Renkaat ja modulit

Tässä osassa käsiteltävät renkaat ovat vaihdannaisia, ellei toisin mainita.

6. Ideaalit

Kuten aikaisemmin on todettu, tekijärenkaassa nollan ekvivalenssiluokkaa vastaa renkaan *ideaali*. Ideaalin käsitteen otti käyttöön Richard Dedekind (1831–1916), ja se pohjautuu Ernst Kummerin (1810–1893) keksimiin “ideaalisiin lukuihin”. Käsitteen synty on siis lukuteoriassa: monissa lukualueissa kokonaislukujen yksikäsitteinen alkutekijöihin jako ei onnistu, mutta toisinaan tämä voidaan korvata jakamalla luvun virittämä ideaali niin sanottuihin alkuideaaleihin.

6.1. Määritelmä ja virittäminen. Ideaali on määritelmän mukaan renkaan additiivisen ryhmän aliryhmä A, jolle pätee $rA = A$ kaikilla renkaan alkioilla r. Jos rengas ei ole vaihdannainen, puhutaan erikseen vasemman- ja oikeanpuoleisista ideaaleista (joille pätee $rA = A$ tai $Ar = A$), ja ideaalilla tarkoitetaan sellaista aliryhmää, joka on sekä vasemman- että oikeanpuoleinen ideaali. Yhdistämällä aliryhmäkriteeri sekä ideaalisuusehto saadaan seuraava tulos.

LAUSE 6.1 (Ideaalisuuskriteeri). *Renkaan R osajoukko A on ideaali, jos ja vain jos*

(I1) $A \neq \emptyset$
(I2) $a - b \in A$ *kaikilla* $a, b \in A$
(I3) $ra \in A$ *kaikilla* $a \in A$ *ja* $r \in R$.

Renkaan osajoukon X virittämä ideaali on pienin ideaali, joka sisältää joukon X, ja sitä merkitään $\langle X \rangle$. Yhden alkion virittämää ideaalia nimitetään *pääideaaliksi*. Pääideaalit ovat aina muotoa $\langle x \rangle = \{rx \mid r \in R\}$.

MÄÄRITELMÄ 6.2. Rengas R on *pääideaalirengas*, jos se on kokonaisalue ja kaikki sen ideaalit ovat pääideaaleja.

Esimerkiksi kokonaislukujen rengas $(\mathbb{Z}, +, \cdot)$ on pääideaalirengas, sillä sen kaikki aliryhmät ovat muotoa $n\mathbb{Z} = \langle n \rangle$. Toinen esimerkki saadaan yhden muuttujan polynomeista, joiden kertoimet ovat kunnassa K. Nämä muodostavat renkaan, jota merkitään $K[X]$. Kyseinen rengas on kokonaisalue, sillä kahden polynomin tulo on nolla, jos ja vain jos jompikumpi tekijöistä on nolla.

LAUSE 6.3. *Polynomirengas $K[X]$ on pääideaalirengas.*

TODISTUS. Oletetaan, että A on renkaan $K[X]$ ideaali. Jos A sisältää jonkin vakiopolynomin $a \neq 0$, niin $a^{-1}a = 1 \in A$, jolloin $A = R = \langle 1 \rangle$. Toisaalta, jos

$A = \{0\}$, niin $A = \langle 0 \rangle$. Voidaan siis olettaa, että $A \neq \{0\}$ ja A ei sisällä nollasta poikkeavia vakiopolynomeja. Valitaan A:sta polynomi $g \neq 0$, jonka aste on pienin mahdollinen (välttämättä siis positiivinen). Jos nyt $f \in A$, niin polynomien jakoalgoritmin perusteella $f = gq + r$, missä r:n aste on pienempi kuin g:n. Toisaalta $r = f - gq \in A$, mutta g:n aste on pienin A:n nollasta poikkeavien polynomien joukossa, joten $r = 0$. Näin ollen $f = gq$, ja koska tämä pätee kaikilla $f \in K[X]$, voidaan päätellä, että $A = \langle g \rangle$. Täten $K[X]$ on pääideaalirengas. □

Useamman kuin yhden muuttujan polynomeille edellinen lause ei päde: esimerkiksi renkaassa $K[X, Y]$ ideaali $\langle X, Y \rangle$ ei ole yhden alkion virittämä, koska X ja Y ovat jaottomia, mutta kumpikaan ei ole toisen tekijä. Lause ei myöskään päde, jos K ei ole kunta: renkaassa $\mathbb{Z}[X]$ ideaali $\langle 2, X \rangle$ ei ole pääideaali. Todistuksessa ongelma tulee vastaan siinä, että vaikka 2 on vakiopolynomi, silti $1 \notin \langle 2, X \rangle$.

6.2. Alkuideaalit ja maksimaaliset ideaalit. Alkuideaalin käsite on keskeinen monissa renkaiden sovelluksissa. Oletetaan seuraavassa, että R rengas ja A sen ideaali.

MÄÄRITELMÄ 6.4. Oletetaan, että $A \neq R$ ja kaikilla $x, y \in R$ pätee:

jos $xy \in A$, niin $x \in A$ tai $y \in A$.

Ideaalia A kutsutaan tällöin *alkuideaaliksi*.

MÄÄRITELMÄ 6.5. Ideaalia A kutsutaan *maksimaaliseksi*, jos $A \neq R$ ja millään ideaalilla B ei päde $A \subsetneq B \subsetneq R$.

Alkuideaalin määritelmä muistuttaa läheisesti kokonaisalueen määritelmää. Yhteys paljastuu seuraavassa lauseessa.

LAUSE 6.6. *Olkoon R rengas ja A sen ideaali. Tällöin*

(a) *A on alkuideaali, jos ja vain jos tekijärengas R/A on kokonaisalue*
(b) *A on maksimaalinen, jos ja vain jos tekijärengas R/A on kunta.*

TODISTUS. Harjoitustehtävä. □

Lauseesta saadaan nyt suoraan seuraava tulos.

KOROLLAARI 6.7. *Jokainen maksimaalinen ideaali on alkuideaali.*

Seuraavassa esimerkkejä alkuideaaleista:

- Kokonaislukujen renkaassa ideaali $\langle p \rangle$ on alkuideaali, jos ja vain jos p on alkuluku tai nolla. Toisaalta, jos p on alkuluku, tekijärengas $\mathbb{Z}/\langle p \rangle = \mathbb{Z}_p$ on äärellinen kokonaisalue. Siksi se on kunta, joten ideaali $\langle p \rangle$ on myös maksimaalinen. Siispä ainoa $\mathbb{Z}$:n alkuideaali, joka ei ole maksimaalinen, on nollaideaali $\{0\}$.
- Yleisemmin, pääideaalirenkaassa R jokainen nollasta poikkeava alkuideaali on maksimaalinen. Jos nimittäin $\langle x \rangle \neq \{0\}$ on alkuideaali ja lisäksi $\langle x \rangle \subsetneq \langle y \rangle$, niin $x \in \langle y \rangle$ eli $x = ry$ jollain $r \in R$. Tällöin $ry \in \langle x \rangle$, mutta $y \notin \langle x \rangle$, joten alkuideaalin määritelmän perusteella $r \in \langle x \rangle$. Edelleen

$r = sx$ jollain $s \in R$, joten $x = ry = sxy$ eli $(1 - sy)x = 0$. Koska R on kokonaisalue, nähdään että $sy = 1$, mistä seuraa $R = \langle y \rangle$.

- Polynomirenkaassa $R[X_1, \dots, X_n]$ pääideaali $\langle f \rangle$ on alkuideaali, jos f on jaoton polynomi.

Todistetaan seuraavaksi tulos, joka varmistaa alkuideaalien riittävän saatavuuden.

LAUSE 6.8 (Krull). *Jokaisella epätriviaalilla renkaalla on maksimaalinen ideaali.*

Lauseen todistus on perusesimerkki *Zornin*[11] *lemman* käytöstä. Koska Zornin lemma on luonteeltaan joukko-opillinen, on tässä yhteydessä hyvä hieman perehtyä siihen liittyviin käsitteisiin.

Zornin lemma on niin sanotun *valinta-aksiooman* toinen muotoilu, joka sopii hyvin erilaisten maksimaalisten rakenteiden olemassaolotodistuksiin. Valinta-aksiooma puolestaan on joukko-opin aksiooma, jota tarvitaan esimerkiksi ei-mitallisen joukon olemassaoloon tai joukkojen välisten mahtavuuksien vertailuun. Aksiooman mukaan mille tahansa epätyhjien joukkojen kokoelmalle voidaan määritellä kuvaus, joka antaa joukon arvoksi aina jonkin sen sisältämän alkion. Tällaista kuvausta kutsutaan yleensä *valintafunktioksi.* Ongelma valinta-aksioomasta — tai yhtä hyvin Zornin lemmasta — riippuvissa olemassaolotodistuksissa on se, että todistuksen tuottamasta joukosta tai rakenteesta ei yleensä voida sanoa mitään täsmällistä. Tässä mielessä valinta-aksiooman on sen naiivin joukko-opin perussäännön vastainen, että jokaisesta alkiosta pitäisi pystyä sanomaan, kuuluuko se annettuun joukkoon vai ei. Muun muassa[12] sen vuoksi on yleensä tapana mainita erikseen, jos todistuksessa nojaudutaan johonkin valinta-aksioomasta riippuvaan tulokseen.

Olkoon $\mathcal{P}$ jokin joukko ja $\leq$ sen kaksipaikkainen relaatio. Tarkastellaan seuraavia ehtoja:

(J1) Jos $a \leq b$ ja $b \leq c$, niin $a \leq c$ (transitiivisuus).
(J2) Jos $a \leq b$ ja $b \leq a$, niin $a = b$ (antisymmetrisyys).
(J3) Kaikilla $a, b \in \mathcal{P}$ pätee $a \leq b$ tai $b \leq a$.

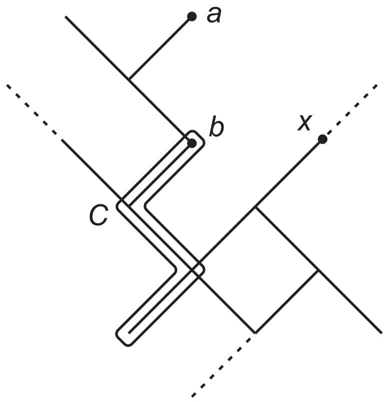
Jos relaatio $\leq$ on transitiivinen ja antisymmetrinen, niin paria $(\mathcal{P}, \leq)$ kutsutaan *osittaisjärjestykseksi.* Jos myös ehto (J3) toteutuu, niin pari on *täydellinen järjestys* eli *lineaarijärjestys.* Jos sekaannuksen vaaraa ei ole, osittaisjärjestykseksi tai lineaariseksi järjestykseksi voidaan nimittää myös joukkoa $\mathcal{P}$ tai relaatiota $\leq$. *Ketju* on osittaisjärjestyksen osajoukko, joka on relaation $\leq$ suhteen lineaarijärjestys. Alkio $m \in \mathcal{P}$ on osajoukon $A \subset \mathcal{P}$ *yläraja*, jos kaikilla $a \in A$ pätee $a \leq m$. Alkio m on *maksimaalinen*, jos ei ole olemassa alkiota $a \in \mathcal{P}$, jolle pätisi $m \leq a$.

LEMMA 6.9 (Zornin lemma). *Oletetaan, että $\mathcal{P}$ on epätyhjä osittaisjärjestys, jossa jokaisella ketjulla on yläraja. Tällöin $\mathcal{P}$ sisältää maksimaalinen alkion.*

[11]Max August Zorn (1906–1993) oli saksalaissyntyinen amerikkalainen matematiikko.

[12]Toinen syy on se, että valinta-aksiooman hyväksyminen todistuksen lähtökohdaksi voi johtaa paradoksaaliselta vaikuttaviin tuloksiin. Eräs tunnettu esimerkki on Banachin-Tarskin paradoksi, jossa valinta-aksiooman avulla konstruoidaan suljetun kuulan jako äärellisen moneen osaan, jotka uudelleenjärjestämällä saadaan kaksi alkuperäisen kokoista kuulaa.

TODISTUS. Zornin lemma on yhtäpitävä joukko-opillisen valinta-aksiooman kanssa. Tämän todistus sivuutetaan (ks. esim. Enderton: Elements of Set Theory). □



KUVA 13. Osa erästä osittaisjärjestystä. Tässä järjestyksessä pätee $b \leq a$, mutta alkiota x ei voi vertailla a:n tai b:n kanssa. Sekä a että b ovat molemmat ketjun C ylärajoja, ja a on maksimaalinen alkio.

LAUSEEN 6.8 TODISTUS. Olkoon R epätriviaali rengas. Tarkastellaan kaikkien R:n aitojen ideaalien muodostamaa kokoelmaa $\mathcal{P}$. Tämä on osittaisjärjestys sisältymisrelaation $\subset$ suhteen. Lisäksi $\mathcal{P}$ on epätyhjä, koska se sisältää vähintään nollaideaalin $\{0\}$. Osoitetaan, että jokaisella ketjulla on yläraja tässä osittaisjärjestyksessä.

Olkoon $\mathcal{A}$ jokin ketju. Selvästi jokainen $\mathcal{A}$:n alkio sisältyy yhdisteeseen $\cup\mathcal{A}$, joten riittää osoittaa, että $\cup\mathcal{A} \in \mathcal{P}$ eli että $\cup\mathcal{A}$ on aito ideaali. Ensinnäkin se on epätyhjä, koska $0 \in \{0\} \in \mathcal{A}$. Oletetaan, että $r \in R$ ja $a, b \in \cup\mathcal{A}$. Nyt löytyy jotkin ideaalit A ja B, joille pätee $a \in A$ ja $b \in B$. Koska $\mathcal{A}$ on ketju, voidaan olettaa, että $A \subset B$. Tällöin $a, b \in B$, ja koska B on ideaali, myös $a - b \in B$ ja $ra \in B$. Näin ollen
$$a - b \in \cup\mathcal{A} \qquad \text{ja} \qquad ra \in \cup\mathcal{A},$$
joten ideaalikriteerin perusteella $\cup\mathcal{A}$ on ideaali. Lisäksi $\cup\mathcal{A} \neq R$, koska kaikilla $B \in \mathcal{P}$ pätee $1 \notin B$. Yhdiste $\cup\mathcal{A}$ on siis eräs ketjun $\mathcal{A}$ yläraja.

Zornin lemman perusteella joukossa $\mathcal{P}$ on maksimaalinen alkio, joka on samalla haluttu maksimaalinen ideaali. □

Krullin lauseen todistusta hieman muuttamalla saadaan seuraava yleisempi tulos. Se voidaan myös johtaa seurauksena Krullin lauseesta.

KOROLLAARI 6.10. *Jos $A \neq \{0\}$ on renkaan R ideaali, niin on olemassa R:n maksimaalinen ideaali, joka sisältää A:n.*

Jos rengas R ei ole vaihdannainen, alkuideaalin määritelmä muuttuu hieman. Tässä tapauksessa sanotaan, että ideaali A on alkuideaali, jos $A \neq R$ ja kaikilla ideaaleilla B ja C pätee
$$BC \subset A \quad \Rightarrow \quad B \subset A \quad \text{tai} \quad C \subset A.$$

Tämä ehto voidaan lausua alkioiden avulla niin, että jos $bRc \subset A$, niin $b \in A$ tai $c \in A$, kun b ja c ovat mitä tahansa renkaan R alkioita. Vaihdannaisella renkaalla tämä palautuu aiempaan määritelmään, sillä jos $bc \in A$, niin $brc = bcr \in A$ kaikilla $r \in R$.

6.3. Jakorenkaat ja lokalisointi. Jakorengas on rengas, johon on lisätty käänteisalkioita, jotta jakolasku tulisi mahdolliseksi. Menetelmä tuli osin tutuksi jo erotusmonoidiesimerkin 1.5 yhteydessä. Tällä kertaa tarkastellaan yleisempää tapausta, jossa käänteisalkiot lisätään vain valituille alkioille.

Olkoon R vaihdannainen rengas ja S jokin kertolaskun suhteen suljettu osajoukko, joka sisältää ykkösalkion. Tarkoitus on lisätä renkaaseen R kaikkien S:n alkioiden käänteisalkiot. Tarkastellaan karteesisen tulon $R \times S$ (joka ei yleensä itse ole rengas) kaksipaikkaista relaatiota

$$(a_1, b_1) \sim (a_2, b_2) \iff c(a_1 b_2 - a_2 b_1) = 0 \quad \text{jollain } c \in S.$$

Tämä on sama ekvivalenssirelaatio kuin erotusmonoidiesimerkissä, nyt vain kirjoitettu eri muotoon renkaan laskutoimitusten avulla. Tekijärakennetta $(R \times S)/\sim$ nimitetään renkaan *jakorenkaaksi joukon S suhteen* ja merkitään $S^{-1}R$. Jakorenkaan alkiota $[(a, b)]_\sim$ voidaan merkitään murtolukumuodossa a/b. Jakorenkaaseen liittyy kanoninen kuvaus $\eta : R \to S^{-1}R$, missä $a \mapsto a/1$.

LAUSE 6.11. *Seuraavat väitteet pätevät renkaan R jakorenkaalle $S^{-1}R$:*

(a) *$S^{-1}R$ on vaihdannainen rengas, laskutoimituksina $a/b \cdot c/d = (ac)/(bc)$ ja $a/b + c/d = (ad + bc)/(bd)$.*
(b) *Kanoninen kuvaus η on rengashomomorfismi.*
(c) *Jos $s \in S$, kuva-alkiolla $\eta(s) \in S^{-1}R$ on käänteisalkio.*
(d) *Kanoninen kuvaus η on injektio, jos ja vain jos S ei sisällä nollanjakajia.*
(e) *$S^{-1}R$ on nollarengas, jos ja vain jos $0 \in S$.*

TODISTUS. Harjoitustehtävä. □

Edellisestä lauseesta seuraa erityisesti, että jos $S = R \setminus \{0\}$, jakorengas $S^{-1}R$ on kunta. Jos lisäksi R on kokonaisalue, kuntaa $S^{-1}R$ nimitetään R:n *osamääräkunnaksi.* Esimerkiksi $\mathbb{Q}$ on $\mathbb{Z}$:n osamääräkunta.

Ryhdytään seuraavaksi tarkastelemaan jakorenkaisiin liittyvää prosessia, jota nimitetään renkaan *lokalisoinniksi.*

MÄÄRITELMÄ 6.12. Rengasta, jolla on vain yksi maksimaalinen ideaali, kutsutaan *lokaaliksi* tai *paikalliseksi* renkaaksi.

Alkuideaalin avulla voidaan tuottaa paikallinen jakorengas.

LAUSE 6.13 (Lokalisointi). *Olkoon R rengas ja P sen jokin alkuideaali. Tällöin $S = R \setminus P$ on kertolaskun suhteen suljettu joukko, joka sisältää ykkösalkion, ja jakorengas $R_P = S^{-1}R$ on paikallinen rengas.*

TODISTUS. Koska $P \neq R$, nähdään että $1 \in S$. Olkoot $a, b \in S$. Jos tulo ab ei olisi joukossa S, se kuuluisi alkuideaaliin P. Alkuideaalin määritelmän mukaan joko $a \in P$ tai $b \in P$, mikä on mahdotonta. Täten S on kertolaskun suhteen suljettu.

Osoitetaan sitten, että joukko $M = \{a/b \mid a \in P, b \in S\}$ on ideaali renkaassa R_P. Koska $0 \in P$, nähdään että $M \neq \emptyset$. Olkoot sitten $a/b, c/d \in M$ ja $r/s \in R_P$. Tällöin $ac - bd \in P$, koska P on ideaali, ja $bd \in S$, koska S on kertolaskun suhteen suljettu. Näin ollen

$$\frac{a}{b} - \frac{c}{d} = \frac{ac - bd}{bd} \in M.$$

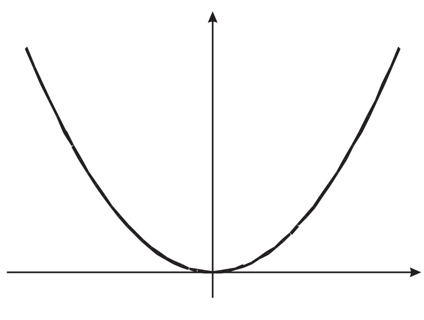
Samoin $ra \in P$ ja $sb \in S$, joten

$$\frac{r}{s} \cdot \frac{a}{b} = \frac{ra}{sb} \in M.$$

Ideaalikriteerin perusteella M on ideaali.

Näytetään lopuksi, että M on renkaan R_P ainoa maksimaalinen ideaali. Jos $A \not\subset M$ jollain ideaalilla A, niin löytyy alkio $a/b \in A \setminus M$. Tällöin $a \notin P$, joten $a \in S$, mistä seuraa, että a/b on kääntyvä alkio renkaassa R_P. Koska ideaali A sisältää kääntyvän alkion, se sisältää automaattisesti myös ykkösalkion, ja on siksi koko rengas. Tästä seuraa, että jokainen aito ideaali sisältyy ideaaliin M, joten M on ainoa maksimaalinen ideaali. □

Esimerkki 6.14. Lokalisointi-nimitys tulee algebrallisesta geometriasta. Tarkastellaan reaalikertoimisen polynomin $p = X^2 - Y$ nollakohtien joukkoa tasossa. Tämä joukko on paraabelin muotoinen algebrallinen käyrä. Koska f on jaoton renkaassa $\mathbb{R}[X, Y]$, sen virittämä ideaali $\langle p \rangle$ on alkuideaali. Lokalisoimalla voidaan muodostaa paikallinen rengas $\mathbb{R}[X, Y]_{\langle p \rangle}$. Se koostuu rationaalifunktioista f/g, missä f ja g ovat polynomeja ja $g \notin \langle p \rangle$.



Kuva 14. Polynomin $X^2 - Y$ nollakohtien joukko on paraabeli.

Renkaalla $\mathbb{R}[X, Y]_{\langle p \rangle}$ on sellainen ominaisuus, että sen sisältämät funktiot ovat määriteltyjä melkein kaikissa paraabelin pisteissä. Nimittäin, olkoon g sellainen polynomi, että $g(x, y) = 0$ äärettömän monessa paraabelin pisteessä. Tällöin voidaan osoittaa muun muassa, että g saa arvon nolla kaikissa paraabelin pisteissä ja että p jakaa polynomin g. Näin ollen $g \in \langle p \rangle$, joten kaikilla f pätee $f/g \notin \mathbb{R}[X, Y]_{\langle p \rangle}$. Voidaan ajatella, että lokalisoinnin avulla huomio on keskitetty kaikkien rationaalifunktioiden sijaista sellaiseen alueeseen, jonka funktiot on määritelty melkein koko paraabelilla. Vastaava konstruktio toimii myös korkeammissa ulottuvuuksissa.

Jos rengas ei ole vaihdannainen, tämän luvun menetelmät eivät sovellu sellaisinaan käytettäviksi. Itse asiassa ei ole edes selvää, että epävaihdannaisen renkaan alkioille ylipäätään voidaan lisätä käänteisalkioita. Jakorengas-nimitystä käytetään kuitenkin myös epävaihdannaisessa tapauksessa sellaisesta renkaasta, jossa jakolasku on mahdollinen. Tällaista rakennetta voidaan toisaalta ajatella epävaihdannaisena kuntana, ja silloin sitä nimitetään *vinokunnaksi*.