Euklidiset Renkaat

LuK-tutkielma
Eetu Lehtonen
Op#: 2583020
Matematiikan tutkinto-ohjelma
Oulun yliopisto
Kevät 2021

Sisällys

Johdanto

Tutkielmassa on käytetty lähteenä pääasiassa J.J. Rotmannin teosta *Advanced modern algebra* [1]. Tutkielmaa varten lukijalla on hyvä olla peruskäsitys kongruenssista ja algebrallisista ryhmärakenteista sekä niiden operaatioista. Ensimmäisessä luvussa käsitelään renkaiden $(R, +, \cdot)$ ja niiden ideaalien määritelmiä ja ominaisuuksia ja laajennetaan siitä kokonaisalueen määritelmään, jossa kahden renkaan nolla-alkiosta eroavien alkioiden $(\cdot)$-operaation tulos ei voi olla renkaan nolla-alkio 0_R, millään alkioilla. Tutkielmassa käydään myös läpi kuntien ja polynomirenkaiden määritelmä tässä luvussa, sillä niistä on hyödynnettävissä muutama esimerkki ja lause tutkielman loppua varten.

Toisessa luvussa käsitellään euklidisen renkaan määritelmä, jossa kokonaisalueelle määritellään astefunktio ja tämän astefunktion avulla määriteltävä jakoalgoritmi. Lopuksi käydään läpi kolme esimerkkiä euklidisista renkaista ja tärkeimpänä Gaussin kokonaisluvut, jotka ovat muotoa $a + bi$, missä $a, b \in \mathbb{Z}$ ja $i^2 = -1$. Tässä luvussa käsitellään myös mitä tarkoittaa, kun astefunktio on normi.

Kolmannessa luvussa käsittellään euklidisten renkaiden ominaisuuksia kuten, että jokainen euklidinen rengas on pääideaalirengas sekä yleisen jakajan määritelmä. Lopuksi tutkielma päätetään näiden ominaisuuksien ja muutaman apulemman avulla päästävään Fermat'n kahden neliön lauseeseen, jonka mukaan pariton alkuluku $p \equiv 1 \mod 4$ jos ja vain jos on olemassa kokonaisluvut a ja b siten, että $p = a^2 + b^2$.

1 Renkaat ja ideaalit

1.1 Johdanto

Jotta euklidisten renkaiden ja niiden pääideaalien määritelmät olisivat selkeitä, tulee lukijan tietää myös renkaiden, ideaalien ja kokonaisalueiden määritelmät ja niihin liittyvät tärkeimmät lauseet. Lisäksi käydään myös läpi lyhyesti polynomirenkaan ja sen astefunktion määritelmä, sillä siitä on esimerkki tutkielman varsinaisessa aiheessa.

1.2 Renkaat

Määritelmä 1.1. Olkoon R epätyhjä joukko, sekä $(+)$ ja $(\cdot)$ joukon R operaatioita. Kolmikko $(R, +, \cdot)$ on *rengas* mikäli:

- Joukko $(R, +)$ on Abelin ryhmä, eli

  1. Operaatio $(+)$ on binäärinen, eli:
     Kaikilla a, $b \in R$ pätee

     $$a + b \in R \text{ ja alkio } a + b \text{ on yksikäsitteinen.}$$

  2. Operaatio $(+)$ on assosiatiivinen, eli:
     Kaikilla a, b, $c \in R$ pätee

     $$a + (b + c) = (a + b) + c.$$

  3. Joukossa R on neutraalialkio $(+)$-operaation suhteen eli nollaalkio 0_R. Tällöin

     $$0_R + a = a + 0_R = a \text{ kaikilla } a \in R.$$

     Eli joukossa R on olemassa yksikäsitteinen alkio, jolla operoimalla jokainen joukon alkio pysyy muuttumattomana.

  4. Jokaisella joukon R alkiolla a on olemassa käänteisalkio $(+)$-operaation suhteen eli vasta-alkio $-a$. Tällöin

     $$a + (-a) = (-a) + a = 0_R.$$

  5. Operaatio $(+)$ on kommutatiivinen, eli:
     Kaikilla a, $b \in R$ pätee

     $$a + b = b + a.$$

- Joukko $(R, \cdot)$ on monoidi, eli

  1. Operaatio $(\cdot)$ on binäärinen, eli:
     Kaikilla a, $b \in R$ pätee

     $$a \cdot b \in R \text{ ja alkio } a \cdot b \text{ on yksikäsitteinen.}$$

  2. Operaatio $(\cdot)$ on assosiatiivinen, eli:
     Kaikilla a, b, $c \in R$ pätee

     $$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

  3. Joukossa R on neutraalialkio $(\cdot)$-operaation suhteen eli ykkösalkio 1_R. Tällöin

     $$1_R \cdot a = a \cdot 1_R = a \text{ kaikilla } a \in R.$$

     Eli joukossa R on olemassa yksikäsitteinen alkio, jolla operoimalla jokainen joukon alkio pysyy muuttumattomana.

- Joukolle $(R, +, \cdot)$ pätee distributiivisuus eli osittelulait siten, että

  1. $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla a, b, $c \in R$.
  2. $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla a, b, $c \in R$.

Esimerkkejä renkaista ovat mm. kokonaisluvut $\mathbb{Z}$, rationaaliluvut $\mathbb{Q}$, reaaliluvut $\mathbb{R}$ ja 2x2-matriisit. Kaikissa näissä pätee yllä olevat laskusäännöt yhteenlaskun ja kertolaskun suhteen. Huomioitavaa on, että joukon operaatio ei välttämättä ole aina yksinkertainen yhteen- tai kertolasku, vaikka operaatioita yleisimmin merkitään $(+)$- ja $(\cdot)$-merkeillä.

Määritelmä 1.2. Olkoon $(R, +, \cdot)$ rengas. Rengasta sanotaan *kommutatiiviseksi renkaaksi*, jos se on kommutatiivinen $(\cdot)$-operaation suhteen, eli

$$a \cdot b = b \cdot a \text{ kaikilla } a, b \in R.$$

Käytetään tästä eteenpäin merkinnästä $a \cdot b$ muotoa, jossa $(\cdot)$-operaation merkki jätetään pois, eli muotoa ab. Tällä merkinnällä siis viitataan renkaan jälkimmäiseen operaatioon.

1.3 Ideaalit

Määritelmä 1.3. Olkoon $(R, +, \cdot)$ rengas ja I sen epätyhjä osajoukko. Joukko I on renkaan R *ideaali*, mikäli

1. $a - b = a + (-b)$ on joukon I alkio kaikilla a, $b \in I$.
2. $ra \in I$ kaikilla $a \in I$ ja $r \in R$.
3. $ar \in I$ kaikilla $a \in I$ ja $r \in R$.

Esimerkki 1.4. Käydään läpi muutamia esimerkkejä ideaaleista:

- $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ on kokonaislukurenkaan $(\mathbb{Z}, +, \cdot)$ ideaali, sillä
  1. $2n + (-2m) = 2n - 2m = 2(n - m) \in 2\mathbb{Z}$,
  2. $2n \cdot z = 2(nz) \in 2\mathbb{Z}$,
  3. $z \cdot 2n = 2(nz) \in 2\mathbb{Z}$.
- Renkaan R triviaalit ideaalit ovat $\{0_R\}$ ja R.

Määritelmä 1.5. Olkoon $(R, +, \cdot)$ rengas ja a joukon R alkio. Nyt suppeinta ideaalia I, joka sisältää alkion a sanotaan *alkion a generoimaksi pääideaaliksi* ja siitä käytetään merkintää (a).

Esimerkki 1.6. Nollan muodostama joukko $\{0\}$ on kokonaislukurenkaan $\mathbb{Z}$ alkion 0 generoima pääideaali, sillä se on suppein ideaali, joka sisältää alkion 0.

1.4 Kokonaisalueet ja kunnat

Määritelmä 1.7. Renkaan $(R, +, \cdot)$ nolla-alkiosta poikkeava alkio a on renkaan *nollanjakaja*, mikäli renkaassa on olemassa sellainen nolla-alkiosta eroava alkio b, että $ab = 0_R$ tai $ba = 0_R$.

Määritelmä 1.8. Kommutatiivista rengasta R, jossa ei ole nollanjakajia, sanotaan *kokonaisalueeksi*.

Määritelmä 1.9. Olkoon R kokonaisalue ja $a, b \in R$. Alkio a jakaa alkion b, eli alkio a on alkion b *tekijä*, jos on olemassa sellainen alkio $u \in R$, että $b = ua$.

Määritelmä 1.10. Olkoon R kokonaisalue ja a sen alkio. Jos alkio a jakaa ykkösalkion 1_R joukossa R, merkitään $a|1_R$, niin a on joukon R *yksikkö*. Lisäksi, jos joukossa R on olemassa sellainen alkio b, että $ab = ba = 1_R$, niin alkiota b sanotaan alkion a *käänteisalkioksi.*

Lause 1.11. *Olkoon R kokonaisalue, $a, b, c \in R$ ja $a \neq 0_R$. Jos $ab = ac$, niin $b = c$.*

Todistus: Olkoon R kokonaisalue, $a, b, c \in R$ ja $a \neq 0_R$. Nyt koska R on kokonaisalue ja $a \neq 0$. Tällöin

$$\begin{aligned} & ab = ac \\ \Leftrightarrow\ & ab + (-ac) = 0_R \\ \Leftrightarrow\ & ab + a(-c) = 0_R \\ \Leftrightarrow\ & a(b + (-c)) = 0_R \\ \Leftrightarrow\ & b + (-c) = 0_R \\ \Leftrightarrow\ & b = c \end{aligned}$$

□

Määritelmä 1.12. Olkoon R kokonaisalue ja $a \in R$. Alkio a on *jakautuva* kokonaisalueessa R, jos se ei ole nolla-alkio tai ykkösalkio ja $a = uv$, missä $u, v \in R$ eivät ole yksiköitä.

Määritelmä 1.13. Olkoon R kokonaisalue ja $a \in R$. Alkio a on *jakautumaton* kokonaisalueessa R, jos se ei ole nolla-alkio tai ykkösalkio ja kaikissa sen tekijöihinjaoissa muotoa $a = uv$, missä $u, v \in R$, joko u tai v on yksikkö. Lisäksi jos $b, a \in R$ ovat *vastaavia alkioita*, niin on olemassa sellainen yksikkö $u \in R$, että $b = ua$.

Määritelmä 1.14. Kommutatiivinen rengas $(R, +, \cdot)$ on *kunta*, jos $(R\backslash\{0_R\}, \cdot)$ on Abelin ryhmä. Tällöin ryhmä $(R, +)$ on kunnan R *additiivinen ryhmä* ja ryhmä $(R\backslash\{0_R\}, \cdot)$ on kunnan R *multiplikatiivinen ryhmä.*

1.5 Polynomirenkaat

Määritelmä 1.15. Olkoon $(K, +, \cdot)$ kunta. Merkitään

$$K[x] = \{a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 | a_i \in K, n \in \mathbb{N}\}.$$

Tämän joukon alkioita kutsutaan *K-kertoimisiksi polynomeiksi* ja koko joukkoa $K[x]$ varustettuna $(+)$- ja $(\cdot)$-operaatioilla *polynomirenkaaksi kunnan K suhteen.*

Esimerkki 1.16. Reaalilukukertoimisten polynomien joukko $\mathbb{R}[x]$ on polynomirengas kunnan $\mathbb{R}$ suhteen.

Määritelmä 1.17. Olkoon K kunta. Jos

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in K[x],$$

ja $a_n \neq 0_K$, niin kyseisen polynomin *aste* on n; merkitään $\deg(f) = n$. Edelleen, jos $a_0 \neq 0_K$, niin vakiopolynomin $f(x) = a_0$ aste on $\deg(f(x)) = \deg(a_0) = 0$. Lisäksi nollapolynomin $0_{K[x]} = 0_K$ aste on $\deg(0_K) = -\infty$.

2 Euklidiset renkaat

2.1 Johdanto

On olemassa muitakin joukkoja, kuin kokonaisluvut $\mathbb{Z}$ ja polynomirengas $K[x]$, joille pätee jakoalgoritmi. Tässä luvussa keskitytään algebrallisiin rakenteisiin, joissa on voimassa astefunktio ja niiden avulla määriteltävä jakoalgoritmi.

2.2 Euklidisen renkaan määritelmä

Määritelmä 2.1. Kokonaisalue R on *euklidinen rengas*, jos sille on olemassa funktio

$$\partial : R\backslash\{0_R\} \to \mathbb{N},$$

nimeltään *astefunktio* siten, että

1. $\partial(a) \leq \partial(ab)$ kaikilla $a, b \in R\backslash\{0_R\}$.
2. Kaikille $a, b \in R$, missä $b \neq 0_R$, on olemassa sellaiset $q, r \in R$, että

$$a = qb + r,$$

missä joko $r = 0_R$ tai $\partial(r) < \partial(b)$.

Huomioitavaa on, että jos kokonaisalueella R on astefunktio ∂ siten, että $\partial(a) = 0$ kaikilla $a \in R\backslash\{0_R\}$, niin 2. ehdon nojalla $r = 0_R$ aina. Lisäksi, jos asetetaan $a = 1_R$ niin huomataan, että R on kunta.

Esimerkki 2.2. Todistetaan, että kokonaislukujen joukko $\mathbb{Z}$ on määritelmän 2.1 mukainen euklidinen rengas astefunktiolla $\partial : \mathbb{Z} \to \mathbb{N},\ \partial(m) = |m|$. Kokonaislukujen joukko on kokonaisalue, sillä se on kommutatiivinen rengas, jossa ei ole nollanjakajia.

1. Olkoon $m, n \in \mathbb{Z}\backslash\{0\}$. Joukossa $\mathbb{Z}\backslash\{0\}$ pätee

$$\partial(m) = |m| \leq |mn| = \partial(mn) = |m||n| = \partial(m)\partial(n).$$

2. Olkoon $m, n \in \mathbb{Z}$ ja $n \neq 0$. Nyt näille luvuille pätee jakoalgoritmi siten, että

$$m = qn + r,$$

missä $q, r \in \mathbb{Z}$ ja $0 \leq r < |n|$, eli $r = 0$ tai $r = |r| = \partial(r) < \partial(n) = |n|$. Näin ollen kokonaislukujen joukko $\mathbb{Z}$ on euklidinen rengas astefunktiolla $\partial(m) = |m|, m \in \mathbb{Z}$.

Kokonaislukujen muodostaman euklidisen renkaan avulla päästään myös seuraavaan määritelmään:

Määritelmä 2.3. Jos astefunktio ∂ on multiplikatiivinen, eli

$$\partial(fg) = \partial(f)\partial(g),$$

niin astefunktiota ∂ kutsutaan *normiksi*.

Esimerkki 2.4. Todistetaan nyt, että jos K on kunta, niin polynomirengas $K[x]$ on määritelmän mukainen euklidinen rengas määritelmän 1.13 mukaisella astefunktiolla $\deg(f)$, joka antaa yleisen polynomifunktion asteen kaikille $f \in K[x]$. Eli $\partial(f) = \deg(f)$. Polynomirengas $K[x]$ on kokonaisalue, sillä siinä ei ole nollanjakajia, toisin sanoin $fg \neq 0_K$ kaikilla $f, g \in K[x]\backslash\{0_K\}$.

1. Olkoon $f, g \in K[x]\backslash\{0_K\}$ ja $\deg(f) = n$ ja $\deg(g) = m$. Nyt polynomirenkaassa $K[x]$ pätee

   $$f \cdot g = (a_n x^n + ... + a_0)(b_m x^m + ... + b_0) = a_n b_m x^{n+m} + ... + a_0 b_0.$$

   Tämän perusteella voidaan todeta, että

   $$\partial(f) = n \leq n + m = \deg(f) + \deg(g) = \deg(fg) = \partial(fg).$$

   Lisäksi huomataan, että

   $$\partial(fg) = \deg(fg) = \deg(f) + \deg(g) \neq \deg(f) \cdot \deg(g) = \partial(f) \cdot \partial(g),$$

   eli astefunktio ei ole normi.

2. Olkoon $f, g \in K[x]$ ja $g \neq 0_K$. Polynomeille pätee jakoalgoritmi siten, että

   $$f = qg + r,$$

   missä $q, r \in K[x]$ ja $\deg(r) < \deg(g)$.

   Tämän perusteella polynomirengas $K[x]$ on euklidinen rengas astefunktiolla $\partial(f) = \deg(f)$.

Esimerkki 2.5. Tutkitaan vielä kolmantena, muodostavatko Gaussin kokonaislukujen joukko $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ euklidisen renkaan, jonka astefunktio on

$$\partial(a + bi) = a^2 + b^2.$$

Olkoon $\alpha = a + bi$, $\beta = c + di \in \mathbb{Z}[i]\backslash\{0\}$. Nyt

$$\alpha\beta = (a + bi)(c + di) = ac - bd + (ad + bc)i.$$

Tässä vähintään yksi termi on erisuuri kuin nolla eli $\alpha\beta \neq 0$. Tämän perusteella Gaussin kokonaisluvut on kokonaisalue.

Jos oletetaan, että $\alpha = a + bi \in \mathbb{Z}[i]$, niin sen kompleksikonjugaatti on $\overline{\alpha} = a - bi$. Tämän avulla voidaan siis merkitä:

$$\partial(\alpha) = a^2 + b^2 = (a + bi)(a - bi) = \alpha\overline{\alpha}.$$

Tämän avulla saadaan

$$\partial(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \partial(\alpha)\partial(\beta),$$

eli Gaussin kokonaislukujen astefunktio on normi.

1. Nyt määritelmän 2.1 mukaisesti tutkitaan euklidisen renkaan ehdot. Olkoon $\beta = c + di \in \mathbb{Z}[i]$ ja $\beta \neq 0$, nyt

   $$1 \leq \partial(\beta),$$

   sillä $\partial(\beta) = c^2 + d^2$ on positiivinen kokonaisluku. Tästä siis seuraa, että jos $\alpha, \beta \in \mathbb{Z}[i]\backslash\{0\}$, niin

   $$\partial(\alpha) \leq \partial(\alpha)\partial(\beta) = \partial(\alpha\beta).$$

2. Olkoon $\alpha, \beta \in \mathbb{Z}[i]$ ja $\beta \neq 0$. Nyt $\alpha/\beta \in \mathbb{C}$ ja

   $$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{\partial(\beta)},$$

   missä $\partial(\beta) \in \mathbb{Z}_+$. Tämän perusteella siis

   $$\frac{\alpha}{\beta} = x + yi,\ x, y \in \mathbb{Q}.$$

Nyt voidaan merkitä $x = a + u$ ja $y = b + v$, missä a ja b ovat rationaalilukujen x ja y lähimmät kokonaisluvut. Vastaavasti seuraa, että $|u|, |v| \leq \frac{1}{2}$. Tätä hyödyntämällä saadaan siis

$$\frac{\alpha}{\beta} = a + bi + u + vi,$$

eli

$$\alpha = \beta(a + bi) + \beta(u + vi).$$

Huomataan, että $\beta(u + vi) = \alpha - \beta(a + bi) \in \mathbb{Z}[i]$.

Lopuksi tutkitaan $\partial(\beta(u + vi))$. Eli ∂ on euklidisen renkaan astefunktio, jos

$$\partial(\beta(u + vi)) < \partial(\beta).$$

Nyt, koska $|u| \leq \frac{1}{2}$ ja $|v| \leq \frac{1}{2}$, niin tästä seuraa

$$\partial(u + vi) = u^2 + v^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Tästä seuraa suoraan, että

$$\partial(\beta(u + vi)) = \partial(\beta)\partial(u + vi) < \partial(\beta) \cdot 1 \leq \partial(\beta).$$

Tässä on tärkeää huomata, että $u + vi \notin \mathbb{Z}[i]$, mutta $\beta(u + vi) \in \mathbb{Z}[i]$.

Tämän avulla voidaan todeta, että Gaussin kokonaislukujen joukko $\mathbb{Z}[i]$ on euklidinen rengas astefunktiolla $\partial(a + bi) = a^2 + b^2$, joka on lisäksi normi.

3 Euklidisten renkaiden sovelluksia

3.1 Euklidisten renkaiden ominaisuuksia

Lause 3.1. *Olkoon R euklidinen rengas. Jos astefunktio $\partial(a) = 0$ kaikilla $a \in R$, niin euklidinen rengas R on kunta.*

Todistus: Olkoon R euklidinen rengas ja $\partial(a) = 0$ kaikilla $a \in R$. Nyt on olemassa sellaiset $b \in R\backslash\{0_R\}$ ja $q, r \in R$, että

$$1_R = qb + r.$$

Nyt $\partial(r) < \partial(b)$ tai $r = 0_R$. Koska oletetaan, että $\partial(a) = 0$ kaikilla euklidisen renkaan R alkioilla, niin tästä seuraa, että $r = 0_R$. Tästä siis puolestaan seuraa, että

$$1_R = qb,$$

eli jokainen euklidisen renkaan nolla-alkiosta eroava alkio on yksikkö ja euklidinen rengas on tällöin kunta. □

Seuraus: Jos euklidinen rengas R ei ole kunta, niin sen astefunktion arvo kaikilla nolla-alkiosta eroavilla alkioilla on erisuuri kuin nolla.

Lause 3.2. *Jokainen euklidinen rengas on pääideaalirengas, eli kaikki sen ideaalit ovat pääideaaleja.*

Todistus: Olkoon R euklidinen rengas ja I sen ideaali. Jos $I = \{0_R\}$, niin $I = (0_R)$ on triviaali pääideaali. Voidaan siis olettaa, että $I \neq \{0_R\}$. Pienimmän kokonaisluvun aksiooman nojalla kaikkien ideaalin I alkioiden astelukujen joukossa on olemassa pienin asteluku n. Kuitenkin pitää muistaa, että $0_R \in I$. Valitaan nyt $b \in I$ siten, että $\partial(b) = n$. Osoitetaan nyt, että $I = (b)$. Selvästi $(b) \subseteq I$, sillä joko $(b) = I$, tai on olemassa ideaalia I suppeampi ideaali, johon alkio b kuuluu. Riittää siis todistaa, että $I \subseteq (b)$.

Olkoon $a \in I$, nyt on olemassa sellaiset $q, r \in R$, että

$$a = qb + r,$$

missä $r = 0_R$ tai $\partial(r) < \partial(b)$. Koska $r = a - qb \in I$ ja alkion b aste on pienin ei-nolla-alkion aste, niin $r = 0_R$ ja näin ollen $a = qb \in (b)$, eli $I \subseteq (b)$. Siispä $I = (b)$. □

Määritelmä 3.3. Kokonaisalueen R alkio a on joukon R *yleinen jakaja*, jos se ei ole yksikkö ja jos jokaiselle $r \in R$ pätee, että $a|r$ tai on olemassa sellainen yksikkö $s \in R$, että $a|(r+s)$.

Lause 3.4. *Jos R on euklidinen rengas, mutta ei ole kunta, niin sillä on yleinen jakaja*

Todistus: Olkoon

$$S = \{\partial(v) : v \neq 0_R \text{ ja } v \text{ ei ole yksikkö}\},$$

missä ∂ on euklidisen renkaan R astefunktio ja $v \in R$. Pienimmän kokonaisluvun aksiooman nojalla tiedetään, että joukossa S on olemassa pienin alkio $\partial(u)$. Nyt jos $x \in R$, niin on olemassa sellaiset alkiot $q, r \in R$, että $x = qu+r$, missä $r = 0_R$ tai $\partial(r) < \partial(u)$. Jos $r = 0_R$, niin $x = qu$, eli $u|x$. Toisaalta, jos $r \neq 0_R$, niin alkion r täytyy olla yksikkö, sillä muuten sen olemassaolo on ristiriidassa astefunktion arvon $\partial(u)$ kanssa, joka on joukon S pienin alkio. Tällöin, koska

$$x = qu + r$$

eli

$$qu = x - r \in R,$$

niin $u|(x + (-r))$, missä $-r$ on yksikkö. Näiden perusteella siis alkio u on euklidisen renkaan R yleinen jakaja. □

Lause 3.5.

1. *Olkoon R euklidinen rengas, joka ei ole kunta. Jos sen astefunktio ∂ on normi, niin alkio $a \in R$ on yksikkö jos ja vain jos $\partial(a) = 1$.*

2. *Olkoon R euklidinen rengas, joka ei ole kunta. Jos sen astefunktio ∂ on normi ja alkion $a \in R$ asteluku on $\partial(a) = p$, missä p on alkuluku, niin a on jakautumaton.*

3. *Ainoat yksiköt Gaussin kokonaislukujen muodostamassa euklidisessa renkaassa $\mathbb{Z}[i]$ ovat ± 1 ja $\pm i$.*

Todistus: 1. Koska euklidisen renkaan R astefunktio ∂ on normi, niin

$$\partial(1_R)^2 = \partial(1_R^2) = \partial(1_R)$$

ja tästä seuraa, että $\partial(1_R) = 0$ tai $\partial(1_R) = 1$.

Jos $\partial(1_R) = 0$, niin

$$\partial(a) = \partial(1_R a) = \partial(1_R)\partial(a) = 0$$

kaikille $a \in R$. Koska R ei ole kunta, siinä ei ole jokaiselle alkiolle käänteisalkiota, joten astefunktion ∂ arvo ei voi olla kaikille euklidisen renkaan R alkioille 0. Tämän perusteella siis $\partial(1_R) = 1$.

Jos $a \in R$ on yksikkö, niin on olemassa $b \in R$ siten, että $ab = 1_R$. Toisinsanoin $b = a^{-1}$. Koska astefunktio on normi, niin $\partial(ab) = \partial(a)\partial(b) = 1$. Koska astefunktio saa vain ei-negatiivisia kokonaislukuarvoja, niin $\partial(a) = 1$.

Toisaalta, olkoon nyt $\partial(a) = 1$. Nyt on olemassa sellaiset $q, r \in R$, että $a = qa^2 + r$, missä $r = 0_R$ tai $\partial(r) < \partial(a^2)$. Koska astefunktio on normi, niin

$$\partial(a^2) = \partial(a \cdot a) = \partial(a)^2 = 1,$$

eli joko $r = 0_R$ tai $\partial(r) = 0$. Toisaalta koska ∂ on normi, niin

$$\partial(b) \leq \partial(rb) = \partial(r)\partial(b)$$

kaikilla $b \in R\backslash\{0_R\}$. Tämän avulla voidaan todeta, että $\partial(r) \neq 0$, sillä muuten euklidinen rengas olisi kunta, koska $\partial(b) = 0$ kaikilla $b \in R\backslash\{0_R\}$. Alkio r on täten euklidisen renkaan nolla-alkio 0_R. Tämän perusteella $a = qa^2$. Tästä seuraa lauseen 1.11 nojalla, että $1_R = qa$, eli alkio a on yksikkö.

2. Olkoon $a \in R\backslash\{0_R\}$ ja $\partial(a) = p$, missä p on alkuluku. Tehdään vastaoletus, että $a = bc$, missä b ja c eivät ole yksiköitä. Nyt

$$p = \partial(a) = \partial(bc) = \partial(b)\partial(c).$$

Nyt koska p on alkuluku niin $\partial(b) = 1$ tai $\partial(c) = 1$. Nyt lauseen ensimmäisen kohdan perusteella b tai c on yksikkö. Tämä on ristiriidassa määritelmän 1.12 kanssa ja näin ollen alkio a on jakautumaton euklidisessa renkaassa R.

3. Olkoon alkio $\alpha = a + bi \in \mathbb{Z}[i]$ yksikkö. Nyt lauseen ensimmäisen kohdan ja Gaussin kokonaislukujen astefunktion perusteella $1 = \partial(\alpha) = a^2 + b^2$. Tämä pätee ainoastaan, jos $a^2 = 1$ ja $b^2 = 0$ tai $a^2 = 0$ ja $b^2 = 1$. Täten siis $\alpha = \pm 1$ tai $\alpha = \pm i$. □

3.2 Fermat'n kahden neliön lause

Jos n on pariton luku, niin joko $n \equiv 1 \mod 4$ tai $n \equiv 3 \mod 4$. Tämän avulla myös parittomat alkuluvut voidaan jakaa kahteen ryhmään. Esimerkiksi 5, 13 ja 17 ovat kongruenssissa luvun 1 kanssa mod 4 kun taas 3, 7 ja 11 ovat kongruenssissa luvun 3 kanssa mod 4.

Lause 3.6. (Aritmetiikan peruslause) *Kaikki positiiviset kokonaisluvut poislukien 1 voidaan muodostaa yksikäsitteisesti yhden tai useamman alkuluvun tulona.*

Lause 3.7. (Eukleideen lemma) *Jos alkuluku p jakaa kahden kokonaisluvun a ja b tulon ab, niin alkuluvun p täytyy jakaa ainakin toinen luvuista a ja b.*

Lemma 3.8. *Jos p on alkuluku ja $p \equiv 1 \mod 4$, niin on olemassa kokonaisluku m siten, että*

$$m^2 \equiv -1 \mod p.$$

Todistus: Olkoon $G = (\mathbb{Z}_p^*, \cdot)$ kaikkien nollasta eroavien kokonaislukujen alkuluvun p jäännösluokkien multiplikatiivinen ryhmä. Nyt $|G| = p - 1 \equiv 0 \mod 4$; näin ollen siis ryhmän G alkioiden määrä on jaollinen neljällä. Eli ryhmällä G on olemassa aliryhmä S, jossa on neljä alkiota. Koska jäännösluokat muodostavat Abelin ryhmän, niin S on joko syklinen tai $a^2 = [1]$ kaikille $a \in S$. Koska jäännösluokat modulo p on kunta, niin sillä ei voi olla neljää ratkaisua yhtälölle $x^2 - 1$. Näin ollen siis S on syklinen, eli $S = \langle [m] \rangle$, missä $[m]$ on luvun m jäännösluokka modulo p. Koska $|S| = 4$, niin $[m]^4 = [1]$. Koska $[m]^4 = [1]$, niin $[m]^2 = [1]$ tai $[m]^2 = [-1]$. Koska $|S| = 4$, niin $[m]^2 = [1]$ ei ole mahdollinen. Näin ollen siis $[m]^2 = [m^2] = [-1]$, eli $m^2 \equiv -1 \mod p$. □

Lause 3.9. (Fermat'n kahden neliön lause). *Pariton alkuluku p on kahden kokonaisluvun a ja b neliön summa*

$$p = a^2 + b^2,$$

jos ja vain jos $p \equiv 1 \mod 4$.

Todistus:

$\Rightarrow$: Olkoon $p = a^2 + b^2$. Koska p on pariton, niin luvuista a ja b toinen on parillinen ja toinen pariton. Olkoon a parillinen ja b pariton. Nyt siis $a = 2m$ ja $b = 2n + 1$, missä $m, n \in \mathbb{Z}$. Nyt

$$p = a^2 + b^2 = (2m)^2 + (2n+1)^2 = 4m^2 + 4n^2 + 4n + 1 \equiv 1 \mod 4,$$

sillä $4 \mid (4m^2 + 4n^2 + 4n + 1) - 1$.

$\Leftarrow$: Olkoon p alkuluku ja $p \equiv 1 \mod 4$. Lemman 3.8. nojalla on olemassa nollasta eroava kokonaisluku m siten, että

$$p \mid m^2 + 1,$$

sillä p ei jaa lukua yksi. Gaussin kokonaislukujen joukossa voidaan jakaa tekijöihin $m^2 + 1 = (m + i)(m - i)$, eli

$$p \mid (m + i)(m - i),$$

Gaussin kokonaislukujen joukossa. Jos p on jakautumaton ja $p|(m+i)(m-i)$, niin on olemassa sellaiset kokonaisluvut u ja v, että $(m+i) = p(u + vi)$ tai $(m - i) = p(u + vi)$. Kun näiden imaginääriosia verrataan, saadaan $pv = 1$ tai $pv = -1$, mikä tarkoittaa, että p on yksikkö Gaussin kokonaisluvuissa. Tämä on ristiriita lauseen 3.5 kanssa. Koska $m \neq 0$, niin $m + i$ ja $m - i$ eivät ole lauseen 3.5 mukaisia yksiköitä. Tästä voidaan päätellä, että alkuluku p on jakautuva alkio Gaussin kokonaisluvuissa $\mathbb{Z}[i]$. Tästä päästään alkuluvun p ositteluun siten, että

$$p = \alpha\beta \in \mathbb{Z}[i],$$

missä $\alpha = a + bi$ ja $\beta = c + di$ eivät ole yksiköitä. Nyt ottamalla astefunktio, saadaan

$$p^2 = \partial(p) = \partial(\alpha\beta) = \partial(\alpha)\partial(\beta) = (a^2 + b^2)(c^2 + d^2).$$

Nyt siis lauseen 3.5 nojalla, ainoat yksiköt Gaussin kokonaislukujen joukossa $\mathbb{Z}[i]$ ovat ± 1 ja $\pm i$, eli kaikkien nollasta ja yksiköistä eroavien alkioiden Gaussin kokonaislukujen astefunktion arvo on suurempi kuin 1. Tämän perusteella siis $a^2 + b^2 \neq 1$ ja $c^2 + d^2 \neq 1$. Nyt siis $p^2 = p \cdot p = (a^2 + b^2)(c^2 + d^2)$. Tästä aritmetiikan peruslauseen nojalla saadaan, että $p = a^2 + b^2$ ja $p = c^2 + d^2$. $\square$

Lähdeluettelo

[1] Rotman, J. J. *Advanced modern algebra (1st ed.)* Prentice Hall. 2009.

[2] Myllylä, K. et. al *Algebran perusteet*, Oulun yliopisto. 2018.

[3] Myllylä, K. et. al *Algebralliset rakenteet* Oulun yliopisto. 2018.