1 Algebralliset perusteet

1.1 Renkaat

Tämän luvun jälkeen opiskelijoiden odotetaan muistavan, mitä ovat renkaat, vaihdannaiset renkaat, alirenkaat, homomorfismit, ideaalit, tekijärenkaat, maksimaaliset ideaalit. He osaavat todistaa tuloksia näissä struktuureissa ja erottaa rakenteet toisistaan.

Määritelmä 1.1. *Rengas* R on Abelin ryhmä operaation $+$ suhteen, ja lisäksi R:ssä on assosiatiivinen binäärioperaatio $\cdot$, jolle pätee $a(b+c) = ab+ac$ ja $(a+b)c = ac+bc$.

Määritelmä 1.2. Renkaan R osajoukko on *alirengas*, jos se on suljettu operaatioiden $+$ ja $\cdot$ suhteen, siihen kuuluu additiivinen nolla-alkio.

Algebrallisia rakenteita tutkittaessa on hyödyllistä yrittää identifioida alijoukkoja, joilla itseasiassa on sama rakenne kuin itse isolla joukolla. Esimerkiksi ryhmällä on aliryhmä, ja jos jaamme ryhmän normaalilla aliryhmällä, saamme jakoryhmän. Renkaitten kohdalla normaalin aliryhmän paikan ottavat ideaalit.

Määritelmä 1.3. Renkaan R osajoukko I on *ideaali*, jos se on renkaan R additiivinen aliryhmä, ja kaikille $a \in I$ ja $r \in R$ pätee, että $ar \in I$ ja $ra \in I$. Jos vain toinen näistä pätee, kutsutaan ideaalia oikeaksi tai vasemmaksi ideaaliksi. Ideaali on aito, jos $I \neq R$. Ideaali I on *maksimaalinen*, jos ja vain jos $I \subseteq J \subseteq R$ ja J on ideaali, tästä seuraa, että $J = I$ ja $J = R$.

Määritelmä 1.4. Rengas R

1. on *vaihdannainen*, jos $xy = yx$ kaikille $x, y \in R$.
2. *sisältää ykkösalkion*, jos on olemassa yksikäsitteinen $0 \neq 1 \in R$, jolle pätee $1x = x1 = x\ \forall x$.
3. on *kokonaisalue*, jos se on vaihdannainen, ja siinä on ykkösalkio, sekä $ab = 0$ väistämättä tarkoittaa sitä, että $a = 0$ tai $b = 0$.
4. on *jakorengas*, jos siinä on ykkösalkio ja $R \setminus \{0\}$ on multiplikatiivinen ryhmä.
5. on *kunta*, jos se on kommutatiivinen jakorengas.

Esimerkki 1.5. (a) Kokonaisluvut $\mathbb{Z}$ on rengas, se on vaihdannainen, sillä kertolasku on vaihdannainen. Sillä on ykkösalkio 1, se on myös kokonaisalue, koska vain kertomalla nollalla saadaan nolla. Kuitenkaan $\mathbb{Z} \setminus \{0\}$ ei ole multiplikatiivinen ryhmä, sillä käänteisalkioita ei ole. Näin ollen, $\mathbb{Z}$ ei ole myöskään kunta.

(b) Tuttuja esimerkkejä kunnista ovat $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$.

(c) Rengas $\mathbb{Z}/m\mathbb{Z}$, eli kokonaisluvut $\mod m$ on selvästikin rengas. Se on vaihdannainen, ja siinä on ykkösalkio, mutta kokonaisalue se on vain siinä tapauksessa, että m on alkuluku. Esimerkiksi $m = 6$, silloin $2 \cdot 3 \equiv 0 \mod 6$, joten renkaassa on nollajakajia. Jos m on alkuluku, on rakenne myös kunta.

(d) $n \times n$ matriisit muodostavat renkaan, joka ei ole vaihdannainen, mutta sisältää ykkösalkion.

Määritelmä 1.6. Olkoot R ja S renkaita. Kuvaus $\varphi : R \longrightarrow S$ on *rengashomomorfismi*, jos $\varphi(a + b) = \varphi(a) + \varphi(b)$ ja $\varphi(ab) = \varphi(a)\varphi(b)$ kaikille $a, b \in R$.

Lause 1.7. *Olkoon R rengas, ja I ideaali, silloin on olemassa rengas R/I, jonka operaatio on $(a+I)(b+I) = ab+I$ ja lisäksi, R/I on vaihdannainen, jos R on vaihdannainen. R/I sisältää ykkösalkion jos $I \neq R$ ja R sisältää ykkösalkion.*

Todistus. Algebra I. □

Esimerkki 1.8. $\mathbb{Z}$ on rengas, $m\mathbb{Z}$ on ideaali, ja $\mathbb{Z}/m\mathbb{Z}$ on tekijärengas.

1.2 Kokonaisalueet ja kunnat

Tämän luvun jälkeen opiskelija osaa määritellä kokonaisalueet ja kunnat, antaa esimerkkejä näistä tietäen, mitkä määritelmät sisältyvät toisiinsa sekä antaa esimerkkejä, miksi nämä määritelmät ovat kaikki erilaisia struktuureja.

Tästä lähtien rengas tarkoittaa aina vaihdannaista rengasta ja se sisältää ykkösalkion.

Määritelmä 1.9. *Kokonaisalue* on kommutatiivinen rengas, jossa on ykkösalkio, ja jossa pätee $ab = 0$ vain jos $a = 0$ tai $b = 0$. (no zero divisors)

Esimerkki 1.10. $\mathbb{Z}$, $k[x]$, missä k on mikä tahansa kunta.

Lemma 1.11. *Äärellinen kokonaisalue on aina kunta.*

Todistus. Käytiin luennolla. □

Määritelmä 1.12. Olkoon R kommutatiivinen rengas, jossa on ykkösalkio. Olkoon $I \lhd R$ ideaali. Silloin I on *alkuideaali* jo $ab \in I \Rightarrow a \in I$ tai $b \in I$.

Esimerkki 1.13. $\mathbb{Z}$, jossa $I = p\mathbb{Z}$.

Lause 1.14. *Okoon R kommutatiivinen rengas, jossa on ykkösalkio, ja olkoon $I \lhd R$. Silloin I on alkuideaali, jos ja vain jos R/I on kokonaisalue.*

Todistus. Olkoon I alkuideaali. Tehdään vastaoletus, että renkaassa R/I on olemassa nollajakajia $a, b \neq 0$. Eli $(a + I)(b + I) = 0 + I = 0_{R/I}$. Silloin $ab + I = 0 + I$, mistä seuraa, että $ab \in I$. Koska I on alkuideaali, tämä tarkoittaa sitä, että $a \in I$ tai $b \in I$, joten oikeasti $a+I = 0+I$ tai $b+I = 0+I$, ja nollasta eroavia nollajakajia ei ole.

Oletetaan, että R/I on kokonaisalue, ja todistetaan, että I on alkuideaali. Oletetaan, että $ab \in I$, jolloin $ab + I = 0 + I$, mistä seuraa $(a + I)(b + I) = 0 + I = 0_{R/I}$. Koska R/I on kokonaisalue, tästä seuraa, että $a + I = 0 + I$ tai $b + I = 0 + I$ ja näin ollen $a \in I$ tai $b \in I$, ja I on alkuideaali. □

Lause 1.15. *Okoon R kommutatiivinen rengas, jossa on ykkösalkio, ja olkoon $I \lhd R$. Silloin I on maksimaalinen ideaali, jos ja vain jos R/I on kunta.*

Todistus. Harjoitustehtävä I/3. □

Määritelmä 1.16. Olkoon R kokonaisalue, ja olkoot I, J ideaaleja. Silloin

$$IJ = \{\sum_{i=1}^{k} a_i b_i : a_i \in I, b_i \in J, k \geq 1\}.$$

Huomaa, että IJ koostuu äärellisistä summista, mutta että summan pituus k vaihtelee.

1.3 Yksiköt, alkuluvut, alkuideaalit, irredusoimattomat alkiot

Koska kyseessä on lukuteorian kurssi, palautetaan mieleen Aritmetiikan peruslause, sillä pitkälti tässä kurssissa on kyse aritmetiikan peruslauseen laajennuksista erilaisiin renkaisiin.

Lause 1.17. *Luonnollisten lukujen joukossa, jos $n > 1$, silloin $n = p_1^{n_1} \dots p_k^{n_k}$, missä $p_1, \dots, p_k$ ovat erillisiä alkulukuja, ja $n_1, \dots, n_k \geq 1$. Jos $n \in \mathbb{Z}$, ja $|n| > 1$ se hajoaa tekijöiksi $n = q_1 \dots q_m$ missä q_i tai $-q_i$ on alkuluku $\mathbb{N}$:ssä. (Huomaa, että sama alkuluku voi toistua monta kertaa.)*

Tämän luvun tarkoituksena on laajentaa tämä määritelmä mille tahansa kokonaisalueelle, ensin tarvitsemme sopivan yleistyksen alkuluvuille ja jaottomille alkioille.

Määritelmä 1.18. Olkoon R kokonaisalue.

1. $u \in R$ on *yksikkö/kääntyvä alkio*, jos $\exists v \in R$, jolle pätee $uv = vu = 1$.
2. $a \in R$ on *jaoton/redusoimaton*, jos $a \neq 0$, a ei ole yksikkö ja $a = bc$ tarkoittaa, että joko b tai c on yksikkö.
3. $a \in R$ on *alkualkio*, jos $a \neq 0$, a ei ole yksikkö, ja $a \mid bc$ johtaa siihen, että $a \mid b$ tai $a \mid c$.

Lemma 1.19. *Kun R on kokonaisalue, alkualkiot ovat jaottomia.*

Todistus. Olkoon p alkualkio, ja oletetaan, että $p = ab$. Alkualkion määritelmän nojalla $p \mid a$ tai $p \mid b$. Valitaan, $p \mid a$, joten $a = pc$, jollekin c. Siispä $p = ab = pcb$. Tästä seuraa, että $p(1 - cb) = 0$, koska $p \neq 0$, ja kyseessä on kokonaisalue, tästä seuraa, että $cb = 1$, ja b on yksikkö. Näin ollen p on redusoimaton. □

Huomaa, että jaottomat alkiot eivät välttämättä ole alkualkioita. Tämä on totta kun R on pääideaalialue. Palaamme tähän myöhemmin.

Esimerkki 1.20. Renkaassa $\mathbb{Z}$ yksiköt ovat alkiot ± 1. Sen jaottomat alkiot ovat täsmälleen $\pm p$, jossa p on alkuluku, nämä ovat myös alkualkiot. Renkaassa $K[x]$, mikä tahansa astetta 1 oleva polynomi on jaoton. Yksiköitä ovat nollasta eroavat vakiopolynomit.

Määritelmä 1.21. Kokonaisalueella R on *yksikäsitteinen tekijöihinjako*, jos jokaiselle $a \in R$, joka ei ole nolla tai yksikkö, pätee

1. $a = p_1 p_2 \dots p_k$ jossa jokainen p_i on alkualkio.
2. Jos $p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$, missä p_i ja q_j ovat alkualkioita, silloin $k = l$ ja on olemassa indeksien $\{1, 2, \dots, k\}$ permutaatio σ, ja yksiköt $u_1, u_2, \dots, u_k$ siten, että

   $$p_i = u_i q_{\sigma(i)}$$

   kaikille $i = 1, 2, \dots, k$.

Propositio 1.22. *Olkoon K kunta. Jos $f \in K[x]$ on vähintään astetta 1 oleva polynomi, silloin on olemassa jaottomat polynomit $q_1, \dots, q_k$ joille pätee $f = q_1 \dots q_k$. (PID, joten yksikäsitteinen tekijöihinjako! mutta sitä emme vielä tiedä). Tässä vain olemassaolo!*

Todistus. Todistetaan väite induktiolla. Jos f:n aste on 1, on se redusoimaton. Oletetaan, että väite on tosi polynomeille, joiden asti on $< k$. Olkoon f polynomi, jonka aste on täsmälleen k. Jos f on redusoimaton, silloin ei ole mitään todistettavaa. Jos f ei ole redusoimaton, se voidaan kirjoittaa $f = gh$, ja $deg\ g, deg\ h < k$. Nyt voidaan soveltaa induktio hypoteesia polynomeihin g ja h, ja ne voidaan kirjoittaa redusoimattomien polynomien tulona

$$\begin{aligned} g =& q_1 \dots q_s \\ h =& q_{s+1} \dots q_r, \end{aligned}$$

mistä seuraa, että $f = q_1 \dots q_s$. □

Jaottomuus riippuu kunnasta! Esimerkiksi $x^2 - 2$ on jaoton kunnassa $\mathbb{Q}$, kun taas kunnassa $\mathbb{R}$ se hajoaa tuloksi $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Polynomi $x^2 + 1$ on jaoton kunnassa $\mathbb{Q}$ tai $\mathbb{R}$, mutta hajoaa kunnassa $\mathbb{C}$ kahden tuloksi $x^2 + 1 = (x - i)(x + i)$. Palaamme tähän asiaan parin luennon päästä, kun puhumme kuntalaajennusten teoriasta. Algebran peruslauseen nojalla tiedämme, että epävakio polynomi $f \in \mathbb{C}[x]$ hajoaa aina äärelliseksi tuloksi lineaarisia tekijöitä. Aina ei kuitenkaan tarvitse mennä kompleksilukujen kuntaan $\mathbb{C}$ saakka, jotta saamme polynomin hajoamaan lineaarisiksi tekijöiksi. Esimerkiksi kunta $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ on kunta, se on reaalilukujen $\mathbb{R}$ pienen alikunta, jossa $f(x) = x^2 - 2$ voidaan kirjoittaa lineaaristen polynomien tulona.

Samalla lailla $\{a + bi : a, b \in \mathbb{Q}\}$ on pienin kompleksilukujen $\mathbb{C}$ alikunta, jossa $x^2 + 1$ hajoaa lineaarisiksi tekijöiksi.

Kappaleen lopuksi kirjoitamme jäännöslauseen, joka on oiva aasinsilta Eukleideen algoritmiin.

Lause 1.23. *Jos $f \in K[x]$, missä K on kunta. Olkoon $a \in K$, silloin $(x-a) \mid f$ jos ja vain jos $f(a) = 0$.*

Todistus. $f(x) = (x-a)q(x)+r(x)$, missä $r(x) = 0$ tai se on vakiopolynomi. Sijoita $x = a$ ja silloin $f(a) = r$. □

1.4 Eukleideen alue, pääideaalialue, yksikäsitteinen tekijöihinjako

Tässä luvussa edelleen R tarkoittaa aina kokonaisaluetta. Tämän vuoksi emme puhu pääideaalirenkaista, emmekä faktorirenkaista.

Määritelmä 1.24. Olkoon R kokonaisalue. Silloin R on *Eukleideen alue*, jos on olemassa funktio

$$d : R \setminus \{0\} \longrightarrow \mathbb{N},$$

joka toteuttaa seuraavat ehdot

1. $d(ab) \geq d(a)$ $\forall a, b \neq 0$
2. Jos $a, b \neq 0$, on olemassa $q, r \in R$, joille pätee $a = bq + r$, missä joko $r = 0$ tai $r \neq 0$ ja $d(r) < d(b)$.

R:ssä voidaan siis soveltaa Eukleideen algoritmia. Tällaisia kokonaisalueita ovat mm $\mathbb{Z}$, ja $F[x]$. Ensimmäisessä astefunktio on $d(n) = |n|$ ja toisessa $d(p(x))$= polynomin p aste.

Propositio 1.25. *Gaussin kokonaisluvut $\mathbb{Z}[i]$ on Eukleideen alue.*

Todistus. Määritellään ensin Eukleideen astefunktio d asettamalla $d(m + ni) = m^2 + n^2 = |\ m + in|^2 \in \mathbb{Z}$. Tarkistetaan ensin, että tämä funktio on multiplikatiivinen. Jos $a, b \in \mathbb{Z}[i]$, silloin $d(ab) = |ab|^2 = |a|^2|b|^2 = d(a)d(b) \geq d(a)$ if $b \neq 0$, koska nämä ovat aina positiivisia kokonaislukuja. Tarkistetaan vielä Eukleideen algoritmin toimivuus.

Olkoot $a, b \in \mathbb{Z}[i]$, $a, b \neq 0$ ja $\frac{a}{b} \in \mathbb{C}$. Olkoon q kompleksitason pisteen $\frac{a}{b}$ lähin piste $\mathbb{Z}[i]$. Geometrisesti katsoen näemme, että $|q - \frac{a}{b}| \leq \frac{1}{\sqrt{2}}$. Nyt $r = a - bq \in \mathbb{Z}[i]$, silloin $a = bq + r$ ja $d(r) = |r|^2 = |a - bq|^2 = |(\frac{a}{b} - q)b|^2 = |\frac{a}{b} - q|^2|b|^2 \leq \frac{1}{2}|b|^2 = \frac{1}{2}d(b) < d(b)$. □

Määritelmä 1.26. Olkoon R kokonaisalue, ja $I \lhd R$. Silloin I on *pääideaali*, jos $I = aR$, jollekin $a \in I$. Usein kirjoitetaan myös $I = (a)$. Sanotaan, että R on *pääideaalialue*, jos jokainen sen ideaaleista on pääideaali.

Esimerkki 1.27. Pääideaalialueitea ovat $\mathbb{Z}$, $F[x]$, jossa F on mikä tahansa kunta. Toisaalta $\mathbb{Z}[x]$ ei ole pääideaalialue.

Lause 1.28. *Olkoon R Eukleideen alue. Silloin R on myös pääideaalialue.*

Todistus. Olkoon R Eukleideen alue ja olkoon $I \lhd R$. Tavoitteena on osoittaa, että $I = aR$, jollekin $a \in R$.

Jos $I = \{0\}$, silloin $I = aR$ on ok.

Jos $I \neq \{0\}$, valitaan $0 \neq b \in I$, jolle Eukleideen aste $d(b)$ on pienin mahdollinen. Osoitetaan, että $I = bR$. Ensiksi havaintaan, että koska $b \in I$ myös $br \in I$ kaikille r, joten $bR \leq I$.

Oletetaan, että $a \in I$, koska R on Eukleideen alue, on olemassa $q, r \in R$, joille pätee

$$a = bq + r,$$

missä $r = 0$ tai sitten $r \neq 0$ ja $d(r) < d(b)$. Koska $a \in I$ ja $bq \in I$, myös $r = a - bq \in I$. Koska b oli valittu minimaaliseksi, väistämättä $r = 0$. □

Määritelmä 1.29. Olkoon R kokonaisalue, ja $a, b \in R$, $(a, b \neq 0)$. Kutsumme alkiota d alkioiden a, b *suurimmaksi yhteiseksi tekijäksi*, jos i) $d \mid a$ ja $d \mid b$ eli d on kummankin tekijä. ii) jos $e \mid a$ ja $e \mid b$, silloin $e \mid d$, eli d on suurin yhteinen tekijä. Alkioita a ja b kutsutaan suhteellisiksi alkuluvuiksi, jos niiden suurin yhteinen tekijä d on yksikkö.

Esimerkki 1.30. Kokonaislukujen joukossa, luvut a, b ovat suhteellisia alkulukuja, jos ja vain jos $+1$ on a:n ja b:n suurin yhteinen tekijä. Renkaassa $K[x]$, polynomit f, g ovat suhteellisia alkulukuja, jos ja vain jos $d \mid f$ ja $d \mid g$ tarkoittavat yhdessä sitä, että d on vakiopolynomi.

Seuraava ominaisuus on kenties tärkein pääideaalialueen ominaisuuksista. Kuten Eukleideen alueella, myös pääideaalialueella on aina mahdollista löytää suurin yhteinen tekijä. Tämä on tärkeä lemma monissa todistuksissa, joten painakaa se mieleenne.

Lause 1.31. *Olkoon R pääideaalialue, ja olkoot $a, b \in R$. Silloin on olemassa a:n ja b:n suurin yhteinen tekijä $d \in R$, ja lisäksi pätee $d = ar + bs$, joillekin $r, s \in R$.*

Todistus. Olkoon $I = \{ar + bs : r, s \in R\}$. Tämä I sisältää nolla-alkion, on suljettu yhteen- ja kertolaskun suhteen, kuten myös R:n alkioitten kertolaskun suhteen. Näin ollen $I \lhd R$.

Koska R on pääideaalialue, $I = dR$, jollekin d. Koska $d \in I$, tästä seuraa, että $d = ar + bs$, joillekin r, s. Nyt $a = a \cdot 1 + b \cdot 0 \in I$, joten $d \mid a$, ja $b = a \cdot 0 + b \cdot 1$, joten $d \mid b$. Näin ollen d on yhteinen tekijä. Ja jos $e \mid a$ ja $e \mid b$, silloin $e \mid ar + bs = d$, joten d on suurin yhteinen tekijä. □

Lemma 1.32. *Jos R on pääideaalialue, silloin redusoimattomat alkiot ovat alkualkioita.*

Todistus. Olkoon R pääideaalialue, ja olkoon $a \in R$ redusoimaton. Oletaan, että $a \mid bc$. Olkoon $d = syt(a, b)$. Edellisen lemman perusteella voidaan kirjoittaa $d = ar + bs$, joillekin r, s. Nyt $d \mid a$, joten $a = de$ jollekin e. Koska a on redusoimaton, joko d tai e on yksikkö.

Jos d on yksikkö, silloin $c = cdd^{-1} = c(ar + bs)d^{-1} = acrd^{-1} + bcsd^{-1}$. Näin ollen $a \mid c$, koska $a \mid bc$.

Jos puolestaan e on yksikkö, silloin $a = de$ ja $d = ae^{-1}$. Mutta $d \mid b$ joten $b = df = ae^{-1}$ jollekin f. Näin $a \mid b$. □

Lause 1.33. *Olkoon R pääideaalialue, silloin R:ssä on myös yksikäsitteinen tekijöihinjako.*

Todistus. Todistus ei ole erityisen hankala, mutta se on työläs ja pitkä, joten sitä ei esitetä tässä. Kenties luennoilla tai laskuharjoituksissa. □