esimerkki. Kokonaislukujen renkaan $(\mathbb{Z}, +, \cdot)$ ideaalit ovat $n\mathbb{Z}$, $n \in \mathbb{N}$. Olkoon nimittäin I renkaan $(\mathbb{Z}, +, \cdot)$ ideaali. Jos $I = \{0\}$, niin $I = 0 \cdot \mathbb{Z}$. Oletetaan sitten, että $I \neq \{0\}$, jolloin $\{0\} \subsetneq I$. Koska kaikilla $x \in I$ pätee $-x = 0 - x \in I$, niin on olemassa $n = \min\{\, m \in I \mid m > 0 \,\}$. Tällöin jokainen $m \in I$ voidaan kirjoittaa muodossa $m = k \cdot n + l$, missä $k, l \in \mathbb{Z}$ ja $0 \leqslant l < n$. Koska I on ideaali, niin $l = \underbrace{m}_{\in I} - \underbrace{k \cdot n}_{\in I} \in I$. Koska n on I:n pienin positiivinen alkio ja l on I:n alkio, jolle $l < n$, niin l ei voi olla positiivinen, vaan $l = 0$. Siis $m = k \cdot n \in n\mathbb{Z}$. On siis todistettu $I \subseteq n\mathbb{Z}$, mutta selvästi toisaalta $n\mathbb{Z} \subseteq I$, joten $I = n\mathbb{Z}$.

Vastaava kanoninen homomorfismi on

$$p\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ p(k) = k + n\mathbb{Z},$$

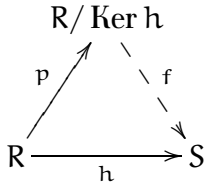
ja sen ydin on $\operatorname{Ker} p = n\mathbb{Z}$.

Ideaalit ja kongruenssit ovat siis tavallaan vain kaksi eri näkökulmaa samaan asiaan, nimittäin siihen, miten tekijärenkaita muodostetaan. Homomorfismien ja ideaalien yhteydestä taas tiedetään jo, että homomorfismien ytimet ovat ideaaleja. Ydin ei kuitenkaan yksin määrää homomorfismia, mikä on helppoa nähdä esimerkiksi siitä, että renkaalla voi olla runsaasti automorfismeita ja kaikilla näillä on triviaali ydin. Tietyssä mielessä tämä onkin täsmälleen se ylimääräinen informaatio, mikä homomorfismeihin sisältyy ytimen lisäksi; täsmällinen formulaatio tälle asialle on seuraava lause.

3.11. Pseudorenkaiden homomorfialause. *Olkoon* h *homomorfismi pseudorenkaasta* $(R, +, \cdot)$ *pseudorenkaaseen* $(S, +, \cdot)$*. Tällöin*

$$(R/\operatorname{Ker} h, +, \cdot) \cong (\operatorname{Im} h, +, \cdot).$$

Itse asiassa on olemassa sellainen isomorfismi $f\colon (R/\operatorname{Ker} h, +, \cdot) \cong (\operatorname{Im} h, +, \cdot)$*, että* $h = f \circ p$*, missä* $p\colon R \to R/\operatorname{Ker} h$ *on kanoninen homomorfismi.*



Todistus. Kuvaus h on erityisesti homomorfismi ryhmästä $(R, +)$ ryhmään $(S, +)$, joten ryhmien homomorfialauseen nojalla

$$f\colon (R/\operatorname{Ker} h, +) \cong (\operatorname{Im} h, +),$$

missä $f\colon R/I \to \operatorname{Im} h$, $f(a + I) = h(a)$ ja on merkitty $I = \operatorname{Ker} h$. Tämä f on homomorfismi myös kertolaskun suhteen, sillä kun $a, b \in R$, niin

$$f((a + I)(b + I)) = f(ab + I) = h(ab) = h(a)h(b) = f(a + I)f(b + I).$$

Siis $f\colon (R/\operatorname{Ker} h, +, \cdot) \cong (\operatorname{Im} h, +, \cdot)$.

Ryhmien homomorfialauseen perusteella tiedetään myös, että $h = f \circ p$, missä p on kanoninen homomorfismi $R \to R/I$. □

Huomautus. Homomorfialause on itse asiassa yksi algebran isomorfialauseista. Kyse on luonnollisesti siitä, nimetäänkö tulos oletusten mukaan (homomorfismi oletetaan annetuksi) vai tulosten mukaan (lauseessa väitetään isomorfismin olevan olemassa).

3.12. Seuraus (renkaiden homomorfialause). *Olkoon* h *homomorfismi renkaasta* $(R, +, \cdot)$ *renkaaseen* $(S, +, \cdot)$*. Tällöin on olemassa sellainen isomorfismi*

$$f : (R/\operatorname{Ker} h, +, \cdot) \cong (\operatorname{Im} h, +, \cdot),$$

että $h = f \circ p$*, missä* $p\colon R \to R/\operatorname{Ker} h$ *on kanoninen homomorfismi.* □

4. Pääideaalialueet ja suurin yhteinen tekijä

Seuraavissa kolmessa pääideaali-, euklidisia ja faktoriaalisia alueita käsittelevissä alaluvuissa analysoidaan, mitkä kahden pääesimerkkimme, renkaiden $(\mathbb{R}[x], +, \cdot)$ ja $(\mathbb{Z}, +, \cdot)$ ominaisuuksista ovat keskeisiä. Tiedämme jo, että ne ovat molemmat kokonaisalueita mutteivat kuntia. Niillä on kuitenkin paljon oleellisia piirteitä, jotka eivät ole yhteisiä kaikille kokonaisalueille; ne ovat jopa euklidisia alueita. Monien sovellusten kannalta on kuitenkin riittävää, että ne ovat faktoriaalisia alueita.

4.1. Lause. *Olkoon* $\boldsymbol{R} = (R, +, \cdot)$ *vaihdannainen rengas ja olkoon* $A \subseteq R$*. Tällöin on olemassa suppein (eli pienin sisältyvyyden suhteen)* $\boldsymbol{R}$*:n ideaali* I*, jolle* $A \subseteq I$*. Itse asiassa*

$$I = \Big\{ \sum_{i=0}^{n} r_i a_i \;\Big|\; n \in \mathbb{N},\ a_0, \ldots, a_n \in A,\ r_0, \ldots, r_n \in R \Big\}.$$

Todistus. Merkitään

$$I_0 = \Big\{ \sum_{i=0}^{n} r_i a_i \;\Big|\; n \in \mathbb{N},\ a_0, \ldots, a_n \in A,\ r_0, \ldots, r_n \in R \Big\}.$$

Valitsemalla $n = 0$, $a_0 = a$ ja $r_0 = 1$ huomataan, että $a \in I_0$ jokaisella $a \in A$, joten $A \subseteq I_0$. Osoitetaan, että I_0 on ideaali. Olkoot $t, u \in I_0$ ja $r \in R$. Valitaan sellaiset $a_0, \ldots, a_n \in A$, $r_0, \ldots, r_n \in R$ ja $s_0, \ldots, s_n \in R$, että

$$t = \sum_{i=0}^{n} r_i a_i \text{ ja } u = \sum_{i=0}^{n} s_i a_i,$$

jolloin

$$t - u = \sum_{i=0}^{n} (r_i - s_i) a_i \in I_0$$

ja

$$rt = \sum_{i=0}^{n} (rr_i)a_i \in I_0.$$

Siis I_0 on $\boldsymbol{R}$:n ideaali, jolle $A \subseteq I_0$.

Olkoon J $\boldsymbol{R}$:n ideaali, jolle $A \subseteq J$. Kun $n \in \mathbb{N}$, $a_0, \ldots, a_n \in A$ ja $r_0, \ldots r_i \in R$, niin $a_0, \ldots, a_n \in J$, joten myös $r_0 a_0, \ldots, r_n a_n \in J$, mistä seuraa $\sum_{i=0}^{n} r_i a_i \in J$, sillä J on ideaali. Siis $I_0 \subseteq J$. □

4.2. Määritelmä. Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas ja $A \subseteq R$. Tällöin suppeinta $\boldsymbol{R}$:n ideaalia I, joka sisältää joukon A, merkitään $I = \langle A \rangle$. Jos $A = \{a_0, \ldots, a_n\}$ on äärellinen, merkitään lyhyesti $\langle a_0, \ldots, a_n \rangle = \langle A \rangle$. Muotoa $\langle a \rangle$ olevia ideaaleja kutsutaan *pääideaaleiksi*. Jos $\boldsymbol{R}$ on kokonaisalue ja sen kaikki ideaalit ovat pääideaaleja, sitä kutsutaan *pääideaalialueeksi* (lyhenne: PID).

4.3. Esimerkki.

a) Kokonaislukujen rengas on paitsi kokonaisalue, myös jopa pääideaalialue, sillä sen kaikki ideaalit ovat muotoa $n\mathbb{Z}$ jollakin $n \in \mathbb{Z}$.

b) Tarkastellaan kunnan $(K, +, \cdot)$ polynomirengasta $(K[x], +, \cdot)$. Tämän tiedetään olevan kokonaisalue. Olkoon I $(K[x], +, \cdot)$:n ideaali. Jos $I = \{0\}$, niin $I = \langle 0 \rangle$, joten oletetaan, että $\{0\} \subsetneq I$. Valitaan joukosta I polynomi $s \neq 0$ niin, että sen aste on pienin mahdollinen. Osoitetaan, että $I = \langle s \rangle = \{ qs \mid q \in K[x] \}$. Triviaalisti $\langle s \rangle \subseteq I$. Olkoon $p \in I$. Jakoyhtälön nojalla on olemassa $q, r \in K[x]$, joille $p = qs + r$ ja $\deg(r) < \deg(s)$. Tällöin $r = \underbrace{p}_{\in I} - \underbrace{qs}_{\in I} \in I$. Koska s minimoi I:n nollasta poikkeavien polynomien asteet, täytyy olla $r = 0$. Siis $p = qs \in \langle s \rangle$, $I = \langle s \rangle$ on pääideaali ja $(K[x], +, \cdot)$ on pääideaalialue.

c) Kokonaiskertoimisten polynomien rengas $(\mathbb{Z}[x], +, \cdot)$ sen sijaan on kokonaisalue, muttei pääideaalialue. $(\mathbb{Z}[x], +, \cdot)$ on kokonaisalueen $(\mathbb{R}[x], +, \cdot)$ alirenkaana kokonaisalue. Merkitään I:llä niiden polynomien $p \in \mathbb{Z}[x]$ joukkoa, joiden vakiokerroin on parillinen. Tällöin I on $(\mathbb{Z}[x], +, \cdot)$:n ideaali. I ei kuitenkaan ole pääideaali: Tietenkin $2 \in I$. Jos olisi $I = \langle s \rangle$, niin jollain $q \in \mathbb{Z}[x]$ pätisi $2 = qs$, jolloin $0 = \deg(2) = \deg(qs) = \deg(q) + \deg(s)$, mistä seuraa $\deg(s) = 0$. Siis s olisi vakio, jolla on monikertana 2, joten $s = \pm 2$. Kuitenkaan $x^2 + x + 2$ ei ole alkion ± 2 monikerta $(\mathbb{Z}[x], +, \cdot)$:ssä, mikä on ristiriita.

4.4. Määritelmä. Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas. Alkioiden $a, b \in R$ *suurin yhteinen tekijä* on mikä tahansa alkio $d \in R$, jolle pätee

1) $d \mid a$ ja $d \mid b$ eli d on alkioiden a ja b yhteinen tekijä ja
2) jos alkiolle $e \in R$ pätee $e \mid a$ ja $e \mid b$, niin $e \mid d$.

Huomautus. Suurin yhteinen tekijä ei aina ole olemassa eikä yleisesti ottaen ole yksikäsitteinen silloinkaan, kun se on olemassa, vaan suurimman yhteisen tekijän kaikki liittoalkiotkin ovat sellaisia. Joissakin renkaissa on mahdollista valita liittoalkioiden joukosta kanoninen edustaja. Tällöin alkioiden a ja b kanonista suurinta yhteistä tekijää voidaan merkitä $\mathrm{syt}(a, b)$:llä. Seuraavat kaksi tapausta valaiskoot tätä:

1) Kokonaislukujen renkaassa lukujen $a, b \in \mathbb{Z}$ suurimmaksi yhteiseksi tekijäksi kelpaa edelliseen määritelmän mukaan luvut, jotka ovat toistensa vastalukuja. Näistä valitaan $\mathrm{syt}(a, b)$:ksi epänegatiivinen tapaus. Esimerkiksi $2 \mid 6$ ja $2 \mid 10$, mutta myös $-2 \mid 6$

ja $-2 \mid 10$; voidaan päätellä, että molemmat 2 ja -2 ovat alkioiden 6 ja 10 suurimpia yhteisiä tekijöitä. Koska $2 > 0$, valitaan $\mathrm{syt}(6, 10) = 2$.

2) Jos $\boldsymbol{K} = (K, +, \cdot)$ on kunta, niin polynomirenkaassa $\boldsymbol{K}[x]$ voidaan valita polynomien $p, q \in K[x]$ suurimmista yhteisistä tekijöistä se polynomi s, jonka korkeimman asteen kerroin on 1. Tämän luvun viimeinen lause osoittaa, että valinta on yksikäsitteinen, ja voidaan merkitä $s = \mathrm{syt}(p, q)$.

4.5. Lause. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas, $a, b \in R$. Jos c ja d ovat molemmat alkioiden a ja b suurimpia yhteisiä tekijöitä, niin ne ovat toistensa liittoalkioita.*

Todistus. Suurimman yhteisen tekijän määritelmän kohdasta 2 seuraa suoraan $c \mid d$ ja $d \mid c$, joten c ja d ovat liittoalkioita. □

Huomautus. Liittoalkiorelaatio on renkaassa ekvivalenssi. Tarkemmin: Jos merkitään $a \sim b$, kun $a \mid b$ ja $b \mid a$, niin

1) $a = 1 \cdot a$, joten $a \mid a$, mistä seuraa $a \sim a$,
2) Jos $a \sim b$ eli $a \mid b$ ja $b \mid a$ eli $b \mid a$ ja $a \mid b$, niin $b \sim a$,
3) Jos $a \sim b$ ja $b \sim c$, niin $a \mid b$, $b \mid a$, $b \mid c$ ja $c \mid b$. Ehdoista $a \mid b$ ja $b \mid c$ seuraa $a \mid c$, kun taas ehdoista $c \mid b$ ja $b \mid a$ seuraa $c \mid a$. Siis $a \sim c$.

4.6. Lause. *Olkoon $\boldsymbol{K} = (K, +, \cdot)$ kunta ja $p, q \in K[x]$. Tällöin p:llä ja q:lla on suurin yhteinen tekijä polynomirenkaassa $\boldsymbol{K}[x]$. Tämä suurin yhteinen tekijä s on yksikäsitteinen, jos polynomin s korkeimman asteen termin kertoimen vaaditaan olevan 1 ja $p, q \neq 0$.*

Todistus. Tarkastellaan ideaalia

$$I = \langle p, q \rangle = \{ ap + bq \mid a, b \in K[x] \}.$$

Koska $\boldsymbol{K}[x]$ on pääideaalialue, niin on olemassa $s \in K[x]$, jolle $I = \langle s \rangle = \{ cs \mid c \in K[x] \}$. Koska

$$\langle s \rangle = \langle p, q \rangle,$$

niin $p, q \in \langle s \rangle$ ja $s \mid p$, $s \mid q$. Siis s on polynomien p ja q yhteinen tekijä. Olkoon $t \in K[x]$ myös yhteinen tekijä eli $t \mid p$ ja $t \mid q$. Koska $s \in \langle s \rangle = \langle p, q \rangle$, niin $s = ap + bq$ joillakin $a, b \in K[x]$. Siis $t \mid ap + bq = s$. Siten s on polynomien p ja q suurin yhteinen tekijä.

Jos c on polynomin s korkeimman asteen termin kerroin, niin polynomin $c^{-1}s$ vastaava kerroin on 1. Koska s ja $c^{-1}s$ ovat liittoalkiota, niin c^{-1} on siis polynomien p ja q suurin yhteinen tekijä, jonka korkeimman asteen termin kerroin on 1. Jos s^* on toinen tällainen suurin yhteinen tekijä, niin $c^{-1}s - s^* \in I$, joten $s \mid c^{-1}s - s^*$ ja $\deg(s) \leqslant \deg(c^{-1}s - s^*)$, mikä on mahdotonta, koska erotuksessa $c^{-1}s - s^*$ korkeimman asteen termit kumoavat toisensa. Siis $c^{-1}s$ on yksikäsitteinen p:n ja q:n suurin yhteinen tekijä, jonka korkeimman asteen termin kerroin on 1. □

Eukleideen algoritmi kuntakertoimisessa polynomirenkaassa

Olkoon $\boldsymbol{K} = (K, +, \cdot)$ kunta ja $a, b \in K[x]$, $a, b \neq 0$. Määritellään rekursiivisesti jono polynomeja p_i, joille

$$p_0 = a,\ p_1 = b$$

ja

$$p_i = q_i p_{i+1} + p_{i+2} \text{ ja } \deg(p_{i+2}) < \deg(p_{i+1}).$$

Palautuskaavassa esiintyvä p_{i+2} on jakoyhtälön mukaan olemassa ja yksikäsitteinen, kunhan $p_{i+1} \neq 0$. Koska asteiden ketju

$$\deg(p_1) > \deg(p_2) > \cdots$$

ei voi laskea loputtomasti, on oltava olemassa sellainen $i \in \mathbb{N}$, että $p_i = 0$. Olkoon $k \in \mathbb{N}$ suurin luku, jolle $p_k \neq 0$.

Merkitään $r = p_k$ ja osoitetaan, että $r \in K[x]$ on polynomien a ja b suurin yhteinen tekijä. Kun $s \in K[x]$, seuraavat ovat nimittäin yhtäpitävät:

1) $s \mid a = p_0$, $s \mid b = p_1$,
2) $s \mid a = p_{k-1}$, $s \mid r = p_k$ ja
3) $s \mid a = p_i$ jokaisella $i = 0, \ldots, k$.

Kohdasta 3 seuraavat nimittäin triviaalisti kohdat 1 ja 2. Kohdasta 1 seuraa toisaalta kohta 3 induktiolla, missä kaksi aloitusaskelta $s \mid p_0$, $s \mid p_1$ ovat oletuksia ja induktioaskel on

$$s \mid p_i,\ s \mid p_{i+1} \Rightarrow s \mid p_i - q_i p_{i+1} = p_{i+2}.$$

Kohdasta 2 seuraa kohta 3 vastaavasti takaperoisella induktolla, missä aloitusaskeleet $s \mid p_k$ ja $s \mid p_{k-1}$ ovat oletuksia ja induktioaskel on

$$s \mid p_i,\ s \mid p_{i-1} \Rightarrow s \mid q_{i-2} p_{i-1} + p_i = p_{i-2}.$$

Erityisesti, jos $s \mid a$ ja $s \mid b$, niin $s \mid p_k = r$ eli polynomien a ja b yhteiset tekijät ovat polynomin r tekijöitä. Toisaalta

$$p_{k-1} = q_{k-1} p_k + p_{k+1} = q_{k-1} r + 0 = q_{k-1} r.$$

Siis $r \mid p_{k-1}$ ja triviaalisti $r \mid r = p_k$, joten kun edellä todistetusta kohtien 1–3 yhtäpitävyydestä käytetään implikaatiota 2) $\Rightarrow$ 1), seuraa $r \mid a$ ja $r \mid b$. Siis r on polynomien a ja b suurin yhteinen tekijä.

Koska jakoyhtälössä jakojäännöksen laskeminen voidaan algoritmisoida, polynomit p_i, $i \in \{0, \ldots, k\}$ voidaan määrittää algoritmisesti. Näin saatua algoritmia polynomien suurimmalle yhteiselle tekijälle kutsutaan *Eukleideen algoritmiksi*.

Eukleideen algoritmista saadaan sivutuotteena suurimmalle yhteiselle tekijälle r esitys

$$r = ca + db,$$

missä $c, d \in K[x]$. Osoitetaan nimittäin induktiolla, että jokaisella $i \in \{0, \ldots, k\}$ on olemassa sellaiset $c_i, d_i \in K[x]$, että

$$p_i = c_i a + d_i b.$$

Aloitusaskel on selvä, sillä

$$p_0 = 1 \cdot a + 0 \cdot b,\ (c_0 = 1, d_0 = 0),$$
$$p_1 = 0 \cdot a + 1 \cdot b,\ (c_1 = 0, d_1 = 1).$$

Induktioaskel: Jos $p_i = c_i a + d_i b$ ja $p_{i+1} = c_{i+1} a + d_{i+1} b$, niin

$$\begin{aligned} p_{i+2} &= p_i - q_i p_{i+1} \\ &= c_i a + d_i b - q_i(c_{i+1} a + d_{i+1} b) \\ &= (c_i - q_i c_{i+1}) a + (d_i - q_i d_{i+1}) b \\ &= c_{i+2} a + d_{i+2} b, \end{aligned}$$

missä $c_{i+2} = c_i - q_i c_{i+1}$ ja $d_{i+2} = d_i - q_i d_{i+1}$. Erityisesti $r = p_k = c_k a + d_k b$.

4.7. Esimerkki. Tarkastellaan rationaalikertoimisia polynomeja $a = x^5 + 1 \in \mathbb{Q}[x]$ ja $b = x^3 + 1 \in \mathbb{Q}[x]$. Merkitään $p_0 = a$, $p_1 = b$. Koska

$$p_0 = a = x^5 + 1 = x^5 + x^2 - x^2 + 1 = x^2(x^3 + 1) + (-x^2 + 1) = x^2 p_1 + (-x^2 + 1)$$

ja $\deg(-x^2 + 1) = 2 < 3 = \deg(p_1)$, niin $p_2 = -x^2 + 1$. Edelleen

$$p_1 = x^3 + 1 = x^3 - x + x + 1 = -x(-x^2 + 1) + x + 1 = -x p_2 + x + 1$$

ja $\deg(x+1) = 1 < 2 = \deg(p_2)$, joten $p_3 = x + 1$. Koska $p_2 = 1 - x^2 = (1-x)(1+x) = (1-x)p_3$, niin $p_4 = 0$. Siis polynomien a ja b suurin yhteinen tekijä on $p_3 = x + 1$.

5. Euklidiset alueet

5.1. Määritelmä. Kokonaisalue $\boldsymbol{R} = (R, +, \cdot)$ on *euklidinen alue*, jos on olemassa *astefunktioksi* kutsuttu kuvaus $d\colon R \setminus \{0\} \to \mathbb{N}$, jolle pätee seuraavaa:

1) Kun $a, b \in R \setminus \{0\}$, niin $d(a) \leqslant d(ab)$.
2) Kaikilla $a, b \in R$, $b \neq 0$, on olemassa sellaiset $q, r \in R$, että $a = qb + r$ ja $r = 0$ tai $d(r) < d(b)$.

Huomautus.

1) Kohdan 1 voisi muotoilla myös: jos $a \mid c \neq 0$, niin $d(a) \leqslant d(c)$.
2) Kohdan 2 voisi kirjoittaa: joko $b \mid a$ tai on olemassa $q, r \in R$, joille $a = qb + r$ ja $d(r) < d(b)$.
3) Useissa lähteissä vaaditaan lisäksi, ettei euklidinen alue saa olla kunta.

5.2. Lause. *Euklidiset alueet ovat pääideaalialueita.*

Todistus. Olkoon $\boldsymbol{R} = (R, +, \cdot)$ euklidinen alue, jolloin se määritelmän mukaan on kokonaisalue. Olkoon I $\boldsymbol{R}$:n ideaali, josta voidaan olettaa, että $I \neq \{0\}$. Merkitään $m = \min d[I \setminus \{0\}]$, missä d on $\boldsymbol{R}$:n astefunktio. Valitaan $a \in I \setminus \{0\}$, jolle $m = d(a)$. Triviaalisti $\langle a \rangle \subseteq I$; osoitetaan, että itse asiassa yhtäsuuruus pätee.

Olkoon $b \in I$. Jos $b = 0$, niin $b = 0 = 0 \cdot a$, joten oletetaan, että $b \neq 0$. Koska euklidisessa alueessa pätee oma muotonsa jakoyhtälöstä, niin on olemassa sellaiset $q, r \in R$, että $b = qa + r$ ja joko $r = 0$ tai $d(r) < d(a) = m$. Koska $r = b - qa \in I$, niin luvun m minimaalisuuden vuoksi jälkimmäinen vaihtoehto on mahdoton. Siis $r = 0$, joten $b = qa$ ja $b \in \langle a \rangle$. On päätelty $I \subseteq \langle a \rangle$. □

5.3. Esimerkki.

1) Kokonaislukujen rengas on euklidinen alue. Astefunktioksi kelpaa $d\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, $d(m) = |m|$. Kun $a \mid b$, $b \neq 0$, pätee nimittäin $d(a) = |a| \leqslant |b| = d(b)$. Lisäksi jakoyhtälö toimii muodossa $a = qb + r$, missä $q, r \in \mathbb{Z}$, $|r| < |b|$.
2) Edellisessä luvussa huomattiin oikeastaan, että kuntien polynomirenkaat $(K[x], +, \cdot)$ ovat euklidisia alueita. Astefunktio on tuttu $d = \deg \restriction (K \setminus \{0\})$. Määritelmän kohdat 1 ja 2 ovat kuntakertoimisien polynomien tunnettuja ominaisuuksia, kuten $d(pq) = \deg(pq) = \deg(p) + \deg(q) \geqslant \deg(p)$, kun $p, q \in K \setminus \{0\}$.
3) Tarkastellaan Gaussin kokonaislukuja eli rengasta $(\mathbb{Z}[i], +, \cdot)$. Määritellään $d\colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$, $d(a + bi) = a^2 + b^2 = |a + bi|^2$, kun $a, b \in \mathbb{Z}$. Tarkastetaan, että d on astefunktio. Kun u ja v ovat Gaussin kokonaislukuja, niin

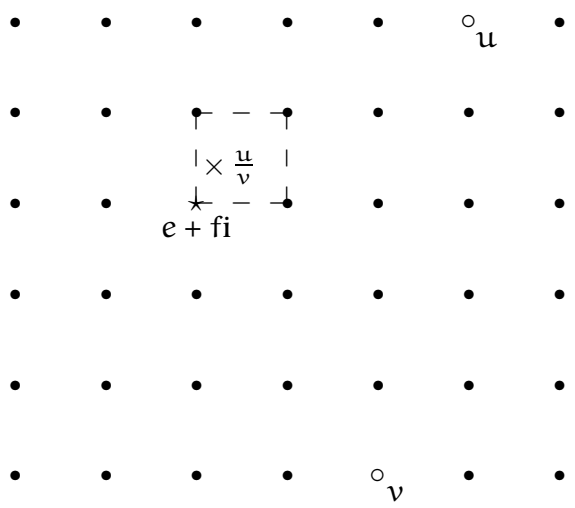
$$d(uv) = |uv|^2 = |u|^2|v|^2 \geqslant |u|^2 = d(u),$$

sillä $d(v) = |v|^2 \geqslant 1$.

Määritelmän 5.1 jälkimmäisen kohdan tarkastaminen on haastavampaa: Olkoot $u = a + bi, v = c + di \in \mathbb{Z}[i]$, missä $a, b, c, d \in \mathbb{Z}$ ja $v \neq 0$. Merkitään

$$\frac{u}{v} = x + yi = (e + \varepsilon) + (f + \eta)i,$$

missä $|\varepsilon| \leqslant 1/2$, $|\eta| \leqslant 1/2$, $e, f \in \mathbb{Z}$. Kuvio havainnollistaa esimerkkitilannetta, johon on merkitty neljä lukua u/v lähinnä sijaitsevaa hilapistettä.



Tällöin

$$u = \underbrace{(e + fi)}_{\in \mathbb{Z}[i]} v + \underbrace{(\varepsilon + \eta i)v}_{\in \mathbb{Z}[i]},$$

missä $r = (\varepsilon + \eta i)v$ toteuttaa ehdon

$$d(r) = |r|^2 = |(\varepsilon + \eta i)|^2|v|^2 \leqslant \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) \cdot |v|^2 = \frac{1}{2}|v|^2 < |v|^2 = d(v).$$

Siis d on astefunktio ja $(\mathbb{Z}[i], +, \cdot)$ euklidinen alue.

5.4. Esimerkki. $(\mathbb{Z}[\frac{1}{2} + i\sqrt{19}], +, \cdot)$ on pääideaalialue, joka ei ole euklidinen alue. Todistus käydään osittain läpi laskuharjoituksissa.

Huomautus. Edellisessä alaluvussa esitetyn polynomien Eukleideen algoritmin voi helposti yleistää euklidisissa alueissa toimivaksi.

6. Faktoriaaliset alueet

6.1. Määritelmä. Vaihdannaisen renkaan $(R, +, \cdot)$ alkio a on *jaoton*, jos $a \neq 0$, a ei ole yksikkö eikä alkiolla a ole muita tekijöitä kuin yksiköt ja a:n liittoalkiot. Alkion $b \in R$ tekijä $c \in R$ on *aito*, jos se se ei ole alkion b liittoalkio.

6.2. Määritelmä. Kokonaisalue $(R, +, \cdot)$ on *faktoriaalinen*, jos

1) jokainen $a \in R \setminus \{0\}$, joka ei ole yksikkö, on jaottomien alkioiden tulo, ts. joillakin jaottomilla $a_0, \ldots, a_{n-1} \in R$, $n \in \mathbb{Z}_+$, pätee $a = a_0 \cdots a_{n-1} = \prod_{k=0}^{n-1} a_k$.
2) Kohdan 1 esitys on siinä mielessä yksikäsitteinen, että jos pätee myös $a = \prod_{j=0}^{m-1} a'_j$, missä alkiot a'_j ovat jaottomia, kun $j \in \{0, \ldots, m-1\}$ ($m \in \mathbb{Z}_+$), niin $m = n$ ja on olemassa joukon $\{0, \ldots, n-1\}$ permutaatio σ, joka luo seuraavan vastaavuuden esitysten välille: jokaisella $i \in \{0, \ldots, n-1\}$ alkiot $a'_{\sigma(i)}$ ja a_i ovat liittoalkioita.

Huomautus. Kurssilla noudatetaan tässä bourbakilaista terminologiaa. (Bourbaki oli merkittävän ranskalaisen matemaatikkoryhmän salanimi.) Vaihtoehtoinen nimitys faktoriaalisille alueille olisi *yksikäsitteisen tekijöinnin alue* eli UFD (engl. unique factorization domain).

6.3. Lemma. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ pääideaalialue. Tällöin $\boldsymbol{R}$:ssa ei ole ääretöntä aidosti nousevaa ideaalien ketjua.*

Todistus. Oletetaan vastoin väitettä, että olisi olemassa $\boldsymbol{R}$:n ideaalit I_k, $k \in \mathbb{N}$, joille

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

Tarkastellaan ideaalia

$$I = \bigcup_{k \in \mathbb{N}} I_k.$$

Koska $\boldsymbol{R}$ on pääideaalialue, niin on olemassa $a \in R$, jolle $I = \langle a \rangle$. Koska toisaalta $I = \bigcup_{k \in \mathbb{N}} I_k$, niin jollakin $k_0 \in \mathbb{N}$ on voimassa $a \in I_{k_0}$. Siis $I = \langle a \rangle \subseteq I_{k_0} \subsetneq I_{k_0+1} \subseteq I$, mikä on ristiriita. □

6.4. Seuraus. *Pääideaalialueessa $\boldsymbol{R} = (R, +, \cdot)$ jokainen $a \in R \setminus \{0\}$, joka ei ole yksikkö, voidaan esittää jaottomien alkioiden tulona.*

Todistus. Tarkastellaan niiden alkioiden $a \in R \setminus \{0\}$ joukkoa X, jotka eivät ole yksiköitä mutta joita ei myöskään voi esittää jaottomien alkioiden tulona. Kun $a \in X$, niin a ei erityisesti ole jaoton, joten $a = bc$ joillakin $b, c \in R \setminus \{0\}$, jotka eivät ole yksiköitä eivätkä a:n liittoalkioita.

Ainakin toinen näistä alkioista, olkoon se vaikkapa b, kuuluu välttämättä joukkoon X, sillä muuten alkiolle a saataisiin esitys jaottomien alkioiden tulona. Siis jokaisella alkiolla $a \in X$ on aito tekijä $b \in X$, jolloin $\langle a \rangle \subsetneq \langle b \rangle$. Jos X on epätyhjä, on siis olemassa ääretön aidosti nouseva ketju ideaaleja. Siis täytyy olla $X = \emptyset$, joka on yhtäpitävää väitteen kanssa. □

6.5. Määritelmä. Vaihdannaisen renkaan $\boldsymbol{R} = (R, +, \cdot)$ ideaali I on *alkuideaali*, jos $I \neq R$ ja kaikilla $a, b \in R$ pätee: jos $ab \in I$, niin $a \in I$ tai $b \in I$.

6.6. Lemma. *Pääideaalialuessa $\boldsymbol{R} = (R, +, \cdot)$ ideaalit $\langle p \rangle$ ovat alkuideaaleja, kun $p \in R$ on jaoton.*

Todistus. Olkoot $a, b \in R$, $p \in R$ jaoton. Oletetaan, että $ab \in \langle p \rangle$ eli $p \mid ab$. Tarkastellaan ideaalia $J = \langle p, b \rangle$. Koska $\boldsymbol{R}$ on pääideaalialue, niin $J = \langle d \rangle$ jollakin $d \in R$. Koska $p \in \langle p, b \rangle = J = \langle d \rangle$, niin $d \mid p$, mutta p on jaoton, joten d on p:n liittoalkio tai yksikkö. Edellisessä tapauksessa $p \mid d$ ja $d \mid b$, sillä $b \in \langle p, b \rangle = J = \langle d \rangle$. Tässä tapauksessa siis $p \mid b$ eli $b \in \langle p \rangle$. Jälkimmäisessä tapauksessa d on yksikkö ja $J = R$. Erityisesti $1 \in J = \langle p, b \rangle$, joten $1 = sb + tp$ joillakin $s, t \in R$. Koska $p \mid ab$, niin $p \mid sab + atp = (ab + tp)a = a$ eli $a \in \langle p \rangle$. Siis $\langle p \rangle$ on alkuideaali. □

6.7. Lause. *Pääideaalialueet ovat faktoriaalisia.*

Todistus. Olkoon $\boldsymbol{R} = (R, +, \cdot)$. Seurauksena 6.4 on jo todistettu, että jokainen $\boldsymbol{R}$:n nollasta poikkeava alkio voidaan esittää jaottomien alkioiden tulona. Pitää vielä osoittaa, että tämä esitys on oleellisesti yksikäsitteinen. Olkoon $a \in R \setminus \{0\}$ ja

$$a = \prod_{i=0}^{m-1} p_i = \prod_{j=0}^{n-1} q_j$$

alkion a kaksi esitystä jaottomien alkioiden tulona. Todistetaan esityksen oleellinen yksikäsitteisyys induktiolla luvun $\min\{m, n\}$ suhteen. Voidaan olettaa, että $m \leqslant n$.

1° Jos $\min\{m, n\} = 1$, niin $a = p_0$ on jaoton, joten sitä ei voi esittää epätriviaalilla tavalla jaottomien alkioiden tulona. Siis $m = 1 = n$ ja $p_0 = q_0$.

2° Oletetaan, että $\min\{m, n\} > 1$ ja induktio-oletus pätee pienemmille positiivisille kokonaisluvuille kuin $\min\{m, n\}$. Tiedetään, että $p_{m-1} \mid a$ eli $\prod_{j=0}^{n-1} q_j = a \in \langle p_{m-1} \rangle$. Lisäksi edellisen lemman perusteella tiedetään, että $\langle p_{m-1} \rangle$ on alkuideaali, joten jollakin $k \in \{0, \ldots, n-1\}$ pätee $q_k \in \langle p_{m-1} \rangle$. Siis $p_{m-1} \mid q_k$. Koska p ja q_k ovat molemmat jaottomia, tämä on mahdollista vain, jos ne ovat liittoalkioita, ts. $p_{m-1} = uq_k$ jollakin yksiköllä $u \in R$. Koska $\boldsymbol{R}$ on kokonaisalue, saadaan

$$a = u \left(\prod_{i=0}^{m-2} p_i \right) q_k = \left(\prod_{\substack{j \in \{0, \ldots, n-1\}, \\ j \neq k}} q_j \right) q_k,$$

josta supistussäännön perusteella seuraa

$$u \left(\prod_{i=0}^{m-2} p_i \right) = \prod_{\substack{j \in \{0, \ldots, n-1\}, \\ j \neq k}} q_j.$$

Jälkimmäinen yhtälö tarkoittaa tietenkin, että eräällä alkiolla on kaksi esitystä jaottomien alkioiden tulona (joista vasemmanpuoleisessa esityksessä yksi on up_0), joten induktio-oletuksesta seuraa, että $m - 1 = n - 1$ eli $m = n$ ja on olemassa joukon $\{0, \ldots, m-1\}$ permutaatio ρ, jolle $\rho(m-1) = k$ ja p_i ja $q_{\rho(i)}$ ovat liittoalkioita, kun $i \in \{0, \ldots, m-1\}$. Tämä osoittaa alkion a esityksen oleellisen yksikäsitteisyyden. □

Rengasteoria päätetään kaavioon, joka kuvaa eri rengaskategorioiden välisiä suhteita. Kaaviossa esiintyy sopivissa kohdissa myös muutama esimerkkirakenne.