P-adiset luvut ja avaruuksien $\mathbb{Z}_p$ euklidiset mallinnukset

Eemu Tuominen

Pro Gradu -tutkielma

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2019

Tiivistelmä

Eemu Tuominen, *P-adiset luvut ja avaruuksien $\mathbb{Z}_p$ euklidiset mallinnukset* (engl. *P-adic numbers and euclidean models of $\mathbb{Z}_p$*), matematiikan pro gradu -tutkielma, 55 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, maaliskuu 2019.

Tutkielmassa lähdetään liikkeelle metristen avaruuksien täydellistämisestä täydellisiksi metrisiksi avaruuksiksi, missä Cauchy-jonoilla on merkittävä rooli. Täydellistymisprosessista käydään läpi esimerkkinä rationaalilukujen täydellistäminen reaaliluvuiksi euklidisella normilla. Myöhemmin tutkitaan rationaalilukujen täydellistämistä toisenlaisella normilla, josta tulee hyvin erilainen kunta. Kappaleen 2 lopuksi käsitellään lause, jonka avulla saadaan muodostettua täydellinen metrinen avaruus kätevästi tietyillä ehdoilla. Tämän jälkeen tutkitaan kunnan normin erilaisia tuloksia ja määritellään jonon ominaisuuksia. Lisäksi perehdytään vahvaan kolmioepäyhtälöön, jonka toteuttavaa normia sanotaan epäarkhimediseksi. Seuraavaksi on järkevää yhdistää kahden aiemman kappaleen tuloksia ja tutkia normilla varustettujen kuntien täydellistämistä.

Näiden tulosten nojalla Kappaleessa 5 voidaan siirtyä pääasiaan eli p-adisiin lukuihin. P-adisia lukuja varten määritellään p-adinen normi, joka riippuu alkuluvusta p. P-adisten lukujen kunta $\mathbb{Q}_p$ saadaan täydellistämisprosessilla rationaaliluvuista p-adisella normilla. P-adisten lukujen joukosta saadaan myös toinen mielenkiintoinen joukko, p-adisten kokonaislukujen joukko $\mathbb{Z}_p$. Kun ollaan päästy p-adisiin lukuihin, niin tutkitaan kuinka niiden aritmeettiset laskutoimitukset toimivat. Ne eroavat jossain määrin perinteisistä reaalilukujen laskutoimituksista, mutta jossain mielessä ne ovat jopa helpompia laskea. Tämän jälkeen tutkitaan rationaalilukujen ja p-adisten lukujen yhteyttä. Tarkoituksena on myös selvittää, voidaanko p-adisen luvun laajennuksesta päätellä minkälaista lukua se esittää. Seuraavaksi tutkitaan kongruenssiin liittyviä tuloksia avaruudessa $\mathbb{Q}_p$. Keskeisin asia kongruenssiin liittyvissä tuloksissa on Henselin Lemma, jolla voidaan ratkaista polynomin juuria, kun kertoimet ovat p-adisia lukuja. Tämä on periaatteessa p-adinen versio Newtonin menetelmästä, jolla etsitään reaalikertoimisen polynomin juuria.

Kappaleessa 9 tutkitaan topologisia perusominaisuuksia. Tästä päästään avaruuden $\mathbb{Q}_p$ palloihin, jotka käyttäytyvät hyvin eri lailla kuin avaruuden $\mathbb{R}$ pallot. Seuraavaksi tutkitaan Cantorin joukkoa eli "Cantorin kolmasosajoukkoa" ja sen ominaisuuksia. Lisäksi kappaleessa kerrataan metristen avaruuksien kuvauksiin liittyviä ominaisuuksia. Näiden avulla luodaan yhteyksiä Cantorin joukkojen ja p-adisten kokonaislukujen joukon $\mathbb{Z}_p$ välille. Viimeisessä kappaleessa tutkitaan avaruuden $\mathbb{Z}_p$ euklidisia mallinnuksia. Tätä varten muodostetaan kuvaus joukolta $\mathbb{Z}_p$ välille $[0, 1]$. Joukkojen $\mathbb{Z}_p$ kuvauksilla eri alkuluvun p arvoilla on jotain yhteistä: ne ovat kaikki fraktaaleja.

Sisältö

1. Johdanto 2
2. Rationaalilukujen täydellistäminen reaaliluvuiksi 3
3. Normilla varustetut kunnat 8
4. Normilla varustetun kunnan täydellistäminen 16
5. P-adisten lukujen kunta $\mathbb{Q}_p$ 22
6. Joukon $\mathbb{Q}_p$ aritmeettiset laskutoimitukset 28
7. Rationaaliluvun p-adinen laajennus 31
8. Henselin Lemma ja kongruensseja 34
9. Topologisia perusominaisuuksia 38
10. Cantorin joukot 43
11. Avaruuden $\mathbb{Z}_p$ euklidiset mallinnukset 49

Viitteet 55

1. Johdanto

Tutkielma perustuu suurimmaksi osin Katokin kirjaan *P-adic analysis compared with real* [3], joka on kirjoitettu tarkoituksenaan antaa perehdytys p-adisiin lukuihin lukuteorian, topologian ja analyysin näkökulmista. Tässä tutkielmassa keskitytään lukuteorian ja topologian näkökulmiin.

Tutkielman aiheeseen päädyttiin ohjaajan ehdotuksen perusteella. Lisäksi p-adiset luvut olivat ennestään vieras aihe, mikä herätti kiinnostusta. Tutkielman toiseen pääaiheeseen, avaruuden $\mathbb{Z}_p$ euklidisiin mallinnuksiin, päädyttiin mallinnuksien kauniiden ja symmetristen rakenteiden vuoksi. Analyysin käsitteleminen tutkielmassa olisi myös mielekästä ja se täydentäisi p-adisten lukujen ymmärrystä entisestään. Tämä kuitenkin karsiutui pois tutkielman laajuutta arvioitaessa.

Ensimmäinen henkilö, joka tutki p-adisia lukuja oli Kurt Hensel (1861-1941) 1800-luvun loppupuolella. Vaikka p-adisten lukujen olemassaolosta on tiedetty jo yli sata vuotta, niin Jyväskylän yliopiston matematiikan peruskursseilla niitä ei käsitellä. Niiden tutkiminen on kuitenkin mielenkiintoista, sillä lähestymistapoja on monia: *lukuteoria*, jossa esimerkiksi p-adisten kokonaislukujen p-adinen normi on yksi tai alle yksi, *geometria*, jossa esimerkiksi havaitaan, että p-adisten lukujen kunnassa $\mathbb{Q}_p$ ympyrän jokainen piste on sen keskipiste, *topologia*, jossa huomataan, että avaruuden $\mathbb{Z}_p$ euklidiset mallinnukset ovat fraktaaleja (kuten mahdollisesti tuttu Sierpinskin kolmio), *analyysi*, josta voi lukea enemmän Katokin kirjasta ([3, s.75-134]) ja niin edelleen.

Tutkielma aloitetaan käsittelemällä täydellistämistä. Tämä on tärkeässä roolissa, sillä riippuen normin valinnasta täydellistäminen voi tuottaa hyvin erilaisia metrisiä avaruuksia. Tämän tutkielman tapauksessa päästään vertailemaan rationaalilukujen kahta täydellistystä: reaalilukujen kuntaa $\mathbb{R}$ ja p-adisten lukujen kuntaa $\mathbb{Q}_p$. Nämä kunnat saadaan muodostettua, kun valitaan joko euklidinen normi tai p-adinen normi vastaavassa järjestyksessä. Tutkielman edetessä lukijalle voi herätä kysymys: kuinka p-adisten lukujen joukko rakentuu? Tästä alkaa muodostua jonkinlainen käsitys, kun tutkitaan p-adisten lukujen ominaisuuksia. Tätä päästään havainnoimaan euklidisten mallinnusten kautta viimeisessä kappaleessa.

Kappaleissa 2 - 4 käsitellään täydellistysprosessia metristen avaruuksien ja normilla varustettujen kuntien tapauksessa, sekä näihin liittyviä perusominaisuuksia. Näiden kappaleiden avulla luodaan perusta, jonka avulla rakennetaan p-adisten lukujen kunta $\mathbb{Q}_p$ ja siten p-adiset luvut. Kappaleissa 5 - 6 määritellään p-adinen normi, jonka avulla muodostetaan p-adisten lukujen kunta $\mathbb{Q}_p$ ja tutkitaan p-adisten lukujen laskutoimituksia. Kappaleessa 7 tutkitaan rationaalilukujen ja p-adisten lukujen yhteyttä ja näiden keskinäistä muunnosta toisekseen. Kappaleessa 8 tutkitaan kongruenssiyhtälöitä ja Henselin Lemmaa, jolla voidaan ratkaista yhtälöiden juuria, kun kertoimet ovat p-adisia kokonaislukuja. Kappaleissa 9 - 10 tutkitaan topologisia perusominaisuuksia ja Cantorin joukon yhteyttä p-adisten kokonaislukujen kuntaan $\mathbb{Z}_p$, sekä jatkuvien kuvausten yleisimpiä ominaisuuksia. Viimeisessä kappaleessa 11 tutkitaan avaruuden $\mathbb{Z}_p$ euklidisia mallinnuksia ja mallinnukseen valitun kuvauksen ominaisuuksia.

Tästä edetään tarkoituksena muodostaa p-adisten lukujen kunta $\mathbb{Q}_p$ ja tutkia p-adisia lukuja ja niiden ominaisuuksia. Tarkoituksena ei ole, että lukija tietäisi kaiken p-adisista luvuista, vaan herättää kiinnostusta aiheeseen. Tutkielmaa luettaessa on hyvä miettiä: miten p-adiset luvut eroavat reaaliluvuista ja miten p-adinen normi eroaa tutummasta euklidisesta normista.

2. Rationaalilukujen täydellistäminen reaaliluvuiksi

Rationaalilukujen joukko $\mathbb{Q}$ voidaan täydellistää reaalilukujen joukoksi $\mathbb{R}$. Tutkitaan seuraavaksi kuinka jokainen metrinen avaruus voidaan täydellistää. Olkoon metrinen avaruus M, jossa on metriikka d. Olkoon d kuvaus

$$d : M \times M \longrightarrow \mathbb{R},$$

joka on määritelty pisteparille epätyhjistä joukoista M reaalilukujen joukolle $\mathbb{R}$. Tämän sanotaan olevan *metriikka*, jos seuraavat ominaisuudet pätevät:

$$\begin{aligned}
&(1)\, d(x,y) \geq 0;\ d(x,y) = 0,\ \textit{jos ja vain jos } x = y;\\
&(2)\, d(x,y) = d(y,x)\ \textit{kaikilla } x, y \in M;\\
&(3)\, d(x,y) \leq d(x,z) + d(z,y)\ \textit{kaikilla } x, y, z \in M.
\end{aligned}$$

Kuvausta d sanotaan myös *etäisyysfunktioksi*, sillä $d(x,y)$ on pisteiden välinen etäisyys.

Metrisen avaruuden M jonoa r_n sanotaan *Cauchy-jonoksi*, jos kaikilla $\varepsilon > 0$ on olemassa positiivinen kokonaisluku N siten, että $d(r_n, r_m) < \varepsilon$ aina, kun $n, m > N$. Jos jokainen Cauchy-jono suppenee avaruudessa M, niin avaruus M on *täydellinen metrinen avaruus.*

Lause 2.1. *Jokainen metrinen avaruus M voidaan täydellistää. Toisin sanoen on olemassa metrinen avaruus $(\hat{M}, D)$ siten, että*

(1) *$\hat{M}$ on täydellinen metriikan D suhteen;*
(2) *$\hat{M}$ sisältää osajoukon $\hat{M}_0$ siten, että joukot M ja $\hat{M}_0$ ovat isometrisiä keskenään;*
(3) *$\hat{M}_0$ on tiheä avaruudessa $\hat{M}$ (Jokainen avaruuden $\hat{M}$ piste on avaruuden $\hat{M}_0$ Cauchy-jonon raja-arvo).*

Todistus. Olkoon $\{M\}$ kaikkien avaruuden M Cauchy-jonojen kokoelma, jotka suppenevat tai eivät suppene, ja tehdään tästä metrinen avaruus. Tässä tarvitaan ekvivalenssirelaatiota joukolla $\{M\}$. Kahden Cauchy-jonon a_n ja b_n sanotaan olevan ekvivalentteja, jos $d(a_n, b_n) \to 0$; tällöin merkitään $\{a_n\} \sim \{b_n\}$. Olkoon $\hat{M}$ joukko ekvivalenssiluokkia siten, että $\hat{M} = \{M\}/\sim$. Olkoon D metriikka kahdelle Cauchy-jonojen ekvivalenssiluokalle $A = (\{a_n\})$ ja $B = (\{b_n\})$ seuraava

$$D(A,B) = \lim_{n\to\infty} d(a_n, b_n). \tag{2.1}$$

Todistetaan, että raja-arvo ei riipu ekvivalenssiluokan edustajien valinnasta ja että raja-arvo on olemassa. Näiden lisäksi tarkistetaan että D on metriikka joukossa $\hat{M}$.

Olkoon $\{a_n\}$, $\{a'_n\}$ eri Cauchy-jonoja ekvivalenssiluokasta A ja $\{b_n\}$, $\{b'_n\}$ eri Cauchy-jonoja ekvivalenssiluokasta B. Tällöin

$$\begin{aligned}
(1)\qquad \lim_{n\to\infty} d(a_n, b_n) &\leq \lim_{n\to\infty} d(a_n, a'_n) + d(a'_n, b'_n) + d(b'_n, b_n)\\
&= \lim_{n\to\infty} d(a_n, a'_n) + \lim_{n\to\infty} d(a'_n, b'_n) + \lim_{n\to\infty} d(b'_n, b_n)\\
&= \lim_{n\to\infty} d(a'_n, b'_n);
\end{aligned}$$

$$(2) \qquad \begin{aligned} \lim_{n\to\infty} d(a'_n, b'_n) &\leq \lim_{n\to\infty} d(a'_n, a_n) + d(a_n, b_n) + d(b_n, b'_n) \\ &= \lim_{n\to\infty} d(a'_n, a_n) + \lim_{n\to\infty} d(a_n, b_n) + \lim_{n\to\infty} d(b_n, b'_n) \\ &= \lim_{n\to\infty} d(a_n, b_n). \end{aligned}$$

Yhdistämällä kohdat (1) ja (2) saadaan

$$\lim_{n\to\infty} d(a_n, b_n) \leq \lim_{n\to\infty} d(a'_n, b'_n) \leq \lim_{n\to\infty} d(a_n, b_n),$$

jolloin täytyy olla

$$\lim_{n\to\infty} d(a_n, b_n) = \lim_{n\to\infty} d(a'_n, b'_n).$$

Raja-arvo ei siis riipu ekvivalenssiluokan edustajan valinnasta.

Raja-arvon olemassaolo seuraa, kun osoitetaan, että $(d(a_n, b_n))$ on Cauchy-jono reaalilukujen joukossa. Olkoon $\varepsilon/2 > 0$. Tällöin on olemassa N_1 siten, että aina, kun $n, m > N_1$, niin $d(a_n, a_m) < \varepsilon/2$. Tällöin on myös N_2 siten, että aina, kun $n, m > N_2$, niin $d(b_n, b_m) < \varepsilon/2$. Nyt kaikilla $n, m > \max(N_1, N_2)$ pätee, että

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

Lopuksi todistetaan, että metriikka D on joukossa $\hat{M}$ todella metriikka. Olkoon A, B ja C Cauchy-jonojen ekvivalenssiluokkia ja näiden edustajat vastaavasti $\{a_n\}$, $\{b_n\}$ ja $\{c_n\}$. Tällöin

(1) $D(A, B) = \lim_{n\to\infty} d(a_n, b_n) \geq 0$. Kun $D(A, B) = 0$, niin

$$D(A, B) = \lim_{n\to\infty} d(a_n, b_n) = 0,$$

jolloin Cauchy-jonojen a_n ja b_n sanotaan olevan ekvivalentteja ja täytyy olla $A = B$;

$$(2) \qquad D(A, B) = \lim_{n\to\infty} d(a_n, b_n) = \lim_{n\to\infty} d(b_n, a_n) = D(B, A);$$

$$(3) \qquad \begin{aligned} D(A, B) = \lim_{n\to\infty} d(a_n, b_n) &\leq \lim_{n\to\infty} d(a_n, c_n) + d(c_n, b_n) \\ &= \lim_{n\to\infty} d(a_n, c_n) + \lim_{n\to\infty} d(c_n, b_n) \\ &= D(A, C) + D(C, B). \end{aligned}$$

Täten D on metriikka joukossa $\hat{M}$ ja Lauseen 2.1 (1)-kohta on todistettu.

Olkoon $p \in M$ ja muodostetaan vakiojono $\bar{p} = (p, p, p, ...)$. Tämä on selvästi Cauchy-jono, ja vakiojonojen $\bar{p}$ ja $\bar{q}$ välinen etäisyys D on sama kuin pisteiden p ja q etäisyys d. Tällöin voidaan valita $M = \hat{M}_0$, jolloin $\hat{M}_0$ on luonnollisesti joukon $\hat{M}$ metrinen aliavaruus ja avaruudet $\hat{M}_0$ ja M ovat isometrisiä. Tästä saatiin Lauseen 2.1 (2)-kohta.

Viimeiseksi todistetaan, että $\hat{M}$ on täydellinen avaruus ja $\hat{M}_0$ on tiheä avaruudessa $\hat{M}$ eli jokainen piste joukossa $\hat{M}$ on avaruuden $\hat{M}_0$ Cauchy-jonon raja-arvo. Olkoon $(P_k)_{k\in\mathbb{N}}$ Cauchy-jono avaruudessa $\hat{M}$. Nyt etsitään raja-arvo $Q \in \hat{M}$, johon jono P_k suppenee, kun $k \to \infty$. (Huomaa, että (P_k) on jono ekvivalenssiluokkia, eikä jono

pisteitä joukossa M, ja suppenemisella viitataan metriikkaan D, eikä metriikkaan d.) Koska metriikka D on hyvin määritelty, saadaan todistusta hieman lyhennettyä. Väitetään, että on olemassa edustaja $(p_{k,n}) \in P_k$ siten, että kaikille m, $n \in \mathbb{N}$ pätee, että

$$d(p_{k,m}, p_{k,n}) < \frac{1}{k}. \tag{2.2}$$

Kaikki termit, jotka ovat edellä olevassa esitysmuodossa ovat lähekkäin, eivät vain jonojen häntäpäiden termit. Todistetaan edellinen väittämä ja etsitään haluttu joukon P_k edustaja. Olkoon $(p^*_{k,n})_{n\in\mathbb{N}}$ jokin joukon P_k edustaja. Koska jono on Cauchy-jono, niin on olemassa $N = N(k)$ siten, että kaikille m, $n \geq N$ pätee, että

$$d(p^*_{k,m}, p^*_{k,n}) < \frac{1}{k}.$$

Jono $p_{k,n} = p^*_{k,n+N}$ on ekvivalentti Cauchy-jonon $(p^*_{k,n})$ kanssa ja toteuttaa ehdon (2.2).

Jokaiselle luvulle k valitaan edustaja $(p_{k,n}) \in P_k$, joka toteuttaa ehdon (2.2) ja määritellään $q_n = p_{n,n}$. Väitetään, että (q_n) on Cauchy-jono avaruudessa $M = \hat{M}_0$ ja että P_k suppenee kohti ekvivalenssiluokkaa $Q \in \hat{M}_0$, kun $k \to \infty$. Tämä näyttämällä saadaan todistus loppuun.

Olkoon $\varepsilon > 0$. Tällöin on olemassa $N \geq 3/\varepsilon$ siten, että jos k, $l \geq N$, niin

$$D(P_k, P_l) < \frac{\varepsilon}{3}.$$

Jos k, $l \geq N$, niin ehdosta (2.2) saadaan

$$\begin{aligned} d(q_k, q_l) &= d(p_{k,k}, p_{l,l}) \\ &\leq d(p_{k,k}, p_{k,n}) + d(p_{k,n}, p_{l,n}) + d(p_{l,n}, p_{l,l}) \\ &\leq \frac{1}{k} + d(p_{k,n}, p_{l,n}) + \frac{1}{l} \\ &\leq \frac{2\varepsilon}{3} + d(p_{k,n}, p_{l,n}). \end{aligned}$$

Epäyhtälö on totta kaikilla luvun n arvoilla, eikä epäyhtälön vasen puoli riipu luvun n valinnasta. Etäisyyden $d(p_{k,n}, p_{l,n})$ raja-arvo on $D(P_k, P_l)$, jonka tiedetään olevan $< \varepsilon/3$, kun $n \to \infty$. Tällöin, jos k, $l \geq N$, niin $d(q_k, q_l) < \varepsilon$ ja (q_n) on Cauchy-jono. Vastaavasti nähdään, että $P_k \to Q$, kun $k \to \infty$. Annetulle $\varepsilon > 0$ valitaan $N \geq 2/\varepsilon$ siten, että jos k, $l \geq N$, niin $d(q_k, q_n) < \varepsilon/2$. Tästä seuraa, että

$$\begin{aligned} d(p_{k,n}, q_n) &\leq d(p_{k,n}, p_{k,k}) + d(p_{k,k}, q_n) \\ &= d(p_{k,n}, p_{k,k}) + d(q_k, q_n) \\ &< \frac{1}{k} + \frac{\varepsilon}{2} \leq \varepsilon. \end{aligned}$$

Epäyhtälön vasemman puolen $d(p_{k,n}, q_n)$ raja-arvo on $D(P_k, Q)$, kun $k \to \infty$. Siten saadaan

$$\lim_{n\to\infty} P_k = Q,$$

jolloin Lauseen 2.1 (3)-kohta on todistettu ja $\hat{M}$ on täydellinen metrinen avaruus. $\square$

Täydellistämisprosessi voidaan tehdä avaruudelle $M = \mathbb{Q}$ *euklidisen normin* suhteen

$$d(r_1, r_2) = \mid r_1 - r_2 \mid, \tag{2.3}$$

jolloin saadaan reaalilukujen avaruus $\mathbb{R}$. Huomaa, että euklidinen normi rationaaliluvuille $\mathbb{Q}$ on euklidinen *itseisarvo*.

Toinen tapa täydellistää avaruus $\mathbb{Q}$ avaruudeksi $\mathbb{R}$ on hieman tutumpi ja se perustuu päättymättömiin desimaalimurtolukuihin. Jokainen positiivinen reaaliluku a voidaan kirjoittaa päättymättömänä desimaalimurtolukuna

$$a = \sum_{k=m}^{\infty} a_k \cdot 10^{-k}, \tag{2.4}$$

missä m on jokin tietty kokonaisluku ja kertoimet a_k saavat arvoja

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

Tämä esitystapa on yksikäsitteinen paitsi jos $a_k = 0$ kaikilla $k > n$ ja $a_n \neq 0$, missä tapauksessa luvulla a on toinen esitys luvuilla $a'_k = a_k$, kun $k < n$, $a'_n = a_n - 1$ ja $a'_k = 9$ kaikilla luvuilla $k > n$. Käänteisesti, kaikki päättymättömät desimaalimurtoluvut esittävät pisteitä lukusuoralla ja siten on kätevää samaistaa reaaliluvut päättymättömillä desimaalimurtoluvuilla.

Jos rationaaliluvut esitetään päättymättömillä desimaalimurtoluvuilla, niistä tulee lopulta jaksollisia (Todistus sivuutetaan). On helppoa konstruoida Cauchy-jono rationaalilukuja, joilla ei ole raja-arvoa rationaalilukujen joukossa $\mathbb{Q}$:

$$.1,\ .1011,\ .10110111,\ .1011011101111\ldots;$$

täten $\mathbb{Q}$ ei ole täydellinen euklidisella normilla. Toisaalta rationaalilukujen Cauchy-jonojen ekvivalenssiluokalla on edustaja, joka on kaavan (2.4) sarjan osittaisten summien jono. Tämän raja-arvo on päättymätön desimaalimurtoluku. Tämä sama pätee mille tahansa Cauchy-jonolle päättymättömistä desimaalimurtoluvuista. Toisin sanoen reaalilukujen joukko on täydellinen euklidisella normilla. Reaalilukujen konstruointi päättymättömillä desimaalimurtoluvuilla ja täydellistämisprosessi euklidisella normilla ovat ekvivalentteja prosesseja.

Tämä esitys voidaan yleistää esitykseen kannassa g, missä $g \in \mathbb{Z}_+$, $g \geq 2$, jolloin

$$a = \sum_{k=m}^{\infty} a_k \cdot g^{-k},$$

missä kerroin a_k saa arvoja joukosta $\{0, 1, \ldots, g-1\}$. Huomaa, että kerroin $-k$ on negatiivinen ja lähestyy kohti $-\infty$.

Seuraavat huomiot voidaan määrittää jokaisessa metrisessä avaruudessa.

Määritelmä 2.2. Olkoon (M, d) metrinen avaruus ja $\mathbb{R}^+$ joukko positiivisia reaalilukuja. *Avoin pallo*, jonka säde on $r \in \mathbb{R}^+$ ja keskipiste on $a \in M$ on joukko

$$B(a, r) = \{x \in M \mid d(a, x) < r\}.$$

Suljettu pallo, jonka säde on $r \in \mathbb{R}^+$ ja keskipiste on $a \in M$ on joukko

$$\overline{B}(a, r) = \{x \in M \mid d(a, x) \leq r\}.$$

Olkoon $A \subset M$. Joukko A on *avoin*, jos kaikille $x \in A$ on olemassa avoin pallo $B(x, r) \subset A$. Joukko A on *suljettu*, jos sen komplementti M/A on avoin.

Käytännössä metrisen avaruuden täydellistymä saadaan yleensä erilaisella konstruktiolla kuin mitä määritelmässä käytetään, josta seuraavana lisää.

Lemma 2.3. *Olkoon M täydellinen metrinen avaruus ja olkoon X avaruuden M osajoukko. Tällöin X on täydellinen, jos ja vain jos se on suljettu joukossa M. Erityisesti joukon X sulkeuma joukossa M voidaan valita sen täydellistymäksi.*

Todistus. Todistus on suoraviivainen, mutta ohitetaan tässä tapauksessa. □

3. Normilla varustetut kunnat

Rationaaliluvut ja reaaliluvut ovat ensimmäisiä esimerkkejä rakennelmasta, jota kutsutaan kunnaksi. *Kunta* F on joukko, joka on varustettu kahdella laskuoperaatiolla, joita sanotaan yleisesti *yhteen-* ja *kertolaskuksi* ja ne toteuttavat ehdot (1)-(10). Nämä ehdot ovat

(1) kaikilla a, $b \in F$, $a + b = b + a$ (yhteenlaskun vaihdannaisuus),
(2) kaikilla a, b, $c \in F$, $a + (b + c) = (a + b) + c$ (yhteenlaskun liitännäisyys),
(3) on olemassa $0 \in F$ siten, että kaikilla $a \in F$, $0 + a = a$ (yhteenlaskun neutraalialkion olemassaolo),
(4) kaikilla $a \in F$ on olemassa $-a \in F$ siten, että $a + (-a) = 0$ (vastaluvun olemassaolo),
(5) kaikilla a, $b \in F$, $a \cdot b = b \cdot a$ (kertolaskun vaihdannaisuus),
(6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (kertolaskun liitännäisyys),
(7) on olemassa $1 \in F$ siten, että kaikilla $a \in F^\times = F/\{0\}$, $1 \cdot a = a$ (kertolaskun neutraalialkion olemassaolo),
(8) kaikilla $a \in F^\times$ on olemassa $a^{-1} \in F^\times$ siten, että $a \cdot a^{-1} = 1$ (kertolaskun käänteisalkion olemassaolo),
(9) kaikilla a, b, $c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$ (vaihdannaisuus),
(10) $0 \neq 1$.

Joukkoa, jolla on yksi binäärinen laskuoperaatio, joka toteuttaa kohdat (1) - (4) kutsutaan *Abelin (tai kommutaatiiviseksi) ryhmäksi.* Vastaavasti kuntaa F varustettuna yhteenlaskulla kutsutaan kunnan F *additiiviseksi ryhmäksi*, ja ryhmää $F^\times$ varustettuna kertolaskulla kutsutaan kunnan F *multiplikatiiviseksi ryhmäksi.* Joukkoa, jolla on kaksi binääristä laskuoperaatiota, jotka toteuttavat kohdat (1) - (6) ja (9), kutsutaan *kommutatiiviseksi renkaaksi.*

Tärkeä ominaisuus kunnalle on, että se ei sisällä *nollanjakajia*, toisin sanoen alkioita a, $b \in F^\times$ siten, että $a \cdot b = 0$.

Seuraavaksi tarkastellaan normia, joka ilmaisee joukon alkioiden välistä etäisyyttä. Keskeisimpiä normeja ovat euklidinen normi eli euklidinen itseisarvo ja *p-adinen normi*, joka liittyy keskeisesti p-adisiin lukuihin ja avaruuteen $\mathbb{Q}_p$. P-adista normia käsitellään tarkemmin Kappaleessa 5.

Määritelmä 3.1. Olkoon F kunta. Normia kunnassa F merkitään $\|\cdot\|$ ja se on kuvaus kunnalta F ei-negatiivisille reaaliluvuille siten, että

(1) $\|x\| = 0$, jos ja vain jos $x = 0$;
(2) $\|xy\| = \|x\|\|y\|$ kaikilla x, $y \in F$;
(3) $\|x + y\| \leq \|x\| + \|y\|$ kaikilla x, $y \in F$ (*kolmioepäyhtälö*).

Sanotaan, että normi on *triviaali*, jos $\|0\| = 0$ ja $\|x\| = 1$ kaikilla $x \neq 0$. Huomaa, että kaikille luonnollisille luvuille $n \in \mathbb{N}$ pätee, että

$$1 \cdot n := \underbrace{1 + \cdots + 1}_{n\,\text{kertaa}} \in F.$$

Merkitään edellä olevaa alkiota symbolilla n samoin kuin vastaavaa luonnollista lukua.

Lemma 3.2. *Kaikille x, $y \in F$ pätee, että*

(a) $\|1\| = \|-1\| = 1$;
(b) $\|x\| = \|-x\|$;
(c) $\|x \pm y\| \geq |\, \|x\| - \|y\| \,|$;
(d) $\|x - y\| \leq \|x\| + \|y\|$;
(e) $\|x/y\| = \|x\|/\|y\|$;
(f) $\|n\| \leq n$ *kaikilla* $n \in \mathbb{N}$.

Todistus. Olkoon x, $y \in F$.

(a) Normin peruslaskuominaisuuksilla saadaan $\|1\| = \|\pm 1 \cdot \pm 1\| = \|\pm 1\|^2$. Ottamalla edellisestä lausekkeesta puolittain neliöjuuri saadaan $\|\pm 1\| = 1$.
(b) $\|-x\| = \|(-1) \cdot x\| = \|-1\| \cdot \|x\| = 1 \cdot \|x\| = \|x\|$.
(c) $\|x\| = \|x - y + y\| \leq \|x - y\| + \|y\|$ tai $\|x\| = \|x - y + y\| \leq \|x + y\| + \|-y\| = \|x + y\| + \|y\|$, josta seuraa $\|x\| - \|y\| \leq \|x \pm y\|$. Sama voidaan tehdä vaihtamalla lukujen x ja y paikkaa, jolloin saadaan $\|y\| - \|x\| \leq \|x \pm y\|$, joka on sama asia kuin $\|x\| - \|y\| \geq -\|x \pm y\|$. Yhdistämällä kaksi edellistä kohtaa saadaan $-\|x \pm y\| \leq \|x\| - \|y\| \leq \|x \pm y\|$, joka on toisin sanoen $|\|x\| - \|y\|| \leq \|x \pm y\|$.
(d) $\|x - y\| = \|x + (-y)\| \leq \|x\| + \|-y\| = \|x\| + \|y\|$.
(e) $\|x/y\|\|y\| = \|(x/y)y\| = \|x\| = (\|x\|/\|y\|)\|y\|$. Jakamalla edellinen lauseke luvulla $\|y\|$ saadaan $\|x/y\| = \|x\|/\|y\|$.
(f) $\|n\| = \|n - 1 + 1\| \leq \|n - 1\| + \|1\| = \|n - 1\| + 1 = \cdots = \|n - 2\| + 2 = \cdots = \|n - n\| + n = \|0\| + n = 0 + n = n$ kaikilla $n \in \mathbb{N}$.

□

Olkoon $d(x, y) = \|x - y\|$. Määritelmästä 3.1 ja Lemmasta 3.2 seuraa suoraan, että kuvaus d on etäisyysfunktio. Määritelmän 3.1 kohta (1) viittaa, että $d(x, y) = 0$, jos ja vain jos $x = y$, kun taas Lemman 3.2 kohta (b) viittaa symmetriaan ja sen kohta (d) tuottaa kolmioepäyhtälön. Sanotaan, että tämä etäisyys on saatu aikaan normilla $\|\cdot\|$, jolloin joukkoa $(F, \|\cdot\|)$ pidetään metrisenä avaruutena.

Määritelmä 3.3. Jonon $\{a_n\}$ kunnassa F sanotaan

- olevan *rajoitettu*, jos on olemassa vakio $C > 0$ siten, että
$$\|a_n\| \leq C \textit{ kaikilla } n;$$
- olevan *nollajono*, jos
$$\lim_{n\to\infty} \|a_n\| = 0.$$
Toisin sanoen mille tahansa $\varepsilon > 0$ on olemassa N siten, että kaikilla $n > N$ pätee $\|a_n\| < \varepsilon$;
- olevan *Cauchy-jono*, jos
$$\lim_{n,m\to\infty} \|a_n - a_m\| = 0.$$
Toisin sanoen mille tahansa $\varepsilon > 0$ on olemassa N siten, että kaikilla n, $m > N$ pätee $\|a_n - a_m\| < \varepsilon$;
- *suppenevan* kohti lukua $a \in F$ (kirjoitetaan, että $\lim_{n\to\infty} a_n = a$), jos
$$\lim_{n\to\infty} \|a_n - a\| = 0.$$

Toisin sanoen mille tahansa $\varepsilon > 0$ on olemassa N siten, että kaikilla $n > N$ pätee $\|a_n - a\| < \varepsilon$.

Määritelmästä seuraa, että nollajonot suppenevat kohti lukua 0 ja kolmioepäyhtälöstä seuraa, että suppenevat jonot ovat Cauchy-jonoja: oletetaan, että $\lim_{n\to\infty} a_n = a$. Tällöin

$$\|a_n - a_m\| = \|a_n + a - a - a_m\| \leq \|a_n - a\| + \|a - a_m\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

kun n, $m > N$, jotka on valittu luvulle $\varepsilon/2$ raja-arvon määritelmästä. Erityisesti jokainen nollajono on Cauchy-jono. Vastaavanlaisia ominaisuuksia saadaan todistettua samanlaisella perusidealla kuin edellä. Näitä ovat seuraavat.

Lemma 3.4.

(1) *Jokainen Cauchy-jono on rajoitettu.*
(2) *Olkoon $\{a_n\}$ Cauchy-jono ja olkoon $\{n_1, n_2, \dots\}$ kasvava jono positiivisia kokonaislukuja. Jos osajono $a_{n_1}, a_{n_2}, \dots$ on nollajono, niin jono $\{a_n\}$ on nollajono.*
(3) *Jos jonot $\{a_n\}$ ja $\{b_n\}$ ovat nollajonoja, niin jono $\{a_n \pm b_n\}$ on nollajono. Jos jono $\{a_n\}$ on nollajono ja jono $\{b_n\}$ on rajoitettu, niin jono $\{a_n b_n\}$ on nollajono.*
(4) *Olkoon $\{a\}$ Cauchy-jono, mutta ei nollajono. Tällöin on olemassa luku $c > 0$ ja positiivinen kokonaisluku N siten, että kaikille $n > N$ pätee, että joko $a_n > c$ tai $a_n < -c$.*

Todistus.

(1) Olkoon $\{a_n\}$ Cauchy-jono. Tällöin luvulle $\varepsilon > 0$ on olemassa N siten, että kaikille n, $m > N$ pätee, että $\|a_n - a_m\| < \varepsilon$. Tällöin

$$\|a_n\| = \|a_n - a_m + a_m\| \leq \|a_n - a_m\| + \|a_m\| < \varepsilon + \|a_m\|.$$

Olkoon $m = N + 1$, jolloin $\|a_n\| < \varepsilon + \|a_{N+1}\|$ kaikilla $n > N$. Tällöin $\|a_n\| \leq \max(\|a_1\|, \|a_2\|, \dots, \|a_N\|, \|a_{N+1}\|, \varepsilon + \|a_{N+1}\|) = C$. Tällöin $\{a_n\}$ on rajoitettu.

(2) Olkoon $\{a_n\}$ Cauchy-jono, $\{n_1, n_2, \dots\}$ kasvava jono positiivisia kokonaislukuja ja osajono $a_{n_1}, a_{n_2}, \dots$ on nollajono. Tällöin luvulle $\varepsilon/2 > 0$ on olemassa N siten, että kaikille n, $n_i > N$ pätee, että $\|a_n - a_{n_i}\| < \varepsilon/2$, sekä M siten, että kaikille $n_i > M$ pätee, että $\|a_{n_i}\| < \varepsilon/2$, kun $i \in \{1, 2, \dots\}$

$$\|a_n\| = \|a_n - a_{n_i} + a_{n_i}\| \leq \|a_n - a_{n_i}\| + \|a_{n_i}\| = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Tällöin $\{a_n\}$ on nollajono.

(3) (i) Olkoon $\{a_n\}$ ja $\{b_n\}$ nollajonoja. Tällöin luvulle $\varepsilon/2 > 0$ on olemassa luvut N ja M siten, että kaikille $n > N$ pätee, että $\|a_n\| < \varepsilon/2$ ja että kaikille $n > M$ pätee, että $\|b_n\| < \varepsilon/2$. Tällöin kaikille $n > \max(N, M)$ pätee, että $\|a_n \pm b_n\| \leq \|a_n\| + \| \pm b_n\| = \|a_n\| + \|b_n\| < \varepsilon/2 + \varepsilon/2 = \varepsilon$. Tällöin $\{a_n \pm b_n\}$ on nollajono.

(ii) Olkoon $\{a_n\}$ nollajono ja jono $\{b_n\}$ rajoitettu. Tällöin luvulle ε/C on olemassa N siten, että kaikilla $n > N$ pätee, että $\|a_n\| < \varepsilon/C$ ja kaikille

$n > M$ pätee, että $\|b_n\| \leq C$. Tällöin kaikilla $n > \max(N, M)$ pätee, että $\|a_n b_n\| = \|a_n\|\|b_n\| < \varepsilon/C \cdot C = \varepsilon$. Tällöin $\{a_n b_n\}$ on nollajono.

(4) Olkoon $\{a_n\}$ Cauchy-jono, mutta ei nollajono. Kohdan (1) nojalla Cauchy-jonot ovat rajoitettuja ja $\|a_n\| \leq C$ kaikilla kokonaisluvuilla n. Olkoon nyt $\varepsilon > 0$. Tällöin $\|a_n\| < C + \varepsilon$ kaikilla $n > N$. Jos $a_n < 0$, niin $-a_n < C + \varepsilon$, josta seuraa $a_n > -(C + \varepsilon)$. Jos taas $a_n > 0$, niin $a_n < C + \varepsilon$. Voidaan siis valita $c := C + \varepsilon$, jolloin kaikilla $n > N$ pätee, että joko $a_n > c$ tai $a_n < -c$.

□

Seuraava tulos on yksinkertainen, mutta erittäin käytännöllinen.

Lemma 3.5. $\|x\| < 1$, *jos ja vain jos* $\lim_{n\to\infty} x^n = 0$.

Todistus. Olkoon $\|x\| < 1$. Koska $\|x^n\| = \|x\|^n$, niin saadan, että

$$\lim_{n\to\infty} \|x^n\| = 0,$$

toisin sanoen $\lim_{n\to\infty} x^n = 0$. Toisaalta, jos $\|x\| \geq 1$, niin kaikille positiivisille kokonaisluvuille n pätee, että $\|x^n\| \geq 1$, jolloin $0 \neq \lim_{n\to\infty} x^n$. □

Määritelmä 3.6. Metriikat d_1 ja d_2 ovat *ekvivalentteja* kunnassa F, jos jono on Cauchy-jono metriikalla d_1, jos ja vain jos se on Cauchy-jono metriikalla d_2. Normit $\|\cdot\|_1$ ja $\|\cdot\|_2$ ovat ekvivalentteja ($\|\cdot\|_1 \sim \|\cdot\|_2$), jos ne tuottavat ekvivalentit metriikat.

Lemma 3.7. *Olkoon* $\|\cdot\|_1 \sim \|\cdot\|_2$. *Tällöin*

(1) $\|\cdot\|_1 < 1$, *jos ja vain jos* $\|\cdot\|_2 < 1$,
(2) $\|\cdot\|_1 = 1$, *jos ja vain jos* $\|\cdot\|_2 = 1$ *ja*
(3) $\|\cdot\|_1 > 1$, *jos ja vain jos* $\|\cdot\|_2 > 1$.

Todistus. Olkoon $\|\cdot\|_1 \sim \|\cdot\|_2$.

(1) Tehdään vastaoletus, jolloin jollekin alkiolle a pätee, että $\|a\|_1 < 1$, mutta $\|a\|_2 \geq 1$. Koska ollaan kunnassa, voidaan muodostaa potenssien jono $(a_n) = (a^n)$, missä $a^n = a \cdot \cdots \cdot a$. Lemman 3.5 nojalla tämä on Cauchy-jono ensimmäisen normin suhteen, sillä $\|a^n\|_1 = \|a\|_1^n \to 0$, kun $n \to \infty$.

Väitetään, että jono (a_n) ei ole Cauchy-jono toisen normin suhteen. Lemman 3.2 nojalla $a \neq 1$, sillä muuten olisi $\|a\|_1 = 1$. Nyt $\|a^n - a^{n+1}\|_2 = \|a\|_2^n \|a - 1\|_2 \geq \|a - 1\|_2$ kaikilla luvuilla n. Siis (a^n) ei voi olla Cauchy-jono normin $\|\cdot\|_2$ suhteen. Ristiriita todistaa, että jos $\|\cdot\|_1 < 1$, niin $\|\cdot\|_2 < 1$. Väite tulee toiseen suuntaan, kun vaihdetaan normit keskenään.

(2) Oletetaan, että $a \neq 1$. Tehdään vastaoletus, jolloin jollekin alkiolle a pätee, että $\|a\|_1 = 1$, mutta $\|a\|_2 > 1$ (tai $\|a\|_2 < 1$, mutta tämä hylätään kohdan (1) nojalla). Jos $a = 1$, niin väite selvä. Oletetaan, että $a \neq 1$. Koska ollaan kunnassa, voidaan muodostaa potenssien jono $(a_n) = (a^n)$, missä $a^n = a \cdot \cdots \cdot a$. Tämä on Cauchy-jono ensimmäisen normin suhteen, sillä $\|a^n - 1\|_1 \leq \|a\|_1^n + \|-1\|_1 = 1 - 1 = 0$, kaikilla luvun n arvoilla.

Väitetään, että jono (a_n) ei ole Cauchy-jono toisen normin suhteen. Nyt $\|a^n - a^{n+1}\|_2 = \|a\|_2^n \|a - 1\|_2 \geq \|a - 1\|_2$ kaikilla luvuilla n. Siis (a^n) ei voi olla Cauchy-jono normin $\|\cdot\|_2$ suhteen. Ristiriita todistaa, että jos $\|\cdot\|_1 = 1$, niin $\|\cdot\|_2 = 1$. Väite tulee toiseen suuntaan, kun vaihdetaan normit keskenään.

(3) Olkoon $\|\cdot\|_1 > 1$. Kohtien (1) ja (2) nojalla täytyy olla $\|\cdot\|_2 > 1$. Väite tulee toiseen suuntaan, kun vaihdetaan normit keskenään.

□

Lemma 3.8. *Olkoon $\|\cdot\|_1$ ja $\|\cdot\|_2$ kaksi normia kunnassa F. Tällöin $\|\cdot\|_1 \sim \|\cdot\|_2$, jos ja vain jos on olemassa kokonaisluku α siten, että*

$$\|x\|_2 = \|x\|_1^{\alpha}, \text{ kaikilla } x \in F. \tag{3.1}$$

Todistus. Olkoon $\|\cdot\|_1$ ja $\|\cdot\|_2$ normeja. Jos $\|\cdot\|_1$ on triviaali, niin $\|x\|_2 = \|x\|_1 = 1$ kaikilla $x \neq 0$ ja $\|0\|_2 = \|0\|_1 = 0$, jolloin myös $\|\cdot\|_2$ on triviaali ja tällöin Lauseke (3.1) toteutuu, millä tahansa α arvolla.

Jos $\|\cdot\|_1$ ei ole triviaali, niin voidaan valita alkio $a \in F$ siten, että $\|a\|_1 \neq 1$. Korvaamalla luku a sen käänteisalkiolla a^{-1} tarvittaessa voidaan olettaa, että $\|a\|_1 < 1$. Merkitään

$$\alpha = \frac{\log \|a\|_2}{\log \|a\|_1}.$$

Koska normit ovat ekvivalentteja, saadaan Lemman 3.7 nojalla, että $\|a\|_2 < 1$. Tällöin molemmat logaritmit ovat negatiivisia ja $\alpha > 0$.

Näytetään seuraavaksi, että α toteuttaa Lausekkeen (3.1). Olkoon $x \in F$ siten, että $\|x\|_1 < 1$. Tapaukset $\|x\|_1 > 1$ ja $\|x\|_1 = 1$ seuraavat Lemmasta 3.7. Olkoon joukko

$$S = \{r = m/n \mid m, n \in \mathbb{N},\ \|x\|_1^r < \|a\|_1\}. \tag{3.2}$$

Mille tahansa $r \in S$ pätee, että

$$\|x\|_1^m < \|a\|_1^n, \text{ joten } \left\|\frac{x^m}{a^n}\right\|_1 < 1.$$

Tällöin Lemman 3.7 nojalla saadaan, että

$$\left\|\frac{x^m}{a^n}\right\|_2 < 1,$$

jolloin $\|x\|_2^m < \|a\|_2^n$, ja $\|x\|_2^r < \|a\|_2$. Sama tulos pätee normeille $\|\cdot\|_2$ ja $\|\cdot\|_1$, jolloin pätee myös

$$S = \{r = m/n \mid m, n \in \mathbb{N},\ \|x\|_2^r < \|a\|_2\}. \tag{3.3}$$

Ottamalla logaritmit lausekkeiden (3.2) ja (3.3) ehdoista saadaan ne kirjoitettua uudelleen muodossa

$$r > \frac{\log \|a\|_1}{\log \|x\|_1}, \quad r > \frac{\log \|a\|_2}{\log \|x\|_2}, \tag{3.4}$$

sillä kaikki kyseessä olevat logaritmit ovat negatiivisia. Mutta tällöin täytyy päteä

$$\frac{\log \|a\|_1}{\log \|x\|_1} = \frac{\log \|a\|_2}{\log \|x\|_2},$$

koska muutoin olisi rationaalinen luku r näiden kahden luvun välillä ja vain toinen lausekkeista (3.4) olisi voimassa. Joten

$$\frac{\log \|x\|_1}{\log \|x\|_2} = \frac{\log \|a\|_2}{\log \|a\|_1} = \alpha,$$

ja Lauseke (3.1) toteutuu.

Oletetaan siten, että $\|x\|_2 = \|x\|_1^\alpha$. Olkoon $\{a_n\}$ on Cauchy-jono etäisyydellä, joka on saatu normilla $\|\cdot\|_1$. Annetulle $\varepsilon > 0$ valitaan N luvulle $\varepsilon^{1/\alpha}$. Tällöin luvuille n, $m \geq N$ pätee, että $\|x_n - x_m\|_1 < \varepsilon^{1/\alpha}$, josta seuraa $\|x_n - x_m\|_2 < \varepsilon$. Sama päättely toimii, kun normit $\|\cdot\|_1$ ja $\|\cdot\|_2$ vaihdetaan, mikä päättää todistuksen. □

Tästä eteenpäin kaikki normit ajatellaan rationaalilukujen joukossa $\mathbb{Q}$ itseisarvona $|\cdot|$. Toisin sanoen kaikilla $a \geq 0$ pätee, että $|a| = a$ ja kaikilla $a < 0$ pätee, että $|a| = -a$.

Lemma 3.9. *$\|x\| = |x|^\alpha$, missä $\alpha > 0$, on normi joukossa $\mathbb{Q}$, jos ja vain jos $\alpha \leq 1$. Tällöin se on ekvivalentti normin $|\cdot|$ kanssa.*

Todistus. Olkoon $\alpha \leq 1$. Ensimmäinen normin ehto saadaan, kun $x \neq 0$, niin $|x| \neq 0$ ja $|x|^\alpha \neq 0$, lisäksi $|0|^\alpha = 0^\alpha = 0$. Seuraavaksi huomataan, että $|xy|^\alpha = (|x||y|)^\alpha = |x|^\alpha |y|^\alpha$ kaikilla x, $y \in \mathbb{Q}$, mikä toteuttaa toisen vaatimuksen. Viimeiseksi jää tarkistaa kolmas ehto eli kolmioepäyhtälö. Oletetaan, että $|y| \leq |x|$. Tällöin

$$\begin{aligned} |x+y|^\alpha &\leq (|x|+|y|)^\alpha = |x|^\alpha \left(1 + \frac{|y|}{|x|}\right)^\alpha \\ &\leq |x|^\alpha \left(1 + \frac{|y|}{|x|}\right) \leq |x|^\alpha \left(1 + \frac{|y|^\alpha}{|x|^\alpha}\right) = |x|^\alpha + |y|^\alpha. \end{aligned}$$

Ensimmäinen epäyhtälö seuraa siitä, että $t^\alpha \leq t$, kun $t \geq 1$ ja seuraava siitä, että $t^\alpha \geq t$, kun $0 \leq t \leq 1$.

Toisaalta, jos $a > 1$ niin kolmioepäyhtälö ei toteudu, esimerkiksi $|1+1|^\alpha = 2^\alpha > |1|^\alpha + |1|^\alpha = 2$. □

Määritelmä 3.10. Normin sanotaan olevan *epäarkhimedinen*, jos se toteuttaa lisäehdon

(4) $\|x+y\| \leq \max(\|x\|, \|y\|)$;

muuten sanotaan, että normi on *arkhimedinen*.

Huomautus 3.11. Normin ehdolla (4) viitataan ehtoon (3), kolmioepäyhtälöön, sillä arvo $\max(\|x\|, \|y\|)$ ei ylitä summan $\|x\| + \|y\|$ arvoa. Tätä ominaisuuttaa sanotaan *vahvaksi kolmioepäyhtälöksi*.

Epäarkhimedisella normilla tuotettua metriikkaa sanotaan *ultrametriseksi*. Yleisen metriikan kolmioepäyhtälön

$$d(x,z) \leq d(x,y) + d(y,z),$$

sijaan se toteuttaa vahvan kolmiepäyhtälön

$$d(x,z) \leq \max(d(x,y), d(y,z)).$$

Tätä vastaavia metrisiä avaruuksia sanotaan *ultrametrisiksi avaruuksiksi*.

Seuraava lause on välttämätön ja riittävä ehto, jotta normi olisi epäarkhimedinen.

Lemma 3.12. *Seuraavat ehdot ovat yhtäpitäviä*

(a) *$\|\cdot\|$ on epäarkhimedinen;*
(b) *$\|n\| \leq 1$ kaikille kokonaisluvuille n.*

Todistus. (a) $\implies$ (b). Todistetaan tämä induktiolla.

Perusaskel. $\|1\| = 1 \leq 1$.

Induktioaskel. Oletetaan, että $\|k\| \leq 1$, kaikilla $k \in \{1, 2, \ldots, n-1\}$ ja todistetaan, että $\|n\| \leq 1$.

Huomataan, että $\|n\| = \|(n-1)+1\| \leq \max(\|n-1\|, 1) = 1$.

Epäyhtälöstä $\|1\| = 1 \leq 1$ ja induktio-oletuksesta saadaan, että $\|n\| \leq 1$ kaikilla $n \in \mathbb{N}$. Koska $\|-n\| = \|n\|$, niin saadaan, että $\|n\| \leq 1$ kaikilla kokonaisluvuilla $n \in \mathbb{Z}$.

(b) $\implies$ (a). Saadaan

$$\begin{aligned}
\|x+y\|^n = \|(x+y)^n\| &= \left\| \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right\| \\
&\leq \sum_{k=0}^{n} \left\| \binom{n}{k} \right\| \|x\|^k \|y\|^{n-k} \leq \sum_{k=0}^{n} \|x\|^k \|y\|^{n-k} \\
&\leq (n+1)[\max(\|x\|, \|y\|)]^n.
\end{aligned}$$

Tällöin jokaiselle kokonaisluvulle n pätee, että

$$\|x+y\| \leq \sqrt[n]{n+1} \max(\|x\|, \|y\|).$$

Kun luku n lähetyy kohti ∞, saadaan

$$\|x+y\| \leq \max(\|x\|, \|y\|).$$

Tässä käytettiin tietoa, että $\binom{n}{k}$ on kokonaisluku ja tunnettu raja-arvo on

$$\lim_{n\to\infty} \sqrt[n]{n+1} = 1.$$

□

Edellinen lemma auttaa ymmärtämään eron arkhimedisen ja epäarkhimedisen normin välillä. Se voidaan ilmaista myös toisin: normi on arkhimedinen, jos ja vain jos sillä on *arkhimedinen ominaisuus*: *olkoon* x, $y \in F$, $x \neq 0$. *Tällöin on olemassa positiivinen kokonaisluku* n *siten, että* $\|nx\| > \|y\|$. Tämän nähdäkseen tulee valita x, $y \in F$ siten, että $\|y\| > \|x\|$. Tällöin arkhimedisesta ominaisuudesta seuraa, että on olemassa positiivinen kokonaisluku n siten, että $\|n\| > \|y\|/\|x\| > 1$. Toisin sanoen normi on arkhimedinen. Käänteisesti, jos normi on arkhimedinen, niin on olemassa kokonaisluku n siten, että $\|n\| > 1$. Tällöin $\|n\|^k \to \infty$, kun $k \to \infty$ ja jollain luvun k arvolla $\|n^k\| > \|y\|/\|x\|$, mistä seuraa arkhimedinen ominaisuus $\|n^k x\| > \|y\|$.

Nähdään, että arkhimedinen ominaisuus on ekvivalentti sen kanssa, että on olemassa kokonaislukuja, joiden normin arvo on mielivaltaisen suuri:

$$\sup\{\|n\| : n \in \mathbb{Z}\} = +\infty. \tag{3.5}$$

Todistetaan, että normi on arkhimedinen, jos ja vain jos lauseke (3.5) toteutuu. Oletetaan, että normi on arkhimedinen, jolloin $\sup\{\|n\| : n \in \mathbb{Z}\} = C$ ja $C > 1$, sillä Lemman 3.12 mukaan epäarkhimediselle normille pätee, että $\|n\| \leq 1$. Tällöin täytyy olla olemassa kokonaisluku, jonka normi on aidosti suurempaa kuin yksi. Mutta tällöin $\|m^k\| = \|m\|^k$ kasvaa mielivaltaisen suureksi, kun k kasvaa. Tällöin C ei voi olla äärellinen ja normin saadessa positiivisia arvoja on $C = +\infty$. Oletetaan nyt

$\sup\{\|n\| : n \in \mathbb{Z}\} = +\infty$. Jos normi olisi epäarkhimedinen, niin $\|n\| \leq 1$ kaikilla luvun n arvoilla Lemman 3.12 mukaan ja olisi $\sup\{\|n\| : n \in \mathbb{Z}\} = 1$, mikä on ristiriita. Normin täytyy siis olla arkhimedinen.

Epäarkhimedisella ominaisuudella on muita yllättäviä sovelluksia.

Lemma 3.13. *Jos alkiot a ja x epäarkhimedisesta kunnasta F toteuttavat epäyhtälön $\|x - a\| < \|a\|$, niin tällöin $\|x\| = \|a\|$.*

Todistus. Vahvasta kolmioepäyhtälöstä saadaan, että

$$\|x\| = \|x - a + a\| \leq \max(\|x - a\|, \|a\|) = \|a\|.$$

Toisaalta pätee, että

$$\|a\| = \|a - x + x\| \leq \max(\|x - a\|, \|x\|).$$

Tällöin, jos olisi $\|x - a\| > \|x\|$ niin siitä seuraisi, että $\|a\| \leq \|x - a\|$, mikä on ristiriita. Siten täytyy olla, että $\|x - a\| \leq \|x\|$ ja saadaan $\|a\| \leq \|x\|$. Tästä seuraa, että $\|x\| = \|a\|$. □

Huomautus 3.14. Edellinen ominaisuus voidaan ilmaista toisin seuraavasti: alkioille a, b epäarkhimedisesta kunnasta F pätee, että

$$\|a\| > \|b\| \implies \|a + b\| = \|a\| : \textit{vahvin voittaa.}$$

Geometriaa hyödyntäen voidaan sanoa, että: *Mikä tahansa kolmio ultrametrisessä avaruudessa on tasakylkinen ja sen kannan pituus ei ylitä sen sivujen pituuksia.*

Lemma 3.15. *Jos normi $\|\cdot\|$ on epäarkhimedinen, niin silloin mikä tahansa avoimen pallon $B(a, r) = \{x : \|x - a\| < r\}$ piste kunnassa F on sen keskipiste. Toisin sanoen, jos b kuuluu joukkoon $B(a, r)$, niin $B(b, r) = B(a, r)$. Sama pätee suljetuille palloille.*

Todistus. Olkoon $b \in B(a, r) = \{x : \|x - a\| < r\}$. Tällöin $\|x - b\| = \|x - a + a - b\| \leq \max(\|x - a\|, \|a - b\|) = \max(\|x - a\|, \|b - a\|)$.

- Jos $\max(\|x - a\|, \|b - a\|) = \|x - a\|$, niin tällöin $\|x - b\| \leq \|x - a\| < r$ ja $B(b, r) = B(a, r)$.
- Jos $\max(\|x - a\|, \|b - a\|) = \|b - a\|$, niin tällöin $\|x - b\| \leq \|b - a\| < r$, koska $b \in B(a, r)$ ja $B(b, r) = B(a, r)$.

□

Tämä kappale saadaan käsitellyksi, kun näytetään, että epäarkhimedinen normi ja arkhimedinen normi eivät voi olla ekvivalentteja.

Lemma 3.16. *Kaksi ekvivalenttia normia ($\|\cdot\|_1 \sim \|\cdot\|_2$) kunnassa F ovat molemmat joko epäarkhimedisiä tai arkhimedisiä.*

Todistus. Olkoon $\|\cdot\|_1 \sim \|\cdot\|_2$. Tällöin mille tahansa kokonaisluvulle n pätee, että jos $\|n\|_1 > 1$, niin $\|n\|_2 > 1$ Lemman 3.7 nojalla. Tästä seuraa, että molemmat normit ovat Lemman 3.12 nojalla arkhimedisia. Jos taas mille tahansa kokonaisluvulle n pätee, että $\|n\|_1 \leq 1$, niin $\|n\|_2 \leq 1$ ja tällöin normit ovat epäarkhimedisia. □

4. Normilla varustetun kunnan täydellistäminen

Tässä kappaleessa lähdetään liikkeelle mielivaltaisesta kunnasta F, joka on varustettu normilla. (Kunta F ei ole välttämättä täydellinen tällä normilla $\|\cdot\|$.) Muodostetaan toinen kunta $\hat{F}$, joka sisältää kunnan F ja varustetaan se normilla (Tämä normi on saatu aikaan kunnan F normista) siten, että $\hat{F}$ on täydellinen kunta varustettuna normilla.

Kappaleessa 2 nähtiin, kuinka rationaaliluvuista varustettuna euklidisella normilla saatiin reaaliluvut $\mathbb{R}$ täydellistämisellä. Tämä sama prosessi tehdään myöhemmin rationaaliluvuille (Kappale 5), joka varustetaan täysin erilaisella normilla, jolla saadaan aikaan p-adiset luvut. Täydellistämisessä tärkein rooli on Cauchy-jonoilla. Kunnan F Cauchy-jonojen ekvivalenssiluokista muodostetaan kunnan $\hat{F}$ alkiot. Tutkitaan Cauchy-jonoja mielivaltaisessa kunnassa varustettuna normilla.

Cauchy-jonoja voidaan laskea yhteen, vähentää toisistaan ja kertoa keskenään. Tämä todistetaan seuraavaksi.

Lemma 4.1. *Jos jonot $\{a_n\}$ ja $\{b_n\}$ ovat Cauchy-jonoja, niin*

$$\{a_n + b_n\}, \{a_n - b_n\} \text{ ja } \{a_n b_n\},$$

ovat Cauchy-jonoja.

Todistus.

(i) Olkoon $\{a_n\}$ ja $\{b_n\}$ Cauchy-jonoja. Tällöin luvulle $\varepsilon/2 > 0$ on olemassa N siten, että kaikille n, $m > N$ pätee, että $\|a_n - a_m\| < \varepsilon/2$ ja luvulle $\varepsilon/2 > 0$ on olemassa M siten, että kaikille n, $m > M$ pätee, että $\|b_n - b_m\| < \varepsilon/2$. Tällöin kaikille n, $m > \max(N, M)$ pätee, että

$$\|a_n + b_n - (a_m + b_m)\| \leq \|a_n - a_m\| + \|b_n - b_m\| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Tästä seuraa, että $\{a_n + b_n\}$ on Cauchy-jono.

(ii) Olkoon $\{a_n\}$ ja $\{b_n\}$ Cauchy-jonoja. Tällöin luvulle $\varepsilon/2 > 0$ on olemassa N siten, että kaikille n, $m > N$ pätee, että $\|a_n - a_m\| < \varepsilon/2$ ja luvulle $\varepsilon/2 > 0$ on olemassa M siten, että kaikille n, $m > M$ pätee, että $\|b_n - b_m\| < \varepsilon/2$. Tällöin kaikille n, $m > \max(N, M)$ pätee, että

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

Tästä seuraa, että $\{a_n - b_n\}$ on Cauchy-jono.

(iii) Olkoon $\{a_n\}$ ja $\{b_n\}$ Cauchy-jonoja. Koska Cauchy-jonot ovat rajoitettuja (todistettu aiemmin), niin on olemassa $M_1 > 0$ ja $M_2 > 0$ siten, että kaikille n pätee, että $\|b_n\| \leq M_1$ ja $\|a_n\| \leq M_2$. Tällöin

$$\begin{aligned}\|a_n b_n - a_m b_m\| &= \|a_n b_n - a_m b_n + a_m b_n - a_m b_m\| \\ &\leq \|b_n(a_n - a_m) + a_m(b_n - b_m)\| \\ &\leq \|b_n\|\|a_n - a_m\| + \|a_m\|\|b_n - b_m\| \\ &\leq M_1\|a_n - a_m\| + M_2\|b_n - b_m\|.\end{aligned}$$

Olkoon $\varepsilon/2M_1 > 0$ ja $\varepsilon/2M_2 > 0$. Cauchy-jonoille saadaan, että on olemassa N_1 siten, että kaikille n, $m > N_1$ pätee, että $\|a_n - a_m\| < \varepsilon/2M_1$ ja luvulle

$\varepsilon/2M_2 > 0$ on olemassa N_2 siten, että kaikille n, $m > N_2$ pätee, että $\|b_n - b_m\| < \varepsilon/2M_2$. Tällöin kaikille n, $m > \max(N_1, N_2)$ pätee, että

$$\begin{aligned}\|a_n b_n - a_m b_m\| &\leq M_1\|a_n - a_m\| + M_2\|b_n - b_m\| \\ &< M_1\frac{\varepsilon}{2M_1} + M_2\frac{\varepsilon}{2M_2} \\ &= \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.\end{aligned}$$

□

Edellisistä laskuoperaatioiden ominaisuuksista seuraa, että Cauchy-jonojen kokoelma joukossa $(F, \|\cdot\|) = \{F\}$ on kommutatiivinen rengas. Sen neutraalialkio yhteenlaskun suhteen on jono

$$\hat{0} = \{0, 0, 0, \dots\}$$

ja neutraalialkio kertolaskun suhteen on jono

$$\hat{1} = \{1, 1, 1, \dots\}.$$

On selvää, että F ei ole kunta, sillä se sisältää nollanjakajia:

$$\{1, 0, 0, \dots\}\{0, 1, 0, 0, \dots\} = \hat{0}.$$

Jokaiselle alkiolle $a \in F$ vakiojono

$$\hat{a} = \{a, a, a, \dots\}$$

on Cauchy-jono ja kuuluu siten joukkoon $\{F\}$. Täten $\{F\}$ sisältää alirenkaan, joka on isomorfinen joukolle F. Erityisen tärkeä joukko on P, joka on kaikkien nollajonojen kokoelma. Aiemmin huomattiin, että P on joukon $\{F\}$ osajoukko. Itse asiassa P on *ideaali* joukossa $\{F\}$. (Toisin sanoen P on alirengas siten, että kaikille $p \in P$ ja kaikille $a \in F$ pätee, että $ap \in P$.) Jos $\{a_n\}$ ja $\{b_n\}$ kuuluvat joukkoon P, niin myös $\{a_n \pm b_n\}$ kuuluu joukkoon P ja jos $\{a_n\}$ kuuluu joukkoon P ja $\{b_n\}$ on rajoitettu (erityisesti, jos se on Cauchy-jono), niin $\{a_n b_n\}$ kuuluu joukkoon P. (Lemma 3.4.(3))

Olkoon $\hat{F} = \{F\}/P$. Sen alkioita ovat joukon $(F, \|\cdot\|)$ Cauchy-jonojen ekvivalenssiluokat. Kahden Cauchy-jonon sanotaan olevan ekvivalentteja keskenään, jos niiden erotus on nollajono. Huomataan, että vakiojonot

$$\hat{a} = \{a, a, a, \dots\},$$

missä $a \in F$, kuuluvat eri ekvivalenssiluokkiin joukossa $\hat{F}$ eri alkion a arvoilla. Merkitään Cauchy-jonojen $\{a_n\}$ ekvivalenssiluokkaa $(\{a_n\})$, jolloin $(\{a_n\})$ on alkio joukosta $\hat{F}$. Joukko F ajatellaan joukon $\hat{F}$ osajoukkona ja alkio $a \in F$ samaistetaan alkion $(\hat{a}) \in \hat{F}$ kanssa.

Todistetaan seuraavaksi pieni aputulos, jota tarvitaan tulevan lauseen todistuksessa.

Lemma 4.2. *Jos $\{a_n\} \sim \{a'_n\}$ ja $\{b_n\} \sim \{b'_n\}$ ovat kaksi paria ekvivalentteja Cauchy-jonoja, niin silloin $\{a_n \pm b_n\} \sim \{a'_n \pm b'_n\}$ ja $\{a_n \cdot b_n\} \sim \{a'_n \cdot b'_n\}$.*

Todistus. Olkoon $\{a_n\} \sim \{a'_n\}$ ja $\{b_n\} \sim \{b'_n\}$ kaksi paria ekvivalentteja Cauchy-jonoja.

(i) Olkoon $\varepsilon/2 > 0$. Ekvivalenteille Cauchy-jonoille saadaan, että kaikilla $n > N_1$ pätee, että $\|a_n - a'_n\| < \varepsilon/2$ ja kaikilla $n > N_2$ pätee, että $\|b_n - b'_n\| < \varepsilon/2$. Tällöin kaikille $n > \max(N_1, N_2)$ pätee, että

$$\begin{aligned}\|(a_n \pm b_n) - (a'_n \pm b'_n)\| &= \|a_n - a'_n \pm b_n \mp b'_n\| \\ &\leq \|a_n - a'_n\| + \|\pm(b_n - b'_n)\| \\ &= \|a_n - a'_n\| + \|b_n - b'_n\| < \varepsilon/2 + \varepsilon/2 = \varepsilon.\end{aligned}$$

Tästä seuraa $\{a_n \pm b_n\} \sim \{a'_n \pm b'_n\}$. (Huomaa, että edellä joko molemmissa summataan tai vähennetään.)

(ii) Cauchy-jonot ovat rajoitettuja, joten on olemasa M_1 ja M_2 siten, että kaikille luvuille n pätee, että $\|a_n\| \leq M_1$ ja $\|b'_n\| \leq M_2$. Tällöin

$$\begin{aligned}\|a_n \cdot b_n - a'_n \cdot b'_n\| &= \|a_n \cdot b_n - a_n \cdot b'_n + a_n \cdot b'_n - a'_n \cdot b'_n\| \\ &\leq \|a_n(b_n - b'_n)\| + \|b'_n(a_n - a'_n)\| \\ &= \|a_n\|\|b_n - b'_n\| + \|b'_n\|\|a_n - a'_n\| \\ &\leq M_1\|b_n - b'_n\| + M_2\|a_n - a'_n\|.\end{aligned}$$

Olkoon $\varepsilon/2M_1 > 0$ ja $\varepsilon/2M_2 > 0$. Ekvivalenteille Cauchy-jonoille saadaan, että kaikilla $n > N_1$ pätee, että $\|a_n - a'_n\| < \varepsilon/2M_2$ ja kaikilla $n > N_2$ pätee, että $\|b_n - b'_n\| < \varepsilon/2M_1$. Tällöin kaikille $n > \max(N_1, N_2)$ pätee, että

$$\begin{aligned}\|a_n \cdot b_n - a'_n \cdot b'_n\| &\leq \cdots \leq M_1\|b_n - b'_n\| + M_2\|a_n - a'_n\| \\ &< M_1\frac{\varepsilon}{2M_1} + M_2\frac{\varepsilon}{2M_2} = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.\end{aligned}$$

Tästä seuraa $\{a_n \cdot b_n\} \sim \{a'_n \cdot b'_n\}$.

□

Lause 4.3. *Joukko $\hat{F}$ on kunta.*

Todistus. Määritellään joukon $\hat{F}$ laskuoperaatiot seuraavasti. Jos $\{a_n\} \in A$ ja $\{b_n\} \in B$, niin $A + B = (\{a_n + b_n\})$ ja $A \cdot B = (\{a_n \cdot b_n\})$. Tällöin joukko $\hat{F}$ on selvästi kommutatiivinen rengas yhteenlaskun neutraalialkiolla $(\hat{0})$ ja kertolaskun neutraalialkiolla $(\hat{1})$. Lemman 4.2 nojalla laskuoperaatiot eivät riipu edustajien valinnasta. Seuraavaksi todistetaan, että $\hat{F}$ on kunta. Olkoon A ekvivalenssiluokka joukosta $\hat{F}$ eri kuin nollaluokka $(\hat{0}) = P$. Olkoon $\{a_n\}$ Cauchy-jono joukosta A. Lemman 3.4(4) kohdan nojalla on olemassa positiivinen luku c ja positiivinen kokonaisluku N siten, että

$$\|a_n\| > c, \ \textit{kaikilla } n \geq N.$$

Määritellään uusi jono $\{a^*_n\}$ seuraavasti

$$a^*_n = \begin{cases} 0, & \text{jos } 1 \leq n \leq N-1 \\ 1/a_n, & \text{jos } n \geq N. \end{cases}$$

Väitetään, että tämä on Cauchy-jono. Jos n, $m \geq N$, niin

$$0 \leq \|a^*_m - a^*_n\| = \left\|\frac{1}{a_m} - \frac{1}{a_n}\right\| = \frac{\|a_m - a_n\|}{\|a_m\| \cdot \|a_n\|} \leq c^{-2}\|a_m - a_n\|.$$

Väite seuraa, sillä $\{a_n\}$ on Cauchy-jono, jolloin luvulle $\varepsilon/c^{-2} > 0$ on olemassa N siten, että kaikilla n, $m > N$ pätee, että $\|a_m - a_n\| < \varepsilon/c^{-2}$. Tästä saadaan

$$0 \leq \|a_m^* - a_n^*\| = \cdots \leq c^{-2}\|a_m - a_n\| < c^{-2}\frac{\varepsilon}{c^{-2}} = \varepsilon.$$

Merkitään jonon $\{a_n^*\}$ ekvivalenssiluokkaa A^{-1}. Tällöin

$$\{a_n\}\{a_n^*\} = \{\underbrace{0, \ldots, 0}_{N-1 \text{ nollaa}}, 1, 1, 1, \ldots\},$$

missä oikeanpuoleinen Cauchy-jono eroaa jonosta $(\hat{1})$ nollajonolla

$$\{\underbrace{-1, \ldots, -1}_{N-1 \text{ lukua } (-1)}, 0, 0, 0, \ldots\}.$$

Täten $AA^{-1} = (\hat{1})$, mikä todistaa, että $\hat{F}$ on kunta. □

Seuraavaksi laajennetaan normi $\|\cdot\|$ kunnasta F kuntaan $\hat{F}$.

Määritelmä 4.4. Mille tahansa alkiolle $A \in \hat{F}$ määritellään

$$\|A\| = \lim_{n\to\infty} \|a_n\|,$$

missä $\{a_n\}$ on Cauchy-jono joukosta A.

Näytetään seuraavaksi, että normi on hyvin määritelty. Normin raja-arvon olemassaolo tulee näyttää ja normi ei saa riippua Cauchy-jonon $\{a_n\} \in A$ valinnasta. Lemman 3.2 (c) kohdan nojalla

$$|\|a_n\| - \|a_m\|| \leq \|a_n - a_m\|,$$

mistä seuraa, että jono reaalilukuja $\{\|a_n\|\}$ on Cauchy-jono itseisarvolla. Koska reaalilukujen joukko $\mathbb{R}$ on täydellinen, niin normin $\|\cdot\|$ määrittelemä raja-arvo on olemassa. Seuraavaksi valitaan toinen jono $\{a_n'\} \in A$. Edellä olevalla epäyhtälöllä saadaan myös

$$0 \leq \lim_{n\to\infty} |\|a_n\| - \|a_n'\|| \leq \lim_{n\to\infty} \|a_n - a_n'\| = 0,$$

josta seuraa, että $\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|a_n'\|$.

Lemma 4.5. *$\|\cdot\|$ on normi kunnassa $\hat{F}$.*

Todistus. Seuraavaksi täytyy todistaa kolme ominaisuutta, jotka on esitelty Määritelmässä 3.1.

(1) Jos $A = (\hat{0})$, niin silloin $\{a_n\}$ on nollajono ja $\|A\| = 0$. Jos $A \neq (\hat{0})$ ja $A = (\{a_n\})$, niin silloin on olemassa positiivinen luku c ja positiivinen kokonaisluku N siten, että kaikille $n \geq N$ pätee, että $\|a_n\| \geq c > 0$. Tällöin $\|A\| > 0$.

(2) Olkoon $A = (\{a_n\})$ ja $B = (\{b_n\})$. Reaalilukujen raja-arvojen ominaisuuksilla,

$$\begin{aligned}\|AB\| &= \lim_{n\to\infty} \|a_n b_n\| = \lim_{n\to\infty} \|a_n\|\|b_n\| \\ &= \lim_{n\to\infty} \|a_n\| \lim_{n\to\infty} \|b_n\| = \|A\|\|B\|.\end{aligned}$$

(3) Olkoon $A = (\{a_n\})$ ja $B = (\{b_n\})$. Reaalilukujen raja-arvojen ominaisuuksilla,

$$\begin{aligned}\|A + B\| &= \lim_{n\to\infty} \|a_n + b_n\| \leq \lim_{n\to\infty} \|a_n\| + \|b_n\| \\ &= \lim_{n\to\infty} \|a_n\| + \lim_{n\to\infty} \|b_n\| = \|A\| + \|B\|.\end{aligned}$$

□

Nyt voidaan määritellä rajoitettu jono, Cauchy-jono ja nollajono kunnassa $\hat{F}$ normin $\|\cdot\|$ suhteen.

Lause 4.6. *Kunta $\hat{F}$ on täydellinen normilla $\|\cdot\|$ ja F on kunnan $\hat{F}$ tiheä osajoukko.*

Todistus. Ensiksi todistetaan lauseen toinen osa. Olkoon $A \in \hat{F}$ ja olkoon $\{a_m\}$ kunnan F Cauchy-jono, joka edustaa ekvivalenssiluokkaa A. Olkoon jokaista positiivista kokonaislukua n vastaava vakiojono $\hat{a}_n$. Tällöin jono $\{a_m - a_n\}_{m=1}^{\infty}$ edustaa jonoa $A - (\hat{a}_n)$ ja koska $\{a_m\}$ on Cauchy-jono voidaan kirjoittaa

$$\lim_{n\to\infty} \|A - (\hat{a}_n)\| = \lim_{n,m\to\infty} \|a_m - a_n\| = 0. \tag{4.1}$$

Tämä todistaa, että F on tiheä kunnassa $\hat{F}$. Olkoon $\{A_n\} = \{A_1, A_2, \dots\}$ Cauchy-jono kunnassa $\hat{F}$. Koska F on tiheä kunnassa $\hat{F}$, niin jokaiselle A_n on olemassa alkio $a_n \in F$ siten, että

$$\|A_n - (\hat{a}_n)\| < \frac{1}{n}. \tag{4.2}$$

Tällöin $\{A_n - (\hat{a}_n)\}$ on nollajono ja siten Cauchy-jono kunnassa $\hat{F}$. Koska

$$\{(\hat{a}_n)\} = \{A_n\} - \{A_n - (\hat{a}_n)\},$$

niin $\{(\hat{a}_n)\}$ on Cauchy-jono kunnassa $\hat{F}$, mutta koska sen alkiot kuuluvat kuntaan F, niin $\{a_n\}$ on Cauchy-jono kunnassa F. Olkoon Cauchy-jonon $\{a_n\}$ ekvivalenssiluokka A (aiemmilla merkinnöillä $(\{a_n\}) = A$). Lausekkeista (4.1) ja (4.2) seuraa, että jonot $\{A - (\hat{a}_n)\}$ ja $\{A_n - (\hat{a}_n)\}$ ovat nollajonoja kunnassa $\hat{F}$ ja tällöin niiden erotus

$$\{A - A_n\} = \{A - (\hat{a}_n)\} - \{A_n - (\hat{a}_n)\}$$

on nollajono, kunnassa $\hat{F}$. Tästä seuraa, että

$$\lim_{n\to\infty} \|A - A_n\| = 0,$$

mutta tämä tarkoittaa juuri sitä, että $A = \lim_{n\to\infty} A_n$. □

Lemma 4.7. *Laskuoperaatiot kunnassa $\hat{F}$ saadaan kunnasta F jatkuvuuden seurauksena. Toisin sanoen, jos*

$$A = \lim_{n\to\infty} (\hat{a}_n), \;\; B = \lim_{n\to\infty} (\hat{b}_n),$$

niin

$$A + B = \lim_{n\to\infty} (\hat{a}_n + \hat{b}_n), \;\; A \cdot B = \lim_{n\to\infty} (\hat{a}_n \cdot \hat{b}_n).$$

Todistus. Olkoon $A = \lim_{n\to\infty}(\hat{a}_n)$ ja $B = \lim_{n\to\infty}(\hat{b}_n)$, niin tällöin jonot $\{A - (\hat{a}_n)\}$ ja $\{B - (\hat{b}_n)\}$ ovat nollajonoja ja

$$\lim_{n\to\infty} \|A - (\hat{a}_n)\| = 0 \text{ ja } \lim_{n\to\infty} \|B - (\hat{b}_n)\| = 0.$$

Tällöin

$$\begin{aligned}\lim_{n\to\infty} \|A + B - (\hat{a}_n + \hat{b}_n)\| &= \lim_{n\to\infty} \|A - (\hat{a}_n) + B - (\hat{b}_n)\| \\ &\le \lim_{n\to\infty} \|A - (\hat{a}_n)\| + \lim_{n\to\infty} \|B - (\hat{b}_n)\| = 0\end{aligned}$$

ja

$$\begin{aligned}
\lim_{n\to\infty} \|A \cdot B - (\hat{a}_n \cdot \hat{b}_n)\| &= \lim_{n\to\infty} \|A \cdot B - A \cdot (\hat{b}_n) + A \cdot (\hat{b}_n) - (\hat{a}_n) \cdot (\hat{b}_n)\| \\
&= \lim_{n\to\infty} \|A \cdot [B - (\hat{b}_n)] + (\hat{b}_n) \cdot [A - (\hat{a}_n)]\| \\
&\leq \lim_{n\to\infty} \|A\|\|B - (\hat{b}_n)\| + \lim_{n\to\infty} \|(\hat{b}_n)\|\|A - (\hat{a}_n)\| \\
&= \lim_{n\to\infty} \|A\| \lim_{n\to\infty} \|B - (\hat{b}_n)\| + \lim_{n\to\infty} \|(\hat{b}_n)\| \lim_{n\to\infty} \|A - (\hat{a}_n)\| \\
&= \|A\| \cdot 0 + \|B\| \cdot 0 = 0.
\end{aligned}$$

($\|A\| \cdot 0 = 0$, koska Cauchy-jonot ovat rajoitettuja.) Kahdesta edellisestä epäyhtälöstä saadaan, että $\lim_{n\to\infty} \|A - (\hat{a}_n)\| = 0$ ja $\lim_{n\to\infty} \|B - (\hat{b}_n)\| = 0$. $\square$

5. P-adisten lukujen kunta $\mathbb{Q}_p$

Perusesimerkki rationaalilukujen $\mathbb{Q}$ normista on itseisarvo $|\cdot|$. Tästä johdettu metriikka $d(x,y) = |x-y|$ on euklidinen etäisyys lukusuoralla ja kuten kappaleessa 2 kerrottiin, niin reaalilukujen kunta $\mathbb{R}$ on rationaalilukujen $\mathbb{Q}$ täydellistys tällä normilla.

Nyt voidaan miettiä, onko euklidinen etäisyys rationaaliluvuille kaikista "luonnollisin" tapa ilmaista etäisyyttä? Onko mitään muuta tapaa kuvata rationaalilukujen läheisyyttä? Käy ilmi, että toinenkin tapa löytyy.

Uusi tapa mitata rationaalilukujen etäisyyttä seuraa aritmeettisesta konstruktiosta.

Olkoon $p \in \mathbb{N}$ alkuluku ja olkoon kuvaus $|\cdot|_p$ rationaalilukujen joukosta:

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x}, & \text{jos } x \neq 0, \\ 0, & \text{jos } x = 0, \end{cases} \tag{5.1}$$

missä

$$\mathrm{ord}_p x = \begin{cases} \text{suurin luku } k \text{ siten, että } p^k | x, \text{ jos } x \in \mathbb{Z}, \\ \mathrm{ord}_p a - \mathrm{ord}_p b, \text{ jos } x = a/b,\ a, b \in \mathbb{Z},\ b \neq 0 \end{cases}$$

on luvun x *p-adinen kertaluku* (kutsutaan myös *p-adiseksi arvoksi*).

Huomautus 5.1. Huomaa, että normi $|\cdot|_p$ voi saada vain diskreettejä arvoja joukosta $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$.

Huomautus 5.2. Jos $a, b \in \mathbb{N}$, niin $a \equiv b \pmod{p^n}$, jos ja vain jos $|a-b|_p \leq 1/p^n$.

Lemma 5.3. *$|\cdot|_p$ on epäarkhimedinen normi rationaalilukujen joukossa.*

Todistus. Kohta (1) Määritelmästä 3.1 on selvä ja $|x|_p = 0$, jos ja vain jos $x = 0$. Kohta (2) seuraa tuloksesta

$$\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y). \tag{5.2}$$

Tällöin

$$|xy|_p = p^{-\mathrm{ord}_p(xy)} = p^{-\mathrm{ord}_p(x) - \mathrm{ord}_p(y)} = p^{-\mathrm{ord}_p(x)} p^{-\mathrm{ord}_p(y)} = |x|_p |y|_p.$$

Todistetaan seuraavaksi kohta (3). Jos $x = 0$ tai $y = 0$, niin (3) on triviaali, joten oletetaan, että $x, y \neq 0$. Olkoon $x = a/b$ ja $y = c/d$. Tällöin

$$x + y = \frac{ad + bc}{bd}$$

ja

$$\begin{aligned} \mathrm{ord}_p(x+y) &= \mathrm{ord}_p(ad+bc) - \mathrm{ord}_p(bd) \\ &\geq \min(\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)) - \mathrm{ord}_p b - \mathrm{ord}_p d \\ &= \min(\mathrm{ord}_p a - \mathrm{ord}_p b, \mathrm{ord}_p c - \mathrm{ord}_p d) \\ &= \min(\mathrm{ord}_p x, \mathrm{ord}_p y). \end{aligned}$$

Tästä seuraa, että

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

Edellisestä huomataan myös, että $|\cdot|_p$ toteuttaa vahvan kolmioepäyhtälön ja on siten epäarkhimedinen. $\square$

Huomautus 5.4. Myöhemmin nähdään, että rationaalilukujen joukko $\mathbb{Q}$ ei ole täydellinen normilla $|\cdot|_p$.

Huomautus 5.5. Normi $|\cdot|_{p_1}$ ei ole ekvivalentti normin $|\cdot|_{p_2}$ kanssa, jos p_1 ja p_2 ovat eri alkulukuja (Jos otetaan jono $x_n = (p_1/p_2)^n$, niin $|x_n|_{p_1} \to 0$, mutta $|x_n|_{p_2} \to \infty$).

Seuraavaksi määritellään kappaleen keskeisin asia. Olkoon p alkuluku. Määritellään, että joukko $\mathbb{Q}_p$ on joukon $\mathbb{Q}$ täydellistys normilla $|\cdot|_p$, joka on määritelty Lausekkeessa (5.1). P-adinen normi on laajennettu joukkoon $\mathbb{Q}_p$ Määritelmän 4.4 mukaan ja ($\mathbb{Q}_p$, $|\cdot|_p$) on täydellinen normilla varustettu kunta. Joukkoa $\mathbb{Q}_p$ kutsutaan *p-adisten lukujen kunnaksi.* Joukon $\mathbb{Q}_p$ alkiot ovat joukon $\mathbb{Q}$ Cauchy-jonojen ekvivalenssiluokkia, kun käytetään laajennettua p-adista normia. Kuten aiemminkin on todettu, niin joukko $\mathbb{Q}$ voidaan samaistaa joukon $\mathbb{Q}_p$ osajoukon kanssa, joka koostuu vakioiden Cauchy-jonojen ekvivalenssiluokista.

Olkoon alkiolle $a \in \mathbb{Q}_p$ Cauchy-jono rationaalilukuja $\{a_n\}$, joka edustaa alkiota a. Tällöin määritelmän mukaan

$$|a|_p = \lim_{n\to\infty} |a_n|_p. \tag{5.3}$$

Tällöin normin $|\cdot|_p$ arvojoukko on sama joukoille $\mathbb{Q}_p$ ja $\mathbb{Q}$ ja se on $\{p^n,\, n \in \mathbb{Z}\} \cup \{0\}$. Tämä ilmiö eroaa selvästi euklidisen itseisarvon tapauksesta, joka saa kaikki positiiviset reaalilukuarvo, kun se laajennetaan rationaaliluvuilta $\mathbb{Q}$ reaaliluvuille $\mathbb{R}$. Lisäksi, jos $|a|_p \neq 0$, niin normien jonon $\{|a_n|_p\}$ arvojen tulee vakiintua riittävän suurilla luvun n arvoilla.

Olkoon sarja

$$\frac{d_{-m}}{p^m} + \frac{d_{-m+1}}{p^{m-1}} + \cdots + d_0 + d_1 p + d_2 p^2 + \ldots, \tag{5.4}$$

missä $0 < d_{-m} < p$ ja $0 \le d_i < p$ kaikille $i > -m$. Sen osittaiset summat muodostavat Cauchy-jonon, sillä kaikille $\varepsilon > 0$ voidaan valita N siten, että $p^{-N} < \varepsilon$ ja kaikille $k > n > N$ pätee, että

$$\left|\sum_{-m}^{k} d_i p^i - \sum_{-m}^{n} d_i p^i\right|_p = \left|\sum_{n+1}^{k} d_i p^i\right|_p \le \max_{n<i\le k}(|d_i p^i|_p) \le p^{-N} < \varepsilon.$$

Tällöin jokainen sarja, joka on muotoa (5.4) esittää kunnan $\mathbb{Q}_p$ alkiota. Käänteinen väite pitää myös paikkaansa. Näytetään, että jokainen Cauchy-jonojen, joukosta $\mathbb{Q}$, ekvivalenssiluokka sisältää yksikäsitteisen *kanonisen* Cauchy-jono edustajan, joka on muotoa (5.4) olevan sarjan osittaisten summien jono.

Edeltävän käsitteen konstruointiin tarvitaan seuraavaa lemmaa.

Lemma 5.6. *Jos $x \in \mathbb{Q}$ ja $|x|_p \le 1$, niin jokaiselle luvulle i on olemassa kokonaisluku $\alpha \in \mathbb{Z}$ siten, että $|\alpha - x|_p \le p^{-i}$. Kokonaisluku α voidaan valita joukosta $\{0, 1, 2, \ldots, p^i - 1\}$, jolloin sen valinta on yksikäsitteinen.*

Todistus. Olkoon $x = a/b$, missä a ja b ovat keskenään jaottomia (tällöin merkitään $(a, b) = 1$). Koska $|x|_p \le 1$, niin siitä seuraa, että luku p ei jaa lukua b, jolloin b ja

p^i ovat keskenään jaottomia. Tällöin voidaan löytää kokonaisluvut m ja n (Bezout'n Lemman nojalla) siten, että $mb + np^i = 1$. Olkoon $\alpha = am$. Tällöin

$$\begin{aligned}|\alpha - x|_p &= |am - a/b|_p = |a/b|_p|mb-1|_p \\ &\leq |mb-1|_p = |np^i|_p = |n|_p p^{-i} \leq p^{-i}.\end{aligned}$$

Lopuksi käyttäen vahvaa kolmioepäyhtälöä voidaan lisätä luvun p^i monikertoja kokonaislukuun α, jolloin saadaan kokonaisluku lukujen 0 ja p^i väliltä, jolle $|\alpha - x|_p \leq p^{-i}$ pätee. □

Lause 5.7. *Jokaisella ekvivalenssiluokalla a kunnassa $\mathbb{Q}_p$, joka toteuttaa ehdon $|a|_p \leq 1$ on tasan yksi edustaja $\{a_n\}$ siten, että*

(1) $a_i \in \mathbb{Z}$, $0 \leq a_i < p^i$, *kun* $i = 1, 2, \ldots$
(2) $a_i \equiv a_{i+1} \, (mod p^i)$, *kun* $i = 1, 2, \ldots$

Todistus. Olkoon $\{b_i\}$ Cauchy-jono, joka edustaa alkiota a. Halutaan löytää ekvivalentti jono $\{a_n\}$, joka toteuttaa ehdot (1) ja (2). Koska

$$|b_i|_p \longrightarrow |a|_p \leq 1, \text{ kun } i \to \infty,$$

niin poistamalla useita alkuperäisiä termejä tarpeen mukaan, voidaan olettaa, että $|b_i|_p \leq 1$ kaikilla luvuilla i.

Kaikille luvuille $j = 1, 2, \ldots$ on olemassa positiivinen kokonaisluku $N(j)$ siten, että

$$|b_i - b_{i'}|_p \leq p^{-j}, \text{ kaikilla } i, i' \geq N(j).$$

Jono $N(j)$ voidaan valita siten, että se kasvaa, kun luku j kasvaa, jolloin $N(j) \geq j$.

Lemman 5.6 nojalla voidaan valita kokonaisluvut a_j, $0 \leq a_j < p^j$ siten, että

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

Näytetään, että $a_j \equiv a_{j+1} \, (\mathrm{mod}\, p^j)$ ja $(b_i) \sim (a_j)$.

Ensimmäinen väite seuraa, kun

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

jolloin $a_j \equiv a_{j+1} \, (\mathrm{mod}\, p^j)$.

Toisen väitteen todistukseen valitaan mikä tahansa j, jolloin luvulle $i \geq N(j)$ pätee, että

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

Tällöin

$$|a_i - b_i|_p \longrightarrow 0, \text{ kun } i \to \infty.$$

Seuraavaksi todistetaan yksikäsitteisyys. Jos $\{a'_n\}$ on eri jono, joka toteuttaa lauseen ehdot siten, että $a_{i_0} \neq a'_{i_0}$, joillain luvun i_0 arvoilla, niin silloin $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$,

koska molemmat luvut a_{i_0} ja a'_{i_0} ovat lukujen 0 ja p^{i_0} väliltä. Tällöin kohdasta (2) seuraa, että

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}}.$$

Toisin sanoen $a_i \not\equiv a'_i \pmod{p^{i_0}}$. Mutta tämä tarkoittaa juuri sitä, että

$$|a_i - a'_i|_p > \frac{1}{p^{i_0}}, \ \textit{kaikilla } i \geq i_0,$$

mistä seuraa, että $(a_i) \not\sim (a'_i)$. □

Jos $a \in \mathbb{Q}_p$, jolle pätee $|a|_p \leq 1$, niin on kätevää kirjoittaa edustavan jonon termit a_i, jotka on saatu edellisestä lauseesta seuraavasti:

$$a_i = d_0 + d_1 p + \cdots + d_{i-1} p^{i-1},$$

missä kertoimet d_i ovat kokonaislukuja joukosta $\{0, 1, \ldots, p-1\}$. Edellisen lauseen ehto (2) tarkoittaa juurikin sitä, että

$$a_{i+1} = d_0 + d_1 p + \cdots + d_{i-1} p^{i-1} + d_i p^i,$$

missä "p-adiset numerot" numerosta d_0 numeroon d_{i-1} ovat samat kuin luvulle a_i. Tällöin luku a esitetään suppenevalla (p-adisen normin suhteen) sarjalla

$$a = \sum_{n=0}^{\infty} d_n p^n,$$

joka voidaan ajatella lukuna, joka on kirjoitettu kannassa p, joka jatkuu äärettömästi vasemmalle tai sillä on äärettömän monta p-adista numeroa. Kirjoitetaan

$$a = \ldots d_n \ldots d_2 d_1 d_0$$

ja kutsutaan tätä luvun a *kanoniseksi p-adiseksi laajennukseksi* tai *kanoniseksi muodoksi.*

Jos $|a|_p > 1$, niin luku a voidaan kertoa luvun p potenssilla (merkitään $p^m = |a|_p$), jollon saadaa p-adinen luku $a' = ap^m$, joka toteuttaa ehdon $|a'|_p = 1$.

Tällöin voidaan kirjoittaa

$$a = \sum_{n=-m}^{\infty} d_n p^n, \tag{5.5}$$

missä $d_{-m} \neq 0$ ja $d_i \in \{0, 1, 2, \ldots, p-1\}$. Se ilmaisee p-adisen luvun a murtolukuna kannassa p äärettömän monella p-adisella numerolla ennen pistettä ja äärellisen monella numerolla pisteen jälkeen:

$$a = \ldots d_n \ldots d_2 d_1 d_0 . d_{-1} \ldots d_{-m}; \tag{5.6}$$

tätä esitystä kutsutaan luvun a *kanoniseksi p-adiseksi laajennukseksi.*

Seuraava lemma kertoo, että p-adisen luvun normin määrittää ensimmäisen nollasta eroavan kertoimen indeksi sen kanonisessa laajennuksessa.

Lemma 5.8. *Jos $a = \sum_{n=0}^{\infty} d_n p^n$, missä $d_n = 0$ kaikille $0 \leq n < k$ ja $d_k \neq 0$, niin $|a|_p = p^{-k}$ ja jos $a = \sum_{n=-m}^{\infty} d_n p^n$, missä $d_{-m} \neq 0$, niin $|a|_p = p^m$.*

Todistus. Kaavan (5.3) määritelmän mukaan $|a|_p$ on sarjaesityksensä osittaisten summien p-adisten normien jonon raja-arvo. Ensimmäisessä tapauksessa olkoon vakiojono $p^{-k}, p^{-k}, p^{-k}, \ldots$. Tällöin $|d_k|_p = 1$ (huomaa, että $0 < d_k < p$) ja vahvan kolmioepäyhtälön nojalla seuraa, että $|a|_p = p^{-k}$. Jos $a = \sum_{n=-m}^{\infty} d_n p^n$, missä $d_{-m} \neq 0$, niin samalla päättelyllä saadaan, että $|a|_p = p^m$. □

Lisäksi huomio *kertaluvusta*, joka määriteltiin Kappaleen 5 alussa, rationaaliluvuille. Tämä voidaan laajentaa kaikille p-adisille luvuille: luvulle $a \in \mathbb{Q}_p$ pätee, että $\mathrm{ord}_p(a)$ on sama kuin luvun a kanonisen laajennuksen ensimmäinen nollasta eroava kerroin.

Huomautus 5.9. Lauseen 5.7 väite yksikäsitteisyydestä ei päde luvuille päättymättömässä murtolukukehitelmässä kannassa g, joka esiteltiin Kappaleessa 2. Esimerkiksi olkoon $g = 10$, jolloin

$$1.0000\cdots = 0.9999\ldots.$$

Tällaisia poikkeuksia ei ole olemassa p-adisessa tapauksessa. Jos kaksi p-adista laajennusta suppenee samaan p-adiseen lukuun, niin ne ovat samat. Toisin sanoen kaikki niiden numerot ovat samat.

Määritelmä 5.10. P-adisen luvun $a \in \mathbb{Q}_p$ sanotaan olevan *p-adinen kokonaisluku*, jos sen kanoninen laajennus sisältää vain positiivisia (nolla mukaan lukien) potensseja luvulle p.

P-adisten kokonaislukujen joukkoa merkitään $\mathbb{Z}_p$, jolloin

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \right\}.$$

Nähdään, että $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$. Koska $\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i\}$, niin Lemman 5.8 mukaan $|a|_p = p^{-i}$, missä $i \in \{0, 1, 2, \ldots\}$. Tällöin $|a|_p = p^{-i} \leq 1$.

Lause 5.11. *Jokaisella p-adisen kokonaisluvun päättymättömällä jonolla on suppeneva osajono.*

Todistus. Muistetaan, että jonon $\{x_n\}$ *osajono* $\{x_{n_k}\}$ saadaan jonolla positiivisia kokonaislukuja $\{n_k\}$ siten, että $n_1 < n_2 < n_3 < \ldots$.

Olkoon $\{x_n\}$ jono joukossa $\mathbb{Z}_p$. Kirjoitetaan jokainen termi kanonisessa laajennuksessa,

$$x_k = \ldots a_2^k a_1^k a_0^k.$$

Koska numerolle a_0^k on vain äärellisen monta vaihtoehtoa (ne ovat $0, 1, \ldots, p-1$), niin löydetään $b_0 \in \{0, 1, \ldots, p-1\}$ ja päättymättömän jonon $\{x_n\}$ osajono $\{x_{0k}\}$ siten, että kaikkien jonojen x_{0k} ensimmäinen numero on aina b_0. Samanlaisella ajattelulla löydetään $b_1 \in \{0, 1, \ldots, p-1\}$ ja jonon $\{x_{0k}\}$ osajono $\{x_{1k}\}$, jonka kaksi ensimmäistä numeroa ovat $b_1 b_0$. Tätä prosessia voidaan jatkaa, jolloin saadaan numerot $b_0, b_1, b_2, \ldots$ ja jono jonoja

$$\begin{array}{l} x_{00}, x_{01}, x_{02}, \ldots, x_{0s}, \ldots, \\ x_{10}, x_{11}, x_{12}, \ldots, x_{1s}, \ldots, \\ x_{20}, x_{21}, x_{22}, \ldots, x_{2s}, \ldots, \\ \ldots\ldots\ldots\ldots\ldots \end{array}$$

siten, että jokainen jono on edellisen jonon osajono ja siten, että jokainen jono riviltä $(j+1)$ alkaa $b_j \dots b_1 b_0$. Jokaiselle luvulle $j = 1, 2, \dots$ pätee

$$x_{jj} \in \{x_{j-1j}, x_{j-1j+1}, \dots\}$$

ja $x_{00} \in \{x_0, x_1, x_2, \dots\}$. Tällöin diagonaalinen jono $x_{00}, x_{11}, \dots$ on vieläkin alkuperäisen jonon osajono ja selvästi suppenee kohti jonoa $\dots b_3 b_2 b_1 b_0$. □

Huomautus 5.12. Edellisen laajennus rajoitetuille jonoille ei ole kovin vaikeaa ja se todistetaan seuraavassa lemmassa. Sama tulos pätee reaalilukujen rajoitetuille jonoille (Bolzano-Weierstrassin Lause) ja reaalilukujen jonon $0 \leq x_n \leq 1$ todistusta voidaan soveltaa edeltävän todistukseen käyttäen reaalilukujen päättymätöntä desimaalimurtoluku esitystä.

Lemma 5.13. *Jokaisella rajoitetulla jonolla $\{x_n\}$, jossa $x_n \in \mathbb{Q}_p$ on suppeneva osajono.*

Todistus. Muistetaan, että jonon $\{x_n\}$ osajono $\{x_{n_k}\}$ saadaan jonolla positiivisia kokonaislukuja $\{n_k\}$ siten, että $n_1 < n_2 < n_3 < \dots$.

Olkoon $\{x_n\}$, jossa $x_n \in \mathbb{Q}_p$. Lauseen 5.11 nojalla tulos pätee, kun jonon $\{x_n\}$ termeille pätee $x_n \in \mathbb{Z}_p$. Oletetaan siis, että jonojen termit eivät ole p-adisia kokonaislukuja ja ovat rajoitettuja, jolloin on olemassa C siten, että $|x_n|_p = p^m \leq C$, jollain kokonaisluvulla m ja ne ovat siten Lausekkeen (5.6) muodossa

$$x_k = \dots d_2^k d_1^k d_0^k . d_{-1}^k \dots d_{-m}^k.$$

Koska numerolle d_{-m}^k on vain äärellisen monta vaihtoehtoa, niin tällöin löydetään $b_{-m} \in \{0, 1, \dots, p-1\}$ ja päättymättömän jonon $\{x_n\}$ osajono $\{x_{-mk}\}$ siten, että kaikkien jonojen x_{-mk} ensimmäinen numero on aina b_{-m}. Tämä jatkuu vastaavasti kuin Lauseen 5.11 todistuksessa, jolloin lopuksi saadaan, että diagonaalinen jono $x_{(-m)(-m)}, \dots, x_{(-1)(-1)}, x_{00}, x_{11}, \dots$ on vieläkin alkuperäisen jonon osajono ja selvästi suppenee kohti jonoa $\dots b_1 b_0 b_{-1} \dots b_{-m}$. □

Lemma 5.14. *Avaruuden $\mathbb{Z}_p$ kardinaalisuus on kontinuumi.*

Todistus. Joukot $\mathbb{Z}_p$ ja $[0, 1]$ ovat ylinumeroituvia ja tämä todistetaan Cantorin lävistäjämenetelmällä, joka esitellään Lemmassa 10.2, mutta tässä kohdassa se ohitetaan.

Olkoon kuvaus $f : \mathbb{Z}_p \to [0, 1]$,

$$f(a) = \frac{1}{a} = \frac{1}{\sum_{i=0}^{\infty} d_i p^i},$$

missä $d_i \in \{0, 1, \dots, p-1\}$. Tällöin kuvaus f on bijektiivinen, p-adisten lukujen yksikäsitteisen esityksen vuoksi. Tästä seuraa, että avaruuden $\mathbb{Z}_p$ kardinaalisuus on sama kuin suljetun välin $[0, 1]$, jonka kardinaalisuus on kontinuumi (sama kuin reaalilukujen joukon). □

6. Joukon $\mathbb{Q}_p$ aritmeettiset laskutoimitukset

P-adinen laajennus sallii aritmeettisten laskutoimitusten käytön joukossa $\mathbb{Q}_p$ hyvin samoin tavoin kuin joukossa $\mathbb{R}$. Lisäksi huomataan, että laskutoimitukset ovat helpompia joukossa $\mathbb{Q}_p$ kuin joukossa $\mathbb{R}$. Olkoon

$$a = \sum_{n=-m}^{\infty} a_n p^n, \ b = \sum_{n=-m}^{\infty} b_n p^n,$$

missä a_n ja b_n ovat p-adisia numeroita, $a_{-m} \neq 0$, mutta mahdollisesti yksi tai useampi numeroista $b_{-m}, b_{-m+1}, \ldots$ on nolla. Tällöin

$$a \pm b = \sum_{n=-m}^{\infty} (a_n \pm b_n) p^n$$

on suppeneva sarja, mutta se ei yleisesti ole kuitenkaan kanonisessa muodossa (5.5). Palauttaminen kanoniseen muotoon Lauseen 5.7 tavoin vastaa yleistä summaamista (tai vähentämistä) oikealta vasemmalle sovellettuna p-adisiin lukuihin muodossa (5.6) ja käyttää muistilukuja (saman tapaisia kuin desimaalimurtoluvuille käytettäessä).

Havainnollistaaksemme summausta, etsitään luvun -1 kanoninen p-adinen laajennus joukossa $\mathbb{Q}_p$. Joukossa $\mathbb{Q}_p$ pätee, että $1 = \ldots 00001$. Olkoon $a = \ldots a_3 a_2 a_1 a_0$, joka toteuttaa Lausekkeen $1 + a = 0$ (Tällöin $a = -1$). Alkaen oikealta täytyy päteä $1 + a_0 \equiv 0 \pmod{p}$, mutta koska a_0 kuuluu joukkoon $\{0, 1, \ldots, p-1\}$, niin ainut tapa mahdollistaa tämä on $1 + a_0 = p$ ja ottaa luku 1 muistiin. Tällöin $a_0 = p - 1$. Jatkamalla tätä prosessia nähdään että kaikki numerot a_n ovat $p - 1$. Toisin sanoen

$$-1 = \ldots (p-1)(p-1)(p-1).$$

Kertolasku suoritetaan samantapaisella tavalla. Olkoon

$$a = \sum_{n=-m}^{\infty} a_n p^n, \ b = \sum_{n=-k}^{\infty} b_n p^n$$

kanonisessa muodossa. Kertomalla sarjat termeittäin ja uudelleen järjestelemällä termit saadaan

$$ab = \sum_{n=-m-k}^{\infty} u_n p^n,$$

missä

$$\begin{aligned} u_{-m-k} &= a_{-m} b_{-k}, \\ u_{-m-k+1} &= a_{-m+1} b_{-k} + a_{-m} b_{-k+1}, \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Tämä sarja ei taas yleisesti ole kanonisessa muodossa, mutta voidaan Lemman 5.7 tapaan palauttaa sellaiseen muotoon. Tämä vastaa yleistä kertolaskua tehtynä p-adisille luvuille, jotka ovat kanonisessa muodossa (5.6).

Havainnollistaaksemme jakamista, olkoon a, $b \in \mathbb{Q}_p$ ja $b \neq 0$. Voidaan olettaa, että $b \in \mathbb{Z}_p$, $b = \ldots b_2 b_1 b_0$, missä $b_0 \neq 0$, kun

$$a = \ldots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \ldots a_{-k}$$

on mielivaltainen p-adinen luku. Koska $b_0 \neq 0$ ja jäännösluokkarengas $\mathbb{Z}/p\mathbb{Z}$ alkuluvulle p on kunta, niin aina voidaan löytää kokonaisluku $c_{-k} \in \{0, 1, \ldots, p-1\}$ siten, että $c_{-k}b_0 \equiv a_{-k} \pmod{p}$. Jatkamalla yleistä jakolaskua (vähennyslaskun kohdassa tarvittaessa lainataan seuraavasta numerosta ja kertolaskussa siirretään luvun p monikerrat seuraavaan numeroon) saadaan osamäärä a/b kanonisessa muodossa.

Tästä seuraa, että jos $a = \ldots a_2 a_1 a_0$ on p-adinen kokonaisluku, missä $a_0 \neq 0$, niin sen kertolaskun käänteisalkio on myös p-adinen kokonaisluku. (Tämä p-adisten kokonaislukujen ominaisuus voi vaikuttaa aluksi oudolta, mutta se on kieltämättä kätevä tulos.) Toisaalta koska

$$p \cdot \sum_{i=0}^{\infty} a_i p^i = a_0 p + a_1 p^2 + \cdots \neq 1 + 0p + 0p^2 + \ldots,$$

niin luvulla p ei ole kertolaskun käänteisalkiota joukossa $\mathbb{Z}_p$, mutta kertolaskun käänteisalkio luvulle p löytyy joukosta $\mathbb{Q}_p$. Koska

$$p \cdot \sum_{i=-m}^{\infty} a_i p^i = a_{-m} p^{-m+1} + \cdots + a_{-1} p^0 + a_0 p + a_1 p^2 + \cdots = 0p^{-m+1} + \cdots + 1 + 0p + 0p^2 + \ldots,$$

niin käänteisalkio on löytynyt. Samantapaisella argumentilla, millä näytettiin ettei luvulla p ole käänteisalkiota joukossa $\mathbb{Z}_p$ näytetään, että p-adisella kokonaisluvulla, jonka ensimmäinen numero a_0 on nolla, ei ole kertolaskun käänteisalkiota joukossa $\mathbb{Z}_p$. Tästä tehdään yhteenveto seuraavassa lemmassa.

Lemma 6.1. *P-adisella kokonaisluvulla*

$$a = \ldots a_1 a_0 \in \mathbb{Z}_p$$

on kertolaskun käänteisalkio joukossa $\mathbb{Z}_p$, jos ja vain jos $a_0 \neq 0$.

Todistus. Olkoon $a = \ldots a_1 a_0 \in \mathbb{Z}_p$, $b = \ldots b_1 b_0 \in \mathbb{Z}_p$ ja tehdään vastaoletus, jolloin $a_0 = 0$. Tällöin

$$ab = \left(\sum_{i=0}^{\infty} a_i p^i \right) \left(\sum_{i=0}^{\infty} b_i p^i \right) = a_0 b_0 + a_1 b_0 p + a_0 b_1 p + a_1 b_1 p^2 + \ldots.$$

Ainut tapa saada luku yksi edellisestä summasta on, että olisi $a_0 b_0 = 1$, mutta koska $a_0 = 0$, niin $a_0 b_0 = 0 \neq 1$ kaikilla $b_0 \in \{0, 1, \ldots, p-1\}$. □

Merkitään joukon $\mathbb{Z}_p$ kääntyvien alkioiden joukkoa $\mathbb{Z}_p^\times$,

$$\mathbb{Z}_p^\times = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0 \right\}.$$

Tätä joukkoa kutsutaan myös *p-adisten yksiköiden* joukoksi. Lemmasta 5.8 seuraa, että

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}.$$

Seuraava lemma seuraa suoraan p-adisen normin määritelmästä ja edeltävästä p-adisten yksiköiden joukon esityksestä.

Lemma 6.2. *Olkoon x p-adinen luku, jonka p-adinen normi on p^{-n}. Tällöin luku x voidaan kirjoittaa tulona $x = p^n u$, missä $u \in \mathbb{Z}_p^\times$.*

Huomaa, että aritmeettiset laskutoimitukset joukossa $\mathbb{Q}_p$ laajentavat tavanomaiset aritmeettiset laskutoimitukset luonnolliseille luvuille (kirjoitettuna kannassa p). Tuttuja algoritmeja yhteen-, vähennys- ja kertolaskulle tehdään mahdollisesti päättymättömästi oikealta vasemmalle. P-adinen jakolasku tapahtuu myös oikealta vasemmalle ja siten se eroaa tutusta jakokulmasta, missä aloitetaan etsimällä numero, joka on "korkeimmalla" paikalla ja se tapahtuu vasemmalta oikealle.

Tässä on esimerkkejä aritmeettisista laskutoimituksista joukossa $\mathbb{Q}_7$ siten, että vasemmalla on allekain yhteen- ja vähennyslasku, keskellä on allekain kertolasku ja oikealla jakokulmassa jakolasku:

$$
\begin{array}{r}
\ldots 42023.34 \\
+ \quad \ldots 31415.22 \\
\hline
\ldots 03441.56 \\
\\
\ldots 42023.3 \\
- \quad \ldots 31415.2 \\
\hline
\ldots 10315.1
\end{array}
\qquad
\begin{array}{r}
\ldots 251 \\
\times \ldots 151 \\
\hline
\ldots 251 \\
\ldots 6450 \\
+ \ldots 25100 \\
\hline
\ldots 131
\end{array}
\qquad
\begin{array}{r|l}
 & \ldots 151 \\
\hline
\ldots 251 & \ldots 131 \\
- & \ldots 151 \\
\hline
 & \ldots 550 \\
- & \ldots 6450 \\
\hline
 & \ldots 100 \\
- & \ldots 25100 \\
\hline
 & \ldots\ldots
\end{array}
$$

7. Rationaaliluvun p-adinen laajennus

Jokainen rationaalinen kokonaisluku (toisin sanoen kokonaisluku joukosta $\mathbb{Q}$) on p-adinen kokonaisluku (kirjoitetaan sen laajennus kannassa p). Toisaalta rationaalisten murtolukujen joukossa on olemassa p-adisia kokonaislukuja. Aiemmin ollaan todettu, että

$$-1 = (p-1)\sum_{i=0}^{\infty} p^i,$$

jolloin

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p},\ \frac{1}{1-p} = \ldots 1111,$$

joka on avaruudessa $\mathbb{Z}_p$. Huomaa, että tämän p-adisen kokonaisluvun p-adinen laajennus on päättymätön. Lemmasta 7.1 nähdään välttämättömät ja riittävät ehdot p-adisen laajennuksen päättymiselle.

Lemma 7.1. *Luvun $a \in \mathbb{Q}_p$ p-adinen laajennus päättyy (toisin sanoen $a_i = 0$ kaikilla luvilla $i > N$), jos ja vain jos a on ei $-$ negatiivinen rationaaliluku, jonka nimittäjä on luvun p potenssi.*

Todistus. Oletetaan, että luvun $a \in \mathbb{Q}_p$ p-adinen laajennus päättyy. Tällöin

$$\begin{aligned} a &= a_{-m}p^{-m} + \cdots + a_0 + a_1 p + \cdots + a_k p^k \\ &= \frac{a_{-m} + \cdots + a_0 p^m + a_1 p^{1+m} + \cdots + a_k p^{k+m}}{p^m}, \end{aligned}$$

missä nimittäjässä on luvun p potenssi ja luvut a_i saavat arvoja joukosta $\{0, 1, \ldots, p-1\}$ kaikilla $i \in \{-m, \ldots k\}$, jolloin luvun a arvo on rationaalinen ja ei-negatiivinen.

Oletetaan käänteinen väittämä, että luku a on ei-negatiivinen rationaaliluku, jonka nimittäjä on luvun p potenssi. Tällöin

$$a = \sum_{i=-m}^{\infty} a_i p^i = \frac{b}{p^k},$$

missä b on kokonaisluku ja $(b, p^k) = 1$. Tästä saadaan, että

$$\sum_{i=-m+k}^{\infty} a_i p^i = b.$$

Koska luku b on kokonaisluku, niin täytyy olla kokonaisluku N siten, että $a_i = 0$, kun $i > N$, sillä muutoin $b = \sum_{i=-m+k}^{\infty} a_i p^i \to \infty$. Tällöin

$$a = \sum_{i=-m+k}^{N} a_i p^i = a_{-m+k}p^{-m+k} + \cdots + a_0 + \cdots + a_N p^N$$

ja väite tulee todistetuksi. □

Seuraava lause antaa keinon tunnistaa rationaaliluvut niiden p-adisesta laajennuksesta, samaan tapaan kuin rationaaliluvut tunnistetaan reaalilukujen joukosta niiden desimaalilaajennuksesta.

Lause 7.2. *Kanoninen p-adinen laajennus (5.6) vastaa rationaalilukua, jos ja vain jos se on lopulta jaksollinen vasemmalle edetessä.*

Todistus. Oletetaan, että p-adinen laajennus on lopulta jaksollinen. Kertomalla (tarvittaessa) annettu p-adinen luku x luvun p potenssilla ja vähentämällä rationaaliluku, voidaan olettaa tapaus, jolloin luvulla $x \in \mathbb{Z}_p$ on jaksollinen laajennus muotoa

$$x = x_0 + x_1 p + x_2 p^2 + \dots x_{k-1} p^{k-1} + x_0 p^k + x_1 p^{k+1} \dots .$$

Luku $a = x_0 + x_1 p + x_2 p^2 + \cdots + x_{k-1} p^{k-1}$ on rationaalinen kokonaisluku ja luku x voidaan ilmaista muodossa

$$x = a(1 + p^k + p^{2k} + \dots) = a\frac{1}{1 - p^k},$$

jolloin x on rationaaliluku.

Oletetaan käänteinen väittämä, että

$$\frac{a}{b} = \sum_{i \geq 0} x_i p^i \in \mathbb{Z}_p. \tag{7.1}$$

Voidaan olettaa, että a ja b ovat keskenään jaottomia ja b ja alkuluku p ovat keskenään jaottomia. Koska $(b, p^n) = 1$, on olemassa c_n ja d_n (Bezout'n lemman nojalla) siten, että

$$1 = c_n b + d_n p^n.$$

Kertomalla yhtälö puolittain luvulla a saadaan

$$a = a c_n b + a d_n p^n.$$

Lisäämällä luvun p^n monikerta kokonaislukuun ac_n, saadaan kokonaisluvut A_n, jolle pätee $0 \leq A_n \leq p^n - 1$ ja r_n siten, että yhtälö

$$a = A_n b + r_n p^n$$

on totta. Jakamalla yhtälö puolittain luvulla b, saadaan

$$\frac{a}{b} = A_n + p^n \frac{r_n}{b}.$$

Tällöin $r_n = (a - A_n b)/p^n$ ja siten

$$\frac{a - (p^n - 1)b}{p^n} \leq r_n \leq \frac{a}{p^n}.$$

Riittävän suurilla luvun n arvoilla saadaan $-b \leq r_n \leq 0$, mikä tarkoittaa, että r_n saa vain äärellisen monta arvoa. Nyt voidaan kirjoittaa

$$\frac{a}{b} = A_n + p^n \frac{r_n}{b} = A_{n+1} + p^{n+1} \frac{r_{n+1}}{b}. \tag{7.2}$$

Koska $A_{n+1} - A_n = p^n(\frac{r_n - p r_{n+1}}{b})$ on kokonaisluku ja $(b, p^n) = 1$, niin $\frac{r_n - p r_{n+1}}{b}$ on kokonaisluku. Tällöin $A_{n+1} \equiv A_n \pmod{p^n}$ ja Lauseen 5.7 yksikäsitteisyyden nojalla jono $\{A_n\}$ on luvun a/b kanonisen p-adisen esityksen (7.1) osittaisten summien jono. Tällöin yhtälöstä $A_{n+1} = A_n + x_n p^n$ ja Lausekkeesta (7.2) seuraa, että $r_n = x_n b + p r_{n+1}$ kaikilla luvuilla n. Koska r_n saa vain äärellisen monta arvoa, niin on olemassa indeksi m ja positiivinen kokonaisluku P siten, että $r_m = r_{m+P}$. Tällöin

$$x_m b + p r_{m+1} = x_{m+P} b + p r_{m+P+1}, \tag{7.3}$$

josta saadaan

$$(x_m - x_{m+P})b = p(r_{m+P+1} - r_{m+1}).$$

Koska $(b, p) = 1$, seuraa, että p jakaa luvun $x_m - x_{m+P}$. Mutta luvut x_m ja x_{m+P} ovat numeroita väliltä $\{0, 1, \ldots, p-1\}$, mistä seuraa, että $x_m = x_{m+P}$. Jos tämä vaihdetaan Lausekkeeseen (7.3), saadaan myös, että $r_{m+1} = r_{m+P+1}$. Toistamalla tätä argumenttia saadaan, että

$$r_n = r_{n+P} \text{ ja } x_n = x_{n+P} \, (n \geq m),$$

mikä todistaa, että ei vain numeroilla x_n, mutta myös osoittajien r_n jonolla on jaksollinen pituus P kaikille luvuille $n \geq m$. □

Onko mahdollista päätellä rationaaliluvun p-adisesta laajennuksesta onko se positiivinen vai negatiivinen? Vastaus on kyllä ja se selviää seuraavassa lemmassa.

Lemma 7.3. *Olkoon $r \in \mathbb{Q}$ ja $k = -ord_p(r)$. Tällöin rp^k on p-adinen kokonaisluku ja sen p-adinen laajennus voidaan esittää muodossa $\ldots aaaaab$, missä osilla a ja b on sama määrä numeroita. Tällöin $r > 0$, jos ja vain jos $b > a$.*

Todistus. Olkoon $r \in \mathbb{Q}$ ja $k = -\mathrm{ord}_p(r)$. Tällöin $|rp^k|_p = |r|_p |p^{-\mathrm{ord}_p r}|_p = p^{-\mathrm{ord}_p r} p^{\mathrm{ord}_p r} = p^0 = 1$. Tällöin rp^k on p-adinen kokonaisluku ja sen esitys on lopulta jaksollinen vasemmalle edetessä Lauseen 7.2 mukaan. Oletetaan, että luvun rp^k p-adisen laajennuksen jaksollisen osuuden pituus on N ja jaksollisuutta edeltävän osuuden pituus on M. Lisätään jaksollisuutta edeltävään osaan jaksollisen osan numeroita kunnes sen pituudeksi tulee, jokin pituuden N monikerta. Olkoon tällöin $M + t = n \cdot N$, jolloin uusien jaksollisuutta edeltävän osan b ja jaksollisen osan a pituus on $n \cdot N = L$. Nyt luvun rp^k p-adinen laajennus voidaan esittää muodossa $\ldots aaaaab$. Jakamalla $\ldots aaaaab$ luvulla p^k se muuttaa vain lukujen p potensseja ja voidaan kirjoittaa

$$r = \ldots aaab = b + ap^L + ap^{2L} + ap^{3L} + \cdots = b + \frac{ap^L}{1 - p^L},$$

sillä $|p^L|_p < 1$. Jos $r > 0$, niin tällöin

$$0 < r = b + a\frac{p^L}{1 - p^L},$$

mistä seuraa, että

$$a < a\frac{p^L}{p^L - 1} < b.$$

Tämä on todistaa juurin sen, että $r > 0$, jos ja vain jos $b > a$. □

8. Henselin Lemma ja kongruensseja

Määritetään $\sqrt{6}$ avaruudessa $\mathbb{Q}_5$. Tämä tarkoittaa, että halutaan löytää 5-adisten numeroiden jono $a_0, a_1, a_2, \ldots, 0 \leq a_i \leq 4$, siten, että

$$(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots)^2 = 1 + 1 \cdot 5. \tag{8.1}$$

Lausekkeesta (8.1) saadaan $a_0^2 \equiv 1 \pmod 5$, mistä seuraa, että $a_0 = 1$ tai $a_0 = 4$. Jos $a_0 = 1$, niin

$$2a_1 \cdot 5 \equiv 1 \cdot 5 \pmod{5^2} \implies 2a_1 \equiv 1 \pmod 5 \implies a_1 = 3.$$

Seuraavaksi saadaan

$$1 + 1 \cdot 5 \equiv (1 + 3 \cdot 5 + a_2 \cdot 5^2)^2 \equiv 1 + 1 \cdot 5 + 2a_2 \cdot 5^2 \pmod{5^3},$$

mistä seuraa, että $2a_2 \equiv 0 \pmod 5$ ja edelleen $a_2 = 0$.

Tällöin saadaan sarja

$$a = 1 + 3 \cdot 5 + 0 \cdot 5^2 + \ldots,$$

missä jokainen a_i numeron a_0 jälkeen on yksikäsitteisesti määritelty.

Jos valitaan $a_0 = 4$, niin saadaan ratkaisu

$$-a = 4 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + \ldots.$$

Ei ole vaikeaa nähdä, että on olemassa avaruuden $\mathbb{Q}_5$ lukuja, joilla ei ole neliöjuurta (esimerkiksi $2 + 1 \cdot 5$).

Äskeinen keino ratkaista yhtälöitä (kuten $x^2 - 6 = 0$ avaruudessa $\mathbb{Q}_5$) voidaan yleistää käyttämällä erittäin tärkeää tulosta, jota sanotaan "Henselin Lemmaksi".

Yleistämällä Huomautusta 5.2 sanotaan, että a ja $b \in \mathbb{Q}_p$ ovat ekvivalentit, jolloin kirjoitetaan

$$a \equiv b \pmod{p^n},$$

jos ja vain jos $|a - b|_p \leq 1/p^n$.

Lause 8.1 (Henselin Lemma). *Olkoon $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ polynomi, jonka kertoimet ovat p-adisia kokonaislukuja. Olkoon*

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \cdots + nc_n x^{n-1}$$

polynomin $F(x)$ derivaatta. Oletetaan, että $\overline{a}_0$ on p-adinen kokonaisluku, joka toteuttaa ehdon $F(\overline{a}_0) \equiv 0 \pmod p$ ja $F'(\overline{a}_0) \not\equiv 0 \pmod p$. Tällöin on olemassa yksikäsitteinen p-adinen kokonaisluku a siten, että $F(a) = 0$ ja $a \equiv \overline{a}_0 \pmod p$.

Todistus. Todistetaan p-adisen kokonaisluvun a olemassaolo konstruoimalla sen kanoninen p-adinen laajennus $a = b_0 + b_1 p + b_2 p^2 + \ldots$ induktiolla. Induktion vaiheessa k saadaan $a_k = b_0 + \ldots b_k p^k$, joka on k:nnes approksimaatio luvusta a käyttäen Newtonin menetelmän p-adista versiota (todistukseen jälkeen asia esitellään huomautuksena). Jokainen a_k ei tule olemaan polynomin $F(x)$ aito juuri, mutta ne ovat "juuria modulo p^{k+1}" (toisin sanoen $F(a_k) \equiv 0 \pmod{p^{k+1}}$) kaikilla luvuilla k. Kun $k \to \infty$, niin raja-arvona saadaan a, joka on polynomin F tarvittu aito juuri.

Tarkemmin todistetaan seuraava väittämä induktiolla luvulle k:

$S(k)$: *on olemasa p-adinen kokonaisluku, joka on muotoa*

$$a_k = b_0 + b_1 p + \cdots + b_k p^k,$$

(*jonka numerot* b_i *ovat joukosta* $\{0, 1, \ldots, p-1\}$ *kaikilla luvun* i *arvoilla*) *siten, että*

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

Induktion perusaskel on selvä: valitaan luvuksi b_0 ensimmäinen p-adisen luvun $\overline{a}_0$ numero ja saadaan $a_0 \equiv \overline{a}_0$ ja $F(a_0) \equiv 0 \pmod{p}$.

Seuraavaksi tehdään induktioaskel, jolloin toisin sanoen todistetaan, että kohdasta $S(k-1)$ seuraa $S(k)$. Tätä varten olkoon $a_k = a_{k-1} + b_k p^k$ jollain (vielä tuntemattomalla) numerolla b_k, joka toteuttaa ehdon $0 \leq b_k < p$ ja avataan termi $F(a_k)$, missä ei huomioida termejä jotka ovat jaollisia luvulla p^{k+1}:

$$\begin{aligned} F(a_k) = F(a_{k-1} + b_k p^k) &= \sum_{i=0}^{n} c_i (a_{k-1} + b_k p^k)^i \\ &= c_0 + \sum_{i=1}^{n} c_i (a_{k-1}^i + i a_{k-1}^{i-1} b_k p^k + \text{termit, jotka jaollisia luvulla } p^{k+1}) \\ &\equiv F(a_{k-1}) + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}. \end{aligned}$$

Koska $F(a_{k-1}) \equiv 0 \pmod{p^k}$ induktio-oletuksen nojalla, voidaan kirjoittaa

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

jollain kokonaisluvulla $\alpha \in \{0, 1, \ldots p-1\}$. Tällöin päädytään seuraavaan yhtälöön tuntemattoman numeron b_k osalta:

$$\alpha_k + b_k F'(a_{k-1}) \equiv 0 \pmod{p}. \tag{8.2}$$

Tämä voidaan ratkaista, kun tiedetään $F'(a_{k-1}) \not\equiv 0 \pmod{p}$. Edellinen seuraa, koska pätee, että $a_{k-1} \equiv \overline{a}_0 \pmod{p}$, josta seuraa, että

$$F'(a_{k-1}) \equiv F'(\overline{a}_0) \not\equiv 0 \pmod{p}.$$

Jakamalla Lauseke (8.2) derivaatalla $F'(a_{k-1})$, saadaan tarvittu numero b_k, jolloin

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

jonka avulla saadaan $F(a_k) \equiv 0 \pmod{p^{k+1}}$, joka päättää induktioaskeleen.

Nyt olkoon

$$a = b_0 + b_1 p + b_2 p^2 + \ldots.$$

Huomataan, että $F(a) = 0$, sillä kaikilla luvuilla k pätee, että

$$F(a) \equiv F(a_k) \equiv 0 \pmod{p^{k+1}}.$$

Yksikäsitteisyys seuraa jonon $\{a_k\}$ yksikäsitteisyydestä. □

Huomautus 8.2. Toinen ehto ($F'(\overline{a}_0) \not\equiv 0 \pmod{p}$) Lauseessa 8.1 on tarpeellinen (katso Esimerkki 8.6). Lauseesta 8.1 on monia eri versioita kirjallisuudessa, mutta kaikista niistä puhutaan "Henselin Lemmana".

Huomautus 8.3. Arviointimenetelmä, jota käytettiin Henselin Lemman todistuksssa vastaa oleellisesti Newtonin menetelmää, jolla etsitään reaalikertoimisen polynomin

$f(x)$ reaaliset juuret. Reaalisessa tapauksessa, jos $f'(a_{n-1}) \neq 0$, niin Newtonin menetelmällä seuraava arvio luvusta a_n saadaan kaavalla

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

Korjaustermi näyttää hyvin samalta kuin Henselin Lemman todistuksessa käytetty "korjaustermi":

$$b_n p^n \equiv -\frac{\alpha_n p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

Tietyllä tavalla Henselin Lemma on kuitenkin parempi kuin Newtonin menetelmä reaalisessa tapauksessa: p-adisessa tapauksessa suppeneminen polynomin juureen on taattu Henselin Lemman ehdoilla ratkaisuyritteelle $\overline{a}_0$, jonka esitys ei riipu polynomista. Reaalisessa tapauksessa Newtonin menetelmä suppenee, jos ratkaisuyrite on tarpeeksi lähellä oikeaa juurta, mutta ehto lähelläolosta riippuu polynomista. Esimerkiksi jos $f(x) = x^3 - x$ ja valitaan epäonnekas ratkaisuyrite $a_0 = 1/\sqrt{5}$, niin saadaan $a_1 = -1/\sqrt{5}$, $a_2 = 1/\sqrt{5}$ ja niin edelleen, jolloin jono $\{a_n\}$ ei suppene.

Lause 8.4. *Polynomilla, jolla on kokonaislukukertoimet on juuri avaruudessa $\mathbb{Z}_p$, jos ja vain jos sillä on kokonaislukujuuri modulo p^k millä tahansa $k \geq 1$.*

Todistus. Olkoon $F(x)$ polynomi, jolla on kertoimet avaruudessa $\mathbb{Z}$. Oletetaan, että $a \in \mathbb{Z}_p$ on sen juuri. Toisin sanoen

$$F(a) = 0. \tag{8.3}$$

Lauseen 5.7 mukaan on olemassa kokonaislukujen jono $\{a_1, a_2, \ldots, a_k, \ldots\}$, missä $a_k = b_0 + b_1 p + b_2 p^2 + \cdots + b_{k-1} p^{k-1}$ siten, että

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

Tällöin tiedoista $F(a_k) \equiv F(a) \pmod{p^k}$ ja $F(a) = 0$ seuraa, että

$$F(a_k) \equiv 0 \pmod{p^k}. \tag{8.4}$$

Toiseen suuntaan todistaessa oletetaan, että kongruenssilla (8.4) on kokonaislukuratkaisu a_k mille tahansa $k \geq 1$. Lauseen 5.11 mukaan jono $\{a_k\}$ sisältää suppenevan osajonon $\{a_{k_i}\}$, $\lim_{i\to\infty} a_{k_i} = a$. Halutaan näyttää, että a on ratkaisu yhtälölle (8.3). Koska polynomi on jatkuva funktio saadaan, että

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

(tässä käytetään Lausetta 4.7). Toisaalta

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

Tällöin $\lim_{i\to\infty} F(a_{k_i}) = 0$ ja tästä seuraa, että $F(a) = 0$. □

Käytännöllinen seuraus Lauseesta 8.4 on seuraava. Jos kokonaislukukertoimisella polynomilla ei ole juuria modulo p, niin tällöin sillä ei ole juuria avaruudessa $\mathbb{Z}_p$. Yleensä sen juuria ei ole kovin vaikea löytää modulo p, jos sillä niitä on. Jos juuri modulo p ei ole derivaatan juuri modulo p, niin Henselin Lemmalla löydetään juuri avaruudesa $\mathbb{Z}_p$.

Sanotaan, että rationaalinen kokonaisluku a, joka ei ole jaollinen luvulla p on *neliönjäännös modulo* p, jos kongruenssilla

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

on ratkaisu joukossa $\{1, 2, \ldots, p-1\}$. Muutoin lukua a sanotaan *neliönepäjäännökseksi.*

Lemma 8.5. *Rationaalisella kokonaisluvulla a, joka ei ole jaollinen luvulla p on neliöjuuri avaruudessa $\mathbb{Z}_p$ $(p \neq 2)$, jos ja vain jos a on neliönjäännös modulo p.*

Todistus. Olkoon $P(x) = x^2 - a$. Tällöin $P'(x) = 2x$. Jos a on neliönjäännös, niin

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

jollain $a_0 \in \{1, 2, \ldots, p-1\}$. Tästä seuraa, että $P(a_0) \equiv 0 \pmod{p}$. Mutta

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

seuraa suoraan, sillä $(a_0, p) = 1$, jolloin ratkaisu on olemassa Henselin Lemman nojalla. Toiseen suuntaan todistaessa, jos a on neliönjäännös, niin Lauseen 8.4 nojalla, sillä ei ole neliöjuurta avaruudessa $\mathbb{Z}_p$. □

Esimerkiksi $\sqrt{-1}$ on avaruudessa $\mathbb{Z}_5$, sillä $-1 = 4-5 \equiv 2^2 \pmod{5}$ on neliönjäännös modulo 5, kun taas $\sqrt{-1}$ ei ole avaruudessa $\mathbb{Z}_3$, sillä $-1 = 2-3$ on neliönepäjäännös modulo 3. Kuuluuko $\sqrt{p}$ avaruuteen $\mathbb{Z}_p$?

Esimerkki 8.6. On olemassa polynomi, jolla on juuri modulo 2, mutta ei juuria avaruudessa $\mathbb{Q}_2$.

Todistus. Olkoon polynomi $f(x) = x^2 - 3$. Tällöin polynomilla $f(x)$ on juuri $x = 1$ modulo 2, mutta ei juuria avaruudessa $\mathbb{Q}_2$. Oletetaan, että $x \in \mathbb{Q}_2$ on juuri eli $x^2 = 3$. Normin kertolasku ominaisuudella saadaan, että $|x|_2^2 = |3|_2 = 1$, jolloin $|x|_2 = 1$. Tällä perusteella, jos juuri on olemassa avaruudessa $\mathbb{Q}_2$, niin sen täytyy myös olla avaruudessa $\mathbb{Z}_2$. Luvulla $3 = 1 + 1 \cdot 2$ ei ole juuria avaruudessa $\mathbb{Z}_2$ (samantapainen päättely kuin kappaleen alussa, kun etsitään ratkaisua $\sqrt{6}$ avaruudessa $\mathbb{Q}_5$), sillä täytyisi olla $(a_0 + a_1 \cdot 2 + a_2 \cdot 2 + \ldots)^2 = 1 + 1 \cdot 2$, missä $a_i \in \{0, 1\}$. Tästä seuraa, että $a_0^2 \equiv 1 \pmod{2}$, jolloin $a_0 = 1$. Seuraavaksi saataisiin $2a_1 \cdot 2 \equiv 1 \cdot 2 \pmod{2^2}$, josta seuraa, että $2a_1 \equiv 1 \pmod{2}$ eli $0 \equiv 1 \pmod{2}$, mikä on mahdotonta. Tällöin polynomilla $f(x)$ ei ole juuria avaruudessa $\mathbb{Q}_2$. □

9. Topologisia perusominaisuuksia

P-adisten lukujen kunta on monella tapaa analoginen reaalilukujen kunnan $\mathbb{R}$ kanssa. $\mathbb{R}$ ja $\mathbb{Q}_p$ ovat molemmat normilla varustettuja kuntia ja täydellisiä metrisiä avaruuksia. Joukon $\mathbb{Q}$ molemmat täydellistymät sisältävät joukon $\mathbb{Q}$ tiheänä osajoukkona (metrisiä avaruuksia, jotka sisältävät numeroituvan tiheän osajoukon kutsutaan *separoituviksi*). Kunta $\mathbb{R}$ on *lokaalisti kompakti.* Toisin sanoen jokaisella pisteellä on kompakti ympäristö. Myös kunta $\mathbb{Q}_p$ on lokaalisti kompakti, mikä nähdään myöhemmin (Lause 9.10).

Tutkitaan joukkoja $\mathbb{R}$ ja $\mathbb{Q}_p$ metristen avaruuksien näkökulmasta. Avaruudessa $\mathbb{R}$ avoimet pallot ovat avoimia välejä $B(a,r) = |x-a| < r$. Avaruudessa $\mathbb{Q}_p$ avoimet pallot ovat joukkoja

$$B(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\},$$

mutta koska p-adinen normi saa diskreetteja arvoja joukosta $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$, niin otetaan huomioon vain pallot joiden säde on $r = p^n$, missä $n \in \mathbb{Z}$.

Olkoon $\mathcal{G}$ kaikkien avoimien osajoukkojen kokoelma joukosta M ja olkoon $\mathcal{F}$ kaikkien suljettujen osajoukkojen kokoelma joukosta M. Määritelmän mukaan jokainen joukon $\mathcal{F}$ alkio on joukon $\mathcal{G}$ tietyn alkion komplementti ja päinvastoin. Avoimilla ja suljetuilla joukoilla on seuraavia ominaisuuksia.

Lemma 9.1.

(1) *Jos $\mathcal{C} \subset \mathcal{G}$ on mikä tahansa kokoelma avoimia joukkoja, niin $\bigcup_{G\in\mathcal{C}} G$ kuuluu joukkoon $\mathcal{G}$ ja jos $G_1, \ldots, G_n \in \mathcal{G}$ on mikä tahansa äärellinen kokoelma avoimia joukkoja, niin $\bigcap_{i=1}^n G_i$ kuuluu joukkoon $\mathcal{G}$.*

(2) *Jos $\mathcal{C} \subset \mathcal{F}$ on mikä tahansa kokoelma suljettuja joukkoja, niin $\bigcap_{F\in\mathcal{C}} F$ kuuluu joukkoon $\mathcal{F}$ ja jos $F_1, \ldots, F_n \in \mathcal{F}$ on mikä tahansa äärellinen kokoelma suljettuja joukkoja, niin $\bigcup_{i=1}^n F_i$ kuuluu joukkoon $\mathcal{F}$.*

Todistus. [6, Lause 2.24]. □

Tällöin $\mathcal{G}$ on avoin mielivaltaisilla yhdisteillä ja äärellisillä leikkauksilla ja $\mathcal{F}$ on suljettu mielivaltaisilla leikkauksilla ja äärellisillä yhdisteillä. Avoimien joukkojen kokoelma $\mathcal{G}$ määrittelee metrisessä avaruudessa *topologian.* Käsitteet ympäristö, rajaarvo, suppeneminen, jatkuvuus ja niin edelleen voidaan määritellä topologian termeillä ilman, että tukeudutaan metriikkaan. Itse asiassa topologian käsite on yleisempi ja *topologinen avaruus* on määritelty joukkona, joka on kokoelma avoimia joukkoja, jotka toteuttavat määritelmän 9.1 ehdon (1) (lisäksi tietysti triviaalit oletukset, että koko avaruus ja tyhjä joukko ovat avoimia). Yleisesti *topologiset avaruudet* voivat olla melko patologisia ja melko erilaisia kuin avaruudet, joissa topologia on johdettu metriikasta.

Jos M on topologinen avaruus ja $X \subset M$, niin joukosta X tulee topologinen avaruus *indusoidulla topologialla*, korvaamalla joukon M avointen joukkojen leikkaukset joukon X avointen joukkojen leikkauksilla.

Palataan p-adisiin lukuihin ja olkoon avaruuden $\mathbb{Q}_p$ *pallo* :

$$S(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p = r\}.$$

Tähän liittyy erikoinen ominaisuus, josta seuraavaksi lisää.

Lemma 9.2. *Avaruuden $\mathbb{Q}_p$ pallo $S(a,r)$ on avoin joukko.*

Todistus. Olkoon $x \in S(a,r)$ ja $\varepsilon < r$. Näytetään, että $B(x,\varepsilon) \subset S(a,r)$. Olkoon $y \in B(x,\varepsilon)$. Tällöin $|y-a-(x-a)|_p = |y-x|_p = |x-y|_p < |x-a|_p = r$ ja Lemman 3.13 nojalla $|y-a|_p = |x-a|_p = r$, mikä tarkoittaa juuri, että $y \in S(a,r)$. □

Tämä on erikoista, sillä avaruudessa $\mathbb{R}^n$ (erityisesti avaruudesa $\mathbb{R}$) pallot eivät ole avoimia. Tutkitaan, mitä tästä ominaisuudesta seuraa.

Lemma 9.3. *Avaruuden $\mathbb{Q}_p$ avoimet pallot ovat suljettuja ja avoimia.*

Todistus. Mikä tahansa avoin pallo $B(a,r)$ on avoin missä tahansa metrisessä avaruudessa, sillä mikä tahansa piste $x \in B(a,r)$ kuuluu joukkoon $B(a,r)$ mikä sisältyy palloon $B(a,r)$. Todistaaksemme, että $B(a,r)$ on suljettu avaruudessa $\mathbb{Q}_p$ näytetään, että sen komplementti

$$C = \{x \in \mathbb{Q}_p \mid |x-a|_p \geq r\}$$

on avoin. Kuitenkin $C = S(a,r) \cup D$, missä

$$D = \{x \in \mathbb{Q}_p \mid |x-a|_p > r\}.$$

Joukko D on avoin (tämä on totta kaikissa metrisissä avaruuksissa). Tämän todistukseen olkoon $y \in D$. Tällöin $|y-a|_p = r_1 > r$. Väitetään, että avoin pallo $B(y, r_1 - r)$ kuuluu joukkoon D. Jos näin ei olisi, niin olisi olemassa $x \in B(y, r_1 - r)$ siten, että $|x-a|_p \leq r$. Mutta kolmioepäyhtälöllä

$$r_1 = |y-a|_p = |a-x+x-y|_p \leq |a-x|_p + |x-y|_p < r + r_1 - r = r_1,$$

mikä on ristiriita. Väite seuraa, sillä kahden avoimen joukon yhdiste on avoin. □

Muistellaan, että piste $x \in M$ on joukon $A \subset M$ *reunapiste*, jos kaikki avoimet x-keskipisteiset avoimet pallot sisältävät pisteitä joukosta A, sekä pisteitä, jotka eivät ole joukossa A. Joukko A on suljettu, jos ja vain jos se sisältää kaikki reunapisteensä. Lemmasta 9.3 seuraa, että $S(a,r)$ ei ole avoimen pallon $B(a,r)$ reuna. Itse asiassa Lemmasta 9.3 seuraa, että joukolla $B(a,r)$ ei ole reunaa ollenkaan. Tietenkään suljettu pallo

$$\begin{aligned} \overline{B}(a,p^n) &= \{x \in \mathbb{Q}_p \mid |x-a|_p \leq p^n\} \\ &= \{x \in \mathbb{Q}_p \mid |x-a|_p < p^{n+1}\} = B(a,p^{n+1}) \end{aligned} \tag{9.1}$$

ei ole avoimen pallon $B(a,p^n)$ sulkeuma.

Lausekkeesta (9.1) seuraa, että kaikki väittämät avoimille palloille pätevät suljetuille palloille avaruudessa $\mathbb{Q}_p$.

Seuraavaksi tutkitaan toista paradoksista ominaisuutta palloille avaruudessa $\mathbb{Q}_p$.

Lemma 9.4. *Jos $b \in B(a,r)$, niin $B(b,r) = B(a,r)$. Toisin sanoen jokainen pallon piste on sen keskipiste.*

Todistus. Koska joukon $\mathbb{Q}_p$ normi $|\cdot|_p$ on epäarkhimedinen, niin tulos seuraa suoraan Lemmasta 3.15. □

Tässä on vielä lisäominaisuus palloille.

Lemma 9.5. *Kahdella pallolla joukossa $\mathbb{Q}_p$ on epätyhjä leikkaus, jos ja vain jos toinen pallo kuuluu toiseen palloon. Toisin sanoen*

$$B(a,r) \cap B(b,s) \neq \varnothing, \text{ jos ja vain jos } B(a,r) \subset B(b,s) \text{ tai } B(b,s) \subset B(a,r).$$

Todistus. Selvästikin, jos toinen pallo on toisen osajoukko, niin niiden leikkaus on epätyhjä. Käänteisen todistamiseksi oletetaan, että $r \leq s$ ja $y \in B(a,r) \cap B(b,s)$. Tällöin Lemman 9.4 nojalla $B(a,r) = B(y,r)$ ja $B(b,s) = B(y,s)$. Mutta $B(y,r) \subset B(y,s)$, niin tarpeellinen väite seuraa. □

Lemma 9.6. *Pallo $S(a,r)$ on avoin ja suljettu.*

Todistus. Lemman 9.2 nojalla tiedetään, että pallo $S(a,r)$ on avoin. Tiedetään myös, että pallo $\overline{B}(a,r)$ on suljettu, ja koska $B(a,r)$ on avoin, niin sen komplementti $\{x \in \mathbb{Q}_p \mid |x-a|_p \geq r\}$ on suljettu. Mutta koska $S(a,r)$ on näiden kahden suljetun joukon leikkaus, niin se on myös itse suljettu ($S(a,r) = \overline{B}(a,r) \cap \{x \in \mathbb{Q}_p \mid |x-a|_p \geq r\}$). Huomiona vielä, että todistus sille, että pallo $S(a,r)$ on suljettu, toimii kaikissa metrisissä avaruuksissa. □

Kaikkien pallojen kokoelma avaruudessa $\mathbb{R}$ on ylinumeroituva, koska kaikkien positiivisten reaalilukujen kokoelma on ylinumeroituva (Cantorin Lause). Sama väite pätee kaikille keskipisteiden a kokoelmalle ja säteiden ρ kokoelmalle, joten se todellakin on totta pallojen $B(a,\rho)$ kokoelmalle avaruudessa $\mathbb{R}$. Täysin toinen tulos pätee kaikkien pallojen kokoelmalle avaruudessa $\mathbb{Q}_p$.

Lemma 9.7. *Avaruuden $\mathbb{Q}_p$ kaikkien pallojen kokoelma on numeroituva.*

Todistus. Kirjoitetaan pallon $B(a,p^{-s})$ keskipiste kanonisessa muodossa

$$a = \sum_{n=-m}^{\infty} a_n p^n$$

ja olkoon

$$\hat{a}_0 = \sum_{n=-m}^{s} a_n p^n.$$

Selvästi a_0 on rationaaliluku ja Lemman 5.8 nojalla $|a - \hat{a}_0|_p < p^{-s}$ toisin sanoen $\hat{a}_0 \in B(a,p^{-s})$. Tällöin Lemman 9.4 nojalla

$$B(\hat{a}_0, p^{-s}) = B(a, p^{-s}).$$

Edellä oleva keskipiste ja säde ovat peräisin numeroituvista joukoista. Tällöin myös näistä muodostuvien parien $(\hat{a}_0, s)$ tulojoukko on numeroituva ja siten myös avaruuden $\mathbb{Q}_p$ kaikkien pallojen kokoelma. □

Käyttämällä Kappaleen 5 merkintöjä pätee, että

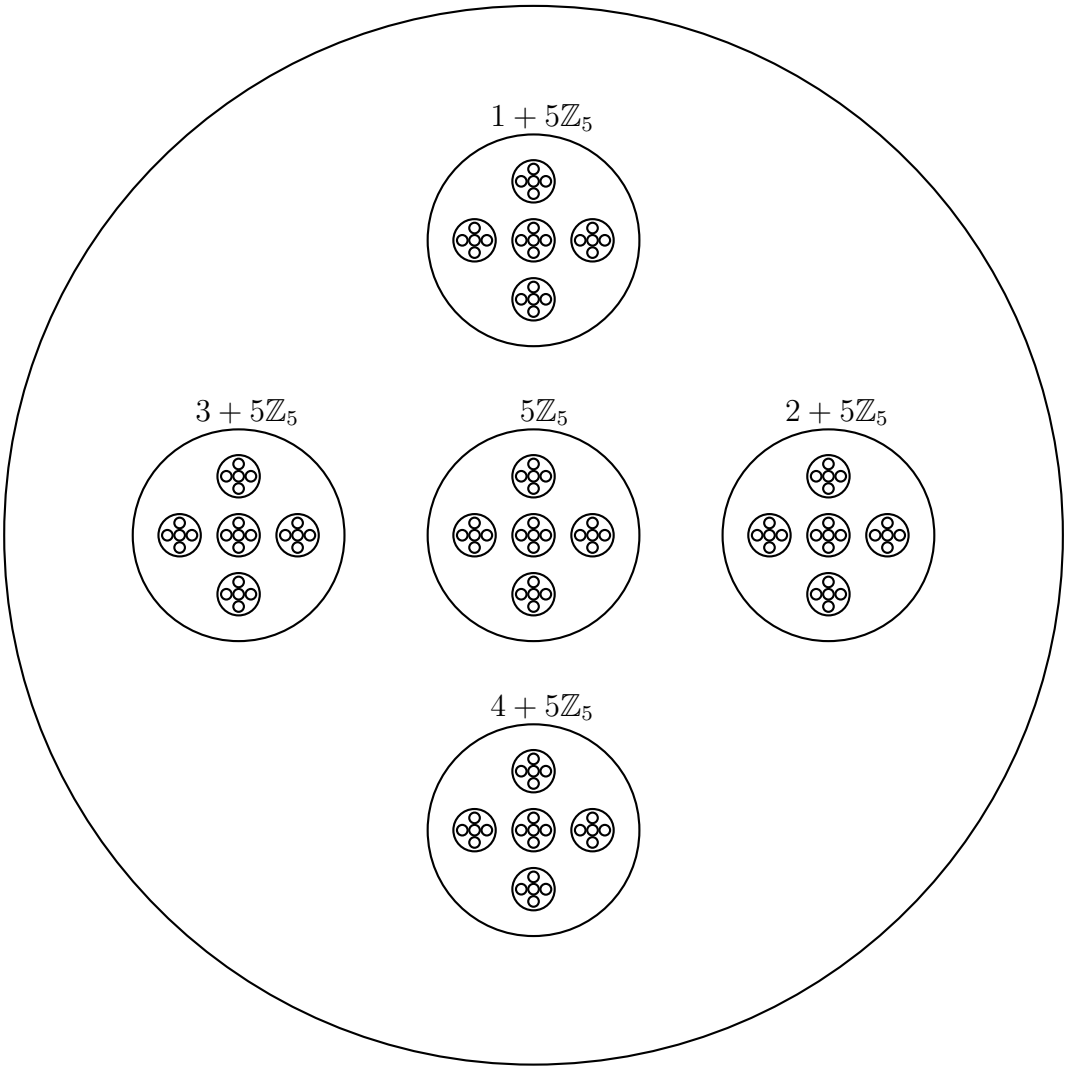
$$\mathbb{Z}_p = \overline{B}(0,1) = B(0,p)$$

ja

$$\mathbb{Z}_p^\times = S(0,1) = (1 + p\mathbb{Z}_p) \cup (2 + p\mathbb{Z}_p) \cup \cdots \cup ((p-1) + p\mathbb{Z}_p).$$

Tätä havainnollistetaan symbolisesti Kuvassa 9.1, kun $p = 5$. Pallo $\mathbb{Z}_5^\times$ on neljän avoimen pallon yhdiste ja sille pätee Lemman 9.6 väite. Keskimmäinen pallo esittää renkaan $\mathbb{Z}_5$ maksimalista ideaalia $5\mathbb{Z}_5$ (vertaa Kappaleen 11 Kuvaan 11.3, joka on euklidinen mallinnus).

Määritelmä 9.8. Metrisessä avaruudessa osajoukkoa K sanotaan *jonokompaktiksi*, jos jokainen joukon K päättymätön pistejono sisältää osajonon, joka suppenee joukon K pisteeseen.



KUVA 9.1. $\mathbb{Z}_5$

Metrisen avaruuden osajoukkoa K sanotaan *kompaktiksi*, jos mikä tahansa joukon K avointen joukkojen peite sisältää äärellisen osapeitteen.

Samantapaisesti voidaan määritellä *jonokompaktit* ja *kompaktit* metriset avaruudet.

Heine-Borelin Lauseen mukaan edellä mainitut ominaisuudet ovat ekvivalentteja metrisessä avaruudessa ja avaruudessa $\mathbb{R}^n$ ne ovat ekvivalentteja sen kanssa, että joukko on suljettu ja rajoitettu (esimerkiksi $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$ ja [6, Lause 2.41]).

Lemma 9.9. *Olkoon $A_1 \supset A_2 \supset A_3 \cdots \supset A_n \supset A_{n+1} \supset \ldots$ metrisen avaruuden M epätyhjien kompaktien joukkojen jono. Tällöin $\bigcap_{n=1}^{\infty} A_n$ on epätyhjä ja kompakti.*

Todistus. Koska joukot A_n ovat epätyhjiä ja sisäkkäisiä, niin on olemassa alkio $a \in A_n$ kaikilla n. Tästä seuraa, että $a \in \bigcap_{n=1}^{\infty} A_n$ ja $\bigcap_{n=1}^{\infty} A_n$ on epätyhjä. Koska kaikki joukot A_n ovat kompakteja, niin niiden päättymättömällä pistejonolla on olemassa suppeneva osajono $\{a_n\}$, joka suppenee joukkoon A_n. Tällöin myös joukon $\bigcap_{n=1}^{\infty} A_n$

päättymättömällä pistejonolla on suppeneva osajono $\{a_n\}$, joka suppenee joukkoon $\bigcap_{n=1}^{\infty} A_n$. Tällöin $\bigcap_{n=1}^{\infty} A_n$ on kompakti. □

Aiemmin ollaan nähty (Lemma 5.11), että $\mathbb{Z}_p$ on jonokompakti. Tällöin $\mathbb{Z}_p$ on kompakti ja niin on myös mikä tahansa pallo avaruudessa $\mathbb{Q}_p$ Lemman 5.13 nojalla. Tästä seuraa tulos:

Lause 9.10. *Joukko $\mathbb{Z}_p$ on kompakti ja avaruus $\mathbb{Q}_p$ on lokaalisti kompakti.*

Lauseesta 9.10 seuraa suoraan, että:

Lemma 9.11. *Avaruus $\mathbb{Z}_p$ on täydellinen.*

Todistus. Koska mikä tahansa Cauchy-jono avaruudessa $\mathbb{Z}_p$ sisältää osajonon, joka suppenee alkioon avaruudessa $\mathbb{Z}_p$, olkoon tuo alkio a, niin alkuperäisen jonon, joka suppenee avaruudessa $\mathbb{Q}_p$ täydellisyyden nojalla, täytyy supeta alkioon a. Tämä todistaa avaruuden $\mathbb{Z}_p$ täydellisyyden. □

Lause 9.12. *Joukko $\mathbb{N}$ on tiheä joukossa $\mathbb{Z}_p$.*

Todistus. Olkoon $x = \ldots a_2 a_1 a_0 \in \mathbb{Z}_p$. Jokaiselle luvulle $n \in \mathbb{N}$ on

$$x_n = \ldots 00 a_n a_{n-1} \ldots a_0 = \sum_{i=0}^{n} a_i p^i.$$

Tällöin $x_n \in \mathbb{N}$ ja $|x - x_n|_p < p^{-n}$ ja väite seuraa. □

Määritelmä 9.13. Topologinen avaruus X on *epäyhtenäinen*, jos se voidaan esittää kahden erillisen epätyhjän avoimen (tai suljetun) osajoukon yhdisteenä. Muutoin sanotaan, että avaruus X on *yhtenäinen*.

Avaruuden X osajoukko C on *yhtenäinen*, jos se on yhtenäinen avaruus indusoidussa topologiassa.

Avaruus X on *täysin epäyhtenäinen*, jos avaruuden X ainoat yhtenäiset osajoukot ovat tyhjä joukko ja yhden pisteen joukot $\{a\}$, missä $a \in X$.

Esimerkki 9.14. Jokainen avaruuden $\mathbb{R}$ väli on yhtenäinen.

Lause 9.15. *Avaruus $\mathbb{Q}_p$ on täysin epäyhtenäinen.*

Todistus. Jokaiselle alkiolle $a \in \mathbb{Q}_p$ ja kokonaisluvulle $n \in \mathbb{N}$ joukko

$$U_n(a) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^{-n}\} = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^{-n+1}\}$$

on avoin ja suljettu alkion a ympäristö. Oletetaan, että $a \in A$ siten, että $A \neq \{a\}$. Tällöin on olemassa $n \in \mathbb{N}$ siten, että $U_n(a) \cap A \neq A$. Tästä seuraa, että

$$A = (U_n(a) \cap A) \cup (\mathbb{Q}_p \setminus U_n(a) \cap A),$$

missä $U_n(a)$ ja sen komplementti $\mathbb{Q}_p \setminus U_n(a)$ ovat avoimia ja epätyhjiä. Tästä seuraa, että A ei ole yhtenäinen. □

10. Cantorin joukot

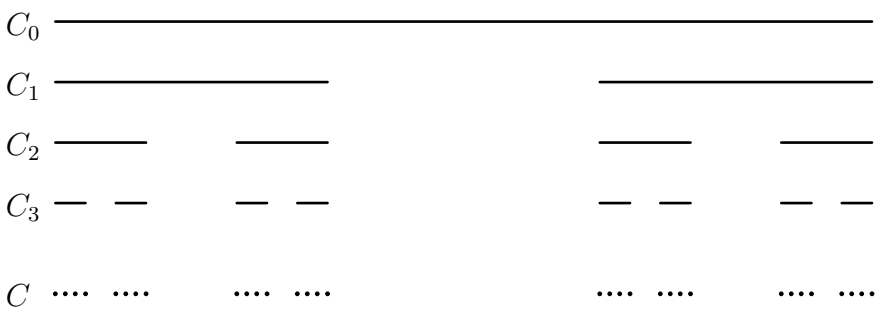
Tässä kappaleessa keskitytään enimmäkseen reaalilukujen analyysiin. Olkoon

$$C_0 = I = [0,1], C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right],$$
$$C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right], \ldots.$$

Jokainen joukko C_n on yhdiste 2^n monesta suljetusta välistä, joiden jokaisen pituus on 3^{-n} ja tällöin joukot C_n ovat sisäkkäisiä seuraavasti $C_0 \supset C_1 \supset C_2 \supset \ldots$. Koska jokainen joukko C_n on suljettu, niin

$$C := \bigcap_{n=0}^{\infty} C_n \neq \varnothing$$

on yksikkövälin I suljettu osajoukko (katso Kuva 10.1). Joukko C on epätyhjä Lemman 9.9 nojalla joukon I epätyhjien kompaktien osajoukkojen laikkauksena, mutta tämä nähdään suoraan siitäkin, että joukko C selvästi sisältää joukon C_n jokaisen välin päätepisteet. Itse asiassa joukko C sisältää ylinumeroituvan monta muuta pistettä kuin nämä välien päätepisteet. Joukkoa C sanotaan *Cantorin joukoksi.*



Kuva 10.1. Cantorin joukon C konstruktio

Esitetään reaaliluvut väliltä $I = [0,1]$ päättymättöminä murtolukuina kannassa kolme. Huomaa, että kaikillä välien päätepisteillä, jotka muodostavat joukon C_n on kaksi laajennusta kannassa kolme, kuten

$$\frac{2}{9} = 0.02 = 0.12222\ldots, \ \frac{1}{3} = 0.1 = 0.022222\ldots$$

ja toinen niistä ei sisällä numeroa yksi. Valitsemalla päätepisteiden esityksen niin, että se ei sisällä numeroa yksi, voidaan jokainen joukon C piste esittää laajennuksena kannassa kolme siten, että siinä esiintyy vain numerot nolla ja kaksi. Joukon C jäljelle jääneillä pisteillä on yksikäsitteiset esitykset, niin konstruoimalla esitykset tietyllä tavalla ne eivät sisällä numeroa yksi.

Käänteisesti jokainen välin I piste, joka esitetään laajennuksena kannassa kolme niin, että siinä esiintyy vain lukuja nolla ja kaksi, kuuluu joukkojen C_n leikkaukseen: jos ensimmäinen luku on nolla, niin piste kuuluu välille $[0, 0.02222\ldots]$; jos ensimmäinen luku on kaksi niin piste kuuluu välille $[0.2, 0.2222\ldots]$; toinen numero määrää kuuluuko piste joukon C_2 vasemmalle (0) vai oikealle (2) välille ja niin edelleen.

Tiivistetään edellinen asia seuraavasti.

Lemma 10.1. *Cantorin joukko C koostuu kaikista joukon I pisteistä, jotka voidaan esittää kannassa kolme numeroilla nolla ja kaksi.*

Seuraavan väittämän todistus esittelee äärettömien joukkojen alkeisteorian hyödyllisen menetelmän, niin sanotun *Cantorin lävistäjämenetelmän.*

Lemma 10.2. *Cantorin joukko C on ylinumeroituva.*

Todistus. Oletetaan, että joukko C on numeroituva ja luetellaan kaikki sen pisteet kannassa kolme:

$$\begin{aligned} x_1 =& 0.a_{11}a_{12}\dots, \\ x_2 =& 0.a_{21}a_{22}\dots, \\ & \dots\dots\dots\dots \end{aligned}$$

Muodostetaan piste

$$c = 0.c_1c_2\dots,$$

missä $c_1 = \{0,2\} \setminus a_{11}$, $c_2 = \{0,2\} \setminus a_{22}$ ja niin edelleen. Tällöin $c \in C$ Lemman 10.1 nojalla, mutta koska kaikilla $k \geq 1$, $c_k \neq a_{kk}$, niin se ei kuuluu aiemmalle luetellulle joukon C pisteiden listalle, mikä on ristiriita. □

Määritelmä 10.3. Joukko on *perfekti*, jos se on suljettu ja se ei sisällä erakkopisteitä.

Propositio 10.4. *Cantorin joukko C on perfekti.*

Todistus. Olkoon $x \in C$ ja olkoon S mikä tahansa väli, joka sisältää pisteen x. Koska $x \in \bigcap_{n=0}^{\infty} C_n$, niin $x \in C_n$. Olkoon I_n joukon C_n väli joka sisältää pisteen x. Tarpeeksi suurelle luvulle n pätee, että $I_n \subset S$. Olkoon x_n välin I_n päätepiste siten, että $x_n \neq x$. Joukon C konstruktiolla pätee, että $x_n \in C$ ja $x_n \in S$. Tällöin mikä tahansa väli S, joka sisältää pisteen x sisältää muita joukon C pisteitä. □

Myöhemmin nähdään, että Cantorin joukko esittää geometrista mallia p-adisille kokonaisluvuille millä tahansa alkuluvulla p. Ennen tätä muistellaan metristen avaruuksien välisiä jatkuvien kuvausten määritelmiä ja joitain jatkuvien kuvausten tärkeitä tiettyjä luokkia.

Määritelmä 10.5. Olkoon (X, d) ja (Y, ρ) kaksi metristä avaruutta. Tällöin

- kuvaus (funktio) $f : X \to Y$ on *jatkuva*, jos jokaisen avoimen joukon $V \subset Y$ alkukuva $f^{-1}(V)$ on joukon X avoin joukko;
- kuvaus f on *avoin*, jos jokaisen joukon X avoimen joukon U kuva $f(U)$ on joukon Y avoin joukko;
- kuvaus f on *homeomorfismi*, jos se on jatkuva ja bijektiivinen, sekä sen käänteiskuvaus on jatkuva;
- kuvaus f on *jatkuva pisteessä x*, jos jokaiselle joukon Y pisteen $f(x)$ ympäristöille A pätee, että alkukuva $f^{-1}(A)$ sisältää pisteen x ympäristön;
- kuvaus f on *tasaisesti jatkuva*, jos jokaiselle $\varepsilon > 0$ on olemassa $\delta > 0$ siten, että kun $d(x_1, x_2) < \delta$, niin $\rho(f(x_1), f(x_2)) < \varepsilon$.

Esimerkki 10.6. Isometrinen kuvaus $f : (X, d) \to (Y, \rho)$ on tasaisesti jatkuva.

Todistus. Olkoon $\varepsilon > 0$. Tällöin on olemassa $\delta = \varepsilon/2$ ja kun $d(x_1, x_2) < \delta$, niin $\rho(f(x_1), f(x_2)) = d(x_1, x_2) < \delta = \varepsilon/2 < \varepsilon$ (Isometrinen kuvaus säilyttää etäisyydet. Toisin sanoen kaikilla x_1, $x_2 \in X$, $\rho(f(x_1), f(x_2)) = d(x_1, x_2)$). Tällöin kuvaus f on tasaisesti jatkuva. □

Lause 10.7. *2-adisten kokonaislukujen joukko $\mathbb{Z}_2$ varustetuna 2-adisella normilla $|\cdot|_2$ on homeomorfinen Cantorin joukon C kanssa, joka on varustettu euklidisella normilla $|\cdot|$.*

Todistus. Olkoon kuvaus $\psi : \mathbb{Z}_2 \to C$,

$$\psi : \sum_{i=0}^{\infty} a_i 2^i \mapsto \sum_{i=0}^{\infty} \frac{2a_i}{3^{i+1}}.$$

Näytetään, että ψ on homeomorfismi. Ensiksi huomataan, että joukkojen $\mathbb{Z}_2$ ja C alkioiden yksikäsitteisten esitysten perusteella kuvaus ψ on bijektio.

Jos x_1, $x_2 \in C$ siten, että $|x_1 - x_2| < 1/3^n$, niin luvut x_1 ja x_2 kuuluvat välin I osituksen osaväleihin, joiden pituus on $1/3^n$ samaan tai vierekkäisiin väleihin. Kuitenkin koska suljetuilla väleillä, jotka muodostavat joukon C_n ei ole yhteisiä päätepisteitä, niin x_1 ja x_2 kuuluvat samaan joukon C_n osaan I_n, jolloin niiden ensimmäiset n numeroa ovat samat.

Käänteisesti, jos ensimmäiset numerot paikkaan n ovat samat luvuilla x_1, $x_2 \in C$, niin ne kuuluvat osaan $I_n \subset C_n$. Toisaalta kahden 2-adisen luvun y_1 ja y_2 ensimmäiset n numeroa ovat samat, jos ja vain jos $|y_1 - y_2|_2 < 1/2^n$.

Koska molemmat $1/2^n$ ja $1/3^n$ suppenevat nollaan, kun $n \to \infty$, niin voidaan päätellä, että molemmat ψ ja ψ^{-1} ovat jatkuvia. □

Huomautus 10.8. Lauseesta 10.7 seuraa, että joukoilla C ja $\mathbb{Z}_2$ on sama kardinaalisuus ja Lemman 5.14 nojalla avaruuden $\mathbb{Z}_2$ kardinaalisuus on sama kuin reaaliluvuilla $\mathbb{R}$, jolloin joukon C kardinaalisuus on myös sama kuin reaaliluvuilla $\mathbb{R}$. Yksikkövälin I ylinumeroituvan ei missään tiheän osajoukon olemassaolo on hämmästyttävää. Mutta vielä enemmänkin saadaan todistetuksi: Cantorin joukon "pituus on nolla" siinä mielessä, että siitä poistettujen välien pituuksien summa on yksi. Tämä nähdään, kun vaiheessa n pois jäävien välien lukumäärä on 2^{n-1} ja niiden pituus on $\frac{1}{3^n}$, jolloin niiden summa voidaan laskea kaavalla

$$\sum_{n=1}^{\infty} \frac{2^{n-1}}{3^n} = \frac{\frac{1}{3}}{1 - \frac{2}{3}} = 1.$$

Huomautus 10.9. Cantorin joukon C iteratiivisessa konstruktiossa jokaisessa vaiheessa poistetaan keskimmäiset kolmannekset jäljelle jääneistä väleistä. Tämän takia joukkoa C kuulee monesti kutsuttavan *Cantorin "kolmasosajoukoksi"*. Konstruktiota voidaan muokata siten, että poistetaan välien keskimmäiset neljännekset tai kuudennekset tai jokin muu osa kunhan poistettava väli kuuluu joukkoon $]0, 1[$, jolloin poistettavien välien pituuksien summaksi tulee silti aina 1 (lasku tehdään kuten humautuksessa 10.8). On olemassa myös muita muokkauksia konstruktiosta, jotka johtavat niin sanottuihin *lihaviin Cantorin joukkoihin* eli ei missään tiheisiin Cantorin tapaisiin joukkoihin, joiden pituus on positiivnen (ideana poistaa suhteessa yhä pienempiä ja pienempiä osia).

Seuraus 10.10. *Cantorin joukko C on täysin epäyhtenäinen.*

Todistus. Lauseesta 9.15 seuraa, että $\mathbb{Z}_2$ on täysin epäyhtenäinen. Lauseessa 10.7 määritelty kuvaus ψ on homeomorfismi ja siten jatkuva kuvaus. Koska yhtenäisen joukon kuvajoukko jatkuvalla kuvauksella on yhtenäinen (todistus sivuutetaan), niin seuraa, että joukon C täytyy olla täysin epäyhtenäinen. □

Määritelmä 10.11. Osajoukkoa $A \subset X$ sanotaan *tiheäksi* joukossa X, jos sen sulkeuma $\overline{A}$ on joukko X. Osajoukkoa $A \subset X$ sanotaan *ei missään tiheäksi* joukossa X, jos joukko $X \setminus A$ on tiheä joukossa X.

Huomautus 10.12. Määritelmästä seuraa suoraan, että suljettu joukko on ei missään tiheä, jos ja vain jos se ei sisällä yhtään avointa palloa.

Seurauksesta 10.10 saadaan, että Cantorin joukko on ei missään tiheä, sillä se ei sisällä yhtään väliä.

Tutkitaan nyt avaruutta $\mathbb{Z}_p$. On olemassa erityinen Cantorin joukon tapainen joukko, joka on homeomorfinen avaruuden $\mathbb{Z}_p$ kanssa: kaikkien reaalilukujen joukko väliltä $I = [0, 1]$, joiden laajennus kannassa $2p - 1$ koostuu vain parillisista numeroista. Se muodostetaan samantapaisella prosessilla kuin Cantorin kolmasosajoukko C. Joukon C_1 muodostamiseksi jaetaan joukko I $2p - 1$ moneen yhtäsuureen osaväliin ja poistetaan joka toinen avoin väli. Joukko C_1 voidaan luokitella sen perusteella, että se sisältää kaikki joukon I pisteet, jotka voidaan kirjoittaa kannassa $2p - 1$ muodossa $0.a_1a_2\ldots$, missä a_1 on parillinen. Toistamalla prosessia kaikille joukon C_1 osaväleille saadaan suljettu joukko C_2, jonka pisteiden kaksi ensimmäistä numeroa a_1 ja a_2 ovat parillisia ja niin edelleen. Leikkaus $C^p = \bigcap_{n=0}^{\infty} C_n$ on Cantorin joukon tapainen joukko, joka on ylinumeroituva ja täydellinen. Kuvaus

$$\psi_{2p-1} : \sum_{i=0}^{\infty} a_i p^i \mapsto \sum_{i=0}^{\infty} \frac{2a_i}{(2p-1)^{i+1}} \tag{10.1}$$

joukolta $\mathbb{Z}_p$ joukolle C^p on homeomorfismi, mikä voidaan osoittaa vastaavalla argumentilla kuin Lauseessa 10.7. Havainnolistava kuva joukosta $\mathbb{Z}_5$ on Kuvassa 9.1.

Lisäksi avaruudet $\mathbb{Z}_2$ ja $\mathbb{Z}_p$ ovat homeomorfisia, millä tahansa alkuluvulla p. Tämän todistamiseen riittää muodostaa homeomorfismi kahden Cantorin joukon C^p ja C välille. Kuten usein on tapana matematiikassa, yleistämällä asioita ne helpottuvat. Todistetaan yleisempi väittämä (Lause 10.15), mutta siihen tarvitaan tarvitaan kahta lemmaa.

Lemma 10.13. *Olkoon $A \subset \mathbb{R}$ avoin joukko. Tällöin joukko A on korkeintaan numeroituvan monen avoimen välin pistevieras yhdiste.*

Todistus. Huomioidaan aluksi, että joukon A yhtenäiset komponentit ovat avoimia välejä (Lemma 10.17). Joukon A yhtenäisten osien tulee olla avoimia, sillä muutoin niiden yhdiste ei ole avoin. Seuraava argumentti on yleinen analyysissä ja siinä hyödynnetään tietoa, että rationaaliluvut $\mathbb{Q}$ ovat tiheässä reaalilukujen joukossa $\mathbb{R}$: jokainen joukon A yhtenäinen komponentti sisältää rationaalisen pisteen ja koska rationaalipisteiden joukko on numeroituva, niin joukon A yhtenäiset komponentit ovat aina pistevieraita. Tällöin yhtenäisten komponenttien joukko on korkeintaan numeroituva. □

Lemma 10.14. *Olkoon $f : A \to B$ monotonisesti kasvava bijektiivinen kuvaus kahden reaalilukujen $\mathbb{R}$ suljetun osajoukon välillä. Tällöin f on homeomorfismi.*

Todistus. Huomataan, että kuvaus f^{-1} on myös monotoninen bijektio, jolloin riittää todistaa monotonisen bijektion jatkuvuus (kuvauksesta tulee välttämättä aidosti monotoninen). Olkoon $x \in A$ joukon A raja-arvo. Koska A on suljettu, niin on olemassa joukon A monotoninen pisteiden jono (voidaan olettaa, että tämä on aidosti monotoninen) siten, että $\lim_{n\to\infty} x_n = x$. Tällöin $\{f(x_n)\}$ on joukon B aidosti kasvava jono siten, että $f(x_n) < f(x)$. Koska joukko B on suljettu, niin $\lim_{n\to\infty} f(x_n) = L \in B$, $f(x_n) < L$ ja tällöin $L \leq f(x)$. Jos oletetaan, että $L < f(x)$, niin $f^{-1}(L) < x$, jolloin voidaan löytää sellainen x_n, että $f(x_n) > L$, mikä on ristiriidassa sen kanssa mitä aiemmin todistettiin. Tällöin $\lim_{n\to\infty} f(x_n) = f(x)$. □

Lause 10.15. *Kaikki reaalilukujen joukon kompaktit perfektit täysin epäyhtenäiset osajoukot A ovat homeomorfisia Cantorin joukon C kanssa.*

Todistus. Koska joukko A on kompakti, se on rajoitettu ja koska se on täysin epäyhtenäinen, niin joukko A on ei missään tiheä (se ei sisällä mitään välejä). Olkoon $m = \inf A$ (suurin alaraja) ja $M = \sup A$ (pienin yläraja). Muodostetaan aidosti monotoninen funktio $F : [m, M] \to [0, 1]$ siten, että $F(A) = C$. Joukko $[m, M] \setminus A$ on enintään numeroituvan monen pistevieraan välin yhdiste, joilla ei ole yhteisiä päätepisteitä (koska A on perfekti). Tämä välien joukko ei voi olla äärellinen, sillä A on ei missään tiheä, joten se on numeroituvasti ääretön. Olkoon tämä pistevieraiden välien joukko $\mathcal{I}$.

Määritellään bijektio joukolta $\mathcal{I}$ Cantorin joukon C komplementin muodostamien välien joukolle. Otetaan yksi väli, jonka pituus on suurin mahdollinen (näitä on enimmillään äärellinen määrä) ja merkitään sitä I_1. Määritellään F joukolta I_1 kasvavana lineaarisena kuvauksena, jonka kuvajoukko on väli $]1/3, 2/3[$. Olkoon pisimmät välit I_{21} ja I_{22} joukon I_1 vasemmalla ja oikealla puolella. Kuvataan nämä välit lineaarisesti väleihin $]1/9, 2/9[$ ja $]7/9, 8/9[$ vastaavassa järjestyksessä ja niin edelleen. Jatkamalla tätä prosessia saadaan aidosti monotoninen bijektiivinen kuvaus $[m, M] \setminus A \to [0, 1] \setminus C$. Tämän ymmärtämiseksi huomioidaan, että suurimmat mahdolliset välien pituudet, jotka on valittu prosessin jokaisessa vaiheessa pienenevät. Tämän vuoksi jokaiselle välille $I \subset [m, M] \setminus A$ on vain äärellisen monta väliä joukosta $[m, M] \setminus A$, joiden pituus on suurempaa kuin $|I|$. Tästä päätellään, että kaikki joukon $[m, M] \setminus A$ välit tulevat käytetyiksi. Tällöin on olemassa bijektio välien joukon $\mathcal{I}$, joka kuuluu joukkoon $[m, M] \setminus A$ ja välien kuvajoukkojen kokoelman, jotka ovat joukossa $[0, 1] \setminus C$ kanssa. Bijektio säilyttää välien järjestyksen. Toisin sanoen A on joukon B vasemmalla puolella, jos ja vain jos $F(A)$ on joukon $F(B)$ vasemmalla puolella. Tällöin kuvaus $[m, M] \setminus A \to [0, 1] \setminus C$ on bijektio. Se on aidosti monotoninen jokaisella välillä joukossa $[m, M] \setminus A$ konstruktion perusteella ja jos x ja y kuuluvat eri väleille ja $x < y$, niin $F(x) < F(y)$, sillä kuvaus F säilyttää välien järjestyksen. Kuvaus F voidaan laajentaa jatkuvuuden nojalla poistettujen välien E päätepisteille monotonisesti kasvavaksi kuvaukseksi. Olkoon mille tahansa pisteelle $a \in A$ osajoukko

$$L_a = \{x \in E \mid x < a\}$$

ja määritellään $F(a) = \sup\{f(x) \mid x \in L_a\}$. Koska $a = \sup(L_a)$ ja funktio F on monotonisesti kasvava joukossa $[m, M] \setminus A \cup E$, niin kuvaus F laajentuu koko suljetulle välille $[m, M]$ monotonisesti kasvavaksi kuvaukseksi. Rajoittamalla se joukkoon A ja käyttämällä Lemmaa 10.14 huomataan, että haluttu homeomorfismi joukon C kanssa on muodostettu. □

Seuraus 10.16. *Avaruudet $\mathbb{Z}_2$ ja $\mathbb{Z}_p$ ovat homeomorfisia.*

Lemma 10.17. *Avoimen joukon $A \subset \mathbb{R}$ yhtenäiset komponentit ovat avoimia välejä.*

Todistus. Olkoon joukko $A \subset \mathbb{R}$ avoin. Tällöin sen yhtenäiset komponentit voivat olla eri välejä. Jos ne olisivat muita kuin avoimia välejä, niin niiden yhdiste ei olisi enää avoin, sillä välit ovat pistevieraita. Huomioidaan myös, jos olisi välit $]a, b[$ ja $[b, c[$ niin nämä ajatellaan yhtenä komponenttina sillä $]a, b[\cup[b, c[=]a, c[$ voidaan ajatella yhtenä välinä. $\square$

11. Avaruuden $\mathbb{Z}_p$ euklidiset mallinnukset

Tässä kappaleessa tutkitaan avaruuden $\mathbb{R}^n$ osajoukkoja, jotka ovat homeomorfisia joukkojen $\mathbb{Z}_p$ kanssa. Näitä joukkoja kutsutaan avaruuden $\mathbb{Z}_p$ *euklidisiksi mallinnuksiksi.*

Cantorin joukon tapainen joukko C^p, joka esiteltiin Kappaleessa 10 kuvaa yksiulotteistamallinnusta avaruudesta $\mathbb{Z}_p$. Tämä kuuluu yksiulotteisten mallinnuksien joukkoon, jotka riippuvat muuttujasta b ja saadaan kuvauksella $\psi_b : \mathbb{Z}_p \to [0,1]$,

$$\psi_b\left(\sum_{i\geq 0} a_i p^i\right) = \frac{b-1}{p-1}\sum_{i\geq 0}\frac{a_i}{b^{i+1}}.$$

Kuvaus ψ_b määrää p-adiselle kokonaisluvulle pisteen väliltä $[0,1]$ kannassa b. Kuvaus ψ_b on jatkuva, kun $b > 1$ ja homeomerfismi, jos ja vain jos $b > p$ (Lemma 11.1).

Lemma 11.1. *Olkoon kokonaisluku $b > 1$ ja olkoon $\psi_b : \mathbb{Z}_p \to [0,1]$ kuvaus*

$$\psi_b\left(\sum_{i\geq 0} a_i p^i\right) = \alpha\sum_{i\geq 0}\frac{a_i}{b^{i+1}},$$

joka määrää p-adiselle kokonaisluvulle pisteen väliltä $[0,1]$ kannassa b, jolloin $0 \leq a_i < b$ ja α on normalisoiva vakio, joka antaa kuvaukselle ψ_b maksimiarvoksi yksi. Tällöin

(1) $\alpha = \frac{b-1}{p-1}$;
(2) *kuvaus ψ_b on jatkuva, kun $b \geq p$;*
(3) *kuvaus ψ_b on injektio, jos ja vain jos $b > p$ ja tässä tapauksessa homeomorfismi.*

Todistus.

(1) $\alpha\sum_{i\geq 0}\frac{a_i}{b^{i+1}}$ saa maksimiarvonsa, kun a_i saa suurimman mahdollisen arvonsa. Suurin arvo, jonka se voi saada on $p-1$, sillä se on p-adisen luvun kerroin. Tällöin

$$\alpha\sum_{i\geq 0}\frac{p-1}{b^{i+1}} = \alpha\sum_{i\geq 1}\frac{p-1}{b^i} = \alpha\frac{\frac{p-1}{b}}{1-\frac{1}{b}} = 1.$$

$$\alpha = \frac{1-\frac{1}{b}}{\frac{p-1}{b}} = \frac{b-1}{p-1}.$$

(2) Jatkuvuus todistetaan samalla tavalla kuin Lauseessa 10.7.
(3) Kuvaus ψ_b on injektio, kun $\psi_b\left(\sum_{i>j}(p-1)p^i\right) \neq \psi_b(p^j)$. Tästä saadaan

$$\alpha\frac{p-1}{b^{j+1}(b-1)} = \alpha\frac{p-1}{b^i(b-1)} = \alpha\sum_{i\geq j}\frac{p-1}{b^{i+1}} = \alpha \neq \alpha\frac{1}{b^{j+1}},$$

josta edelleen seuraa, että $p \neq b$. Jos olisi $p > b$, niin tällöin, kun $a_i = p-1$, niin $a_i \geq b$, mikä on ristiriita (kaikilla $a_i < b$). Täytyy siis olla $b > p$.

Homeomorfisuus todistetaan samaan tapaan kuin Lauseessa 10.7.

□

Cantorin joukon tapainen joukko C^p vastaa tilannetta, kun $b = 2p - 1$. Jos $b = p$, niin saadaan surjektiivinen kuvaus, joka ei ole injektio.

Kuten kirjassa [5], kuvataan avaruuden $\mathbb{Z}_p$ korkeampiulotteisia malleja seuraavalla konstruktiolla. Olkoon $E = \mathbb{R}^n$ ja ν injektiivinen kuvaus

$$\nu : S = \{0, 1, \ldots, p-1\} \to E, \quad \nu(S) = \Sigma \subset E.$$

Olkoon nyt kuvaus $\psi = \psi_{\nu,b} : \mathbb{Z}_p \to E$

$$\psi\left(\sum_{i\geq 0} a_i p^i\right) = \alpha \sum_{i\geq 0} \frac{\nu(a_i)}{b^{i+1}}. \tag{11.1}$$

Tutkitan kuvausta $\psi(\mathbb{Z}_p)$. Koska $\mathbb{Z}_p = \bigsqcup_{a_0 \in S}(a_0 + p\mathbb{Z}_p)$ (erillisten joukkojen yhdiste), niin tällöin

$$\psi(\mathbb{Z}_p) = \bigcup_{v\in\Sigma}\left(\alpha\frac{v}{b} + \frac{1}{b}\psi(\mathbb{Z}_p)\right).$$

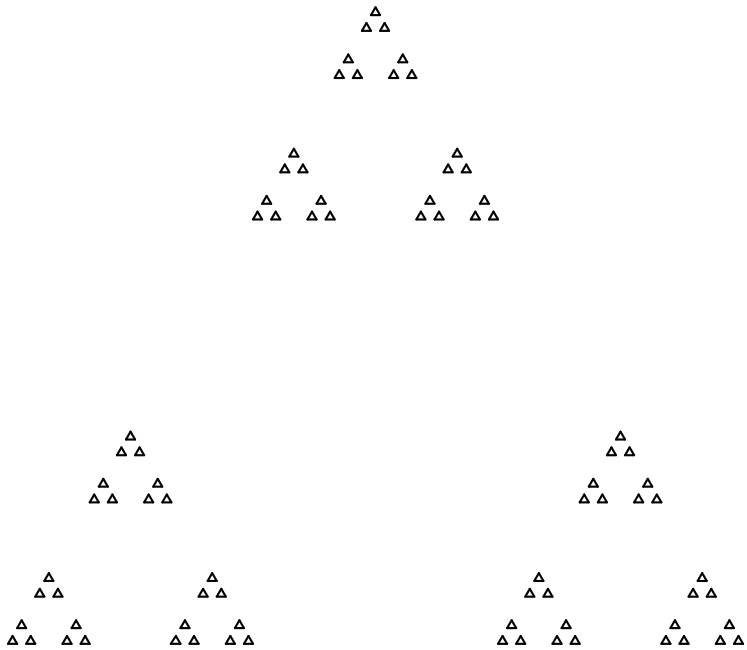
Tarpeeksi isolle luvulle b ja hyvin valitulle normalisoivalle vakiolle α (esimerkiksi, $\alpha = b - 1$ kelpaa) kuvajoukko $\psi(\mathbb{Z}_p)$ on itsesimilaaristen kuvajoukkojen pistevieras yhdiste.

Havainnollistetaan tämä konstruktio usealla esimerkillä.

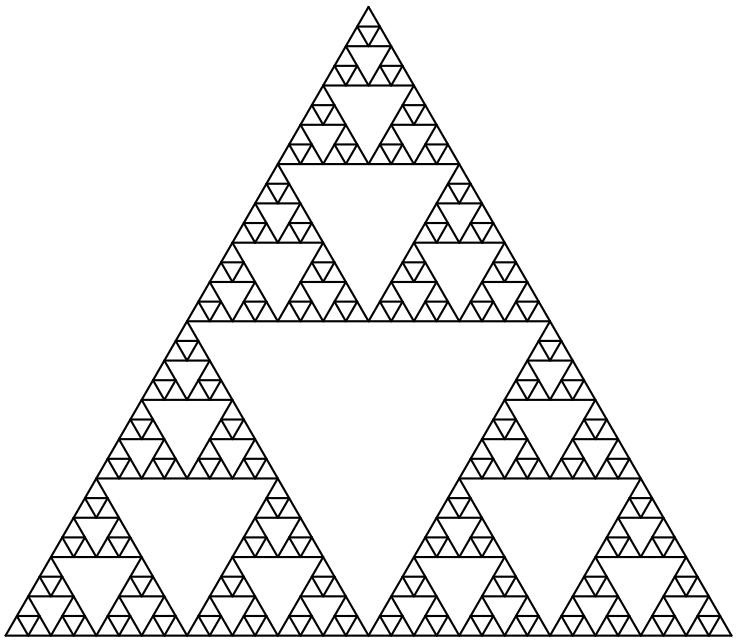
Esimerkki 11.2. Olkoon $p = 3$ ja $E = \mathbb{R}^2$ kannalla $e_1 = (1, 0)$, $e_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$. Määritellään kuvaus ν seuraavasti: $\nu(0) = 0$, $\nu(1) = e_1$ ja $\nu(2) = e_2$. Olkoon kuvaus $\psi : \mathbb{Z}_3 \to \mathbb{R}^2$

$$\psi\left(\sum_{i\geq 0} a_i 3^i\right) = \alpha \sum_{i\geq 0} \frac{\nu(a_i)}{b^{i+1}}.$$

Olkoon $\alpha = b - 1$. Tällä normalisoinnilla $\psi(0) = 0$, $\psi(1) = \frac{b-1}{b}e_1$ ja $\psi(2) = \frac{b-1}{b}e_2$. Huomataan myös, että $e_2 = \psi\left(\sum_{i\geq 0} 2 \cdot 3^i\right) = \psi(-1)$ ja $e_1 = \psi\left(\sum_{i\geq 0} 1 \cdot 3^i\right) = \psi(-\frac{1}{2})$. Lisäksi kuvajoukko $\psi(\mathbb{Z}_3)$ sisältyy tasasivuiseen kolmioon, jonka kärjet ovat pisteissä 0, e_1 ja e_2 (Lemma 11.4 kappaleen lopussa). Kuvaus ψ on injektio, kun $b > 2$ (Lemma 11.1) ja tällöin se tuottaa homeomorfisen kuvajoukon (mallinnus) avaruudesta $\mathbb{Z}_3$ kolmion sisällä (katso Kuva 11.1, kun $b = 3$). Kun $b = 2$, niin kuvajoukko on *Sierpinskin kolmio* (Kuva 11.2), joka on yhtenäinen.



KUVA 11.1. Avaruuden $\mathbb{Z}_3$ malli: $b = 3$



KUVA 11.2. Sierpinskin kolmio: b=2

Esimerkki 11.3. Mille tahansa alkuluvulle $p > 3$ voidaan muodostaa kaksiulotteinen mallinnus avaruudesta $\mathbb{Z}_p$, jolloin se on säännöllinen $(p-1)$-kulmio. Tämän keskipiste on origo ja kärkipisteet $e_1, \ldots, e_{p-1}$ määritellään kuvauksella ν siten, että

$$\nu(0) = 0,\ \nu(1) = e_1, \ldots, \nu(p-1) = e_{p-1}$$

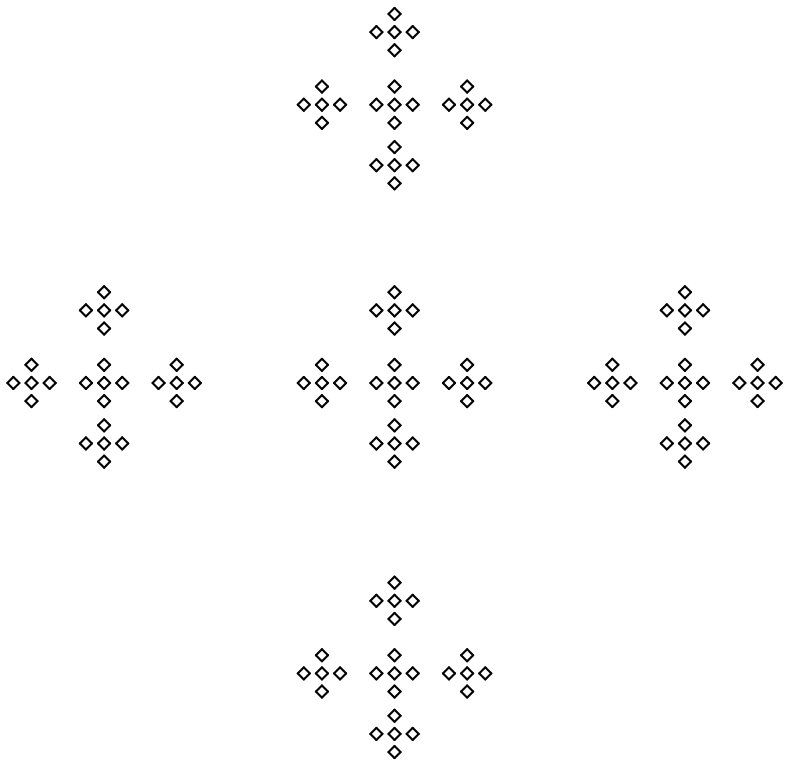
ja kuvaus $\psi = \psi_{\nu,b}$ Lausekkeen (11.1) mukaan. Valitaan $\alpha = b - 1$, jolloin voidaan olla varmoja, että $(p-1)$-kulmion kärjet kuuluvat kuvajoukkoon, esimerkiksi

$$\psi\left(\sum_{i\geq 0}(p-1)\cdot p^i\right) = \psi(-1) = (b-1)\sum_{i\geq 0}\frac{1}{b^{i+1}}e_{p-1} = e_{p-1}.$$

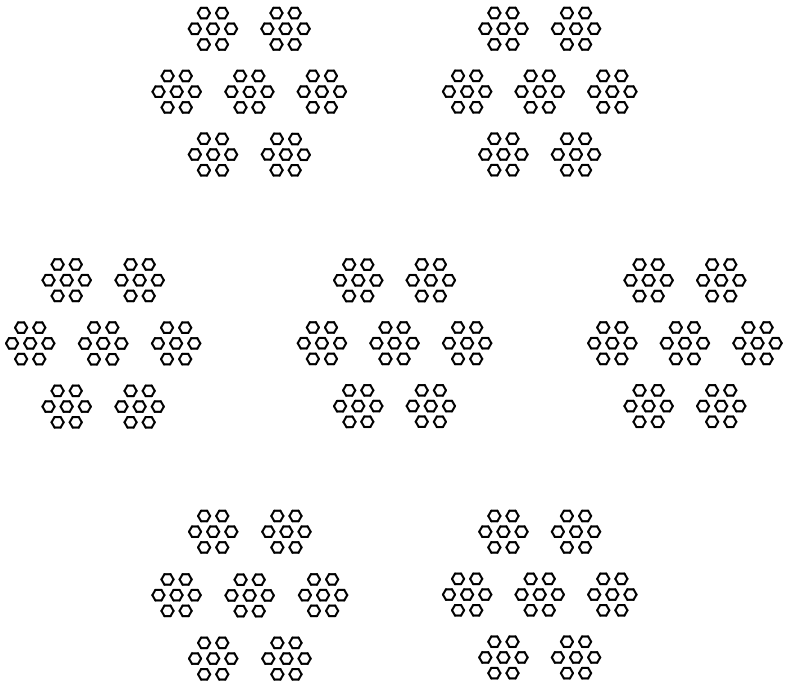
Mille tahansa $a \in \mathbb{Z}_p$ pätee, että $\psi(a)$ on lineaarikombinaatio pisteistä $0, e_1, \ldots, e_{p-1}$, joiden kertoimet ovat ei negatiivisia ja niiden summa on yksi. Tästä seuraa, että $\psi(a)$ kuuluu joukon $e_1, \ldots, e_{p-1}$ *konveksiin sulkeumaan* (toisin sanoen pienin konveksi joukko, joka sisältää mainitut pisteet). Tämä konveksi sulkeuma on joukko

$$\mathcal{C} = \left\{\sum_{i=1}^{p-1} e_i\lambda_i : \lambda_i \geq 0, \sum_{i=1}^{p-1}\lambda_i = 1\right\},$$

joka on $(p-1)$-kulmio. Tarpeeksi suurilla luvun b arvoilla kuvajoukko $\psi(\mathbb{Z}_p)$ on itsesimilaaristen kuvajoukkojen pistevieras yhdiste (katso kuvat 11.3 ja 11.4).



KUVA 11.3. Avaruuden $\mathbb{Z}_5$ malli: $b = 4$



KUVA 11.4. Avaruuden $\mathbb{Z}_7$ malli: $b = 4$

Kaikilla tämän kappaleen esimerkeillä on yhteinen ominaisuus: kuva A on fraktaali. Toisin sanoen m kopion itsestään yhdiste, joista jokaista on skaalattu kertoimella $1/b$. Niiden itsesimilaarisuusulottuvuus d on "määritelty" seuraavalla kaavalla:

$$E(A) = mE\left(\frac{1}{b}A\right) = m\left(\frac{1}{b}\right)^d E(A),$$

missä $E(A)$ on joukon A *laajennuksen* intuitiivinen käsite, joka on astetta d oleva homogeeninen funktio. Tällöin $d = \frac{\log m}{\log b}$. Seuraava taulukko käsittelee Cantorin "kolmasosajoukkoa" ja esimerkkejä 11.2 ja 11.3.

Fraktaali	m	b	$d = \frac{\log m}{\log b}$
Kuva 10.1 (Cantorin joukko C)	2	3	0.63
Kuva 11.1 (avaruuden $\mathbb{Z}_3$ malli)	3	3	1
Kuva 11.2 (Sierpinskin kolmio)	3	2	1.58
Kuva 11.3 (avaruuden $\mathbb{Z}_5$ malli)	5	4	1.16
Kuva 11.4 (avaruuden $\mathbb{Z}_7$ malli)	7	4	1.4

Lemma 11.4. *Esimerkissä 11.2 kuvajoukko $\psi(\mathbb{Z}_3)$ sisältyy tasasivuiseen kolmioon, jonka kärkipisteet ovat $0, e_1$ ja e_2.*

Todistus. Olkoon $a \in \mathbb{Z}_3$. Koska $a_i \in \{0, 1, 2\}$, niin tällöin

$$\begin{aligned}
\psi(a) &= (b-1) \sum_{i \geq 0} \frac{\nu(a_i)}{b^{i+1}} \\
&= (b-1) \sum_{\forall\, a_i = 0} \frac{0}{b^{i+1}} + (b-1) \sum_{\forall\, a_i = 1} \frac{e_1}{b^{i+1}} + (b-1) \sum_{\forall\, a_i = 2} \frac{e_2}{b^{i+1}} \\
&= \left(\sum_{\forall\, a_i = 1} \frac{b-1}{b^{i+1}} \right) e_1 + \left(\sum_{\forall\, a_i = 2} \frac{b-1}{b^{i+1}} \right) e_2.
\end{aligned}$$

Merkitään $\lambda_1 = \sum_{\forall\, a_i = 1} \frac{b-1}{b^{i+1}}$ ja $\lambda_2 = \sum_{\forall\, a_i = 2} \frac{b-1}{b^{i+1}}$, missä $\lambda_1, \lambda_2 \geq 0$. Tällöin $\lambda_1 + \lambda_2 \leq 1$, sillä $\sum_{i \geq 0} \frac{b-1}{b^{i+1}} = 1$. Tästä seuraa, että kuvapisteen $\psi(a)$ on kuuluttava tasasivuiseen kolmioon, jonka kärkipisteet ovat $0, e_1$ ja e_2. $\square$

Viitteet

[1] J. W. S. Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986.
[2] F. Q. Gouvêa, *P-adic numbers*, Springer-Verlag, Berlin, Heidelberg, toinen painos, 1997.
[3] S. Katok, *P-adic analysis compared with real*, American Mathematical Society, Yhdysvallat, 2007.
[4] C. C. Pugh, *Real mathematical analysis*, Springer Science+Business Media, Inc.,Yhdysvallat, 2002.
[5] A. M. Robert, *A Course in p-adic analysis*, Springer-Verlag, Berlin, Heidelberg, NewYork, 2000.
[6] W. Rudin, *Principles of mathematical analysis*, Kolmas painos, McGraw-Hill, Inc., Japani, 1976.