
TAMPEREEN YLIOPISTO

Pro gradu -tutkielma

Anne Keskinen

Johdatus p -adisiin lukuihin

Matematiikan ja tilastotieteen laitos

Matematiikka

Maaliskuu 2010

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

KESKINEN, ANNE: Johdatus p -adisiin lukuihin

Pro gradu -tutkielma, 46 s.

Matematiikka

Maaliskuu 2010

Tiivistelmä

Tämän tutkielman tarkoitus on johdattaa lukija p -adiseen maailmaan. Päämääränä on rationaalilukujen kunnan \mathbb{Q} täydentäminen p -adisen normin suhteen. Tuloksena saadaan p -adisten lukujen kunta \mathbb{Q}_p . Luvussa 2 annetaan tutkielman varsinaisen aiheen ymmärtämisen kannalta olennaisimmat määritelmät ja tulokset. Luku 2 on käytännössä lukuteorian ja algebran perusasioiden kertausta. Luvussa 3 määritellään p -eksponentti ja tavallisesta normista poikkeava p -adinen normi. Lisäksi palautetaan mieleen käsitteet Cauchyn jono ja nollajono. Luvussa 4 selvitetään, mitä p -adiset luvut ovat ja osoitetaan, että \mathbb{Q}_p on todellakin kunta. Neljännessä luvussa todistetaan myös Henselin lemma. Kyseinen tulos on tärkeä p -adisten lukujen ominaisuus. Henselin lemmän avulla voidaan selvittää, onko polynomilla juuria p -adisten kokonaislukujen renkaassa \mathbb{Z}_p . Luvussa 5 tutustutaan hiukan kunnan \mathbb{Q}_p topologiaan.

Sisältö

1	Johdanto	4
2	Esitietoja	5
2.1	Lukuteoriaa	5
2.2	Algebraa	8
2.3	Tekijärengas	9
3	p-adinen normi	10
3.1	Määritelmä	10
3.2	Cauchyn jono ja p -adinen normi	15
3.3	Nollajono ja p -adinen normi	17
4	p-adiset luvut	19
4.1	Renkaan R täydentäminen normin N suhteen	19
4.2	p -adisten lukujen kunta \mathbb{Q}_p	27
4.3	Henselin lemma ja kongruenssit	35
5	Teichmüllerin laajennus	40
	Viitteet	46

1 Johdanto

Tämän tutkielman tarkoitus on johdattaa lukija p -adiseen maailmaan. Päämääränä on rationaalilukujen kunnan \mathbb{Q} täydentäminen p -adisen normin suhteen. Tuloksena saadaan p -adisten lukujen kunta \mathbb{Q}_p .

Luvussa 2 annetaan tutkielman varsinaisen aiheen ymmärtämisen kannalta olennaisimmat määritelmät ja tulokset. Luku 2 on käytännössä lukuteorian ja algebran perusasioiden kertausta. Hyvin opitut ja sisäistetyt perusasiat riittävät tämän tutkielman ymmärtämiseen. Vasta varsinaiset p -adisten lukujen sovellukset, joihin ei tässä esityksessä perehdytä, vaativat syvällistä matematiikkaa. Tämä on syy siihen, miksi p -adisia lukuja ei oikeastaan käsitellä lukuteorian peruskursseilla.

Luvussa 3 määritellään p -eksponentti ja tavallisesta normista poikkeava p -adinen normi. Lisäksi palautetaan mieleen käsitteet Cauchyn jono ja nollajono. Jokaista aihepiiriä myös havainnollistetaan esimerkeillä.

Luvussa 4 selvitetään, mitä p -adiset luvut ovat ja osoitetaan, että \mathbb{Q}_p on todellakin kunta. Lisäksi perehdytään esimerkkien avulla kunnan \mathbb{Q}_p aritmeetiikkaan. Neljännessä luvussa todistetaan myös Henselin lemma. Kyseinen tulos on tärkeä p -adisten lukujen ominaisuus. Viimeinen luku käsittelee kunnan \mathbb{Q}_p topologiaa. Aluksi perehdytään topologian peruskäsitteisiin ja lopuksi esitellään Teichmüllerin funktiot.

Lukijan odotetaan hallitsevan matematiikan peruskursseilla esitetyt asiat. Lisäksi tutkielmassa käsitellään melko paljon jonoja, joten lukijalla oletetaan olevan hallussa jonon käsite. Vaikka perusasioiden osaaminen sinänsä riittää tämän tutkielman ymmärtämiseen, lukijalta odotetaan kuitenkin matemaattista kypsyyttä ja kykyä omaksua uusia asioita. Aiheena p -adiset luvut on varmasti monelle lukijalle toistaiseksi aivan uusi.

Toisen luvun materiaali on peräisin Pentti Haukkasen luentomonisteista [3], [4] ja [5]. Muuten tutkielma noudattelee hyvin pitkälle A. J. Bakerin luentomonistetta *An Introduction to p -adic Numbers and p -adic Analysis* [1]. Jotta asioista muodostuisi konkreettinen kuva, joitakin kyseisen monisteen asioita on kuitenkin esitetty toisin muita lähteitä käyttäen. Näistä mainittakoon Svetlana Katokin kirja *p -adic Analysis Compared with Real* [6]. Lisäksi on hyödynnetty Matematiikkalehti Solmun artikkelia [8]. Esimerkit ja lauseiden todistukset ovat tekijän laatimia, jos niiden yhteydessä ei ole lähdeviittoa. Koska ainakin päälähteenä käytetty Bakerin luentomoniste on itsessään melko tiivis ja lyhytsanainen esitys, tekijä on pääsääntöisesti täydentänyt muun muassa lauseiden todistuksia kirjoittamalla enemmän perusteluja näkyviin.

Teoria p -adisista luvuista on suhteellisen uusi. Kurt Hensel julkaisi p -adisia lukuja koskevan teoriansa vuoden 1900 paikkeilla. Vasta 20 vuotta myöhemmin teoriasta tuli yleisemmin tunnettu, kun Henselin oppilas Helmut Hasse ratkaisi kuuluisan neliömuotoja koskevan probleeman p -adisia lukuja käyttäen. [8, s. 4–5.]

p -adiset luvut kuuluvat lukuteorian piiriin, vaikka p -adisessa maailmassa liikuttaessa tarvitaan myöskin algebran ja analyysin osaamista. Nykyään p -adisella analyysillä on keskeinen merkitys modernissa lukuteoriassa.

2 Esitietoja

Tässä luvussa käydään läpi tutkielman ymmärtämisen kannalta tärkeimmät käsitteet ja tulokset.

2.1 Lukuteoriaa

Tämän luvun materiaali on pääsääntöisesti lähteestä [3]. Tutustutaan lukuteorian peruskäsitteisiin, kuten jaollisuuteen, kongruenssiin ja alkulukuihin.

Määritelmä 2.1. Olkoot $a, b \in \mathbb{Z}$. Luku a on luvun b tekijä, jos on olemassa sellainen luku $c \in \mathbb{Z}$, että $b = ac$.

Jos luku a on luvun b tekijä, niin merkitään tällöin $a \mid b$. Muuten $a \nmid b$.

Esimerkki 2.1. Koska luku 10 voidaan kirjoittaa muodossa $10 = 2 \cdot 5$, niin luku 5 on luvun 10 tekijä eli $5 \mid 10$.

Koska lukua 16 ei voida kirjoittaa muodossa $16 = 5 \cdot c$, missä $c \in \mathbb{Z}$, niin luku 5 ei ole luvun 16 tekijä. Siis $5 \nmid 16$.

Määritelmä 2.2. Olkoot $a, b \in \mathbb{Z}$ ja olkoon ainakin toinen luvuista nolasta poikkeava. Silloin luku c on lukujen a ja b suurin yhteinen tekijä, jos

(1) $c \mid a$, $c \mid b$ ja

(2) $d \mid a$, $d \mid b \Rightarrow d \leq c$.

Lukujen a ja b suurinta yhteistä tekijää merkitään (a, b) .

Esimerkki 2.2. Lukujen 2 ja 7 suurin yhteinen tekijä $(2, 7) = 1$. Lukujen 3 ja 12 suurin yhteinen tekijä $(3, 12) = 3$.

Määritelmä 2.3. Luvut a ja b ovat suhteellisia alkulukuja, jos $(a, b) = 1$.

Lause 2.1 (Jakoalgoritmi). Jokaista lukua a ja $b \neq 0$ kohti on olemassa sellaiset yksikäsitteiset luvut q ja r , että

$$a = bq + r, \quad \text{missä } 0 \leq r < b.$$

Todistus. Sivuuutetaan. Ks. [3, s. 6]. □

Jakoalgoritmin avulla voidaan todistaa seuraava tulos.

Lause 2.2. Olkoon $b \geq 2$. Jokainen luku $a \in \mathbb{Z}^+$ voidaan esittää yksikäsitteisesti muodossa

$$a = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0,$$

missä $0 \leq a_i < b$, $i = 0, 1, \dots, m$.

Esimerkki 2.3. Luku 27 esitettynä kannassa 4 on

$$27 = 4^2 + 2 \cdot 4 + 3.$$

Luku 154 esitettynä kannassa 2 on

$$154 = 2^7 + 2^4 + 2^3 + 2.$$

Lause 2.3. Olkoot $a, b \in \mathbb{Z}$. Silloin on olemassa sellaiset kokonaisluvut x ja y , että

$$(a, b) = ax + by.$$

Todistus. Sivutetaan. Ks. [3, s. 8]. □

Määritelmä 2.4. Luku $p > 1$ on *alkuluku*, jos sen ainoat positiiviset tekijät ovat luvut 1 ja p itse.

Esimerkki 2.4. Koska luku 5 voidaan kirjoittaa vain muodossa $5 = 1 \cdot 5$, niin luku 5 on alkuluku.

Koska luvulla 6 on tekijöinä myös luvut 2 ja 3, niin luku 6 ei ole alkuluku.

Lause 2.4 (Aritmetiikan peruslause). Jokainen kokonaisluku $a \geq 2$ voidaan esittää alkulukujen tulona yksikäsitteisesti.

Todistus. Sivutetaan. Ks. [3, s. 14]. □

Esimerkki 2.5. Luku 624 esitettynä alkulukujen tulona on $624 = 2^4 \cdot 3 \cdot 13$. Tässä tekijät 2^4 , 3 ja 13 voisivat olla myös eri järjestyksessä.

Määritelmä 2.5. Olkoot $a, b \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}^+$. Luku a on *kongruentti* luvun b kanssa *modulo* m , jos

$$m \mid (a - b).$$

Jos luku a on kongruentti luvun b kanssa modulo m , niin merkitään

$$a \equiv b \pmod{m}.$$

Esimerkki 2.6. Koska $7 \mid (16 - 2)$, niin $16 \equiv 2 \pmod{7}$.

Lause 2.5. *Kongruenssi \equiv on ekvivalenssirelaatio.*

Todistus. Olkoot $a, b, c \in \mathbb{Z}$. Koska $m \mid 0$, niin $a \equiv a \pmod{m}$. Siis kongruenssirelaatio on refleksiivinen.

Oletetaan, että $a \equiv b \pmod{m}$. Siis $m \mid (a - b)$, joten voidaan kirjoittaa, että $a - b = mk$, missä $k \in \mathbb{Z}$. Kun kerrotaan yhtälö puolittain luvulla -1 , saadaan, että $b - a = -(mk)$. Tämä on yhtäpitävää sen kanssa, että $b - a = m(-k)$, joten $m \mid (b - a)$. Siis $b \equiv a \pmod{m}$, joten kyseinen relaatio on myös symmetrinen.

Oletetaan sitten, että $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$. Siis $m \mid (a - b)$ ja $m \mid (b - c)$, joten voidaan kirjoittaa, että $a - b = mk_1$ ja $b - c = mk_2$, missä $k_1, k_2 \in \mathbb{Z}$. Huomataan, että $a - c = (a - b) + (b - c)$. Tästä edelleen saadaan, että $a - c = mk_1 + mk_2$. Siis $a - c = m(k_1 + k_2)$, missä $k_1 + k_2$ on kokonaisluku. Siis $m \mid (a - c)$, joten $a \equiv c \pmod{m}$. Näin on osoitettu, että kongruenssirelaatio on myös transitiivinen.

Kokonaisuudessaan relaatio \equiv on siis ekvivalenssirelaatio. □

Lause 2.6. *Olkoon $a \equiv b \pmod{m}$. Silloin $f(a) \equiv f(b) \pmod{m}$ aina, kun f on kokonaislukukertoiminen polynomi.*

Todistus. Sivutetaan. Katso vinkki [3, s. 19]. □

Lause 2.7. *Olkoon $(a, m) = d$. Silloin*

$$ab \equiv ac \pmod{m} \Leftrightarrow b \equiv c \pmod{m/d}.$$

Todistus. Sivutetaan. Ks. [3, s. 19]. □

Tarkastellaan seuraavaksi hiukan lineaarista kongruenssia

$$ax \equiv b \pmod{m}.$$

Lause 2.8. *Kongruenssi*

$$ax \equiv b \pmod{m}$$

on ratkeava täsmälleen silloin, kun $(a, m) \mid b$.

Todistus. Sivutetaan. Ks. [3, s. 24]. □

Määritelmä 2.6. (Ks. [5, s. 7]). Olkoon $(a, m) = 1$. Silloin kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua x sanotaan luvun a *käänteislukuksi modulo m* . Merkitään $x = a^{-1}$.

Lause 2.9. (Ks. [5, s. 7]). *Kun $(a, m) = 1$, niin kongruenssin $ax \equiv b \pmod{m}$ ratkaisu on $x \equiv a^{-1}b \pmod{m}$.*

Lause 2.10 (Fermat'n pieni lause). *Jos p on alkuluku ja $p \nmid a$, niin*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Todistus. Sivutetaan. Ks. [5, s. 6]. □

2.2 Algebraa

Tutustutaan nyt erilaisiin algebrallisiin rakenteisiin. Yhden laskutoimituksen algebrallinen rakenne tarkoittaa paria $(A, *)$, missä A on jokin epätyhjä joukko ja $*$ on joukon A laskutoimitus. Lukijan oletetaan tietävän, mikä on laskutoimitus. Lähteenä on edelleen [3].

Määritelmä 2.7. Algebrallinen rakenne $(G, *)$ on *ryhmä*, jos se toteuttaa seuraavat ehdot:

(1) $(a * b) * c = a * (b * c)$ aina, kun $a, b, c \in G$.

(2) On olemassa sellainen $e \in G$, että

$$a * e = e * a = a$$

aina, kun $a \in G$.

(3) Jokaiselle $a \in G$ on olemassa sellainen $a' \in G$, että

$$a * a' = a' * a = e.$$

Ehto (1) tarkoittaa, että laskutoimitus on *assosiatiivinen*, ehto (2) tarkoittaa, että joukossa G on *neutraalialkio* kyseisen laskutoimituksen suhteen ja ehto (3) sitä, että jokaisella joukon G alkion a on *käänteisalkio*.

Jos laskutoimitus $*$ on *vaihdannainen* (*kommutatiivinen*) eli $a * b = b * a$ aina, kun $a, b \in G$, niin sanotaan, että $(G, *)$ on *Abelin ryhmä*.

Siirrytään nyt kahden laskutoimituksen algebrallisiin rakenteisiin. Tässä esityksessä kahden laskutoimituksen algebrallisista rakenteista mainitaan rengas ja kunta.

Määritelmä 2.8. Kolmikko $(R, +, \cdot)$ on *rengas*, jos se toteuttaa seuraavat ehdot:

(1) $(R, +)$ on Abelin ryhmä.

(2) Laskutoimitus \cdot on assosiatiivinen.

(3)

$$a(b + c) = ab + ac \quad \text{aina, kun } a, b, c \in R.$$

$$(a + b)c = ac + bc \quad \text{aina, kun } a, b, c \in R.$$

Jos on olemassa laskutoimituksen \cdot neutraalialkio, niin rengas $(R, +, \cdot)$ on *ykkösrengas* ja kyseinen neutraalialkio on *ykkösalkio*. Ykkösalkiota merkitään symbolilla 1. Rengas $(R, +, \cdot)$ on *kommutatiivinen*, jos laskutoimitus \cdot on kommutatiivinen. Ryhmän $(R, +)$ neutraalialkioa sanotaan *nolla-alkioksi* ja sitä merkitään symbolilla 0.

Määritelmä 2.9. Renkaan R alkio $a \in R \setminus \{0\}$ on *nollanjakaja*, jos on olemassa sellainen $b \in R \setminus \{0\}$, että $ab = ba = 0$.

Määritelmä 2.10. Olkoon $\emptyset \neq S \subseteq R$. Jos S on rengas, niin sanotaan, että S on renkaan R *alirengas*.

Määritelmä 2.11. Kommutatiivinen ykkösrengas $(F, +, \cdot)$ on *kunta*, jos jokaisella nollasta poikkeavalla joukon F alkiolla on käänteisalkio.

Esimerkki 2.7. Joukot \mathbb{Q} ja \mathbb{R} varustettuna tavanomaisilla yhteen- ja kertolaskuilla ovat kuntia. Sen sijaan $(\mathbb{Z}, +, \cdot)$ ei ole kunta. Nimittäin esimerkiksi alkiolla 2 ei ole joukossa \mathbb{Z} olevaa käänteisalkiota ($2^{-1} = 1/2$, mutta $1/2 \notin \mathbb{Z}$).

2.3 Tekijärengas

Tässä luvussa käytetään lähteenä monistetta [4, s. 31–35].

Määritelmä 2.12. Olkoon R rengas ja I renkaan R alirengas. Tällöin I on renkaan R *ideaali* eli *ihanne*, jos

$$ra, ar \in I$$

aina, kun $r \in R$, $a \in I$.

Olkoon $(R, +, \cdot)$ rengas ja I sen ideaali. Siis I on renkaan R alirengas. Tällöin siis algebrallinen struktuuri $(I, +)$ on Abelin ryhmä. Koska $\emptyset \neq I \subseteq R$, niin I on ryhmän R aliryhmä. Aliryhmän I määräämä ekvivalenssirelaatio $\equiv \pmod{I}$ joukossa R on muotoa

$$a \equiv b \pmod{I} \Leftrightarrow a \in b + I.$$

Siis kaksi alkia ovat ekvivalentit, jos niiden erotus kuuluu ideaaliin I . Ekvivalenssirelaation $\equiv \pmod{I}$ ekvivalenssiluokkien joukko on

$$R/I = \{a + I \mid a \in R\}.$$

Pari $(R/I, +)$ on ryhmä ja yhteenlasku ryhmässä $(R/I, +)$ määritellään kaavalla

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

Pari $(R/I, \cdot)$ on algebrallinen struktuuri, missä kertolasku määritellään kaavalla

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

Lisäksi laskutoimitus \cdot on assosiatiivinen.

Lause 2.11. *Olkoon $(R, +, \cdot)$ rengas ja I sen ideaali. Silloin $(R/I, +, \cdot)$ on rengas.*

Todistus. Sivutetaan. Katso vinkit [4, s. 35]. □

Huomautus. Renkaasta $(R/I, +, \cdot)$ käytetään nimitystä *tekijärengas* tai *osamäärärengas*.

3 p -adinen normi

Tavanomaisesta normista puhuttaessa tarkoitetaan yleensä itseisarvoa. Metriikka $d(x, y) = |x - y|$ on tavallinen euklidinen kahden pisteen etäisyys luku suoralla. Tavallisen etäisyyden lisäksi on olemassa muitakin etäisyyksiä. Rationaalilukujen p -adinen etäisyys saadaan selville p -adisen normin avulla.

3.1 Määritelmä

Tässä luvussa annetaan p -adisen normin määritelmä. Sitä ennen määritellään kuitenkin käsitteet normi ja p -eksponentti.

Olkoon R rengas.

Määritelmä 3.1. Funktio

$$N : R \rightarrow \mathbb{R}^+ \cup \{0\} = \{r \in \mathbb{R} : r \geq 0\}$$

on *normi*, jos sille on voimassa seuraavat ehdot.

(N1) $N(x) = 0$, jos ja vain jos $x = 0$.

(N2) $N(xy) = N(x)N(y)$ aina, kun $x, y \in R$.

(N3) $N(x + y) \leq N(x) + N(y)$ aina, kun $x, y \in R$.

Ehtoa (N3) kutsutaan *kolmioepäyhtälöksi*. Normi on *epäarkhimedinen*, jos ehto (N3) voidaan korvata vahvemmalla ehdolla

(N4) $N(x + y) \leq \max\{N(x), N(y)\}$ aina, kun $x, y \in R$.

Ehto (N4) on *ultrametrinen epäyhtälö*. Jos ehto (N4) ei ole voimassa, niin normi on arkhimedinen.

Huomautus. Epäarkhimediselle normille N ehto (N4) voidaan korvata vahvemmalla ehdolla

(N4') $N(x + y) \leq \max\{N(x), N(y)\}$ aina, kun $x, y \in R$. Yhtäsuuruus on voimassa, kun $N(x) \neq N(y)$.

Esimerkki 3.1. (Vrt. [1, s. 15]). Olkoon $R \subseteq \mathbb{C}$ kompleksilukujen \mathbb{C} alirenkas. Tällöin tavallinen itseisarvo on normi renkaassa R . Voidaan siis asettaa $N(x) = |x|$. Samanlainen normi voidaan määritellä myös tapauksissa $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ tai \mathbb{C} .

Osoitetaan, että ehto (N4) ei toteudu normin $N(x) = |x|$ tapauksessa, joten kyseinen normi on arkhimedinen. Selvästi

$$N(2 + 2) = |2 + 2| = 4.$$

Toisaalta

$$\max \{N(2), N(2)\} = \max \{2, 2\} = 2.$$

Siis $N(2+2) > \max \{N(2), N(2)\}$, joten ehto (N4) ei ole voimassa ja normi on siis arkhimedinen.

Olkoon nyt $R = \mathbb{Q}$. Siis joukon R alkiot ovat muotoa a/b , missä $a, b \in \mathbb{Z}$ ja $b \neq 0$. Olkoon lisäksi $p \geq 2$ alkuluku.

Määritelmä 3.2. Olkoon $x \in \mathbb{Z} \setminus \{0\}$. Luvun x p -eksponentti on

$$\text{ord}_p x = \max \{r : p^r \mid x\} \geq 0.$$

Jos $x = a/b \in \mathbb{Q}$, niin luvun x p -eksponentti on

$$\text{ord}_p x = \text{ord}_p \frac{a}{b} = \text{ord}_p a - \text{ord}_p b.$$

Lisäksi sovitaan, että $\text{ord}_p 0 = \infty$.

Huomautus. Luvun x p -eksponentti on sekä kokonaislukujen että rationaalilukujen tapauksessa kokonaisluku ja lisäksi rationaaliluvulle a/b p -eksponentti on hyvin määritelty.

Esimerkki 3.2. (Ks. [7, teht. 11, s. 7]). Lasketaan $\text{ord}_3 54$ ja $\text{ord}_2 128$.

Ratkaisu. Kirjoitetaan $54 = 2 \cdot 3^3$. Siis $\text{ord}_3 54 = 3$. Vastaavasti kirjoitetaan $128 = 2^7$. Siis $\text{ord}_2 128 = 7$.

Esimerkki 3.3. (Ks. [7, teht. 11, s. 7]). Lasketaan $\text{ord}_2 \frac{128}{7}$ ja $\text{ord}_3 \frac{7}{9}$.

Ratkaisu. Nyt esimerkin 3.2 mukaan $\text{ord}_2 128 = 7$. Koska luvun 7 ainoat tekijät ovat luvut 1 ja 7, niin $\text{ord}_2 7 = 0$. Siis määritelmän nojalla

$$\text{ord}_2 \frac{128}{7} = \text{ord}_2 128 - \text{ord}_2 7 = 7 - 0 = 7.$$

Myöskään luku 3 ei ole luvun 7 tekijä, joten $\text{ord}_3 7 = 0$. Luku 9 voidaan kirjoittaa muodossa $9 = 3^2$. Siis nähdään, että $\text{ord}_3 9 = 2$. Nyt kokonaisuudessaan

$$\text{ord}_3 \frac{7}{9} = \text{ord}_3 7 - \text{ord}_3 9 = 0 - 2 = -2.$$

Seuraavassa lauseessa esitellään p -eksponentin ominaisuuksia.

Lause 3.1. *Olkoot $x, y \in \mathbb{Q}$. Tällöin seuraavat ominaisuudet ovat voimassa.*

(1) $\text{ord}_p x = \infty$, jos ja vain jos $x = 0$.

(2) $\text{ord}_p(xy) = \text{ord}_p x + \text{ord}_p y$.

(3) $\text{ord}_p(x+y) \geq \min \{\text{ord}_p x, \text{ord}_p y\}$. *Yhtäsuuruus on voimassa, kun $\text{ord}_p x \neq \text{ord}_p y$.*

Todistus. (Vrt. [1, s. 16]).

Ominaisuus (1) on selvä. Todistetaan ominaisuus (2). Olkoot $x, y \in \mathbb{Q} \setminus \{0\}$. Voidaan kirjoittaa $x = p^r \frac{a}{b}$ ja $y = p^s \frac{c}{d}$, missä $a, b, c, d \in \mathbb{Z}$, $p \nmid a, b, c, d$ ja $r, s \in \mathbb{Z}$. Siis $\text{ord}_p x = r$ ja $\text{ord}_p y = s$. Nyt

$$xy = p^r \frac{a}{b} p^s \frac{c}{d} = p^r p^s \frac{ac}{bd}.$$

Siis

$$\text{ord}_p(xy) = r + s = \text{ord}_p x + \text{ord}_p y.$$

Näin ominaisuus (2) on todistettu.

Todistetaan sitten ominaisuus (3). Olkoot x ja y kuten ominaisuuden (2) oletuksessa. Oletetaan, että $r = s$. Nyt

$$\begin{aligned} x + y &= p^r \frac{a}{b} + p^s \frac{c}{d} \\ &= p^r \left(\frac{a}{b} + \frac{c}{d} \right) \\ &= p^r \frac{(ad + bc)}{bd}. \end{aligned}$$

Koska $p \nmid b, d$, niin $p \nmid bd$. Koska voi olla, että $p \mid (ad + bc)$, niin kokonaisuudessaan saadaan, että

$$\text{ord}_p(x + y) \geq r = \min\{\text{ord}_p x, \text{ord}_p y\}.$$

Oletetaan sitten, että $r \neq s$ ja $s > r$. Nyt

$$\begin{aligned} x + y &= p^r \frac{a}{b} + p^s \frac{c}{d} \\ &= p^r \left(\frac{a}{b} + p^{s-r} \frac{c}{d} \right) \\ &= p^r \frac{(ad + p^{s-r} cb)}{bd}. \end{aligned}$$

Koska $s - r > 0$, niin $p \mid p^{s-r}$ ja edelleen $p \mid p^{s-r} cb$. Toisaalta, koska $p \nmid a, d$, niin $p \nmid ad$. Siis jaollisuusrelaation ominaisuuksien perusteella $p \nmid (ad + p^{s-r} cb)$. Koska lisäksi $p \nmid bd$, niin

$$\text{ord}_p(x + y) = r = \min\{\text{ord}_p x, \text{ord}_p y\}.$$

Tapaus $s < r$ käsitellään vastaavasti. Tapaus, jossa ainakin jompikumpi luvuista x ja y on nolla on helppo nähdä. Näin lause 3.1 on todistettu. \square

Määritellään seuraavaksi p -adinen normi p -eksponentin avulla.

Määritelmä 3.3. Olkoon $x \in \mathbb{Q}$. Luvun x p -adinen normi määritellään kaavalla

$$|x|_p = \begin{cases} p^{-\text{ord}_p x}, & \text{kun } x \neq 0, \\ 0, & \text{kun } x = 0. \end{cases}$$

Esimerkki 3.4. Lasketaan $|12|_3$ ja $|\frac{16}{3}|_2$.

Ratkaisu. Selvitetään ensin, mikä on luvun 12 3-eksponentti. Koska $12 = 4 \cdot 3$, niin $\text{ord}_3 12 = 1$. Nyt sijoitetaan saatu tulos kaavaan ja saadaan, että

$$|12|_3 = 3^{-1} = \frac{1}{3}.$$

Lasketaan ensin $\text{ord}_2 \frac{16}{3}$. Koska $16 = 2^4$, niin $\text{ord}_2 16 = 4$. Luku 2 ei ole luvun 3 tekijä, joten $\text{ord}_2 3 = 0$. Nyt p -eksponentin määritelmän nojalla

$$\text{ord}_2 \frac{16}{3} = \text{ord}_2 16 - \text{ord}_2 3 = 4 - 0 = 4.$$

Siis

$$\left| \frac{16}{3} \right|_2 = 2^{-4} = \frac{1}{16}.$$

Huomautus. Lauseke $|a - b|_p$ antaa rationaalilukujen a ja b p -adisen etäisyyden. Huomataan, että kahden rationaaliluvun etäisyys p -adisessa metriikassa on sitä pienempi, mitä korkeammalla p :n potenssilla niiden erotus on jaollinen. [8, s. 2.]

Esimerkki 3.5. (Ks. [7, teht. 15, s. 7]). Lasketaan $|1 - 26|_5$ ja $|\frac{1}{9} + \frac{1}{16}|_5$.

Ratkaisu.

$$|1 - 26|_5 = |-25|_5 = 5^{-2} = \frac{1}{25}.$$

$$\left| \frac{1}{9} + \frac{1}{16} \right|_5 = \left| \frac{25}{144} \right|_5 = 5^{-2} = \frac{1}{25}.$$

Lause 3.2. (Ks. [6, s. 20]). Olkoot $a, b \in \mathbb{Z}^+$. Tällöin $a \equiv b \pmod{p^n}$, jos ja vain jos $|a - b|_p \leq 1/p^n$.

Todistus. Olkoot $a, b \in \mathbb{Z}^+$. Oletetaan ensin, että $a \equiv b \pmod{p^n}$. Siis $p^n \mid a - b$. Tällöin voidaan kirjoittaa $a - b = p^n \cdot c$, missä $c \in \mathbb{Z}$. On mahdollista, että luku p on luvun c tekijä, joten $\text{ord}_p(a - b) \geq n$. Siis

$$|a - b|_p = p^{-\text{ord}_p(a-b)} \leq 1/p^n.$$

Oletetaan sitten, että $|a - b|_p \leq 1/p^n$. Siis $\text{ord}_p(a - b) \geq n$. Voidaan siis kirjoittaa $a - b = p^n \cdot c$, missä $c \in \mathbb{Z}$ ja mahdollisesti $p \mid c$. Tällöin edelleen $p^n \mid a - b$, joten $a \equiv b \pmod{p^n}$. \square

Seuraavaksi osoitetaan, että edellä määritelty p -adinen normi on itse asiassa epäarkhimedinen normi kunnassa \mathbb{Q} .

Lause 3.3. *Funktiolla $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}^+$ on seuraavat ominaisuudet:*

(1) $|x|_p = 0$, jos ja vain jos $x = 0$.

(2) $|xy|_p = |x|_p |y|_p$.

(3) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. *Yhtäsuuruus on voimassa, kun $|x|_p \neq |y|_p$.*

Siis ominaisuuksien (1)–(3) perusteella p -adinen normi on epäarkhimedinen.

Todistus. (Vrt. [6, s. 20]).

Ominaisuus (1) on selvä. Todistetaan ominaisuus (2). Olkoot x ja y nollasta poikkeavia rationaalilukuja. Nyt p -adisen normin määritelmän ja lauseen 3.1 kohdan (2) nojalla voidaan kirjoittaa

$$\begin{aligned} |xy|_p &= p^{-\text{ord}_p(xy)} = p^{-(\text{ord}_p x + \text{ord}_p y)} \\ &= \frac{1}{p^{\text{ord}_p x + \text{ord}_p y}} \\ &= \frac{1}{p^{\text{ord}_p x}} \cdot \frac{1}{p^{\text{ord}_p y}} \\ &= p^{-\text{ord}_p x} \cdot p^{-\text{ord}_p y} \\ &= |x|_p |y|_p. \end{aligned}$$

Tapaus, jossa ainakin jompikumpi luvuista x ja y on nolla, on selvä. Näin ominaisuus (2) on todistettu.

Todistetaan sitten ominaisuus (3). Oletetaan, että $x, y \neq 0$. Lauseen 3.1 kohdan (3) nojalla

$$\text{ord}_p(x + y) \geq \min\{\text{ord}_p x, \text{ord}_p y\}.$$

Tällöin on selvää, että

$$-\text{ord}_p(x + y) \leq \max\{-\text{ord}_p x, -\text{ord}_p y\}.$$

Edelleen on voimassa, että

$$\begin{aligned} p^{-\text{ord}_p(x+y)} &\leq p^{\max\{-\text{ord}_p x, -\text{ord}_p y\}} \\ &= \max\{p^{-\text{ord}_p x}, p^{-\text{ord}_p y}\} \\ &= \max\{|x|_p, |y|_p\}. \end{aligned}$$

Muut tapaukset ovat helposti osoitettavissa. Näin kohta (3) on todistettu. \square

3.2 Cauchyn jono ja p -adinen normi

Olkoon seuraavassa R rengas ja N renkaan R normi. Aiemmin on jo käytetty termiä kahden pisteen välinen etäisyys. Määritellään tämä käsite nyt tarkemmin.

Määritelmä 3.4. Alkioiden $x, y \in R$ välinen *etäisyys* normin N suhteen on

$$d_N(x, y) = N(x - y) \in \mathbb{R}^+.$$

Normin ominaisuuksista seuraa, että seuraavat ominaisuudet ovat voimassa:

(D1) $d_N(x, y) = 0$, jos ja vain jos $x = y$.

(D2) $d_N(x, y) = d_N(y, x)$ kaikilla $x, y \in R$.

(D3) $d_N(x, y) \leq d_N(x, z) + d_N(z, y)$, missä $z \in R$.

Jos N on epäarkhimedinen, niin ominaisuus (D3) korvataan ominaisuudella

(D4) $d_N(x, y) \leq \max \{d_N(x, z), d_N(z, y)\}$. Tässä on yhtäsuuruus, kun $d_N(x, z) \neq d_N(z, y)$.

Lause 3.4 (Tasakylkisen kolmion periaate). *Olkoon N renkaan R epäarkhimedinen normi. Olkoot $x, y, z \in R$ sellaisia, että $d_N(x, z) \neq d_N(z, y)$. Silloin*

$$d_N(x, y) = \max \{d_N(x, z), d_N(z, y)\}.$$

Todistus. Käytetään kohtaa (D4). □

Siis lauseen 3.4 nojalla jokainen kolmio on tasakylkinen erityisesti p -adisessa metriikassa.

Olkoon nyt $(a_n)_{n \geq 1}$ renkaan R jono ja N renkaan R normi. Määritellään seuraavaksi käsite jonon suppeneminen.

Määritelmä 3.5. Jonolla $(a_n)_{n \geq 1}$ on *raja-arvo* $a \in R$ normin N suhteen, jos jokaista lukua $\varepsilon > 0$ kohti on olemassa sellainen luku $M \in \mathbb{N}$, että

$$n > M \Rightarrow N(a - a_n) = d_N(a, a_n) < \varepsilon.$$

Merkitään tällöin $\lim_{n \rightarrow \infty}^{(N)} a_n = a$ ja sanotaan, että jono (a_n) *suppenee* kohti alkioita $a \in R$.

Seuraavaksi määritellään Cauchyn jono normin N suhteen.

Määritelmä 3.6. Jono (a_n) on *Cauchyn jono* normin N suhteen, jos jokaista lukua $\varepsilon > 0$ kohti on olemassa sellainen luku $M \in \mathbb{N}$, että

$$m, n > M \Rightarrow N(a_m - a_n) = d_N(a_m, a_n) < \varepsilon.$$

Lause 3.5. Jos $\lim_{n \rightarrow \infty}^{(N)} a_n$ on olemassa, niin (a_n) on Cauchyn jono normin N suhteen.

Todistus. (Vrt. [1, s. 18]).

Oletetaan, että $\lim_{n \rightarrow \infty}^{(N)} a_n = a$. Olkoon $\varepsilon > 0$. Koska $\lim_{n \rightarrow \infty}^{(N)} a_n = a$, niin määritelmän 3.5 nojalla on olemassa sellainen luku $M \in \mathbb{N}$, että

$$n > M \Rightarrow N(a - a_n) < \frac{\varepsilon}{2}.$$

Oletetaan, että $m, n > M$. Tällöin siis

$$(3.1) \quad N(a - a_n) < \frac{\varepsilon}{2}$$

ja

$$(3.2) \quad N(a - a_m) < \frac{\varepsilon}{2}.$$

Nyt kaavojen (3.1) ja (3.2) sekä ominaisuuden (N3) nojalla saadaan, että

$$\begin{aligned} N(a_m - a_n) &= N((a_m - a) + (a - a_n)) \\ &\leq N(a_m - a) + N(a - a_n) \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Siis mielivaltaista lukua $\varepsilon > 0$ kohti on olemassa sellainen luku $M \in \mathbb{N}$, että

$$m, n > M \Rightarrow N(a_m - a_n) < \varepsilon.$$

Näin on todistettu, että jono (a_n) on Cauchyn jono normin N suhteen. \square

Huomautus. Jos N on epäarkhimedinen normi, niin ominaisuuden (N4) perusteella saadaan seuraava epäyhtälö:

$$\begin{aligned} N(a_m - a_n) &= N((a_m - a) + (a - a_n)) \\ &\leq \max \{N(a_m - a), N(a - a_n)\} \\ &< \frac{\varepsilon}{2}. \end{aligned}$$

Siirrytään nyt yleisestä renkaasta R renkaaseen \mathbb{Q} ja normista N p -adiseen normiin $|\cdot|_p$. Käsitellään seuraavaksi esimerkki lukujonon suppenemisesta p -adisen normin suhteen.

Esimerkki 3.6. (Vrt. [1, s. 18]). Olkoon $a_n = 1 + p + p^2 + \cdots + p^{n-1}$. Osoitetaan, että (a_n) on Cauchyn jono.

Olkoon $\varepsilon > 0$. Valitaan nyt sellainen luku $M \in \mathbb{N}$, että $p^M \geq \frac{1}{\varepsilon}$. Olkoon $n > M$ ja $k \in \mathbb{N}$. Nyt

$$\begin{aligned} |a_{n+k} - a_n|_p &= |(1 + p + p^2 + \cdots + p^{n+k-1}) - (1 + p + p^2 + \cdots + p^{n-1})|_p \\ &= |p^n + p^{n+1} + \cdots + p^{n+k-1}|_p \\ &= |p^n(1 + p + p^2 + \cdots + p^{k-1})|_p \\ &= \frac{1}{p^n}. \end{aligned}$$

Nyt oletusten perusteella pätee edelleen, että

$$|a_{n+k} - a_n|_p = \frac{1}{p^n} < \frac{1}{p^M} \leq \frac{1}{1/\varepsilon} = \varepsilon.$$

Näin on osoitettu, että (a_n) on Cauchyn jono.

Osoitetaan vielä, että tällä jonolla on raja-arvo $a = \frac{1}{1-p}$ p -adisen normin suhteen. Huomataan aluksi, että itse asiassa a_n on geometrinen summa. Siis a_n voidaan esittää muodossa $a_n = \frac{1-p^n}{1-p}$.

Olkoon sitten $\varepsilon > 0$. Edetään nyt kuten edellä. Valitaan siis sellainen luku $M \in \mathbb{N}$, että $p^M \geq \frac{1}{\varepsilon}$, ja oletetaan, että $n > M$. Nyt

$$\left| a_n - \frac{1}{1-p} \right|_p = \left| \frac{1-p^n}{1-p} - \frac{1}{1-p} \right|_p = \left| \frac{-p^n}{1-p} \right|_p = \left| \frac{p^n}{p-1} \right|_p = \frac{1}{p^n}.$$

Oletuksen nojalla saadaan aivan kuten aikaisemmassakin päättelyssä, että

$$\left| a_n - \frac{1}{1-p} \right|_p = \frac{1}{p^n} < \frac{1}{p^M} < \varepsilon.$$

Näin on osoitettu, että jonon (a_n) raja-arvo normin $|\cdot|_p$ suhteen on $\frac{1}{1-p}$.

Merkitään tätä

$$\lim_{n \rightarrow \infty}^{(p)} (1 + p + \cdots + p^{n-1}) = \frac{1}{1-p}.$$

3.3 Nollajono ja p -adinen normi

Määritellään seuraavaksi käsite nollajono yleisellä tasolla. Käsitellään sen jälkeen esimerkkejä tapauksista, joissa renkaana on jälleen \mathbb{Q} ja normina p -adinen normi.

Määritelmä 3.7. Jono (a_n) on *nollajono* normin N suhteen, jos

$$\lim_{n \rightarrow \infty}^{(N)} a_n = 0.$$

Esimerkki 3.7. (Vrt. [1, esim. 2.14, s. 19]). Olkoon $a_n = p^n$. Nyt $|p^n|_p = \frac{1}{p^n}$. Selvästi $\frac{1}{p^n} \rightarrow 0$, kun $n \rightarrow \infty$. Siis on osoitettu, että $\lim_{n \rightarrow \infty}^{(p)} a_n = 0$. Näin ollen jono (a_n) on nollajono p -adisen normin suhteen.

Esimerkki 3.8. (Vrt. [1, esim. 2.15, s. 19]). Olkoon nyt $a_n = (1+p)^{p^n} - 1$. Kun $n = 1$, niin $a_1 = (1+p)^p - 1$. Jotta saadaan laskettua $|a_1|_p$, ensin on selvitettävä $\text{ord}_p((1+p)^p - 1)$. Newtonin binomikaavan nojalla voidaan kirjoittaa

$$\begin{aligned} (1+p)^p - 1 &= \sum_{n=0}^p \binom{p}{n} 1^{p-n} p^n - 1 \\ &= \binom{p}{0} 1 + \binom{p}{1} p + \binom{p}{2} p^2 + \cdots + \binom{p}{p-1} p^{p-1} + \binom{p}{p} p^p - 1 \\ &= \binom{p}{1} p + \binom{p}{2} p^2 + \cdots + \binom{p}{p-1} p^{p-1} + \binom{p}{p} p^p \\ &= \binom{p}{1} p + \binom{p}{2} p^2 + \cdots + \binom{p}{p-1} p^{p-1} + p^p \\ &= p^2 \left(1 + \binom{p}{2} + \binom{p}{3} p + \cdots + \binom{p}{p-1} p^{p-3} + p^{p-2} \right). \end{aligned}$$

Tässä viimeinen yhtälö saadaan sen perusteella, että $\binom{p}{1} = \frac{p!}{(p-1)!} = p$. Nyt nähdään, että $\text{ord}_p((1+p)^p - 1) = 2$. Lopulta siis

$$|a_1|_p = |(1+p)^p - 1|_p = \frac{1}{p^2}.$$

Induktiolla voidaan todistaa, että $|a_n|_p = \frac{1}{p^{n+1}}$. Koska $\frac{1}{p^{n+1}} \rightarrow 0$, kun $n \rightarrow \infty$, niin $\lim_{n \rightarrow \infty}^{(p)} a_n = 0$ ja kyseinen lukujono on nollajono p -adisen normin $|\cdot|_p$ suhteen.

Esimerkki 3.9. (Vrt. [1, esim. 2.16, s. 19]). Olkoon $R = \mathbb{Q}$ ja $N = |\cdot|$ tavallinen normi. Olkoon (a_n) jono, jonka n :s termi on luvun $\sqrt{2}$ desimaalikehitelmä, jossa on n desimaalia. Siis $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$ jne. On tunnettua, että $\sqrt{2}$ ei ole rationaaliluku, mutta (a_n) on Cauchyn jono. Siis kyseisen Cauchyn jonon raja-arvo ei ole kunnassa \mathbb{Q} .

Edellinen esimerkki osoittaa sen, että kunta \mathbb{Q} ei ole täydellinen tavallisen normin suhteen. Tämä tarkoittaa sitä, että jokaisella rationaaliluvuista muodostetulla Cauchyn jonolla ei ole kunnassa \mathbb{Q} olevaa raja-arvoa. Tiedetään, että reaalilukujen kunta \mathbb{R} on kunnan \mathbb{Q} täydennys tavallisen normin suhteen. Seuraavassa luvussa täydennetään rationaalilukujen kunta \mathbb{Q} p -adisen normin suhteen.

4 p -adiset luvut

Tässä luvussa esitellään p -adisten lukujen rengas \mathbb{Q}_p ja osoitetaan, että \mathbb{Q}_p on itse asiassa kunta. Lopuksi tutkitaan p -adisten lukujen ja kongruenssien välisiä yhteyksiä. Lähdetään liikkeelle yleisestä renkaasta R ja sen normista N .

4.1 Renkaan R täydentäminen normin N suhteen

Olkoon R rengas ja N renkaan R normi. Muodostetaan joukot $\text{CS}(R, N)$ ja $\text{Null}(R, N)$ seuraavalla tavalla.

$$\text{CS}(R, N) = \{(a_n) \mid (a_n) \text{ renkaan } R \text{ Cauchyn jono normin } N \text{ suhteen}\}$$

$$\text{Null}(R, N) = \{(a_n) \mid (a_n) \text{ renkaan } R \text{ nollajono normin } N \text{ suhteen}\}$$

Selvästi on voimassa, että $\text{Null}(R, N) \subseteq \text{CS}(R, N)$. Osoitetaan seuraavaksi, että kahden Cauchyn jonon summa ja tulo ovat edelleen Cauchyn jonoja.

Lause 4.1. *Olkoot $(a_n), (b_n) \in \text{CS}(R, N)$. Silloin jonot*

$$(a_n) + (b_n) = (a_n + b_n) \quad \textit{ja}$$

$$(a_n) \times (b_n) = (a_n b_n)$$

ovat Cauchyn jonoja.

Todistus. Olkoot $(a_n), (b_n) \in \text{CS}(R, N)$. Olkoon $\varepsilon > 0$. Koska jonot (a_n) ja (b_n) ovat Cauchyn jonoja, tiedetään, että on olemassa sellaiset luvut M_1 ja M_2 , että

$$m, n > M_1 \Rightarrow N(a_m - a_n) < \frac{\varepsilon}{2}$$

ja

$$m, n > M_2 \Rightarrow N(b_m - b_n) < \frac{\varepsilon}{2}.$$

Olkoon $M = \max\{M_1, M_2\}$. Oletetaan, että $m, n > M$. Nyt

$$\begin{aligned} N((a_m + b_m) - (a_n + b_n)) &= N((a_m - a_n) + (b_m - b_n)) \\ &\leq N(a_m - a_n) + N(b_m - b_n) \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Siis jono $(a_n + b_n)$ on Cauchyn jono.

Lauseen toisen kohdan osoittamiseksi oletetaan tunnetuksi, että Cauchyn jonot ovat rajoitettuja. Siis on olemassa sellaiset luvut $C_1, C_2 > 0$, että kaikille indeksin n arvoille on voimassa

$$N(a_n) \leq C_1$$

ja

$$N(b_n) \leq C_2.$$

Olkoon $\varepsilon > 0$. Koska jonot (a_n) ja (b_n) ovat Cauchyn jonoja, tiedetään, että on olemassa sellaiset luvut M_1 ja M_2 , että

$$m, n > M_1 \Rightarrow N(a_m - a_n) < \frac{\varepsilon}{2C_2}$$

ja

$$m, n > M_2 \Rightarrow N(b_m - b_n) < \frac{\varepsilon}{2C_1}.$$

Olkoon nyt $M = \max\{M_1, M_2\}$. Oletetaan, että $m, n > M$. Nyt

$$\begin{aligned} N(a_m b_m - a_n b_n) &= N((a_m b_m + a_m b_n) - (a_m b_n + a_n b_n)) \\ &= N(a_m(b_m - b_n) + b_n(a_m - a_n)) \\ &\leq N(a_m(b_m - b_n)) + N(b_n(a_m - a_n)) \\ &= N(a_m)N(b_m - b_n) + N(b_n)N(a_m - a_n) \\ &\leq C_1 \frac{\varepsilon}{2C_1} + C_2 \frac{\varepsilon}{2C_2} = \varepsilon. \end{aligned}$$

Siis jono $(a_n b_n)$ on Cauchyn jono. □

Näin ollen joukko $\text{CS}(R, N)$ muodostaa edellä esiteltyjen laskutoimitusten kanssa (kommutatiivisen) renkaan. Sen nolla-alkio on $0_{\text{CS}} = (0) = (0, 0, 0, \dots)$ ja ykkösalkio on $1_{\text{CS}} = (1_R) = (1_R, 1_R, \dots)$, missä 0 on renkaan R nolla-alkio ja 1_R on renkaan R ykkösalkio. Rengas $\text{CS}(R, N)$ ei ole kuitenkaan kunta, koska siellä on nollanjakajia.

Joukko $\text{Null}(R, N)$ on renkaan $\text{CS}(R, N)$ ideaali. Jos nimittäin $(a_n) \in \text{CS}(R, N)$ ja $(b_n) \in \text{Null}(R, N)$, niin $(a_n b_n), (b_n a_n) \in \text{Null}(R, N)$.

Määritellään sitten *osamäärärengas* $\text{CS}(R, N)/\text{Null}(R, N)$. Kutsutaan tätä renkaan R *täydennykseksi normin N suhteen* ja merkitään \hat{R}_N tai yksinkertaisemmin \hat{R} , jos normi on asiayhteydestä selvä. Renkaan \hat{R}_N alkioit ovat joukon $\text{CS}(R, N)$ ekvivalenssiluokkia. Tällöin siis kaksi Cauchyn jonoa ovat ekvivalentit, jos niiden erotus on nollajono.

Merkitään Cauchyn jonon (a_n) ekvivalenssiluokkaa $\{a_n\}$. Siis $\{a_n\}$ on renkaan \hat{R}_N alkio. Lisäksi ajatellaan, että $R \subset \hat{R}$. Näin voidaan tehdä sen perusteella, että jos $a \in R$, niin $(a_n) = (a)$ on Cauchyn jono ja siis $\{a\} \in \hat{R}$.

Määritellään seuraavaksi renkaan \hat{R}_N laskutoimitukset.

Määritelmä 4.1. Olkoot $\{a_n\}, \{b_n\} \in \hat{R}_N$. Alkioiden *summa* ja *tulo* saadaan kaavoilla

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}, \quad \{a_n\} \times \{b_n\} = \{a_n b_n\}.$$

Lisäksi, jos R on kommutatiivinen rengas, niin myös \hat{R}_N on kommutatiivinen.

Tarkastellaan seuraavaksi renkaan \hat{R}_N normia \hat{N} .

Lause 4.2. *Olkoon $\{c_n\} \in \hat{R}_N$. Alkion $\{c_n\}$ normi on*

$$\hat{N}(\{c_n\}) = \lim_{n \rightarrow \infty} N(c_n).$$

Lisäksi \hat{N} on epäarkhimedinen, jos ja vain jos N on epäarkhimedinen.

Todistus. (Vrt. [1, s. 20–22]).

Todistetaan ensin, että \hat{N} on todellakin normi. Huomautetaan, että esityksessä käytetään jo termiä normi, vaikka varsinaisesti vasta ollaan todistamassa, että \hat{N} on normi.

Olkoon $\{a_n\} \in \hat{R}_N$. Osoitetaan aluksi, että normin \hat{N} määritelmä on järkevä. Todistetaan sitä varten seuraava väite oikeaksi.

Väite:

$$|N(x) - N(y)| \leq N(x - y) \quad \text{aina, kun } x, y \in R.$$

Olkoot $x, y \in R$. Ominaisuuden (N3) nojalla pätee epäyhtälö

$$N(x) = N((x - y) + y) \leq N(x - y) + N(y).$$

Tästä saadaan edelleen, että

$$N(x) - N(y) \leq N(x - y).$$

Aivan vastaavasti vaihtamalla alkioiden x ja y rooleja saadaan, että

$$N(y) - N(x) \leq N(y - x).$$

Näin ollen siis

$$|N(x) - N(y)| \leq N(x - y).$$

Edellinen epäyhtälö on voimassa, koska $N(-z) = N(z)$ aina, kun $z \in R$. Tässä siis $N(x - y) = N(y - x)$. Näin väite on todistettu.

Palataan lauseen 4.2 todistukseen. Koska (a_n) on Cauchyn jono normin N suhteen, niin jokaista lukua $\varepsilon > 0$ kohti on olemassa sellainen luku M , että

$$m, n > M \Rightarrow N(a_m - a_n) < \varepsilon.$$

Tästä ja edellä osoitetusta väitteestä seuraa, että jokaista lukua $\varepsilon > 0$ kohti on olemassa sellainen luku M , että

$$m, n > M \Rightarrow |N(a_m) - N(a_n)| \leq N(a_m - a_n) < \varepsilon.$$

Siis jono $(N(a_n))$ on Cauchyn jono tavallisen normin eli itseisarvon suhteen. Oletetaan tunnetuksi, että reaalilukujen joukossa kaikki Cauchyn jonot supenevat. Näin ollen kyseisellä jonolla on siis raja-arvo. Olkoon se

$$l = \lim_{n \rightarrow \infty} N(a_n).$$

Näin on osoitettu, että $\hat{N}(\{a_n\}) = l$ on määritelty.

Todistetaan seuraavaksi, että \hat{N} on todellakin normi käymällä läpi kohdat (N1)–(N3). Seuraava ekvivalenssiketju, joka seuraa suoraan edellä esitetyistä määritelmistä, todistaa ominaisuuden (N1).

$$\begin{aligned}\hat{N}(\{a_n\}) = 0 &\Leftrightarrow \lim_{n \rightarrow \infty} N(a_n) = 0 \\ &\Leftrightarrow (a_n) \text{ on nollajono} \\ &\Leftrightarrow \{a_n\} = 0.\end{aligned}$$

Olkoot sitten $\{a_n\}, \{b_n\} \in \hat{R}_N$. Kun käytetään renkaan \hat{R}_N laskutoimitusta \times ja normin N ominaisuutta (N2), niin saadaan seuraava yhtälöketju.

$$\begin{aligned}\hat{N}(\{a_n\} \times \{b_n\}) &= \hat{N}(\{a_n b_n\}) = \lim_{n \rightarrow \infty} N(a_n b_n) \\ &= \lim_{n \rightarrow \infty} N(a_n) N(b_n).\end{aligned}$$

Edelleen tulon raja-arvoa koskevan raja-arvon ominaisuuden ja normin \hat{N} määritelmän nojalla saadaan, että

$$\begin{aligned}\lim_{n \rightarrow \infty} N(a_n) N(b_n) &= \lim_{n \rightarrow \infty} N(a_n) \lim_{n \rightarrow \infty} N(b_n) \\ &= \hat{N}(\{a_n\}) \hat{N}(\{b_n\}).\end{aligned}$$

Siis ominaisuus (N2) on voimassa.

Osoitetaan vielä, että myös ominaisuus (N3) pätee. Nyt renkaan \hat{R}_N laskutoimituksen $+$, normin ominaisuuden (N3) sekä summan raja-arvoa koskevan raja-arvon ominaisuuden nojalla saadaan, että

$$\begin{aligned}\hat{N}(\{a_n\} + \{b_n\}) &= \hat{N}(\{a_n + b_n\}) = \lim_{n \rightarrow \infty} N(a_n + b_n) \\ &\leq \lim_{n \rightarrow \infty} (N(a_n) + N(b_n)) \\ &= \lim_{n \rightarrow \infty} N(a_n) + \lim_{n \rightarrow \infty} N(b_n) \\ &= \hat{N}(\{a_n\}) + \hat{N}(\{b_n\}).\end{aligned}$$

Näin siis myös ominaisuus (N3) pätee ja voidaan todeta, että \hat{N} on todella normi.

Vielä on osoitettava lauseen jälkimmäinen osa. Todistetaan sitä varten apulause 4.1.

Apulause 4.1. *Olkoon R rengas ja N renkaan R epäarkhimedinen normi. Oletetaan, että (a_n) on Cauchyn jono ja $b \in R$ sellainen, että $b \neq \lim_{n \rightarrow \infty}^{(N)} a_n$. Tällöin on olemassa sellainen luku M , että aina, kun $m, n > M$, niin*

$$N(a_m - b) = N(a_n - b).$$

Huomautus. Siis indeksistä M lähtien reaalilukujen jono $(N(a_n - b))$ on muuttumaton.

Todistetaan nyt apulause 4.1.

Todistus. Huomataan ensin, että lauseen 4.2 todistuksen yhteydessä todistetun väitteen nojalla

$$|N(a_m - b) - N(a_n - b)| \leq N(a_m - a_n).$$

Koska (a_n) on Cauchyn jono, niin myös jono $(N(a_n - b))$ on Cauchyn jono itseisarvon suhteen reaalilukujen joukossa \mathbb{R} . Näin ollen kyseisellä jonolla on raja-arvo. Olkoon se $l = \lim_{n \rightarrow \infty} N(a_n - b)$. Huomataan lisäksi, että $l > 0$. Tällöin jonon raja-arvon määritelmän nojalla on olemassa sellainen luku M_1 , että

$$n > M_1 \Rightarrow |N(a_n - b) - l| < \frac{l}{2}.$$

Tästä saadaan, että

$$(4.1) \quad n > M_1 \Rightarrow N(a_n - b) > \frac{l}{2}.$$

Koska (a_n) on Cauchyn jono normin N suhteen, niin on olemassa sellainen luku M_2 , että

$$(4.2) \quad m, n > M_2 \Rightarrow N(a_m - a_n) < \frac{l}{2}.$$

Olkoon sitten $M = \max\{M_1, M_2\}$. Oletetaan, että $m, n > M$. Nyt normin ominaisuuden (N4) sekä kaavojen (4.1) ja (4.2) nojalla voidaan kirjoittaa

$$\begin{aligned} N(a_m - b) &= N((a_n - b) + (a_m - a_n)) \\ &\leq \max\{N(a_n - b), N(a_m - a_n)\} \\ &= N(a_n - b). \end{aligned}$$

Vastaavasti vaihtamalla indeksien m ja n rooleja saadaan, että

$$N(a_n - b) \leq N(a_m - b).$$

Näin apulause 4.1 on todistettu. \square

Palataan jälleen takaisin lauseen 4.2 todistukseen. Jotta normi \hat{N} olisi epäarkhimedinen, on osoitettava, että ominaisuus (N4) on voimassa kyseiselle normille.

Olkoot $\{a_n\}, \{b_n\} \in \hat{R}_N$ sellaisia, että $\hat{N}(\{a_n\}) \neq \hat{N}(\{b_n\})$. Jos $\{a_n\}$ tai $\{b_n\}$ on $\{0\}$, niin ominaisuus (N4) on selvästi voimassa. Oletetaan siksi, että $\{a_n\}, \{b_n\} \neq \{0\}$. Hyödynnetään nyt apulauseetta 4.1 tilanteessa, jossa $b = 0$. Apulauseen 4.1 mukaan on siis olemassa sellainen luku M_1 , että

$$m, n > M_1 \Rightarrow N(a_m) = N(a_n).$$

Tämä tarkoittaa sitä, että

$$n > M_1 \Rightarrow N(a_n) = \lim_{n \rightarrow \infty} N(a_n).$$

Siis normin \hat{N} määritelmän nojalla edelleen

$$(4.3) \quad n > M_1 \Rightarrow N(a_n) = \lim_{n \rightarrow \infty} N(a_n) = \hat{N}(\{a_n\}).$$

Myös jonon $(N(b_n))$ tapauksessa on olemassa sellainen luku M_2 , että

$$m, n > M_2 \Rightarrow N(b_m) = N(b_n).$$

Vastaavasti kuin edellä voidaan jälleen päätellä, että

$$(4.4) \quad n > M_2 \Rightarrow N(b_n) = \lim_{n \rightarrow \infty} N(b_n) = \hat{N}(\{b_n\}).$$

Valitaan nyt $M = \max\{M_1, M_2\}$ ja oletetaan, että $n > M$. Tällöin ominaisuuden (N4') sekä kaavojen (4.3) ja (4.4) nojalla saadaan, että

$$\begin{aligned} \hat{N}(\{a_n\} + \{b_n\}) &= \hat{N}(\{a_n + b_n\}) = \lim_{n \rightarrow \infty} N(a_n + b_n) \\ &= \lim_{n \rightarrow \infty} \max\{N(a_n), N(b_n)\} \\ &= \max \left\{ \lim_{n \rightarrow \infty} N(a_n), \lim_{n \rightarrow \infty} N(b_n) \right\} \\ &= \max \left\{ \hat{N}(\{a_n\}), \hat{N}(\{b_n\}) \right\}. \end{aligned}$$

Näin on osoitettu, että normille \hat{N} on voimassa myöskin ehto (N4). Tämä päättää lauseen 4.2 todistuksen. \square

Määritelmä 4.2. Olkoon R rengas ja N renkaan R normi. Rengas R on *täydellinen normin N suhteen*, jos jokaisella renkaan R Cauchyn jonolla (a_n) on raja-arvo $a \in R$ normin N suhteen.

Määritelmä 4.3. Olkoon R rengas, N renkaan R normi ja olkoon $X \subseteq R$. Joukko X on *tiheä* renkaassa R , jos jokainen renkaan R alkio on joidenkin joukon X alkioden raja-arvo normin N suhteen.

Lause 4.3. *Olkoon R rengas ja N renkaan R normi. Tällöin rengas \hat{R} on täydellinen normin \hat{N} suhteen. Lisäksi R on renkaan \hat{R} tiheä alirengas.*

Todistus. (Vrt. [1, s. 23–24]).

Osoitetaan ensin, että R on renkaan \hat{R} tiheä alirengas. On jo todettu, että R on renkaan \hat{R} osajoukko. Voidaan osoittaa, että R on renkaan \hat{R} alirengas. Sivuutetaan tämä tarkastelu ja osoitetaan, että R on tiheä renkaassa \hat{R} . Käytetään tässä lähdettä [6, s. 18].

Olkoon $A \in \hat{R}$ ja (a_m) renkaan R Cauchyn jono, joka on ekvivalenssiluokan A edustaja. Muodostetaan nyt jokaista positiivista kokonaislukua n kohti vakiojono (a_n) . Nyt jono $(a_m - a_n)$ on ekvivalenssiluokan $A - \{a_n\}$ edustaja. Siis

$$\lim_{n \rightarrow \infty} \hat{N}(A - \{a_n\}) = \lim_{m, n \rightarrow \infty} N(a_m - a_n) = 0.$$

Tässä käytettiin sitä tietoa, että jono (a_m) on Cauchyn jono. Siis rengas R on tiheä renkaassa \hat{R} määritelmän 4.3 nojalla.

Vielä on osoitettava, että rengas \hat{R} on täydellinen normin \hat{N} suhteen. Olkoon (α_n) renkaan \hat{R} Cauchyn jono. On siis osoitettava, että on olemassa sellainen $\alpha \in \hat{R}$, että

$$\lim_{n \rightarrow \infty}^{(\hat{N})} \alpha_n = \alpha.$$

Koska (α_n) on renkaan \hat{R} Cauchyn jono, niin jokainen jonon (α_n) alkio α_m on jonkin renkaan R Cauchyn jonon (a_{mn}) ekvivalenssiluokka. On selvää, että jokaisen renkaan R Cauchyn jonon raja-arvo on kyseisen jonon ekvivalenssiluokka. Tämän perusteella jokaiselle jonolle (a_{mn}) voidaan kirjoittaa

$$\alpha_m = \lim_{n \rightarrow \infty}^{(\hat{N})} a_{mn}.$$

Konstruoidaan nyt sellainen renkaan R Cauchyn jono (c_n) , että

$$\{c_n\} = \lim_{m \rightarrow \infty}^{(\hat{N})} \alpha_m.$$

Tällöin $\alpha = \{c_n\}$ on jonon (α_n) raja-arvo.

Koska $\alpha_m = \lim_{n \rightarrow \infty}^{(\hat{N})} a_{mn}$, niin jonon raja-arvon määritelmän perusteella jokaiselle indeksille m on olemassa sellainen indeksi M_m , että

$$(4.5) \quad n > M_m \Rightarrow \hat{N}(\alpha_m - a_{mn}) < \frac{1}{m}.$$

Valitaan nyt jokaista indeksiiä m kohti kokonaisluku $k(m) > M_m$. Oletetaan, että $k(1) < k(2) < \dots < k(m) < \dots$. Määritellään nyt jono (c_n) asettamalla $c_n = a_{nk(n)}$. Osoitetaan, että kyseinen jono on Cauchyn jono normin \hat{N} suhteen, ja että todellakin $\lim_{m \rightarrow \infty}^{(\hat{N})} \alpha_m = \{c_n\}$. Tehdään tämä apulauseiden 4.2 ja 4.3 avulla.

Apulause 4.2. *Jono (c_n) on Cauchyn jono normin \hat{N} suhteen.*

Todistus. (Vrt. [1, s. 23]).

Olkoon $\varepsilon > 0$. Koska jono (α_n) on Cauchyn jono normin \hat{N} suhteen, niin on olemassa sellainen luku M' , että

$$n_1, n_2 > M' \Rightarrow \hat{N}(\alpha_{n_1} - \alpha_{n_2}) < \frac{\varepsilon}{3}.$$

Käytetään nyt jonon (c_n) määritelmää sekä normin ominaisuutta (N3). Lisäksi vähennetään ja lisätään sopivasti termejä. Näin saadaan, että

$$\begin{aligned}\hat{N}(c_{n_1} - c_{n_2}) &= \hat{N}((a_{n_1 k(n_1)} - \alpha_{n_1}) + (\alpha_{n_1} - \alpha_{n_2}) + (\alpha_{n_2} - a_{n_2 k(n_2)})) \\ &\leq \hat{N}(a_{n_1 k(n_1)} - \alpha_{n_1}) + \hat{N}(\alpha_{n_1} - \alpha_{n_2}) + \hat{N}(\alpha_{n_2} - a_{n_2 k(n_2)}).\end{aligned}$$

Olkoon nyt $M = \max\{M', 3/\varepsilon\}$. Kun $n_1, n_2 > M$, niin kaavan (4.5) nojalla

$$\begin{aligned}\hat{N}(a_{n_1 k(n_1)} - \alpha_{n_1}) &< \frac{1}{n_1} < \frac{1}{3/\varepsilon} = \frac{\varepsilon}{3} \quad \text{ja} \\ \hat{N}(a_{n_2 k(n_2)} - \alpha_{n_2}) &< \frac{1}{n_2} < \frac{1}{3/\varepsilon} = \frac{\varepsilon}{3}.\end{aligned}$$

Kokonaisuudessaan saadaan siis, että kun $n_1, n_2 > M$, niin

$$\hat{N}(c_{n_1} - c_{n_2}) < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.$$

Näin on osoitettu, että (c_n) on Cauchyn jono. □

Apulause 4.3. $\lim_{m \rightarrow \infty}^{(\hat{N})} \alpha_m = \{c_n\}$.

Todistus. (Vrt. [1, s. 24]).

Olkoon $\varepsilon > 0$. Merkitään $\{c_n\} = \gamma$. Nyt käyttämällä normin ominaisuutta (N3) saadaan, että

$$\begin{aligned}\hat{N}(\gamma - \alpha_m) &= \hat{N}((\gamma - a_{mk(m)}) + (a_{mk(m)} - \alpha_m)) \\ &\leq \hat{N}(\gamma - a_{mk(m)}) + \hat{N}(a_{mk(m)} - \alpha_m) \\ &= \lim_{n \rightarrow \infty} N(a_{nk(n)} - a_{mk(m)}) + \hat{N}(a_{mk(m)} - \alpha_m).\end{aligned}$$

Viimeinen yhtälö saadaan sen perusteella, että normin \hat{N} määritelmän perusteella

$$\hat{N}(\gamma - a_{mk(m)}) = \lim_{n \rightarrow \infty} N(a_{nk(n)} - a_{mk(m)}).$$

Olkoon M'' sellainen luku, että $M'' > 2/\varepsilon$. Koska jono $(c_n) = (a_{nk(n)})$ ja apulauseessa 4.2 osoitettiin, että (c_n) on Cauchyn jono, niin tällöin

$$N(a_{n_1 k(n_1)} - a_{n_2 k(n_2)}) < \frac{\varepsilon}{2}$$

aina, kun $n_1, n_2 > M''$. Oletetaan, että $m, n > M''$. Tällöin kaavan (4.5) nojalla

$$\hat{N}(a_{mk(m)} - \alpha_m) < \frac{1}{m} < \frac{1}{M''} < \frac{1}{2/\varepsilon} = \frac{\varepsilon}{2}.$$

Kokonaisuutena siis

$$\lim_{n \rightarrow \infty} N(a_{nk(n)} - a_{mk(m)}) + \hat{N}(a_{mk(m)} - \alpha_m) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Näin ollen on siis osoitettu, että

$$\hat{N}(\gamma - \alpha_m) < \varepsilon \quad \text{aina, kun } m > M''.$$

Siis

$$\lim_{m \rightarrow \infty} {}^{(\hat{N})} \alpha_m = \{c_n\}.$$

□

Näin lause 4.3 on todistettu. □

4.2 p -adisten lukujen kunta \mathbb{Q}_p

Tässä luvussa siirrytään yleisestä renkaasta R ja sen normista N tapaukseen, jossa $R = \mathbb{Q}$ ja normina on p -adinen normi $|\cdot|_p$. Määritellään ensin p -adisten lukujen rengas.

Määritelmä 4.4. p -adisten lukujen rengas \mathbb{Q}_p on renkaan \mathbb{Q} täydennys p -adisen normin $|\cdot|_p$ suhteen. Käytetään myös renkaan \mathbb{Q}_p normille merkintää $|\cdot|_p$.

Siis edellisessä luvussa opitun perusteella renkaan \mathbb{Q}_p alkiot ovat kunnan \mathbb{Q} Cauchyn jonojen ekvivalenssiluokkia p -adisen normin laajennuksen suhteen. p -adisen normin laajennus saadaan lauseessa 4.2 esitetyllä tavalla.

Määritellään seuraavaksi p -adiset kokonaisluvut.

Määritelmä 4.5. p -adisten kokonaislukujen joukko on

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\}.$$

Huomautus. Selvästi p -adisten kokonaislukujen joukko \mathbb{Z}_p on renkaan \mathbb{Q}_p alirenkas. Tämän osoittamiseksi oletetaan, että $\alpha, \beta \in \mathbb{Z}_p$. Nyt normin ominaisuuden (N4) nojalla

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}.$$

Koska oletuksen perusteella $|\alpha|_p \leq 1$ ja $|\beta|_p \leq 1$, saadaan $|\alpha + \beta|_p \leq 1$. Siis $\alpha + \beta \in \mathbb{Z}_p$.

Vastaavasti ominaisuuden (N2) ja oletuksen perusteella

$$|\alpha\beta|_p = |\alpha|_p |\beta|_p \leq 1.$$

Siis $\alpha\beta \in \mathbb{Z}_p$.

Tutkitaan nyt tarkemmin renkaan \mathbb{Q}_p alkioita. Tieto siitä, että ne ovat Cauchyn jonojen ekvivalenssiluokkia, ei anna alkioista konkreettista kuvaa. Todistetaan aluksi seuraava apulause.

Apulause 4.4. (Ks. [6, Lemma 1.29, s. 22]). Jos $x \in \mathbb{Q}$ ja $|x|_p \leq 1$, niin jokaista lukua i kohti on olemassa sellainen kokonaisluku $\alpha \in \mathbb{Z}$, että

$$|\alpha - x|_p \leq p^{-i}.$$

Luku α voidaan valita joukosta $\{0, 1, 2, \dots, p^i - 1\}$. Jos luku α valitaan tästä joukosta, niin se on yksikäsitteinen.

Todistus. (Vrt. [6, s. 22]).

Oletetaan, että $x \in \mathbb{Q}$ ja $|x|_p \leq 1$. Olkoon $x = a/b$, missä luvut a ja b ovat suhteellisia alkulukuja. Siis $(a, b) = 1$. Koska lisäksi oletuksen nojalla $|x|_p \leq 1$, niin on oltava $p \nmid b$. Näin ollen siis myös luvut b ja p^i ovat suhteellisia alkulukuja eli $(b, p^i) = 1$. Siis lauseen 2.3 nojalla on olemassa sellaiset luvut $m, n \in \mathbb{Z}$, että $mb + np^i = 1$. Olkoon $\alpha = am$. Selvästi $\alpha \in \mathbb{Z}$. Nyt käyttämällä normin ominaisuutta (N2) ja oletusta $|\frac{a}{b}|_p \leq 1$ saadaan, että

$$\begin{aligned} |\alpha - x|_p &= \left| am - \frac{a}{b} \right|_p = \left| \frac{a}{b} \right|_p |mb - 1|_p \\ &\leq |mb - 1|_p. \end{aligned}$$

Huomataan, että lauseke $mb - 1$ voidaan esittää muodossa $mb - 1 = -np^i$. Koska $|-np^i|_p = |np^i|_p$, saadaan edelleen käyttämällä lisäksi ominaisuutta (N2) ja konkreettisesti laskemalla, että

$$\begin{aligned} |mb - 1|_p &= |np^i|_p = |n|_p |p^i|_p \\ &= |n|_p p^{-i} \leq p^{-i}. \end{aligned}$$

Normin ominaisuuden (N4) nojalla kokonaislukuun α voidaan lisätä luvun p^i monikertoja niin, että saadaan luku, joka on joukossa $\{0, \dots, p^i - 1\}$, ja jolle pätee edelleen, että $|\alpha - x|_p \leq p^{-i}$. \square

Lause 4.4. (Ks. [2, Lause 3.3.4(iii), s. 61]). Olkoon $\alpha \in \mathbb{Z}_p$. Tällöin on olemassa Cauchyn jono (a_i) , jonka raja-arvo on α . Tälle Cauchyn jonolle on voimassa seuraavat ominaisuudet:

(1) $a_i \in \mathbb{Z}$, $0 \leq a_i < p^i$, $i = 1, 2, \dots$

(2) $a_i \equiv a_{i+1} \pmod{p^i}$, $i = 1, 2, \dots$

Todistus. (Vrt. [6, Lause 1.30, s. 22]).

Olkoon $\alpha \in \mathbb{Z}_p$ ja (b_i) Cauchyn jono, joka on ekvivalenssiluokan α edustaja. Lauseen todistamiseksi on siis löydettävä sellainen jonon (b_i) kanssa ekvivalentti jono (a_i) , jolle on voimassa ehdot (1) ja (2).

Nyt $|\alpha|_p = \lim_{i \rightarrow \infty} |b_i|_p$ lauseen 4.2 nojalla. Koska $\alpha \in \mathbb{Z}_p$, niin $|\alpha|_p \leq 1$. Näin ollen voidaan olettaa, että $|b_i|_p \leq 1$ jokaiselle indeksille i .

Olkoon nyt $K(j)$, missä $j = 1, 2, \dots$, sellainen positiivinen kokonaisluku, että

$$(4.6) \quad |b_i - b_{i'}|_p \leq \frac{1}{p^j} \quad \text{aina, kun } i, i' \geq K(j).$$

Näin voidaan asettaa, koska (b_i) on Cauchyn jono. Voidaan myös olettaa, että $K(j) \geq j$. Nyt apulauseen 4.4 nojalla on olemassa sellaiset kokonaisluvut a_j , missä $0 \leq a_j < p^j$, että

$$(4.7) \quad |a_j - b_{K(j)}|_p \leq \frac{1}{p^j}.$$

Näin on osoitettu, että jono (a_j) toteuttaa ehdon (1).

Osoitetaan sitten, että kyseiselle jonolle (a_j) on voimassa myös ominaisuus

$$a_j \equiv a_{j+1} \pmod{p^j}.$$

Käytetään tässä lausetta 3.2. Kirjoitetaan

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{K(j)} - (a_j - b_{K(j)})|_p \\ &\leq \max \{ |a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{K(j)}|_p, |a_j - b_{K(j)}|_p \} \\ &\leq \max \{ 1/p^{j+1}, 1/p^j, 1/p^j \} = 1/p^j. \end{aligned}$$

Edellisessä epäyhtälöt

$$|a_{j+1} - b_{N(j+1)}|_p \leq 1/p^{j+1}$$

ja

$$|a_j - b_{K(j)}|_p \leq 1/p^j$$

saadaan kaavan (4.7) nojalla. Epäyhtälö

$$|b_{N(j+1)} - b_{K(j)}|_p \leq 1/p^j$$

seuraa kaavasta (4.6).

Nyt lauseen 3.2 nojalla jonolle (a_j) on voimassa myös $a_j \equiv a_{j+1} \pmod{p^j}$ eli ehto (2) toteutuu.

Osoitetaan lopuksi, että jonot (a_j) ja (b_i) ovat ekvivalentit. Siis riittää osoittaa, että niiden erotus on nollajono p -adisen normin suhteen.

Olkoon j mielivaltainen ja $i \geq K(j)$. Nyt

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{K(j)} - (b_i - b_{K(j)})|_p \\ &\leq \max \{ |a_i - a_j|_p, |a_j - b_{K(j)}|_p, |b_i - b_{K(j)}|_p \} \\ &\leq \max \{ 1/p^j, 1/p^j, 1/p^j \} = 1/p^j. \end{aligned}$$

Tässä

$$|a_i - a_j|_p \leq 1/p^j$$

seuraa ominaisuudesta (2),

$$|a_j - b_{K(j)}|_p \leq 1/p^j$$

kaavasta (4.7) ja

$$|b_i - b_{K(j)}|_p \leq 1/p^j$$

saadaan kaavan (4.6) perusteella.

Nyt siis $|a_i - b_i|_p \rightarrow 0$, kun $i \rightarrow \infty$, joten määritelmän 3.7 nojalla jonojen (a_j) ja (b_i) erotus on nollajono. Siis kyseiset jonot ovat ekvivalentit.

Lisäksi jonon (a_j) raja-arvo on α sen perusteella, että $|\alpha - a_j|_p \leq p^{-j}$. Näin lause 4.4 on todistettu. \square

Todistetaan seuraavaksi, että jokaisella lauseen 4.4 mukaisella jonolla on raja-arvo p -adisten lukujen renkaassa \mathbb{Z}_p .

Lause 4.5. *Olkoon (a_n) lauseen 4.4 ominaisuudet täyttävä jono. Tällöin jonolla (a_n) on raja-arvo $a \in \mathbb{Z}_p$.*

Todistus. (Vrt. [2, teht. 101, s. 252]).

Olkoon (a_n) jono, jolle on voimassa lauseen 4.4 ominaisuudet (1) ja (2). Tällöin (a_n) on selvästi Cauchyn jono. Näin ollen sillä on raja-arvo a . Osoitetaan nyt, että $a \in \mathbb{Z}_p$.

Koska $a_n \in \mathbb{Z}$ kaikilla indekseillä n , niin $\text{ord}_p a_n \geq 0$ kaikille indekseille n . Tällöin voidaan helposti todeta, että $|a_n|_p \leq 1$. Koska $\lim_{n \rightarrow \infty} a_n = a$ p -adisen normin suhteen, niin on olemassa sellainen luku M , että

$$n > M \Rightarrow |a_n - a|_p < 1.$$

Nyt

$$|a|_p = |a_n + (a - a_n)|_p \leq \max\{|a_n|_p, |a - a_n|_p\} \leq 1.$$

Näin on osoitettu, että $a \in \mathbb{Z}_p$. \square

Jos $\alpha \in \mathbb{Z}_p$, niin lauseen 4.4 nojalla ekvivalenssiluokan α edustajan (a_i) termit voidaan kirjoittaa muodossa

$$a_i = \alpha_0 + \alpha_1 p + \cdots + \alpha_{i-1} p^{i-1},$$

missä jokainen α_i on jokin kokonaisluku joukosta $\{0, 1, \dots, p-1\}$. Nyt ehdon (2) nojalla

$$a_{i+1} = \alpha_0 + \alpha_1 p + \cdots + \alpha_{i-1} p^{i-1} + \alpha_i p^i.$$

Esitystä

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$$

sanotaan luvun $\alpha \in \mathbb{Z}_p$ *p-adiseksi laajennukseksi*. Tässä esityksessä luvut α_i ovat *p-adiset numerot*.

Osoitetaan seuraavaksi, että kyseinen *p*-adinen laajennus on yksikäsitteinen.

Lause 4.6. *Olkoon $\alpha \in \mathbb{Z}_p$. Luvun α p-adinen laajennus*

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$$

on yksikäsitteinen.

Todistus. (Vrt. [1, s. 25–26]).

Olkoon nyt $\alpha \in \mathbb{Z}_p$ ja

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$$

luvun α *p*-adinen laajennus. Tehdään vastaoletus, että luvulle α on olemassa toinenkin laajennus

$$\alpha = \alpha'_0 + \alpha'_1 p + \alpha'_2 p^2 + \dots$$

ja laajennukset eivät ole samat. Siis vähintään yhdelle i on oltava $\alpha_i \neq \alpha'_i$.
Olkoon d ensimmäinen tällainen kokonaisluku. Siis $\alpha_d \neq \alpha'_d$. Oletetaan, että $\alpha_d < \alpha'_d$. Koska luvut α_d ja α'_d ovat joukossa $\{0, 1, \dots, p-1\}$, niin oletuksesta $\alpha_d < \alpha'_d$ seuraa, että $1 \leq \alpha'_d - \alpha_d \leq p-1$.

Oletetaan, että

$$\begin{aligned} a_{n+1} &= \alpha_0 + \alpha_1 p + \dots + \alpha_n p^n \quad \text{ja} \\ a'_{n+1} &= \alpha'_0 + \alpha'_1 p + \dots + \alpha'_n p^n. \end{aligned}$$

Nyt

$$a'_{d+1} - a_{d+1} = (\alpha'_d - \alpha_d) p^d.$$

Selvästi

$$|a'_{d+1} - a_{d+1}|_p = \frac{1}{p^d}.$$

Toisaalta

$$\begin{aligned} |a'_{d+1} - a_{d+1}|_p &= |(a'_{d+1} - \alpha) + (\alpha - a_{d+1})|_p \\ &\leq \max \{ |a'_{d+1} - \alpha|_p, |\alpha - a_{d+1}|_p \} \\ &< \frac{1}{p^d}. \end{aligned}$$

Tulos $|a'_{d+1} - a_{d+1}|_p < \frac{1}{p^d}$ nähdään, kun suoritetaan laskut $|a'_{d+1} - \alpha|_p$ ja $|\alpha - a_{d+1}|_p$. Koska $|a'_{d+1} - a_{d+1}|_p = \frac{1}{p^d}$ ja $|a'_{d+1} - a_{d+1}|_p < \frac{1}{p^d}$, on päädytty ristiriitaan. Siis luvun α *p*-adinen laajennus on yksikäsitteinen. \square

Edellä käsiteltiin tapaus $\alpha \in \mathbb{Z}_p$ eli $\alpha \in \mathbb{Q}_p$ ja $|\alpha|_p \leq 1$. Siirrytään nyt tapaukseen, jossa $\alpha \in \mathbb{Q}_p$ mutta $|\alpha|_p > 1$. Tarkoitus on löytää myös tällaiselle p -adiselle luvulle p -adinen laajennus.

Olkoon siis $\alpha \in \mathbb{Q}_p$ sellainen p -adinen luku, että $|\alpha|_p > 1$. Siis $|\alpha|_p = p^k$, missä $k > 0$. Kerrotaan nyt luku α luvulla p^k . Saadaan p -adinen luku $\beta = p^k \alpha$. Tälle luvulle pätee, että $|\beta|_p \leq 1$. Näin ollen luvulle β on olemassa p -adinen laajennus. Olkoon se

$$\beta = \beta_0 + \beta_1 p + \beta_2 p^2 + \dots$$

Sijoitetaan nyt β yhtälöön $\beta = p^k \alpha$. Siis saadaan, että

$$\beta_0 + \beta_1 p + \beta_2 p^2 + \dots = p^k \alpha.$$

Jaetaan yhtälö nyt puolittain luvulla p^k . Saadaan, että

$$\alpha = \frac{\beta_0}{p^k} + \frac{\beta_1 p}{p^k} + \dots + \frac{\beta_{k-1} p^{k-1}}{p^k} + \frac{\beta_k p^k}{p^k} + \frac{\beta_{k+1} p^{k+1}}{p^k} + \dots + \frac{\beta_{k+r} p^{k+r}}{p^k} + \dots$$

Kun suoritetaan sievennykset, niin saadaan edelleen, että

$$\alpha = \frac{\beta_0}{p^k} + \frac{\beta_1}{p^{k-1}} + \dots + \frac{\beta_{k-1}}{p} + \beta_k + \beta_{k+1} p + \dots + \beta_{k+r} p^r + \dots,$$

missä kertoimet β_n ovat välillä $0 \leq \beta_n \leq p - 1$. Näin luvulle α on saatu p -adinen laajennus. Seuraava lause yhdistää edelliset tarkastelut.

Lause 4.7. *Jokaisella p -adisella luvulla $\alpha \in \mathbb{Q}_p$ on yksikäsitteinen p -adinen laajennus*

$$\alpha = \alpha_{-r} p^{-r} + \alpha_{1-r} p^{1-r} + \alpha_{2-r} p^{2-r} + \dots + \alpha_{-1} p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots,$$

missä $\alpha_n \in \mathbb{Z}$ ja $0 \leq \alpha_n \leq p - 1$. Lisäksi $\alpha \in \mathbb{Z}_p$, jos ja vain jos $\alpha_{-r} = 0$ aina, kun $r > 0$.

Todistus. Lause seuraa edellisistä tarkasteluista. □

Tavallisen desimaaliesityksen tapaan tällainen lauseen 4.7 mukainen p -adinen laajennus voidaan esittää muodossa

$$\alpha_{-r} \alpha_{1-r} \alpha_{2-r} \dots \alpha_{-1} \alpha_0, \alpha_1 \alpha_2 \dots$$

[8, s. 3].

Huomautus. Vaikka ns. tavallisesta, lukijalle tutusta desimaaliesityksestä poiketen luvun p potenssit kasvavat oikealle päin mentäessä, käytännössä p -adisten laajennusten muodostamisessa kannattaa lähteä liikkeelle korkeimmasta potenssista, joka ei ylitä sitä lukua, jolle laajennusta kehitetään

[8, s. 3].

Huomautus. Tavallisessa kymmenjärjestelmässä esimerkiksi luvulla 1 on kaksi eri desimaalikehitelmää. Nimittäin $1 = 0,999\dots = 1,000\dots$. Tämä ei siis p -adisien lukujen tapauksessa ole mahdollista.

Käydään seuraavaksi läpi konkreettinen esimerkki p -adisista laajennuksista.

Esimerkki 4.1. Kirjoitetaan luvun 133 3-adinen laajennus.

$$133 = 1 \cdot 3^0 + 2 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4.$$

5-adisesti esitys 321,421 tarkoittaa lukua

$$3 \cdot 5^{-2} + 2 \cdot 5^{-1} + 1 \cdot 5^0 + 4 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3.$$

p -adisilla luvuilla voidaan laskea kuten tavallisilla desimaaliluvuilla. Käsitellään seuraavaksi esimerkki yhteen-, vähennys- ja kertolaskusta. Suoriteetaan laskut allekkain. On huomattava, että poiketen tavallisista allekkainlaskuista nyt edetään vasemmalta oikealle.

Esimerkki 4.2. Lasketaan yhteen 7-adiset luvut 4,213 ja 6,105.

$$\begin{array}{rcccc|c} 4, & 2 & 1 & 3 & & \\ 6, & 1 & 0 & 5 & & + \\ \hline 3, & 4 & 1 & 1 & 1 & \end{array}$$

Vähennetään 7-adisesta luvusta 5,43 luku 2,51.

$$\begin{array}{rccc|c} 5, & 4 & 3 & & \\ 2, & 5 & 1 & & - \\ \hline 3, & 6 & 1 & & \end{array}$$

Esimerkki 4.3. (Ks. [8, s. 4]). Kerrotaan 5-adinen luku 1,3042 itsellään.

$$\begin{array}{rcccccc|c} 1, & 3 & 0 & 4 & 2 & & & \\ 1, & 3 & 0 & 4 & 2 & & & \cdot \\ \hline 1, & 3 & 0 & 4 & 2 & & & \\ & 3 & 9 & 0 & 12 & 6 & & \\ & & 0 & 0 & 0 & 0 & 0 & \\ & & & 4 & 12 & 0 & 16 & 8 \\ & & & & 2 & 6 & 0 & 8 & 4 & + \\ \hline 1, & 1 & 0 & 0 & 0 & 3 & 3 & 4 & 2 & 1 \end{array}$$

Osoitetaan nyt, että \mathbb{Q}_p on kunta.

Lause 4.8. \mathbb{Q}_p on kunta.

Todistus. (Vrt. [1, s. 27] ja [2, Lemma 3.2.8, s. 55]).

Lauseen todistamiseksi riittää osoittaa, että jokaisella nolasta poikkeavalla alkiolla on käänteisalkio.

Olkoon siis $\alpha \in \mathbb{Q}_p$ sellainen, että $\alpha \neq 0$. Tällöin normin ominaisuuksien nojalla $|\alpha|_p \neq 0$. Olkoon nyt

$$l = |\alpha|_p = \lim_{n \rightarrow \infty} |a_n|_p > 0.$$

Nyt raja-arvon määritelmän nojalla on olemassa sellainen luku M_1 , että

$$n > M_1 \Rightarrow |a_n|_p > l/2.$$

Tämä taas tarkoittaa sitä, että kun $n > M_1$, niin $a_n \neq 0$. Näin ollen jokaisella a_n on käänteisalkio kunnassa \mathbb{Q} indeksistä $M_1 + 1$ lähtien.

Määritellään nyt jono (b_n) seuraavasti:

$$b_n = \begin{cases} 0, & \text{kun } n \leq M_1, \\ \frac{1}{a_n}, & \text{kun } n > M_1. \end{cases}$$

Osoitetaan, että näin määritelty jono (b_n) on Cauchyn jono p -adisen normin suhteen.

Olkoon $\varepsilon > 0$. Koska (a_n) on Cauchyn jono, niin tällöin on olemassa sellainen luku M_2 , että

$$m, n > M_2 \Rightarrow |a_m - a_n|_p < \frac{\varepsilon l^2}{4}.$$

Valitaan $M = \max\{M_1, M_2\}$. Oletetaan, että $m, n > M$. Nyt

$$|b_m - b_n|_p = \left| \frac{1}{a_m} - \frac{1}{a_n} \right|_p = \left| \frac{a_n - a_m}{a_m a_n} \right|_p = \frac{|a_m - a_n|_p}{|a_m a_n|_p} = \frac{|a_m - a_n|_p}{|a_m|_p |a_n|_p} < \frac{\frac{\varepsilon l^2}{4}}{\frac{l^2}{4}} = \varepsilon.$$

Siis (b_n) on Cauchyn jono.

Muodostetaan nyt jono $(a_n b_n)$. On helppo nähdä, että jono on seuraavanlainen:

$$a_n b_n = \begin{cases} 0, & \text{kun } n \leq M_1, \\ 1, & \text{kun } n > M_1. \end{cases}$$

Siis vielä konkreettisemmin

$$(a_n b_n) = (\underbrace{0, \dots, 0}_{M_1 \text{ kpl}}, 1, 1, 1, \dots).$$

Nyt jonossa (a_nb_n) on siis äärellinen määrä alkioita 0 ja ääretön määrä alkioita 1, joten on selvää, että $\lim_{n \rightarrow \infty} a_nb_n = 1$. Edelleen jonojen (1) ja (a_nb_n) erotukseksi saadaan

$$\begin{aligned} (1) - (a_nb_n) &= (1, 1, \dots) - \underbrace{(0, \dots, 0, 1, 1, 1, \dots)}_{M_1 \text{ kpl}} \\ &= \underbrace{(1, \dots, 1, 0, 0, 0, \dots)}_{M_1 \text{ kpl}}. \end{aligned}$$

Tämän jonon raja-arvo on 0, joten kyseessä on nollajono. Siis $\alpha\beta = 1$, joten $\beta = \alpha^{-1}$. Näin on osoitettu, että \mathbb{Q}_p on kunta. \square

4.3 Henselin lemma ja kongruenssit

Henselin lemma on luultavasti tärkein p -adisten lukujen ominaisuus. Sen avulla voidaan selvittää, onko polynomilla juuria renkaassa \mathbb{Z}_p . [2, s. 69.] Tässä luvussa käydään läpi polynomien juurten ja kongruenssien välisiä yhteyksiä. Luvun lähteenä on [6, s. 34–38].

Lause 4.9 (Henselin lemma). *Olkoon $F(x) = c_0 + c_1x + \dots + c_nx^n$ polynomi, jonka kertoimet ovat p -adisia kokonaislukuja. Olkoon*

$$F'(x) = c_1 + 2c_2x + 3c_3x^2 + \dots + nc_nx^{n-1}$$

polynomien F muodollinen derivaatta. Oletetaan, että \bar{a}_0 on p -adinen kokonaisluku, jolle pätee $F(\bar{a}_0) \equiv 0 \pmod{p}$ ja $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$. Tällöin on olemassa yksikäsitteinen p -adinen kokonaisluku a , jolle pätee $F(a) = 0$ ja $a \equiv \bar{a}_0 \pmod{p}$.

Todistus. Osoitetaan, että tällainen p -adinen kokonaisluku a on olemassa konstruoimalla sen p -adinen laajennus $a = b_0 + b_1p + b_2p^2 + \dots$ induktiivisesti. Tämä tarkoittaa sitä, että induktioaskeleessa saadaan luvulle a approksiimaatio $a_k = b_0 + \dots + b_kp^k$. Jokainen a_k on polynomien $F(x)$ juuri modulo p^{k+1} eli $F(a_k) \equiv 0 \pmod{p^{k+1}}$ kaikille indekseille k . Kun $k \rightarrow \infty$, niin lopulta saadaan a , joka on vaadittu todellinen polynomien F juuri.

Muotoillaan todistettava väite edellä esitettyä ideaa vastaavaksi:

On olemassa sellainen p -adinen kokonaisluku

$$a_k = b_0 + b_1p + \dots + b_kp^k,$$

missä $b_i \in \{0, 1, \dots, p-1\}$ kaikille indekseille i , että

$$F(a_k) \equiv 0 \pmod{p^{k+1}} \quad \text{ja} \quad a_k \equiv \bar{a}_0 \pmod{p}.$$

Todistetaan nyt väite k :n suhteen.

Kun $k = 0$, niin asetetaan $b_0 = \bar{a}_{0_0}$, missä \bar{a}_{0_0} on luvun \bar{a}_0 ensimmäinen numero. Nyt siis $a_0 = \bar{a}_{0_0}$ ja

$$\begin{aligned} a_0 - (\bar{a}_{0_0} + \bar{a}_{0_1}p + \bar{a}_{0_2}p^2 + \cdots) &= -(\bar{a}_{0_1}p + \bar{a}_{0_2}p^2 + \cdots) \\ &= -p(\bar{a}_{0_1} + \bar{a}_{0_2}p + \cdots). \end{aligned}$$

Siis $p \mid (a_0 - \bar{a}_0)$, joten $a_0 \equiv \bar{a}_0 \pmod{p}$ ja edelleen $F(a_0) \equiv 0 \pmod{p}$. Näin siis induktion perusaskel on kunnossa.

Tehdään sitten induktio-oletus, että väite pätee lukuun $k - 1$ saakka. Osoitetaan, että väite pätee myös luvulle k . Asetetaan sitä varten, että $a_k = a_{k-1} + b_k p^k$, missä b_k on jokin toistaiseksi tuntematon numero, jolle on voimassa $0 \leq b_k < p$.

Huomataan ensin, että polynomi F voidaan esittää seuraavasti summalausekkeena

$$F(x) = \sum_{i=0}^n c_i x^i.$$

Lasketaan nyt $F(a_k)$ seuraavalla tavalla. Sijoitetaan aluksi polynomiin F a_k :n paikalle lauseke $a_{k-1} + b_k p^k$. Lausekkeen $(a_{k-1} + b_k p^k)^i$ ensimmäiset termit kirjoitetaan näkyviin Newtonin binomikaavaa käyttäen. Muista termeistä käytetään nimitystä luvulla p^{k+1} jaolliset termit. Se, että loput termit todella ovat jaollisia luvulla p^{k+1} , on selvää Newtonin binomikaavan nojalla. Siis

$$\begin{aligned} F(a_k) &= F(a_{k-1} + b_k p^k) = \sum_{i=0}^n c_i (a_{k-1} + b_k p^k)^i \\ &= c_0 + \sum_{i=1}^n c_i (a_{k-1}^i + i a_{k-1}^{i-1} b_k p^k + \text{luvulla } p^{k+1} \text{ jaolliset termit}) \\ &= c_0 + c_1 (a_{k-1} + b_k p^k + \text{luvulla } p^{k+1} \text{ jaollisia termejä}) \\ &\quad + c_2 (a_{k-1}^2 + 2a_{k-1} b_k p^k + \text{luvulla } p^{k+1} \text{ jaollisia termejä}) + \cdots \\ &\quad + c_n (a_{k-1}^n + n a_{k-1}^{n-1} b_k p^k + \text{luvulla } p^{k+1} \text{ jaollisia termejä}) \\ &= c_0 + c_1 a_{k-1} + c_2 a_{k-1}^2 + \cdots + c_n a_{k-1}^n + c_1 b_k p^k + 2c_2 a_{k-1} b_k p^k + \cdots \\ &\quad + n c_n a_{k-1}^{n-1} b_k p^k + \text{luvulla } p^{k+1} \text{ jaolliset termit.} \end{aligned}$$

Koska

$$F(a_{k-1}) = c_0 + c_1 a_{k-1} + c_2 a_{k-1}^2 + \cdots + c_n a_{k-1}^n$$

ja

$$F'(a_{k-1}) = c_1 + 2c_2 a_{k-1} + \cdots + n c_n a_{k-1}^{n-1},$$

niin kokonaisuudessaan

$$F(a_k) \equiv F(a_{k-1}) + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}.$$

Induktio-oletuksen nojalla $F(a_{k-1}) \equiv 0 \pmod{p^k}$, joten siis $F(a_{k-1}) = \alpha_k p^k$ jollekin kokonaisluvulle $\alpha_k \in \{0, 1, \dots, p-1\}$. Näin ollen siis

$$\begin{aligned} F(a_k) &\equiv F(a_{k-1}) + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}} \\ &\equiv \alpha_k p^k + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}. \end{aligned}$$

Koska luvun a_k on toteutettava ehto $F(a_k) \equiv 0 \pmod{p^{k+1}}$, on siis ratkaistava kongruenssiyhtälö

$$\alpha_k p^k + b_k p^k F'(a_{k-1}) \equiv 0 \pmod{p^{k+1}}$$

tuntemattoman numeron b_k suhteen. Kun jaetaan puolittain luvulla p^k , niin yhtälö sievenee lauseen 2.7 nojalla muotoon

$$\alpha_k + b_k F'(a_{k-1}) \equiv 0 \pmod{p}.$$

Induktio-oletuksen nojalla $a_{k-1} \equiv \bar{a}_0 \pmod{p}$, joten myös $F'(a_{k-1}) \equiv F'(\bar{a}_0) \pmod{p}$ lauseen 2.6 nojalla. Koska lauseen oletuksen nojalla $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$, niin myös $F'(a_{k-1}) \not\equiv 0 \pmod{p}$. Siis $(F'(a_{k-1}), p) = 1$. Nyt lauseen 2.9 nojalla kongruenssin ratkaisuksi saadaan

$$b_k \equiv \frac{-\alpha_k}{F'(a_{k-1})} \pmod{p}.$$

Nyt

$$\begin{aligned} F(a_k) &\equiv \alpha_k p^k - \frac{\alpha_k}{F'(a_{k-1})} p^k F'(a_{k-1}) \pmod{p^{k+1}} \\ &\equiv 0 \pmod{p^{k+1}}. \end{aligned}$$

Lisäksi huomataan, että koska $a_k = a_{k-1} + b_k p^k$, ja induktio-oletuksen nojalla $a_{k-1} \equiv \bar{a}_0 \pmod{p}$, niin $a_k \equiv \bar{a}_0 \pmod{p}$. Näin väite on todistettu.

Olkoon

$$a = b_0 + b_1 p + b_2 p^2 + \dots$$

Koska

$$\begin{aligned} a - a_k &= b_0 + b_1 p + b_2 p^2 + \dots - (b_0 + b_1 p + b_2 p^2 + \dots + b_k p^k) \\ &= b_{k+1} p^{k+1} + b_{k+2} p^{k+2} + \dots \\ &= p^{k+1} (b_{k+1} + b_{k+2} p + \dots), \end{aligned}$$

niin $a \equiv a_k \pmod{p^{k+1}}$. Näin ollen myös $F(a) \equiv F(a_k) \pmod{p^{k+1}}$ kaikille indekseille k . Koska $F(a_k) \equiv 0 \pmod{p^{k+1}}$, niin tällöin myös $F(a) \equiv 0 \pmod{p^{k+1}}$. Siis välttämättä on oltava $F(a) = 0$, koska $F(a)$ on p -adinen kokonaisluku.

On jo todettu, että $a_k \equiv \bar{a}_0 \pmod{p}$. Kun lasketaan erotus $a - a_k$, huomataan, että $a \equiv a_k \pmod{p}$. Näin ollen siis $a \equiv \bar{a}_0 \pmod{p}$.

Koska p -adinen laajennus on yksikäsitteinen, niin luku a on yksikäsitteinen. Näin Henselin lemma on todistettu. \square

Huomautus. Lauseen 4.9 ehto $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$ on olennainen. Kuitenkin lauseesta 4.9 on olemassa kirjallisuudessa erilaisia versioita. Näistä käytetään myös nimitystä Henselin lemma.

Huomautus. Lauseen 4.9 todistuksen tekniikka vastaa analyysin kurseilla opittua Newtonin menetelmää etsittäessä reaalisia juuria reaalilukukertoimille polynomille.

Apulause 4.5. (*Ks. [6, s. 25]*). Jokaisella p -adisista kokonaisluvuista koostuvalla päättymättömällä lukujonolla on suppeneva osajono.

Todistus. Sivuuetaan. Katso [6, s. 25–26]. □

Seuraava lause yhdistää p -adiset luvut ja kongruenssit.

Lause 4.10. Kokonaislukukertoimisella polynomilla F on juuri $a \in \mathbb{Z}_p$, jos ja vain jos sillä on kokonaislukujuuri modulo p^k aina, kun $k \geq 1$.

Todistus. Olkoon $F(x)$ polynomi, jonka kertoimet ovat kokonaislukuja. Oletetaan ensin, että polynomilla F on juuri $a \in \mathbb{Z}_p$. Siis luvulle a pätee

$$F(a) = 0.$$

Nyt lauseen 4.4 nojalla on olemassa jono (a_k) , missä a_k on kokonaisluku ja $k = 1, 2, \dots$. Edelleen jokainen jonon termi on muotoa

$$a_k = b_0 + b_1p + b_2p^2 + \dots + b_{k-1}p^{k-1}.$$

Lisäksi tiedetään, että

$$a \equiv a_k \pmod{p^k}$$

sen perusteella, että $|a - a_k|_p \leq p^{-k}$. Nyt lauseen 2.6 nojalla

$$F(a_k) \equiv F(a) \pmod{p^k}.$$

Koska oletuksen nojalla $F(a) = 0$, niin selvästi siis edelleen

$$F(a_k) \equiv 0 \pmod{p^k}.$$

Siis polynomilla F on kokonaislukujuuri modulo p^k kaikille luvuille $k \geq 1$.

Oletetaan sitten, että polynomilla F on kokonaislukujuuri modulo p^k kaikille $k \geq 1$ eli että kongruenssilla

$$F(a_k) \equiv 0 \pmod{p^k}$$

on kokonaislukuratkaisu a_k kaikille $k \geq 1$. Nyt apulauseen 4.5 mukaan jonolla (a_k) on suppeneva osajono (a_{k_i}) . Siis osajonolla on raja-arvo. Olkoon se $\lim_{i \rightarrow \infty} a_{k_i} = a$. Tarkoituksena on nyt osoittaa, että $F(a) = 0$. Koska polynomit ovat jatkuvia funktioita, niin siitä, että $\lim_{i \rightarrow \infty} a_{k_i} = a$ seuraa, että

$$F(a) = F(\lim_{i \rightarrow \infty} a_{k_i}) = \lim_{i \rightarrow \infty} F(a_{k_i}).$$

Koska oletuksen nojalla

$$F(a_{k_i}) \equiv 0 \pmod{p^{k_i}},$$

niin $\lim_{i \rightarrow \infty} F(a_{k_i}) = 0$. Siis tällöin myös $F(a) = 0$. \square

Seuraus 4.1. Jos kokonaislukukertoimisella polynomilla ei ole juuria modulo p , niin sillä ei ole juuria renkaassa \mathbb{Z}_p .

Määritelmä 4.6. Olkoon $a \in \mathbb{Z}$ sellainen luku, että $(a, p) = 1$. Tällöin luku a on *neliönjäännös modulo p* , jos kongruenssilla

$$x^2 \equiv a \pmod{p}$$

on ratkaisu joukossa $\{1, 2, \dots, p-1\}$. Muuten a on *neliönepäjäännös modulo p* .

Lause 4.11. Olkoon $a \in \mathbb{Z}$ sellainen luku, että $(a, p) = 1$. Tällöin luvun a neliöjuuri on renkaassa \mathbb{Z}_p , missä $p \neq 2$, jos ja vain jos a on neliönjäännös modulo p .

Todistus. Olkoon $P(x) = x^2 - a$. Tällöin $P'(x) = 2x$. Oletetaan ensin, että a on neliönjäännös modulo p . Siis kongruenssilla

$$a \equiv a_0^2 \pmod{p}$$

on ratkaisu $a_0 \in \{1, 2, \dots, p-1\}$. Tällöin

$$P(a_0) = a_0^2 - a \equiv a - a \equiv 0 \pmod{p}.$$

Koska $a_0 \in \{1, 2, \dots, p-1\}$, niin selvästi $(a_0, p) = 1$. Siis $p \nmid a_0$, joten

$$P'(a_0) = 2a_0 \not\equiv 0 \pmod{p}.$$

Nyt Henselin lemmän nojalla on olemassa sellainen $b \in \mathbb{Z}_p$, että

$$P(b) = b^2 - a = 0.$$

Siis luvun a neliöjuuri on renkaassa \mathbb{Z}_p .

Osoitetaan lauseen toinen suunta oikeaksi kontrapositioperiaatteen nojalla. Jos a on neliönepäjäännös modulo p , niin seurauksen 4.1 nojalla luvun a neliöjuuri ei ole renkaassa \mathbb{Z}_p . \square

Havainnollistetaan asiaa esimerkillä.

Esimerkki 4.4. Tutkitaan, onko voimassa $\sqrt{-1} \in \mathbb{Z}_5$.

Koska $2^2 = 4 \equiv -1 \pmod{5}$, niin -1 on neliönjäännös modulo 5. Siis lauseen 4.11 nojalla neliöjuuri $\sqrt{-1} \in \mathbb{Z}_5$.

Tutkitaan, onko voimassa $\sqrt{-1} \in \mathbb{Z}_3$.

Koska sekä $1^2 = 1 \not\equiv -1 \pmod{3}$ että $2^2 = 4 \not\equiv -1 \pmod{3}$, niin -1 on neliönepäjäännös modulo 3. Siis $\sqrt{-1} \notin \mathbb{Z}_3$ lauseen 4.11 nojalla.

Lähteessä [6, s. 38] esitettyyn kysymykseen, onko $\sqrt{p} \in \mathbb{Z}_p$ tekijä vastaa, että kyseiseen tapaukseen ei voida soveltaa lausetta 4.11. Nimittäin lauseen ehto $(a, p) = 1$ ei toteudu tässä tapauksessa $a = p$.

5 Teichmüllerin laajennus

Tässä luvussa perehdytään hiukan kunnan \mathbb{Q}_p topologiaan. Päämääränä on saada p -adiselle kokonaisluvulle p -adisen laajennuksen rinnalle toinen esitysmuoto, jota kutsutaan Teichmüllerin laajennukseksi. Aloitetaan määrittelemällä muutamia topologian peruskäsitteitä.

Olkoon $\alpha \in \mathbb{Q}_p$ ja $\delta > 0$ reaalityyppinen luku.

Määritelmä 5.1. *Avointa palloa*, jonka *keskipiste* on α ja *säde* on δ , merkitään

$$D(\alpha; \delta) = \{\gamma \in \mathbb{Q}_p : |\gamma - \alpha|_p < \delta\}.$$

Suljettua palloa, jonka *keskipiste* on α ja *säde* on δ , merkitään

$$\overline{D(\alpha; \delta)} = \{\gamma \in \mathbb{Q}_p : |\gamma - \alpha|_p \leq \delta\}.$$

Selvästi on voimassa, että $D(\alpha; \delta) \subseteq \overline{D(\alpha; \delta)}$. Seuraava tulos poikkeaa reaalianalyysistä.

Lause 5.1. *Olkoon $\beta \in D(\alpha; \delta)$. Silloin*

$$D(\beta; \delta) = D(\alpha; \delta).$$

Vastaavasti, jos $\beta' \in \overline{D(\alpha; \delta)}$, niin

$$\overline{D(\beta'; \delta)} = \overline{D(\alpha; \delta)}.$$

Siis jokainen pallon $D(\alpha; \delta)$ alkio on kyseisen pallon keskipiste. Sama tulos on voimassa myös suljetulle pallolle.

Todistus. (Vrt. [1, s. 33]).

Oletetaan, että $\beta \in D(\alpha; \delta)$ ja $\gamma \in D(\alpha; \delta)$. Nyt normin ominaisuuden (N4) ja oletuksen perusteella saadaan, että

$$\begin{aligned} |\gamma - \beta|_p &= |(\gamma - \alpha) + (\alpha - \beta)|_p \\ &\leq \max\{|\gamma - \alpha|_p, |\alpha - \beta|_p\} \\ &< \delta. \end{aligned}$$

On siis osoitettu, että $D(\alpha; \delta) \subseteq D(\beta; \delta)$. Vastaavasti voidaan osoittaa, että $D(\beta; \delta) \subseteq D(\alpha; \delta)$. Siis $D(\beta; \delta) = D(\alpha; \delta)$. Samoin nähdään suljetun pallon tapaus. \square

Olkoon nyt $X \subseteq \mathbb{Q}_p$. Esimerkkinä tällaisesta joukosta X on p -adisten kokonaislukujen joukko \mathbb{Z}_p . Määritellään avoimet ja suljetut pallot joukossa X .

Määritelmä 5.2. Joukko

$$D_X(\alpha; \delta) = D(\alpha; \delta) \cap X$$

on *avoin pallo* joukossa X . Sen *keskipiste* on α ja *säde* on δ . Vastaavasti joukko

$$\overline{D_X(\alpha; \delta)} = \overline{D(\alpha; \delta)} \cap X$$

on *suljettu pallo* joukossa X . Sen *keskipiste* on α ja *säde* on δ .

Määritellään seuraavaksi jatkuva funktio. Olkoon $f : X \rightarrow \mathbb{Q}_p$ funktio.

Määritelmä 5.3. Funktio f on *jatkuva pisteessä* $\alpha \in X$, jos jokaista positiivista lukua ε kohti on olemassa sellainen positiivinen luku δ , että

$$\gamma \in D_X(\alpha; \delta) \Rightarrow f(\gamma) \in D(f(\alpha); \varepsilon).$$

Jos funktio f on jatkuva jokaisessa joukon X pisteessä, niin f on *jatkuva joukossa* X .

Huomautus. Kuten reaalianalyysissäkin, jatkuvien funktioiden summat ja tulot ovat jatkuvia.

Seuraava tulos on voimassa reaalianalyysissä.

Lause 5.2. Olkoon $f : (a, b) \rightarrow \mathbb{R}$ jatkuva funktio. Jos jokaista välin (a, b) pistettä x kohti on olemassa sellainen positiivinen luku t , että $(x - t, x + t) \subseteq (a, b)$ ja f on vakio välillä $(x - t, x + t)$ eli f on paikallisesti vakio, niin f on vakio välillä (a, b) .

Määritelmä 5.4. Olkoon $X \subseteq \mathbb{Q}_p$ ja $f : X \rightarrow \mathbb{Q}_p$ funktio. Funktio f on *paikallisesti vakio* joukossa X , jos jokaista joukon X alkiota α kohti on olemassa sellainen positiivinen reaaliluku δ_α , että f on vakio joukossa $D_X(\alpha; \delta_\alpha)$.

Käsitellään seuraavaksi esimerkki funktioista, jotka ovat paikallisesti vakioita joukossa \mathbb{Q}_p .

Esimerkki 5.1. (Vrt. [1, esim. 4.9, s. 35]). Olkoon nyt $X = \mathbb{Z}_p$ ja $\alpha \in \mathbb{Z}_p$. Tiedetään, että luvulle α on olemassa p -adinen laajennus

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots,$$

missä kertoimet $\alpha_n \in \mathbb{Z}$ ja $0 \leq \alpha_n \leq p - 1$.

Olkoon $f_n : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ funktio, jolle $f_n(\alpha) = \alpha_n$. Tällainen funktio on määritelty jokaiselle indeksille $n \geq 0$. On helposti todettavissa, että nämä funktiot ovat paikallisesti vakioita. Nimittäin, jos luku α korvataan jollakin sellaisella luvulla $\beta \in \mathbb{Z}_p$, jolle on voimassa, että $|\beta - \alpha|_p < 1/p^n$, niin funktio f_n pysyy muuttumattomana. Tämä pätee siis jokaiselle indeksille n ja perustuu siihen, että tällöin luvut α ja β ovat välttämättä yhtäsuuret. Nyt määritelmän 5.4 nojalla kyseiset funktiot f_n ovat paikallisesti vakioita.

Lause 5.3. *Olkoon $f : X \rightarrow \mathbb{Q}_p$ funktio, joka on paikallisesti vakio joukossa X . Silloin f on jatkuva joukossa X .*

Todistus. Sivutetaan. Ks. [1, s. 35]. □

Esimerkki 5.2. (Vrt. [1, esim. 4.11, s. 35]). Olkoon $Y = D(0; 1) \subseteq \mathbb{Z}_p$. Määritellään nyt joukon Y karakteristinen funktio $\chi_Y : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ seuraavasti

$$\chi_Y(\alpha) = \begin{cases} 1, & \text{kun } \alpha \in Y, \\ 0, & \text{kun } \alpha \notin Y. \end{cases}$$

Selvästi funktio χ_Y on vakio jokaisessa joukossa $D(k; 1)$, missä $0 \leq k \leq p-1$. Näin ollen määritelmän 5.4 nojalla funktio χ_Y on paikallisesti vakio joukossa \mathbb{Z}_p .

Määritellään seuraavaksi *Teichmüllerin funktiot*. Tehdään tämä lauseessa 5.4. Lauseen todistusta varten tarvitaan seuraava aputuloks.

Apulause 5.1. (Ks. [1, s. 29]). *Jono (α_n) on Cauchyn jono kunnassa \mathbb{Q}_p , jos ja vain jos jono $(\alpha_{n+1} - \alpha_n)$ on nollajono.*

Lause 5.4. *On olemassa yksikäsitteinen paikallisesti vakioiden, ja siten myös jatkuvien, funktioiden $\omega_n : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ jono, joka toteuttaa seuraavat ominaisuudet.*

$$(T1) \quad \omega_n(\alpha)^p = \omega_n(\alpha), \quad \text{kun } n \geq 0.$$

$$(T2) \quad \alpha = \sum_{n=0}^{\infty} \omega_n(\alpha)p^n.$$

Todistus. (Vrt. [1, s. 36-37]).

Määritellään aluksi *Teichmüllerin karakteri* $\omega : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$. Tämä karakteri tulee olemaan funktio ω_0 . Olkoon $\alpha \in \mathbb{Z}_p$. Nyt jono (α^{p^n}) on jono p -adisia kokonaislukuja. Osoitetaan, että kyseisellä jonolla on raja-arvo. Tehdään tämä osoittamalla, että jono on Cauchyn jono. Koska \mathbb{Q}_p on täydellinen p -adisen normin suhteen, niin jokaisella Cauchyn jonolla on raja-arvo.

Edellä opitun perusteella tiedetään, että luvulla α on p -adinen laajennus

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots,$$

missä $\alpha_k \in \mathbb{Z}$ ja $0 \leq \alpha_k \leq p-1$. Erityisesti on voimassa, että

$$|\alpha - \alpha_0|_p < 1.$$

Fermat'n pienen lauseen nojalla $\alpha_0^p \equiv \alpha_0 \pmod{p}$, joten lauseen 3.2 nojalla $|\alpha_0^p - \alpha_0|_p < 1$. Käytetään nyt tietoa $\left| \alpha^k \alpha_0^{p-1-k} \right|_p \leq 1$, normin ominaisuutta

(N2) ja kolmioepäyhtälöä eli normin ominaisuutta (N3). Saadaan pääteltyä, että

$$\begin{aligned} |\alpha^p - \alpha_0^p|_p &= |(\alpha - \alpha_0)(\alpha^{p-1} + \alpha^{p-2}\alpha_0 + \cdots + \alpha_0^{p-1})|_p \\ &\leq |\alpha - \alpha_0|_p \\ &< 1. \end{aligned}$$

Nyt kokonaisuutena saadaan, että

$$\begin{aligned} |\alpha^p - \alpha|_p &= |(\alpha^p - \alpha_0^p) + (\alpha_0^p - \alpha_0) + (\alpha_0 - \alpha)|_p \\ &\leq \max\{|\alpha^p - \alpha_0^p|_p, |\alpha_0^p - \alpha_0|_p, |\alpha_0 - \alpha|_p\} \\ &< 1. \end{aligned}$$

Osoitetaan seuraavaksi induktiolla, että jokaiselle luvulle $n \geq 0$ on voimassa, että

$$(5.1) \quad \left| \alpha^{p^{n+1}} - \alpha^{p^n} \right|_p < \frac{1}{p^n}.$$

Edellä juuri osoitettiin, että $|\alpha^p - \alpha|_p < 1$. Siis kaava (5.1) toteutuu, kun $n = 0$. Tehdään nyt induktio-oletus, että kaava (5.1) on voimassa luvulle $n \geq 0$. Todistetaan, että kaava on voimassa myös luvulle $n + 1$. Koska induktio-oletuksen nojalla $\left| \alpha^{p^{n+1}} - \alpha^{p^n} \right|_p < \frac{1}{p^n}$, voidaan kirjoittaa

$$\alpha^{p^{n+1}} = \alpha^{p^n} + \beta,$$

missä $|\beta|_p < 1/p^n$. Nyt korottamalla potenssiin p ja hyödyntämällä Newtonin binomikaavaa saadaan, että

$$\begin{aligned} \alpha^{p^{n+2}} &= (\alpha^{p^n} + \beta)^p \\ &= \alpha^{p^{n+1}} + p\alpha^{p^n(p-1)}\beta + \cdots + \binom{p}{k}\alpha^{p^nk}\beta^{p-k} + \cdots + \beta^p, \end{aligned}$$

missä jokaisen termin p -adinen normi on pienempi kuin $1/p^{n+1}$ ensimmäistä termiä lukuun ottamatta. Nyt siis normin ominaisuuden (N4) nojalla saadaan, että

$$\left| \alpha^{p^{n+2}} - \alpha^{p^{n+1}} \right|_p < \frac{1}{p^{n+1}}.$$

Näin on todistettu, että kaava (5.1) on voimassa jokaiselle luvulle $n \geq 0$. Nyt selvästi jono $\alpha^{p^{n+1}} - \alpha^{p^n}$ on nollajono. Siis apulauseen 5.1 nojalla jono (α^{p^n}) on Cauchyn jono. Näin ollen kyseisellä jonolla on raja-arvo.

Määritellään nyt *Teichmüllerin karakteri*,

$$\omega : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p; \quad \omega(\alpha) = \lim_{n \rightarrow \infty} {}^{(p)}\alpha^{p^n}.$$

Tälle funktiolle on voimassa

$$|\alpha - \omega(\alpha)|_p < 1, \quad \omega(\alpha)^p = \omega(\alpha).$$

Epäyhtälö $|\alpha - \omega(\alpha)|_p < 1$ seuraa kaavasta (5.1). Yhtälö $\omega(\alpha)^p = \omega(\alpha)$ seuraa siitä, että

$$\begin{aligned} \left(\lim_{n \rightarrow \infty} {}^{(p)}\alpha^{p^n} \right)^p &= \lim_{n \rightarrow \infty} {}^{(p)}(\alpha^{p^n})^p \\ &= \lim_{n \rightarrow \infty} {}^{(p)}(\alpha^{p^{n+1}}). \end{aligned}$$

Asetetaan nyt, että $\omega_0(\alpha) = \omega(\alpha)$. Muut *Teichmüllerin funktiot* saadaan rekursiolla seuraavasti

$$\omega_{n+1}(\alpha) = \omega \left(\frac{\alpha - (\omega_0(\alpha) + \omega_1(\alpha)p + \cdots + \omega_n(\alpha)p^n)}{p^{n+1}} \right).$$

Päätetään lauseen 5.4 todistus tähän. □

Määritelmä 5.5. Olkoon $\alpha \in \mathbb{Z}_p$. Laajennus

$$\alpha = \omega_0(\alpha) + \omega_1(\alpha)p + \cdots + \omega_n(\alpha)p^n + \cdots$$

on luvun α *Teichmüllerin laajennus* ja kertoimet $\omega_n(\alpha)$ ovat luvun α *Teichmüllerin numerot*.

Teichmüllerin laajennusta käytetään usein sen sijaan, että käytettäisiin aiemmin esiteltyä p -adista laajennusta. Yksi syy tähän on funktion ω multiplikatiivisuus. Seuraavassa lauseessa käydään läpi funktion ω ominaisuudet.

Lause 5.5. *Funktio $\omega : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ on paikallisesti vakio ja toteuttaa ehdot*

$$\omega(\alpha\beta) = \omega(\alpha)\omega(\beta),$$

$$|\omega(\alpha + \beta) - \omega(\alpha) - \omega(\beta)|_p < 1.$$

Funktion ω kuvajoukko muodostuu renkaan \mathbb{Z}_p alkioista. Tarkemmin sanottuna funktion ω kuvajoukko koostuu polynomien $X^p - X$ erisuurista juurista, joita on p kappaletta.

Todistus. Sivuuutetaan. Ks. [1, s. 37]. □

Käydään läpi esimerkki Teichmüllerin laajennuksesta.

Esimerkki 5.3. (Vrt. [1, esim. 4.15, s. 38]). Olkoon $p = 3$. Polynomien $X^3 - X$ juuret ovat 0, 1 ja -1 .

Etsitään luvulle $\alpha = 1/5$ Teichmüllerin laajennus. Käytetään tässä lausetta 5.4. Koska $5 \equiv -1 \pmod{3}$, niin $|5 - (-1)|_3 \leq \frac{1}{3}$. Siis varmasti on voimassa, että

$$|5 - (-1)|_3 < 1.$$

Nyt siis lauseen 5.4 nojalla $\omega(5) = -1$. Koska selvästi $\omega(1) = 1$ ja funktion ω multiplikatiivisuuden nojalla

$$\omega(5)\omega\left(\frac{1}{5}\right) = \omega(1),$$

on nyt oltava, että $\omega(1/5) = -1$. Asetetaan siis $\omega_0(1/5) = \omega(1/5) = -1$.

Loput Teichmüllerin numerot saadaan rekursiokaavalla

$$\omega_{n+1}(\alpha) = \omega\left(\frac{\alpha - (\omega_0(\alpha) + \omega_1(\alpha)p + \dots + \omega_n(\alpha)p^n)}{p^{n+1}}\right).$$

Nyt siis

$$\omega_1(1/5) = \omega\left(\frac{1/5 - \omega_0(1/5)}{3}\right).$$

Kun sijoitetaan kaavaan $\omega_0(1/5) = -1$, saadaan, että

$$\omega_1(1/5) = \omega\left(\frac{1/5 - (-1)}{3}\right).$$

Tästä edelleen laskemalla saadaan, että

$$\omega_1(1/5) = \omega(2/5).$$

Koska $2 \equiv -1 \pmod{3}$ ja $5 \equiv -1 \pmod{3}$, niin lopulta

$$\omega_1(1/5) = \omega(1) = 1.$$

Ratkaistaan seuraavaksi $\omega_2(1/5)$ samaa rekursiokaavaa käyttäen. Nyt

$$\omega_2(1/5) = \omega\left(\frac{1/5 - \omega_0(1/5) - \omega_1(1/5) \cdot 3}{9}\right).$$

Sijoitetaan yhtälöön $\omega_0(1/5) = -1$ ja $\omega_1(1/5) = 1$. Saadaan siis, että

$$\omega_2(1/5) = \omega\left(\frac{1/5 - (-1) - 3}{9}\right).$$

Laskemalla saadaan

$$\omega_2(1/5) = \omega(-1/5).$$

Nyt nähdään helposti, että

$$\omega_2(1/5) = \omega(-1/5) = 1.$$

Nyt on saatu luvulle $\alpha = 1/5$ Teichmüllerin laajennus

$$\frac{1}{5} = -1 + 1 \cdot 3 + 1 \cdot 3^2 + \dots$$

Teichmüllerin numeroita voitaisiin laskea lisää samaan tapaan kuin edellä.

Viitteet

- [1] Baker, A. J. , *An Introduction to p -adic Numbers and p -adic Analysis*, Department of Mathematics, University of Glasgow, Scotland, 2007.
URL <http://www.maths.gla.ac.uk/~ajb>.
- [2] Gouvêa, Fernando Q. , *p -adic Numbers: An Introduction*, 2. painos, Berlin: Springer, 1997.
- [3] Haukkanen, Pentti, *Algebra I*, Opetusmoniste, Tampereen yliopisto.
URL <http://mtl.uta.fi/Opetus/Algebra/algI04.pdf>
- [4] Haukkanen, Pentti, *Algebra II*, Opetusmoniste, Tampereen yliopisto.
URL <http://mtl.uta.fi/Opetus/Algebra/algII04.pdf>
- [5] Haukkanen, Pentti, *Lukuteoriaa*, Opetusmoniste, Tampereen yliopisto.
URL <http://mtl.uta.fi/Opetus/Algebra/Lukuteoria/lukuteoria.pdf>
- [6] Katok, Svetlana, *p -adic Analysis Compared with Real*, Providence (R.I.): American Mathematical Society, 2007.
- [7] Koblitz, Neal, *p -adic Numbers, p -adic Analysis, and Zeta-Functions*, 2. painos, New York: Springer, 1984.
- [8] Metsänkylä, Tauno, *Lukujen uusi maailma: p -adiset luvut*, Matematiikkalehti Solmu, 2008.
URL <http://solmu.math.helsinki.fi/2008/3/maailma.pdf>.