p-adski brojevi i algebarska proširenja

Šakić, Tina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Tina Šakić

p-ADSKI BROJEVI I ALGEBARSKA PROŠIRENJA

Diplomski rad

Voditelj rada:
doc.dr.sc. Igor Ciganović

Zagreb, rujan, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj rad nastao je iz moje silne želje da barem mali dio studiranja posvetim teorijskoj matematici.

Zahvaljujem se svim ljudima koji su me podržavali tokom cijelog mojeg obrazovanja.

Zahvaljujem se i svim prijateljima, kolegama i profesorima.

Također, hvala mom mentoru ovog diplomskog rada, doc.dr.sc. Igoru Ciganoviću na susretljivosti i spremnom odgovoru na sva moja pitanja.

Iskreno se zahvaljujem nekima od svojih srednjoškolskih profesora; profesoru fizike Saši Celiću, sjajnim profesoricama matematike Aleksandri Floreani i Zlati Korpar te profesoru filozofije Željku Rogini. Posebno ističem svog razrednika i profesora hrvatskog jezika, Davora Tanockog. Profesor Tanocki svojim osebujnim, iznimno kreativnim i nekonvencionalnim načinom predavanja gradi generacije mladih intelektualaca.

Za kraj, najveća hvala mojoj obitelji - mami Snježani, tati Milenku i bratu Mati kojima posvećujem ovaj diplomski rad.

Sadržaj

Uvod

Ovaj ćemo rad započeti proučavajući svojstva skupa formalnih redova $\{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, ..p-1\}, i \in \mathbb{N}_0\}$, gdje je p fiksan prost broj. Elemente toga skupa nazivat ćemo p-adskim cijelim brojevima. U prvom ćemo poglavlju proučavati neka osnovna svojstva toga skupa, kao što je kardinalnost. Od posebnog će nam interesa biti rezultat da uz prikladnu definiciju zbrajanja + taj skup postaje komutativna grupa. Tada ćemo skup p-adskih cijelih brojeva početi označavati sa $\mathbb{Z}_p$. Nakon toga ćemo demonstrirati i postupak množenja $\cdot$. Pokazat ćemo da tada $(\mathbb{Z}_p, +, \cdot)$ postaje komutativni prsten. Ispitat ćemo neka standardna svojstva od $\mathbb{Z}_p$ kao prstena. Konkretno, pokazat ćemo da je $\mathbb{Z}_p$ domena glavnih ideala te vidjeti koji su to ideali.Također ćemo dati karakterizaciju skupa svih invertibilnih elemenata od $\mathbb{Z}_p$ u oznaci $\mathbb{Z}_p^{\times}$. Kroz prvo ćemo se poglavlje također podsjetiti osnovih definicija i rezultata iz područja algebarskih struktura koji su važni za ovaj rad. Vidjet ćemo nekoliko primjera p-adskih brojeva za konkretni prost broj p.
Nakon što promotrimo $\mathbb{Z}_p$ kao grupu i prsten, uvidjet ćemo da na tom skupu možemo i definirati metriku d te ćemo se ukratko prisjetiti tzv. *aksioma* metrike. Nakon toga ćemo vidjeti da je $\mathbb{Z}_p$ topološka grupa i topološki prsten, uz topologiju induciranu metrikom d. Budući da je $\mathbb{Z}_p$ integralna domena, moguće je definirati polje razlomaka tog prstena, kojeg ćemo označavati sa $\mathbb{Q}_p$ i svojstva toga polja proučavat ćemo u *Poglavlju 2*. Elemente toga polja jednostavno ćemo zvati p-adskim brojevima. Dat ćemo nekoliko jednostavnih karakterizacija toga polja. Proširit ćemo definiciju metrike d iz *Poglavlja 1.* na $\mathbb{Q}_p$ na vrlo prirodan i intuitivan način. Usporedit ćemo udaljenosti nekih brojeva u standardnoj, *Euklidskoj metrici* te u metrikama vezanim za $\mathbb{Q}_p$. Pokazat ćemo da metrika d zadovoljava svojstvo ultrametrike, tj. da

$$d(x, z) \leq max\{d(x, y), d(y, z)\} \forall x, y, z \in \mathbb{Q}_p.$$

Skup p-adskih brojeva prvi je opisao njemački matematičar Kurt Hensel (1861. - 1941.). Kurt Hensel prvi je put došao do pojma p-adskoga broja 1897. godine, stoga možemo zaključiti da su p-adski brojevi relativno nov, ali ništa manje zanimljiv pojam u matematici. Po Kurtu Henselu nazvana je jedna od fundamentalnih tvrdnji vezana za p-adske brojeve, tzv. *Henselova lema*. Tom ćemo se tvrdnjom baviti u *Poglavlju 3.* gdje ćemo je iskazati

i dokazati. *Henselova lema* govori o postojanju rješenja jednadžbe $P(x) = 0$ za $x \in \mathbb{Z}_p$ i polinom $P \in \mathbb{Z}_p[x]$. Vidjet ćemo da je tvrdnja *Henselove leme* usko vezana za vrlo često korištenu *Newtonovu metodu* aproksimacije nultočki derivabilne funkcije f.
Ukratko, *Henselova lema* nam govori da ukoliko krenemo od neke početne aproksimacije $x_0 \in \mathbb{Z}_p$ t.d. $P(x) \equiv 0\ (mod p^n)$ za neki $n \in \mathbb{N}$, možemo doći do jedinstvenog rješenja $x \in \mathbb{Z}_p$ ako su zadovoljeni određeni uvjeti. Na kraju ćemo vidjeti da su posljedice *Henselove leme* kvadratna proširenja od $\mathbb{Q}_p$. Koristeći *Henselovu lemu*, pokazat ćemo da neki polinomi nemaju rješenja u $\mathbb{Q}_p$, dok ćemo za neke polinome na jednostavan način doći do rješenja u $\mathbb{Q}_p$. U zadnjem poglavlju ovoga rada, promatrat ćemo algebarska proširenja p-adskih brojeva. Upoznat ćemo se s pojmom ultrametričkoga polja te vidjeti da je $\mathbb{Q}_p$ ultrametričko polje zajedno s apsolutnom vrijednošću koja inducira ultrametriku d iz *Poglavlja 2* . Također ćemo iskazati teorem Ostrowskog, poznati teorem u teoriji brojeva. Kratko ćemo se dotaći konačnih Galoisovih proširenja i vidjeti primjer konačnog Galoisovog proširenja od $\mathbb{Q}_3$. Napomenimo da se u ovom radu za teorijske rezultate i njihove dokaze oslanjamo na [3].

Poglavlje 1

Osnovna svojstva prstena $\mathbb{Z}_p$

Neka je p fiksan prost broj. U ovomu ćemo poglavlju promatrati skup formalnih redova $X = X_p = \{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, ..p-1\}, i \in \mathbb{N}_0\}$. Elemente ovog skupa zvat ćemo p-adski cijeli brojevi. Osnovni ciljevi ovog poglavlja jesu promotriti X_p u kontekstu teorije skupova, pokušati ga opisati kao algebarsku strukturu te definirati metriku na tom skupu kako bismo dobili metrički prostor. Krenut ćemo iz perspektive teorije skupova, odnosno htjet ćemo odrediti kardinalnost tog skupa i definirati relaciju jednakosti između dvaju elemenata tog skupa. Nakon toga ćemo prijeći na opis skupa p-adskih cijelih brojeva u terminima algebarskih struktura. Tada ćemo taj skup početi označavati sa $\mathbb{Z}_p$. Kroz primjer ćemo demonstrirati (pogodan) način zbrajanja i množenja uz koje je $(\mathbb{Z}_p, +)$ postaje Abelova grupa, a $(\mathbb{Z}_p, +, \cdot)$ komutativni prsten. Pokazat ćemo neka osnovna svojstva od $\mathbb{Z}_p$ kao grupe i prstena. Definirat ćemo fukncju $d : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}$ koja će zadovoljavati svojstva metrike, odnosno $(\mathbb{Z}_p, d)$ ćemo moći promatrati i kao metrički prostor. Budući da svaka metrika inducira topologiju, vidjet ćemo i neka topološka svojstva od $\mathbb{Z}_p$. U ovom ćemo dijelu također vidjeti i neke primjere p-adskih brojeva za neke konkretne proste brojeve p.

1.1 Skup p-adskih cijelih brojeva

Definicija 1.1.1. *Neka je p prost broj. Formalni red $\sum_{i=0}^{\infty} a_i p^i$, gdje su $a_i \in \{0, 1, ..., p-1\}$ $\forall i \in \mathbb{N}_0$ zovemo p-adskim cijelim brojem.*

Uočimo, p-adski cijeli broj možemo identificirati nizom njegovih koeficijenata $(a_i)_{i \geq 0}$. Nadalje, uočimo također da X_p možemo promatrati kao Kartezijev produkt $X = X_p = \prod_{i=0}^{\infty} \{0, 1, \dots, p-1\} = \{0, 1, \dots\ p-1\}^{\mathbb{N}_0}$

Propozicija 1.1.2. *X_p je neprebrojiv.*

Dokaz. Lako se vidi da vrijedi $X_p = \{f | f : \mathbb{N}_0 \to \{0, 1, \dots p-1\}\}$.
Ako sa $k(X)$ označimo kardinalnost skupa X znamo da vrijedi
$k(X_p) = k(\{0, 1, \dots p-1\}^{k(\mathbb{N}_0)} = p^{\aleph_0}$.
Iz

$$c = 2^{\aleph_0} \leq p^{\aleph_0} \leq {\aleph_0}^{\aleph_0} = c,$$

zaključujemo da je skup svih p-adskih cijelih brojeva neprebrojiv. □

Pogledajmo sada nekoliko konkretnih primjera p-adskih cijelih brojeva.

Primjer 1.1.3. *U sljedećim je primjerima broj a raspisan kao p-adski cijeli broj, tj $a = \sum_{i=0}^{\infty} a_i p^i$.*

a) $1 = 1p^0 + 0p^1 + 0p^2 + ...$ 1 *kao p-adski broj za općenit prost broj p*
b) $23 = 3 \cdot 5^0 + 4 \cdot 5^1 + 0 \cdot 5^2 + ...$ 23 *kao 5-adski broj*
c) Za svaki prirodni broj $n \in \mathbb{N}$ jasno je da je raspis kao p-adski broj zapravo identičan raspisu u bazi p i da je taj zapis konačan.

1.2 Prsten $\mathbb{Z}_p$

U ovomu ćemo odjeljku kroz primjere pokušati ilustrirati na koji način ćemo zbrajati i množiti p-adske cijele brojeve kako bi $(X_p, +)$ postao Abelova grupa, a $(X_p, +, \cdot)$ prsten te proučiti svojstva od X_p kao grupe, tj. prstena.

Dva p-adska cijela broja, $a = \sum_{i=0}^{n} a_i p^i$ i $b = \sum_{i=0}^{n} b_i p^i$ zbrajat ćemo po komponentama. Cilj nam je da koeficijenti dobivenog zbroja ostanu u rasponu $\{0, 1, \dots, p-1\}$. Prvi koeficijent zbroja bit će jednak $a_0 + b_0$ ako je $a_0 + b_0 < p$, a inače će iznositi $a_0 + b_0 - p$. U oba slučaja smo osigurali da je prvi koeficijent zbroja u dopustivom rasponu. U drugom ćemo slučaju prenijeti ostatak od p na sljedeći koeficijent i nastaviti sa zbrajanjem na isti način. Iz ovakvog načina zbrajanja vidimo da vrijedi

$$(a+b)_n = (\sum_{i=0}^{n} a_i p^i + \sum_{i=0}^{n} b_i p^i)_n, \ n \in \mathbb{N}_0,$$

gdje $(a+b)_n$ predstavlja n-ti koeficijent pri zbrajanju za $n \in \mathbb{N}_0$.

Ilustrirajmo sada na konkretnim primjerima gornje opisan postupak zbrajanja dva p-adska cijela broja.

Primjer 1.2.1. *a) Za fiksan broj p zbrojimo brojeve* $a = 1 = 1p^0 + 0p^1 + 0p^2 + \ldots$ *i* $b = \sum_{i=0}^{\infty}(p-1)p^i$. *Stavimo* $c = \sum_{i=0}^{\infty} c_i p^i = a + b$.
Pogledajmo zbroj prvih komponenti brojeva a i b, vrijedi $a_0 + b_0 = 1 + (p-1) = p$. *Međutim p nije u rasponu* $\{0, 1, \ldots, p-1\}$. *No, možemo reći da zbrojeći ove dvije komponente, imamo "nula p-ova na nultu i jedan p na prvu". Točno ćemo tako i nastaviti proceduru zbrajanja.*
Stavimo $c_0 = 0$ *i "zapamtimo jedan p na prvu" koji nam je ostao te ga pribrajamo sljedećoj komponenti.*
Pogledajmo sada zbroj $a_1 + b_1 = 0 + (p-1) = p - 1$. *Uz član p sada ćemo imati* $(p-1)+1$ *koji smo zapamtili. Kao i u prethodnoj opservaciji, opet možemo zaključiti da "imamo nula p-ova i prvu i jedan p na drugu". Analogno nastavimo dalje i zaključujemo da vrijedi* $1 + b = 0$, *odnosno da će nam sve komponente pri zbrajanju iščeznuti. Pišemo* $b = -1$.
Primijetimo sada da je za $p = 7$ *broj* -1 *ima zapis* $6666666..._7$, *dok broj* -1 *kao* 5*-adski broj ima zapis* $4444444..._5$.

b) Zbrojimo brojeve 123 *i* 44 *kao* 7*-adske brojeve. Vrijedi:*

$$123 = 4 \cdot 7^0 + 3 \cdot 7^1 + 2 \cdot 7^2$$

$$44 = 2 \cdot 7^0 + 6 \cdot 7^1$$

Sada ponavljamo postupak iz dijela a).
Zbrojimo članove uz 7^0. $0 \leq 4 + 2 = 6 < 7$, *tj. prvi koeficijent u dopustivom je rasponu.*
Zbrajajući druge komponente, imamo: $0 \leq 3 + 6 = 9 > 7$.
Vrijedi: $9 \cdot 7^1 = (2+7) \cdot 7^1 = 2 \cdot 7^1 + 1 \cdot 7^2$. *Dakle, "prenosimo" 1. Na kraju, uz treći član ćemo imati* $2 + 0 + 1 = 3$ *što je u dopustivom rasponu.*
Dakle, $123 + 44 = 6 \cdot 7^0 + 2 \cdot 7^1 + 3 \cdot 7^2 = 623_7$.

Prisjetimo se sada nekih osnovnih pojmova iz kolegija *Algebarske strukture* koji su od fundamentalnog značaja za ovaj rad. Svi pojmovi mogu se pronaći u [2], [3] i [4].

Definicija 1.2.2. *Neka je G neprazan skup i* $\cdot : G \times G \to G$. *Uređeni par* $(G, \cdot)$ *zovemo grupom ako vrijede sljedeća svojstva:*

$(G1)$	$(x \cdot y) \cdot z = x \cdot (y \cdot z),\ \forall x, y, z \in G$	*(asocijativnost)*
$(G2)$	$(\exists e) \in G\ \ x \cdot e = e \cdot x = x,\ \forall x \in G$	*(postojanje neutrala)*
$(G3)$	$(\forall x \in G)(\exists x^{-1} \in G)\ x \cdot x^{-1} = x^{-1} \cdot x = e$	*(postojanje inverza)*

Ako još k tome vrijedi i $x \cdot y = y \cdot x\ \ \forall x, y \in G$, tada kažemo da je $(G, \cdot)$ komutativna, odnosno Abelova grupa. Inače za G kažemo da je nekomutativna grupa.

Napomena 1.2.3. *Ako imamo neprazan skup G i operaciju $\cdot : G \times G \to G$ tj. $\forall x, y \in G$ $x \cdot y \in G$ tada ćemo $(G, \cdot)$ zvati grupoidom. Za grupoid u kojem vrijedi i svojstvo asocijativnosti reći ćemo da je polugrupa. Polugrupu u kojoj postoji neutralni element zvat ćemo monoidom. Jasno, za monoid u kojem za svaki element postoji njemu inverzan vrijedi da je grupa*

Definicija 1.2.4. *Neka je X skup i $\sigma : X \to X$ funkcija na tom skupu. Za σ kažemo da je involucija ako vrijedi $\sigma \circ \sigma = id$, odnosno $\forall x \in X$vrijedi $\sigma(\sigma(x)) = x$.*

Vratimo se *Primjeru 1.2.1*. Uočimo, $1 + b = 0$, tj. b je aditivni inverz od 1.
Definirajmo preslikavanje $\sigma : X_p \to X_p$ kao

$$\sigma(a) = \sum_{i=0}^{\infty} (p - 1 - a_i)p^i \tag{1.1}$$

Lako se vidi da je σ dobro definirana jer $\forall i$ vrijedi $0 \leq p - 1 - a_i \leq p - 1$.
Također, vrijedi da je $a + \sigma(a) + 1 = 0$, odnosno $\sigma(a) + 1$ aditivni je inverz p-adskog broja a. Iz gornje relacije lako vidimo da je funkcija σ involucija.

Propozicija 1.2.5. *Ako je p neparan, involucija σ definirana s* (1.1) *ima fiksnu točku.*

Dokaz. Neka je p neparan prost broj. Tvrdimo da je fiksna točka involucije σ jednaka

$$a = \sum_{i=0}^{\infty} \frac{p-1}{2} p^i$$

Jer je p neparan, vrijedi da je $\frac{p-1}{2} \in \{0, 1, \ldots p - 1\}$. Vrijedi

$$\sigma(a) = \sum_{i=0}^{\infty} (p - 1 - \frac{p-1}{2})p^i = \sum_{i=0}^{\infty} \frac{p-1}{2} p^i$$

□

Lema 1.2.6. *Skup p-adskih cijelih brojeva sa zbrajanjem opisanim kao u Primjeru 1.2.1 čini Abelovu grupu.*

Dokaz. Potrebno je provjeriti aksiome grupe iz *Definicije 1.2.2*.
Zbog načina zbrajanja opisanog u *Primjeru 1.2.1* vrijedi $x + y \in X_p$ $\forall x, y \in X_p$. Asocijativnost slijedi iz asocijativnosti zbrajanja cijelih brojeva. Neutral za zbrajanje je $0 = 0 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \ldots$. Za proizvoljni element $x \in X_p$, njemu inverzni element dan je s $\sigma(x) + 1$ gdje je σ funkcija dana s (1.1). □

Napomena 1.2.7. *Uočimo također da imamo injektivni homomorfizam grupa $\mathbb{Z} \to X_p$ koji je proširenje ulaganja monoida $\mathbb{N}_0$ u X_p. (Sjetimo se, homomorfizam $h : G_1 \to G_2$ je preslikavanje između grupa takvo da $h(a \cdot_{G_1} b) = h(a) \cdot_{G_2} h(b), \forall a, b \in G_1$)*

Napomena 1.2.8. *Od sada pa nadalje, skup p-adskih cijelih brojeva označavat ćemo sa $\mathbb{Z}_p$.*

Kao što smo u *Primjeru 1.2.1* pokazali kako zbrajamo dva p-adska cijela broja, sada bismo htjeli uvesti i operaciju množenja. Neka su ponovo $a = \sum_{i=0}^{\infty} a_i p^i$ i $b = \sum_{i=0}^{\infty} b_i p^i$ dva p-adska cijela broja. Umnožak $a \cdot b$ definirat ćemo tako što ćemo članove reda pomnožiti svaki sa svakim s ciljem da koeficijenti $(a \cdot b)_n$, $n \in \mathbb{N}_0$ ostanu u rasponu $\{1, 2, \dots, p-1\}$. Da bismo osigurali to svojstvo, ponovo ćemo koristiti sustav prijenosa. Takav način množenja je zapravo proširen način množenja dvaju prirodnih brojeva zapisanih u bazi p. S množenjem opisanim kao gore, vidimo da vrijedi

$$(a \cdot b)_n = ((\sum_{i=0}^{n} a_i p^i) \cdot (\sum_{i=0}^{n} b_i p^i))_n.$$

Primjer 1.2.9. *Uzmimo $p = 3, a = 5, b = 4$. Demonstrirajmo na ovom primjeru kako množimo dva p-adska cijela broja. Prvo raspisujemo 4 i 5 kao 3-adske brojeve.*

$$4 = 1 \cdot 3^0 + 1 \cdot 3^1$$

$$5 = 2 \cdot 3^0 + 1 \cdot 3^1.$$

$$4 \cdot_p 5 = (1 \cdot 3^0 + 1 \cdot 3^1) \cdot (2 \cdot 3^0 + 1 \cdot 3^1) = \cdots = 2 \cdot 3^0 + 3 \cdot 3^1 + 1 \cdot 3^2.$$

Drugi koeficijent nije u dopustivom rasponu. Sada postupamo slično kao pri zbrajanju. Dakle,

$$2 \cdot 3^0 + 3 \cdot 3^1 + 1 \cdot 3^2 = 2 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 = 4 \cdot_p 5.$$

Uočimo, množenje dvaju p-adskih cijelih brojeva slično je množenju redova, samo trebamo paziti da nam koeficijenti ostanu u rasponu $\{0, 1, \dots, p-1\}$.

U *Primjeru 1.2.1* smo vidjeli da je

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

Odnosno, vrijedi

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

Iz čega slijedi:

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

Odnosno, multiplikativni inverz broja $1-p$ je $\sum_{i=0}^{\infty} p^i$. Zaključujemo da na ovaj način računamo sumu geometrijskog reda. Uzmemo li $x = \frac{3}{-2} = \frac{3}{1-3}$, lako vidimo da njegovu 3-adsku reprezentaciju možemo zapisati kao $x = 3 \cdot \frac{1}{1-3} = 3 \cdot (1 + 3 + 3^2 + 3^3 + \cdots) = 0 \cdot 3^0 + 1 \cdot 3^1 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots$.

Napomena 1.2.10. *Prost broj p nema multiplikativni inverz u $\mathbb{Z}_p$. Naime, kada bi postojao broj $a = \sum_{i=0}^{\infty} a_i p^i$ t.d. $pa = 1$, vrijedilo bi $pa = p \sum_{i=0}^{\infty} a_i p^i = a_0 p^1 + a_1 p^2 + a_2 p^3 + \cdots \neq 1$.*

Definicija 1.2.11. *Neka je P neprazan skup $+ : P \times P \to P$ te $\cdot : P \times P \to P$ binarne operacije na skupu P. Za $(P, +, \cdot)$ reći ćemo da je prsten ako vrijedi:*
(P1) $(P, +)$ *je Abelova grupa*
(P2) $(P, \cdot)$ *je polugrupa*
(P3) $(a + b) \cdot c = a \cdot c + b \cdot c$
$a \cdot (b + c) = a \cdot c + a \cdot b \quad \forall a, b, c \in P.$
Ako je $\cdot$ komutativna operacija reći ćemo da je $(P, +, \cdot)$ komutativni prsten.

Napomena 1.2.12. *Napomenimo da ako u prstenu P postoji neutralni element za množenje, prsten P nazivamo prstenom s jedinicom. Ako ne napomenemo drugačije, u ovom radu ćemo podrazumijevati da kada govorimo o prstenu, zapravo govorimo o prstenu s jedinicom.*

Lema 1.2.13. *$(\mathbb{Z}_p, +, \cdot)$ sa zbrajanjem kao u Primjeru 1.2.1 i množenjem kao u Primjeru 1.2.9. je komutativni prsten s jedinicom.*

Dokaz. Potrebno je provjeriti aksiome prstena iz *Definicije 1.2.11.*
U *Lemi 1.2.6* smo već pokazali da je $(\mathbb{Z}_p, +)$ Abelova grupa. Da je $(Z_p, \cdot)$ polugrupa lako vidimo iz načina na koji smo definirali množenje. Naime, u *Primjeru 1.2.8.* smo vidjeli da zahtijevamo $\forall x, y \in \mathbb{Z}_p$ je i $x \cdot y \in \mathbb{Z}_p$. Asocijativnost množenja slijedi iz asocijativnosti množenja cijelih brojeva. Direktnim računom provjeri se da aksiom *(P3)* zapravo slijedi iz istog svojstva cijelih brojeva kao i komutatitivnost operacije $\cdot$. Lako se vidi da je neutral za množenje $1 = 1 \cdot p^0 + 0 \cdot p + 0 \cdot p^2 + \ldots$. □

U nastavku ćemo definirati pojam reda p-adskog cijelog broja te pokazati neka dodatna svojstva od $\mathbb{Z}_p$ kao prstena.

Definicija 1.2.14. *Neka je $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ proizvoljan p-adski cijeli broj, $a \neq 0$. Red cijelog broja a je prvi indeks $i \in \mathbb{N}_0$ takav da $a_i \neq 0$. Red cijelog broja a označavamo s $ord(a)$.*

Iako smo se već podsjetili pojma homomorfizma grupa, formalizirajmo ga u sljedećoj definiciji.

Definicija 1.2.15. *Neka su $(G,\cdot)$ i $(H,\cdot)$ grupe. Neka je $f : G \to H$. Funkciju f zvat ćemo homomorfizam između G i H ako vrijedi $f(a\cdot b) = f(a)\cdot f(b)$ $\forall a,b \in G$.*
Ako je f još dodatno injekcija, zvat ćemo ju monomorfizmom. Ako je f dodatno surjekcija, zvat ćemo ju epimorfizmom. Ako je f još i bijekcija, zvat ćemo ju izomorfizmom. Ako je $G = H$, tada funkciju f zovemo endomorfizmom. Ako je $G = H$ i f bijekcija, to preslikavanje zvat ćemo automorfizmom.

Napomena 1.2.16. *Ako su $(P,+,\cdot)$ i $(R,+,\cdot)$ prstenovi, također je moguće definirati homomorfizam. Naime, reći ćemo da je $f : P \to R$ homomorfizam prstenova ako je to preslikavanje aditivno i multiplikativno, tj. $f(a+b) = f(a)+f(b)$ i $f(a\cdot b) = f(a)\cdot f(b), \forall a,b \in P$. Na analogan način definiramo i ostale pojmove za prstenove iz Definicije 1.2.15.*

Definicija 1.2.17. *Neka je $(P,+,\cdot)$ prsten i $a,b \in P$ takvi da $a \neq 0, b \neq 0$ i $a\cdot b = 0$. Tada a i b zovemo djeliteljima nule. Prsten bez djelitelja nule nazivamo integralnom domenom.*

Propozicija 1.2.18. *$\mathbb{Z}_p$ je integralna domena.*

Dokaz. Budući da $\mathbb{Z}_p \neq \{0\}$, moramo pokazati da u $\mathbb{Z}_p$ ne postoje djelitelji nule. Neka je $a = \sum_{i=0}^{\infty} a_i p^i \neq 0$ i $\sum_{i=0}^{\infty} b_i p^i \neq 0 \in \mathbb{Z}_p$. Neka je $v = ord(a)$ i $w = ord(b)$. Jasno je da vrijedi $a_v, b_w \neq 0 (mod\, p)$. Direktnim računom se pokaže da je prvi ne-nul koeficijent u $a\cdot b$ jednak $a_v b_w (mod\, p) \neq 0$, iz čega slijedi da $a\cdot b \neq 0$. □

Korolar 1.2.19. *Red p-adskog cijelog broja $ord : \mathbb{Z}_p - \{0\} \to \mathbb{N}_0$ zadovoljava sljedeća svojstva:*
a) $ord(a\cdot b) = ord(a) + ord(b)$
b) $ord(a+b) \geq min\{ord(a), ord(b)\}$
ako $a,b,a+b \neq 0$.

Dokaz. a) Slično kao u *Propoziciji 1.2.18*, ako $a,b \neq 0$, i $v = ord(a), w = ord(b)$ direktnim računom provjerimo da je jedini kandidat za prvi ne-nul koeficijent u $a\cdot b$ upravo $a_v b_w (mod\, p)$. Taj broj nikad nije jednak nuli zbog $a_w, b_v \neq 0 (mod\, p)$.
b) Označimo s $c = \sum_{i=0}^{\infty} c_i p^i = a+b$ Neka je, BSO $v \leq w$. Očito, za $i < v$ vrijedi $c_i = 0$. Ako je $v < w$, tada je $c_i = a_i$ za $i < w$ pa specijalno $ord(c) = ord(a) = v = min\{v,w\}$. Ako je $w = v$, tada je $c_v = a_v + b_v (mod\, p)$, što ne mora biti različito od nule, odnosno, $ord(c) \geq v = w = min\{v,w\}$. □

Korolar 1.2.20. *Neka je $x \in \mathbb{Z}_p \neq 0$. Vrijedi $ord(x) = ord(-x)$.*

Dokaz. Po *Korolaru 1.2.19 a)* znamo da je $ord(x \cdot y) = ord(x) + ord(y)\ \forall x, y \in \mathbb{Z}_p - \{0\}$. Specijalno, ako je $x \neq 0$ proizvoljan i $y = -1 = \sum_{i=0}^{\infty}(p-1)p^i$, sada lako vidimo da je $ord(-1) = 0$. Stoga slijedi da je $ord(-x) = ord((-1)\cdot x) = ord(-1) + ord(x) = 0 + ord(x) = ord(x)$. □

Definicija 1.2.21. *Neka je P prsten i $I \subseteq P$ također prsten takav da je $1_p \in I$. Tada I nazivamo potprsten prstena P u oznaci $I \leq P$.*

Definicija 1.2.22. *Neka je P prsten i $I \leq P$. Potprsten I zvat ćemo lijevim idealom ako $(\forall a \in P)(\forall x \in I)\ ax \in I$ tj. $RI \subseteq I$. Potprsten I zvat ćemo desnim idealom ako vrijedi $(\forall a \in P)(\forall x \in I)\ xa \in I$ tj. $IR \subseteq I$. Ukoliko je I i lijevi i desni ideal, zvat ćemo ga obostranim idealom u oznaci $I \trianglelefteq P$.*

Definicija 1.2.23. *Za prsten P reći ćemo da je tijelo ili prsten s dijeljenjem ako svaki ne-nul element ima multiplikativni inverz. Komutativno tijelo zovemo poljem.*

Neka je $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Očito je $\mathbb{F}_p$ konačno polje s p elemenata. Promotrimo preslikavanje

$$a = \sum_{i=0}^{\infty} a_i p^i \mapsto a_0 (mod\, p).$$

Lako se provjeri da gornje preslikavanje definira surjektivni homomorfizam grupa $\epsilon : \mathbb{Z}_p \to \mathbb{F}_p$ s jezgrom $\{a \in \mathbb{Z}_p \mid a_0 = 0\} = p\mathbb{Z}_p$. Preslikavanje ϵ bit će nam od koristi pri dokazu sljedeće propozicije.

Propozicija 1.2.24. *Vrijedi $\mathbb{Z}_p^{\times} = \{\sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0\}$, gdje smo sa $\mathbb{Z}_p^{\times}$ označili skup svih invertibilnih elemenata skupa $\mathbb{Z}_p$.*

Dokaz.
$\boxed{\subseteq}$ Neka je $a \in \mathbb{Z}_p^{\times}$. Tada je $\epsilon(a) = a_0 (mod\, p)$ također invertibilan u $\mathbb{F}_p$. Zaključujemo da $a_0 \neq 0 (mod\, p)$.

$\boxed{\supseteq}$ Moramo pokazati da $\forall a \in \mathbb{Z}_p$ t.d. $ord(a) = 0$ postoji $b \in \mathbb{Z}_p$ takav da $a \cdot b = 1$. Budući da $ord(a) = 0$, jasno je da je $a_0 \neq 0$ iz čega slijedi da $\epsilon(a) \neq 0 \implies \epsilon(a)$ je invertibilan u $\mathbb{F}_p$. Uzmimo sada $b_0 \in \{0, 1, \ldots, p-1\}$ t.d. $a_0 b_0 \equiv 1 mod(p)$. Vrijedi da je $a_0 b_0 = kp + 1$ za neki $k \in \mathbb{Z}$ i $a = lp + a_0$ za neki $l \in \mathbb{Z}$. Iz gornje dvije relacije vidimo da je $ab_0 = (lp + a_0)b_0 = lpb_0 + a_0 b_0 = lpb_0 + kp + 1 = (lb_0 + k)p + 1 = mp + 1$ za neki $m \in \mathbb{Z}$. Sada je dovoljno pokazati da je $mp + 1$ invertibilan jer će tada slijediti $a^{-1} = b_0(mp+1)^{-1}$. Lako se vidi da je $(mp+1)^{-1} = 1 - mp + (mp)^2 - (mp)^3 + \cdots = 1 + c_1 p + c_2 p^2 - \ldots$, gdje je $c_i \in \{0, 1, \ldots, p-1\}$ kada taj broj zapišemo kao p-adski cijeli broj.

□

Definicija 1.2.25. *Za ideal $I \trianglelefteq P$ kažemo da je glavni ideal prstena P ako je generiran jednim elementom, tj. ako $\exists x \in P$ takav da je*

$$I = (x) = \bigcap_{J \trianglelefteq P, x \in J} J.$$

Definicija 1.2.26. *Ako je svaki ideal I u prstenu P glavni reći ćemo da je P prsten glavnih ideala. Ako je P još i integralna domena, reći ćemo da je P domena glavnih ideala.*

Propozicija 1.2.27. *$\mathbb{Z}_p$ je domena glavnih ideala. Glavni ideali od $\mathbb{Z}_p$ su $\{0\}$ i $(p^k) = p^k\mathbb{Z}_p = \{x \in \mathbb{Z}_p \mid v(x) \geq k\}, k \in \mathbb{N}$.*

Dokaz. Neka je $I \neq \{0\}$ proizvoljni ideal u $\mathbb{Z}_p$ i neka je $0 \neq a \in I$ element u I s najmanjim redom k, $ord(a) = k < \infty$. Vrijedi da je $a = p^k(a_k + a_{k+1}p + a_{k+2}p^2 + \dots) = p^k u$. Po *Propoziciji 1.2.24* znamo da je $u \in \mathbb{Z}_p$ invertibilan. Stoga vrijedi da je $p^k = au^{-1}$, a budući da je I ideal, zaključujemo da je $p^k \in I$ i $(p^k) \subseteq I$. Obratno, ako je $b \in I$ t.d. $ord(b) = w \geq k$, tada vrijedi $b = p^w u' = p^k p^{w-k} u' \in (p^k)$. □

Definicija 1.2.28. *Za ideal M od prstena P reći ćemo da je maksimalan ako vrijedi:*
(M1) $M \neq P$
(M2) $(\forall N \trianglelefteq P)\ (M \subseteq N \subseteq P \Rightarrow M = N$ ili $N = P)$

Korolar 1.2.29. *Jedinstveni maksimalni ideal od $\mathbb{Z}_p$ je $p\mathbb{Z}_p = \mathbb{Z}_p - \mathbb{Z}_p^\times$.*

Dokaz. Iz *Propozicije 1.2.24* odmah vidimo da je $\mathbb{Z}_p = p\mathbb{Z}_p \sqcup \mathbb{Z}_p^\times$. Također, lako se vidi da vrijedi jednakost

$$\mathbb{Z}_p - \{0\} = \bigsqcup_{k \geq 0} p^k \mathbb{Z}_p^\times,$$

odakle slijedi tvrnja. □

1.3 Metrika na $\mathbb{Z}_p$

Za početak, prisjetimo se definicije metrike kao funkcije.

Definicija 1.3.1. *Neka je X skup i $d : X \times X \to \mathbb{R}$ funkcija koja zadovoljava sljedeća svojstva:*
(D1) $d(x, y) = 0 \Leftrightarrow x = y\ \forall x, y \in X$.
(D2) $d(x, y) = d(y, x)\ \forall x, y \in X$
(D3) $d(x, z) \leq d(x, y) + d(y, z)\ \forall x, y, z \in X$
tada funkciju $d : X \times X \to \mathbb{R}$ zovemo metrikom na X, a uređeni par (X, d) zovemo metričkim prostorom.

Definirajmo funkciju $|\cdot| : \mathbb{Z}_p \to \mathbb{R}$ kao

$$|x| = \begin{cases} p^{-v} & x \neq 0 \ (v = ord(x)) \\ 0 & x = 0 \end{cases} \tag{1.2}$$

Također definirajmo funkciju $d : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}$ kao $d(x, y) = |x - y|$.

Propozicija 1.3.2. *Funkcija $|\cdot| : \mathbb{Z}_p \to \mathbb{R}$ definirana s* (1.2) *zadovoljava sljedeća svojstva:*
(N1) $|x| \geq 0 \ \forall x \in X$
(N2) $|x| = 0 \Leftrightarrow x = 0$
(N3) $|xy| = |x|\,|y| \quad \forall x, y \in X$
(N4) $|x + y| \leq |x| + |y| \ \forall x, y \in X$

Dokaz. Uzmimo proizvoljni $x, y \in \mathbb{Z}_p, x = \sum_{i=0}^{\infty} x_i p^i$, $y = \sum_{i=0}^{\infty} y_i p^i$, i označimo s $v = ord(x), w = ord(y)$.
(N1) vrijedi jer je $0 \geq 0$ i $p^{-v} \geq 0$ za svaki fiksni p prost broj i za svaki $v \geq 0$.
(N2) vrijedi jer $p^{-v} > 0$ za svaki fiksni prost broj p i za svaki $v \geq 0$. Dakle $|x| = 0$ ako i samo ako $x = 0$.
Po *Korolaru 1.2.19 a)* znamo da vrijedi $ord(xy) = ord(x) + ord(y) = v + w$. Stoga vrijedi sljedeća jednakost: $|xy| = p^{-(v+w)}$. S druge strane, $|x|\,|y| \overset{\text{def}}{=} p^{-v}p^{-w} = p^{-(v+w)}$, odnosno vrijedi *(N3)*.
BSO, pretpostavimo da je $v \leq w$. Po *Korolaru 1.2.19 b)* vrijedi $ord(x + y) \geq v$. $\Rightarrow |x + y| = p^{-ord(x+y)} \leq p^{-v}$. Stoga zaključujemo $|x+y| \leq p^{-v} \leq p^{-v}+p^{-w} = |x|+|y|$ pa vrijedi i *(N4)*. □

Napomena 1.3.3. *Uočimo, $|\cdot|$ nije norma (ne zadovoljava sve aksiome norme). Da bi $|\cdot|$ bila norma potreban nam je i aksiom $|\lambda x| = |\lambda|\,|x| \ \forall x \in X, \lambda \in \mathbb{F}$. Međutim, nije jasno koje bi polje $\mathbb{F}$ bilo prikladno (budući da množenje dvaju p-adskih brojeva nije "standradno" množenje, umnožak λx ne mora imati smisla). Ova se funkcija često naziva p-adska apsolutna vrijednost.*

Propozicija 1.3.4. *Funkcija $d : X \times X \to \mathbb{R}$ definirana s $d(x, y) = |x - y|$ je metrika na $\mathbb{Z}_p$.*

Dokaz. Potrebno je dokazati aksiome metrike iz *Definicije 1.3.1*. Vrijedi $d(x, y) = 0 \Leftrightarrow |x - y| = 0$, a po *Propoziciji 1.3.2* to je moguće ako i samo ako je $x - y = 0$, tj. $x = y$. Dakle, vrijedi *(D1)*. Pokažimo da vrijedi i *(D2)*. Ako je $x = y$ tada tvrdnja trivijalno slijedi. Pretpostavimo da $x \neq y$. Po definiciji je $d(x, y) = |x - y| = p^{-ord(x-y)}$ i $d(y, x) = |y - x| = p^{-ord(y-x)}$. Po *Korolaru 1.2.20* znamo da je $ord(x - y) = ord((-1)(x - y)) = ord(y - x)$. Stoga je $d(x, y) = d(y, x)$. Neka su sada $x, y, z \in \mathbb{Z}_p$. Primijenimo *(N4)* iz *Propozicije 1.3.2* na brojeve $x - y$ i $y - z$, imamo $d(x, z) = |x - z| = |(x - y) + (y - z)| \leq |x - y| + |y - z| = d(x, y) + d(y, z)$. □

Budući da svaka metrika inducira topologiju, to čini i p-adska metrika d koju smo definirali na početku ovog odjeljka. U nastavku rada ćemo kratko proučiti neka topološka svojstva od $\mathbb{Z}_p$. Definirat ćemo neke osnovne pojmove iz opće topologije te navesti neke rezultate bitne za ovaj rad, a više o njima se može pronaći u [3] te [1].

Definicija 1.3.5. *Neka je G grupa opskrbljena topologijom. Ako je preslikavanje $(x, y) \mapsto x \cdot y^{-1}$ neprekidno, G ćemo zvati topološkom grupom.*

Primjer 1.3.6. *Pokažimo da su $(\mathbb{Z}_p, +)$ i $(\mathbb{Z}_p^\times, \cdot)$ topološke grupe gdje $p^n\mathbb{Z}_p$ čine bazu topologije oko 0, a $1+p^n\mathbb{Z}_p$ bazu topologije oko 1. Ovaj primjer kao i druge primjere topoloških grupa mogu se pronaći u [3].*

Uzmimo $a' \in a + p^n\mathbb{Z}_p$ i $b' \in b + p^n\mathbb{Z}_p$. Tada je $a' - b' \in a - b + p^n\mathbb{Z}_p$ za svaki $n \geq 0$. Odnosno, koristeći p-adsku metriku, vrijedi:

$$|x - a| \leq p^{-n}, |y - b| \leq p^{-n} \Rightarrow |(x - y) - (a - b)| \leq p^{-n},$$

iz čega zaključujemo da je preslikavanje $(x, y) \mapsto x - y$ neprekidno u proizvoljnoj točki (a, b).

Poromatrajmo sada $(\mathbb{Z}_p^\times, \cdot)$. Osnovni sustav okolina oko neturala 1 su podgrupe:

$$1 + p\mathbb{Z}_p \supset 1 + p^2\mathbb{Z}_p \supset \cdots \supset 1 + p^n\mathbb{Z}_p \supset \ldots$$

Uzmimo sada $\alpha, \beta \in \mathbb{Z}_p$. Vrijedi da je $(1 + p^n\beta)^{-1} = 1 + p^n\beta'$ za neki $\beta' \in \mathbb{Z}_p$. Tada za $a = 1 + p^n\alpha$ i $b = 1 + p^n\beta$ vrijedi

$$ab^{-1} = (1 + p^n\alpha)(1 + p^n\beta') = 1 + p^n\gamma,$$

za neki $\gamma \in \mathbb{Z}_p$. Stoga vrijedi

$$a' \in a(1 + p^n\mathbb{Z}_p),\ b \in b(1 + p^n\mathbb{Z}_p) \Rightarrow ab^{-1} \in ab^{-1}(1 + p^n\mathbb{Z}_p),\ n \geq 1$$

Iz gornje implikacije sada zaključujemo da je preslikavanje $(x, y) \mapsto xy^{-1}$ neprekidno.

Sada ćemo na analogan način definirati topološki prsten i pokazati da je $\mathbb{Z}_p$ topološki prsten.

Definicija 1.3.7. *Za prsten P opskrbljen topologijom reći ćemo da je topološki prsten ako su preslikvanja*
$(x, y) \mapsto x + y : P \times P \to P$, te
$(x, y) \mapsto x \cdot y : P \times P \to P$
neprekidna.

Propozicija 1.3.8. *$\mathbb{Z}_p$ je topološki prsten uz p-adsku metriku d.*

Dokaz. Budući da znamo da je $\mathbb{Z}_p$ topološka grupa, dovoljno je pokazati neprekidnost množenja. Neka su $a, b \in \mathbb{Z}_p$ proizvoljni. Stavimo $x = a + h, y = b + k \in \mathbb{Z}_p$. Vrijedi

$$|xy - ab| = |(a+h)(b+k) - ab| = |ak + hb - hk| \leq max\{|a|, |b|\}(|h| + |k|) + |h|\,|k| \longrightarrow 0,$$

kada $|h|, |k| \longrightarrow 0$. Sada zaključujemo da je preslikavanje $(x, y) \mapsto xy$ neprekidno u svakoj točki $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$. □

1.4 Projektivni limes

Pretpostavimo da imamo niz $(E_n)_{n\geq 0}$ takvih da je $\forall n \in \mathbb{N}_0\ E_n = \prod_{i=0}^{n-1} X_i$ za neki niz skupova $(X_i)_i$. Željeli bismo na neki način reći da $E_n \longrightarrow E = \prod_{i=0}^{\infty} X_i$ kada $n \to \infty$. Jasno je da takvu konvergenciju ne možemo opisati standardnim alatima realne analize. Zbog toga uvodimo sljedeće funkcije

$$p_n : E \to E_n,\ n \geq 0$$
$$\varphi_n : E_{n+1} \to E_n,\ n \geq 0$$

Takve da za $e = (e_0, e_1, e_2, \dots) \in E$ vrijedi

$$p_n(e) = (e_0, e_1, \dots, e_{n-1})$$

te

$$\varphi_n(e_0, e_1, \dots, e_n) = (e_0, e_1, \dots e_{n-1}).$$

Shematski vezu gornjih projekcija možemo pokazati ovako:

$$p_n : E \to \dots \overset{\varphi_{n+2}}{\to} E_{n+2} \overset{\varphi_{n+1}}{\to} E_{n+1} \overset{\varphi_n}{\to} E_n$$

Možemo reći da će bilo koji skup X sa danim nizom funkcija $(f_n)_{n\geq 0}$, $f_n : X \to E_n$ biti *gornja međa* niza $(E_n)_n$ ako taj niz funkcija zadovoljava gornje svojstvo. Limes će u tom slučaju biti, slično kao u realnoj analizi *najmanja gornja međa*. Dakle, limes $(E, (p_n)_n)$ će biti *najmanja gornja međa* u smislu da se sve *gornje međe* $(X, (f_n)_n)$ mogu dobiti komponiranjem funkcije $f : X \to E$ na sljedeći način:

$$f_n = p_n \circ f : X \overset{f}{\to} E \to \dots \to E_{n+1} \to E_n$$

Također, želimo da vrijedi

$$f_n = \varphi_n \circ f_{n+1} = \varphi_n \circ \varphi_{n+1} \circ f_{n+2} = \psi_n \circ f.$$

To nas motivira da uvedemo sljedeću definiciju.

Definicija 1.4.1. *Niz $(E_n, \varphi_n)_{n\geq 0}$ skupova $(E_n)_n$ i preslikavanja $\varphi_n : E_{n+1} \to E_n$ zovemo projektivnim sustavom. Skup E zajedno s preslikavanjem $\psi_n : E \to E_n$ takvim da vrijedi $\psi_n = \varphi_n \circ \psi_{n+1}$ za svaki $n \geq 0$ zovemo projektivnim limesom niza $(E_n, \varphi_n)_{n\geq 0}$ ako vrijedi: za svaki skup X i niz preslikavanja $(f_n)_{n\geq 0}$, $f_n : X \to E_n$ takvih da $f_n = \varphi_n \circ f_{n+1}$ postoji jedinstvena funkcija f takva da je*

$$f_n = \psi_n \circ f : X \to E \to E_n, \ \forall n \geq 0.$$

Preslikavanja $(\varphi_n)_{n\geq 0}$ zovemo tranzicijskim preslikavanjima.

Kada sustav prikažemo na sljedeći način

$$E_1 \leftarrow E_2 \leftarrow \cdots \leftarrow E$$

zvat ćemo ga *inverznim sustavom*. Projektivni limes E označavamo s $\varprojlim E_n$.

Primijetimo, ne možemo unaprijed znati postoji li uopće projektivni limes nekog projektivnog sustava i ako postoji, je li jedinstven. Sljedeći rezultat koji navodimo bez dokaza daje odgovor na ta pitanja. Dokaz teorema može se pogledati u [3].

Teorem 1.4.2. *Za svaki projektivni sustav $(E_n, \varphi_n)_{n\geq 0}$ postoji projektivni limes $E = \varprojlim E_n \subset \prod_{n\geq 0} E_n$ sa preslikavanjima $(\psi_n)_n$ kao u Definiciji 1.4.1.*

Napomena 1.4.3. *Pokaže se da eksplicitno možemo odrediti projektivni limes nekog sustava (do na bijekciju iz prehodnog teorema) $(E_n, \varphi_n)_n$ i on je jednak*

$$E = \{x_n \mid \varphi_n(x_{n+1}) = x_n, \ n \geq 0\} \subset \prod_{n=0}^{\infty} E_n$$

Napomena 1.4.4. *Analogno definiramo projektivni sustav (topoloških) prstena i njegov projektivni limes pri čemu zahtijevamo da su sva preslikavanja (neprekidni) homomorfizmi (topoloških) prstena.*

Pokazali smo da je $\mathbb{Z}_p$ topološki prsten i uveli smo pojam projektivnog limesa topološkog prstena. Sljedeći teorem koji navodimo bez dokaza daje karakterizaciju od $\mathbb{Z}_p$ u terminima topologije i projektivnih limesa. Tvrdnju sljedećega teorema možemo smatrati i alternativnom definicijom p-adskog cijelog broja. Dokaz sljedeće tvrdnje može se pronaći u [3].

Teorem 1.4.5. *Preslikavanje $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ koje p-adskom broju $x = \sum_{i=0}^{\infty} x_i p^i$ pridružuje njegov niz parcijalnih suma $x_n = \sum_{i=0}^{n-1} x_i p^i \ (mod p^n)$, $n \geq 0$ je izomorfizam topoloških prstenova.*

Iako prethodni teorem nismo dokazali, on zapravo govori da je $\mathbb{Z}_p$ moguće promatrati kao projektivni limes sustava $(Z_p/p^nZ_p, \varphi_n)_{n\geq 0}$ gdje je φ_n preslikavanje takvo da

$$\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \ni \sum_{i\leq n} x_i p^i \ (mod p^{n+1}\mathbb{Z}_p) \mapsto \sum_{i<n} x_i p^i \ (mod p^n\mathbb{Z}_p) \in \mathbb{Z}_p/p^n\mathbb{Z}_p$$

U ovom smo poglavlju promatrali $\mathbb{Z}_p$ u kontekstu teorije skupova, algebarskih struktura i metričkoga prostora. Naime, pokazali smo da je $\mathbb{Z}_p$ neprebrojiv skup kada smo ga promatrali kao Kartezijev produkt $\{1, 2, ..., p-1\}^{\mathbb{N}_0}$. Zatim smo zaključili da uz prikladnu definiciju zbrajanja možemo $\mathbb{Z}_p$ promatrati kao Abelovu grupu, a uz prikladnu definiciju množenja $\mathbb{Z}_p$ postaje i komutativni prsten. Pokazali smo i neke karakteristike prstena $\mathbb{Z}_p$. Naime, vidjeli smo da je $\mathbb{Z}_p$ integralna domena i čak štoviše domena glavnih ideala. Na konktetnim smo primjerima vidjeli kako funkcionira zbrajanje i množenje p-adskih cijelih brojeva. Definirali smo i funkcije $|\cdot| : \mathbb{Z}_p \to \mathbb{R}$, $|x| = \mathbf{1}_{\{x\neq 0\}} p^{-ord(x)}$ i $d : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}$, $d(x, y) = |x - y|$. Za funkciju $d : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}$ pokazali smo da zadovoljava svojstva metrike. Budući da svaka metrika inducira topologiju, na kraju smo se upoznali i sa nekim topološkim svojstvima od $\mathbb{Z}_p$. Naime, pokazali smo da je $\mathbb{Z}_p$ topološka grupa i topološki prsten uz topologiju induciranu p-adskom metrikom. Kasnije smo definirali pojam projektivnog sustava i projektivnog limesa. Ustvrdili smo da projektivni limes postoji za svaki projektivni sustav te da je jedinstven do na bijekciju. Pojam projektivnog limesa bio nam je važan jer nam je omogućio da na alternativni način definiramo $\mathbb{Z}_p$.

Poglavlje 2

Polje razlomaka $\mathbb{Q}_p$

Neka je p ponovo fiksni prost broj. U ovom ćemo poglavlju opisati polje razlomaka od $\mathbb{Z}_p$ koje ćemo označavati sa $\mathbb{Q}_p$ te dati nekoliko karakterizacija toga polja.Elemente toga polja nazivat ćemo p-adski brojevi. Jedan od najbitnijih pojmova u ovomu radu, pojam reda p-adskog cijelog broja proširit ćemo na polje razlomaka $\mathbb{Q}_p$. Pokazat ćemo da p-adsku apsolutnu vrijednost i metriku koje smo definirali u prošlom poglavlju, možemo proširiti na polje razlomaka. Na kraju ćemo za metriku $d : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}$ pokazati da zadovoljava svojstvo $d(x, z) \leq max\{d(x, y), d(y, z)\}\ \ \forall x, y, z \in \mathbb{Q}_p$, tj. da je d ultrametrika na $\mathbb{Q}_p$.

2.1 Definicija i karakterizacije polja $\mathbb{Q}_p$

Prisjetimo se prvo kako za danu integralu domenu D konstruiramo polje razlomaka. Tvrdnje nećemo dokazivati niti ćemo previše ulaziti u teoriju budući da to izlazi iz okvira ovoga rada. Neka je D integralna domena i neka je $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. Na S definiramo relaciju $\sim$ kao $(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$. Pokazuje se da je $\sim$ relacija ekvivalencije. Označimo s $[a, b]$ klasu ekvivalencije od (a, b). Operacije zbrajanja i množenja definiramo kao $[a, b]+[c, d] = [a{\cdot}d+b{\cdot}c, b{\cdot}d]$ i $[a, b]{\cdot}[b, c] = [a{\cdot}c, b{\cdot}d]$ za koje se pokazuje da su dobro definirane. Pokazuje se također da je skup svih takvih klasa ekvivalencija polje s definicijom zbrajanja i množenja kao gore i za danu integralnu domenu označavamo ga s $Frac(D)$.

U *Poglavlju 1.* pokazali smo da je $\mathbb{Z}_p$ integralna domena. Stoga označimo s $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$. Također smo vidjeli da se svaki $x \in \mathbb{Z}_p, x \neq 0$ može zapisati kao $x = p^{ord(x)}u$ gdje je $u \in \mathbb{Z}_p^{\times}$. Inverz od x u polju razlomaka je $1/x = p^{-m}u^{-1}$ tj. $1/x \in p^{-m}\,\mathbb{Z}_p$. Sada vidimo da je:

$$\mathbb{Q}_p = \bigcup_{m \geq 0} p^{-m}\,\mathbb{Z}_p.$$

Iz gornje opservacije jednostavno se vidi da $\forall x \in \mathbb{Q}_p$ postoji $m \in \mathbb{N}_0$ takav da je $x = p^{-m}a$ za neki $a \in \mathbb{Z}_p$. Ukoliko $x \neq 0$, tada $a \neq 0$. Sjetimo se da $a \neq 0 \in \mathbb{Z}_p$ možemo na jedinstven način zapisati kao $p^k u$ gdje je $k = ord(a)$ i $u \in \mathbb{Z}_p^\times$. Stoga lako vidimo da $x \in \mathbb{Q}_p - \{0\}$ na jedinstven način možemo zapisati kao $x = p^{-m}p^k u = p^l u$ za neki $l \in Z$ i $u \in \mathbb{Z}_p^\times$. Budući da je $\mathbb{Q}_p$ polje, odnosno $\mathbb{Q}_p^\times = \mathbb{Q}_p - \{0\}$, vrijedi

$$\mathbb{Q}_p^\times = \bigsqcup_{m\in\mathbb{Z}} p^m \mathbb{Z}_p^\times$$

Proširimo sada definiciju reda na polje razlomaka $\mathbb{Q}_p$.

Definicija 2.1.1. *Neka je $x \neq 0 \in \mathbb{Q}_p$ i $x = p^m u,\ m \in \mathbb{Z}, u \in \mathbb{Z}_p^\times$ jedinstven prikaz p-adskog broja x. Definiramo funkciju $ord : \mathbb{Q}_p \to \mathbb{Z}$ formulom $ord(x) = m$. Broj $ord(x)$ nazivamo redom p-adskog broja x.*

Napomena 2.1.2. *Funkcija $ord : \mathbb{Q}_p - \{0\} \to \mathbb{Z}$ zadovoljava sva svojstva kao i u slučaju $\mathbb{Z}_p$. Ta funkcija je homomorfizam između $\mathbb{Q}_p$ i $\mathbb{Z}$. Također, ako je $x \neq 0, x = a/b$ za $a, b \in \mathbb{Z}_p,\ b \neq 0$, vidimo da je $ord(x) = ord(a/b) = ord(a\cdot\frac{1}{b}) = ord(a)+ord(\frac{1}{b}) = ord(a)-ord(b)$. Zadnja jednakost slijedi iz diskusije na početku poglavlja.*

Napomena 2.1.3. *Po konvenciji, uzimat ćemo da je $ord(0) = +\infty$.*

Neka je ponovo $x \in \mathbb{Q}_p^\times$ i $v = ord(x)$. Znamo da je tada $x = p^v u$ za neki $u \in Z_p^\times$. Tada znamo da u možemo zapisati kao $u = \sum_{i=0}^{\infty} a_i p^i$ gdje $a_0 \neq 0$ i $0 \leq a_i \leq p-1,\ \forall i \geq 0$. Sada vidimo da je $x = p^v u = \sum_{i=0}^{\infty} a_i p^{i+v} = \sum_{i=v}^{\infty} x_i p^i$.

Također, lako se vidi da je za $m \in Z\ ord_p^{-1}(m) = \{a \in \mathbb{Q}_p \mid ord(a) = m\} = p^m\ \mathbb{Z}_p^\times$. Vrijedi $ord(a) \geq 0 \Leftrightarrow a \in \mathbb{Z}_p$.

2.2 Ultrametrika na $\mathbb{Q}_p$

U ovom odjeljku ćemo definirati ultrametriku na $\mathbb{Q}_p$. Vidjet ćemo da je ona zapravo poopćenje ultrametrike iz *Poglavlja 1*.

Definicija 2.2.1. *Neka je X skup i $d : X \times X \to \mathbb{R}$ metrika na tom skupu. Ako d zadovoljava i dodatno svojstvo $d(x,z) \leq max\{d(x,y), d(y,z)\}\ \forall x, y, z \in X$, tada funkciju d zovemo ultrametrikom na X. Gornje svojstvo nazivamo još i jakom nejednakošću trokuta.*

Definirajmo funkciju $|\cdot| : \mathbb{Q}_p \to \mathbb{R}$ kao

$$|x| = \begin{cases} p^{-v} & x \neq 0\ (v = ord(x)) \\ 0 & x = 0 \end{cases} \tag{2.1}$$

Gornju funkciju često zovemo p-adska apsolutna vrijednost. Uočimo, ova je funkcija prirodno proširenje funkcije definirane s (1.2) na polje razlomaka $\mathbb{Q}_p$. Jasno je i da vrijedi $|\cdot|_{\mid \mathbb{Z}_p}$ dana s (1.2). Direktnim računom se provjeri da ova funkcija zadovoljava i sva svojstva iz *Propozicije 1.3.2*. Analogno, definirat ćemo i funkciju $d : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}$ kao $d(x, y) = |x - y|$. Trivijalno se vidi da je ona proširenje iste funkcije iz *Poglavlja 1.* na polje razlomaka. Da je d metrika nećemo pokazivati u ovom poglavlju jer je dokaz potpuno analogan onomu iz *Poglavlja 1.* nego ćemo se baviti nekim novim svojstvima te funkcije.

Označimo sada s $v = ord(x)$, $w = ord(y)$ za $x, y \in \mathbb{Q}_p^\times$. Po *Napomeni 2.1.2* znamo da vrijedi $ord(x + y) \geq min\{v, w\} \Leftrightarrow |x + y| = p^{-ord(x+y)} \leq max\{p^{-v}, p^{-w}\} = max\{|x|, |y|\}$.

Propozicija 2.2.2. *Funkcija $d : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}$ definirana s $d(x, z) = |x - y|$ zadovoljava sljedeća svojstva:*
a) $d(x, y) \leq max\{d(x, y), d(y, z)\} \leq d(x, y) + d(y, z)$ $\forall x, y, z \in \mathbb{Q}_p$., (d je ultrametrika)
b) $d(x + z, y + z) = d(x, y)$ $\forall x, y, z \in \mathbb{Q}_p$, (d je invarijantna na zbrajanje)
c) $d(zx, zy) = |z|\, d(x, y)$ $\forall x, y, z \in \mathbb{Q}_p$
specijalno $d(px, py) = \frac{d(x,y)}{p}$.

Dokaz. a) Vrijedi $d(x, z) = |x - z| = |(x - y) + (y - z)|$ što je po gornjem komentaru manje ili jednako od $max\{|x - y|, |y - z|\} = max\{d(x, y), d(y, z)\}$.
b) $d(x + z, y + z) = |(x + z) - (y + z)| = |x - y| = d(x, y)$.
c) Budući da $|\cdot|$ zadovoljava svojstvo *(N3)* kao u *Propoziciji 1.3.2* imamo $d(zx, zy) = |zx - zy| = |z(x - y)| = |z|\,|x - y| = |z|\, d(x, y)$. □

Primjer 2.2.3. *Usporedimo udaljenosti brojeva 2 i $2001/1000$ u standardnoj Euklidskoj metrici te našoj p-adskoj metrici za različite p-ove.*

$|2001/1000 - 2|_{2,Eukl} = 0.001$
$|2001/1000 - 2|_2 = |1/1000|_2 = 2^{-ord_2(1/1000)} \overset{Nap.2.1.2.}{=} 2^{-(-ord_2(1000))} = 2^{ord_2(1000)}$
$= 2^{ord(2^3 5^3)} \overset{Kor.\ 1.2.19}{=} 2^{ord(2^3)+ord(5^3)} = 2^{3+0} = 2^3 = 8.$
Na sličan način se dobije da je $|2001/1000 - 2|_5 = |1/1000|_5 = 5^3 = 125$
Zaključujemo da su brojevi 2 i $2001/1000$ najudaljeniji u $|\cdot|_5$. Zanimljivo je vidjeti kako su ti brojevi "vrlo blizu" u standardnoj Euklidskoj metrici, a "vrlo daleko" u $|\cdot|_5$.

Sljedeći teorem govori o nekim topološkim svojstvima od $\mathbb{Q}_p$, a preuzet je iz [3].

Teorem 2.2.4. *Polje razlomaka $\mathbb{Q}_p$ inducira p-adsku topologiju na $\mathbb{Z}_p$. Također, $\mathbb{Q}_p$ je lokalno kompaktno polje s karakteristikom jednakom nuli, tj. $char\, \mathbb{Q}_p = 0$. $\mathbb{Q}_p$ možemo identificirati kao upotpunjenje prstena $Z[1/p] = \{ap^v \mid a \in \mathbb{Z}, v \in \mathbb{Z}\}$ ili $\mathbb{Q}$ uz p-adsku metriku d.*

Dokaz. Primijetimo, uz metriku d definiranu kao gore, $\mathbb{Z}_p$ je zapravo zatvorena jedinična kugla sa centrom u 0, odnosno vrijedi

$$x \in \mathbb{Z}_p \Leftrightarrow ord(x) \geq 0 \Leftrightarrow |x| \leq 1 \Leftrightarrow d(x, 0) \leq 1.$$

Slično, ako je $k \geq 0$, ideali $p^k \mathbb{Z}_p = \{x \in \mathbb{Z}_p \mid ord(x) \geq k\}$ zapravo čine kugle radijusa p^{-k} oko 0 u $\mathbb{Q}_p$. Te kugle čine glavni sustav okolina oko 0 u $\mathbb{Q}_p$. Budući da $\mathbb{Z}_p$ sadržava okolinu oko 0, ona je otvorena (i zatvorena) kugla. Odnosno, $\mathbb{Z}_p$ je kompaktna okolina oko 0 u $\mathbb{Q}_p$. Sada zaključujemo da je $\mathbb{Q}_p$ lokalno kompaktno polje pa stoga i potpuno (za dokaz vidi *Korolar 3., Poglavlje 3.2.* u [3].)

Neka je sada $x \in \mathbb{Q}_p - \{0\}$, $x = \sum_{i=v}^{\infty} x_i p^i$ ($v = ord(x)$). Lako se vidi da je niz $(x_n)_{n\in\mathbb{N}} \subset \mathbb{Z}[1/p]$, $x_n = \sum_{i=v}^{n-1} x_i p^i$ Cauchyjev niz u $\mathbb{Z}[1/p]$ koji konvergira prema x. Naime, vrijedi

$$x - x_n = \sum_{i \geq n} x^i p_i \in p^n \mathbb{Z}_p,$$

odnosno

$$d(x, x_n) \leq p^{-n} \to 0 \text{ kad } n \to \infty.$$

Dakle, za proizvoljni ne-nul element u $\mathbb{Q}_p$ pokazali smo da postoji Cauchyjev niz iz $\mathbb{Z}[1/p]$ koji konvergira prema x, odnosno da je $\mathbb{Z}[1/p]$ gust u $\mathbb{Q}_p$.

□

Poglavlje 3

Henselova lema

Kao što smo spomenuli u uvodu, Kurt Hensel bio je njemački matematičar koji je djelovao u drugoj polovini 19. i prvoj polovini 20. stoljeća, a jedan od njegovih najvećih doprinosa matematici jesu njegovi radovi o p-adskim brojevima koje je prvi opisao. U ovom će nam poglavlju glavni cilj biti iskazati i dokazati tvrdnju nazvanu po njemu, tzv. *Henselovu lemu* koja opisuje rješenje jednadžbe $P(x) = 0$ za $P \in \mathbb{Z}_p[X]$, $x \in \mathbb{Z}_p$. Prisjetimo se, kada god imamo neki komutativni prsten (ili polje) brojeva $\mathbb{A}$, od koristi je promatrati i prsten $\mathbb{A}[X]$, tj. prsten polinoma nad $\mathbb{A}$ u varijabli X (ili općenitije, u varijablama $X = (X_1, \cdots, X_n)$), te pokušati pronaći nultočke polinoma P iz $\mathbb{A}[X]$, tj. broj x koji zadovoljava jednadžbu $P(x) = 0$ u nekom specifičnom skupu $B \subseteq D_P$. Pri traženju rješenja takve jednadžbe, prirodno je postaviti pitanje koliko ima takvih rješenja i imaju li ta rješenja određena svojstva, tj. opisati skup rješenja. Također, kada opišemo skup rješenja možemo se pitati i koje su daljnje posljedice naših razmatranja.
U ovom ćemo poglavlju tražiti rješenje jednadžbe $P(x) = 0$ u već nam poznatome skupu $\mathbb{Z}_p$, dok će P biti polinom sa koeficijentima iz $\mathbb{Z}_p$. Tada ćemo dokazati tzv. *Henselovu lemu*, koja tvrdi da ako krenemo od neke početne aproksimacije x koje zadovoljava $P(x) \equiv 0 \ (mod\ p^n)$ za neki $n \in \mathbb{N}$, možemo doći do jedinstvenoga rješenja u $y \in \mathbb{Z}_p$ za koje vrijedi $y \equiv x \ (mod\ p^m)$ za specifičan $m \in \mathbb{N}$. Nakon toga ćemo vidjeti da su posljedice ove tvrdnje kvadratna proširenja polja $\mathbb{Q}_p$.

3.1 Tvrdnja i dokaz Henselove leme

U ovom nam je odjeljku osnovni cilj iskazati i dokazati Henselovu lemu. Prije nego što krenemo na dokaz tvrdnje, potrebno je pokazati nekoliko tehničkih detalja te se prisjetiti još ponekoga pojma iz algebre.

Prisjetimo se prvo, ako je P neki komutativni prsten, tada s $P[X_1, X_2, \cdots, X_n]$ označavamo skup svih polinoma u varijablama $X_1, X_2, \cdots, X_n$ sa koeficijentima iz P. Lako se provjeri da je i $P[X_1, X_2, \cdots, X_n]$ također komutativni prsten. Naravno, kada govorimo o polinomima jedno od najzanimljivijih pitanja jest postoji li x takav da je $P(x) = 0$. Kao što smo spomenuli u uvodu poglavlja, često nas zanima i koliko ima rješenja x i možemo li na neki način okarakterizirati skup rješenja jednadžbe $P(x) = 0$.

Krenimo s nekoliko tvrdnji koje će nam biti potrebna kako bismo došli do Henselove leme.

Propozicija 3.1.1. *Neka je $P \in \mathbb{Z}[X, Y]$. Sljedeće tvrdnje su ekvivalentne:*
a) $P(x, y) = 0$ za neke $x, y \in \mathbb{Z}_p$
b) $\forall n \geq 0$ postoji rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ gdje je $\mathbb{Z}/p^n\mathbb{Z}$ sustav ostataka modulo p^n
c) $\forall n \geq 0$ postoje $a_n, b_n \in \mathbb{Z}$ takvi da $P(a_n, b_n) \equiv 0 \ (mod\ p^n)$

Dokaz. Da je $b) \Leftrightarrow c)$ slijedi trivijalno.
Pretpostavimo sada da imamo rješenje $(x, y) \in \mathbb{Z}_p$ te neka je standardno $x = \sum_{i=0}^{\infty} a_i p^i$. Sada $\forall n \in \mathbb{N}_0$ definiramo $x_n = \sum_{i=0}^{\infty} a_i p^i \ (mod\ p^n) \in \mathbb{Z}/p^n\mathbb{Z}$. Na isti način definiramo i niz $(y_n)_{n\geq 0}$. Sada vidimo da ako je $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$, tada je zbog svojstva funkcije $mod p^n$ $P(x_n, y_n) = P(x, y)(mod p^n) \in \mathbb{Z}/p^n\mathbb{Z}$. Dakle $a) \Rightarrow b)$.
Pokažimo sada $b) \Rightarrow a)$. Definirajmo za svaki $n \in \mathbb{N}$ konačni skup $X_n = \{(x, y) \in \mathbb{Z}/p^n\,\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \mid P(x, y) = 0\}$.Po pretpostavci slijedi da $X_n \neq \emptyset$, $\forall n \in \mathbb{N}$. Definirajmo funkciju $\varphi_n : X_{n+1} \to X_n$ kao $\varphi_n(x) = (x(mod p^n), y(mod p^n))$. Lako se vidi da je φ_n neprekidni homomorfizam prstena $\forall n \in \mathbb{N}$. Sada po *Teoremu 1.4.2* znamo da $(X_n, \varphi_n)_{n\in\mathbb{N}}$ ima projektivni limes $X = \varprojlim X_n \subset \mathbb{Z}_p \times \mathbb{Z}_p$. *Korolar Propozicije 1.* u *Poglavlju 4.4* u [3] garantira da je $X \neq \emptyset$ budući da $X_n \neq \emptyset$ za svaki $n \in \mathbb{N}$. Stoga postoji $(x, y) \in X$ takav da je $P(x, y) = 0$. □

Propozicija 3.1.2. *Neka je A prsten i $P \in A[X]$ proizvoljni polinom. Tada postoje P_1 i P_2 u $A[X, Y]$ takvi da je $P(x + h) = P(x) + hP_1(x, h) = P(x) + hP'(x) + h^2P_2(x, h)$.*

Dokaz. Znamo da je $P(x+h) = \sum_{n=0}^{d} a_n(x+h)^n = \sum_{n=0}^{d} a_n(x^n+nx^{n-1}h+h^2(...)) = \sum_{n=0}^{d} a_n x^n + h\sum_{n=1}^{d} na_n x^{n-1} + h^2P_2(x, h)$. □

Kao što smo već napomenuli, u ovom nam je poglavlju jedan od ciljeva pronaći nultočke nekog polinoma P. Naravno, pronaći nultočku polinoma nije uvijek jednostavno pa često numeričkim metodama tražimo aproksimacije rješenja za neku danu točnost. Sjetimo se da je jedna od najpoznatijih metoda za pronalaženje nultočki neke funkcije f tzv. *Newtonova metoda*. Da bismo mogli koristiti *Newtonovu* metodu u realnoj analizi, funkcija f mora biti derivabilna i mora vrijediti $f'(x) \neq 0\ \forall x \in D_f$. Ona se temelji na nizu aproksimacija nultočke dok ne dođemo do željene točnosti. Uzmemo početku aproksimaciju x_0 i

definiramo

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, n \in N_0.$$

Uzmimo sada polinom $P \in \mathbb{Z}[X]$ i $x \in \mathbb{Z}$ takav da je $P(x) \equiv 0\ (mod\ p)$. BSO, možemo pretpostaviti da je $x = a_0 \in \{0, 1, \cdots, p-1\}$ jer $\forall n \in \mathbb{Z}$ je ostatak pri dijeljenju s prostim brojem p unutar toga skupa. Prisjetimo se, ako za neki broj x vrijedi $x \equiv 0\ (mod\ p^n)$, tada je $x \equiv 0\ (mod\ p^{n-1})$ za $n \in \mathbb{N}$, stoga možemo pokušati pronaći u tom smislu "finije" rješenje tj. $\hat{a}$ za koji želimo da vrijedi i $P(\hat{a}) \equiv 0\ mod(p^2)$. Iz svojstva funkcije modulo znamo da ako vrijedi $P(a_0) \equiv 0\ (mod\ p)$, tada je i $P(a_0 + a_1 p) \equiv 0\ (mod\ p)$ za neki $a_1 \in \{0, 1, \cdots, p-1\}$. Stavimo stoga $\hat{a} = a_0 + a_1 p$. Po *Propoziciji 3.1.2* znamo da je $P(\hat{a}) = P(a_0 + a_1 p) = P(a_0) + P'(a_0)a_1 p + b(a_1 p)^2$ za neki cijeli broj b (zato što je P_2 iz prethodne propozicije prsten nad $\mathbb{Z}$). Po pretpostavci znamo da je $P(a_0) = pt$ za neki t. Sada uz pretpostavku $P'(a_0) \neq 0$ vidimo da će vrijediti

$$P(\hat{a}) \equiv 0\ (mod\ p^2) \Leftrightarrow t + P'(a_0)a_1 \equiv 0\ (mod\ p) \Leftrightarrow a_1 \equiv \frac{-t}{P'(a_0)}\ (mod\ p) \text{ uz } P'(a_0) \not\equiv 0\ (mod\ p).$$

Stavimo li sada $\hat{a} = a_0 - \frac{pt}{P'(a_0)} = a_0 - \frac{P(a_0)}{P'(a_0)}$ vidimo da je zadovoljena tražena jednakost, odnosno $P(\hat{a}) \equiv 0\ (mod\ p^2)$. Uočimo da smo dobili istu jednakost kao i u Newtonovom nizu aproksimacija. Napomenimo da ćemo za izraz $N_p(x) = x - \frac{P(x)}{P'(x)}$ nazivati Newtonovim preslikavanjem.

Pokažimo sada neka svojstva Newtonovog preslikavanja.

Propozicija 3.1.3. *Neka je $P \in \mathbb{Z}_p[X]$ i $x \in \mathbb{Z}_p$ t.d. $P(x) \equiv 0\ (mod\ p^n)$. Ako je $k = ord(P'(x)) < n/2$, tada Newtonovo preslikavanje $\hat{x} = N_p(x) = x - P(x)/P'(x)$ zadovoljava sljedeća svojstva:*
a) $P(\hat{x}) \equiv 0\ (mod\ p^{n+1})$
b) $\hat{x} \equiv x\ (mod\ p^{n-k})$
c) $ord(P'(\hat{x})) = ord(P'(x))$.

Dokaz. Stavimo $P(x) = p^n y$ za neki $y \in \mathbb{Z}_p$ i $P'(x) = p^k u$ za $u \in \mathbb{Z}_p^\times$. Sada vidimo da je

$$\hat{x} - x = -P(x)/P'(x) = -p^{n-k} y u^{-1} \in p^{n-k}\mathbb{Z}_p,$$

odnosno pokazali smo b). Raspišemo li sada $P(x)$ kao u *Propoziciji 3.1.2* oko točke $\hat{x}$ dobivamo:

$$P(x) = P(\hat{x}) + P'(\hat{x})(x - \hat{x}) + P''(x)(x - \hat{x})^2 = P(\hat{x}) + P'(\hat{x})(x - \hat{x}) + t(x - \hat{x})^2.$$

Budući da je P'' polinom nad $\mathbb{Z}_p$ vrijedi da je $t \in \mathbb{Z}_p$. Uvrštavanjem $\hat{x} = -P(x)/P'(x)$ u gornju jednakost dobivamo da je

$$P(\hat{x}) = t(x - \hat{x})^2 \in p^{2n-2k}\,\mathbb{Z}_p = p^n p^{n-2k}\,\mathbb{Z}_p \subset p^{n+1}\,\mathbb{Z}_p$$

budući da je $2k < n$. Dakle, vrijedi i a). Preostaje pokazati c). Označimo sa $k = ord(P'(x))$. Iz *Propozicije 3.1.2* znamo da je

$$P'(\hat{x}) = P'(x + (\hat{x} - x)) = P'(x) + (\hat{x} - x)s = p^k u + p^{n-k} zs = p^k(u + p^{n-2k} zs) = p^k v$$

za neke $s, v \in \mathbb{Z}_p$, $u, z \in \mathbb{Z}_p^\times$. Još samo preostaje pokazati da je v invertibilan, no to lako slijedi jer je $n - 2k > 0$ te $v = u + p^{n-2k} zs \in u + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$. Sada je jasno da vrijedi tvrdnja c). □

Sada smo spremni dokazati Henselovu lemu.

Teorem 3.1.4. *(Henselova lema) Neka je $P \in \mathbb{Z}_p[X]$ i $x \in \mathbb{Z}_p$ takav da*

$$P(x) \equiv 0 \,(mod\, p^n).$$

Ako je $k = ord(P'(x)) < n/2$, tada postoji jedinstveni korijen $y \in \mathbb{Z}_p$ od P koji zadovoljava:

$$y \equiv x \,(mod\, p^{n-k})$$

$$i$$

$$ord(P'(y)) = ord(P'(x)) = k$$

Dokaz. Egzistencija. Konstruirajmo niz $(x_n)_{n\geq 0}$ na sljedeći način:

$$x_0 = x$$

$$x_1 \equiv x_0 \,(mod\, p^{n-k})$$
$$P(x_1) \equiv 0 \,(mod\, p^{n+1})$$
$$ord(P'(x_1)) = k.$$

Analogno nastavimo dalje, stavimo

$$x_2 \equiv x_1 \,(mod\, p^{n+1-k})$$

$$P(x_2) \equiv 0 \,(mod\, p^{n+2})$$
$$ord(P'(x_2)) = k$$

i tako dalje. Po *Propoziciji 3.1.3* znamo da takav niz postoji. Na taj smo način konstruirali Cauchyjev niz $(x_n)_{n\geq 0}$ za čiji p-adski limes y vrijedi $P(y) = 0$ i $y \equiv x \ (mod\, p^{n-k})$.

Jedinstvenost. Pretpostavimo da postoje dva p-adska cijela broja y, z koji zadovoljavaju svojstva iz teorema. Tada mora vrijediti $z \equiv y \ (mod\, p^{n-k})$. Jer je $n > 2k$ imamo da je $n - k \geq k + 1$, stoga vrijedi i $z \equiv y \ (mod\, p^{k+1})$. Sada po *Propoziciji 3.1.2*

$$P(z) = P(y) + P'(y)(z - y) + a(z - y)^2$$

za neki $a \in \mathbb{Z}_p$. Budući da je $P(z) = P(y) = 0$, imamo da je

$$(z - y)(P'(y) + a(z - y)) = 0.$$

Znamo da je $ord(P'(y)) = k \geq 0$, a zbog $z \equiv y \ (mod\, p^{k+1})$, zaključujemo da je $ord(a(z-y)) \geq k + 1$, pa je gornja jednakost jednaka ako i samo ako je $y = z$. □

Napomena 3.1.5. *Primijetimo, specijalni slučaj Henselove leme za $n = 1$ nas zapravo dovodi do "standardnih" iteracija Newtonove metode u smislu kongruencija. Naime, pretpostavka $k = ord(P'(x)) < n/2$ iz teorema vrijedit će ako i samo ako je $k = 0$, a to vrijedi ako i samo ako $P'(x) = a_0 + a_1 p + a_2 p^2 + \cdots$ uz $a_0 \neq 0$ što vrijedi ako i samo ako $P'(x) \not\equiv 0 \ (mod\, p)$.*

Primjer 3.1.6. *Pogledajmo jednadžbu $X^2 - 2 = 0$ u $\mathbb{Z}_7$.*
Tražimo rješenje jednadžbe $\alpha = a_0 + a_1 7 + a_2 7^2 + \cdots \in \mathbb{Z}_p$ (ako postoji). Tada je $a_0^2 - 2 \equiv 0 \ (mod\, 7)$. Imamo dvije mogućnosti: $\alpha_1 = a_0 = 3$ i $\alpha_1 = a_0 = 4$. Odaberemo $\alpha_1 = a_0 = 3$. Stavimo $\alpha_2 = a_0 + a_1 \cdot 7 \in \mathbb{Z}/49\mathbb{Z}$. Lako se provjeri da vrijedi

$$\alpha_2^2 - 2 \equiv 0 \ (mod\, 7^2) \Leftrightarrow a_1 \equiv 1 \ (mod\, 7).$$

Uočimo da na ovaj način zapravo kreiramo niz sve boljih aproksimacija iz Teorema 3.1.4 Iterirajući dolazimo do rješenja:

$$\alpha = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + 2 \cdot 7^5 + \cdots$$

3.2 Primjene Henselove leme

Pogledajmo sada neke od posljedica Henselove leme.

Invertibilni elementi u $\mathbb{Z}_p$

Neka je $P \in \mathbb{Z}_p[X]$, $P(x) = aX - 1, a \neq 0$. Jasno je da je $P(x) = 0 \Leftrightarrow aX = 1$. Pretpostavimo da je $ord(a) = 0$, tj. ako je $a = a_0 + a_1 p + a_2 p^2 + \cdots$, tada $a_0 \neq 0$ jer u suprotnom

ne možemo početnu aproksimaciju $x \in \mathbb{Z}_p$ t.d. $P(x) \equiv 0\,(mod\,p)$. Tada je jasno da je $ord(P'(x)) = ord(a) = 0$. Sada iteracijom sve boljih aproksimacija (u smislu modulo p^n) dolazimo do rješenja u $\mathbb{Z}_p$ po Henselovoj lemi. Možemo zaključiti da je nužan uvjet kako bismo na ovaj način došli do rješenja $a_0 \neq 0$, odnosno po *Propoziciji 1.2.24* $a \in \mathbb{Z}_p^\times$.

Uočimo sada, u prvom koraku *Newtonove metode* imat ćemo

$$\hat{x} = x - \frac{P(x)}{P'(x)} = \frac{1}{a}.$$

Međutim, *Newtonova metoda* pretpostavlja da znamo što znači podijeliti. Da smo u polju relanih ili kompleksnih brojeva, odmah bi bilo jasno da je rješenje gornje jednadžbe $\frac{1}{a}$, tj. već bi druga aproksimacija bila stvarno rješenje. Iz toga razloga ovu opservaciju shvaćamo više kao ilustrativnu. Za numeričko pronalaženje inverza bolja je opcija koristiti funkciju $f(X) = 1/X - a$. Tada je $\hat{x} = 2x - ax^2$ te izbjegavamo dijeljenje u pronalasku inverza.

Kvadratna proširenja od $\mathbb{Q}_p$

Promotrimo sada jednadžbu $P(X) = X^2 - a$ gdje je $P \in \mathbb{Z}_p[X]$. Pokušajmo pronaći rješenja ove jednadžbe. Jasno je da vrijedi $P(X) = 0 \Leftrightarrow a = X^2$, a za to je nužno da je $ord(a) = ord(X^2) = ord(X \cdot X) = 2ord(X)$, odnosno red p-adskog cijelog broja a mora biti paran. Ako sada podijelimo a s p^{2m} za odgovarajući $m \in \mathbb{N}_0$, ponovo dolazimo do invertibilnog elementa u $\mathbb{Z}_p$. Budući da je $ord(P'(X)) = ord(2X) = ord(2) + ord(X)$, vidimo da u slučaju $p = 2$, $ord(P'(X)) = 1$, a nula inače. Stoga ćemo posebno promatrati slučaj kada je $p = 2$ i kada je p neparan.

1. p je neparan.

Neka je $1 < a < p$ takav da $a \not\equiv x^2 (mod\,p)$ za neki x. Tada vrijedi da a, ap i p nemaju kvadratnih korijena u $\mathbb{Q}_p$. Oni čine skup reprezentanata za klase modula kvadrata, tj.

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (p^{\mathbb{Z}}/p^{2\mathbb{Z}}) \times (\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{3.1}$$

Budući da je svako kvadratno proširenje polja karakteristike 0 (kakvo je $\mathbb{Q}_p$) generirano kvadratnim korijenom, zaključujemo da imamo sva kvadratna proširenja do na izomorfizam, a to su:

$$\mathbb{Q}_p(\sqrt{a}), \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{ap}).$$

Objasnimo ukratko kako smo došli do izomorfizama u (3.1). Uočimo prvo da je $p^{\mathbb{Z}} \cong \mathbb{Z}$, a pripadni izomorfizam je $\mathbb{Z} \ni n \mapsto p^n \in p^{\mathbb{Z}}$. Slično, $p^{2\mathbb{Z}} \cong 2\mathbb{Z}$. Od tuda slijedi $p^{\mathbb{Z}}/p^{2\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$. Sjetimo se sada da je

$$\mathbb{Q}_p^\times = \bigsqcup_{m\in\mathbb{Z}} p^m \mathbb{Z}_p^\times.$$

Budući da je unija disjunktna, sada lako vidimo da je $p^Z \times \mathbb{Z}_p^\times \ni (p^m, u) \mapsto p^m \cdot u \in \mathbb{Q}_p^\times$ izomorfizam, odnosno slijedi da je

$$\mathbb{Q}_p^\times \cong p^Z \times \mathbb{Z}_p^\times$$

i to neovisno o (parnosti) od p. Od tuda slijedi

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (p^{\mathbb{Z}}/p^{2\mathbb{Z}}) \times (\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2).$$

Još samo preostaje pokazati da je $(\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2) \cong \mathbb{Z}/2\mathbb{Z}$, a tu će nam pomoći Henselova lema. Kao prvo, vrijedi da je

$$\mathbb{Z}_p \overset{mod p}{\mapsto} \mathbb{Z}/p\mathbb{Z}$$

epimorfizam, pa je i restrikcija

$$\mathbb{Z}_p^\times \overset{mod p}{\mapsto} (\mathbb{Z}/p\mathbb{Z})^\times$$

također epimorfizam. Označimo jezgru ovog epimorfizma s U_1. Lako vidimo da je

$$U_1 = 1 + p\mathbb{Z}_p \overset{Hen.lema}{\subseteq} (\mathbb{Z}_p^\times)^2$$

Sada imamo

$$(\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2) \cong (\mathbb{Z}/p\mathbb{Z})^\times/((\mathbb{Z}/p\mathbb{Z})^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

2. p je paran, tj. $p = 2$
Uočimo prvo da je $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$.

Propozicija 3.2.1. *Invertibilni element a u $\mathbb{Z}_2$ je kvadrat ako i samo ako $a \in 8\mathbb{Z}_2 + 1$.*

Dokaz. Neka je $a = b^2 \in \mathbb{Z}_2^\times$ za neki $b \in \mathbb{Z}_2$, tj $b = 1 + 2b_1 + 2^2b_2 + \cdots = 1 + 2c$. Tada je $b^2 = 1 + 4(c + c^2)$ za neki c. Jer je $c \equiv c^2 \,(mod\, 2\mathbb{Z}_2)$, jasno je da je $a \in 8\mathbb{Z}_2 + 1$.

Obratno, uzmimo proizvoljni element $a \equiv 1\,(mod\, 8\mathbb{Z}_2)$. Lako vidimo da je a invertibilan. Sada primjenjujemo Henselovu lemu na $X^2 - a = 0$ uz početnu aproksimaciju $x = 1$. Očito je sada $P(x) = X^2 - a \equiv 0\,(mod\, 2^3)$.Te je zadovoljena pretpostavka $3 = n > 2k = 1$. Sada konstruiramo niz sve boljih aproksimacija točno kao u dokazu *Henselove leme*. Na kraju dolazimo do pravog rješenja y za koje vrijedi $y \equiv x\,(mod\, 2^{3-1})$ za koje vrijedi $y^2 = a$ u $\mathbb{Z}_p$. □

Imamo:

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (2^\mathbb{Z}/2^{2\mathbb{Z}}) \times (\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2). \tag{3.2}$$

Znamo da je $(2^\mathbb{Z}/2^{2\mathbb{Z}}) \cong \mathbb{Z}/2\mathbb{Z}$ pa preostaje odrediti čemu je izomorfno $(\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2)$. Već smo napomenuli da je

$$\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2 = \{\pm 1\}(1 + 4\mathbb{Z}_2),$$

uvrštavanjem u gornju relaciju i po prethodnoj propoziciji imamo:

$$\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2). \tag{3.3}$$

Jasno je da je $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. Sada još pokažimo čemu je do na izomorfizam jednako $(1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2)$. Promotrimo preslikavanja

$$\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z},\ n \geq 1.$$

Jasno je da je π_n epimorfizam za svaki $n \geq 1$, stoga je i restrikcija

$$\pi_n : \mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times,\ n \geq 1.$$

također epimorfizam. Označimo jezgre ovih epimorfizama s U_n, $n \geq 1$. Lako se vidi da je $U_n = 1 + p^n\mathbb{Z}_p$. Ako sada pogledamo preslikavanje $mod p : U_n \to \mathbb{Z}/p\mathbb{Z}$, tj. $1 + p^n z \mapsto z\,(mod p)$, jasno je da će jezgra ovog preslikavanja biti U_{n+1}. Po prvom teoremu o izomorfizmu (za dokaz i tvrdnju vidi [4]) zaključujemo da je

$$U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}.$$

Iz gornjega jednostavno slijedi da je $(1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2) \cong U_2/U_3 \cong \mathbb{Z}/2\mathbb{Z}$. stoga je

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Uočimo da je $5 \in (1+4\mathbb{Z}_2)/(1+8\mathbb{Z}_2)$. Nadalje, zbog (3.2) i (3.3) sada je jasno da ćemo imati proširenja generirana s: $5, (-1), 2$ te $\pm 5 \cdot 2, \pm 2, \pm 5$. Zaključujemo da do na izomorfizam imamo sedam kvadratnih proširenja od $\mathbb{Q}_2$, a to su:

$$\mathbb{Q}_2(\sqrt{-1}),\ \mathbb{Q}_2(\sqrt{\pm 2}),\ \mathbb{Q}_2(\sqrt{\pm 5}) \text{ i } \mathbb{Q}_2(\sqrt{\pm 10}).$$

Primjer 3.2.2.
a) Lako se vidi da je $-7 = 1 - 8 \equiv 1\,(mod\,8)$ *iz čega zaključujemo da je* $\sqrt{-7} \in \mathbb{Z}_2^\times \subset \mathbb{Q}_2$. *Također, korijeni brojeva* $9, 17, 41$ *nalaze se u* $\mathbb{Q}_2$ *jer svi ti brojevi pri dijeljenju s* 8 *daju ostatak* 1.
b) Jednadžbe $X^2 + 1 = 0$, $X^2 - 3 = 0$ *nemaju rješenja u* $\mathbb{Q}_2$ *jer brojevi* -1 *i* 3 *ne zadovoljavaju uvjete Propozicije 3.2.1.*

Poglavlje 4

Algebarska proširenja p-adskih brojeva

U ovom će nas poglavlju zanimati proširenje p-adske metrike na konačna algebarska proširenja polja p-adskih brojeva.

Definicija 4.0.1. *Apsolutna vrijednost na polju $\mathbb{K}$ je homomorfizam $f : \mathbb{K}^\times \to \mathbb{R}_{>0}$ proširen s $f(0) = 0$ takav da $f(x+y) \leq f(x) + f(y)$ $\forall x, y \in \mathbb{K}$.*

Napomena 4.0.2. *Apsolutnu vrijednost na polju $\mathbb{K}$ označavamo s $|\cdot|$. Trivijalnom apsolutnom vrijednošću smatrat ćemo onu za koju je $|x| = 1$ $\forall x \in \mathbb{K}^\times$.*

Definicija 4.0.3. *Ultrametričko polje je uređeni par $(\mathbb{K}, |\cdot|)$ gdje je $\mathbb{K}$ polje, a $|\cdot|$ apsolutna vrijednost koja zadovoljava jaku nejednakost trokuta, tj.*

$$|x+y| \leq \ max\{|x|, |y|\} \leq |x| + |y| \ \forall x, y \in \mathbb{K}.$$

Iskažimo sada neka svojstva apsolutne vrijednosti na polju $\mathbb{K}$ čiji dokaz izostavljamo.

Propozicija 4.0.4. *Neka je $x \mapsto |x|$ apsolutna vrijednost na polju $\mathbb{K}$. Tada vrijedi:*
1) funkcija $d(x, y) = |x - y|$ je metrika na $\mathbb{K}$.
2) $\forall\ 0 < \alpha \leq 1$ preslikavanje $x \mapsto |x|^\alpha$ također je apsolutna vrijednost.
3) Ako je $x \mapsto |x|$ ultrametrička apsolutna vrijednost, tada je i $x \mapsto |x|^\alpha$ također ultrametrička apsolutna vrijednost.

Napomena 4.0.5. *Uočimo, $(\mathbb{Q}_p, |\cdot|_p)$ je ultrametričko polje.*

Navedimo bez dokaza teorem koji je Ostrowski dokazao 1916. godine (za polje $\mathbb{Q}$), a daje poveznicu između netrivijane ultrametričke apsolutne vrijednosti na polju $\mathbb{Q}$ i p-adske apsolutne vrijednosti. Dokaz se može pogledati u [3].

Teorem 4.0.6. *(Ostrowski) Neka je $x \mapsto |x|$ netrivijalna ultrametrička apsolutna vrijednost na polju $\mathbb{Q}$. Tada postoji prost broj p i $\alpha \in \mathbb{R}, \alpha > 0$ takvi da vrijedi*

$$|x| = |x|_p^\alpha, \ x \in \mathbb{Q}.$$

Neka je $\mathbb{K}$ konačno proširenje od $\mathbb{Q}_p$ (dakle, nadskup od $\mathbb{Q}_p$ koje je i samo polje). Možemo smatrati $\mathbb{K}$ konačnodimenzionalnim vektorskim prostorom nad poljem $\mathbb{Q}_p$ (bit će zadovoljen *aksiom množenja skalarom* vektorskog prostora). Svaka apsolutna vrijednost koja proširuje p-adsku apsolutnu vrijednost od $\mathbb{Q}_p$ je norma na $\mathbb{K}$, odnosno dobivamo normirani prostor $(\mathbb{K}, |\cdot|)$. Sljedeća propozicija koju navodimo bez dokaza precizira da postoji najviše jedna takva norma, a dokaz se može pogledati u [3].

Propozicija 4.0.7. *Postoji najviše jedna apsolutna vrijednost na $\mathbb{K}$ koje proširuje p-adsku apsolutnu vrijednost na $\mathbb{Q}_p$.*

Sada ćemo prethodnu propoziciju i razmatranja primijeniti na tzv. konačno *Galoisovo proširenje*, nazvano po francuskom matematičaru Évaristeu Galoisu, jednom od utemeljitelja teorije grupa. Ukratko, konačno Galoisovo proširenje nekoga polja je proširenje koje je algebarsko i separabilno. Napomenimo da se svako konačno proširenje može uložiti u konačno Galoisovo proširenje. Za više o konačnim Galoisovim proširenjima može se pročitati u [1]. Neka je $\mathbb{K}$ konačno Galoisovo proširenje od $\mathbb{Q}_p$ te pretpostavimo da postoji p-adska apsolutna vrijednost na $\mathbb{Q}_p$ koju proširujemo na $\mathbb{K}$. Promatrajmo za svaki automorfizam σ od $K/\mathbb{Q}_p$ apsolutnu vrijednost $|x|' = |\sigma(x)|$. Napomenimo da će $\mathbb{K}$ fiksirati polje $\mathbb{Q}_p$ po svakom automorfizmu. Po prethodnoj propoziciji znamo da postoji najviše jedna apsolutna vrijednost koja će proširiti p-adsku apsolutnu vrijednost. Označimo sada s $G = Gal(K/\mathbb{Q}_p)$ Galoisovu grupu proširenja i za $x \in \mathbb{K}$ promotrimo element

$$N(x) = \prod_{\sigma \in G} \sigma(x) \in \mathbb{Q}_p$$

Sada imamo:

$$|N(x)| = |\prod_{\sigma \in G} \sigma(x)| = \prod_{\sigma \in G} |\sigma x| = |x|^d$$

gdje je $d = [K : \mathbb{Q}_p] = dim_{\mathbb{Q}_p}(K)$. Napomenimo da broj d zovemo *stupanj proširenja*. Dakle, apsolutna vrijednost koja proširuje p-adsku apsolutnu vrijednost je $|x| = |N(x)|^{1/d}$.

Za kraj ovog poglavlja upoznat ćemo se s još dva pojma, *indeksom grananja* i *reziudualnim stupnjem* te vidjeti u kojoj su oni vezi s već spomenutim stupnjem proširenja.

Neka je $\mathbb{K}$ opet konačno proširenje od $\mathbb{Q}_p$, tada je $\mathbb{K}$ lokalno kompaktno i potpuno. Označimo s $R = \{x \in \mathbb{K} \,\big|\, |x| \leq 1\}$. Maksimalni ideal tog prstena je $P = \pi R$ gdje je π element od $\mathbb{K}$ s najvećom apsolutnom vrijednošću takvom da vrijedi $0 < |\pi| = \theta < 1$. Za $k = R/P$ vrijedi da je konačno proširenje od $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}$. (Prisjetimo se *Korolara 1.2.29* koji kaže da je jedinstveni maksimalni ideal od $\mathbb{Z}_p$ upravo $p\mathbb{Z}_p$.) Označimo sada s $f = [k : \mathbb{F}_p] = dim_{\mathbb{F}_p}(k)$. Tada vrijedi

$$k \cong \mathbb{F}_p,\ q = \#(k) = \#(\mathbb{F}_p)^f = p^f.$$

Također, budući da je $p \in P$, vrijedi

$$|p| = 1/p = \theta^e,\ |\pi| = |p|^{1/e}$$

za neki cijeli broj $e \geq 1$.

Definicija 4.0.8. *Broj*

$$f = [k : \mathbb{F}_p] = dim_{\mathbb{F}_p}(k)$$

zvat ćemo rezidualnim stupnjem konačnog proširenja $\mathbb{K}$ od $\mathbb{Q}_p$. Broj

$$e = [|K^\times| : \mathbb{Q}_p^\times] = [|K^\times| : p^Z] = \#(|K^\times|/p^Z)$$

zvat ćemo indeksom grananja.

Za kraj istaknimo teorem koji daje vezu između brojeva f i g iz prethodne definicije, a dokaz tog teorema može se pogledati u [3].

Teorem 4.0.9. *Za svako konačno proširenje $\mathbb{K}$ od $\mathbb{Q}_p$ vrijedi*

$$fe = [K : \mathbb{Q}_p],$$

gdje su oznake kao u Definiciji 4.0.8 .

Primjer 4.0.10. *Pogledajmo proširenje $\mathbb{Q}_3(\sqrt{3})$.*
Iz Poglavlja 3. znamo da $\sqrt{3} \notin \mathbb{Q}_3$. Proširenje $\mathbb{Q}_3(\sqrt{3})$ je proširenje stupnja 2 koje je konačno Galoisovo proširenje. Naime, proširenje polja karakteristike 0 kakvo je $\mathbb{Q}_p$ je separabilno, a generirano je svim korijenima jednadžbe $X^2 - 3 = 0$ pa je normalno. Galoisova grupa proširenja ima dva elementa, a netrivijalni automorfizam fiksira $\mathbb{Q}_3$ te $\sqrt{3}$ preslikava u $-\sqrt{3}$. Nadalje, uočimo da je

$$|a + b\sqrt{3}| = |(a + b\sqrt{3})(a - b\sqrt{3})|_3^{1/2} = |a^2 - 3b^2|_3^{1/2} \leq max\{|a|_3, 3^{-1/2}|b|_3\}$$

Vidimo da je maksimalna vrijednost, strogo manja od 1, koja se postiže $\frac{1}{\sqrt{3}}$ za $\sqrt{3}$. Dakle, π sa diskusije na početku stranice jednak je $\sqrt{3}$. Kako je $|3| = 1/3 = (\frac{1}{\sqrt{3}})^2 = |\sqrt{3}|^2$, imamo $e = 2$, a iz prethodnog teorema sada slijedi $ef = 2$, tj. $f = 1$.

Bibliografija

[1] S. Lang, *Algebra*, Springer-Verlag, 2002.

[2] F. Najman, *Algebarske strukture - bilješke s vježbi*, 2011., https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASvjezbe.pdf.

[3] A. M. Robert, *A course in p-adic analysis*, Springer, 2000.

[4] B. Širola, *Algebarske strukture*, https://web.math.pmf.unizg.hr/nastava/alg_prof/predavanja/ASpred.pdf.

Sažetak

U ovom smo se radu bavili proučavanjem p-adskih brojeva koje je prvi puta opisao njemački matematičar Kurt Hensel 1897. godine. Skup p-adskih brojeva opisali smo u kontekstu teorije skupova, algebre i metričkoga prostora. Prvo smo krenuli od prstena $\mathbb{Z}_p$ p-adskih cijelih brojeva, a budući da smo pokazali da je $\mathbb{Z}_p$ integralna domena, proširili smo $\mathbb{Z}_p$ na polje razlomaka koje smo označavali sa $\mathbb{Q}_p$. Vidjeli smo da je na $\mathbb{Q}_p$ moguće definirati ultrametriku. Iskazali smo i dokazali jednu od osnovnih tvrdnji vezanu za p-adske brojeve, *Henselovu lemu*, koja govori da možemo doći do jedinstvenog rješenja jednadžbe $P(x) = 0$ za polinom $P \in \mathbb{Z}_p[x]$. Vidjeli smo da je *Henselova lema* usko vezana na *Newtonovu metodu* pronalaženja aproksimacije nultočki. Dotaknuli smo se kvadratnih proširenja polja $\mathbb{Q}_p$ kao direktne posljedice *Henselove leme*. Na kraju smo proučavali algebarska proširenja p-adskih brojeva i vidjeli primjer konačnog Galoisovog proširenja.

Summary

In this master's thesis we study p-adic numbers which were first described by Kurt Hensel, German mathematician, in 1897. We describe the set of p-adic numbers in context of set theory, algebra and metric spaces. First we observe the ring of p-adic integers, denoted by $\mathbb{Z}_p$. Ring $\mathbb{Z}_p$ is shown to be an integral domain, so it's possible to define the field of fractions of $\mathbb{Z}_p$, which we denote by $\mathbb{Q}_p$. Also, we define an ultrametrics on $\mathbb{Q}_p$. We give a proof of *Hensel's lemma*, one of the fundamental statements of p-adic theory, which shows that there is an unique solution of $P(x) = 0$ for $x \in \mathbb{Z}_p$ and $P \in \mathbb{Z}_p[x]$. Also, we observe some connections between *Newton's method* for finding an approximate solutions for $f(x) = 0$, and *Hensel's lemma*. As direct consequence of *Hensel's lemma* we observe quadratic extensions of $\mathbb{Q}_p$. In the very end of this paper, we study algebraic extensions of p-adic numbers and show an example of a finite Galois extension.

Životopis

Rođena sam 1998. godine u Osijeku. Osnovnu školu završila sam u Ladimirevcima. Nakon završene osnovne škole, 2013. godine upisala sam III. gimnaziju Osijek, prirodoslovno-matematičku gimnaziju. Na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu 2017. godine upisala sam *Preddiplomski sveučilišni studij Matematika*. Diplomu sveučilišnog prvostupnika matematike stekla sam 2020. godine završivši preddiplomski studij. Iste godine upisujem diplomski studij *Financijska i poslovna matematika* također na PMF-MO. Osim neizmjernog interesa za prirodoslovne predmete, posebice za matematiku, oduvijek gajim interes i za neka druga područja. Posebice me interesiraju psihologija, filozofija i književnost. Također, u 2019. godini u sklopu studentske amaterske radionice bavila sam se glumom.