Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Matemaatika ja statistika instituut
Matemaatika eriala

Kristiina Mähar

p-aadilised arvud

Bakalaureusetöö (9 EAP)

Juhendaja: Lauri Tart

Tartu 2017

p-aadilised arvud

Bakalaureusetöö
Kristiina Mähar

Lühikokkuvõte. Käesoleva bakalaureusetöö eesmärgiks on anda ülevaade p-aadilistest arvudest ja nende omadustest. Töös on käsitletud normeeritud korpusi ja ultrameetrilisi ruume, p-aadiliste arvude korpust ning selle algebralisi, topoloogilisi ja analüütilisi omadusi, p-aadilist aritmeetikat, ratsionaalarvude p-aadilist reaksarendust ning p-aadiliste polünoomide juuri. Muuhulgas vaadeldakse erinevaid ratsionaalarvude korpusel defineeritud norme ja nende ekvivalentsust ning tehakse sissejuhatus p-aadiliste kompleksarvude ja g-aadiliste arvude valdkondadesse (kordarvulise g jaoks).

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria.

Märksõnad. p-aadilised arvud, p-aadiline analüüs, ühejuured, normeeritud korpused

p-adic numbers

Bachelor's thesis
Kristiina Mähar

Abstract. The purpose of this bachelor's thesis is to consider p-adic numbers and their properties. Topics covered include normed fields and ultrametric spaces, the field of p-adic numbers and its algebraic, topological and analytical properties, p-adic arithmetic, the p-adic expansion of rational numbers and roots of p-adic polynomials. Additionally, we will take a look at the equivalence of norms over rational numbers and make an introduction to the topics of p-adic complex numbers and g-adic numbers (for a composite number g).

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory.

Keywords. p-adic numbers, p-adic analysis, roots of unity, normed fields

Sisukord

Sissejuhatus

Käesoleva bakalaureusetöö eesmärgiks on anda ülevaade p-aadilistest arvudest ning nende omadustest. Esimesena kirjeldas p-aadilisi arve Kurt Hensel 19. sajandi lõpul. Kuigi kohe alguses neile praktilist rakendust ei leitud ja neid käsitleti kui eksootilist osa puhtast matemaatikast, siis tänapäeval on p-aadilistel arvudel matemaatikas oluline koht. Seda näiteks arvuteoorias, kus p-aadilised arvud võimaldavad kasutada matemaatilise analüüsi meetodeid erinevate probleemide lahendamiseks, astmeridadega seotud tehnikate arvuteooriasse sissetoomine oligi üks p-aadiliste arvude esimesi matemaatikasiseseid rakendusalasid. Kõige tuntuimaks p-aadilisi arvude rakendusteks on ilmselt Andrew Wiles'i Fermat' suure teoreemi tõestus. p-aadilite arvude põhjal on isegi välja töötatud terve matemaatika valdkond, mida kutsutaks p-aadilisteks analüüsiks, ning mis pakub alternatiivi klassikalisele matemaatilisele analüüsile.

p-aadilistel arvudel leidub mitmeid kasutusalasid ka väljaspool matemaatikat. Näiteks leidub neil olulisi rakendusi füüsikas, kus teatud mudeleid on kasulikum kirjeldada just p-aadiliste arvude abil. Samuti kasutatakse p-aadilisi arve näiteks arvutiteaduses pseudojuhuslike arvude genereerimiseks, bioloogias keeruliste süsteemide kirjeldamiseks ning veel paljudes teistes valdkondades. Huvitatud lugejal on p-aadiliste arvude ning nende rakendustega võimalik põhjalikumat tutvuda artikli [8] abil.

Siin esitatud materjal täiendab Toivo Leigeri poolt koostatud mittearhimeedilise funktsionaalanalüüsi loengukonspektile [9], mis on praktiliselt ainus põgusam sellealane eestikeelne käsitlus. Seetõttu on edasipidi eelnimetatud loengukonspektis juba tõestatud tulemustele ületõestamistest loobutud ning vastavate konspekti [9] osadele viidatud.. Käesolev bakalaureusetöö on referatiivne ning selle kirjutamisel oli peamiseks allikaks Svetlana Katoki poolt kirjutatud õpik [7]. Lisaks sellele kasutati töö kirja panekul raamatuid [3],[4],[1], elektroonilisi märkmeid [5], [6] ja loengukonspekte [9] ,[2].

Esimeses, sissejuhatavas peatükis on ära toodud meetriliste ruumide ja normeeritud korpustega seotud põhimõisted ning nende omadused, mida töös hiljem vaja läheb. Lisaks antakse ülevaade normeeritud korpuse täielikustamise protsessist.

Teises peatükis tuuakse sisse mittearhimeedilise normi ja ultrameetrilise ruumi mõisted ning vaadeldakse nende omadusi. Samuti näidatakse erinevust arhimeediliste ning mittearhimeediliste normide vahel ning kirjeldatakse mõningaid olulisemaid ultrameetriliste ruumide omadusi.

Kolmandas peatükis defineeritakse p-aadiline norm ja konstrueeritakse p-aadiliste arvude korpus. Näidatakse, et p-aadilistel arvudel on ühene nn. kanooniline esitus, ja tehakse sellest mõned järeldused.

Järgmises ehk neljandas peatükis vaadatakse lähemalt p-aadiliste arvude aritmeetikat nii abstraktselt, kui ka konkreetsete näidet abil. Kirjeldatakse täisarvu mõistet laiendavaid p-aadilisi täisarve ning nende pööratavust. Tuleb välja, et leidub p-aadilisi täisarve, mille pöördelemendid on samuti p-aadilised täisarvud.

Viiendas peatükis on esitatud meetod ratsionaalarvude arendamiseks p-aadilisteks arvudeks ning esitatud tingimus p-aadilise arvu ratsionaalarvuks olemise jaoks. On näidatud, kuidas seda teha mitmetel erijuhtudel ning toodud selle kohta ka konkreetseid näited.

Sellele järgnevas, kuuendas peatükis tõestatakse oluline tulemus polünoomide juurte leidmiseks p-aadiliste arvude korpuses (Henseli lemma). Viimasest tuletatakse kriteeriumid juurte kuulumiseks p-aadiliste täisarvude hulka ja ruutjuurte leidumiseks p-aadiliste arvude korpuses.

Seitsmendas peatükis on eraldi vaatluse all p-aadiliste arvude analüütilised, topoloogilised ning algebralised omadused. Kirjeldatakse näiteks kerasid ning nende vahekordi korpuses $\mathbb{Q}_p$, p-aadiliste täisarvude täielikkust, p-aadiliste ridade koonduvust ja absoluutselt koonduvust, p-aadilisi ühejuuri ning näidatakse, et p-aadilised täisarvude hulk on p-aadiliste arvude korpuse kõikjal tihe alamhulk. Tuleb välja, et p-aadilistel arvudel on reaalarvudega sarnaseid omadusi, aga ka selliseid huvitavaid omadusi, mida reaalarvude hulgal ei ole, näiteks koonduvad read parajasti siis, kui rea üldliige hääbub, kõik kerad p-aadiliste arvude ruumis on nii kinnised kui lahtised hulgad ning neil pole kindlat keskpunkti ja $\sqrt{-1} \in \mathbb{Q}_p$ parajasti siis, kui $p \equiv 1 \pmod 4$. Peatükki lõpus on tehtud sissejuhatus p-aadiliste kompleksarvude valdkonda.

Kaheksandas peatükis sõnastatakse ning tõestatakse Ostrowski teoreem, mis näitab, et kõik mittetriviaalsed normid ratsionaalarvude korpusel on ekvivalentsed kas absoluut väärtusega või ühega p-aadilistest normidest. Sellest järeldub, et ratsionaalarvude korpuse ainsateks täielditeks on reaalarvude korpus ning p-aadiliste arvude korpused.

Üheksandas ehk viimases peatükis antakse lühike ülevaade g-aadilistest normidest ja arvudest ehk sellest, mis juhtub siis, kui proovida defineerida p-aadilisele normile sarnane g-aadiline norm, kus g on kordarv.

1 Normeeritud korpused

Selles peatükis tuletame meelde vajalikud funktsionaalanalüüsi mõisted ja defineerime normeeritud korpused, kirjeldame, mida kujutab endast normide ekvivalentsus ning kuidas normeeritud korpuseid on võimalik täielikustada.

1.1 Normid ja jadad

Tuletame esiteks meelde meetrika ja selle järgi koonduvusega seotud mõisted ning vaatleme neid normeeritud korpuste kontekstis.

Definitsioon 1.1. *Meetriline ruum* on selline hulk M, millel on määratud kujutus $d : M \times M \to \mathbb{R}$, mida nimetatakse *meetrikaks* ning millel on järgmised omadused:

(a) $d(x, y) \geq 0$; $d(x, y) = 0 \iff x = y$,

(b) $d(x, y) = d(y, x)\ \forall x, y \in M$,

(c) $d(x, y) \leq d(x, z) + d(z, y)\ \forall x, y, z \in M$. (kauguse kolmnurga võrratus)

Arvu $d(x, y)$ nimetatakse punktide x, y vaheliseks *kauguseks.*
Enne järgmise definitsiooni juurde minekut, teeme kõigepealt vaikimisi eelduse, et selles töös on kõik korpused kommutatiivsed.

Definitsioon 1.2. Olgu $(K, +, \cdot)$ korpus**.** *Norm* korpused K on kujutus $\|\cdot\| : K \to [0, \infty)$, millel on järgmised omadused:

(A1) $\|x\| = 0$ ainult siis, kui $x = 0$,

(A2) $\|xy\| = \|x\| \, \|y\| \quad \forall x, y \in K$,

(A3) $\|x + y\| \leq \|x\| + \|y\|, \quad \forall x, y \in K$ (normi kolmnurga võrratus).

Normiga varustatud korpust $K = (K, \|\cdot\|)$ nimetatakse *normeeritud korpuseks* ningo omadusi (A1)-(A3) *normi aksioomideks.* Normi kutsutakse *triviaalseks,* kui $\|0\| = 0$ ja $\|x\| = 1$ iga $0 \neq x \in K$ korral. Olgu 1 korpuse K ühikelement ja -1 ühikelemendi vastandelement. Paneme tähele, et iga $n \in \mathbb{N}$ korral

$$n \cdot 1 = \underbrace{1 + ... + 1}_{n \text{ liidetavat}} \in K.$$

Edaspidi tähistame sellist elementi lihtsalt naturaalarvuga n.

Lause 1.3 ([9, lause 2.1])**.** *Mis tahes $x, y \in K$ korral kehtivad järgmised omadused:*

(a) $\|1\| = \|-1\| = 1$,

(b) $\|x\| = \|-x\|$,

(c) $\|x \pm y\| \geq |\|x\| - \|y\||$,

(d) $\|x - y\| \leq \|x\| + \|y\|$,

(e) $\left\|\frac{x}{y}\right\| = \frac{\|x\|}{\|y\|}$,

(f) $\|n\| \leq n \; \forall n \in \mathbb{N}$.

Olgu $d(x, y) = \|x - y\|$. Normi definitsioonist ning selle omadustest järeldub, et d on meetrika. Tõepoolest, $d(x, y) = 0$ siis ja ainult siis, kui $x = y$; omadusest (b) järeldub, et $d(x, y) = d(y, x)$ ning omadusest (d) järeldub kolmnurga võrratuse kehtimine. Seega on $(K, \|\cdot\|)$ meetriline ruum ning sellisel juhul öeldakse, et see meetrika on *indutseeritud* normi $\|\cdot\|$ poolt.

Definitsioon 1.4. Öeldakse, et jada (x_n), kus $x_n \in K$

(a) on *tõkestatud,* kui leidub selline reaalarv $C > 0$, et

$$\|a_n\| < C \; \forall n \in \mathbb{N};$$

(b) on *hääbuv* ehk *nulljada*, kui

$$\lim_{n\to\infty} \|a_n\| = 0$$

ehk iga $\varepsilon > 0$ korral leidub selline $N(\varepsilon) \in \mathbb{N}$, et iga naturaalarvu $n > N$ korral $\|a_n\| < \varepsilon$;

(c) on *Cauchy jada,* kui

$$\lim_{n,m\to\infty} \|a_n - a_m\| = 0$$

ehk iga $\varepsilon > 0$ korral leidub selline $N(\varepsilon) \in \mathbb{N}$, et kõigi naturaalarvude $n, m > N$ korral $\|a_n - a_m\| < \varepsilon$;

(d) *koondub* arvuks $a \in K$ ehk $\lim_{n\to\infty} a_n = a$, kui

$$\lim_{n\to\infty} \|a - a_n\| = 0$$

ehk iga $\varepsilon > 0$ korral leidub selline $N \in \mathbb{N}$, et iga naturaalarvu $n > N$ korral $\|a_n - a\| < \varepsilon$.

Sellest definitsioonist järeldub, et iga hääbuv jada koondub nulliks. Kolmnurga võrratust kasutades näeme ka, et iga koonduv jada on Cauchy jada. Tõepoolest, olgu $\lim_{n\to\infty} a_n = a$ ning fikseerime vabalt $\varepsilon > 0$. Kui naturaalarvud $n, m > N\left(\frac{\varepsilon}{2}\right) \in \mathbb{N}$, siis

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

Definitsioon 1.5. Meetrilise ruumi M alamhulka A nimetatakse lahtiseks hulgaks, kui igal selle hulga elemendil leidub selline ümbrus, mis kuulub täielikult hulka A.

Definitsioon 1.6. Meetrilise ruumi M alamhulka A nimetatakse kinniseks hulgaks, kui see sisaldab kõiki oma rajapunkte, st kõiki selliseid punkte $a \in M$, et

$$B(a,\varepsilon) = \{x \in M \,|\, \|x-a\| < \varepsilon\} \cap A \neq \emptyset \quad \text{ja} \quad B(a,\varepsilon) \cap (M \backslash A) \neq \emptyset \forall \varepsilon > 0.$$

1.2 Normide ekvivalentsus

Kirjeldame siinkohal võimalike seoseid korpuse K normid vahel..

Definitsioon 1.7. Norme $\|\cdot\|_1$ ja $\|\cdot\|_2$ korpuses K nimetatakse *ekvivalentseteks*, neil on samad Cauchy jadad ehk

$$\lim_{m,n} \|a_n - a_m\|_1 = 0 \Leftrightarrow \lim_{m,n} \|a_n - a_m\|_2 = 0,$$

Viimast situatsiooni tähistatakse $\|\cdot\|_1 \sim \|\cdot\|_2$.

Järgmiseks tõestame ühe lihtsa aga väga kasuliku lause.

Lause 1.8. *Olgu $x \in K$. Sellisel juhul $\|x\| < 1$ parajasti siis, kui $\lim_{n\to\infty} \|x^n\| = 0$.*

Tõestus. Olgu x korpuse K element ning kehtigu $\|x\| < 1$. Kuna $\|x^n\| = \|x\|^n$, siis saame, et

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

Teisipidi, kui $\|x\| \geq 1$, siis iga naturaalarvu n korral $\|x^n\| \geq 1$ ning seega $\lim_{n\to\infty} \|x^n\| \neq 0$. □

Lause 1.9. *Olgu $\|\cdot\|_1$ ja $\|\cdot\|_2$ normid korpusel K. Kui $\|\cdot\|_1$ on triviaalne norm ja $\|\cdot\|_1 \sim \|\cdot\|_2$ siis on ka $\|\cdot\|_2$ triviaalne norm.*

Tõestus. Olgu $\|\cdot\|_1$ triviaalne norm üle korpuse K ning $\|\cdot\|_1 \sim \|\cdot\|_2$. Eeldame vastu väiteliselt, et $\|\cdot\|_2$ ei ole triviaalne. Siis leidub selline $a \in K$ nii, et $0 < \|a\|_2 < 1$ ja seega $\lim_{n\to\infty} \|a^n\|_2 = 0$. Kuid tänu sellele, et normid $\|\cdot\|_1$ ja $\|\cdot\|_2$ on omavahel ekvivalentsed, kehtib ka $\lim_{n\to\infty} \|a^n\|_1 = 0$, mis on aga vastuolus eeldusega, et $\|\cdot\|_1$ on triviaalne, kuna eeldasime, et $a \neq 0$ ning järelikult $\lim_{n\to\infty} \|a^n\|_1 = \lim_{n\to\infty} 1^n \neq 0$. Järelikult on norm $\|\cdot\|_2$ samuti trviaalne □

Lause 1.10. *Kaks normi $\|\cdot\|_1$ ja $\|\cdot\|_2$ korpusel K on ekvivalentsed parajasti siis, kui leidub selline positiivne reaalarv a, et*

$$\|x\|_1 = \|x\|_2^a \ \forall x \in K. \tag{1.1}$$

Tõestus. TARVILIKUS. Olgu $\|\cdot\|_1 \sim \|\cdot\|_2$. Oletame vastuväiteliselt, et võrdus (1.1) ei kehti ehk leiduvad sellised $x, y \in K$, mille korral

$$a(x) = \frac{\ln \|x\|_2}{\ln \|x\|_1} \neq \frac{\ln \|y\|_2}{\ln \|y\|_1} = a(y).$$

Sellisel juhul on vektorid $a = (\ln \|x\|_1, \ln \|x\|_2)$ ja $b = (\ln \|y\|_1, \ln \|y\|_2)$ lineaarselt sõltumatud ning moodustavad vektorruumi $\mathbb{R}^2$ baasi. Olgu $\|\cdot\|$ ruumi ℓ_2^2 norm ehk eukleidiline kaugus ruumis $\mathbb{R}^2$. Iga vektor $v \in \mathbb{R}^2$ on võimalik kirja panna kujul $v = v_1 a + v_2 b$. Defineerime $w = \lfloor v_1 \rfloor a + \lfloor v_2 \rfloor b$, kus $\lfloor \cdot \rfloor$ on alumise täisosa funktsioon. Siis

$$\begin{aligned} \|v - w\| &= \|v_1 a - \lfloor v_1 \rfloor a + v_2 b - \lfloor v_2 \rfloor b\| \\ &\leq \|a\| \|v_1 - \lfloor v_1 \rfloor\| + \|b\| \|v_2 - \lfloor v_2 \rfloor\| \\ &\leq \|a\| + \|b\| =: R., \end{aligned}$$

st, et kõik ruumi $\mathbb{R}^2$ vektorid on mingi raadiuse R kaugusel mõnest "täisarvulisest" vektorist. Muuhulgas on igas keras $\bar{B}(R, a)$ mõni "täisarvuline" vektor. Leiame need järjest keradest, mis on pandud nn "ristkülikutesse" $[2kR, 2(k+1)R] \times (-\infty, -kR]$. See tähendab, et on võimalik leida jada $(v_{k,1}, v_{k,2})$, nii, et iga $k = 1, 2, \ldots$

$$v_{k,1} a + v_{k,2} b \in [2kR, 2(k+1)R] \times (-\infty, -kR].$$

See omakorda tähendab, et $2kR \leq v_{k,1} \ln \|x\|_1 \cdot v_{k,2} \ln \|y\|_1 \leq 2(k+1)R$ ja $v_{k,1} \ln \|x\|_2 + v_{2,1} \ln \|y\|_2 \leq -kR$.

Olgu jada $z_k = x^{v_{k,1}} y^{v_{k,2}} \in K$. Siis

$$\|z_k\|_2 = \|x\|_2^{v_{k,1}} \|y\|_2^{v_{k,2}} = \|x\|_2^{\frac{\ln \|y\|_2}{\ln \|x\|_2} v_{k,2} + v_{k,1}} \leq \|x\|_2^{\frac{-kR}{\ln \|x\|_2}} = e^{-kR}.$$

Kui $k \to \infty$, siis $\|z_k\|_2 \to 0$ ehk z_k on normi $\|\cdot\|_2$ järgi hääbuv jada ning seega Cauchy. Samas

$$\|z_k\|_1 = \|x\|_1^{v_{k,1}} \|y\|_1^{v_{k,2}} = \|x\|_1^{\frac{\ln \|y\|_1}{\ln \|x\|_1} v_{k,2} + v_{k,1}} \in \left[e^{2uR}, e^{2(u+1)R}\right].$$

Kui $u - l \geq 2$, siis

$$\|z_u - z_l\|_1 \geq \|z_u\|_1 - \|z_l\|_1 \geq e^{2uR} - e^{2(l+1)R} \geq e^{2(u+2)R} - e^{2(l+1)R} \geq e^{2R} - 1 > 0.$$

Järelikult (z_n) ei ole Cauchy jada normi $\|\cdot\|_1$ suhtes. See on aga vastuolus meie eeldusega, et normid $\|\cdot\|_1$ ja $\|\cdot\|_2$ on ekvivalentsed.

PIISAVUS. Oletame, et leidub selline positiivne reaalarv a, et

$$\|x\|_1 = \|x\|_2^a, \ \forall x \in K.$$

On lihtne näha, et siis on nendel normidel samad Cauchy jadad. Tõepoolest, kui jada (a_n) on Cauchy jada normi $\|\cdot\|_1$ehk iga $\varepsilon > 0$ jaoks leidub selline indeks $N > 0$, et kõigi

$m, n \geq N_1$ korral

$$\|a_n - a_m\|_1 = \|a_n - a_m\|_2^a < \varepsilon,$$

siis mingi indeks N_2 korral ilmselt

$$\|a_n - a_m\|_2 < \varepsilon,$$

kui $n, m > N_2$. □

Järgmisena kirjeldame kõiki norme ratsionaalarvude korpusel, mis on ekvivalentsed absoluutväärtusega.

Lause 1.11. *Kujutus $\|x\| = |x|^a, 0 < a \in \mathbb{R}$, on norm ratsionaalarvude hulgal $\mathbb{Q}$ siis ja ainult siis, kui $a \leq 1$. Kõik sellised normid on ekvivalentsed absoluutväärtusega $|\cdot|$.*

Tõestus. Olgu $a \leq 1$. Kahe esimese normi aksioomi kehtimine on ilmne, peame kontrollima vaid kolmnurga võrratuse kehtivust. Oletame lihtsue mõttes, et $|y| \leq |x|$, juhul $|y| > |x|$ on tõestus sarnane. Siis

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

Võrratus $|x|^a \left(1 + \frac{|y|}{|x|}\right)^a \leq |x|^a \left(1 + \frac{|y|}{|x|}\right)$ järeldub sellest, et $\left(1 + \frac{|y|}{|x|}\right)^a = t^a \leq t$, kui $t > 1$ ja $a \leq 1$, ning järgmine võrratus asjaolust, et $\frac{|y|}{|x|} < 1$ ehk $t^a \geq t$, kui $0 \leq t \leq 1$ ja $a \leq 1$. Kui aga $a > 1$, siis kolmnurga võrratus ei kehti. Näiteks $|1+1|^a = 2^a > |1|^a + |1|^a = 2$.

See, et $|\cdot|^a \sim |\cdot|$, järeldub otseselt eelmisest lausest. □

1.3 Normeeritud korpuse täielikustamine

Antud alapeatükis anname ülevaate sellest, kuidas suvalise normeeritud korpuse K jaoks konstrueerida seda sisaldav täielik normeeritud korpus $\overline{K}$.

Definitsioon 1.12. Normeeritud korpust K nimetatakse täielikuks, kui iga Cauchy jada selles korpuses koondub.

Definitsioon 1.13. Meetrilisi ruume K ja L koos oma kaugustega d_1 ja d_2 nimetatakse *isomeetriliseks*, kui leidub selline sürjektsioon $\varphi : K \to L$, mis säilitab elementide vahelise kauguse, st

$$d_1(\varphi(x), \varphi(y)) = d_2(x, y),$$

kus $x, y \in K$.

Definitsioon 1.14. Meetrilise ruumi K *täieldiks* nimetatakse sellist täielikku meetrilist ruumi L , mille puhul on M on isomeetriline ruumi L kõikjal tiheda alamruumiga.

Lause 1.15 ([9, peatükk 2.3])**.** *Kui* (a_n) *ja* (b_n) *on Cauchy jadad, siis seda on ka jadad* $(a_n + b_n), (a_n - b_n)$ *ja* $(a_n b_n)$*.*

Olgu $(K, \|\cdot\|)$ normeeritud korpus, millel on defineeritud liitmis-ja korrutamistehe, ning olgu $C(K)$ kõigi selle korpuse Cauchy jadade hulk. Kuna K on kommutatiivne ning eelmise lause põhjal on $C(K)$ kinnine liitmise ja korrutamise suhtes, siis on $C(K)$ kommutatiivne ring. Selle nullelemendiks on jada

$$\bar{0} = (0, 0, 0, \ldots)$$

ja ühikelemendiks jada

$$\bar{1} = (1, 1, 1, \ldots).$$

Definitsioon 1.16. Ringi R nullist erinevat elementi $a \in R$, mille korral leidub kas nullist erinev element $b \in R$ või nullist erinev element $c \in R$ nii, et kas $ab = 0$ või $ca = 0$, nimetatakse *nulliteguriks.*

Lause 1.17 ([1, lause 3.2.21])**.** *Korpus ei sisalda nullitegureid.*

Lause 1.18. $C(K)$ *ei ole korpus.*

Tõestus. $C(K)$ ei ole korpus, sest see sisaldab nullitegureid. Üheks neist on näiteks

$$(1, 0, 0, \ldots) \cdot (0, 1, 0, \ldots) = \bar{0}.$$

□

Definitsioon 1.19. Kommutatiivse ringi R mittetühja alamhulka I nimetatakse selle ringi *ideaaliks*, kui on täidetud järgmised tingimused:

(a) $a, b \in I \Longrightarrow a + b \in I$;

(b) $a \in I \Longrightarrow ar \in I$ mis tahes $a, r \in R$ korral.

Definitsioon 1.20. Olgu R ring, I selle ringi ideaal ning tähistame $R/I = \{\overline{x} = x + i \,|\, x \in R, i \in I\}$. Defineerime tehted võrdustega

$$\overline{x} + \overline{y} = \overline{x + y}, \quad \overline{x} \cdot \overline{y} = \overline{xy}.$$

Hulka R/I nimetatakse ringi R *faktorringiks* ideaali I järgi.

Olgu $P \subset C(K)$ korpuse K kõigi hääbuvate jadade hulk. Hulk P on ringi $C(K)$ ideaal. Tõepoolest, kui $(a_n), (b_n) \in P$, siis tänu $C(K)$ kommutatiivsusele ning lausele 1.5 kuuluvad ka $(a_b \pm b_n)$ ja $(a_n b_n)$ hulka P. Faktoriseerides ringi $C(K)$ tema ideaali P järgi saame uue hulga $\overline{K} = C(K)/P$. Selle hulga elemendid on korpuse K Cauchy jadade ekvivalentsiklassid.

Lemma 1.21 ([9, lemma 6.1.11]). *Kaks klassi on ekvivalentsed parajasti siis, kui nende esindajate vahe on nulljada.*

Olgu $a, b \in K$ suvalised. Paneme tähele, et konstantsed jadad

$$\bar{a} = (a, a, a, \ldots)$$

ja

$$\bar{b} = (b, b, b, \ldots)$$

esindavad hulgas $\overline{K}$ erinevaid ekvivalentsiklasse, sest

$$\bar{a} - \bar{b} = (a - b, a - b, a - b, \ldots)$$

ei ole hääbuv jada, kui $a \neq b$. Seega on korpus K hulga $\overline{K}$ alamhulk: kui $a \in K$, siis samastatakse see hulgas $\overline{K}$ konstantse jadaga $\bar{a} = (a, a, a, \ldots)$. Viimane samastus ongi korpuste vaheline isomeetria.

Lause 1.22 ([9, peatükk 2.3]). *Kui* $(a_n) \sim (a'_n)$ *ning* $(b_n) \sim (b'_n)$ *korpuses* K*, siis ka* $(a_n \pm b_n) \sim (a'_n \pm b'_n)$ *ja* $(a_n b_n) \sim (a'_n b'_n)$.

Olgu $(a_n) \in A$ ja $(b_n) \in B$ hulga $\overline{K}$ erinevad ekvivalentsiklassid . Defineerime tehted järgmiselt:

$$A + B = \overline{(a_n + b_n)} \quad \text{ja} \quad A \cdot B = \overline{(a_n \cdot b_n)}.$$

Lause 1.23 ([9, teoreem 2.5]). $\overline{K}$ *on korpus.*

Definitsioon 1.24. Iga ekvivalentsiklassi $A \in \overline{K}$ jaoks defineerime normi

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

kus jada (a_n) on klassi A suvaline esindaja.

Lause 1.25 ([9, teoreem 2.5]). $\|\cdot\|$ *on norm korpusel* $\overline{K}$.

Teoreem 1.26 ([9, teoreem 2.5, peatükk 2.3]). $\overline{K}$ *on täielik normeeritud korpus, milles* K *on tihe alamkorpus. Korpuse* K *tehted laienevad korpusele* $\overline{K}$ *s.t, kui*

$$A = \lim_{n\to\infty} \overline{(a_n)} \quad \textit{ja} \quad B = \lim_{n\to\infty} \overline{(b_n)},$$

siis

$$A + B = \lim_{n\to\infty} \overline{(a_n + b_n)} \quad \textit{ja} \quad A \cdot B = \lim_{n\to\infty} \overline{(a_n \cdot b_n)}.$$

2 Ultrameetrilised ruumid

Antud peatükis vaatleme üht erilist tüüpi meetrilisi ruume, millel on mitmeid huvitavaid omadusi.

Definitsioon 2.1. Öeldakse, et norm $\|\cdot\|$ korpusel K on *mittearhimeediline*, kui mis tahes $x, y \in K$ korral

$$\|x+y\| \leq \max\{\|x\|, \|y\|\}.$$

Seda normi omadust kutsutakse *tugevaks kolmnurga võrratuseks*. Normi, mis ei ole mittearhimeediline, nimetatakse *arhimeediliseks*.

Definitsioon 2.2. Meetrikat d hulgal X nimetatakse *ultrameetrikaks*, kui mis tahes $x, y, z \in X$ korral

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

Viimast kauguse omadust nimetatakse *tugevaks kolmnurga võrratuseks*. Meetrilist ruumi (X,d) nimetatakse seejuures *ultrameetriliseks ruumiks*.

Märgime, et mittearhimeediline norm $\|\cdot\|$ korpusel K indutseerib ultrameetrika. Tõepoolest, mis tahes $x, y, z \in K$ korral

$$\begin{aligned} d(x,z) &= \|x-z\| = \|(x-y)+(y-z)\| \\ &\leq \max\{\|x-y\|, \|y-z\|\} \\ &= \max\{d(x,y), d(y,z)\}. \end{aligned}$$

Järgmine lause annab piisava ja tarviliku tingimuse selleks, et norm $\|\cdot\|$ korpusel K oleks mittearhimeediline.

Lause 2.3 ([9, lause 2.4])**.** *Olgu $\|\cdot\|$ norm korpusel K. Järgmised väited on samaväärsed:*

(a) *$\|\cdot\|$ on mittearhimeediline,*

(b) *$\|n\| \leq 1$ iga naturaalarvu n korral,*

(c) *$\|n\| \leq 1$ iga täisarvu n korral,*

(d) *kui $a, b \in K$ ja $\|a\| < \|b\|$, siis $\|b-a\| = \|b\|$.*

Lause 2.3. demonstreerib erinevust arhimeediliste ja mittearhimeediliste normide vahel ning sellel on mitmeid olulisi järeldusi.

Lause 2.4. *Kui mittearhimeedilise korpuse K elemendid a ja x rahuldavad võrratust*

$$\|x-a\| < \|a\|, \tag{2.1}$$

siis $\|x\| = \|a\|$.

Tõestus. Tugeva kolmnurga võrratuste järgi

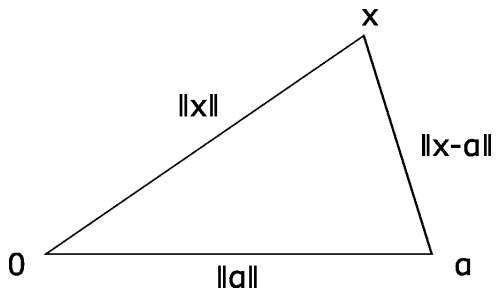
$$\|x\| = \|x-a+a\| \leq \max\{\|x-a\|, \|a\|\} = \|a\|.$$

Sarnaselt

$$\|a\| = \|a-x+x\| \leq \max\{\|a-x\|, \|x\|\}.$$

Kui kehtiks $\|x-a\| > \|x\|$, siis $\|a\| \leq \max\{\|a-x\|, \|x\|\} = \|x-a\|$, mis on vastuolus võrratusega (2.1). Seega $\|x-a\| \leq \|x\|$, järelikult $\|a\| \leq \max\{\|a-x\|, \|x\|\} = \|x\|$ ning kokkuvõttes $\|x\| = \|a\|$. □

Antud järelduse geomeetriline tõlgendus on, et ultrameetrilises ruumis on iga kolmnurk võrdhaarne ja teravnurkne, st selle aluse pikkus ei ületa haarade pikkust:



Lause 2.5. *Norm on arhimeediline, kui ta rahuldab järgmist Archimedese, aksioomi. Olgu $x, y \in K, x \neq 0$. Siis leidub selline $n \in \mathbb{N}$, et $\|nx\| > \|y\|$ ehk* $\sup\{\|n\| : n \in \mathbb{N}\} = \infty$.

Tõestus. Kui norm $\|\cdot\|$ korpusel K on mittearhimeediline, siis $\|n\| \leq 1$ iga $n \in \mathbb{N}$ korral ehk

$$\sup\{\|n\| : n \in \mathbb{N}\} \leq 1.$$

Kui norm $\|\cdot\|$ on arhimeediline siis leidub selline $n \in \mathbb{N}$, et $\|n\| > 1$. Kuna $\|n \cdot n\| = \|n\| \cdot \|n\| > 1$ ja $\lim\limits_{n\to\infty} t^n = \infty$ kui $t > 1$ siis on võimalik sedasi jätkates leida arve, millel on kuitahes suured normid ehk $\sup\{\|n\| : n \in \mathbb{N}\} = \infty$. □

Lause 2.6. *Kui norm $\|\cdot\|$ korpusel K on mitterhimeediline, siis iga reaalarvu $\alpha > 0$ korral on ka $\|\cdot\|^\alpha$ mittearhimeediline.*

Tõestus. Kui $\|\cdot\|$ on korpusel K mittearhimeediline siis iga $n \in \mathbb{Z}$ korral $\|n\| \leq 1$. Reaalarv $\alpha > 0$ ning $\|n\| \leq 1$ korral ka $\|n\|^\alpha \leq 1$. Järelikult lause 2.5. põhjal on ka norm$\|\cdot\|^\alpha$ mittearhimeediline. □

Lause 2.7 ([9, lause 1.6])**.** *Iga kera ultrameetrilises ruumis M on samaaegselt nii kinnine, kui lahtine hulk.*

Lause 2.8 ([9, lause 1.7])**.** *Kui $\|\cdot\|$ on mittearhimeediline norm korpusel K, siis kera $\overline{B_{a,r}} = \{x : \|x-a\| \leq r\}$ iga punkt on selle keskpunkt.*

3 p-aadiliste arvude korpus

Kõige lihtsam näide normist ratsionaalarvude korpusel on absoluutväärtus $|\cdot|$, mille poolt indutseeritud meetrika $d(x,y) = |x-y|$ on kahe arvu vaheline kaugus arvteljel. Selle normi abil ratsionaalarvude täielikustamine annab tulemuseks reaalarvude korpuse. Antud peatükis uurime teisi võimalusi kahe arvu vahelise kauguse mõõtmiseks.

Definitsioon 3.1. Olgu p suvaline algarv. Tähistame ratsionaalarvu x korral

$$\mathrm{ord}_p x = \begin{cases} \text{suurim arvu } p \text{ aste, mis jagab arvu } x, \text{ kui } x \in \mathbb{Z}; \\ \mathrm{ord}_p a - \mathrm{ord}_p b, \text{ kui } x = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0. \end{cases}$$

On kerge näha, et kui $x = \frac{a}{b}$ on ratsionaalarv, siis kujutuse $\mathrm{ord}_p x$ väärtus ei sõltu tegurite a ja b valikust, st, kui $x = \frac{a_1}{b_1} = \frac{a_2}{b_2}$ siis $\mathrm{ord}_p x = \mathrm{ord}_p a_1 - \mathrm{ord}_p b_1 = \mathrm{ord}_p a_2 - \mathrm{ord}_p b_2$.

Lause 3.2 ([9, peatükk 2.4]). *Olgu a, b ja c täisarvud ning $b, c \neq 0$. Siis kehtivad järgmised omadused:*

(a) $ord_p ab = ord_p a + ord_p b$;

(b) $ord_p \frac{a}{b} = ord_p \frac{ac}{bc}$.

Definitsioon 3.3. Olgu $p \in \mathbb{N}$ suvaline algarv. Defineerime ratsionaalarvude korpusel $\mathbb{Q}$ kujutuse $|\cdot|_p$ järgmiselt:

$$|x|_p = \begin{cases} \frac{1}{p^{\mathrm{ord}_p x}} & \text{kui } x \neq 0, \\ 0 & \text{kui } x = 0. \end{cases}$$

Paneme tähele, et kujutus $|x|_p$ saavutab korpuses $\mathbb{Q}$ vaid loenduva arvu erinevaid väärtusi, nimelt $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$.

Lause 3.4. *Kui $a, b \in \mathbb{N}$, siis $a \equiv b \pmod{p^n}$ parajasti siis, kui $|a - b|_p \leq \frac{1}{p^n}$.*

Tõestus. Olgu $a, b \in \mathbb{N}$ sellised, et $a \equiv b \pmod{p^n}$. Siis $a - b \equiv 0 \pmod{p^n}$ ehk p^n jagab arvu $a - b$. Definitsiooni järgi $\mathrm{ord}_p (a - b) \geq n$ nng seega $|a - b|_p \leq \frac{1}{p^n}$. Teisipidi, kehtigu $|a - b|_p \leq \frac{1}{p^n}$. See aga tähendab, et arv p jagub arvu $a - b$ vähemalt n korda ning seega $a - b \equiv 0 \pmod{p^n}$ ehk $a \equiv b \pmod{p^n}$. □

Lause 3.5 ([9, lause 2.6]). *Kujutus $|\cdot|_p$ on mittarhimeediline norm korpusel $\mathbb{Q}$, s.t mis tahes arvude $a, b \in \mathbb{Q}$ ja algarvu p korral*

$$\|a + b\|_p \leq \max \left\{ \|a\|_p, \|b\|_p \right\}.$$

Normi $|\cdot|_p$ nimetatakse *p-aadiliseks normiks* korpusel $\mathbb{Q}$.

Näide 3.6. Leiame $\left|\frac{2058}{385}\right|_7$. Kuna $\frac{2058}{385} = \frac{7^3 \cdot 3 \cdot 2}{7 \cdot 5 \cdot 11}$, siis

$$\mathrm{ord}_7 \frac{2058}{385} = \mathrm{ord}_7 2058 - \mathrm{ord}_7 385 = 3 - 1 = 2$$

ning seega

$$\left|\frac{2058}{385}\right|_7 = \frac{1}{7^{\mathrm{ord}_7 \frac{2058}{385}}} = \frac{1}{7^2} = \frac{1}{49}.$$

Märkus 3.7 ([9, märkus 2.3.]). Kui p_1,$p_2 \in \mathbb{N}$ on erinevad algarvud, siis normid $|x|_{p_1}$ ja $|x|_{p_2}$ ei ole omavahel ekvivalentsed.

Definitsioon 3.8. Olgu $p \in \mathbb{N}$ algarv. Olgu $\mathbb{Q}_p$ korpuse $\mathbb{Q}$ täieldi p-aadilise normi $|\cdot|_p$ suhtes. Lause 1.23. kohaselt laieneb p-aadiline norm hulgale $\mathbb{Q}_p$ ning $\left(\mathbb{Q}_p, |\cdot|_p\right)$ on täielik normeeritud korpus, milles $\mathbb{Q}$ on kõikjal tihe alamkorpus. Korpust $\mathbb{Q}_p$ nimetatakse *p-aadiliste arvude korpuseks.*

Definitsioon 3.9. Korpuse $\mathbb{Q}_p$ elemente nimetatakse *p-aadilisteks arvudeks*, st p-aadilised arvud on ratsionaalarvude Cauchy jadade ekvivalentsiklassid normi $|\cdot|_p$ suhtes, kusjuures ratsionaalarv a samastatakse sellle ekvivalentsiklassiga, kuhu kuulub jada $(a) = (a, a, \ldots)$.

Märkus 3.10 ([9, märkus 2.4])**.** Norm $|\cdot|_p$ väljastab korpustes $\mathbb{Q}$ ja $\mathbb{Q}_p$ samu väärtusi $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$

Viimast omadust ei ole eukleidilisel absoluutväärtusel, kus norm $|\cdot|$ saab ratsionaalarvude täielikustamisel reaalarvudeks omada kõiki mittenegatiivseid reaalarvulisi väärtusi. Lisaks sellele paneme tähele, kui $|a|_p \neq 0$, siis vastava Cauchy jada normide jada $\left(|a_n|_p\right)$ peab mingil hetkel piisavalt suurte n-i väärtuste juures stabiliseeruma, sest normi $|x|_p$ võimalike väärtuste hulga $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$ ainsaks kuhjumispunktiks on 0. Kui $|a|_p = p^n \neq 0$, siis, kuna p^n ei ole selle p-aadilise normi väärtuste kuhjumispunkt, leidub selline $\varepsilon > 0$, et $B(p^n, \varepsilon) = \{p^n\}$. Kuna jada $\left(|a_n|_p\right)$ koondumisel arvuks p^n peab iga $\varepsilon > 0$ korral leiduma keras $B(p^n, \varepsilon) = \{p^n\}$ selle jada elemente siis järelikult peab leidub selline indeks N , et iga $n > N$ korral $|a_n|_p = p^n$.

Iga Cauchy jadade ekvivalentsiklass, mis defineerib mingi elemendi korpuses $\mathbb{Q}_p$, omab teatud kanoonilist kuju. Selle konstrueerimiseks vajame järgmist tulemust.

Teoreem 3.11 ([9, lause 2.8])**.** *Igal ekvivalentsiklassil a korpuses $\mathbb{Q}_p$, mis rahuldab tingimust $|a|_p \leq 1$, on täpselt üks seda esindav Cauchy jada (a_i), millel on järgmised omadused:*

(a) $a_i \in \mathbb{Z}, 0 \leq a_i < p^i$ *iga* $i = 1, 2, \ldots$ *korral,*

(b) $|a_i - a_{i-1}|_p < \frac{1}{p^i}$ *ehk* $a_i \equiv a_{i+1} \pmod{p^i}$ *iga* $i = 1, 2, \ldots$ *korral..*

Kui $a \in \mathbb{Q}_p$ ning $|a|_p \leq 1$, siis on mugav panna kõik eelnevast teoreemist saadud jada (a_i) liikmed kirja järgmisel kujul:

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

kus d_i on täisarvud hulgast $\{0, 1, \ldots, p-1\}$. Teoreemi 3.11. tingimuse (b) tõttu

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

kus kõik nn „p-aadilised numbrid" on hulgast $\{0, 1, \ldots, p-1\}$. Seega korpuses $\left(\mathbb{Q}, |\cdot|_p\right)$ saab p-aadilise arvu a esitada koonduva rea summana

$$a = \lim_{k\to\infty} \sum_{n=0}^{k} d_n p^n = \sum_{n=0}^{\infty} d_n p^n.$$

Sellest saab mõelda, kui arvust alusel p, millel on lõpmata palju p-aadilisi numbrikohti. Kui $|a|_p > 1$ siis võime a läbi korrutada arvuga p^m, sest siis $|ap^m|_p = \frac{1}{p^m}|a|_p = 1$), et saada uus p-aadiline arv $a' = ap^m$, mis rahuldab tingimust $|a'|_p \leq 1$. Seega võime kirjutada, et

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

kus $d_{-m} \neq 0$ ja $d_n \in \{0, 1, \ldots, p-1\}$. Arv a on lõpmatu „p-ndmurd", mille *kanooniliseks kujuks* nimetatakse kirjutist

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

Võtame kogu selle arutelu kokku järgmise teoreemina.

Teoreem 3.12 (**p-aadilise arvu kanooniline esitus**, [9, teoreem 2.9])**.** *Iga p-aadiline arv $a \in \mathbb{Q}_p$ on esitatav kujul $a = \sum_{n=-m}^{\infty} d_n p^n$, kus $d_n \in \{0, 1, \ldots, p-1\}$. Kui $a \neq 0$, siis m on selline nullist erinev täisarv, et $|a|_p = p^m$.*

Märkus 3.13. Paneme tähele, et reaalarvude hulgas ei ole kõik arvud üheselt esitatavad. Näiteks

$$1.000\ldots = 0.9999\ldots$$

p-aadiliste arvudega midagi sellist ei juhtu. Vastavalt teoreemile 3.11. on kahe p-aadilise arvu kanoonilised kujud samad parajasti siis, kui kõik nende numbrikohad ühtivad.

Definitsioon 3.14. Hulga $\mathbb{Z}_p \coloneqq \left\{a \in \mathbb{Q}_p \middle| \, |a|_p \leq 1\right\}$ elemente nimetatakse *p-aadilisteks täisarvudeks.*

Lause 3.15. *Olgu a p-aadiline arv normiga p^{-n}. Siis on arvu a võimalik esitada korrutisena $a = p^n u$, kus $|u|_p = 1$.*

Tõestus. Olgu a selline p-aadiline arv, et $|a|_p = p^{-n} < 1$. Järelikult $a \in \mathbb{Z}_p$. Valime $u \coloneqq a \cdot p^{-n}$, siis normi omaduste tõttu

$$|u|_p = \left|a \cdot p^{-n}\right|_p = |a|_p \left|p^{-n}\right|_p = 1$$

nagu soovitud. □

Lause 3.16. *p-aadiline arv a kuulub hulka $\mathbb{Z}_p$ parajasti siis, kui selle kanooniline kuju sisaldab vaid mittenegatiivseid p astmeid, st*

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

Tõestus. Kui $a = \sum\limits_{i=0}^{\infty} a_i p^i$ siis järeldub p-aadilise normi definitsioonist, et $|a|_p \leq \frac{1}{p^0} = 1$ ehk $a \in \mathbb{Z}_p$. Juhul $a = \sum\limits_{i=-m}^{\infty} a_i p^i$, ≥ 1 saame, et

$$\begin{aligned} |a|_p &= \lim_{n\to\infty} \left| \sum_{i=-m}^{n} a_i p^i \right|_p = \lim_{n\to\infty} \left| p^{-m} \sum_{i=0}^{n} a_i p^i \right|_p \\ &= \lim_{n\to\infty} \left|p^{-m}\right|_p \left| \sum_{i=0}^{n} a_i p^i \right|_p = p^m \lim_{n\to\infty} \left| \sum_{i=0}^{n} a_i p^i \right|_p = p^m \cdot 1 \geq 1. \end{aligned}$$

Seega $a \notin \mathbb{Z}_p$. □

Lause 3.17. *Igal lõpmatu jada, mis koosneb p-aadilistest täisarvudest, omab koonduvat osajada.*

Tõestus. Olgu (x_k) jada hulgas $\mathbb{Z}_p$ ning

$$x_k = \ldots a_{k,2} a_{k,1} a_{k,0}$$

jada liikme x_k kanooniline kuju. Kuna $a_{k,0} \in \{0, 1, \ldots, p-1\}$, siis on võimalik leida selline arv $b_0 \in \{0, 1, \ldots, p-1\}$ ja jada (x_k) lõpmatu osajada $(x_{0,k})$, mille iga liikme viimane numbrikoht on b_0. Samamoodi valime $b_1 \in \{0, 1, \ldots, p-1\}$ ja leiame jada $(x_{0,k})$ sellise lõpmatu osajada $(x_{1,k})$, mille iga liige lõpeb numbritega $b_1 b_0$. Seda protsessi jätkates jõuame arvuni $\ldots b_3 b_2 b_1 b_0$ koos järgmise jadade jadaga

$$\begin{array}{llll} x_{0,0} = \ldots b_0, & x_{0,1} = \ldots b_0, & x_{0,2} = \ldots b_0, & \ldots \\ x_{1,0}, = \ldots b_1 b_0, & x_{1,1} = \ldots b_1 b_0, & x_{1,2} = \ldots b_1 b_0, & \ldots \\ x_{2,0} = \ldots b_2 b_1 b_0, & x_{2,1} = \ldots b_2 b_1 b_0, & x_{2,2} = \ldots b_2 b_1 b_0, & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Konstruktsiooni kohaselt on iga järgmine jada eelneva jada osajada ning iga $(i+1)$ rea element lõpeb numbritega $b_i \ldots b_2 b_1 b_0$. Diagonaalil olev jada $x_{0,0}, x_{1,1}, x_{2,2}, \ldots$ on ka algse jada (x_k) osajada, sest tänu sellele, et kõik vaadeldavad jadad on nendele eelnevate

jadade osajadad. Samuti koondub see jada elemendiks $b = \dots b_3 b_2 b_1 b_0$, kuna

$$\lim_{n\to\infty} |x_{n,n} - b|_p = \lim_{n\to\infty} \left| \sum_{i=n+1}^{\infty} b_i \right|_p \leq \frac{1}{p^n} \to 0$$

ehk $x_{k,k} \to b$. □

Teoreem 3.18 (**Bolzano-Weierstrassi teoreem**, [9, teoreem 2.11]). *Iga tõkestatud p-aadiliste arvude jada sisaldab koonduvat osajada.*

4 p-aadiliste arvude aritmeetika

Korpuse $\mathbb{Q}$ tehete laiendamine võimaldab sooritada aritmeetilisi tehteid p-aadiliste arvudega sarnaselt tehetega reaalarvude hulgas Järgnevalt vaatame eraldi, kuidas p-aadilisi arve liita, lahutada, korrutada ja jagada.

4.1 Liitmine ja lahutamine

Olgu

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

kus a_n ja b_n on p-aadilised numbrikohad, kusjuures $a_{-m} \neq 0$, kuid üks või enam esimestest numbrikohtadest $b_{-m}, b_{-m+1}, \dots$ võivad olla võrdsed nulliga. Siis iga rida

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

on koonduv. Enamasti ei ole niiviisi leidud p-aadiline arv küll oma kanoonilisel kujul. Sarnaselt liitmisele ja lahutamisele reaalarvude hulgas tuleb ka p-aadiliste arvude liitmisel ülekandmisi teha, kusjuures need toimuvad paremalt vasakule. Liitmise algoritmi illustreerimiseks leiame arvu -1 kanoonilise kuju.

Näide 4.1. Teame, et $1 = \dots 00001$. Olgu $a = \dots a_3 a_2 a_1 a_0$ selline p-aadiline arv, et

$$1 + a = 0,$$

st $a = -1$. Alustades paremalt poolt, peab kehtima $a_0 + 1 = 0$. Kuna $a_0 \in (0, 1, \dots, p-1)$, siis ainus võimalus selleks on, et $a_0 + 1 = p$ ehk $a_0 = p - 1$. Samamoodi

$$1 + a_0 + a_1 p \equiv 0 \left(\mathrm{mod}\ p^2\right),$$

st $a_1 p \equiv -p \,(\mathrm{mod}\ p) \iff a_1 \equiv -1 \,(\mathrm{mod}\ p)$ ehk $a_1 = p - 1$.

Seda protsessi jätkates on selge, et kõik arvud a_n on võrdsed arvuga $p-1$ ning

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

Märkus 4.2. p-aadiliste arvude ja reaalarvude aritmeetikal on üks huvitav erinevus. Nimelt on p-aadiliste arvudega arvutamisel võimalik „lõpmatusest laenata". Kui me reaalarvude hulgas soovime teha tehte 24-8, siis kõigepealt me laename vasakul olevast kahest kümne, saades vastuseks 16. Aga kui tahaksime leida 2-6, siis me enam laenata ei saaks, kuna meil ei ole enam vasakult midagi juurde laenata, ning saame vastuseks negatiivse arvu -4. Samas p-aadiliste arvude hulgas on alati võimalik laenata. Kui teeme sama tehte 2-6 7-aadiliste arvude hulgas siis me saame laenata arvust 2 vasakul olevast nullist. Aga seal muidugi ei ole midagi, mis tähendab, et peame veel kord vasakult laenama, ja niimoodi edasi lõpmata palju kordi, saades lõpmatu kuute jada. Seega 2-6 7-aadiliste arvude hulgas on vastuseks $\ldots 66663$.

Näide 4.3. Olgu $\ldots 24641$ ja $\ldots 41052$ 7-aadilised arvud. Liidame need omavahel saades arvu c:

$$\ldots 24641 + \ldots 41052 = \ldots 66023,$$

sest

$$\begin{aligned}
&\left(1\cdot 7^0 + 4\cdot 7^1 + 6\cdot 7^2 + 4\cdot 7^3 + 2\cdot 7^4 + \ldots\right)\\
+&\left(2\cdot 7^0 + 5\cdot 7^1 + 0\cdot 7^2 + 1\cdot 7^3 + 4\cdot 7^4 + \ldots\right)\\
=\ &3\cdot 7^0 + 2\cdot 7^1 + 0\cdot 7^2 + 6\cdot 7^3 + 6\cdot 7^4 + \ldots
\end{aligned}$$

Lühidalt saab selle tehte välja kirjutada järgmiselt:

$$\begin{array}{cccccccc}
 & & & {\scriptstyle +1} & {\scriptstyle +1} & & & \\
 & \ldots & 2 & 4 & 6 & 4 & 1 & \\
+ & \ldots & 4 & 1 & 0 & 5 & 2 & \\
\hline
 & \ldots & 6 & 6 & 0 & 2 & 3 & .
\end{array}$$

Näide 4.4. Olgu $\ldots 43212$ ja $\ldots 20143$ p-aadilised arvud hulgast $\mathbb{Z}_5$. Lahutame need omavahel, saades tulemuseks arvu c:

$$\ldots 43212 - \ldots 20143 = \ldots 23036 = c,$$

sest

$$\begin{aligned}
&\left(2\cdot 5^0 + 1\cdot 5^1 + 2\cdot 5^2 + 3\cdot 5^3 + 4\cdot 5^4 + \ldots\right)\\
-&\left(3\cdot 5^0 + 4\cdot 5^1 + 1\cdot 5^2 + 0\cdot 5^3 + 2\cdot 5^4 + \ldots\right)\\
=\ &4\cdot 5^0 + 1\cdot 5^1 + 0\cdot 5^2 + 3\cdot 5^3 + 2\cdot 5^4 + \ldots
\end{aligned}$$

Lühemalt saab selle tehte üles kirjutada järgmiselt:

$$\begin{array}{rcccccccc} & & & & & \overset{-1}{2} & \overset{-1}{1} & 2 \\ & \ldots & 4 & 3 & 2 & 1 & 2 \\ - & \ldots & 2 & 0 & 1 & 4 & 3 \\ \hline & \ldots & 2 & 3 & 0 & 1 & 4 \end{array} .$$

4.2 Korrutamine

Korrutamist saab teostada liitmisele ja lahutamisele sarnasel viisil. Olgu

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

antud nende kanoonilisel kujul. Ridade liikmeti korrutamisel saame, et

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

kus

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

Tulemuseks saadav arv ei ole samuti enamasti oma kanoonilisel kujul, aga ülekandmiste abil on viimast alati võimalik leida.

Näide 4.5. Olgu $\ldots 45331$ ja $\ldots 20326$ p-aadilised arvud hulgast $\mathbb{Z}_7$. Korrutame need omavahel, saades tulemuseks arvu c:

$$45331 \cdot 20326 = 30166 = c,$$

kuna

$$\begin{aligned} & \left(1 \cdot 7^0 + 3 \cdot 7^1 + 3 \cdot 7^2 + 5 \cdot 7^3 + 4 \cdot 7^4 + \ldots\right) \\ & \cdot \left(6 \cdot 7^0 + 2 \cdot 7^1 + 3 \cdot 7^2 + 0 \cdot 7^3 + 2 \cdot 7^4 + \ldots\right) \\ = \; & 6 \cdot 7^0 + 2 \cdot 7^1 + 3 \cdot 7^2 + 0 \cdot 7^3 + 2 \cdot 7^4 \\ + \; & \quad + 4 \cdot 7^1 + 1 \cdot 7^2 + 3 \cdot 7^3 + 1 \cdot 7^4 + 4 \cdot 7^2 \\ + \; & \quad + 1 \cdot 7^3 + 3 \cdot 7^4 + 2 \cdot 7^3 + 0 \cdot 7^4 + 3 \cdot 7^4 \ldots \\ = \; & 6 \cdot 7^0 + 6 \cdot 7^1 + 1 \cdot 7^2 + 0 \cdot 7^3 + 3 \cdot 7^4 + \ldots \end{aligned}$$

Sellegi tehte saab lühemalt välja kirjutada järgmiselt:

$$\begin{array}{cccccccc}
 & \ldots & 4 & 5 & 3 & 3 & 1 \\
\cdot & \ldots & 2 & 0 & 3 & 2 & 6 \\
\hline
 & & 3^{+4} & 2^{+2} & 4^{+2} & 4 & 6 \\
+ & & 3 & 6 & 6 & 2 & \\
+ & & 2^{+1} & 2 & 3 & & \\
+ & & 0 & 0 & & & \\
+ & & 2 & & & & \\
\hline
 & \ldots & 3 & 0 & 1 & 6 & 6
\end{array} .$$

4.3 Jagamine

Olgu $a, b \in \mathbb{Q}_p$ ning $b \neq 0$. Kuna vajadusel saame arvud a ja b korrutada läbi mingi arvu p astmega, siis üldisust kitsendamata võime eeldada, et $a, b \in \mathbb{Z}_p$, kus $b_0 \neq 0$ ning

$$a = a_0 + a_1 p + a_2 p^2 + \ldots$$

ja

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

Jagamise tulemusel saadava arvu $c = \frac{a}{b}$ saame üles kirjutada kujul

$$c = \frac{a_0 + a_1 p + a_2 p^2 + \ldots}{b_0 + b_1 p + b_2 p^2 + \ldots} = c_0 + c_1 p + c_2 p^2 + \ldots$$

Kuna $a = b \cdot c$, siis

$$a = b \cdot c = \left(b_0 + b_1 p + b_2 p^2 + \ldots\right)\left(c_0 + c_1 p + c_2 p^2 + \ldots\right) = d_0 + d_1 p + d_2 p^2 + \ldots$$

Kuigi $b_0, c_0 \in \{1, \ldots, p-1\}$, ei saa eeldada, et ka arv d_0 sinna hulka kuulub. Seega kirjutame

$$d_0 = b_0 c_0 = a_0 + n_1 p.$$

kus a_0 on arvu $b \cdot c$ esimene numbrikoht ning $n_1 p$ tuleb liita arvule $d_1 p$. Ehk

$$a_0 \equiv b_0 c_0 \pmod{p},$$

kust järeldub, et

$$c_0 \equiv b_0^{-1} d_0 \pmod{p}.$$

Teame, et arvul b_0 tõepoolest leidub pöördelement b_0^{-1}, sest $\mathbb{Q}_p$ on korpus. Sellisel viisil saame leida ka kõik teised arvud c_i.

Näide 4.6. Olgu 6632 ja 164 p-aadilised arvud hulgast $\mathbb{Z}_7$. Jagame me need omavahel

nende kanoonilisel kujul, saades tulemuseks arvu c:

$$\frac{6632}{164} = 34 = c.$$

Pikemalt:

$$\begin{aligned}
&2 \equiv 4 \cdot c_0 \pmod 7, c_0 \equiv 4 \pmod 7, \\
&3 \equiv 4 \cdot c_1 + 6 \cdot c_0 + 2 = 4 \cdot c_1 + 6 \cdot 4 + 2 = 4 \cdot c_1 + 5 \pmod 7 \\
&c_1 \equiv 2 \cdot 5 \equiv 3 \pmod 7 \\
&6 \equiv 4 \cdot c_2 + 6 \cdot c_1 + 1 \cdot c_0 + 5 = 4 \cdot c_1 - 1 \pmod 7 \\
&c_2 \equiv 0 \pmod 7
\end{aligned}$$

ehk $c = 34$. Sellegi tehte saab välja kirjutada lühemalt:

	6	6	3	2	1	6	4
-	1	0	5	2			
	5	5	5				
-	5	5	5				
			0				

.

Lause 4.7. *p-aadiline täisarv*

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

omab p-aadiliste täisarvude ringis pöördelementi parajasti siis, kui $a_0 \neq 0$.

Tõestus. Olgu p-aadiline arv a kujul

$$a = \sum_{i=0}^{\infty} a_i p^i,$$

kus $a_0 \neq 0$. Peame näitama, et leidub p-aadiline arv b kujul

$$b = \sum_{i=0}^{\infty} b_i p^i$$

nii, et $a \cdot b = 1$.

Kui $a_0 \neq 0$, siis paneme tähele, et

$$\left| \sum_{i=0}^{\infty} a_i p^i \right|_p = \lim_{n \to \infty} \left| \sum_{i=0}^{n} a_i p^i \right|_p = 1,$$

sest, arv p ei jaga arvu a_0 ning siis ei jaga see ka täisarve $\sum_{i=0}^{n} a_i p^i$ kõigi indeksi n väärtuste korral. Kuna hulk $\mathbb{Q}_p$ on korpus, siis leidub arvul a pöördelement ning kuna

peab kehtima

$$|a|_p \cdot \left|a^{-1}\right|_p = \left|a \cdot a^{-1}\right|_p = 1,$$

siis järelikult $\left|a^{-1}\right|_p = 1$ ehk $a^{-1} \in \mathbb{Z}_p$.

Eeldame nüüd, et $a_0 = 0$. See tähendab, et arv p jagab arvu a vähemalt ühe korra ehk $\mathrm{ord}_p a \geq 1$ ja seega$|a|_p = \frac{1}{p^{\mathrm{ord}_{p^a}}} < 1$. Kuna taas kord peab kehtima võrdus

$$|a|_p \cdot \left|a^{-1}\right|_p = \left|a \cdot a^{-1}\right|_p = 1,$$

siis järelikult $\left|a^{-1}\right|_p > 1$ ehk $a^{-1} \notin \mathbb{Z}_p$. □

Viimasest lausest järeldub näiteks, et p-aadilised arvul p puudub hulgas $\mathbb{Z}_p$ pöördelement, aga sellel leidub pöördelement hulgas $\mathbb{Q}_p$, milleks on p-aadiline arv $\frac{1}{p} = \frac{1}{10}$.

Definitsioon 4.8. Hulga $\mathbb{Z}_p$ pööratavate elementide hulka tähistatakse sümboliga

$$\mathbb{Z}_p^\times = \left\{ \sum_{i=1}^{\infty} a_i p^i \,|a_0 \neq 0 \right\}.$$

Lause 4.9. *Pööratavate p-aadiliste täisarvude hulk $\mathbb{Z}_p^\times$ on esitatav kujul*

$$\mathbb{Z}_p^\times = \left\{ x \in \mathbb{Z}_p \,\middle|\, |x|_p = 1 \right\}.$$

Tõestus. Olgu $x \in \mathbb{Z}_p$. See tähendab, et $|x|_p \leq 1$. Samas, kuna $x^{-1} \in \mathbb{Z}_p$ siis $\left|x^{-1}\right|_p \leq 1$. Sellest, et peab kehtima

$$|x|_p \left|x^{-1}\right|_p = \left|x \cdot x^{-1}\right|_p = 1$$

järeldubki, et $|x|_p = 1$.

Olgu nüüd x p-aadiline täisarv normiga 1 ja olgu x^{-1} selle pöördelement. Jällegi, kuna

$$|x|_p \left|x^{-1}\right|_p = 1,$$

siis ei ole muud võimalust kui see, et $\left|x^{-1}\right| = 1$ ja järelikult $x^{-1} \in \mathbb{Z}_p$. □

5 Ratsionaalarvude p-aadiline reaksarendus

Reaalarv a on ratsionaalarv parajasti siis, kui selle kümnendesitus on paremale lõpmatult perioodiline. Selles peatükis näitame, et sarnane omadus on ka p-aadiliste arvude korpuses.

Iga täisarv on ilmselt ka p-aadiline täisarv, see on lihtsalt selle sama arvu esitus baasil p. Kuid leidub p-aadilisi täisarve, mis ei ole ratsionaalsed täisarvud. Peatükis 4.1 leidsime,

et

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

kust

$$\sum_{n=0}^{\infty} p^n = \frac{-1}{p-1} \quad \text{ehk} \quad \frac{1}{1-p} = \ldots 1111.$$

Seega $\sum_{n=0}^{\infty} p^n \in \mathbb{Z}_p$, kusjuures tegu on lõpmatu p-aadilise täisarvuga, kuid $\frac{1}{p-1} \notin \mathbb{Z}$. Lõpmatu perioodilise p-aadilise täisarvu on kujul $\overline{n_{k-1}\ldots n_1 n_0} m_{j-1} m_j \ldots m_0$, kus $n_0 n_1 \ldots n_{k-1}$ on selle perioodiliselt osa. Näiteks $\frac{1}{1-p} = \overline{1}$.

Märkus 5.1. Kui p-aadilise arvu x kanooniline kuju on

$$x = c_d p^d + c_{d+1} p^{d+1} + \ldots + c_i p^i + \ldots$$

siis selle vastandelement on leitav korrutades seda arvuga -1 ehk see on kujul

$$\begin{aligned}
-x &= -1 \cdot x \\
&= x \cdot (p-1)\left(\sum_{n=0}^{\infty} p^n\right) \\
&= \left(\sum_{m=d}^{\infty} c_m p^m \cdot (p-1)\right) \cdot \left(\sum_{n=0}^{\infty} p^n\right) \\
&= \left(\left(p - c_d\right) p^d + \left(\sum_{m=d+1}^{\infty} \left(p - c_m - 1\right) p^m\right)\right) \cdot \left(\sum_{n=0}^{\infty} p^n\right) \\
&= (p-c_d)p^d + \left(p - 1 - c_{:d+1}\right) p^{d+1} + \ldots + \left(p - 1 - c_{:i}\right) p^i + \ldots..
\end{aligned}$$

Teoreem 5.2. *p-aadiline arv on ratsionaalarv parajasti siis, kui selle kanooniline kuju on mingist indeksist alates vasakule lõpmatult perioodiline.*

Tõestus. Näitame esiteks, et iga vasakule lõpmatult perioodiline p-aadiline arv on ratsionaalarv. Olgu x selline vasakule lõpmatu perioodiline p-aadiline arv, et $|x|_p = 1$. Siis $x \in \mathbb{Z}_p^{\times}$ ja $x \neq 0$, sest $|0|_p = 0$. Vasakule lõpmatult perioodiline p-aadiline arv, mille p-aadiline norm on võrdne ühega, on kujul

$$x = \overline{n_{k-1}\ldots n_1 n_0} m_{j-1} m_j \ldots m_0 = \ldots n_{k-1} \ldots n_1 n_0 n_{k-1} \ldots n_1 n_0 m_{j-1} m_j \ldots m_0.$$

Paneme selle kirja järgmislt:

$$\overline{n_{k-1}\ldots n_1 n_0} m_{j-1} m_j \ldots m_0$$

$$= m_0 + \ldots m_{j-1} p^{j-1} + \left(n_0 p^j + \ldots + n_{k-1} p^{j+k-1}\right) + \left(n_0 p^{j+k} + \ldots + n_{k-1} p^{j+2k-1}\right).$$

Kasutades geomeetrilise jada summa valemit, saame, et

$$\begin{aligned}\overline{n_{k-1}\dots n_1n_0}m_{j-1}m_j\dots m_0 &= m_{j-1}m_j\dots m_0 + (n_{k-1}\dots n_0)\cdot\left(p^j + p^{j+k} + p^{j+2k} + \dots\right)\\ &= m_{j-1}m_j\dots m_0 + p^j\cdot(n_{k-1}\dots n_0)\cdot\left(1 + p^k + p^{2k} + \dots\right)\\ &= m_{j-1}m_j\dots m_0 + p^j\frac{n_{k-1}\dots n_0}{1-p^k}, \qquad (5.1)\end{aligned}$$

mis on ratsionaalarv. Kuna x' on ratsionaalarv, siis on seda ka $x'p^{-n} = x$. Seega oleme näidanud, et kõik vasakule perioodilised p-aadilised arvud on ratsionaalarvud.

Selleks, et tõestada, et iga ratsionaalarvu p-aadiline esitus on mingist indeksist alates vasakule perioodiline, keskendume lihtsuse mõttes negatiivsel ratsionaalarvul r, mille positiivset vastandelementi on hiljem lihtne leida märkuses 5.1. toodud meetodiga. Viime tõestuse läbi viies osas:

1. Esiteks olgu $r \in \mathbb{Z}$ ning $r < 0$. Tähistame $-r = R \in \mathbb{N}$. Teame, et leidub selline $j \geq 1$, et $p^j > R$ ning

$$r = -R = \left(p^j - R\right) - p^j$$

Kuna $p^j - R$ on mingi täisarv hulgast $\left\{1, \dots, p^j - 1\right\}$, siis saame selle kirjutada baasil p ehk kujul $c_0 + \dots + c_{j-1}p^{j-1}$, saades tulemuseks

$$r = \left(p^j - R\right) - p^j = \sum_{i=0}^{j-1} c_i p^i + (-1)\,p^j = \sum_{i=0}^{\infty}(p-1)\,p^i\cdot p^j = \sum_{i=j}^{\infty}(p-1)\,p^i,$$

mis on indeksist i alates vasakule lõpmatult perioodiline, sest kõik selle numbrid on sellest alates võrdsed arvuga $p-1$.

2. Olgu nüüd $r \in \mathbb{Q}\cap\mathbb{Z}_p^{\times}\cap(-1,0)$. Kuna arv r kuulub hulka $\mathbb{Z}_p^{\times}$, siis $|r|_p = 1$ ja $r < 0$ ning saame kirjutada arvu r kujul

$$r = \frac{a}{b},$$

kus $a < 0$,$b \geq 1$ on täisarvud. Paneme tähele, et arv p ei jaga arve a ja b, sest $|r|_p = 1$. Kuna arvud b ja p on ühisteguriteta, siis arvuteooriast tuntud Euleri teoreemi kohaselt $p^{\varphi(b)} \equiv 1 \pmod{b}$. Tähistame $k = \varphi(b)$, siis järelikult

$$p^k = 1 + bb',$$

kus b' on mingi täisarv. Seega saame arvu r ümber kirjutada kujule

$$r = \frac{a}{b} = \frac{ab'}{bb'} = \frac{-ab'}{1-p^k}.$$

Olgu $N = -ab'$. Kuna $a < 0$, siis $N \in \mathbb{N}$. Võrdusest $-1 < r < 0$ saame, et

$$-1 \leq \frac{N}{1-p^k} < 0,$$

kust

$$0 < N \leq p^k - 1.$$

Järelikult on arvul N baasil p ülimalt k numbrikohta, st N on baasil p kujul

$$N = n_0 + n_1 p + \ldots + n_{k-1} p^{k-1},$$

kus $n_i \in \{0, 1, \ldots, p-1\}$ .Seega on arv r kujul

$$r = \frac{n_{k-1} \ldots n_0}{1 - p^k}.$$

Valemi (5.1) järgi on võimalik tagasi jõuda arvu r perioodilisele p-aadilisele esituseni, st, et kuna $\frac{1}{1-p^k} = \sum\limits_{i=0}^{\infty} p^i$, siis

$$\frac{n_{k-1} \ldots n_0}{1 - p^k} = n_{k-1} \ldots n_0 \cdot \sum_{k=0}^{\infty} p^i = \sum_{k=0}^{\infty} p^i \sum_{i=0}^{k-1} n_i p^i = \overline{n_{k-1} \ldots n_0}. \tag{5.2}$$

Kuna p ei jaga arve a ja b' siis järelikult $|N|_p = 1$ ja seega $n_0 \neq 0$. Paneme tähele, et arvul r puudub mitteperioodiline osa ehk see on vasakule puhtalt perioodiline.

3. Juhul, kui $r \in \mathbb{Q} \cap \mathbb{Z}_p \cap (-1, 0)$ aga $r \notin \mathbb{Z}_p^{\times}$, kirjutame arvu r kujul $r = p^n u$, kus $u \in \mathbb{Z}_p^{\times}$. Siis $u = \frac{r}{p^n}$ on ratsionaalarv, mille p-aadiline norm võrdub ühega ning mis kuulub vahemikku $\left(-\frac{1}{p^n}, 0\right) \subset (-1, 0)$. Tõestuse osa 2 põhjal on arvu u p-aadiline kuju puhtalt perioodiline. Järelikult on ka arvu $r = p^n u$ kuju perioodiline, kuid see on paremale nihutatud ehk selle perioodilisele osale eelneb rida nulle.

4. Vaatleme nüüd juhtu, kus $r \in \mathbb{Z}_p \cap \mathbb{Q}, r \notin \mathbb{Z}$ ning $r < -1$. Selline arv asub mingi kahe negatiivse täisarvu vahel:

$$-(N+1) < r < -N, N \in \mathbb{N}.$$

Seega $-1 < r + N < 0$. Kuna N on täisarv siis ka $r + N \in \mathbb{Z}_p$ ja eelneva arutelu põhjal on selle arvu p-aadiline kuju perioodiline, kuid see ei pruugi alata numbrist kordajaga p^0, sest arv $r + N$ ei pruugi kuuluda hulka $\mathbb{Z}_p^{\times}$. Saame kirjutada

$$r + N = \sum_{i \geq 0} a_i p^i,$$

kus $a_i \in \{0, 1, \ldots, p-1\}$ ja numbrid a_i on perioodilised pärast võimaliku algset nullide rida. Kuna $r + N$ ei ole positiivne ratsionaalne täisarv, siis selle p-aadilisel kanoonilisel kujul on lõpmatult palju nullist erinevaid liikmeid a_i. Seega osasummad $a_0 + a_1 p + \ldots + a_{k-1} p^{k-1}$ järjest suurenevad indeksi k suurenedes ning leidub selline indeks j, et

$$a_0 + a_1 p + \ldots + a_{j-1} p^{j-1} > N. \tag{5.3}$$

Olgu j_0 vähim selline indeks, mis seda võrratust rahuldab. Siis $a_{j-1} \neq 0$ (kuna j on vähim

indeks, mille korral võrratus (5.2) kehtib) ning

$$r + N = a_0 + a_1 p + \ldots + a_{j_0-1} p^{j_0-1} + \sum_{i \geq j_0} a_i p^i,$$

kust

$$r = a_0 + a_1 p + \ldots + a_{j_0-1} p^{j_0-1} - N + \sum_{i \geq j_0} a_i p^i. \tag{5.4}$$

Võrratuse (5.2) järgi on vahe $a_0 + a_1 p + \ldots + a_{j_0-1} p^{j_0-1} - N$ naturaalarv,ja see on selgelt väiksem, kui $(p-1) + (p-1)\, p + \ldots + (p-1)\, p^{j_0-1} = p^{j_0} - 1$. Järelikult saame selle vahe baasil p üles kirjutada :

$$a_0 + a_1 p + \ldots + a_{j_0-1} p^{j_0-1} - N = a'_0 + a'_1 p + \ldots + a'_{j-1} p^{j-1},$$

kus $0 \leq a'_i \leq p-1$, ja viia võrduse (5.3) kujule

$$r = a'_0 + a'_1 p + \ldots + a'_{j-1} p^{j-1} + \sum_{i \geq j_0} a_i p^i.$$

Tulemus on ilmselt lõpmatult vasakule perioodiline, sest indeksist j_0 alates on arvud a_i perioodilised.

5. Lõpuks, kui $r \in \mathbb{Q}, r \notin \mathbb{Z}_p$ ja $r < 0$, siis kuna $p^s r \in \mathbb{Z}_p$ piisavalt suure s korral, saame kasutada ühte eeltoodud skeemidedst arvu $p^s r$ jaoks ning hiljem jagada see tulemus arvuga p^s, saades tulemuseks vasakule lõpmatult perioodilise p-aadilise arvu. □

Toome siinkohal mõned näited ratsionaalarvude p-aadiliste kujude leidmisest.

Näide 5.3. Leiame arvu $\frac{-3}{13}$ 5-aadilise kanoonilise kuju valemi (5.2) põhjal. See arv asub intervallis $[-1, 0)$ ning selle 5-aadiline norm on võrdne ühega. Vähim selline arv k, mille korral $5^k \equiv 1 \pmod{13}$, on 4. Kuna $5^4 - 1 = 13 \cdot 48$, siis

$$-\frac{3}{13} = -\frac{3 \cdot 48}{13 \cdot 48} = \frac{144}{1 - 5^4}.$$

Leiame arvu 144 p-aadilise kuju

$$144 = 5^3 + 3 \cdot 5 + 4.$$

Järelikult selle p-aadiline kanooniline kuju on 1034 ning seega

$$-\frac{3}{13} = \frac{144}{1 - 5^4} = \frac{1034}{1 - 5^4} = \overline{1034} = \ldots 10341034.$$

Arvutuste korrektsuse kontrollimiseks liidame 5-aadilise arvu liikmed uuesti kokku, saa-

des tulemuseks $\frac{-3}{13}$:

$$\begin{aligned}\ldots 10341034 &= 4\sum_{i\geq 0}^{\infty} 5^{4i} + 3\cdot 5\sum_{i\geq 0}^{\infty} 5^{4i} + 5^3\sum_{i\geq 0}^{\infty} 5^{4i} \\ &= \frac{4}{1-5^4} + \frac{15}{1-5^4} + \frac{125}{1-5^4} = \frac{4+15+125}{1-5^4} \\ &= \frac{-144}{624} = \frac{-3\cdot 48}{13\cdot 48} = \frac{-3}{13}.\end{aligned}$$

Näide 5.4. Leiame arvu $\frac{53}{12}$ 3-aadilise kuju. Paneme tähele, et $\frac{53}{12} = \frac{53}{4}\cdot\frac{1}{3}$ ja $\left|\frac{53}{4}\right|_3 = 1$, seega leiame alguses arvu $\frac{53}{4}$ 3-aadilise kuju ning hiljem jagame selle läbi kolmega. Samuti, kuna $\frac{53}{4} > 0$, siis otsime esiteks arvu $r = -\frac{53}{4}$ 3-aadilist kuju.

Paneme tähele, et $-14 < r < -13$, seega valime $N = 13$, sest sellisel juhul $-1 < r + N < 0$ ja $r + 13 = -\frac{1}{4} \in \mathbb{Z}_3^{\times} \cap (-1, 0)$. Leiame arvu $-\frac{1}{4}$ 3-aadilise kuju:

$$r + 13 = -\frac{1}{4} = -\frac{2}{3^2-1} = \frac{2}{1-3^2} = \overline{02} = \ldots 020202.$$

Arvu 13 3-aadiline kuju on 111 ning järelikult

$$r = -13 - \frac{1}{4} = (-111 + 0202) + \overline{02}0000 = \overline{20}021.$$

Leiame nüüd arvu $\frac{53}{4}$ 3-aadilise kuju leides arvu $\overline{20}021$ vastandelemendi:

$$\frac{53}{4} = -r = -\overline{20}021 = \overline{02}202.$$

Lõpuks, jagades saadud arvu kolmega, saame tulemuseks

$$\frac{53}{12} = \frac{\overline{02}202}{3} = \overline{02}20.2.$$

Arvutuste korrektsuse kontrollimiseks liidame 3-aadilise arvu liikmed uuesti kokku, saades tulemuseks $\frac{53}{12}$:

$$\overline{02}20.2 = \frac{2}{3} + 6 + 3^2\cdot\frac{2}{1-3^2} = \frac{16+144-54}{24} = \frac{106}{24} = \frac{54}{12}.$$

6 Henseli lemma ja p-aadiliste arvude kongruentsus

Selles peatükis tutvustame viisi p-aadiliste polünoomide lahendamiseks. Tuleb välja, et p-aadiliste arvude korpuses on polünoome veelgi parem lahendada, kui reaalarvude korpuses. Aga kõigepealt tuletame meelde mõned arvuteooriast pärit teadmised.

Definitsioon 6.1. Öeldakse, et arvud $a, b \in \mathbb{Q}_p$, on kongruentsed mooduli p^n järgi ehk

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

kui $|a-b|_p \leq \frac{1}{p^n}$.

Definitsioon 6.2. Täisarvu a, mis ei jagu algarvuga p, nimetatakse *ruutjäägiks* mooduli p järgi, kui kongruentsil

$$x^2 \equiv a \ (\mod p)$$

leidub hulgas $(1, 2, \ldots, p-1)$ lahend. Vastasel juhul nimetatakse seda *mitteruutjäägiks*.

Proovime leida hulgast $\mathbb{Q}_7$ suurust $\sqrt{11}$. Selleks peame leidma jada selliseid 7-aadilisi numbreid $a_0, a_1, a_2, \ldots$, $0 \leq a_i \leq 6$, et

$$\left(a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots\right)^2 = 4 + 1 \cdot 7.$$

Kõigepealt näeme, et $a_0^2 \equiv 4 \ (\mod 7)$, mille lahendamisel saame tulemuseks $a_0 = 2$ või $a_0 = 5$. Kui $a_0 = 2$, siis

$$4a_1 \cdot 7 \equiv 1 \cdot 7 \ \left(\mod 7^2\right), \text{ kust } 4a_1 \equiv 1 \ (\mod 7) \text{ ja } a_1 = 2.$$

Järgmisena

$$4 + 1 \cdot 7 \equiv \left(2 + 2 \cdot 7 + a_2 \cdot 7^2\right)^2 \equiv 4 + 1 \cdot 7 + (4 + 4a_2) \cdot 7^2 \ \left(\mod 7^3\right),$$

kust saame, et $3a_2 \equiv 4 \ (\mod 7)$ ja seega $a_2 = 6$. Saame rea

$$a = 2 + 2 \cdot 7 + 6 \cdot 7^2 \ldots,$$

kus iga arv pärast a_0 on üheselt määratud, sest $0 \leq a_i \leq 6$. Kui aga võtta $a_0 = 5 \equiv -2 \ (\mod 7)$ siis saame lahendiks

$$-a = 5 + 4 \cdot 7 + 0 \cdot 7^2 + \ldots$$

Kuid igast 7-aadilisest arvust ei saa võtta ruutjuurt. Seda ei ole näiteks arvul $3 + 1 \cdot 7$, sest kongruents

$$a_0^2 \equiv 3 \ (\mod 7)$$

ei ole lahenduv kuna arv 3 on mooduli 7 järgi mitteruutjääk. Ülal näidatud meetodit võrrandite lahendamiseks hulgas $\mathbb{Q}_p$, näiteks $x^2 + 5 = 0$ lahendamiseks hulgas $\mathbb{Q}_7$, saab üldistada järgmise olulise tulemuse abil, mida kutsutakse Henseli lemmaks.

Teoreem 6.3 (***Henseli lemma***)**.** *Olgu $F(x) = c_0 + c_1 x + \ldots + c_n x^n$ polünoom, mille kordajad on p-aadilised täisarvud ja olgu*

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

funktsiooni $F(x)$ tuletis. Kui $\bar{a}_0 \in \mathbb{Z}_p$ on selline arv, mis rahuldab tingimusi

$$F\left(\bar{a}_0\right) \equiv 0 \ (mod\ p)$$

ja

$$F'(\bar{a}_0) \not\equiv 0 \pmod{p},$$

siis leidub täpselt üks p-aadiline täisarv a, mis rahuldab korraga tingimusi $F(a) = 0$ ning $a \equiv \bar{a}_0 \pmod{p}$.

Tõestus. Tõestame induktsiooni abil järgmise väite:
Iga $n \in \mathbb{N} \cup (0)$ jaoks leidub p-aadiline täisarv kujul

$$a_n = b_0 + b_1 p + \ldots + b_n p^n \quad b_i \in \{0, 1, \ldots, p-1\},$$

nii, et

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

On selge, et väide kehtib $n = 0$ korral, võttes $b_0 = \bar{a}_0$, kus b_0 on arvu a_0 esimene p-aadiline number. Siis eelduste kohaselt $b_0 \equiv a_0 \pmod{p}$ ja kuna $F(b_0) \equiv 0 \pmod{p}$ ning $a_0 \equiv b_0 \pmod{p}$ siis järelikult kehtib ka

$$F(a_0) \equiv F(b_0) \equiv 0 \pmod{p}.$$

Nüüd eeldame, et väide kehtib $n-1$ jaoks ning näitame selle kehtivust juhu n jaoks. Selleks võtame $a_n = a_{n-1} + b_n p^n$, kus $b_n \in \{0, 1, \ldots, p-1\}$ on veel tundmatu. Kirjutame valemi $F(a_n)$ lahti, ignoreerides liikmeid, mis jaguvad arvuga p^{n+1}:

$$\begin{aligned} F(a_n) = F(a_{n-1} + b_n p^n) &= \sum_{i=1}^{n} c_i (a_{n-1} + b_n p^n)^i \\ &\equiv \sum_{i=1}^{n} \left(c_i a_{n-1}^i + c_i i a_{n-1}^{i-1} b_n p^n\right) \pmod{p^{n+1}} \\ &= \sum_{i=1}^{n} c_i a_{n-1}^i + c_i b_n p^n \sum_{i=1}^{n} i a_{n-1}^{i-1} \\ &= F(a_{n-1}) + b_n p^n F'(a_{n-1}). \end{aligned}$$

Kuna induktsiooni eelduse kohaselt $F(a_{n-1}) \equiv 0 \pmod{p^n}$, siis järelikult $F(a_{n-1}) = \alpha_n p^n$, kus α_n on mingi arv hulgast $\{0, 1, \ldots, p-1\}$. Seetõttu saame meie soovitava tingimuse $F(a_n) \equiv 0 \pmod{p^{n+1}}$ kirjutada kujul

$$\alpha_n p^n + b_n p^n F'(a_{n-1}) \equiv 0 \pmod{p^{n+1}}, .$$

Arvu b_n leidmiseks viime selle kongruentsi kujule

$$\alpha_n + b_n F'(a_{n-1}) \equiv 0 \pmod{p}. \tag{6.1}$$

Tänu eeldustele $a_{n-1} \equiv \bar{a}_0 \pmod{p}$ ja $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$ saame, et

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

Järelikult leidub arvul $F'(a_{n-1})$ mooduli p järgi pöördelement ja korrutades sellega võrrandi (6.1) mõlemaid pooli läbi on meil võimalik leida number b_n ehk

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

Siit saame, et

$$\begin{aligned} F(a_n) &\equiv F(a_{n-1}) + b_n p^n F'(a_{n-1}) \equiv F(a_{n-1}) - \alpha_n p^n \\ &\equiv F(a_{n-1}) - F(a_{n-1}) = 0 \pmod{p^{n+1}}. \end{aligned}$$

Kuna ilmselt ka

$$a_n \equiv a_{n-1} \equiv \ldots \equiv \bar{a}_0 \pmod{p},$$

siis oleme näidanud, et väide kehtib ka juhul n. Näitame nüüd, et arv $\bar{a}_0$ rahuldab ka ülejäänuid lemma tingimusi.

Alustades $a_0 = \bar{a}_0$ leidsime eelnevalt p-aadilistest täisarvudest koosneva jada $a_0, a_1, a_2, \ldots$, kus iga n korral kehtivad kongruentsid $F(a_n) \equiv 0 \pmod{p^{n+1}}$ ja $a_{n+1} \equiv a_n \pmod{p^{n+1}}$. Paneme tähele, et viimasest järeldub kongruentsi $a_m \equiv a_n \pmod{p^{n+1}}$ kehtivus iga $m > n$ korral. Sealt võime omakorda järeldada, et (a_i) on Cauchy jada, sest $a_m - a_n \equiv 0 \pmod{p^{n+1}}$ ehk

$$|a_m - a_k| \leq \frac{1}{p^{n+1}} \text{ kõigi } m, k \geq n+1 \text{ korral.}$$

Olgu α jada (a_i) piirväärtus. Peame näitama, et $F(\bar{a}_0) = 0$ ning $\bar{a}_0 = \alpha \pmod{p}$. Kuna kõigi indeksite m, n korral kehtib $a_m \equiv a_n \pmod{p^{n+1}}$, siis piiriprotsessis $n \to \infty$ saamegi $\alpha \equiv a_n \pmod{p^{n+1}}$. Valides $n = 0$ näeme, et kehtib $a_0 = \bar{a}_0 = \alpha \pmod{p}$ nagu soovitud. Suvalise $n > 0$ korral kehtib ka

$$\bar{a}_0 \equiv a_n \pmod{p^{n+1}} \Longrightarrow F(\bar{a}_0) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}} \Longrightarrow |F(\bar{a}_0)|_p \leq \frac{1}{p^{n+1}}.$$

Viimane kehtib iga indeksi n korral, seega $\frac{1}{p^{n+1}} \to 0$, kui $n \to \infty$ ning järelikult $F(\bar{a}_0) = 0$.

Lõpuks näitame, et $\bar{a}_0$ on ainus selline polünoomi $F(x)$ juur, mis on kongruentne arvuga α. Eeldame, et $F(\bar{b}_0) = 0$ ning $\alpha \equiv \bar{b}_0 \pmod{p}$. Selleks, et näidata võrduse $\bar{a}_0 = \bar{b}_0$ kehtivust, peame näitama, et $\bar{a}_0 \equiv \bar{b}_0 \pmod{p^n}$ iga n korral. $n = 1$ korral väide ilmselt kehtib. Eeldame, et $n \geq 1$ ning $\bar{a}_0 \equiv \bar{b}_0 \pmod{p^n}$. Sellisel juhul $\bar{b}_0 = \bar{a}_0 + sp^n$, kus s on mingi p-aadiline täisarv ning eelnevalt saadud tulemuse põhjal kehtib

$$F(\bar{b}_0) \equiv F(\bar{a}_0 + sp^n) \equiv F(\bar{a}_0) + F'(\bar{a}_0)\, sp^n \pmod{p^{n+1}}.$$

Kuna $\bar{a}_0$ ja $\bar{b}_0$ on mõlemad polünoomi F juured, siis saame selle kongruentsi kujule

$$0 \equiv F'(\bar{a}_0)\, sp^n \pmod{p^{n+1}}$$

ehk järelikult $F'(\bar{a}_0)\, s \equiv 0 \pmod{p}$. Kuna eelduste kohaselt $F'(\bar{a}_0) \equiv F'(\alpha) \not\equiv 0 \pmod{p}$,

siis peab kehtima $s \equiv 0 \pmod{p}$, mis tähendabki, et $\bar{a}_0 \equiv \bar{b}_0 \pmod{p^{n+1}}$ ehk $\bar{a}_0 = \bar{b}_0$. Samuti teame, et arvude jada (a_n) liikmed on ühesed, seega peab arv $\bar{a}_0$ olema samuti ühene. □

Märkus 6.4. Newtoni meetodi abil polünoomi f reaalarvuliste juurte leidmisel (tingimusel, et $f'(a_{n-1}) \neq 0$) leiame järgmise lähendi valemist

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

mis on väga sarnane Henseli lemmas saadud valemile

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

Henseli lemma erineb aga Newtoni meetodist selle osas. et Henseli lemmas saadud valemi abil saadud jada koondub alati, kuid Newtoni meetodi puhul ei tarvitse iga alglähend omada koonduvat jada.. Viimast näiteks siis, kui alglähend ei ole otisitavale juurele piisavalt lähedal. Võrrandi $f(x) = x^3 - x$ puhul saame $a_0 = \frac{1}{\sqrt{5}}$ valikul, et $a_1 = -\frac{1}{\sqrt{5}}$, $a_2 = \frac{1}{\sqrt{5}}$, jne.

Definitsioon 6.5. Olgu jada (a_k) arvuks a koonduv jada. Öeldakse, et funktsioon $F : \mathbb{Q}_p \to \mathbb{Q}_p$ on pidev punktis a, kui

$$\lim_{k\to\infty} F(a_k) = F(a)$$

Lemma 6.6. *Olgu a p-aadiline täisarv, mille kanooniliseks kujuks on $\sum_{i=0}^{\infty} a_i p^i$. Siis*

$$a - \sum_{i=0}^{k-1} a_i p^i \equiv 0 \left(mod\ p^k\right).$$

Tõestus. Olgu a p-aadiline täisarv. Paneme tähele, et

$$\lim_{n\to\infty} \left| \sum_{i=0}^{n} a_i p^i - \sum_{i=0}^{k-1} a_i p^i \right|_p = \lim_{n\to\infty} \left| \sum_{i=k}^{n} a_i p^i \right|_p \leq \frac{1}{p^k}$$

Kongruentsuse definitsiooni järgi tähendabki see, et $a - \sum_{i=0}^{k-1} a_i p^i \equiv 0 \pmod{p^k}$. □

Teoreem 6.7. *Täisarvuliste kordajatega polünoomil on juur hulgas $\mathbb{Z}_p$ parajasti siis, kui sellel on täisarvuline juur mooduli p^k järgi iga $k \geq 1$ korral.*

Tõestus. Olgu $F(x)$ täisarvuliste kordajatega polünoom ja olgu $a \in \mathbb{Z}_p$ selle juur ehk

$$F(a) = 0.$$

Siis teoreemi 3.11. kohaselt leidub selline täisarvude jada $(a_1, a_2, \ldots)$, kus

$$a_k = b_0 + b_1 p + b_2 p^2 + \ldots + b_{k-1} p^{k-1},$$

et

$$a = a_k \ \left(\mod p^k \right).$$

Kuna $F\left(a_k\right) \equiv F\left(a\right) \ \left(\mod p^k \right)$ ja $F\left(a\right) = 0$ siis

$$F\left(a_k\right) \equiv 0 \ \left(\mod p^k \right).$$

Teisipidi, eeldame, et võrrandil

$$F\left(a_k\right) \equiv 0 \ \left(\mod p^k \right)$$

leidub täisarvuline lahend a_k iga $k \geq 1$ korral. Teoreemi 3.17. põhjal leidub jadal (a_k) koonduv osajada (a_{k_i}). Olgu $\lim\limits_{i \to \infty} a_{k_i} = a$. Peame näitama, et $F\left(a\right) = 0$. Kontrollides saame, et polünoomid on pidevad funktsiooni, seega

$$\lim_{k_i \to \infty} F\left(a_{k_i}\right) = F\left(a\right).$$

Samuti teame eelduste kohaselt, et

$$F\left(a_k\right) \equiv 0 \ \left(\mod p^k \right)$$

ning seega $\lim\limits_{k \to \infty} F\left(a_k\right) = 0$ ehk $F(a) = 0$. □

Selle teoreemi üks praktiline järeldus on see, et kui polünoomil $F(x)$ puuduvad juured mooduli p järgi, siis puuduvad sellel ka juured hulgas $\mathbb{Z}_p$. Kui neid leidub, siis enamasti ei ole arvutuslikult kuigi raske mooduli p järgi polünoomi juuri leida, sest selleks on kandidaate vaid p tükki. Kui meil õnnestub leida selline arv a, mis on polünoomi $F(x)$ juureks, kuid mis ei ole funktsiooni $F'(x)$ juureks mooduli p järgi, siis Henseli lemmat kasutades saame leida polünoomile $F(x)$ juure hulgas $\mathbb{Z}_p$

Lause 6.8. *Täisarv a, mis ei jagu arvuga p, omab ruutjuurt hulgas $\mathbb{Z}_p$ $(p \neq 2)$ siis ja ainult siis, kui a on ruutjääk mooduli p järgi.*

Tõestus. Olgu $P(x) = x^2 - a,$ siis $P'(x) = 2x$. Kui a on ruutjääk mooduli p järgi, siis

$$a \equiv a_1^2 \ (\mod p)$$

mingi $a_1 \in \{1, 2, \ldots, p-1\}$ korral. Seega $P(a_1) \equiv 0 \pmod{p}$ ja

$$P'(a_1) = 2a_1 \not\equiv 0 \pmod{p},$$

kuna $(a_1, p) = 1$ ja järelikult ei ole võimalik, et p jagab arvu $2a_1$. Seega Henseli lemma järgi leidub polünoomil $P(x)$ hulgas $\mathbb{Z}_p$ juur.

Teisipidi, kui a on mitteruutjuut mooduli p järgi siis eelmise teoreemi põhjal ei leidu sellel hulgas $\mathbb{Z}_p$ ruutjuurt, sest ei ole võimalik leida sellist arvu $x = a_1$, et

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

□

Järeldus 6.9. $\sqrt{-1} \in \mathbb{Z}_p \iff p \equiv 1 \,(mod\ p)$.

7 p-aadiliste arvude omadused

Antud peatükis anname ülevaate p-aadiliste arvude mõnedest olulisematest omadustest. Paneme tähele, et kuna $\mathbb{Q}_p$ on ultrameetriline korpus, siis kehtivad selles kõik teises peatükis tõestatud ultrameetriliste ruumide omadused.

7.1 Topoloogilised omadused

Korpusel $\mathbb{Q}_p$ on palju sarnasusi reaalarvude hulgaga: need on mõlemad täielikud normeeritud korpused ning korpuse $\mathbb{Q}$ sellised täieldid, kus $\mathbb{Q}$ on kõikjal tihe alamhulk. Näitame, et korpusel $\mathbb{Q}_p$ on teisigi omadusi, mis on ka korpusel $\mathbb{R}$, kuid ka selliseid omadusi, mida reaalarvude hulgal ei ole.

Definitsioon 7.1. Hulga X alamhulkade süsteem τ on *topoloogia* ehk lahtiste hulkade süsteem hulgal X, kui on täidetud järgmised tingimused:

(T1) Lahtiste hulkade mis tahes ühend on lahtine hulk;

(T2) Lahtiste hulkade lõplik ühisosa on lahtine hulk;

(T3) $\emptyset$ ja X on lahtised hulgad.

Tingimusi T1-T3 nimetatakse *topoloogia aksioomideks* ning hulka X koos topoloogiaga τ *topoloogiliseks ruumiks*, mida tähistatakse(X, τ).

Meetrilises ruumis defineeritakse topoloogia kerade abil: alamhulka $G \subset X$ nimetatakse lahtiseks, kui iga $g \in G$ korral leidub $r > 0$ omadusega $B(g, r) \subset G$. On lihtne kontrollida, et nii defineeritud lahtised hulgad rahuldavad topoloogia aksioome ning seega on iga meetriline ruum topoloogiline ruum. Sealjuures on iga lahtine kera alati lahtine hulk ja kinnine kera kinnine hulk.

Definitsioon 7.2. Olgu (X,τ) topoloogiline ruum ning $Y \subset X$. Hulga Y topoloogiat

$$\tau|_Y = \{Y \cap U : U \in \tau\}$$

nimetatakse *alamruumi topoloogiaks* hulgal Y. Hulka koos topoloogiaga $\tau|_Y$ nimetatakse topoloogilise ruumi (X,τ) *alamruumiks.*

Esiteks vaatleme mõningaid kerade ja sfääride omadusi ruumis $\mathbb{Q}_p$.

Lause 7.3. *Sfäär* $S(a,r) = \left\{x \in \mathbb{Q}_p \,\middle|\, |x-a|_p = r\right\}$ *on ruumis* $\mathbb{Q}_p$ *nii lahtine kui ka kinnine hulk.*

Tõestus. Olgu $S(a,r)$ sfäär ruumis $\mathbb{Q}_p$ ja $\varepsilon < r$. Tõestame esiteks, et see on lahtine hulk. Selleks näitame, et kui $x \in S(a,r)$, siis $B(x,\varepsilon) \subset S(a,r)$. Olgu $y \in B(x,\varepsilon)$. Siis

$$|x-y|_p < \varepsilon < r = |x-a|_p .$$

Lause 2.4. kohaselt teame, et kui p-aadilised arvud k ja l rahuldavad võrratust

$$|k-l|_p < |l|_p ,$$

siis $|k|_p = |l|_p$. Võttes $k = y-a$ ja $l = x-a$ saame, et

$$|y-a-x+a|_p = |y-x|_p < |x-a|_p .$$

See tähendabki, et

$$|y-a|_p = |x-a|_p = r$$

ehk tõepoolest $y \in S(a,r)$.

Näitame nüüd, et $S(a,r)$ on kinnine hulk. Lausest 2.7. teame, et kerad $B(a,r)$ ja $\overline{B}(a,r)$ on ruumis $\mathbb{Q}_p$ nii lahtised kui ka kinnised hulgad. Kuna $B(a,r)$ on lahtine, siis on hulk $\mathbb{Q}_p \setminus B(a,r) = \left\{x \in \mathbb{Q}_p \,\middle|\, |x-a|_p \geq r\right\}$ kinnine. Järelikult on ka hulk $S(a,r)$ kinnine hulk, sest see on kahe kinnise hulga $\mathbb{Q}_p \setminus B(a,r)$ ja $\overline{B}(a,r)$ ühisosa. □

Viimane omadus võib tunduda väga kummaline, sest reaalarvude korpuses ei ole sfäärid kindlasti lahtised hulgad. Samuti, erinevalt p-aadiliste arvude hulgast, ei ole reaalarvude hulga kõik kerad samaaegselt nii lahtised kui ka kinnised hulgad. Tõestame siinkohal veel kaks huvitavat kerade omadust ruumis $\mathbb{Q}_p$.

Lause 7.4. *Kaks kera on ruumis* $\mathbb{Q}_p$ *mittelõikuvad siis ja ainult siis, kui üks neist keradest on sisestatud teisesse ehk*

$$B(a,r) \cap B(b,s) \neq \emptyset \Longleftrightarrow B(a,r) \subset B(b,s) \;\; \textit{või} \;\; B(a,r) \supset B(b,s) .$$

Tõestus. Olgu $B(a,r)$ ja $B(b,s)$ kerad ruumis $\mathbb{Q}_p$, $r \leq s$ ning $y \in B(a,r) \cap B(b,s)$. Siis tänu lausele 2.8. $B(a,r) = B(y,r)$ ning $B(b,s) = B(y,s)$. Kuna $B(y,r) \subset B(y,s)$,

siis $B(a,r) \subset B(b,s)$. Teisipidi, kui $B(a,r) \subset B(b,s)$ või $B(a,r) \supset B(b,s)$ siis nende ühisosa ei ole tühi hulk. □

Lause 7.5. *Ruumi $\mathbb{Q}_p$ kerade hulk on loenduv.*

Tõestus. Olgu $B(a,r)$ kera ruumis $\mathbb{Q}_p$, kus $r = p^{-s}$ kuulub p-aadilise normi võimalike väärtuste hulka. Esitame selle keskpunkti $a \in \mathbb{Q}_p$ kanoonilisel kujul

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

Tähistame

$$a_0 = \sum_{n=-m}^{s} a_n p^n.$$

Ilmselgelt on a_0 ratsionaalarv ning

$$|a - a_0|_p = \left| \sum_{n=s+1}^{\infty} a_n p^n \right|_p < p^{-s},$$

Järelikult $a_0 \in B(a, p^{-s})$ ning lause 2.8. kohaselt $B(a.p^{-s}) = B(a_0, p^{-s})$. Kuna a_0 on ratsionaalarv, siis fikseeritud raadiusega erinevaid kerasid on ülimalt nii palju, kui on erinevaid ratsionaalarve a_0 ehk neid on loenduv arv. Samuti teame, et normi $|\cdot|_p$ väärtuste hulk on loenduv ehk erinevaid mingi kindla keskpunktiga kerasid on samuti vaid loenduv hulk. Järelikult on ka kerade $B(a, p^{-s})$ hulk loenduv. □

Nüüd tõestame veel mõned huvitavad hulkade $\mathbb{Z}_p$ ning $\mathbb{Q}_p$ omadused.

Definitsioon 7.6. Topoloogilist ruumi X nimetatakse *kompaktseks*, kui iga jadal ruumis X leidub koonduv osajada, mis koondub mingiks elemendiks $a \in X$.

Definitsioon 7.7. Topoloogilist ruumi X nimetatakse *lokaalselt kompaktseks*, kui igal punktil hulgast X leidub kompaktne ümbrus.

Teoreem 7.8 ([9, peatükk 3.6])**.** *Normeeritud ruum on kompaktne parajasti siis, kui selle kinnine ühiskkera on kompaktne.*

Lause 7.9. *Normeeritud korpus $\mathbb{Q}_p$ on lokaalselt kompaktne.*

Tõestus. See teoreem järeldub vahetult teoreemist 3.17, kust teame, et korpuse $\mathbb{Q}_p$ kinnine ühikkera on kompaktne. □

Teoreem 7.10. *Hulk $\mathbb{Z}_p$ on täielik.*

Tõestus. Lause 3.16. kohaselt omab iga Cauchy jada (x_n) hulgas $\mathbb{Z}_p$ koonduvat osajada (x_{n_k}), mis koondub mingiks p-aadiliseks arvuks $a \in \mathbb{Z}_p$. Siis leidub selline K, et kui $k \geq K_1$, siis $|a - x_{n_k}|_p < \frac{\varepsilon}{2}$. Kuna (x_n) on Cauchy jada, siis iga $n \geq m \geq K_2$ korral $|x_n - x_m|_p < \varepsilon$.. Valides $K \geq \max\{K_1, K_2\}$ saame, et

$$|x_K - a|_p = |x_K + x_{n_k} - x_{n_k} - a|_p \leq |x_K - x_{n_k}|_p + |x_{n_k} - a|_p < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

ehk jada (x_n) koondub ise samuti p-aadiliseks täisarvuks a. See tähendabki, et $\mathbb{Z}_p$ on täielik. □

Definitsioon 7.11. Hulga X alamhulka A nimetatakse seal hulgas *kõikjal tihedaks*, kui iga punkt hulgas X kas kuulub hulka A või on mingi jada (x_n), kus $x_n \in A$, piirväärtuseks.

Lause 7.12. *Täisarvude hulk $\mathbb{Z}$ on hulgas $\mathbb{Z}_p$ kõikjal tihe.*

Tõestus. Olgu $x = \ldots a_2 a_1 a_0 \in \mathbb{Z}_p$. Tähistame iga naturaalarvu n korral

$$x_n = \ldots 000 a_n a_{n-1} \ldots a_1 a_0 = \sum_{i=0}^{n} a_i p^i$$

Sellisel juhul $x_n \in \mathbb{Z}$ ning $|x - x_n| < p^{-n}$ ehk arv x on jada (x_n) piirväärtuseks. □

Definitsioon 7.13. Topoloogilist ruumi X nimetatakse *nullmõõtmeliseks* ruumiks, kui iga $a \in X$ ja selle mistahes ümbruse $U(a)$ jaoks leidub selline hulk V, $a \in V \subset U(a)$, mis on korraga nii kinnine, kui ka lahtine hulk.

Definitsioon 7.14. Öeldakse, et topoloogilise ruumi X alamruum Y on *mittesidus*, kui on võimalik leida kaks sellist lahtist hulka U ja V , et $U \cap V = \emptyset$, $Y = U \cup V$ ning kumbki hulkadest $Y \cap U$, $Y \cap V$ ei ole tühi. Kui selliseid hulki U ja V ei leidu, siis nimetatakse alamruumi Y *sidusaks*. Ruumi X nimetatakse sidusaks, kui see on sidus iseenda alamruumina.

Definitsioon 7.15. Topoloogilist ruumi X kutsutakse *täielikult mittesidusaks*, kui selle ainast sidusad alamruumid on tühi hulk $\emptyset$ ja ühepunktilised hulgad $\{a\}$, kus $a \in X$.

Teoreem 7.16. *Topoloogiline ruum $\mathbb{Q}_p$ on nullmõõtmeline ja täielikult mittesidus.*

Tõestus. Paneme tähele, et kõigi $a \in \mathbb{Q}_p$ ja naturaalarvude n korral tänu sellele, et p-aadilise normi võimalike väärtuste hulk on $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$, kehtib

$$\begin{aligned} U_n(a) \coloneqq \overline{B}\left(a, \frac{1}{p^n}\right) &= \left\{ x \in \mathbb{Q}_p \,\middle|\, |x - a|_p \leq \frac{1}{p^n} \right\} \\ &= \left\{ x \in \mathbb{Q}_p \,\middle|\, |x - a|_p < \frac{1}{p^{n-1}} \right\} \\ &= B\left(a, \frac{1}{p^{n-1}}\right) \end{aligned}$$

ehk p-aadilise arvu ümbrus $U_n(a)$ on korraga nii lahtine, kui ka kinnine kera. Järelikult on hulk $B\left(a, \frac{1}{p^n}\right)$ samuti kinnine ja lahtine hulk, ning kuna ilmselt $B\left(a, \frac{1}{p^n}\right) \subset B\left(a, \frac{1}{p^{n-1}}\right)$ siis definitsiooni järgi tähendabki see seda, et ruum $\mathbb{Q}_p$ on nullmõõtmeline. Näitame nüüd, et $\mathbb{Q}_p$ on täielikult mittesidus.

Olgu A selline ruumi $\mathbb{Q}_p$ alamruum, et $a \in A$ ja $A \neq \{a\}$. Olgu b mingi teine element ruumis A ja $|a-b|_p = \frac{1}{p^m}$. Antud norm ei saa võrduda nulliga, sest a ja b on erinevad elemendid. Järelikult $b \notin B\left(a, \frac{1}{p^{m-1}}\right) = U_{m-1}(a)$ ehk leidub selline arvu a ümbrus, mis ei sisalda kõiki ruumi A elemente. Järelikult

$$A = U_{m-1}(a) \cup (A \setminus U_{m-1}(a)),$$

kus mõlemad hulgad $A \setminus U_{m+1}(a)$ ja $U_{m+1}(a)$ on mittetühjad. Paneme tähele, et hulgad $U_{m+1}(a)$ ja $A \setminus U_{m+1}(a)$ on lahtised lahtised, sest lause 2.7. kohaselt on kera $B\left(a, \frac{1}{p^{m+1}}\right) = U_{m+1}(a)$ korraga nii lahtine, kui ka kinnine hulk. Kuna kinnise hulga täield on lahtine hulk siis on ka hulk $A \setminus U_m(a)$ lahtine. Sellest järeldub, et A on mittesidus ning seega on ruum $\mathbb{Q}_p$ täielikult mittesidus, kuna selle ainsad sidusad alamhulgad on tõesti tühi hulk ning ühepunktilised hulgad. □

7.2 Jadad ja read korpuses $\mathbb{Q}_p$

Alustuseks tõestame ühe väga kasuliku omaduse jadade kohta korpuses $\mathbb{Q}_p$.

Teoreem 7.17. *p-aadiliste arvude jada (a_n) on Cauchy jada ja seega koonduv parajasti siis, kui*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0. \tag{7.1}$$

Tõestus. Olgu jada (a_n) Cauchy jada korpuses $\mathbb{Q}_p$. Definitsiooni kohaselt on jada Cauchy siis, kui

$$\lim_{m,n\to\infty} |a_m - a_n|_p = 0.$$

Tingimus (6.1) ilmselt kehtib, kui valida $m = n+1$.

Olgu nüüd (a_n) selline jada, et tingimus (7.1) on rahuldatud. See tähendab, et iga $\varepsilon > 0$ jaoks leidub selline indeks N, et iga $n > N$ korral

$$|a_{n+1} - a_n|_p < \varepsilon.$$

Nüüd valime $m > n > N$. Tugevat kolmnurga võrratust kasutades saame, et

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + \ldots - a_n|_p \\ &\leq \max\left\{|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, \ldots, |a_{n+1} - a_n|_p\right\} < \varepsilon \end{aligned}$$

mis tähendabki, et jada (a_n) on Cauchy jada. □

Lause 7.18 ([9, lause 2.17.]). *Koondugu jada (a_n) korpuses $\mathbb{Q}_p$ arvuks a. Siis kas*

$$\lim_{n\to\infty} |a_n|_p = 0$$

või leidub selline indeks N, et $|a_n|_p = |a|_p$ iga $n > N$ korral.

Vaatleme nüüd ridu $\sum_{i=1}^{\infty} a_i$ hulgas $\mathbb{Q}_p$.

Definitsioon 7.19. Rida $\sum_{i=1}^{\infty} a_i$ *koondub* hulgas $\mathbb{Q}_p$, kui tema osasummade jada $S_n = \sum_{i=1}^{n} a_i$ koondub hulgas $\mathbb{Q}_p$.

Definitsioon 7.20. Rida $\sum_{i=1}^{\infty} a_i$ on *absoluutselt koonduv* hulgas $\mathbb{Q}_p$, kui rida $\sum_{i=1}^{\infty} |a_i|_p$ koondub hulgas $\mathbb{R}$.

Lause 7.21. *Hulgas $\mathbb{Q}_p$ on iga absoluutselt koonduv rida koonduv.*

Tõestus. Tähistame $\sum_{i=1}^{\infty} |a_i|_p = \lim_{n\to\infty} S_n$ koondub, siis see on osasummade S_n Cauchy rida, s.t iga $\varepsilon > 0$ jaoks leidub selline indeks N, et iga $m > n > N$ korral

$$S_m - S_n = \sum_{k=n+1}^{m} |a_i|_p < \varepsilon.$$

Kolmnurga võrratust kasutades saame, et

$$|S_m - S_n|_p = \left| \sum_{k=n+1}^{m} a_i \right|_p \leq \sum_{i=1}^{\infty} |a_i|_p < \varepsilon,$$

mis tähendab, et (S_n) on Cauchy jada ja seega rida $\sum_{i=1}^{\infty} a_i$ koondub hulgas $\mathbb{Q}_p$. □

Märkus 7.22. Paneme tähele, et vastupidine väide ei kehti ehk iga korpuses $\mathbb{Q}_p$ koonduv rida ei ole aboluutselt koonduv. Näiteks rida

$$\sum_{i=0}^{\infty} a_n = 1 + \ldots + \underbrace{p^{-i} + \ldots + p^{-i}}_{p^i \text{ tükki}} + \ldots$$

koondub, sest $a_n \to 0$, kui $n \to \infty$ aga

$$\sum_{i=0}^{\infty} |a_n|_p = 1 + p \cdot p^{-1} + p^2 \cdot p^{-2} + \ldots = \infty.$$

Nüüd tõestame ühe huvitava omaduse, mida tihti peale kutsutakse „rebase unistuseks", sest see annab väga lihtsa tingimuse ridade koondumise kontrollimseks korpuses $\mathbb{Q}_p$.

Lause 7.23. *Rida* $\sum_{i=1}^{\infty} a_i$ *, kus* $a_i \in \mathbb{Q}_p$*, koondub siis ja ainult siis, kui*

$$\lim_{n\to\infty} a_n = 0,$$

kusjuures sellisel juhul

$$\left|\sum_{i=1}^{\infty} a_i\right|_p \leq \max_n |a_n|_p .$$

Tõestus. Eeldame, et rida $\sum_{i=1}^{\infty} a_i$ koondub. Kui $\sum_{i=1}^{\infty} a_i = 0$, siis on väide ilmne. Kui $\sum_{i=1}^{\infty} a_i > 0$, siis tänu sellele, et $a_n \to 0$, jada S_n koondub ning lause 7.16 põhjal leidub selline indeks N, et

$$|S|_p = \left|\sum_{i=1}^{\infty} a_i\right|_p = \left|\sum_{i=1}^{N} a_i\right|_p = |S_n|_p .$$

Kuna $|a_n|_p = |a|_p$ iga $n > N$ korral, siis

$$\max\left\{ |a_n|_p \,\middle|\, 1 \leq n \leq N \right\} = \max_n |a_n|_p .$$

Tugeva kolmnurga võrratuse järgi kehtibki

$$\left|\sum_{i=1}^{N} a_i\right|_p \leq \max\left\{ |a_n|_p \,\middle|\, 1 \leq n \leq N \right\} = \max_n |a_n|_p .$$

□

See omadus ei kehti reaalarvude vallas, näiteks hajuva harmoonilise rea $\sum_{i=1}^{\infty} \frac{1}{n}$ üldliige hääbub. Samas paneme tähele, et rida $\sum_{n=1}^{\infty} n!$ on p-aadiliste arvude korpuses koonduv rida, sest $|n!|_p \to 0$, kui $n \to \infty$ ehk $\lim_{n\to\infty} n! = 0$.Kuid eii ole veel teada, kas mõne algarvu p korral rida $\sum_{n=1}^{\infty} n!$ on ka ratsionaalarv.

7.3 Algebralised omadused

Oleme juba näinud, et p-aadilistel täisarvudel on mitmeid huvitavaid omadusi, mida ei ole täisarvudel. Selles alapeatükis näeme, et nende algebralised omadused on vähemalt sama head, kui täisarvude omadused. Meenutame esiteks mõningaid algebra mõisteid.

Definitsioon 7.24. Lõpliku *rühma järguks* nimetatakse selle elementide arvu. *Elemendi a järguks* lõplikus rühmas G nimetatakse vähimat sellist naturaalarvu n, mille korral $a^n = 1$.

Lemma 7.25 ([2, lemma 7.3.]). *Olgu G rühm, olgu elemendi $a \in G$ järk m ning olgu $l \in N$. Siis $a^l = 1$ parajasti siis, kui $m|l$.*

Teoreem 7.26 (***Lagrange'i teoreem***[1, teoreem 6.1.5]). *Lõpliku rühma mistahes alamrühma järk on rühma järgu jagajaks.*

Definitsioon 7.27. Lõplikku rühma G nimetatakse *tsükliliseks*, kui leidub selline element $g \in G$, et kõik selle rühma elemendid on avaldatavad selle elemendi astmena ehk iga $a \in G$ korral $a = g^k$ mingi täisarvu k korral. Sealjuures nimetatakse elementi g rühma G *moodustajaks* ning kasutatakse tähistust $(g) = \{g^k | k \in \mathbb{Z}\} = G$.

Definitsioon 7.28. *Integriteetkonnaks* nimetatakse ühikelemendiga kommutatiivset nullitegurite ringi.

Näiteks moodustab integriteetkonna täisarvude ring. Samuti on integriteetkond $\mathbb{Z}_p$, sest see sisaldub korpuses $\mathbb{Q}_p$ ning seega ei oma nullitegureid.

Definitsioon 7.29. Kommutatiivse ringi R ideaali I nimetatakse selle ringi elemendi a poolt moodustatud *peaideaaliks*, kui $I = aR = \{ax | x \in R\}$. Kui ring R kõik ideaalid on peaideaalid, siis nimetatakse seda *peaideaalringiks* ning kui ring R on korraga nii integreteetkond, kui ka peaideaalring, siis nimetame *peaideaalkonnaks.*

Lause 7.30. *Ring $\mathbb{Z}_p$ on peaideaalkond. Täpsemalt, selle ideaalideks on peaideaalid $\{0\}$ ja $p^k\mathbb{Z}_p$ iga $k \in \mathbb{N}$ korral.*

Tõestus. Olgu $I \neq \{0\}$ integriteetkonna $\mathbb{Z}_p$ ideaal ning $0 \neq a \in I$ selline element, millel on kõikidest selle ideaali elementidest maksimaalse väärtusega norm. Kuna p-aadiline norm väljastab vaid loenduva hulga väärtuseid, ning nende väärtuste hulga kuhjumispunktiks on ainult 0, siis on maksimaalne element alati võimalik leida. Oletame, et $|a|_p = p^{-k}$ mingi $k \in \mathbb{N}$ korral. Siis lause 4.10 põhjal $a = \epsilon p^k$, kus ϵ on mingi pööratav element ringis $\mathbb{Z}_p$. Seega $p^k = \epsilon^{-1}a \in I$ ja järelikult $\left(p^k\right) = p^k\mathbb{Z}_p \subset I$.

Teisipidi, iga $0 \neq b \in I$ korral $|b|_p = p^{-\omega} \leq p^{-k}$ mingi naturaalarvu ω korral. Seega saame kirjutada, et

$$b = p^\omega \epsilon' = p^k p^{\omega - k} \epsilon' \in p^k \mathbb{Z}_p.$$

Ilmselt on ka $0 \in p^k\mathbb{Z}_p$ ja kehtibki $I \subset p^k\mathbb{Z}_p$ ning seega $I = p^k\mathbb{Z}_p$. □

Definitsioon 7.31. Korpuse K *karakteristikaks* nimetatakse vähimat sellist arvu n, et $n1 = 0$, kus 1 on korpuse ühikelement ning seda tähistatakse kui $\mathrm{char}(K)$. Kui sellist arv n ei eksiterri, siis öeldakse, et $\mathrm{char}(K) = 0$.

Kuna ratsionaalarvude korpus $\mathbb{Q}$ on p-aadiliste arvude $\mathbb{Q}_p$ lihtne alamkorpus, siis $\mathrm{char}(\mathbb{Q}_p) = 0$.

Definitsioon 7.32. Korpuse K elementi a nimetatakse *m-nda astme ühejuureks*, kui $a^m = 1$. Kui korpuses K on m-nda astme ühejuuri m tükki ning need kõik on esitatavad m-inda astme ühejuure a astmetena, siis ühejuurt a kutsutakse *m-nda astme algjuureks*.

Teoreem 7.33 ([1, teoreem 7.2.4])**.** *Olgu K korpus, karakteristikaga 0, $f \in K[x]$ ja $a \in K$. Element $a \in K$ on polünoomi f k-kordne juur siis ja ainult siis, kui*

$$f(a) = f^{(1)}(a) = \ldots = f^{(k-1)}(a) = 0,$$

aga $f^{(k)}(a) \neq 0$. Siin $f^{(j)}$ tähistab polünoomi f j-ndat tuletist.

Teoreem 7.34. *Korpuse K, $char(K) = 0$, m-nda astme ühejuurte hulk E_m on ühejuurte korrutamise suhtes $(p-1)$. järku tsükliline rühm.*

Tõestus. Näitame esiteks, et m-nda astme ühejuurte hulk E_m sisaldab m elementi. Kui $m = 1$ on väite kehtimine triviaalne. Kui $m \geq 2$, siis polünoom $x^m - 1$ ning selle tuletis mx^{m-1} ei oma ühiseid juuri, sest tänu sellele, et $\mathrm{char}(K) = 0$ on 0 polünoomi mx^{m-1} ainsaks juureks korpuses K. Kuna $\mathrm{char}(K) = 0$, siis teoreemi 7.30. kohaselt on kõik polünoomi $x^m - 1$ juured ühekordsed ning järelikult on hulgas E_m maksimaalselt m elementi.

Olgu $i, j \in E_m$, siis

$$\left(ij^{-1}\right)^m = i^m \left(j^m\right)^{-1} = 1$$

ehk $ij^{-1} \in E_m$ ja E_m on korrutamise suhtes rühm. Näitame nüüd, et see rühm on tsükliline.

Olgu $m = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$. Iga $i \in \{1, 2, \ldots, k\}$ korral on polünoomil $x^{\frac{m}{p_i}} - 1$ rühmas E_m ülimalt $\frac{m}{p_i}$ juurt, sest polünoomi juurte koguarv ei saa ületada tema astet. Kuna $m > \frac{m}{p_i}$, siis leidub hulgas E_m selliseid elemente, mis ei ole selle polünoomi juurteks. Olgu a_i üks sellistest elementidest ja tähistame

$$b_i = a_i^{\frac{m}{p_i^{r_i}}}.$$

Teame, et $b_i^{p_i^{r_i}} = b^m = 1$, järelikult on lemma 7.25 põhjal elemendi b_i järk arvu $p_i^{r_i}$ jagaja. Teisalt

$$b_i^{p_i^{r_i-1}} = a_i^{\frac{m}{p_i}} \neq 1$$

ehk elementi b_i järk on r_i.

Näitame, et element $b = b_1 b_2 \ldots b_k$ on ühejuurte rühma E_m moodustaja.. Olgu elemendi b järk h, siis Lagrange'i teoreemi tõttu $h|m$. Oletame nüüd vastuväiteliselt, et $h < m$. Järelikult h jagab ka vähemalt ühte arvudest $\frac{m}{p_i}$, $1 \leq i \leq k$, olgu selleks konkreetsuse mõttes $\frac{m}{p_1}$. Siis eelduse kohaselt

$$1 = b^{\frac{m}{p_1}} = b_1^{\frac{m}{p_1}} b_2^{\frac{m}{p_1}} \ldots b_k^{\frac{m}{p_1}}. \tag{7.2}$$

Kui $2 \leq i \leq k$, siis $p_i^{r_i}$ jagab arvu $\frac{m}{p_1}$ ning järelikult $b_i^{\frac{m}{p_1}} = 1$. Seega peab võrduse (7.2) kehtimiseks kehtima ka $b_1^{\frac{m}{p_1}} = 1$ ehk elemendi b_1 järk jagab arvu $\frac{m}{p_1} = p_1^{r_1-1}p_2^{r_2}\dots p_k^{r_k}$, kuid see on võimatu, sest selle järk on eelnevalt näidatu põhjal $p_1^{r_1} > p_1^{r_1-1}$. Järelikult on elemendi b järk m ning E_m on tsükliline rühm moodustajaga b. □

Teoreem 7.35 ([1, teoreem 6.3.10]). *Lõpliku tsüklilise rühma mistahes alamrühm on tsükliline rühm. Kui tsüklilise rühma G järk on n ning m on n jagaja, siis rühmas G leidub selline alamrühm H, mille järk on m, kusjuures juhul, kui võttes $n = lm$ ning tähistades $G = (g)$ siis g^l on rühma H moodustajaks.*

Lause 7.36. *Olgu p algarv ning m selline naturaalarv, millel puuduvad arvuga p ühistegurid. Korpuses $\mathbb{Q}_p$ leidub m-nda astme algjuur siis ja ainul siis, kui $m|(p-1)$. Viimasel juhul on iga m-nda astme ühejuur ka $(p-1)$. järku ühejuur. Korpuse $\mathbb{Q}_p$ $(p-1)$. järku ühejuured moodustavad rühmas $\mathbb{Z}_p^\times$ $(p-1)$. järku tsüklilise alamrühma.*

Tõestus. Näitame esiteks, et iga m-nda astme ühejuur on ka $(p-1)$. järku ühejuur. Olgu p algarv ning m selline naturaalarv, et $m|(p-1)$. Siis mingi naturaalarvu k korral $p-1 = mk$. Kui $a \in \mathbb{Q}_p$ on m-nda astme ühejuur, saame kirjutada, et ehk iga m-ndat järku ühejuur on ka $(p-1)$. järku ühejuur. Samuti paneme tähele, et kui a on m-nda astme ühejuur, siis peab kehtima

$$1 = |a^m|_p = |a|_p^m\,,$$

kust $a \in \mathbb{Z}_p^\times$.

Näitame nüüd, et korpuse $\mathbb{Q}_p$ $(p-1)$ järku ühejuured moodustavad tsüklilise alamrühma. Olgu

$$f(x) = x^{p-1} - 1, f'(x) = (p-1)x^{p-2}.$$

Valime vabalt täisarvu $x_0 \in \{1, \dots, p-1\}$. Siis Fermat' väikese teoreemi kohaselt

$$f(x_0) = x_0^{p-1} - 1 \equiv 0 \pmod{p}$$

aga

$$f'(x_0) = (p-1)x_0^{p-2} \not\equiv 0 \pmod{p}\,,$$

sest $\left|(p-1)x_0^{p-2}\right|_p = 1$, kuna x_0 on täisarv, mis ei jagu arvuga p ja $(p, p-1) = 1$. Seega Henseli lemma kohaselt leidub täpselt üks p-aadiline täisarv a, mis on funktsiooni $f(x)$ juureks ning $a \equiv x_0 \pmod{p}$. Kuna viimane arutelu kehtib iga $x_0 \in \{1, \dots, p-1\}$ korral, siis on meil võimalik leida polünoomile $f(x)$ $p-1$ erinevat juurt, mis on kõik $(p-1)$ järku ühejuured korpuses $\mathbb{Q}_p$, kusjuures nende juurte esimesed numbrikohad on järjest kõik arvud $1, 2, \dots, p-1$. Teoreemi 7.31 järgi ühejuurte hulk E_{p-1} on ühejuurte korrutamise suhtes tsükliline rühm, mille järk on maksimaalselt $(p-1)$. Järelikult rohkem $(p-1)$. järku ühejuuri olla ei saa ning üks nendest on selle rühma moodustajaks ehk $(p-1)$. astme algjuureks.

Lõpuks, olgu $a \in \mathbb{Z}_p^\times$ m-nda astme algjuur. Kui a_0 on arvu a esimene number, siis lause 4.7. kohaselt ei ole see null ning

$$a^m = (a_0 + a_1 p + \ldots)^m \equiv a_0^m \equiv 1 \pmod{p}.$$

Olgu $b \in E_{p-1}$ selline, et

$$a_0 \equiv b \pmod{p}.$$

Siis on polünoomi $g(x) = x^{m(p-1)} - 1$ juurteks nii a, kui ka b. Lisaks

$$m\,(p-1)\,a^{m(p-1)-1} \not\equiv 0 \pmod{p}$$

ja

$$m\,(p-1)\,b^{m(p-1)-1} \not\equiv 0 \pmod{p}$$

Seega a ja b on mõlemad polünoomi $g(x)$ juured. kuid $g'(a) \neq 0$ ja $g'(b) \neq 0$. Kuna

$$a \equiv a_0 \equiv b \pmod{p}$$

siis Henseli lemma ühesuse osa tõttu $a = b$. Seega on a $(p-1)$. astme ühejuur, mis tõttu on tema järk arvu $p-1$ jagaja. Kuna $a^m - 1 = 0$ ning m on vähim selline aste, mille korral see kehtib, siis $m|p-1$.

Teisipidi, eeldame, et $m|p-1$. Teoreemist 7.34 teame, et $(p-1)$. järku ühejuurte rühm E_{p-1} on tsükliline ning selle järk on $p-1 = mk$. Teoreemi 7.36 kohaselt leidub rühmas E_{p-1} tsükliline m. järku alamrühm. Viimase elemendid rahuldavad võrdust $x^m = 1$ ja neid on kokku m tükki, st. tegu on kõigi m. astme ühejuurte hulgaga E_m. Selle tsüklilise rühma moodustaja ongi otsitav m. astme algjuur. □

Viimasest teoreemist saab näiteks järeldada, et $i = \sqrt{-1} \in \mathbb{Q}_5$, sest tõepoolest, kuna $5 \nmid 4$ ja $4|5-1=4$, siis korpuses $\mathbb{Q}_5$ leidub neljanda astme algjuur ehk selline element, mis seega rahuldab võrrandit $x^4 - 1 = 0$, kust $x = i$.

7.4 p-aadiliste kompleksarvude korpus $\mathbb{C}_p$

Anname siinkohal lühikese sissejuhatuse p-aadiliste kompleksarvude valdkonda, mida me selles töös pikemalt ei käsitle.

Definitsioon 7.37. Korpust K nimetatakse *algebraliselt kinniseks*, kui mistahes mittekonstantsel polünoomil $F \in K[x]$ leidub selles korpuses juur.

Definitsioon 7.38. Olgu K ja L korpused. Korpust L nimetatakse korpuse K *algebraliseks laiendiks,* kui leidub injektiivne ringide homomorfism $f : K \to L$ ning iga korpuse L element on mingi polünoomi $F \in K[x]$ juureks.

Definitsioon 7.39. Korpuse K algebralist laiendit F, mis on algebraliselt kinnine, nimetatakse korpuse K *algebraliseks sulundiks.* Korpuse K algebralist sulundit tähistatakse sümboliga K^a .

Teoreem 7.40 ([9, peatükk 2.6]). *Igal korpusel K leidub algebraline sulund.*

On võimalik näidata, et korpus $\mathbb{Q}_p$ ei ole algebraliselt kinnine. Moodustades selle algebralise sulundi $\mathbb{Q}_p^a$, saame korpuse $\mathbb{Q}_p$ algebralise laiendi. Sulundi $\mathbb{Q}_p^a$ täieldit kutsutakse *p-aadiliste kompleksarvude* korpuseks ning seda tähistatakse sümboliga $\mathbb{C}_p$. Korpus $\mathbb{C}_p$ on algebraliselt kinnine. Toome siinkohal ilma tõestuseta mõned olulisemad korpuse $\left(\mathbb{C}_p, |\cdot|_p\right)$ omadused.

Lause 7.41 ([9, peatükk 2.6]). *Väärtuste hulk $|\mathbb{C}_p|_p$ on kõikjal tihe hulgas $[0, \infty)$, täpsemalt $\left|\mathbb{C}_p^\times\right| = p^{\mathbb{Q}}$ ehk pööratavate p-aadiliste kompleksarvude normide väärtuste hulk on ratsionaalarvude teatud alamhulk.*

Lause 7.42 ([9, peatükk 2.6]). *Korpus $\left(\mathbb{C}_p, |\cdot|_p\right)$ on täielik, kuid ei ole sfääriliselt täielik ehk leidub hulk selliseid üksteisesse sisestatud kerasid, mille ühisosa on tühi hulk.*

Lause 7.43 ([9, peatükk 2.6]). *Korpus $\left(\mathbb{C}_p, |\cdot|_p\right)$ on separaabel ehk selles ei leidu kõikjal tihedat ülimalt loenduvat hulka.*

Lause 7.44 ([9, peatükk 2.6]). *Korpus $\left(\mathbb{C}_p, |\cdot|_p\right)$ ei ole lokaalselt kompaktne.*

8 Ekvivalentsed normid korpusel $\mathbb{Q}$

Oleme näinud, et korpusel $\mathbb{Q}$ on määratud nii p-aadiline norm $|\cdot|_p$ iga algarvu p jaoks, kui ka varasemast tuntud absoluutväärtus $|\cdot|$. Nüüd tõestame, et korpusel $\mathbb{Q}$ teisi norme ei olegi ning $\mathbb{Q}$ ainsad täieldid on $\mathbb{R}$ ja $\mathbb{Q}_p$, kus p on algarv.

Teoreem 8.1 (Ostrowski). *Iga mittetriviaalne norm $\|\cdot\|$ korpusel $\mathbb{Q}$ on ekvivalentne kas absoluutväärtusega või normiga $|\cdot|_p$, kus p on algarv.*

Tõestus. Oletame esiteks, et $\|\cdot\|$ on arhimeediline norm. Lause 2.3 põhjal leidub selline naturaalarv n, et $\|n\| > 1$. Olgu n_0 sellistest naturaalarvudest vähim. Siis on võimalik kirjutada $\|n_0\| = n_0^\alpha$, kus $\alpha = \log_{n_0} \|n_0\|$. Esitame suvalise naturaalarvu n alusel n_0, see tähendab, et viime selle kujule

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_s n_0^s, \tag{8.1}$$

kus $a_i \in \{0, 1, \ldots, n_0 - 1\}$ iga $i = 0, \ldots, s$ korral ja $a_s \neq 0$. Paneme tähele, et s on määratud võrratusega $n_0^s \leq n < n_0^{s+1}$, mis ütleb, et

$$s = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor.$$

Siin $\lfloor x \rfloor$ tähistab arvu x alumist täisosa. Nüüd, võttes võrrandist (8.1) normi, saame, et

$$\begin{aligned} \|n\| &\leq \|a_0\| + \|a_1 n_0\| + \left\|a_2 n_0^2\right\| + \ldots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\| \, n_0^\alpha + \|a_2\| \, n_0^{2\alpha} + \ldots + \|a_s\| \, n_0^{s\alpha}. \end{aligned}$$

Kuna eelduste kohaselt n_0 on vähim selline arv, mille korral $\|n\| > 1$ ja kõik numbrid a_i on sellest väiksemad, siis $\|a_i\| \leq 1$ iga i korral ja seega

$$\begin{aligned}\|n\| &\leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \ldots + n_0^{s\alpha} \\ &\leq n_0^{s\alpha}\left(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \ldots + n_0^{-s\alpha}\right) \\ &\leq n^{\alpha}\left(\sum_{i=1}^{\infty}\left(\frac{1}{n_0^{\alpha}}\right)^{i}\right),\end{aligned}$$

sest võrdusest (8.1) ilmselt järeldub $n \geq n_0^s$. Kuna $n_0^{\alpha} > 1$, siis $0 < \frac{1}{n_0^{\alpha}} < 1$ ja järelikult antud geomeetriline rida koondub mingiks positiivseks konstandiks C. Seega saame kirjutada, et

$$\|n\| \leq Cn^{\alpha} \text{ iga } n = 1, 2, \ldots \text{ korral.}$$

Viies eelneva arutelu läbi n^N ($N \in \mathbb{Z}$) jaoks, saame, et

$$\left\|n^N\right\| \leq Cn^{N\alpha} \Rightarrow \|n\| \leq \sqrt[N]{C}n^{\alpha}.$$

Kui mingi fikseeritud n korral protsessis $N \to \infty$, siis $\sqrt[N]{C} \to 1$ ja seega

$$\|n\| \leq n^{\alpha} \tag{8.2}$$

Tõestame ka vastupidise võrratuse. Kuna

$$n_0^{s+1} > n \geq n_0^s,$$

siis saame, et

$$n_0^{(s+1)\alpha} = \left\|n_0^{s+1}\right\| = \left\|n + n_0^{s+1} - n\right\| \leq \|n\| + \left\|n_0^{s+1} - n\right\|,$$

kust järeldub

$$\|n\| \geq \left\|n_0^{s+1}\right\| - \left\|n_0^{s+1} - n\right\| \geq n_0^{(s+1)\alpha} - \left(n_0^{s+1} - n\right)^{\alpha}.$$

Viimane võrratus kehtib tänu omadusele $\left\|n_0^{s+1}\right\| = \|n_0\|^{s+1}$ ning võrratusele (8.2). Järelikult, kuna $n \geq n_0$ ja $\alpha > 0$, siis

$$\begin{aligned}\|n\| &\geq n_0^{(s+1)\alpha} - \left(n_0^{s+1} - n_0^s\right)^{\alpha} \\ &= n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right] \\ &= C' n_0^{(s+1)\alpha} \geq C' n^{\alpha},\end{aligned}$$

kus C' on jällegi mingi arvust n sõltumatu konstant. Nagu eelnevaltki kasutame seda

võrratust n^N jaoks, võtame N-nda juure ja leiame piirväärtuse. Tulemuseks ongi

$$\|n\| \geq n^{\alpha}.$$

Seega on võimalik vaid, et $\|n\| = n^{\alpha}$ iga $n \in \mathbb{N}$ korral. Lause 1.3. omadusest (e) järeldub, et $\|x\| = |x|^{\alpha}$ iga $x \in \mathbb{Q}$ korral. Lause 1.10. kohaselt tähendabki see aga seda, et selline norm on ekvivalentne normiga $|\cdot|$.

Nüüd oletame, et $\|\cdot\|$ on mittearhimeediline ehk lause 2.3 väide (c) tõttu$\|n\| \leq 1$ kõikide $n \in \mathbb{N}$ korral. Kuna eeldasime, et $\|\cdot\|$ on mittetriviaalne, siis saame leida vähemalt ühe arvu n omadusega $\|n\| < 1$. Olgu p nendest arvudest vähim. Paneme tähele, et p peab olema algarv, sest kui oletada, et $p = n_1 n_2$, kus $n_1, n_2 < p$, siis $\|p\| = \|n_1\| \|n_2\| = 1$, mis oleks vastuolus arvu p valikuga.

Olgu n suvaline naturaalarv ja näitame, et kui p ei jaga seda, siis $\|n\| = 1$. Kirjutame $n = rp + s$, kus $0 < s < p$, saame seda sellisel kujul kirjutada, sest eeldasime, et p seda arvu ei jaga. Tänu arvu p minimaalsusele $\|s\| = 1$. Samuti teame, et $\|rp\| < 1$, sest $\|p\| < 1$ ja tänu lause 2.3 väitele (c) $\|r\| \leq 1$. Siit saame, et

$$\|n - s\| < 1 = \|s\|.$$

Lause 2.4. tõttu $\|n\| = \|s\| = 1$. Lõpuks, lause 4.10 tõttu on iga arvu $n \in \mathbb{Z}$ on võimalik kirjutada kujul $n = p^v n'$, kus p ei jaga arvu n' Seega $|n|_p = (1/p)^v$ ja

$$\|n\| = \|p\|^v \left\|n'\right\| = \|p\|^v.$$

Olgu $\rho = \|p\| < 1$. Siis $\rho = \left(\frac{1}{p}\right)^{\alpha}$ mingi reaalarvu $\alpha > 0$ korral ning järelikult

$$\|n\| = \|p\|^v = \left\|\frac{1}{p}\right\|^{\alpha v} = \left(\left\|\frac{1}{p}\right\|^v\right)^{\alpha} = |n|_p^{\alpha}.$$

Lause 1.3 omadusest (a) ja (e) järeldub, et see valem kehtib ka suvalise nullist erineva ratsionaalarvu x jaoks. Lause 1.10. kohaselt saamegi, et

$$\|x\| = \|x\|_p^a \ \forall x \in \mathbb{Q},$$

et $\|\cdot\| \sim |\cdot|_p$. □

Lause 8.2. *Tähistame* $\mathbb{Q}^{\times} = \mathbb{Q}/\{0\}$. *Iga* $x \in \mathbb{Q}^{\times}$ *jaoks kehtib valem*

$$\prod_{p \in \mathbb{P}} |x|_p \cdot |x| = 1.$$

Tõestus. On piisav näidata, et see valem kehtib juhul, kui x on positiivne täisarv, ülejäänud juhtude kehtivus järeldub normide korrutamise ja jagamise omadusest. Seega, olgu $x = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Siis $|x|_q = 1$, kui $q \neq p_i$, $|x|_q = \frac{1}{p_i^{a_i}}$, kui $q = p_i$ ja $|x| = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$.

Järelikult

$$\prod_{p\leq\infty}|x|_p=|x|_{p_1}|x|_{p_2}\ldots|x|_{p_k}|x|=\frac{1}{p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}}\cdot p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}=1$$

□

Viimasel lausel on kasulikke rakendusi algebralises geomeetrias. Näiteks, kui kõikide normide väärtused peale ühe on teada, siis selle teoreemi abil saab puuduva väärtuse leida.

Eeldame, et meil on mingi ratsionaalarvuliste kordajatega polünoomil $F(x)$ korpuses $\mathbb{Q}$ juured, siis leiduvad need juured ka korpustes $\mathbb{R}$ ja $\mathbb{Q}_p$ iga algarvu p korral. Saame teha lihtsa järelduse, et kui polünoomil $F(x)$ ei leidu korpuses $\mathbb{Q}_p$ juuri, siis ei leidu sellel ka ratsionaalarvulisi juuri, sest korpus $\mathbb{Q}$ on korpuse $\mathbb{Q}_p$ alamkorpus. Enamasti vastupidist järeldust teha ei saa, st kui polünoomil $F(x)$ leidub korpuses $\mathbb{Q}_p$ juuri, siis sellest ei saa järeldada, et sellel leidub ka juuri korpuses $\mathbb{Q}$. Kuid on mõned erijuhud, kus ka sedapidi järeldust on võimalik teha.

Lause 8.3. *Arv $x\in\mathbb{Q}$ on mingi arvu $a\in\mathbb{Q}$ ruut parajasti siis, kui see on mingi arvu $b\in\mathbb{Q}_p$ ruut iga $\mathbb{Q}_p$ korral.*

Tõestus. Eeldame esiteks, et arv $x=a^2\in\mathbb{Q}$. Siis, kuna $\mathbb{Q}$ on $\mathbb{Q}_p$ alamkorpus, kuulub arv a ka hulka $\mathbb{Q}_p$ iga algarvu p korral, st $x=a^2\in\mathbb{Q}_p$.

Eeldame nüüd, et arv x on mingi arvu $b\in\mathbb{Q}_p$ ruut iga p korral. Siis saame lause 4.10 kohaselt kirjutada arvu x kujul $x=p^{\mathrm{ord}_p x}u=b^2=\left(p^{\mathrm{ord}_p b}v\right)^2$, kus $u,v\in\mathbb{Z}_p^\times$. Kasutades p-aadilise normi omadusi leiame, et

$$\left(\frac{1}{p}\right)^{\mathrm{ord}_p x}=|x|_p=\left|b^2\right|_p=\left|p^{\mathrm{ord}_p b}v\right|_p^2=\left|p^{\mathrm{ord}_p b}\right|_p^2|v|_p^2=\left(\frac{1}{p^{\mathrm{ord}_p b}}\right)^2=\left(\frac{1}{p}\right)^{2\mathrm{ord}_p b}$$

ehk $\mathrm{ord}_p x$ on paarisarv. Seega on arv x kujul $p^{2l}v^2$, kus l on mingi täisarv, $p\nmid v$. Lahutades arvu x algteguriteks, saame, et

$$x=\prod_{p<\infty}p_i^{k_i}=\prod_{p<\infty}p_i^{\mathrm{ord}_p x}=\prod_{p<\infty}p_i^{2l_i}=\left(\prod_{p<\infty}p_i^{l_i}\right)^2\in\mathbb{Q}.$$

□

9 Hulgad $\mathbb{Q}_g$, kus g ei ole algarv

Et vaadelda hulki $\mathbb{Q}_g$, kus g ei ole algarv, peame normi $|\cdot|_g$ ja kujutuse $\mathrm{ord}_g(x)$ uuesti defineerima. Kui $x\in\mathbb{Z}$, siis $\mathrm{ord}_g(x)$ võrdub ikka suurima arvu g astmega, mis arvu x jagab. Kuid selleks, et defineerida $\mathrm{ord}_g(x)$ juhul $x=\frac{a}{b}$, kus $a,b\in\mathbb{Z}$, vajame järgmist lemmat.

Lemma 9.1. *Olgu $x = \frac{a}{b}, a, b \in \mathbb{Z}$ ja $(a,b) = 1$, kus (a,b) tähistab arvude a ja b suurimat ühistegurit. Siis leiduvad selline täisarv v ja täisarvude paar a' ja b' nii, et $\frac{a}{b} = g^v \frac{a'}{b'}, g \nmid a'$ ja $(a', b') = (g, b') = 1$.*

Tõestus. Juhul, kui $g \nmid a$ ja $(g,b) = 1$, siis saame valida $v = 0$, $a = a'$, $b = b'$ ja lemma ilmselt kehtib.

Kui $g|a$, siis tähistame $v = n \geq 1$ kui suurim arvu g aste, mis jagab arvu a. Valime $a' = ag^{-n}$ ja $b' = b$. Sellised juhul $g \nmid a'$. Kuna $(a, b') = 1$ ja $g|a$ ehk arvu g algteguriteks saavad olla ainult arvu a algtegurid, siis järelikult $(g, b') = 1$. Samuti, kuna $(a,b) = 1$, siis $(a', b') = 1$ ning

$$\frac{a}{b} = g^n \frac{a'}{b'}.$$

Viimaseks vaatleme juhtu, kus $g \nmid a$ ja $(g,b) > 1$. Siis saame arvu b lahutada teguriteks $b = b_1 b_2$ nii, et kõik arvu b_1 algtegurid jagavad arvu g ja arvul b_2 puuduvad arvuga g ühised algtegurid ehk $(b_2, g) = 1$. Sarnaselt saame arvu g jagada teguriteks $g_1 g_2$ nii, et g_1 kõik algtegurid jagavad arvu b_1 aga $(g_2, b_1) = (g_2, b) = 1$. Lisaks on võimalik leida vähim selline naturaalarv $m = -v$, mille korral $b_1 | g^m$ ja seega ka $b_1 | g_1^m$, sest arvudel $b_1$ja g_1 on samad algtegurid. Võrduses

$$g^m \frac{a}{b} = \frac{g_1^m g_2^m}{b_1 b_2} a$$

on arv $u = \frac{g_1^m}{b_1}$ täisarv. Seega, kui me valime $a' = \frac{g_1^m g_2^m}{b_1} a$ ja $b' = b_2$, siis saame, et

$$\frac{a}{b} = g^{-m} \frac{g_1^m g_2^m}{b_1 b_2} a = g^{-m} \frac{a'}{b'},$$

Paneme tähele, et $g \nmid a'$, sest $g \nmid a$, $(g, b') = (g, b_2) = 1$ ning $(a', b') = 1$, sest eelduste kohaselt $(g, b_2) = 1$, m on vähim selline naturaalarvu, mille korral $b_1 | g_1^m$. ning eelevalt leitsime, et $(b_2, g) = 1$. □

Kui $x = \frac{a}{b}$, siis olgu $\mathrm{ord}_g(x)$ eelmises lemmas saadud arvu v ja defineerime g-aadilise normi järgmiselt:

$$|x|_g = \left|\frac{a}{b}\right|_g = g^{-v}.$$

Näide 9.2. Leiame arvu $\frac{4}{23}$ 8-aadilise normi ehk

$$\left|\frac{128}{23}\right|_8.$$

Antud juhul $8|128$ ning suurim arvu 8 aste, mis seda jagab on 2. Järelikult

$$\left|\frac{128}{23}\right|_8 = \left|8^2 \cdot \frac{2}{23}\right|_8 = 8^{-2}.$$

Näide 9.3. Leiame arvu $\frac{7}{300}$ 10-aadilise normi ehk arv

$$\left|\frac{7}{104}\right|_{24}.$$

Paneme tähele, et $(24, 104) = 8$. Jagame arvud $g = 24$ ja $b = 104$ eelmises lauses toodud meetodil teguriteks saades

$$b_1 = 8,\ b_2 = 13$$

ja

$$g_1 = 8,\ g_2 = 3.$$

Antud juhul on 1 vähim naturaalarv m, mille korral $b_1 = 8^m | 24$. Järelikult $a' = \frac{24}{8} \cdot 7 = 21$, $b' = 13$ ning seega

$$\left|\frac{7}{104}\right|_{24} = \left|24^{-1}\frac{21}{13}\right|_{24} = 24^1.$$

Märkus 9.4. Sellise normi korral ei kehti enam normide korrutamise aksioom. Näiteks

$$\left|\frac{1}{675}\right|_{15} = 15^3, \left|\frac{1}{33750}\right|_{15} = 15^4 \text{ aga } \left|\frac{1}{675 \cdot 33750}\right|_{15} = 15^6 < 15^3 \cdot 15^4.$$

Üldiselt, kui g ei ole algarv, siis

$$|ab|_g \leq |a|_g |b|_g .$$

ja $|\cdot|_g$ ei ole norm.

Definitsioon 9.5. Kujutisi mis rahuldavad esimest ja kolmast normi aksioomi, kuid ei rahulda teist ehk korrutamise aksioomi, nimetatakse *pseudonormideks.*

Lause 9.6. *Kui g ei ole algarv, siis on $|\cdot|_g$ pseudonorm.*

Tõestus. Olgu g mingi naturaalarv, mis ei ole algarv. Siis saame g lahti kirjutada mingite algarvude korrutisena $g = g_1^{a_2} g_2^{a_2} \dots g_k^{a_k}$. Olgu $a = g_1^{a_2} g_2^{a_2} \dots g_{k-1}^{a_{k-1}}$ ja $b = g_k^{a_k}$. Paneme tähele, et $|a|_g = \left|g_1^{a_2} g_2^{a_2} \dots g_{k-1}^{a_{k-1}}\right|_g = 1$ ja $|b|_g = \left|g_k^{a_k}\right|_g = 1$ aga

$$|ab|_g = |g|_g = g^{-1} < 1 = |a|_g \cdot |b|_g .$$

□

Kuigi $|\cdot|_g$ on pseudonorm on $d(x, y) = |x - y|_g$ siiski kaugus ning me võime hulga $\mathbb{Q}$ selle kauguse järgi täielikustada hulgaks $\mathbb{Q}_g$, mida kutsutakse *g-aadiliste arvude ringks.* g-aadiliste arvude kanoonilised saab definieerida sarnaselt p-aadiliste arvude kanoonilisele kujule, st, g-aadilise arvu *a kanooniliseks kujuks* on

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

Teoreem 9.7 ([2, Teoreem 4.5.]). *Kui arvud $n_1, \ldots, n_k \in \mathbb{N}$ on paarikaupa ühiseguriteta ja $n = n_1 \ldots n_k$, siis jäägiklassiringid $\mathbb{Z}/n\mathbb{Z}$ ja $\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_kZ$ on omavahel isomorfsed.*

Lause 9.8. *Kui kordarvul g on vähemalt kaks erinevat algtegurit, siis $\mathbb{Q}_g$ ei ole korpus.*

Tõestus. Olgu g selline kordarv, millel on vähemalt kaks erinevat algtegurit $p_1$ja p_2. Paneme tähele, et ring $\mathbb{Q}_g$ ei saa olla korpus kui see sisaldab mittetriviaalseid idempotente, st selliseid nullist ja ühest erinevaid elemente $a \in \mathbb{Q}_g$, et $a^2 = a$. Tõepoolest, sellisel juhul

$$0 = a^2 - a = a\,(1 - a)$$

ehk arvud a ja $1-a$ on nullitegurid. Seega piisab teoreemi tõestuseks näidata, et ringis $\mathbb{Q}_g$ leidub mittetriviaalseid idempotente. Oletame lihtsuse mõttes, et $g = p_1p_2$, sama arutelu võib läbi viia mistahes kordarvu g jaoks, millel on vähemalt kaks erinevat algtegurit. Proovime leida sellise arvu a, mis on ringis $\mathbb{Q}_g$ mittetriviaalne idempotent. Olgu

$$a = \sum_{n=0}^{\infty} a_n g^n$$

otsitava g-aadilise arvu a kanooniline kuju. Kui a on mittetriviaalne idempotent, siis peab esiteks kehtima

$$a_0 \equiv a_0^2 \pmod{g}, \tag{9.1}$$

Kuna $g = p_1p_2$ ei ole algarv, siis teoreemi 9.7. kohaselt $\mathbb{Z}/g\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2Z$. Kuna näiteks $(0,1) \in \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2Z$ on mittetriviaalne idempotent, siis leidub selline element ka hulgas $\mathbb{Z}/g\mathbb{Z}$. Seega on olemas number $a_0 \in \{1, 2, \ldots, g-1\}$, mis rahuldab võrrandit (9.1) tõesti leidub. Numbri a_1 leidmiseks peame lahendama võrrandi

$$a_0 + a_1 g \equiv a_1' \equiv \left(a_1'\right)^2 \equiv (a_0 + a_1 g)^2 \pmod{g^2}.$$

Kuna g^2 omab samuti erinevaid algtegureid, siis teoreemi 9.7. kasutades on number a_1' võimalik taas kord leida. Lahendades võrrandi

$$a_1' \equiv a_0 + a_1 g \pmod{g^2} \tag{9.2}$$

Kuna $a_1' - a_0 \equiv a_1 g \pmod{g^2}$ siis arv g jagab arvu $a_1' - a_0$ ning saame selle võrrandi viia kujule

$$a_1 \equiv \frac{a_1' - a_0}{g} \pmod{g^2}.$$

Paneme tähele, et leitav number $a_1$kuulub hulka $\mathbb{Z}/g\mathbb{Z}$ ning seega $a_1 < g$ nagu soovitud. Seda protsessi lõpmatult jätkates on meil võimalik leida kõik arvu a numbrid, kusjuures iga n on korral

$$a \equiv a_0 + a_1 p + \ldots + a_n p^n \equiv (a_0 + a_1 p + \ldots + a_n p^n)^2 \equiv a^2 \pmod{g^n}.$$

Järelikult

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \sum_{i=0}^{n} a_i g^i = a,$$

kuna mistahes $\varepsilon > 0$ korral on alati võimalik leida selline indeks N nii, et iga $n \geq N$ korral

$$\left|a^2 - a\right|_g < \frac{1}{g^n} \to 0.$$

Kuna ka g-aadilise normi väärtuste hulga ainus kuhujumispunkt on 0 siis järeldub sellest, et $a^2 = a$ ehk meil on tõesti võimalik leida selline element a ringist $\mathbb{Q}_g$, mis on mittetrviaalne idempotent. □

Näide 9.9. Leiame ringis $\mathbb{Q}_6$ mõne idempotentse elemendi. Olgu selle elemendi arvu kanooniline kuju $a = \ldots a_2 a_1 a_0$. Leiame esiteks numbrikoha a_0. Teame, et peab kehtima

$$a_0 \equiv a_0^2 \pmod 6$$

Kuna $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2Z$, siis idempotente leidub. Valime selleks elemendi $(0, 1)$ ehk peab kehtima

$$a_0^2 \equiv 0 \pmod 3$$

ja

$$a_0^2 \equiv 1 \pmod 2.$$

Selleks, et mõlemad kongruentsid korraga kehtiksid peab olema $a_0 = 3$ ning tõepoolest

$$3 \equiv 9 \pmod 6.$$

Nüüd leiame numbrikoha a_1. Selleks peame eelneva teoreemi põhjal lahendama kongruentsi

$$3 + a_1 \cdot 6 \equiv a_1' \equiv \left(a_1'\right)^2 \equiv (3 + a_1 \cdot 6)^2 \pmod{36}.$$

Selle lahendades saame tulemuseks, et $a_1' = 9$. Lahendades nüüd kongruentsi $3 + a_1 6 \equiv 9 \pmod{36}$ näeme, et $a_1 = 1$. Leiame järgmiseks numbrikoha a_2 ehk lahendame kongruentsi

$$3 + 1 \cdot 3 + a_2 \cdot 36 = a_2' \equiv \left(a_2'\right)^2 = (3 + 1 \cdot 3 + a_2 \cdot 36)^2 \pmod{216}.$$

Sealt saame, et $a_2' = 81$ ja $a_2 = 2$. Seda protsessi jätkates on võimalik leida kõik a numbrikohad ning $a = \ldots 213$.

Arvutamise ringis $\mathbb{Q}_g$ saab ruuduvaba g korral taandada p-aadiliste arvutamisele järgmise lause abil.

Teoreem 9.10 ([7, Teoreem 1.9.2.]). *Kui $g = p_1 p_2 \ldots p_k$ on erinevate algarvude korrutis, siis ring $\mathbb{Q}_g \cong \mathbb{Q}_{p_1} \oplus \mathbb{Q}_{p_2} \oplus \ldots \oplus \mathbb{Q}_{p_k}$ on erinevate p-aadiliste korpuste otsesumma.*

Kasutatud kirjandus

[1] **Kilp, M.** Algebra I. Eesti Matemaatika Selts, 2005.

[2] **Laan, V., Tart, L.** Arvuteooria. Loengukonspekt, Tartu Ülikool, 2016. http://courses.ms.ut.ee/2017/arvuteooria/spring/uploads/Main/arv14.pdf, viimati vaadatud 08.05.2017.

[3] **Lidl, R., Niederreiter, H.** Finite Fields. Second edition, Cambridge University Press, 2008.

[4] **Gouvêa, Q. F.** p-adic Numbers: An Introduction. Second edition, Springer, 2003.

[5] **Conrad, K.** Hensel's lemma. Elektroonilised märkmed. http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf, viimati vaadatud 08.05.2017

[6] **Conrad, K.** The p-adic expansion of rational numbers. Elektroonilised märkmed. http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/rationalsinQp.pdf, viimati vaadatud 08.05.2017

[7] **Katok, S.** p-adic Analysis Compared with Real. American Matematical Society, 2007.

[8] **Dragovich, B., Khernnikov, A. Yu., Kozyrev, V. S., Volovich, V. I.** *p-Adic Numbers, Ultrametric Anal. and Appli.* 1(1), 1–17 (2008).

[9] **Toivo, L.** Sissejuhatus mittearhimeedilisse funktsionaalanalüüsi. Tartu Ülikool, 2011.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kristiina Mähar,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "p-aadilised arvud", mille juhendaja on Lauri Tart,

    1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

    1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile;

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartu, 11. mai 2017